

Data Warehouse Service (DWS)
8.1.3.331

Fault Management

Issue 02
Date 2024-05-30



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 Troubleshooting.....	1
1.1 Overview.....	1
1.1.1 Troubleshooting Principles.....	1
1.1.2 Troubleshooting Process.....	2
1.2 Information Collection.....	4
1.2.1 Precautions.....	4
1.2.2 Collecting Basic Information.....	4
1.3 Faults on the Management Side.....	6
1.3.1 UI.....	6
1.3.1.1 GaussDB(DWS) Cluster Monitoring Information Is Not Displayed on Cloud Eye.....	6
1.3.1.2 Flavors Are Not Displayed After GaussDB(DWS) Is Installed.....	8
1.3.1.3 Disk Capacity Displayed on the Cluster Page Is Abnormal.....	12
1.3.1.4 Status of Some Clusters on the GaussDB(DWS) Console Is Abnormal.....	15
1.3.1.5 No GaussDB(DWS) Pod Monitoring Data Is Displayed on ManageOne Maintenance Portal.....	16
1.3.1.6 Cluster Creation Task Failed with Error Code DWS.0105.....	18
1.3.1.7 Displayed DR Status Is Abnormal After the Production Cluster Is Faulty and Recovered.....	19
1.3.2 Cluster.....	20
1.3.2.1 Failed to Create a Cluster.....	20
1.3.2.2 GaussDB(DWS) BMS Cluster Fails to Be Created Due to Mutual Trust Problems.....	22
1.3.2.3 GaussDB(DWS) BMS Cluster Fails to Be Created Due to Insufficient Underlying Resources.....	24
1.3.2.4 GaussDB(DWS) ECS Cluster Fails to Be Created Due to Insufficient ECS Resources.....	26
1.3.2.5 Failed to Create a GaussDB(DWS) Cluster Because the Management Tenant Password Is Changed.....	28
1.3.2.6 Management Side Cannot Communicate with the Internal Public Network Plane.....	31
1.3.2.7 BMS Cluster Fails to Be Created Due to Tenant Name Change.....	32
1.3.2.8 Node Status Fails to Be Changed During Cluster Scale-out.....	34
1.3.2.9 Redistribution Is Suspended Because the Cluster Is Degraded.....	35
1.3.2.10 Failed to Create a BMS Cluster Because the BMS RAID Group Is Incorrectly Configured.....	37
1.3.2.11 Failed to Create a BMS Cluster Because the New Network Segments Are Not Added to the API Gateway Whitelist.....	39
1.3.3 Connectivity.....	41
1.3.3.1 EIP Cannot Be Used Due to Lost Policy Route.....	41
1.3.3.2 Network Disconnection Between DWS and SwiftAdapter.....	42
1.3.4 Snapshot.....	44

1.3.4.1 Backing Up Tenant Plane Data to OBS After Switching to the OBS Scenario.....	44
1.3.4.2 Failed to Create a Snapshot.....	49
1.3.4.3 Failed to Restore a Cluster Using Its Snapshot.....	52
1.3.5 Upgrade.....	53
1.3.5.1 Cluster Upgrade Is Interrupted Due to Packet Delivery Errors.....	54
1.3.5.2 Failed to Upgrade the Cluster.....	56
1.3.5.3 Agent Upgrade Fails.....	57
1.3.5.4 Failed to Upgrade Microservices on the Management Side Because Other Cloud Services Occupy Resources of the CloudAutoDeploy-CDK Nodes.....	58
1.3.6 Instance.....	60
1.3.6.1 EIP Is Unreachable After a Cluster Is Created.....	60
1.3.7 Monitoring.....	61
1.3.7.1 Monitoring Metrics Have Expired.....	61
1.3.7.2 No Monitoring Information Is Displayed on the Monitoring Panel of the GaussDB(DWS) Cluster and an Interface Exception Is Reported.....	64
1.3.8 Others.....	67
1.3.8.1 Abnormal VM Resource Usage.....	67
1.4 Faults on the Tenant Side.....	69
1.4.1 Storage.....	69
1.4.1.1 Skewed Data Is Detected During Routine Inspection and the Disk Usage of Some Nodes Is High.....	69
1.4.1.2 CN Cannot be Connected Because It Is in the down State.....	71
1.4.1.3 Disk Usage Is High and Data Needs to Be Cleared.....	72
1.4.1.4 CN Disk Is Full Because Audit Logs or Logs Are Not Compressed.....	73
1.4.2 Cluster.....	74
1.4.2.1 Low Cluster Performance Displayed on the WebUI.....	74
1.4.2.2 Account Locked.....	75
1.4.2.3 Viewing Audit Logs.....	77
1.4.2.4 An Error Is Reported During Statement Execution, Indicating that the User Does Not Have the Permissions on the Table.....	78
1.4.2.5 Querying Whether a User Has Permissions on a Table.....	79
1.4.2.6 Node Is Faulty Because the Instance Directory Is Deleted.....	81
1.4.2.7 Scale-out Fails on the Tenant Side After the Console on the Management Side Is Upgraded to 8.1.....	83
1.4.2.8 O&M Commands Occasionally Fail to Be Delivered When the Node Machine Is Restarted.....	84
1.4.2.9 An Error Message Is Displayed When a Command Fails to Be Delivered During DMS Configuration.....	85
1.4.3 Communication.....	86
1.4.3.1 Failed to Connect to the Database of the Cluster.....	87
2 Alarm Handling.....	90
2.1 Alarms on the Management Side.....	90
2.1.1 DWS_00001 Script Execution Exception.....	90
2.1.2 DWS_00002 Database Operation Exception.....	93
2.1.3 DWS_00003 Calling IAM Component Failed.....	96

2.1.4 DWS_00004 Failed to Call the IaaS Component.....	99
2.1.5 DWS_00006 Failed to Call the OBS Component.....	107
2.1.6 DWS_00007 REST Component Call Exception.....	110
2.1.7 DWS_00008 Database Internal Exception.....	111
2.1.8 DWS_00009 Failed to Call the DNS Component.....	113
2.1.9 DWS_00010 Snapshot Operation Exception.....	116
2.1.10 DWS_00011 Upgrade Operation Exception.....	118
2.1.11 DWS_00012 Service Node Overloaded.....	120
2.1.12 DWS_00013 Service Certificate Expiration.....	122
2.1.13 DWS_01008 Node Status Fault.....	124
2.1.14 DWS_01010 Cluster Status Is Abnormal.....	127
2.1.15 ECF_01015 Abnormal ECF Monitor Status.....	130
2.1.16 DWS_01016 Failed to Update the Status.....	132
2.1.17 DWS_02002 Cluster Operations Are Abnormal.....	136
2.1.18 DWS_02020 Cluster Redistribution Failed.....	138
2.1.19 DWS_02021 Failed to Pause Cluster Redistribution.....	141
2.1.20 DWS_02022 DMS Kafka Service Unavailable.....	143
2.1.21 DWS_02030 Inconsistent Agent Versions.....	145
2.1.22 DWS_02040 Failed to Synchronize GUC Parameters.....	147
2.1.23 DWS_02070 DWS Failed to Automatically Update the External Data Source Configuration.....	149
2.1.24 DWS_10000 Internal System Exception.....	151
2.1.25 DWS_20003 Cluster Creation Exception.....	153
2.1.26 DWS_20100 Cluster Deletion Exception.....	160
2.1.27 DWS_20200 Failed to Update the AK and SK of the Management Tenant of an Instance.....	162
2.1.28 DWS_20210 Failed to Deliver the Operator Spill Threshold After Disk Capacity Expansion.....	164
2.1.29 DWS_20220 Scale-out Failed.....	165
2.1.30 DWS_20221 Scheduling Task Failed After Resizing a Cluster.....	167
2.1.31 DWS_21110 GaussDB(DWS) Data Migration Task Status Abnormal.....	169
2.1.32 DWS_22001 GaussDB(DWS) Audit Log Dump Exception.....	171
2.1.33 DWS_23001 Inconsistent Resource (Abnormal Cluster) Status.....	173
2.1.34 DWS_23002 Inconsistent Resource (Normal Node) Status.....	175
2.1.35 DWS_23003 Inconsistent Resource (Abnormal Node) Status.....	177
2.1.36 DWS_23052 GaussDB(DWS) Resource Tenant Bucket Freezing/Unfreezing Exception.....	180
2.1.37 DWS_23053 GaussDB(DWS) Resource Tenant Bucket Usage Synchronization Exception.....	181
2.1.38 DWS_24001 Root Directory of the System Disk in the GaussDB(DWS) Cluster Is Not Automatically Expanded.....	183
2.1.39 DWS_30000 GaussDB(DWS) License Is About to Exceed the Threshold.....	185
2.1.40 DWS_30001 DWS License Exceeded Authorized Capacity.....	187
2.1.41 DWS_30002 DWS License Charging Item Is Used but Not Registered.....	188
2.1.42 DWS_41000 Failed to Scale In a GaussDB(DWS) Physical Cluster.....	190
2.1.43 DWS_41001 Fine-grained Restoration Failed.....	192
2.1.44 DWS_41002 Failed to Restore a Snapshot to the Original Cluster.....	193
2.1.45 DWS_50000 Failed to Change Cluster Specifications.....	194

2.1.46 DWS_60000 Failed to Create DR.....	197
2.1.47 DWS_60001 Failed to Start DR.....	198
2.1.48 DWS_60002 Failed to Stop DR.....	200
2.1.49 DWS_60003 Failed to Switch to the DR Cluster.....	202
2.1.50 DWS_60004 Failed to Restore the DR Relationship.....	203
2.1.51 DWS_60005 Failed to Delete the DR Task.....	205
2.1.52 DWS_60006 DWS Logical Cluster Task Failed.....	206
2.1.53 DWS_60007 Failed to Synchronize cgroup Information During DR.....	208
2.1.54 DWS_60016 Failed to Invoke GaussDB(DWS) OpenAPI.....	210
2.1.55 DWS_60017 GaussDB(DWS) DMS-AGENT Process Is Abnormal.....	211
2.1.56 DWS_89002 Failed to Obtain Managed Cluster Information Through the FIM Interface.....	212
2.1.57 1078919294 ECF Monitor Pod Status Alarm.....	214
2.1.58 1078919295 ECF Insight Pod Status Alarm.....	216
2.1.59 1078919297 ECF Event Pod Status Alarm.....	218
2.1.60 1078919298_ECF Cluster Manager Pod Status Alarm.....	219
2.1.61 1078919299 DWS Controller Pod Status Alarm.....	221
2.1.62 Querying Logs Based on the Alarm Generation Time.....	223
2.1.63 DWS_2000000001_OM Node CPU Usage Exceeds the Threshold.....	224
2.1.64 DWS_2000000002_OM Node System CPU Usage Exceeds the Threshold.....	226
2.1.65 DWS_2000000004_OM Node System Disk Usage Exceeds the Threshold.....	228
2.1.66 DWS_2000000005_OM Node Log Disk Usage Exceeds the Threshold.....	229
2.1.67 DWS_2000000006_OM Node Data Disk Usage Exceeds the Threshold.....	231
2.1.68 DWS_2000000007_OM Node System Disk I/O Usage Exceeds the Threshold.....	232
2.1.69 DWS_2000000008_OM Node Log Disk I/O Usage Exceeds the Threshold.....	234
2.1.70 DWS_2000000009_OM Node Data Disk I/O Usage Exceeds the Threshold.....	236
2.1.71 DWS_2000000010_OM Node System Disk Latency Exceeds the Threshold.....	237
2.1.72 DWS_2000000011_OM Node Log Disk Latency Exceeds the Threshold.....	239
2.1.73 DWS_2000000012_OM Node Data Disk Latency Exceeds the Threshold.....	241
2.1.74 DWS_2000000013_OM Node System Disk Inode Usage Exceeds the Threshold.....	242
2.1.75 DWS_2000000014_OM Node Log Disk Inode Usage Exceeds the Threshold.....	244
2.1.76 DWS_2000000015_OM Node Data Disk Inode Usage Exceeds the Threshold.....	245
2.1.77 DWS_2000000016_OM Data Spilled to Disks of the Query Statement Exceeds the Threshold.....	247
2.1.78 DWS_2000000017_OM Number of Queuing Query Statements Exceeds the Threshold.....	249
2.1.79 DWS_2000000018_OM Queue Congestion in the Default Cluster Resource Pool.....	250
2.1.80 DWS_2000000019_OM High TCP Retransmission Rate After Packet Loss.....	252
2.1.81 DWS_2000000020_OM Long SQL Probe Execution Duration in a Cluster.....	253
2.1.82 DWS_2000000022_OM Monitoring Metric Is Not Reported for Too Many Periods.....	255
2.1.83 DWS_2000000023_OM A Vacuum Full Operation That Holds a Table Lock for A Long Time Exists in the Cluster.....	257
2.1.84 DWS_2000000024_OM Residual SQL Threads Exist in the Cluster.....	259
2.1.85 DWS_2000000025_OM GaussDB(DWS) Cluster Job Execution Duration Exceeds the Threshold....	261
2.1.86 DWS_2000000026_OM Data Written by CNs in a DWS Cluster Exceeds the Threshold.....	262
2.1.87 DWS_25xxxxxxxx User-Defined Threshold Alarms.....	264

2.1.88 TASKMGR_00001 Alarm Sending Failure.....	266
2.2 Alarms on the Tenant Side.....	268
2.2.1 Logging In to a Node in the Tenant Cluster.....	268
2.2.2 Querying MySQL Database Information.....	274
2.2.3 1078853633 Missing Data Directory or Redo Log Directory on Data Instance (ALM_AI_MissingDataInstDataOrRedoDir).....	275
2.2.4 1078919169 Data Instance Connections Exceed the Threshold (ALM_AI_TooManyDataInstConn) ..	277
2.2.5 1078919170 GTM Instance Abnormal (ALM_AI_AbnormalGTMInst).....	280
2.2.6 1078919172 DN Abnormal (ALM_AI_AbnormalDatanodeInst).....	283
2.2.7 1078919176 GTM Process Abnormal (ALM_AI_AbnormalGTMProcess).....	286
2.2.8 1078919177 CN Process Abnormal (ALM_AI_AbnormalCoordinatorProcess).....	289
2.2.9 1078919184 DN Process Abnormal (ALM_AI_AbnormalDatanodeProcess).....	292
2.2.10 1078919221 Cluster Table Skew (ALM_AI_AbnormalTableSkewness).....	296
2.2.11 1078919224 Imbalanced Cluster Load (ALM_AI_UnbalancedCluster).....	298
2.2.12 1078919226 CM_Agent Process Abnormal (ALM_AI_AbnormalCMAProcess).....	304
2.2.13 1078919227 CM_Server Process Abnormal (ALM_AI_AbnormalCMSProcess).....	308
2.2.14 1078919231 Inconsistent MTU Values (ALM_AI_AbnormalMTUValue).....	311
2.2.15 1078919239 Abnormal DataNode Disk (ALM_AI_AbnormalDataInstDisk).....	314
2.2.16 1078919242 Failed to Create Connection for Database Service (ALM_AI_AbnormalPhonyDead) ..	315
2.2.17 1078919243 CM_Agent Failed to Connect to the Database (ALM_AI_AbnormalCmaConnFail) ..	318
2.2.18 1078919245 Failed to Recreate the DN (ALM_AI_AbnormalBuild).....	321
2.2.19 1078919246 Process Restarts Abnormally (ALM_AI_INS_RESTART).....	324
2.2.20 1078919256 Database Node Runs Too Slowly (ALM_AI_SLOWNODE).....	327
2.2.21 1078919257 gRPC Certificate File Does Not Exist (ALM_AI_AbnormalGrpcKey).....	330
2.2.22 1078919258 Cluster Read-only (ALM_AI_ReadOnlyMode).....	334
2.2.23 1078919260 Disk Usage Is Too High (ALM_AI_DiskRatioHigh).....	337
2.2.24 1078919264 Remaining Database Disk Capacity Warning (ALM_AI_DiskUsageRisk).....	339
2.2.25 1078919265 Remaining Database Disk Capacity Is Insufficient (ALM_AI_DiskUsageReadOnly)....	342
2.2.26 1078919266 Remaining Database Disk Capacity Is Severely Insufficient (ALM_AI_DiskUsageDanger).....	344
2.2.27 1078919267 Failed to Start DMS Agent.....	347
2.2.28 1078919270 Failed to Install the Plug-In (ALM_AI_InstallPluginFailed).....	349
2.2.29 1078919280 DN Log Redo Operations Are Slow (ALM_AI_DatanodeRedoSlow).....	352
2.2.30 1078919290 Cluster Instance OS Is Restarted (ALM_AI_OSReboot).....	356
2.2.31 1078919300 Failed to Create a Table (ALM_AI_CreateTableFail).....	358
2.2.32 1078919301 Failed to Start the Plug-in (ALM_AI_StartPluginFailed).....	361
2.2.33 1078919306 gs_scheduler Process Abnormal.....	363
2.2.34 1078919307 Big Data Framework Process Abnormal.....	366
2.2.35 1078919309 Table Data Is Damaged in the GaussDB (DWS) Cluster During Data Verification.....	369
2.2.36 1078919310 Table Data Is Damaged After Incremental Build of the GaussDB (DWS) Cluster.....	372
2.2.37 2078918234 D (Dead) Processes or Z (Zombie) Processes Exist on DNs (ALM_AI_AbnormalProcess) ..	375

2.2.38 2078918236 Intermittent Network Disconnection or Network Delay Between DWS Nodes (ALM_AI_AbnormalNetwork).....	377
2.2.39 2078919291 Data Instance Generates Core Files (ALM_AI_CoreFile).....	379
2.2.40 6000000000 GDS-KAFKA Pipeline Abnormal.....	383
2.3 Alarms of Managed Physic Machine Clusters.....	385
2.3.1 Description.....	385
2.3.2 ALM-12001 Audit Log Dump Failure.....	385
2.3.3 ALM-12004 OLdap Resource Is Abnormal.....	388
2.3.4 ALM-12005 OKerberos Resource Is Abnormal.....	390
2.3.5 ALM-12006 Node Fault.....	393
2.3.6 ALM-12007 Process Fault.....	396
2.3.7 ALM-12010 Manager Heartbeat Interruption Between the Active and Standby Nodes.....	399
2.3.8 ALM-12011 Data Synchronization Exception Between the Active and Standby Manager Nodes....	402
2.3.9 ALM-12012 NTP Service Is Abnormal.....	405
2.3.10 ALM-12014 Device Partition Lost.....	412
2.3.11 ALM-12015 Device Partition File System Read-Only.....	415
2.3.12 ALM-12016 CPU Usage Exceeds the Threshold.....	416
2.3.13 ALM-12017 Insufficient Disk Capacity.....	420
2.3.14 ALM-12018 Memory Usage Exceeds the Threshold.....	424
2.3.15 ALM-12027 Host PID Usage Exceeds the Threshold.....	426
2.3.16 ALM-12028 Number of Processes in the D State on the Host Exceeds the Threshold.....	428
2.3.17 ALM-12029 Invalid License File.....	431
2.3.18 ALM-12030 No Valid License.....	433
2.3.19 ALM-12033 Slow Disk Fault.....	435
2.3.20 ALM-12034 Periodic Backup Failure.....	441
2.3.21 ALM-12035 Unknown Data Status After a Restoration Task Fails.....	444
2.3.22 ALM-12036 License File About to Expire.....	446
2.3.23 ALM-12037 NTP Server Is Abnormal.....	448
2.3.24 ALM-12038 Monitoring Indicator Dump Failure.....	451
2.3.25 ALM-12039 Data Inconsistency Between the Active and Standby OMS Databases.....	454
2.3.26 ALM-12040 Insufficient System Entropy.....	457
2.3.27 ALM-12041 Critical File Permission Is Abnormal.....	459
2.3.28 ALM-12042 Critical File Configuration Is Abnormal.....	462
2.3.29 ALM-12045 Read Packet Dropped Rate Exceeds the Threshold.....	465
2.3.30 ALM-12046 Write Packet Dropped Rate Exceeds the Threshold.....	471
2.3.31 ALM-12047 Read Packet Error Rate Exceeds the Threshold.....	474
2.3.32 ALM-12048 Write Packet Error Rate Exceeds the Threshold.....	477
2.3.33 ALM-12049 Read Throughput Rate Exceeds the Threshold.....	480
2.3.34 ALM-12050 Write Throughput Rate Exceeds the Threshold.....	483
2.3.35 ALM-12051 Disk Inode Usage Exceeds the Threshold.....	487
2.3.36 ALM-12052 Usage of Temporary TCP Ports Exceeds the Threshold.....	489
2.3.37 ALM-12053 Host File Handle Usage Exceeds the Threshold.....	492
2.3.38 ALM-12054 The Certificate File Is Invalid.....	495

2.3.39 ALM-12055 The Certificate File Is About to Expire.....	498
2.3.40 ALM-12057 Metadata Not Configured with the Task to Periodically Back Up Data to a Third-Party Server.....	501
2.3.41 ALM-12058 License Is Not Bound to SnS.....	503
2.3.42 ALM-12059 SnS of the License Is About to Expire.....	505
2.3.43 ALM-12060 SnS of the License Has Expired.....	508
2.3.44 ALM-12061 Process Usage Exceeds the Threshold.....	510
2.3.45 ALM-12062 OMS Parameter Configurations Mismatch with the Cluster Scale.....	514
2.3.46 ALM-12063 Unavailable Disk.....	516
2.3.47 ALM-12064 Host Random Port Range Conflicts with FusionInsight Used Port.....	519
2.3.48 ALM-12066 Inter-Node Mutual Trust Fails.....	521
2.3.49 ALM-12067 Tomcat Resource Is Abnormal.....	523
2.3.50 ALM-12068 ACS Resource Is Abnormal.....	525
2.3.51 ALM-12069 AOS Resource Is Abnormal.....	527
2.3.52 ALM-12070 Controller Resource Is Abnormal.....	530
2.3.53 ALM-12071 Httpd Resource Is Abnormal.....	532
2.3.54 ALM-12072 Floating IP Address Resource Is Abnormal.....	534
2.3.55 ALM-12073 CEP Resource Is Abnormal.....	536
2.3.56 ALM-12074 FMS Resource Is Abnormal.....	539
2.3.57 ALM-12075 PMS Resource Is Abnormal.....	541
2.3.58 ALM-12076 GaussDB Resource Is Abnormal.....	543
2.3.59 ALM-12077 User Omm Expired.....	546
2.3.60 ALM-12078 Password of User Omm Expired.....	548
2.3.61 ALM-12079 User omm Is About to Expire.....	550
2.3.62 ALM-12080 Password of User omm Is About to Expire.....	552
2.3.63 ALM-12081 User ommdba Expired.....	554
2.3.64 ALM-12082 User ommdba Is About to Expire.....	556
2.3.65 ALM-12083 Password of User ommdba Is About to Expire.....	558
2.3.66 ALM-12084 Password of User ommdba Expired.....	560
2.3.67 ALM-12085 Service Audit Log Dump Failure.....	562
2.3.68 ALM-12087 System Is in the Upgrade Observation Period.....	565
2.3.69 ALM-12089 Network Connection Between Nodes Is Abnormal.....	567
2.3.70 ALM-12099 Core Dump Occurs.....	569
2.3.71 ALM-25000 LdapServer Service Unavailable.....	571
2.3.72 ALM-25004 Abnormal LdapServer Data Synchronization.....	574
2.3.73 ALM-25005 Abnormal Nscd Service.....	577
2.3.74 ALM-25006 Abnormal Sssd Service.....	581
2.3.75 ALM-25500 KrbServer Service Unavailable.....	585
2.3.76 ALM-37000 MPPDBServer Data Directory or Redo Directory Is Missing.....	588
2.3.77 ALM-37001 Redo Logs of the MPPDBServer Instance Are Missing.....	590
2.3.78 ALM-37002 Number of MPPDB Instance Connections Exceeds the Threshold.....	593
2.3.79 ALM-37003 Asynchronous or Disconnected Primary and Standby GTM Instances.....	595
2.3.80 ALM-37004 Asynchronous or Disconnected Primary and Standby DataNode Instances.....	597

2.3.81 ALM-37005 GTM Process Is Abnormal.....	600
2.3.82 ALM-37006 Coordinator Node Process Is Abnormal.....	601
2.3.83 ALM-37007 DataNode Process Is Abnormal.....	605
2.3.84 ALM-37008 MPPDB Service Unavailable.....	607
2.3.85 ALM-37012 HA Listening Socket of MPPDBServer Instances Is Abnormal.....	609
2.3.86 ALM-37013 MPPDBServer Instance Socket Is Abnormal.....	612
2.3.87 ALM-37014 Lock File of the GaussDB Process Already Exists.....	615
2.3.88 ALM-37015 Insufficient File Handles for the GaussDB Process.....	618
2.3.89 ALM-37016 Xlog Archive Command Fails to Be Executed on the MPPDBServer.....	621
2.3.90 ALM-37017 Number of Database Connections Exceeds the Upper Limit.....	623
2.3.91 ALM-37018 User Is Connected to Excessive Databases.....	626
2.3.92 ALM-37019 Connection Between MPPDBServer Data Instances and GTM Is Abnormal.....	629
2.3.93 ALM-37020 MPPDBServer Connection Authentication Is Abnormal.....	632
2.3.94 ALM-37021 CM_SERVER Process Is Abnormal.....	634
2.3.95 ALM-37022 CM_AGENT Process Is Abnormal.....	636
2.3.96 ALM-37024 Clusters Are Unbalanced.....	638
2.3.97 ALM-37026 MTU Values Are Inconsistent.....	644
2.3.98 ALM-37027 Feature Vector Training Encoding Service Platform Is Unavailable.....	646
2.3.99 ALM-37028 NIC Multi-Queue Is Not Configured.....	649
2.3.100 ALM-37029 MPPDB Service Is Unavailable.....	652
2.3.101 ALM-37031 CM_AGENT Connecting to the Database Failed.....	654
2.3.102 ALM-37032 Creating Connections for Database Service Failed.....	656
2.3.103 ALM-37033 DN Disk Is Faulty.....	657
2.3.104 ALM-37034 Rebuilding DN Failed.....	659
2.3.105 ALM-37035 Cluster Node Is Running Slowly.....	661
2.3.106 ALM-37036 Data Skew Occurs During MPPDBServer Data Import.....	663
2.3.107 ALM-37037 Features Are Not Authorized by the License.....	665
2.3.108 ALM-37039 Connecting to the KMS Service Failed.....	667
2.3.109 ALM-37040 TDE Key File Is Damaged.....	669
2.3.110 ALM-37041 TDE Key Verification Error Occurs.....	672
2.3.111 ALM-37042 MPPDB Client Version Does Not Match the Kernel Version.....	673
2.3.112 ALM-37043 GaussDB AD Users Conflict with Each Other Or Are Invalid.....	675
2.3.113 ALM-37044 GaussDB Failed to Connect to the AD Service.....	677
2.3.114 ALM-37045 GRPC Certificate File Does Not Exist.....	678
2.3.115 ALM-37046 THP Is Running.....	681
2.3.116 ALM-37047 DN Log Redo Operations Are Slow.....	683
2.3.117 ALM-45170 DMSCollector Instance Is Abnormal.....	686
2.3.118 Technical Support.....	687
3 Appendixes.....	689
3.1 Logging In to a Node in the Tenant Cluster.....	689
3.2 Logging In to the CloudAutoDeploy-CDK Master Node.....	695
3.3 Querying MySQL Database Information.....	696

3.4 Logging In to the rms Database on the Management Side.....	697
3.5 Logging In to a dwscontroller Pod.....	697
3.6 Logging In to the GaussDB Database of DMS.....	698
3.7 Collecting dwscontroller Logs.....	699

1 Troubleshooting

1.1 Overview

1.1.1 Troubleshooting Principles

- Principles for Fault Analysis, Locating, and Troubleshooting
 - Recover services as soon as possible.
 - Collect fault information promptly and save it to a portable storage device or another computer on the network.
 - When formulating a troubleshooting scheme, evaluate the impact to ensure service continuity.
 - If a fault occurs on a third-party hardware device, view the documentation of the device or call the service hotline of the supplier for assistance.
 - If a fault cannot be located or rectified as instructed by the documentation, contact technical support to minimize service interruption.
- Precautions
 - Strictly comply with operation regulations and industrial safety regulations to ensure personnel and equipment safety.
 - Analyze the fault symptom, identify the cause, and then rectify the fault. If the causes are unknown, exercise caution to prevent the problem from worsening.
 - Record all onsite information of a fault before troubleshooting. Do not delete any data or log.
 - Obtain the customer's authorization before collecting logs to ensure security and privacy of the customer's network.
 - Before making any modifications, back up data manually or using a script.
 - Take electrostatic discharge (ESD) prevention measures, for example, wearing an ESD wrist strap when replacing or maintaining devices.

- Record the original information about any problem encountered during maintenance.
- Record all important operations, such as process restart, ensure the feasibility of the operations, back up relevant data, and take emergency and safety measures before the qualified personnel perform these operations.
- After the system recovers, observe the system running status to confirm that the fault is rectified. Then, complete a report in a timely manner.
- Exercise caution when performing high-risk operations and running high-risk commands.
- Requirements for Maintenance Personnel
 - Have basic knowledge of network equipment, OSs, and database management. Be adept at using commonly used commands to monitor and maintain the system.
 - Understand the logical structure of the on-site GaussDB(DWS) system, mappings between each component of the GaussDB(DWS) system and the on-site devices, and cable connections between on-site devices.
 - Be familiar with the service processes and system structure of GaussDB(DWS) and be skilled in using the related components.
 - Know how to locate and rectify the fault.
 - Know how to remotely access the system.

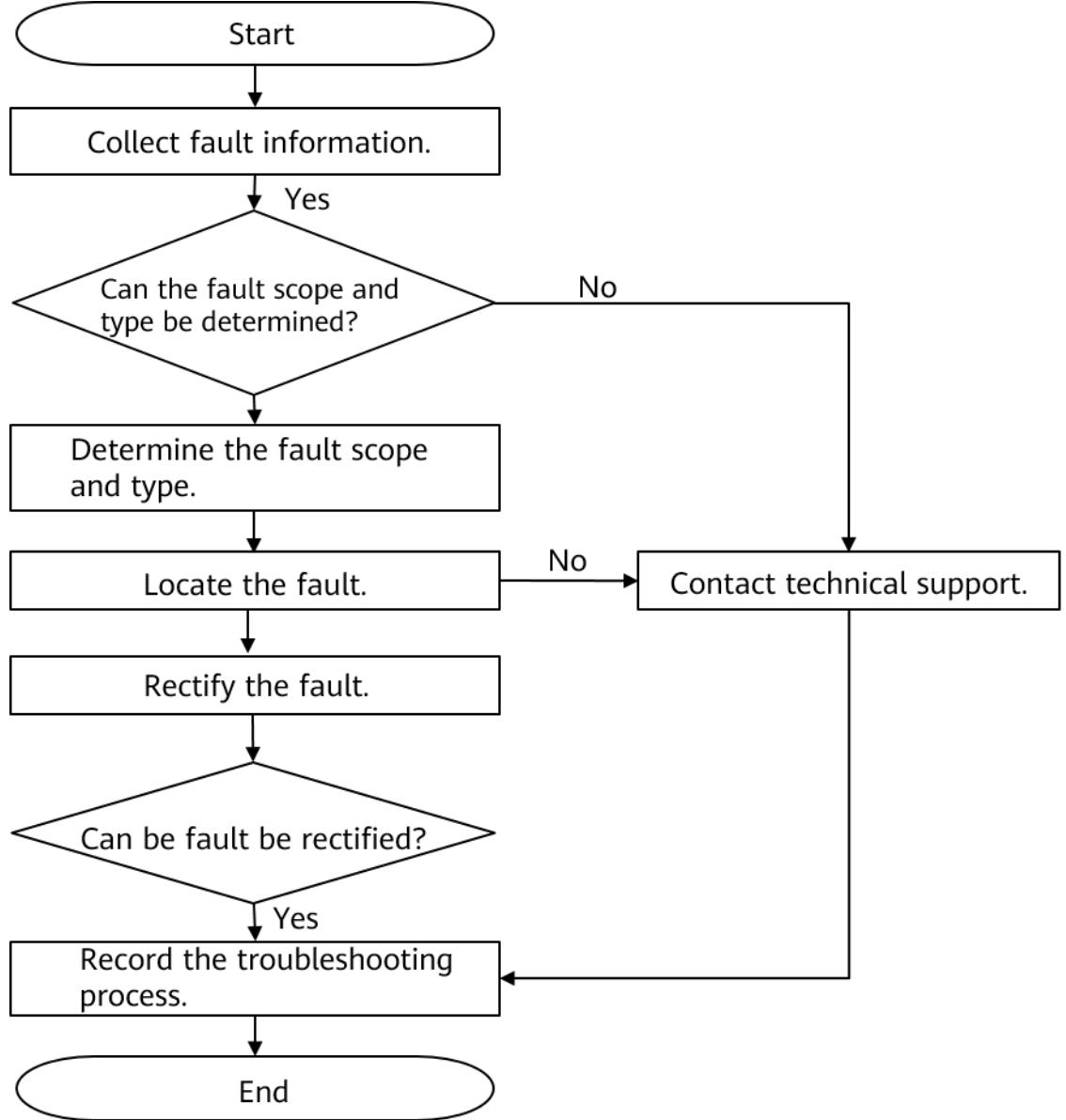
1.1.2 Troubleshooting Process

The troubleshooting process consists of the following operations: collecting fault information, determining the fault scope and type, locating the fault, and rectifying the fault. [Figure 1-1](#) shows the process.

NOTE

1. When a serious system fault occurs, contact Huawei technical support for the most appropriate troubleshooting solution.
2. During the troubleshooting, maintenance engineers may perform operations that may affect service data, such as modifying configuration data and restarting VMs. Therefore, to ensure data security, save onsite data and back up related databases, alarm information, and log files before the troubleshooting.

Figure 1-1 Troubleshooting process



Collecting Fault Information

Collect as much fault information as possible to help maintenance engineers locate and handle faults.

Determining the Fault Scope and Type

Determine the scope and type of the fault based on the collected fault information before rectifying the fault.

Locating the Fault

Identify the possible causes for the fault. Analyze and compare these possible causes and determine the specific root cause.

Rectifying the Fault

Rectify the fault based on fault causes. This process involves checking process status, viewing logs, modifying configuration files, and restarting services.



Contact technical support if the fault persists after troubleshooting is complete.

Verifying Fault Rectification

Verify that the fault has been rectified.

Recording the Troubleshooting Process

Record the fault cases to improve O&M.

1.2 Information Collection

1.2.1 Precautions

Observe the following principles during information collection:

- Perform maintenance operations only after receiving explicit approval from the customer. Any operations without explicit customer approval are prohibited.
- Transfer data required for locating a fault out of the customer's network only after being approved by the customer.

1.2.2 Collecting Basic Information

Collecting Site Information

After a fault occurs, collect site information for technical support and R&D engineers to learn about the site. In addition, provide the phone numbers of onsite engineers to ensure smooth communication.

Table 1-1 Site information to be collected

Carrier or Enterprise	-
Version	-
Networking Diagram	-
Service Environment Type	-
Urgency	-

Onsite Engineer Name and Phone Number	-
--	---

Collecting Basic Fault Information

Collect basic fault information to learn about the site, the device status before the fault occurred, and possible causes of the fault.

Table 1-2 Basic fault information to be collected

Symptom	-
Occurrence time	-
Occurrence frequency	-
Whether the fault is rectified	-
Operations performed in the system when the fault occurs	-
Process in which the fault occurred (capacity expansion, cutover, or upgrade)	-
Operations performed to resolve maintenance problems that occurred prior to the fault	-
Measures taken to handle the fault	-
Effect of the measures taken to handle the fault	-
Whether alarms are generated	-
Whether onsite alarm information is collected	-

Collecting Alarm Information

Table 1-3 Alarm information to be collected

Parameter	Value
Alarm ID	-
Alarm severity	-
Alarm name	-

Parameter	Value
Alarm source/object	-
Generated at	-
Region	-
Type	-
Possible causes	-
Additional information	-

Collecting Log Information

Log information about each GaussDB(DWS) component is critical for fault locating. If the system becomes abnormal, collect logs of each component to facilitate further analysis.

Database logs record problems that occur when GaussDB(DWS) database servers are started, running and stopped. When a problem occurs, analyze logs in the `/home/Ruby/log/` directory. If you cannot locate the root causes, analyze the database logs.

- For details about how to obtain management logs, see "Collecting Logs" *Data Warehouse Service (DWS) x.x.x References (for Huawei Cloud Stack x.x.x)* in [Data Warehouse Service \(DWS\) x.x.x Maintenance Guide \(for Huawei Cloud Stack x.x.x\)](#).
- For details about how to obtain tenant logs, see "Collecting Logs" *Data Warehouse Service (DWS) x.x.x References (for Huawei Cloud Stack x.x.x)* in [Data Warehouse Service \(DWS\) x.x.x Maintenance Guide \(for Huawei Cloud Stack x.x.x\)](#).

1.3 Faults on the Management Side

1.3.1 UI

1.3.1.1 GaussDB(DWS) Cluster Monitoring Information Is Not Displayed on Cloud Eye

Symptom

GaussDB(DWS) cluster monitoring information is not displayed on the Cloud Eye management console.

Priority

High

Impact

A user cannot view cluster monitoring details.

Possible Causes

- An instance in the cluster is faulty.
- Information in the `/home/Ruby/InitCes.json` file is not updated.
- The NTP clock is not synchronized in the cluster.

Estimated Processing Duration

30 min

Handling Method

1. Log in to ManageOne Maintenance Portal, choose **Monitor > Resource Monitoring > Cloud Resources > Data Warehouse Service**, select **Data Warehouse Nodes**, and check whether the number of nodes displayed on the page is the same as the actual number.
2. Log in to the DWS O&M container to access the data warehouse node, and check whether the text "The post request return code is:200, content is success" is in the `/home/Ruby/log/ces/ces.log` file.
3. Run the `ntpq -p` command to check whether the clock is not synchronized.

Emergency Handling Guide

- Step 1** Log in to ManageOne Maintenance Portal, choose **Monitor > Resource Monitoring > Cloud Resources > Data Warehouse Service**, select **Data Warehouse Nodes**, and check whether the number of nodes displayed on the page is the same as the actual number.
- If yes, go to [Step 4](#).
 - If no, go to [Step 2](#).

- Step 2** Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and query the instance name by cluster ID. You can obtain the cluster ID by clicking the cluster name on the management console.

`select name from rds_instance where clusterId='Cluster ID';`

- Step 3** Log in to the faulty instance by referring to [Logging In to a Node in the Tenant Cluster](#) and rectify the fault by referring to [Faults on the Tenant Side](#). 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 data warehouse instance by referring to [Logging In to a Node in the Tenant Cluster](#) and view the `/home/Ruby/log/ces/ces.log` file.

`cat /home/Ruby/log/ces/ces.log`

Check whether **The post request return code is:200, content is success** is displayed.

- If yes, go to **Step 6**.
- If no, go to **Step 5**.

Step 5 Check the AK/SK information in the **/home/Ruby/InitCes.json** file. If the information is updated, modify the **InitCes.json** file and save it.

Step 6 Run the **ntpq -p** command on the cluster node to check whether the clock is synchronized. If the NTP clock on a node is not synchronized, the monitoring information fails to be uploaded. In this case, synchronize NTP and check monitoring details uploaded in the **ces.log** file.

----End

Verification

Log in to the console, locate the row that contains the target cluster, and choose **More > View Metric**. Monitoring details are properly displayed.

Related Information

None

1.3.1.2 Flavors Are Not Displayed After GaussDB(DWS) Is Installed

Symptom

After GaussDB(DWS) is installed, flavors are not displayed on the cluster creation page. As a result, the cluster cannot be created.

Priority

High

Impact

Clusters cannot be created.

Possible Causes

- Information related to **bms.endpoint** cannot be obtained.
- The underlying ECS or BMS flavors of the database are different from those registered on the Service OM page.
- The value of **cluster_spec_id** in the **rds_spec_region** table is **disable**.

Estimated Processing Duration

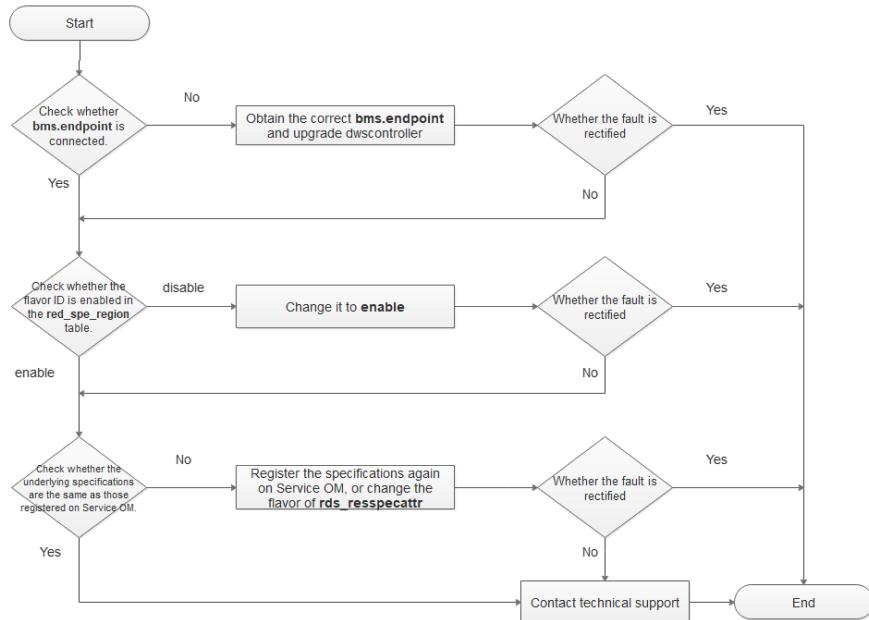
30 min

Handling Method

1. Check whether **bms.endpoint** is connected.

2. Check whether the flavor ID is enabled in the **red_spe_region** table.
3. Check whether the underlying flavors are the same as those registered on Service OM.

Figure 1-2 Handling method



Emergency Handling Guide

Step 1 Log in to CloudScope using a browser as a system administrator.

- URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op_cdk_sso**
- For details about the default password of the account, see the "CloudScopeLite" sheet in [Huawei Cloud Stack 8.x.x Account List](#).

Step 2 Choose **Services > O&M > CloudAutoDeploy-CDK**.

Step 3 In the upper left corner of the page, select the corresponding region. In the navigation pane on the left, choose **Change Mgmt > Upgrade** and select the corresponding cluster, for example, **ei-dbs-region**. Then search for **dwscontroller** in the search box, select the corresponding **dwscontroller**, and click **Next**. Search for **bms.endpoint** in the search box and record the value of this parameter.



Step 4 Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

Step 5 Query the pods.

kubectl get pods -n dws -owide

Step 6 Log in to a **dwscontroller** pod. In the following command, **dwscontroller_pod_name** indicates the name obtained in [Step 5](#).

kubectl exec -ti -n dws dwscontroller_pod_name bash

Step 7 Run the **curl Value_of_bms.endpoint** command to check whether the connection is normal.

Value_of_bms.endpoint indicates the value following **https://** obtained in [Step 3](#), for example, **curl bms.cn-dwsglobal-1.dwscloud.com:443**.

If information similar to the following is displayed, the connection is normal:
`curl: (52) Empty reply from server`

- If the connection is normal, go to [Step 9](#).
- Otherwise, the connection is abnormal. Go to [Step 8](#).

Step 8 If the **curl** command fails for the **bms.endpoint** value configured on the CloudAutoDeploy-CDK page, contact BMS technical support to obtain **bms.endpoint** information in the environment and update it on the CloudAutoDeploy-CDK page. After the upgrade is complete, delete the pod on the CloudAutoDeploy-CDK master node to make the parameter take effect.

1. Contact BMS technical support to obtain the **bms.endpoint** information in the environment.
2. On CloudAutoDeploy-CDK, choose **Service Mgmt > Service Query**. Click **Upgrade** of the DWS Controller service, enter **bms.endpoint** in the search box, click **Edit**, change the value to the obtained value of **bms.endpoint**, and click **OK**. Then click **Next**.
3. Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#) and run the following command to delete all **dwscontroller** pods:

kubectl delete pod dwscontroller_pod_name -n dws

4. View the pod names.

kubectl get pods -n dws -owide

5. Check whether the pods are successfully started.

kubectl describe pod dwscontroller_pod_name -n dws

6. Check whether the fault is rectified. If not, go to [Step 9](#).

Step 9 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and obtain **cluster_spec_id** by flavor.

```
select * from rds_cluster_spec where code = "{flavor}";
```

Information similar to the following is displayed:

id	code	topo	mount	ori_node	min_node	max_node	classify	scenario	serialno	version
17215982-cd1b-37c5-9cc3-6aaaf1c63ebd5	physical.d2.24xlarge.5	ONE_AZ_ONE_PRIMARY_ONE_STANDBY_ONE_DUMMY	DN_BND_VOLUME	3	3	256	dws	production	39	v1.0

Step 10 Query the flavor status in the **rds_spec_region** table based on the obtained **cluster_spec_id**.

```
select * from rds_spec_region where cluster_spec_id = "{cluster_spec_id}";
```

Information similar to the following is displayed.

+-----+-----+-----+-----+	id	cluster_spec_id	region	zone	status
+-----+-----+-----+-----+	24760dab-24c9-11eb-afa5-fa163e61a432	172159e2-cd1b-37c5-9cc3-6aaaf1c63ebd5	cn-dwsglobal-1	az1.dc1	enable
+-----+-----+-----+-----+	24760dce-24c9-11eb-afa5-fa163e61a432	172159e2-cd1b-37c5-9cc3-6aaaf1c63ebd5	cn-dwsglobal-1	az2.dc2	enable

- If **disable** is displayed, go to [Step 11](#).
- If **enable** is displayed, go to [Step 12](#).

Step 11 If the status of target **cluster_spec_id** in the **rds_spec_region** table in the database is **disable**, run the following command to change it to **enable**:

```
update rds_spec_region set status = 'enable' where cluster_spec_id = "{cluster_spec_id}";
```

Check whether the fault is rectified. If no, go to [Step 12](#).

Step 12 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and obtain **specId** by flavor.

```
select * from rds_resspec where specCode= "{flavor}";
```

Information similar to the following is displayed.

MySQL [rms]> select * from rds_resspec where specCode= "physical.d2.24xlarge.5";						
id	instanceType	regionCode	restypeCode	addedCodeInBill	bssProductId	imgType
0	master	southchina	hws.resource.type.dws.bms	physical.d2.24xlarge.5	x86	
0						

1 row in set (0.00 sec)

Step 13 Obtain the underlying flavors of the **rds_resspecattr** table based on the obtained **specId**.

```
select * from rds_resspecattr where specId = "{specId}";
```

Information similar to the following is displayed.

MySQL [rms]> select * from rds_resspecattr where specId = '50506035-c510-4aec-bd51-3e36ed93a56e';				
attrCode	specId	comment	value	disable
cpu	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	96	
dataDisk	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	1800	
diskNum	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	4	
diskSize	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	1800	
dnNum	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	4	
flavor	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	physical.d2.24xlarge.5	
mem	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	512	
raidNum	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	4	
volumeType	50506035-c510-4aec-bd51-3e36ed93a56e	NULL	LOCAL_DISK	

9 rows in set (0.00 sec)

Step 14 Compare the obtained flavors with those registered on Service OM.

- If the flavors are different, go to [Step 15](#).
- If the flavors are the same, go to [Step 16](#).

Step 15 If the underlying ECS or BMS flavors of the database are different from those registered on Service OM, register the ECS or BMS flavors again on Service OM or modify the **flavor** field of **rds_resspecattr** in the database. Check whether the fault is rectified. If no, go to [Step 16](#).

Step 16 Go to the cluster creation page again and check whether the cluster is restored. If the fault persists, contact technical support.

----End

Verification

When you log in to the GaussDB(DWS) console and create a cluster, cluster flavors are displayed.

Related Information

None

1.3.1.3 Disk Capacity Displayed on the Cluster Page Is Abnormal

Symptom

On the cluster details page, the displayed disk capacity is inconsistent with the actual situation.

Priority

High

Impact

Users cannot view the cluster capacity and disk usage.

Possible Causes

The disk capacity is incorrectly configured.

Estimated Processing Duration

30 min

Handling Method

1. On the cluster details page, check whether the cluster specifications are the specifications of the local disk or BMS. In the DWS HCS version, the disk capacity is incorrectly configured for some local disks.

2. Log in to a node and run the **df -h** command to query the actual capacity of the node. Check whether the capacity is consistent with the disk capacity in the **/opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/dataStoreSpecSpecial/datastoreSpec_dws_HWS.xml** file of the **dwscontroller** pod. If the values are inconsistent, modification is required.
3. Query the disk capacity of database **rms**. The query result must be the same as the output of the **df -h** command.

Emergency Handling Guide



For HCS 8.0.3 and earlier versions, perform the following steps. For HCS 8.1.0 and later versions, perform only **Step 10**.

- Step 1** Log in to CloudAutoDeploy-CDK and select the corresponding region in the upper left corner. In the navigation pane on the left, choose **Change Mgmt > Upgrade** and select the corresponding cluster, for example, **ei-dbs-region**. Then search for **dwscontroller** in the search box, select the corresponding **dwscontroller**, and click **START_MODE**.
- Step 2** Check the information of **START_MODE**. If the template parameter is **product**, set **Current Parameter** to **develop**, click **Next**, and click **Upgrade**.

The screenshot shows a configuration interface for a parameter named 'START_MODE'. At the top, there are buttons for 'Import a JSON file' and 'Configure Rendering'. Below is a table with the following data:

Parameter Name	Tag	Data Type	Template Parameter	Current Parameter	Description	Operation
START_MODE	global	string	product	develop	The value can be product or develop	Restore Defaults

- Step 3** Log in to the CloudAutoDeploy-CDK master node and run the following command to query the **dwscontroller** pods:

kubectl get pods -n dws -owide

- Step 4** Delete the corresponding pod and check whether the new pod is started:

kubectl delete pod dwscontroller_pod_name -n dws

kubectl get pods -n dws -owide

kubectl describe pod dwscontroller_pod_name -n dws

- Step 5** Log in to the GaussDB(DWS) cluster instance and run the **df -h** command to query the actual disk capacity of the node.

```
[root@ho:          [1 Mike]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda4        43G   4.6G   37G  12% /
devtmpfs        7.8G    0    7.8G  0% /dev
tmpfs           7.8G    0    7.8G  0% /dev/shm
tmpfs           7.8G  729M  7.1G 10% /run
tmpfs           7.8G    0    7.8G  0% /sys/fs/cgroup
tmpfs           7.8G    0    7.8G  0% /var/chroot/dev/shm
/dev/vda2       976M  146M  764M 16% /boot
/dev/vda1       200M  8.2M  192M  5% /boot/efi
tmpfs           1.6G    0    1.6G  0% /run/user/1001
/dev/vdb        100G  1.2G   99G  2% /var/chroot/DWS/manager
/dev/md1         8.2T  1.5G  8.2T  1% /var/chroot/DWS/datal
/dev/md0         8.2T  788M  8.2T  1% /var/chroot/DWS/data2
tmpfs           1.6G    0    1.6G  0% /run/user/0
tmpfs           1.6G    0    1.6G  0% /run/user/1002
[root@host_172_20_12_11 Mikael]#
```

- Step 6** Go back to the CloudAutoDeploy-CDK master node and run the following command to query the pods:

```
kubectl get pods -n dws -owide
```

- ### **Step 7 Log in to a `dwscontroller` pod.**

```
kubectl exec -ti -n dws dwscontroller_pod_name bash
```

- Step 8** On the **dwscontroller** pod, run the following command to view the cluster flavor and disk capacity in the `/opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/dataStoreSpecSpecial/datastoreSpec_dws_HWS.xml` file. The disk capacity in the XML file must be the same as the actual disk capacity queried by running the `df -h` command.

```
cd /opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/  
dataStoreSpecSpecial
```

```
grep {flavorName} datastoreSpec dws HWS.xml
```

- Step 9** In the `/opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/dataStoreSpecSpecial/datastoreSpec_dws_HWS.xml` file, find the version text block corresponding to the cluster version, correct the localDiskSize values of the `dws` type and the `dws-cn` type, then restart Tomcat.

- Step 10** Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and run the following SQL command to query the disk capacity information in the database:

```
select instance_capacity from rds_cluster_instance_resspec where cluster_spec_id = (select id from rds_cluster_spec where code = '{flavorName}');
```

```
MySQL [rms]> select instance_capacity from rds_cluster_instance_resspec where cluster_spec_id = (select id from rds_cluster_spec where code = "dws.d2.10xlarge");
+-----+
| instance_capacity |
+-----+
| 8381 |
+-----+
1 row in set (0.00 sec)
```

If the value is different from the actual disk capacity, change the disk capacity in the **rds_cluster_instance_resspec** table in the database.

```
update rds_cluster_instance_resspec set instance_capacity = 'Actual_capacity' where cluster_spec_id = (select id from rds_cluster_spec where code = '{flavorName}');
```

----End

Verification

Clear the cache, and reload and check the page.

Related Information

None

1.3.1.4 Status of Some Clusters on the GaussDB(DWS) Console Is Abnormal

Symptom

The status of some clusters on the GaussDB(DWS) console is abnormal.

Priority

High

Impact

The cluster status is abnormal.

Possible Causes

The HA Agent process in the cluster is abnormal.

Estimated Processing Duration

20 min

Handling Method

1. Log in to the abnormal cluster node and check the cluster status.
2. If the cluster is normal, the status reporting is abnormal. In this case, restart the HA Agent process in the cluster.

Emergency Handling Guide

Step 1 Log in to the abnormal cluster node and access the cluster sandbox. For details, see [Logging In to a Node in the Tenant Cluster](#).

Step 2 Log in to the instance where the CMS server is located using SSH.

cm_ctl query -Cvd

Check whether the cluster status is normal.

- If yes, go to [Step 3](#).
- If no, rectify the fault on the tenant side by referring to [Faults on the Tenant Side](#). If the cluster status on the console is normal, no further action is required. If the cluster status is still abnormal, go to [Step 3](#).

Step 3 If the tenant cluster status is normal, an exception is reported. In this case, restart HA Agent.

1. Run the **exit** command to exit the sandbox.
2. Check the HA Agent process.

ps -ef | grep haagent

3. Restart the HA Agent process.

kill -9 Process ID

Check whether the fault has been rectified.

- If yes, no further action is required.
- If no, contact technical support.

----End

Verification

The cluster status is normal.

Related Information

None

1.3.1.5 No GaussDB(DWS) Pod Monitoring Data Is Displayed on ManageOne Maintenance Portal

Symptom

Log in to ManageOne Maintenance Portal and choose **Monitor > Resource Monitoring**. On the page that is displayed, no GaussDB(DWS) pod status is displayed.

Priority

High

Impact

The status of GaussDB(DWS) pods cannot be viewed on ManageOne Maintenance Portal.

Possible Causes

The dos2unix code is incorrect.

Estimated Processing Duration

20 min

Handling Method

Log in to the CloudAutoDeploy-CDK master node and change the encoding format of GaussDB(DWS) files to UNIX.

Emergency Handling Procedure

Step 1 Log in to any CloudAutoDeploy-CDK master node and switch to user **root**. For details, see [Logging In to the CloudAutoDeploy-CDK Master Node](#).

Step 2 Enter the directory in which the script is stored.

(There may be two types of Agents. You can run the **ps -ef|grep moicagent** command to check which type of Agent exists in the software installation path.)

1. Basic Agent form:

/home/moicagent/tools/pyscript/plugins/extenal/6.5.0/xxx

2. CloudAgent form:

/usr/local/CloudAgent/plugins/MOICAgent/tools/pyscript/plugins/extenal/6.5.0/xxx

Step 3 Convert the file encoding format to UNIX.

dos2unix dws_*

Step 4 (Optional) Change the **dws_dws_icagent** encoding format to UNIX.



NOTE

If no service monitoring data is displayed after the preceding operations are performed, convert the following **sudoers** file.

cd /etc/sudoers.d

dos2unix dws_dws_icagent

Step 5 Repeat the preceding steps to modify the configuration files of all three CloudAutoDeploy-CDK master nodes.

----End

Verification

The status of GaussDB(DWS) pods can be monitored on ManageOne Maintenance Portal.

Related Information

None

1.3.1.6 Cluster Creation Task Failed with Error Code DWS.0105

Symptom

After a user submits a task to create a cluster on the GaussDB(DWS) management console, the error message "DWS.0105 ECS interface exception occurs." is displayed.

Priority

High

Impact

The cluster creation task cannot be submitted.

Possible Causes

1. The flavor selected for creating a cluster is available on the GaussDB(DWS) page, but unavailable on the ECS page.
2. The ECS service is abnormal. Interfaces should be checked.

Estimated Processing Duration

5 min

Handling Method

Check whether ECS runs properly. If yes, log in to ManageOne Maintenance Portal, switch to Service OM, and check whether the configured flavor is available.

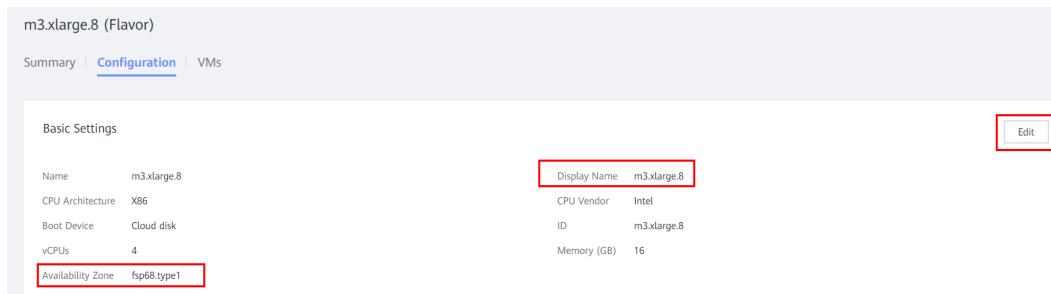
Emergency Handling Procedure

Step 1 Log in to ManageOne Maintenance Portal using a browser as a system administrator.

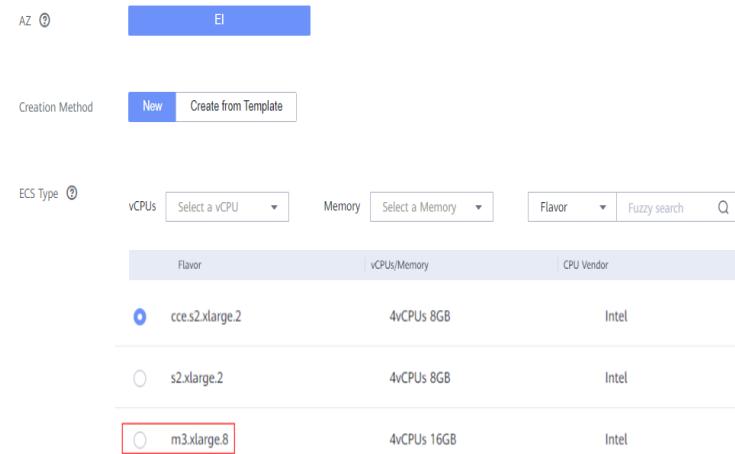
- URL: **https://Address_for_accessing_the_homepage_of_ManageOne_Maintenance_Portal:31943**, for example, **https://oc.type.com:31943**.
- Obtain the IP address of ManageOne Maintenance Portal on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during the installation of Huawei Cloud Stack basic services.
- For the default account and password, search for **ManageOne Maintenance Portal** on the "Type A (Portal)" sheet in the **HUAWEI CLOUD Stack x.x.x Account List**.

Step 2 In the **Common Links** area, click **Service OM**. Select your region and then access the **Service OM** page.

Step 3 Choose **Services > Compute Resource > Flavors**, search for the target flavor, and modify the AZ of the flavor.



Step 4 Log in to ManageOne Operation Portal, switch to the ECS service, and check whether the target flavor can be queried.



Step 5 Submit the cluster creation task again.

----End

1.3.1.7 Displayed DR Status Is Abnormal After the Production Cluster Is Faulty and Recovered

Symptom

When DR is enabled and the production cluster is faulty, the DR status on the frontend page displays **Abnormal** and the production cluster status displays **Unavailable**. In this case, perform operations described in this section.

Locating Method

The cause of this may be production cluster power-off, network disconnection, or other reasons.

Procedure

Step 1 Fix the production cluster and perform the following operations to demote it to a DR cluster:

Step 2 Log in to the background of a production cluster node and access the sandbox.

```
su - Ruby;  
ssh xxx.xxx.xxx.xxx (IP address of the node)
```

Step 3 Perform the following operations:

```
python $GPHOME/script/SyncDataToStby.py -t join-cluster --config-file /DWS/manager/  
backup/dr/disaster_recovery_restore.ini --switchover-config-file /DWS/manager/backup/dr/  
disaster_recovery_backup.ini
```

Step 4 If the output is as shown in the following figure, the original production cluster is allowed to be demoted. Otherwise, the following operations cannot be performed.

```
If you perform the join-cluster operation,  
data from the last incremental backup to the fault point in the original primary cluster will be lost.  
Are you sure you want to execute join-cluster operation?
```

Step 5 Perform **set-join**.

```
python $GPHOME/script/SyncDataToStby.py -t set-join --config-file /DWS/manager/  
backup/dr/disaster_recovery_restore.ini --switchover-config-file /DWS/manager/backup/dr/  
disaster_recovery_backup.ini
```

Step 6 After **Step 5** is successfully executed, perform the following operations to start the DR system:

```
ssh xxx.xxx.xxx.xxx (IP address of the active node in the new production cluster) "nohup  
python3 $GPHOME/script/SyncDataToStby.py -t backup --config-file /DWS/manager/  
backup/dr/disaster_recovery_backup.ini >>/dev/null 2>&1 &"  
nohup python3 $GPHOME/script/SyncDataToStby.py -t restore --config-file /DWS/  
manager/backup/dr/disaster_recovery_restore.ini >>/dev/null 2>&1 &
```

Step 7 Check whether the DR status has turned to normal. If the DR status is **Running**, the fault is fixed.

----End

1.3.2 Cluster

1.3.2.1 Failed to Create a Cluster

Symptom

Clusters fail to be created on the GaussDB(DWS) console.

Priority

High

Impact

Clusters cannot be created.

Possible Causes

- VMs cannot be created due to IaaS layer faults.
- Cluster initialization is abnormal.
- Other exceptions.

Estimated Processing Duration

30 min

Handling Method

1. Log in to database **rms** and obtain the failed **job_id** by cluster name.
2. Locate the cause of the failure in the **dwscontroller** log based on **job_id**.

Emergency Handling Procedure

Step 1 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#).

Step 2 Check the value of **job_id** of the cluster that fails to be created by cluster name.

```
select task.* from taskmgr_task as task left outer join taskmgr_job as job on job.job_id = task.job_id where job.request like '%lhuayi01%' order by job_id, task_index asc;
```

Output similar to the following is displayed. In the row where the task **RdsCreateInstanceTask** is located, the value of **execution_status** is **FAIL**, which indicates that ECSs fail to be created. The value of **job_id** is **2c9080d476dae3340176dc07b7d2009f**.

task_id	begin_time	current_run_type	end_time	execution_status	task_index	job_id	listener_num	prio	retry_num	task_d
2c9080d476dc437c0176dc06ba00045 2021-01-07 05:26:49 EXECUTE		2021-01-07 05:28:54 SUCCESS	0 2c9080d476dc437c0176dc06ba00045 0 5 0 RdsNet							
RdsNotifyRdsForRdbTask										
2c9080d476dc437c0176dc06ba120047 2021-01-07 05:28:50 EXECUTE		2021-01-07 05:29:07 SUCCESS	1 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteBackupTask										
2c9080d476dc437c0176dc06ba2270048 2021-01-07 05:29:12 EXECUTE		2021-01-07 05:29:36 SUCCESS	2 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteCloudTrafficNicsTask										
2c9080d476dc437c0176dc06ba300049 2021-01-07 05:29:40 EXECUTE		2021-01-07 05:30:04 SUCCESS	3 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteInternalPortTask										
2c9080d476dc437c0176dc06ba300049 2021-01-07 05:30:08 EXECUTE		2021-01-07 05:31:18 SUCCESS	4 2c9080d476dc437c0176dc06ba00045 1 5 0 Multie							
RdsDeleteCloudPortTask										
2c9080d476dc437c0176dc06ba00046 2021-01-07 05:31:23 EXECUTE		2021-01-07 05:31:49 SUCCESS	5 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteSecurityGroupTask										
2c9080d476dc437c0176dc06ba00046 2021-01-07 05:31:53 EXECUTE		2021-01-07 05:32:02 SUCCESS	6 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteCloudPortTask										
2c9080d476dc437c0176dc06ba300044 2021-01-07 05:32:07 EXECUTE		2021-01-07 05:32:15 SUCCESS	7 2c9080d476dc437c0176dc06ba00045 0 5 0 Multie							
RdsDeleteClusterAndTask										
2c9080d476dc437c0176dc06ba300044 2021-01-07 05:32:20 EXECUTE		2021-01-07 05:32:20 SUCCESS	8 2c9080d476dc437c0176dc06ba00045 0 5 0 RdsNot							
RdsDeleteCloudPortTask										
2c9080d476dae3340176dc07b0b00047 2021-01-07 02:47:44 ROLLBACK		2021-01-07 02:47:45 SUCCESS	0 2c9080d476dae3340176dc07b0b00047 0 5 0 Resten							
RdsTask										
2c9080d476daea3340176dc07b0b00047 2021-01-07 02:47:49 ROLLBACK		2021-01-07 02:47:54 SUCCESS	1 2c9080d476daea3340176dc07b0b00047 0 5 0 RestUse							
RdsTask										
2c9080d476daea3340176dc07b0e000008 2021-01-07 02:47:59 EXECUTE		2021-01-07 02:48:04 SUCCESS	2 2c9080d476daea3340176dc07b0e000008 0 5 0 RdsBin							
RdsBindIPSTask										
2c9080d476daea3340176dc07b0e000008 2021-01-07 02:48:09 EXECUTE		2021-01-07 02:48:20 EXECUTE	3 2c9080d476daea3340176dc07b0e000008 0 5 0 RdsCre							
RdsBindIPSTask										
2c9080d476daea3340176dc07b0e300004 2021-01-07 02:48:24 EXECUTE		2021-01-07 02:48:25 SUCCESS	4 2c9080d476daea3340176dc07b0e300004 0 5 0 RdsCre							
RdsSecurityGroupTask										
2c9080d476daea3340176dc07b0e300004 2021-01-07 02:48:29 EXECUTE		2021-01-07 02:48:29 SUCCESS	5 2c9080d476daea3340176dc07b0e300004 0 5 0 RdsSer							
RdsSecurityGroupTask										
2c9080d476daea3340176dc07b0e41000c 2021-01-07 02:48:34 EXECUTE		2021-01-07 02:48:36 FAIL	6 2c9080d476daea3340176dc07b0e41000c 0 5 0 RdsCre							
RdsCreateInstanceTask										
2c9080d476daea3340176dc07b0e5700c2 NULL EXECUTE	MULL	MULL								
RdsCreateInstanceManagerTask										
2c9080d476daea3340176dc07b0e6500c5 NULL EXECUTE	MULL	MULL								
RdsShutdownServerTask										
2c9080d476daea3340176dc07b0e7000c8 NULL EXECUTE	MULL	MULL								
RdsStartServerTask										
2c9080d476daea3340176dc07b0e9000c EXECUTE	MULL	MULL								
RdsStartServerTask										
2c9080d476daea3340176dc07b0eb000cb EXECUTE	MULL	MULL								
RdsStartServerTask										
2c9080d476daea3340176dc07b0eb000cb EXECUTE	MULL	MULL								
RdsStartInstanceChannelTask										
2c9080d476daea3340176dc07b0eb6000d EXECUTE	MULL	MULL								
RdsSendInitConfigTask										
2c9080d476daea3340176dc07b1f10006 EXECUTE	MULL	MULL								
RdsInitInstanceTask										
2c9080d476daea3340176dc07bfa10006 EXECUTE	MULL	MULL								
VncEndpointServiceTask										
2c9080d476daea3340176dc07bfa0006 CreateVncEndpointServiceTask	MULL	MULL								
PublicIPTask										
2c9080d476daea3340176dc07bfa0006 CreatePublicIPTask	MULL	MULL								

Step 3 Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

Step 4 You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.
- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.

cat ossres-dws.log | grep jobId | grep ERROR

NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 5 The error code in the error log is "error_code":"Ecs.0219". This problem is caused by the IaaS layer exception. Contact the IaaS layer personnel to solve the problem.

Step 6 The following lists other failure causes and corresponding handling methods:

1. The data warehouse cluster initialization is abnormal.

- The following figure shows that the **[RdsInitInstanceTask]** node initialization fails.

```
catalina.out:2016-10-27 10:08:50,658|ff8080815803cf38015803ddccf50013|ERROR|[RdsInitInstanceTask][listenAfterExecute]listenAfterExecute failed, async job failed; instanceId:[b80bedee-e2a-47bc-8d89-0948fd293535] RdsInstanceUtil checkAsyncCmdJob exception:[2016-10-27 10:08:34][INFO0][7915][140157527295808][doInitDb.py 340][into doInitDb.py 360][doInitDb.py finished!]|com.huawei.hwclouds.rds.executor.RdsInitInstanceTask.listenAfterExecute[RdsInitInstanceTask.java:205]
catalina.out:2016-10-27 10:08:36|[INFO0][7915][140157527295808][doInitDb.py 367][doInitDb.py finished!]|com.huawei.hwclouds.rds.executor.RdsInitInstanceTask.listenAfterExecute[RdsInitInstanceTask.java:206]
catalina.out:2016-10-27 10:08:50,659|ff8080815803cf38015803ddccf50013|ERROR|RdsExecutorExceptionHandler catches exception: TaskMgrException, message: [RdsInitInstanceTask][listenAfterExecute]listenAfterExecute failed, async job failed; instanceId:[b80bedee-e2a-47bc-8d89-0948fd293535] RdsInstanceUtil checkAsyncCmdJob exception:[2016-10-27 8:34][INFO0][7915][140157527295808][doInitDb.py 340][into doInitDb.py 367][doInitDb.py finished!]|locat
catalina.out:2016-10-27 10:08:50,703|ff8080815803cf38015803ddccf50013|INFO0|RdsExecutorExceptionHandler exceptionHandler(RdsExecutorExceptionHandler.java:206)|com.huawei.hwclouds.rds.common.exception.ha
r.RdsExecutorExceptionHandler.exceptionHandler(RdsExecutorExceptionHandler.java:56)
catalina.out:2016-10-27 10:08:50,703|ff8080815803cf38015803ddccf50013|INFO0|RdsExecutorExceptionHandler start to elect RdsInitInstanceTask.onListenFailedAfterExecute()|com.huawei.hwclouds.rds.common.exception.handler.RdsExecut
cptionHandler.exceptionHandler(RdsExecutorExceptionHandler.java:42)
catalina.out:2016-10-27 10:08:50,703|ff8080815803cf38015803ddccf50013|INFO0|task[RdsInitInstanceTask] run end.|com.huawei.hwclouds.taskmgr.job.task.AbstractTask.run(AbstractTask.java:115)
catalina.out:2016-10-27 10:08:50,714|ff8080815803cf38015803ddccf50013|ERROR|task[RdsInitInstanceTask] run fail.|com.huawei.hwclouds.taskmgr.job.impl.CommonJob.dealTaskResult(CommonJob.java:229)
18,71
```

- Log in to the failed nodes of the cluster by referring to [Logging In to a Node in the Tenant Cluster](#).
- View the **cloud-dws-deploy.log** file in the **/home/Ruby/log** directory. Locate the error log according to the task execution time and analyze the cause of the error.

2. Other exceptions occur.

In **Step 2**, the created cluster consists of 15 tasks. You can find the tasks that fail to be executed and contact Huawei technical support.

----End

Verification

A cluster can be created.

Related Information

None

1.3.2.2 GaussDB(DWS) BMS Cluster Fails to Be Created Due to Mutual Trust Problems

Symptom

A GaussDB(DWS) BMS cluster fails to be created, and the percentage displayed on the page is about 70%.

Priority

High

Impact

BMS clusters cannot be created.

Possible Causes

The underlying switch configuration is incorrect.

Estimated Processing Duration

20 min

Handling Method

1. Check the BMS specifications.
2. Log in to a failed node by referring to [Logging In to a Node in the Tenant Cluster](#) and check the error information in the `/home/Ruby/log/cloud-dws-deploy.log` file. The SSH error message `no route` is displayed when mutual trust is established.

Emergency Handling Procedure

- Step 1** Check the BMS specifications. Log in to database `rms` by referring to [Logging In to the rms Database on the Management Side](#) and run the following command to obtain the job ID information used during cluster creation:

```
select jobId from rds_instance where name like "%{clusterName}%";
```

```
MySQL [rms]> select jobId from rds_instance where name like "%l      i04%";  
+-----+  
| jobId |  
+-----+  
| 2c9080f476f0c92a0176f9b1b6bb02bc |  
| 2c9080f476f0c92a0176f9b1b7b402be |  
| 2c9080f476f0c92a0176f9b1b8ac02c0 |  
+-----+  
3 rows in set (0.00 sec)
```

- Step 2** Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

- Step 3** You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for `jobId` in the log file to obtain the logs.
- After obtaining logs from the background, run the `cat` command and filter by `jobId` to obtain cluster creation logs.

```
cat ossres-dws.log | grep jobId | grep ERROR
```

NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

- Step 4** The error information indicates that the error occurs in the Init phase. Log in to the failed nodes or by referring to [Logging In to a Node in the Tenant Cluster](#) and check the error information in the **/home/Ruby/log/cloud-dws-deploy.log**. The SSH error message "no route" is displayed when mutual trust is established.
- Step 5** Check the deployment mode. If the BMS is deployed over high-speed network, mutual trust problems may occur due to network disconnection. The possible cause is that the switch VLAN on the instance is not allowed to pass. In this case, ask the underlying network engineers to allow the VLAN to pass.

----End

Verification

BMS clusters can be created.

Related Information

None

1.3.2.3 GaussDB(DWS) BMS Cluster Fails to Be Created Due to Insufficient Underlying Resources

Symptom

When a user creates a BMS cluster on the console, the underlying BMS resources are insufficient. As a result, the error code **BMS.****** is displayed.

Priority

High

Impact

BMS clusters cannot be created.

Possible Causes

The formatting of the BMS instance is not complete in the background.

Estimated Processing Duration

30 min

Handling Method

1. Check the error code displayed when the BMS cluster fails to be created.
2. Log in to Service OM, switch to the BMS page, and check whether the available BMSs meet the requirements.
3. Check the GaussDB(DWS) background logs based on the job ID of the database and view the error details.

Emergency Handling Procedure

- Step 1** Log in to ManageOne Maintenance Portal and click **Service OM** in the frequently used links area.
- Step 2** Choose **Services > Resource > Bare Metal Resource**, select the corresponding AZ, and check whether the available BMSs meet the specifications requirements. For details about the BMS specifications, see "Supported BMS Flavors" in [Huawei Cloud Stack x.x.x Software Installation Guide for gPaaS & AI DaaS Services](#).

If the number of BMSs does not meet the requirements or some BMSs are faulty or unavailable, contact engineers at the base layer to resolve the problem.

I.101 (Bare Metal Server)

Summary | Configure

Management and System Settings

Processors	2	Memory (MB)	262144
vCPUs	96	Local Disk (GB)	14997
Host cores	48		

- Step 3** If the BMSs are sufficient as shown on Service OM, log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and run the following SQL statement to check the job ID during cluster creation:

```
select jobId from rds_instance where name like "%{clusterName}%";
```

```
MySQL [rms]> select jobId from rds_instance where name like "%l      i04%";  
+-----+  
| jobId |  
+-----+  
| 2c9080f476f0c92a0176f9b1b6bb02bc |  
| 2c9080f476f0c92a0176f9b1b7b402be |  
| 2c9080f476f0c92a0176f9b1b8ac02c0 |  
+-----+  
3 rows in set (0.00 sec)
```

Step 4 Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

Step 5 You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.
- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.

```
cat ossres-dws.log | grep jobId | grep ERROR
```



NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 6 Contact the BMS engineers to rectify the fault.

----End

Verification

Delete the cluster that fails to be created and create a BMS cluster again. A message is displayed, indicating that the cluster is successfully created.

Related Information

None

1.3.2.4 GaussDB(DWS) ECS Cluster Fails to Be Created Due to Insufficient ECS Resources

Symptom

When a user creates an ECS cluster on the console, the underlying ECS resources are insufficient. As a result, the error code **ECS.0204** is displayed.

Priority

High

Impact

ECS clusters cannot be created.

Possible Causes

The ECS resources are insufficient.

Estimated Processing Duration

30 min

Handling Method

1. Check the error code displayed when the ECS cluster fails to be created.
2. Check whether the GaussDB(DWS) flavor is correctly configured in an RDS database on the management side.
3. On Service OM, check whether the flavor exists and whether the CPU and memory information is correctly configured.

Emergency Handling Procedure

Step 1 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#). Run the following SQL command to view the job ID of the cluster. `{clusterName}` indicates the name of the cluster that fails to be created.
`select jobId from rds_instance where name like '%{clusterName}%';`

Step 2 Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

Step 3 You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.
- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.
`cat ossres-dws.log | grep jobId | grep ERROR`



Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 4 You can view the detailed error information returned by the ECS interface from the logs, for example, **There are not enough hosts available**.

Step 5 In database **rms**, run the following SQL command to query the ECS flavor name. In the preceding command, `{dwsFlavor}` indicates the GaussDB(DWS) flavor name.
`select * from rds_resspecattr where specId = (select id from rds_resspec where specCode = "{dwsFlavor}");`

In the command output, the value of the field whose **attrCode** is **flavor** is the name of the underlying ECS flavor.

Step 6 Log in to ManageOne Maintenance Portal and click **Service OM** in the frequently used links area.

Step 7 Choose **Services > Resource > Compute Resource > Flavors** and check whether the flavor name in **Step 5** exists and whether the CPU and memory information is correctly configured.

Step 8 If the ECS flavor is correct, contact ECS engineers to check whether the underlying flavor is ready or sufficient based on the error information.

----End

Verification

Delete the cluster that fails to be created and create a BMS cluster again. A message is displayed, indicating that the cluster is successfully created.

Related Information

None

1.3.2.5 Failed to Create a GaussDB(DWS) Cluster Because the Management Tenant Password Is Changed

Symptom

A GaussDB(DWS) cluster fails to be created and the creation progress is about 5%.

Priority

High

Impact

Clusters cannot be created.

Possible Causes

The password of the management tenant is invalid.

Estimated Processing Duration

20 min

Handling Method

1. Log in to database **rms**, search for the **jobId** column in the **rds_instance** table based on the cluster name, and obtain the cluster creation failure logs from the **dwscontroller** containers based on the job ID. The logs contain the error information of the **createUserByManageTenant** function.
2. According to the code logic, the operation calls the API to create a resource tenant by the management tenant. It is possible that the password of the management tenant is changed by another user and therefore the management tenant password of the database and parameters have become invalid.
3. Obtain the correct password of the management tenant, modify the password, and restart the containers.

Emergency Handling Procedure

Step 1 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#). Run the following SQL command to view the job ID of the cluster. *{clusterName}* indicates the name of the cluster that fails to be created.

```
select jobId from rds_instance where name like '%{clusterName}';
```

Step 2 Obtain DWSController log files by referring to [Collecting dwsccontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

Step 3 You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.
- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.

```
cat ossres-dws.log | grep jobId | grep ERROR
```



NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 4 The **createUserByManageTenant** error information is displayed.

```
[createUserByMgmtTenant]Failed, error is Create user failed, error is [IamClient]  
[getTokenWithoutProjectNameRestResponseWithRetry]retryTimes
```

Step 5 Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and view the latest password ciphertext in the **trust_domain_pwd** column in the namespace table of the database.

```
select trust_domain_pwd from namespace where id = "{Management_tenant_ID}";
```

Step 6 Update the password ciphertext of the following containers to ensure that the password ciphertext is the same as that in **Step 5**.

- Log in to CloudScope using a browser as a system administrator.
 - URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
 - For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of deployment parameter table exported from HCC Turnkey (or HUAWEI CLOUD Stack Deploy in HUAWEI CLOUD Stack 8.1.1 and earlier versions) during Auto Change Platform installation.
 - Default account: **op_cdk_sso**
 - For details about the default password of the account, see the "CloudScopeLite" sheet in [Huawei Cloud Stack x.x.x Account List](#).
- Choose **O&M > CloudAutoDeploy-CDK**.
- For Huawei Cloud Stack 8.0.2 or earlier, choose **Service Mgmt > Service Query** on the left, select the following container names in sequence, and click

Upgrade on the right. Search for the parameter names, upgrade the parameter values to those shown in **Step 5**, click **Next**, and click **Upgrade**.

- **dwscontroller**: trustDomainPwd, dwsTrustDomainPwd, accessDnsUserPwd
 - **dbsmonitor**: opsvc.domain.password
 - **dbsevent**: opvc.domain.password
4. For Huawei Cloud Stack 8.0.3 or later, choose **Change Mgmt > Upgrade** on the left, select the following container names in sequence, and click **Next**. Search for the parameter names, upgrade the parameter values to those shown in **Step 5**, click **Next**, and click **Upgrade**.
 - **dwscontroller**: trustDomainPwd, dwsTrustDomainPwd, accessDnsUserPwd
 - **dbsmonitor**: opsvc.domain.password
 - **dbsevent**: opvc.domain.password

Step 7 After the preceding parameters are modified, delete the containers from the CloudAutoDeploy-CDK master node. When the containers are restarted, create a GaussDB(DWS) cluster again on the page.

1. Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#) and run the following command to delete all **dwscontroller** pods:
kubectl delete pod dwscontroller_pod_name -n dws
 2. View the pod names.
kubectl get pods -n dws -owide
 3. Check whether the containers are successfully started:
kubectl describe pod dwscontroller_pod_name -n dws
 4. Delete all **dbsmonitor** and **dbsevent** containers.
kubectl delete pod dbsmonitor_pod_name -n ecf
kubectl delete pod dbsevent_pod_name -n ecf
 5. View the pod names.
kubectl get pods -n ecf -owide
 6. Check whether the containers are successfully started:
kubectl describe pod dwscontroller_pod_name -n ecf
kubectl describe pod dbsevent_pod_name -n ecf
- End

Verification

Return to the GaussDB(DWS) console. A cluster is successfully created.

Related Information

None

1.3.2.6 Management Side Cannot Communicate with the Internal Public Network Plane

Symptom

A GaussDB(DWS) cluster fails to be created on the console. The internal public network plane IP addresses of service nodes cannot be pinged from **dwscontroller** pods.

Priority

High

Impact

GaussDB(DWS) clusters cannot be created.

Possible Causes

- For Huawei Cloud Stack 8.0.1 or earlier, PEP is used on the management side to communicate with nodes. PEP may be disconnected from the internal public network plane.
- In Huawei Cloud Stack 8.0.1 or later, the management side uses the DMZ_Service IP address to communicate with instance nodes. The DMZ_Service network segment of the CloudAutoDeploy-CDK nodes may be disconnected from the internal public network plane.

Estimated Processing Duration

30 min

Handling Method

1. Check the version of the management side. The communication modes are different between versions earlier than Huawei Cloud Stack 8.0.1 and versions of Huawei Cloud Stack 8.0.1 or later.
2. Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and run the following command to query the **managelp** column in the **rds_instance** table by cluster name:

```
select managelp from rds_instance where name='Cluster_name';
```
3. Log in to a **dwscontroller** pod by referring to [Logging In to a dwscontroller Pod](#) and ping **managelp**.
4. If the ping fails, log in to VNC to check whether the OS is started.
5. If the OS has been started, contact network engineers to check the connection between the internal public network plane and PEP, or between the internal public network plane and the DMZ_Service network segment on the management side.

Emergency Handling Procedure

- Step 1** The OS of the instance cannot be started. As a result, **managelp** cannot be pinged from **dwscontroller**.

Check whether the GaussDB(DWS) images are correct, or whether the image IDs (ARM and x86) are correct. If yes, check whether the BMS startup mode is consistent with that used during image registration. Inconsistent startup modes will cause OS startup failure in BMS scenarios.

Step 2 The OS has been started, the GaussDB(DWS) instance is accessible, but the network is disconnected.

Contact network engineers to check the connection between the internal public network plane and PEP, or between the internal public network plane and the DMZ_Service network segment on the management side. The check method is as follows: Export the parameter summary table during BMS capacity expansion and query the VLAN start value and end value of the Ironic high-speed network of the BMS service plane.

For example, run the following commands on the switch:

dis cur int eth 1001

Port trunk allow-pass vlan 219 260 278 3400 to 3500 3601 to 3700

----End

Verification

GaussDB(DWS) clusters can be created.

Related Information

None

1.3.2.7 BMS Cluster Fails to Be Created Due to Tenant Name Change

Symptom

After the tenant name is changed, the BMS cluster fails to be created due to the NIC mounting failure.

Priority

High

Impact

BMS clusters cannot be created.

Possible Causes

When a NIC is mounted during BMS creation, the token of the tenant whose permission is escalated is required. The token is obtained based on the tenant name saved in the resource tenant table. After the tenant name is changed, it is not updated in the controller background database. As a result, the tenant name is incorrect when the token is obtained, and the token fails to be obtained.

Estimated Processing Duration

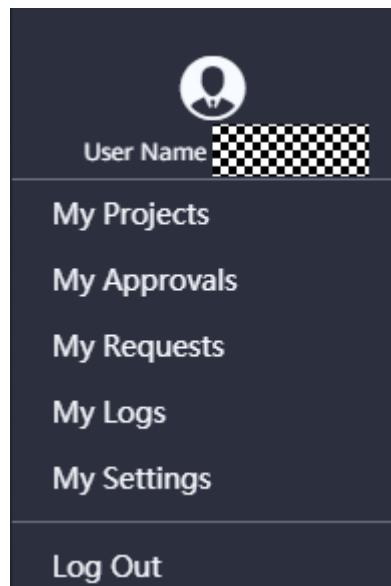
10 min

Handling Method

Synchronize the tenant information to the management side backend.

Emergency Handling Procedure

- Step 1** Log in to ManageOne Operation Portal as a user of the modified tenant, click **My Settings** to obtain the modified tenant ID and tenant name.



A screenshot of the "My Settings" page in the ManageOne Operation Portal. The left sidebar shows "My Space" with options: "My Approvals", "My Requests", "My Logs", and "My Settings" (which is selected). The main content area is titled "My Settings" and contains a "Basic Information" section. It lists the following fields with their values:

Field	Value
Username	[REDACTED]
Alias	--
Tenant	[REDACTED]
Email	--
Password	[REDACTED]
User ID	16bc87586a7f410db3f70a8c7572353a
Tenant ID	fe30d90c17fb4242ada51900a0f5e173
Mobile Number	--
Description	--

Below this section is a "Project List" table with columns: Name, ID, Region, and Description. There is one row in the table, but its details are completely redacted. At the bottom right of the page is a "Guide Help" button.

- Step 2** Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#).

- Step 3** Update the database based on the obtained tenant ID:

```
update rds_restenant set realDomainName = 'Modified tenant name' where realDomainId = 'Tenant ID';
```

- Step 4** Ensure that the database is updated and retry the service.

----End

Verification

Retry the service after the database is updated.

Related Information

None

1.3.2.8 Node Status Fails to Be Changed During Cluster Scale-out

Symptom

The progress of scaling out a GaussDB(DWS) cluster stays at 85% for a long time (more than 10 minutes). **RdsGrowClusterTask** is displayed as failed when you view the scale-out job in the database.

Priority

Medium

Impact

The scale-out operation displays to be suspended, but is actually complete on the tenant side.

Possible Causes

- When a GaussDB(DWS) cluster is scaled out on the tenant side, a task for changing the status of new nodes to **active** will be performed on the management side. If the task fails (a rare case), the entire process is not affected but the operation progress is stuck at 85%. In this case, manually change the status of the database nodes on the management side.

Estimated Processing Duration

10 min

Handling Method

- Step 1** Log in to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and query the node status of the corresponding cluster in the **rds_instance** table.

```
select name,status,createType from rds_instance where clusterId=(select id from rds_cluster where name='Cluster_name') and createType='grow';
```

- Step 2** If the status of a node is **100** or **199**, change the status of the node in the **rds_instance** table to **200**.

```
update rds_instance set status='200' where name='Node_name';
```

- Step 3** Change the node billing status.

```
update rds_resource set isBilling=1,updateAt='yyyy-MM-dd HH:mm:ss' where instId in (select id from rds_instance where clusterId=(select id from rds_cluster where name='Cluster_name') and createType='grow');
```

Step 4 Remove the cluster scale-out information in **rds_action**.

```
delete from rds_action where objId=(select id from rds_cluster where name='Cluster_name');  
delete from rds_action where objId=(select id from rds_instance where clusterId=(select id from rds_cluster  
where name='Cluster_name'));
```

----End

Emergency Handling Procedure

Step 1 The cluster scale-out progress stays at 85% for a long time, which usually takes only 1 to 3 minutes. Connect to database **rms** and check whether the scale-out task in **taskmgr_job** fails at **RdsGrowClusterTask**.

Step 2 The **rds_instance** table shows that the status of the new nodes is **100** or **199**.

Step 3 Log in to a tenant node by referring to [Logging In to a Node in the Tenant Cluster](#) and run the **cm_ctl query -Cv** command to check whether the cluster has been scaled out.

----End

Verification

Clear task information on the page.

Related Information

None

1.3.2.9 Redistribution Is Suspended Because the Cluster Is Degraded

Symptom

During cluster redistribution, a node fault alarm is reported. On the console, the cluster status is **Degraded** and the task information is **Redistributing** or **Redistribution failed**.

Priority

High

Impact

If a node is faulty, data redistribution will be retried in the background. If the fault is not rectified in a timely manner, the redistribution is invalid and will fail.

Possible Causes

- During redistribution, some nodes are faulty due to network or hardware problems.

Estimated Processing Duration

30 min

Handling Method

1. Check the fault cause based on the location information of the node fault alarm. If the fault is caused by the NIC, rectify the fault and click **Retry** on the **View Redistribution Details** page on the tenant console.
2. If other node hardware is faulty, manually stop the redistribution process in the background. The page displays a message indicating that the redistribution fails.
3. After the redistribution failure message is displayed on the page, restore the faulty cluster on Service OM.

Emergency Handling Procedure

Step 1 Log in to a tenant node by referring to [Logging In to a Node in the Tenant Cluster](#) and view the redistribution logs. Logs indicate that the redistribution failed.

```
2021-08-26 02:56:15 worker 14019810594586 [scheduler.scheduler_config] step[4]: Redistribute failed, sleep 60 s and retry.
2021-08-26 02:56:15 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:56:16 worker 14019810594586 [scheduler.scheduler_config] step[4]: set session timeout = 0 successfully
2021-08-26 02:56:17 worker 14019810594586 [scheduler.scheduler_config] step[4]: set enable_analyze_check = off successfully
2021-08-26 02:56:17 worker 14019810594586 [scheduler.scheduler_config] step[4]: SET enable_random_datanode=off successfully
2021-08-26 02:56:17 worker 14019810594586 [scheduler.scheduler_config] step[4]: SET max_query_retry_times=0 successfully
2021-08-26 02:56:17 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:56:18 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:56:18 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect to DB postgres successfully
2021-08-26 02:56:18 worker 14019810594586 [scheduler.scheduler_config] step[4]: set enable_random_datanode=off successfully
2021-08-26 02:56:21 worker 14019810594586 [scheduler.scheduler_config] step[4]: set enable_analyze_check = off successfully
2021-08-26 02:56:21 worker 14019810594586 [scheduler.scheduler_config] step[4]: SET enable_random_datanode=off successfully
2021-08-26 02:56:21 worker 14019810594586 [scheduler.scheduler_config] step[4]: START TRANSACTION successfully
2021-08-26 02:56:22 worker 14019810594586 [scheduler.scheduler_config] step[0]: START TRANSACTION successfully
2021-08-26 02:56:22 worker 14019810594586 [scheduler.scheduler_config] step[0]: execute statement: LOCK TABLE ONLY scheduler.scheduler_config IN ACCESS SHARE MODE, exitOnError: 0, failed: ERROR: pooler: failed to create I connection
2021-08-26 02:56:22 worker 14019810594586 [scheduler.scheduler_config] step[0]: execute statement: Connect to db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:56:22 worker 14019810594586 [scheduler.scheduler_config] step[0]: detail: could not start up connection. Connect to db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:56:30 worker 14019810594586 [scheduler.scheduler_config] step[0]: execute statement: LOCK TABLE ONLY scheduler.scheduler_config IN ACCESS SHARE MODE, failed: ERROR: pooler: failed to create I connection
2021-08-26 02:56:30 worker 14019810594586 [scheduler.scheduler_config] step[0]: detail: could not start up packet: Connection timed out, remote database tn_5003
2021-08-26 02:56:33 worker 14019810594586 [scheduler.scheduler_config] step[4]: Redistributing failed, sleep 60 s and retry.
2021-08-26 02:59:31 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect db:dbname=postgres port=8000 user=rdsreader application_name=gs_redis password=xxx
2021-08-26 02:59:32 worker 14019810594586 [scheduler.scheduler_config] step[4]: connect to DB postgres successfully
2021-08-26 02:59:32 worker 14019810594586 [scheduler.scheduler_config] step[4]: set session timeout = 0 successfully
2021-08-26 02:59:34 worker 14019810594586 [scheduler.scheduler_config] step[4]: set enable_analyze_check = off successfully
```

Step 2 Locate the fault cause based on the node fault alarm and take measures to rectify the fault accordingly.

1. If the NIC is faulty, rectify the fault and try again.
2. If other faults occur, for example, the DN instance directory is abnormal, manually stop the redistribution process. When the page displays **Redistribution failed**, restore the cluster on Service OM.

If the task information does not change to **Redistribution failed**, run the following SQL statement and then restore the cluster:

```
update rds_action set action='REDISTRIBUTE_FAILURE' where type='Cluster' and objId='Cluster_ID';
```

Step 3 Ensure that all background faults are rectified. If the task information **Redistribution failed** remains unchanged, select **View Redistribution Details** in the **Operation** of the target cluster and click **Retry** to deliver a redistribution task again.

Step 4 After the preceding operations are complete, check the cluster task information on the page.

1. If the task information is not updated and the value of **redistributing** in the **cm_ctl** tenant log file is **No**, the cluster is restored.
2. If the task information changes to **Redistribution paused**, the cluster is being redistributed but the current time is not within the time window. The cluster is restored.
3. If the task information remains **Redistributing** and the redistribution process is displayed in the sandbox, the cluster is restored.

Run the following command to check whether any process exists during online and offline redistribution:

```
ps -aux | grep "gs_expand -t redistribute"
```

Run the following command to check whether data is being redistributed during offline scheduling. The value of **status** is **Running** in the command output.

```
gs_scheduler -t list
```

----End

Verification

After the cluster is restored, the cluster status is **Available** and the task information is **Redistribution failed**.

After the retry operation is complete on the redistribution details page, the cluster status is **Available** and the task information is cleared.

Related Information

None

1.3.2.10 Failed to Create a BMS Cluster Because the BMS RAID Group Is Incorrectly Configured

Symptom

When the progress of creating a BMS cluster reaches 86%, a message is displayed indicating that the cluster fails to be created, with error code BMS.0042 displayed in the logs.

Priority

High

Impact

BMS clusters cannot be created.

Possible Causes

The RAID group configuration is incorrect.

Estimated Processing Duration

30 min

Handling Method

View the job progress. **RdsInitInstanceTask** indicates that the database and agents are being installed. However, a BMS error is probably caused by faulty disks.

Log in to iBMC to view the BMS disk group. Choose **System > Storage Management** (for the old version iBMC, choose **System Info > Storage**) and place the data disks in **Logical Drive 0**.

The screenshot shows the iBMC interface with the following details:

- System** menu is selected.
- Storage Management** is chosen under the System menu.
- PCIe Card 6 (9460-8i)** is selected.
- Logical Drive 0** is highlighted with a red box.
- Disk3, Disk4, Disk5, Disk6, Disk7, Disk8** are listed under Logical Drive 0.
- Logical Drive 1, Logical Drive 2, Logical Drive 3, Logical Drive 4** are collapsed.
- Disk24, Disk44** are listed under Logical Drive 1.
- Controller Information** panel on the right shows:
 - Name: AVAGO MegaRAID SAS 9460-8i
 - Firmware Version: 5.090.00-2089
 - Health Status: Normal
 - Mode: RAID
 - Memory Size: 2048 MB

Emergency Handling Procedure

Contact BMS engineers to configure the RAID group again, as shown in the following figure.

The screenshot shows the iBMC interface under the 'System' tab. In the center, a list of storage components is displayed, with 'PCIe Card 6 (9460-8i)' selected. This selection reveals a detailed view of its logical drives. The 'Logical Drive 0' entry is highlighted with a red box. To the right, a panel titled 'Controller Information' provides specific details about the selected controller.

Controller Information
Name: AVAGO MegaRAID SAS 9460-8i
Firmware Version: 5.090.00-2089
Health Status: Normal

Verification

The BMS cluster is successfully created.

Related Information

None

1.3.2.11 Failed to Create a BMS Cluster Because the New Network Segments Are Not Added to the API Gateway Whitelist

Symptom

A BMS cluster fails to be created in **RdsCreateResourceTenantVpcTask** (progress at around 13%), with error code DWS.6000.

Priority

High

Impact

BMS clusters cannot be created.

Possible Causes

The new network segments are not added to the API gateway whitelist.

Estimated Processing Duration

30 min

Handling Method

Step 1 Query the failed step in the database.

1. Log in to the MySQL database of DWS Controller. For details, see [Logging In to the rms Database on the Management Side](#).

2. Run the following statement to query task **job_id**:

```
select task.job_id, task.task_name, task.begin_time, task.listener_num, task.retry_num,
task.execution_status from rds_instance ins left join taskmgr_task task on ins.jobId=task.job_id left
JOIN taskmgr_job job on task.job_id=job.job_id where ins.`name` like '%Cluster_name%' order by
task.job_id,task.begin_time;
```

```
17
18 2c90803276e1850301771e88d3bd18bc | RdsCreatePortTask      | NULL          | 0 | 0 | NULL          |
19 | 2c90803276e1850301771e88d3bd18bc | BindPublicIPTask | NULL          | 0 | 0 | NULL          |
20 | 2c90803276e1850301771e88d3bd18bc | ResTenantTask    | 2021-01-20 06:43:44 | 0 | 0 | SUCCESS        |
21 | 2c90803276e1850301771e88d3bd18bc | ResUserTask     | 2021-01-20 06:43:49 | 0 | 0 | SUCCESS        |
22 | 2c90803276e1850301771e88d3bd18bc | RdsBindEFSTask   | 2021-01-20 06:43:59 | 0 | 0 | SUCCESS        |
23 | 2c90803276e1850301771e88d3bd18bc | RdsCreateResourceTenantVpcTask | 2021-01-20 06:44:09 | 30 | 0 | FAIL          |
24 | 2c90803276e1850301771e88d40b18bc | RdsInstanceStateMonitorTask | NULL          | 0 | 0 | NULL          |
25 | 2c90803276e1850301771e88d40b18bc | RdsPingInstanceManagerIpTask | NULL          | 0 | 0 | NULL          |
26 | 2c90803276e1850301771e88d40b18bc | CreatePcEndpointServiceTask | NULL          | 0 | 0 | NULL          |
27 | 2c90803276e1850301771e88d40b18bc | StartupServerTask   | NULL          | 0 | 0 | NULL          |
28 | 2c90803276e1850301771e88d40b18bc | RdsInstanceStateCreateCompletedTask | NULL          | 0 | 0 | NULL          |
29 | 2c90803276e1850301771e88d40b18bc | RdsCreateInstanceTask  | NULL          | 0 | 0 | NULL          |
30 | 2c90803276e1850301771e88d40b18bc | RdsInitInstanceTask  | NULL          | 0 | 0 | NULL          |
...
```

Obtain the value of **job_id** whose **execution_status** is **FAIL**.

Step 2 Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.

Step 3 You can view log information in different ways based on the log obtaining method.

- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.
- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.

```
cat ossres-dws.log | grep jobId | grep ERROR
```

NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 4 The following error message is displayed: "error_msg":"The IAM user is not authorized to access the API: op_svc user from untrusted ip","error_code":"APIGW.0302"

```
2021-01-20 06:44:14,256|2c90803276e1850301771e88d3bd18bc|ERROR|35f2bec748b04fec8c870e5dd4c22538_2021-01-20 06:43:33 dwscontroller-76c46c4bc8-k8tjn Get highway subnet parameter. Response http status code is: 403; Response message is: {"error_msg":"The IAM user is not authorized to access the API: op_svc user from untrusted ip","error_code":"APIGW.0302","request_id":"66a89f40e40251ff6f4b1ae4ff61cb6a02"}
```

Step 5 According to **Step 1** and **Step 4**, this problem is a network whitelist issue. Contact the API gateway personnel to check whether new network segments are added. If

yes and the newly added segments are used by a CloudAutoDeploy-CDK cluster/DWS Controller server, this problem occurs.

----End

Emergency Handling Procedure

Step 1 Contact the installation personnel to check whether new network segments are added. If yes, collect related information.

Step 2 Add the new network segments to the API gateway whitelist.

/opt/apigateway/resty/etc/router/conf/configure.ini

```
is_hcs_mode=false

[fusioncloud]
iam_url_management=iam-cache-proxy.cn-suzhouivarm-1.ihcscrm.com:26335
region_id=cn-suzhouivarm-1
iam_username=apiGateway_admin
iam_service_key=0000000100000000170C94DFFB9E00B315198853DA4094599BBAAB47B4C1A449FA88E01680E72D2CB
trusted_ips=11.68.0.0/16;172.30.30.0/24;172.30.32.0/24;172.30.34.0/24;172.30.31.0/24;172.30.27.0/24
-- INSERT -- W10: Warning: Changing a readonly file
```

----End

Verification

The BMS cluster is created successfully.

Related Information

None

1.3.3 Connectivity

1.3.3.1 EIP Cannot Be Used Due to Lost Policy Route

Symptom

EIP cannot be used after the VM on the node bound with the EIP is restarted, or the VM where the CN is deployed is restarted.

Priority

High

Impact

Users cannot use the EIP to connect to the cluster.

Possible Causes

The DWS policy-based route is not correctly loaded. As a result, nodes cannot return packets in which EIP is required after receiving them.

Estimated Processing Duration

20 min

Handling Method

1. Log in to a cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the **ip rule show** command as user **Mike** to check whether a policy-based route whose ID is **100** exists. This route is used to set the EIP connection and is forwarded by NIC **eth1** by default.
0: from all lookup local
32765: from 192.168.0.172 lookup 100
32766: from all lookup main
32767: from all lookup default
2. Go to the **/etc/init.d/** directory and check the **addRoute** file.
Run the **sh addRoute** command.
3. Run the **ip rule show** command again to check whether the policy-based route exists. If yes, check whether the EIP can be used to connect to the cluster.

Emergency Handling Procedure

If the policy-based route whose ID is **100** cannot be found in the routing information, run the following command to manually add the policy-based route:

```
sh /etc/init.d/addRoute
```

Verification

Use the EIP to connect to the data warehouse cluster again and check whether the connection is normal.

Related Information

None

1.3.3.2 Network Disconnection Between DWS and SwiftAdapter

Symptom

When DWS is upgraded along with the HCS upgrade from HCS 8.0.1 to HCS 8.0.2, a cluster node cannot download the upgrade software package.

1. A cluster node fails at pinging the **url object-store.cn-xxx.cmbmpp.cn** to download software packages.
2. A cluster node fails at pinging the **domain-mapping IP address** (the domain-mapping IP address is a SwiftAdapter IP address).

Priority

High

Impact

The cluster node cannot download the software package.

Possible Causes

1. The SwiftAdapter equal-cost route is not configured in the network configuration.
2. The swiftadapter IP address is not in the internal public network whitelist of the BMS gateway.

Estimated Processing Duration

90 min

Handling Method

To perform DWS upgrade, connect to Swift to download the upgrade software package.

Process for downloading the software package:

1. A DWS cluster node connects to the Swift reverse proxy VIP (swiftadapter IP address) in the management zone by mapping the internal public network IP address.
2. The equal-cost route of the Swiftadapter IP address points to the PodLB LVS node. The PodLB LVS node communicates with the Swift storage in the management zone. The BMS node downloads the upgrade package from the Swift storage.

Step 1 Contact the cloud infrastructure support personnel to log in to any management VM in the management zone and ping the floating IP address of SwiftAdapter.

- If the pinging fails, it indicates that no equal-cost route is configured for the floating IP address of the SwiftAdapter. Check the equal-cost route configuration of the switch by referring to the [HCS x.x.x Integration Design Guide](#).
- If the pinging is successful, go to [Step 2](#).

Step 2 Log in to the BMS gateway node and query the whitelist configuration of the internal public network.

```
cps template-ext-params-show -service baremetal-gateway neutron-hypervbm-agent001
```

Check whether the floating IP address of SwiftAdapter is in the whitelist:
neutron_hypervbm_ovs.DEFAULT.inner_service_cidr.

If not, add it manually.

2AA10_2288HV5_BMSGW_01:~ # cps template-ext-params-show --service baremetal-gateway neutron-hypervbm-agent001	
Property	Value
hypervbm_ovs_agent.DEFAULT.dhcp_network_filter	ed7d18d3-84c0-4a18-abed-287a3105f01c
hypervbm_ovs_agent.DEFAULT.fip_gw_mac	[REDACTED] /20
hypervbm_ovs_agent.DEFAULT.isolate_relay_cidr	[REDACTED] /32
hypervbm_ovs_agent.DEFAULT.isolate_tenant_cidrs	
hypervbm_ovs_agent.DEFAULT.metadata_external	
hypervbm_ovs_agent.agent.enable_ipv6	True
hypervbm_ovs_agent.agent.enable_mlag	True
hypervbm_ovs_agent.agent.mlag_vrid	80
hypervbm_ovs_agent.ovs.avg_queue	enable
hypervbm_ovs_agent.ovs.dedicate_queue	lacp
hypervbm_ovs_agent.ovs.flow_table_on_dp	True
neutron_hypervbm_ovs.DEFAULT.inner_service_cidr	[REDACTED] /24, [REDACTED] /32

----End

Emergency Handling Guide

Step 1 If the switch does not configure the equal-cost route, configure it by referring to the *Integration Design Guide*.

Step 2 Manually add the BMSGW internal public network whitelist.

cps template-ext-params-update –service baremetal-gateway neutron-hypervbm-agent001

--parameter neutron_hypervbm_ovs.DEFAULT.inner_service_cidr=The IP address list with the missing IP addresses added

----End

Verification

The software package can be downloaded to the cluster node.

Related Information

None

1.3.4 Snapshot

1.3.4.1 Backing Up Tenant Plane Data to OBS After Switching to the OBS Scenario

Scenario

If OBS is not used, the data of the DWS management plane is stored in Swift, and snapshots cannot be created for backup and restoration on the tenant plane. To create snapshots, you need to use OBS 3.0, enable the cluster snapshot function, and back up tenant plane data to OBS 3.0.

NOTICE

The OBS switch only backs up the tenant plane data to OBS (enable the snapshot function). The DWS management plane data is still stored in Swift.

Prerequisites

- OBS 3.0 has been installed on the platform, and you have obtained the global domain name of OBS. You can obtain the value of **OBSv3-Console_default_region_domain** in the "2.2 Tool_generated_Params" sheet of the LLD deployment parameter table exported from the HCC Turnkey project during OBS deployment.
- OBS 3.0 has been installed on the basic platform, and the IP address of OBS has been obtained from LLD.

Procedure

Step 1 Log in to CloudScope using a browser as a system administrator.

- URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op_cdk_sso**
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

Step 2 In the top navigation pane, choose **Services > Change Mgmt > CloudAutoDeploy-CDK**.

Step 3 Choose **Change Mgmt > Upgrade** on the left, select the **dwscontroller** instance names, and click **Next**.

Step 4 Search for **obs.endpoint** in the parameter box and change the value to the actual OBS endpoint information in the format of *OBS global domain name:443*. You can obtain the value of **OBSv3-Console_default_region_domain** in the "2.2 Tool_generated_Params" sheet of the LLD deployment parameter table exported from the HCC Turnkey project during OBS deployment. Example value: **obsv3.sa-fb-1.external-a3.com:443**

Step 5 Click **Next** and then click **Upgrade**.

Step 6 Delete the **dwscontroller** containers and restart them for the configuration to take effect.

1. Log in to the CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).
2. Query the pods.
kubectl get pods -n dws
3. Delete the old containers and restart them. The container names are obtained in [Step 6.2](#).
kubectl delete pod dwscontroller_pod_name -n dws
4. Wait for about 3 minutes and run the following commands to check whether the containers are started:
kubectl get pods -n dws
kubectl describe pod dwscontroller_pod_name -n dws

Step 7 Log in to ManageOne Maintenance Portal via <https://ManageOne Maintenance Portal URL:31943>. Alternatively, log in to the unified portal and choose **OperationCenter**.

- Password login: Enter the username and password of the account.
 - Default account: **bss_admin**

 **NOTE**

For ManageOne upgraded from 8.2.0 or earlier, the default username is **admin**.
For ManageOne 8.2.1 or later, the default username is **bss_admin**.

- Preset password: See the preset password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter the PIN.

Log in to ManageOne Maintenance Portal.

Step 8 On the ManageOne Maintenance Portal homepage, click **Service OM** in the **Common Links** area and select your region to access Service OM.

Step 9 Choose **Services > Resources > Compute Resources > VMs**, search for the Console-Static node in the search box, and record the IP address of the node.

Step 10 Use PuTTY to log in to the Console-Static-01 node as user **opsadmin**, and switch to user **root**.

su - root

- For details about the default password of user **opsadmin**, see the "Type A (Background)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).
- For details about the default password of user **root**, see the "Type A (Background)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).

Step 11 Modify the **config.js** configuration file in the **/opt/cloud/static/private/dws** directory.

1. Run the following command to open the configuration file:

vim /opt/cloud/static/private/dws/config.js

2. Modify the following parameters:

```
"snapshotSwitch": "true"  
"obsEndpointSwitch": "obsv3"
```

3. Press **:wq!** to save the change and exit.

Step 12 Modify the **index.html** configuration file in the **/opt/cloud/static/private/dws** directory to ensure that the console redirection takes effect.

1. Run the following command to open the configuration file:

vim /opt/cloud/static/private/dws/index.html

2. Modify the following parameter:

Set **config.js?yyyymmddhhmmss** to the current time.

```
<!DOCTYPE html>
<html ng-app="app">
<head>
<meta charset="utf-8">
<title>ng-bind=$root.i18n.console_term_title_label</title>
<meta name="description" content="Cfwork">
<!-- <meta name="viewport" content="width=device-width"> -->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta http-equiv="Expires" content="0">
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Cache-control" content="no-cache">
<meta http-equiv="Cache" content="no-cache">
<meta http-equiv="Access-Control-Allow-Origin" content="">
<meta name="format-detection" content="telephone=no">
<link type="image/x-icon" href="https://console-static.cn-dwsglobal-1.dwscloud.com/static/dws/favicon.ico?20210320105631" rel="icon" />
<link rel="stylesheet" type="text/css" href="https://console-static.cn-dwsglobal-1.dwscloud.com/static/dws/theme/default/css/vendor_combined-business.css?20210320105631" />
<script type="text/javascript" src="https://console-static.cn-dwsglobal-1.dwscloud.com/static/dws/config.js?20210320105631"></script>
<script type="text/javascript" src="https://console-static.cn-dwsglobal-1.dwscloud.com/static/dws/runtime.js?20210320105631"></script>
</head>
```

3. Press :wq! to save the change and exit.

Step 13 Log in to the Console-Static-02 node and repeat **Step 11** to **Step 12** to modify the file on the 02 node.

Step 14 Obtain the OBS_AK and OBS_SK for connecting to OBS.

1. Log in to the CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).
2. Connect to the rms database. The database IP address and port number are obtained from [Logging In to the rms Database on the Management Side](#), and the database access password is obtained from the environment administrator.

```
mysql -hDatabase_IP_address -PDatabase_port_number -uecf -pDatabase_access_password;
use rms;
```

3. Run the following SQL statement to query OBS_AK and OBS_SK and record the AK value.
`select ak,sk from rds_restenant;`

4. Run the \q command to exit.

5. Run the following commands to start the tool:

```
cd opsTool
java -jar SccTool.jar
```

6. Enter 3 Ciphertext_SK and press **Enter** to decrypt Ciphertext SK. Ciphertext SK is obtained in [14.3](#).

In the command output, the value below **Decrypt result** is the decrypted SK. Record the SK value.

```
International Encrypt, please input 1 and ' ' and password's plaintext
International Encrypt password in file, please input 2 and ' ' and absolute path of file
WCC International_encrypt Decrypt, please input 3 and ' ' and password's ciphertext
WCC International_encrypt Decrypt password in file, please input 4 and ' ' and absolute path of file
Business Encrypt, please input 5 and ' ' and password's plaintext
Business Encrypt password in file, please input 6 and ' ' and absolute path of file
Business Decrypt, please input 7 and ' ' and password's ciphertext
Business Decrypt password in file, please input 8 and ' ' and absolute path of file
WCC Decrypt and International Encrypt, please input 9 and ' ' and password's plaintext
WCC Decrypt and International Encrypt password in file, please input 10 and ' ' and absolute path of file
International Decrypt and WCC Encrypt, please input 11 and ' ' and password's plaintext
Business Decrypt and International Encrypt, please input 12 and ' ' and password's plaintext
Business Decrypt and International Encrypt password in file, please input 13 and ' ' and password's plaintext
Business Decrypt and International Encrypt, please input 14 and ' ' and password's plaintext
3 (OK)
International Encrypt, please input 1 and ' ' and password's plaintext
International Encrypt password in file, please input 2 and ' ' and absolute path of file
WCC International_encrypt Decrypt, please input 3 and ' ' and password's ciphertext
WCC International_encrypt Decrypt password in file, please input 4 and ' ' and absolute path of file
Business Encrypt, please input 5 and ' ' and password's plaintext
Business Encrypt password in file, please input 6 and ' ' and absolute path of file
Business Decrypt, please input 7 and ' ' and password's ciphertext
Business Decrypt password in file, please input 8 and ' ' and absolute path of file
WCC Decrypt and International Encrypt, please input 9 and ' ' and password's plaintext
WCC Decrypt and International Encrypt password in file, please input 10 and ' ' and absolute path of file
International Decrypt and WCC Encrypt, please input 11 and ' ' and password's plaintext
Business Decrypt and International Encrypt, please input 12 and ' ' and password's plaintext
Business Decrypt and International Encrypt password in file, please input 13 and ' ' and password's plaintext
3 (OK)
International Encrypt, please input 1 and ' ' and password's plaintext
International Encrypt password in file, please input 2 and ' ' and absolute path of file
WCC International_encrypt Decrypt, please input 3 and ' ' and password's ciphertext
WCC International_encrypt Decrypt password in file, please input 4 and ' ' and absolute path of file
Business Encrypt, please input 5 and ' ' and password's plaintext
Business Encrypt password in file, please input 6 and ' ' and absolute path of file
Business Decrypt, please input 7 and ' ' and password's ciphertext
Business Decrypt password in file, please input 8 and ' ' and absolute path of file
WCC Decrypt and International Encrypt, please input 9 and ' ' and password's plaintext
WCC Decrypt and International Encrypt password in file, please input 10 and ' ' and absolute path of file
International Decrypt and WCC Encrypt, please input 11 and ' ' and password's plaintext
Business Decrypt and International Encrypt, please input 12 and ' ' and password's plaintext
Business Decrypt and International Encrypt password in file, please input 13 and ' ' and password's plaintext
3 (OK)
```

Decrypt result:
84Enj lJmjCfeoV3botQq

7. Press **Ctrl+C** to exit the Java program.

Step 15 Query details about the current tenant.

1. Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).
2. Connect to the rms database. The database IP address and port number are obtained from [Querying MySQL Database Information](#), and the database access password is obtained from the environment administrator.

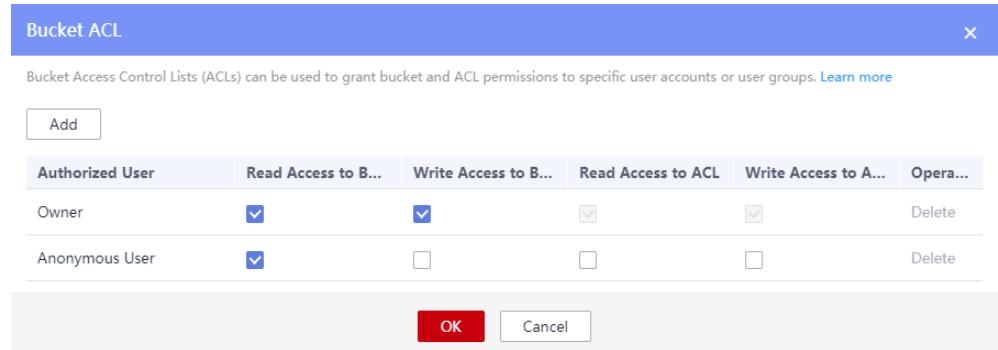
```
mysql -hDatabase_IP_address -PDatabase_port_number -uecf -pDatabase_access_password;
use rms;
```

3. Run the following statement to query the current tenant ID:
`select realDomainId from rds_restenant;`
4. Record all tenant IDs.

Step 16 Connect to the OBS client using OBS Browser+ with the OBS AK obtained in [14.3](#), the decrypted OBS SK in [14.6](#), and the IP address of the OBS server obtained in the prerequisites.

Step 17 Create buckets for all tenants in the current environment.

1. Click **Create Bucket**. Set **Region** to the region ID of the current environment and **Bucket Name** to **rdsbucket-sa-fb-1.dws.Tenant ID**. *sa-fb-1* indicates the region ID of the current environment, and *Tenant ID* is obtained in [15.4](#).
2. After the bucket is created, choose **Operation > Bucket ACL**, and select permissions for the bucket by referring to the following figure. Then click **OK**.



3. Repeat [17.1](#) to [17.2](#) to create buckets for all tenants queried in [Step 15](#).

Step 18 Update the bucket names of all tenants in the **rds_restenant** table.

1. Connect to the **rms** database.
2. Run the following statement to update the **rds_restenant** table. *Bucket_name* indicates the name of the bucket created in [Step 17](#).
`update rds_restenant set obsBucket = Bucket_name where realDomainId = Tenant_ID`
3. Repeat [18.2](#) to update the bucket names of all tenants queried in [Step 15](#).

Step 19 Log in to the ManageOne Operation Portal, select the created cluster, and click **Create Snapshot**. If the snapshot can be created, the system has been switched to OBS 3.0.

----End

1.3.4.2 Failed to Create a Snapshot

Symptom

An error message is displayed when the user clicks **Create Snapshot**.

Priority

Medium

Impact

Cluster snapshots cannot be created.

Possible Causes

- DWS Controller cannot connect to the cluster using SSH.
- The cluster fails to connect to OBS.
- The cluster is faulty.

Estimated Processing Duration

30 min

Handling Method

- Check the network communication.
- Check the cluster status.
- DWS Controller cannot connect to the cluster using SSH.
- The cluster fails to connect to OBS.
- The cluster is faulty.

Emergency Handling Procedure

Step 1 Connect to database **rms** by referring to [Logging In to the rms Database on the Management Side](#). Search for the cluster ID in the **rds_cluster** table, and then search for **managelp** of all nodes in the cluster in the **rds_instance** table.
`select id from rds_cluster where name='Cluster name';`
`The select name,managelp from rds_instance where clusterId='Cluster ID';`

Step 2 Log in to DWS Controller by referring to [Logging In to a dwscontroller Pod](#).

Step 3 Check whether DWS Controller can ping the cluster nodes.

On DWS Controller, ping **managelp** queried in **Step 1**.

- If the operation fails, DWS Controller and the cluster are disconnected. Rectify the network fault.
- Otherwise, go to **Step 4**.

Step 4 Log in to a cluster node by referring to [Logging In to a Node in the Tenant Cluster](#) and check whether the cluster can access OBS.

- If you cannot log in to the cluster, go to [Step 5](#).
- If OBS cannot be pinged, the network from the cluster to OBS is faulty. Rectify the network fault.
- If OBS can be pinged, go to [Step 6](#).

Step 5 Connect to database **rms** by referring to [Logging In to the rms Database on the Management Side](#) and check the cluster status.

```
select id,name,isFrozen,status from rds_cluster where name='Cluster name';
```

id	name	isFrozen	status
c99eed7a-2060-48d7-b7c7-52fc4a3031f4	xxxxxx03	0	200

1 row in set (0.00 sec)

- If the value of **isFrozen** is **1**, the cluster is frozen. Restart the cluster.
- If the value of **status** is **300**, the cluster is faulty. Troubleshoot the fault.

Step 6 View the DWS Controller backend logs.

1. Query the cluster snapshot thread ID by cluster name.

Log in to all **dwscontroller** nodes by referring to [Logging In to a dwscontroller Pod](#) and run the following command to filter DWS Controller backend logs by cluster name:

```
grep '\"name\":\"Cluster name\"' /opt/cloud/3rdComponent/tomcat/logs/ossres-dws*.log
```



- NOTE**
1. **ossres-dws** is followed by an asterisk (*), indicating that all files with their names started with **ossres-dwscontroller** are scanned.
 2. In the preceding command, Cluster ID indicates the ID obtained in [Step 1](#).

2. If different tenants have the same cluster name, there may be more than one result. Each result is displayed in the following format.

```
2017-08-24 18:48:03,700|ff808015e13f880015e1517ea1d00fc|INFO|initDB config json : {"name":"dws-demo004","id":"8c7817b7-fb70-4606-815a-b2fd0a06a437","datastore": "dws","version": "1.0.0-ecra","clusterMode": "sharding","dbPort": 8000,"dbUser": "dbadmin","dbAdmin": "dwsAdmin","dbMonitorUser": "dwsMetric","dbBackupUser": "dwsBackup","haMonitorIps": "10.125.0.0/16","mngNetwork": "10.125.0.0/16","ntpServerIP": "10.125.0.209","replUser": "dwsRepl","timeZone": "UTC","apiGatewayAddr": "10.125.0.11:443","cesVersion": "V1.0","cesTtl": "172800","projectId": "ec1c07d2ca2d4d328255feb3b2aa8540","regionId": "eu-de","cesAK": "N95RKEY2VP8V8ATOKDKQ","curlInstanceId": "a314c5e6-17d4-44c8-b46cb776b7e58213","customConfigs": {"bakKeepDay": "null","clusterName": "mppdbCluster","serviceProvider": "DT","localDisk": "false","ssl": "true"}, "instances": [{"id": "076ceb12-dce0-488c-bd44-35e251b659d0","type": "dws","name": "dws-demo004-dws-dn-6-1","group": "dn-6","cidr": "192.168.0.0/16","internalCidr": "172.16.0.0/16","trafficIclp": "192.168.42.122","trafficVip": "192.168.42.122","internalIpp": "172.16.99.87","internalVip": "172.16.99.87","guestAgentVersion": "V1.1.0","customConfigs": {"ssl": "true"}, "resources": [{"type": "SATA","size": 100,"tag": "backup"}, {"type": "SAS","size": 100,"tag": "data"}, {"type": "SAS","size": 100,"tag": "data"}, {"type": "SATA","size": 100,"tag": "log"}], "promotionTier": 0,"azCode": "eu-de-01"}, {"id": "1016434effe6-4e1f-8432-8f788040ead1","type": "dws","name": "dws-demo004-dws-dn-7-1","group": "dn-7","cidr": "192.168.0.0/16","internalCidr": "172.16.0.0/16","trafficIclp": "192.168.42.112","trafficVip": "192.168.42.112","internalIpp": "172.16.99.78","internalVip": "172.16.99.78","guestAgentVersion": "V1.1.0","customConfigs": {"ssl": "true"}, "resources": [{"type": "SATA","size": 100,"tag": "backup"}, {"type": "SAS","size": 100,"tag": "data"}, {"type": "SAS","size": 100,"tag": "data"}], "promotionTier": 0,"azCode": "eu-de-01"}, {"id": "26e0d7c9-be70-4719-99a6-9e85475e6f8d","type": "dws","name": "dws-demo004-dws-dn-20-1","group": "dn-20","cidr": "192.168.0.0/16","internalCidr": "172.16.0.0/16","trafficIclp": "192.168.42.108","trafficVip": "192.168.42.108","internalIpp": "172.16.99.76","internalVip": "172.16.99.76","guestAgentVersion": "V1.1.0","customConfigs": {"ssl": "true"}, "resources": [{"type": "SAS","size": 100,"tag": "data"}, {"type": "SATA","size": 100,"tag": "backup"}, {"type": "SAS","size": 100,"tag": "data"}]
```

 NOTE

1. **dws-demo004** indicates the cluster name for query.
2. **ff8080815e13f880015e1517ea1d00fc** indicates the thread ID of the cluster creation task found during the search.
3. **2017-08-24 18:48:03** indicates the time displayed on the Linux server where DWS Controller is deployed when the cluster is being created.
4. **ec1c07d2ca2d4d328255feb3b2aa8540** indicates **projectId** of a tenant.

3. Filter DWS Controller logs.

Log in to all DWS Controller services and run the following command to filter backend logs by thread ID:

```
grep "Thread ID" /opt/cloud/3rdComponent/tomcat/logs/ossres-dws*.log
```

Based on the error log information, check the failed step and handle it.

Step 7 Log in to the cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and view snapshot creation logs of the cluster.

```
[root@host-172-16-0-83 ~]# cd /home/Ruby/log  
[root@host-172-16-0-83 log]# vi cloud-dws-deploy.log
```

Information about some logs is as follows:

```
[2017-08-24 11:51:35,302][DEBUG][backup][127121][139667878192960][backup.py 902][Start load backup JSON.]  
[2017-08-24 11:51:35,306][DEBUG][backup][127121][139667878192960][backup.py 911][Success to load backup JSON.]  
[2017-08-24 11:51:35,306][DEBUG][backup][127121][139667878192960][backup.py 572][Start prepare backup.]  
[2017-08-24 11:51:35,307][DEBUG][backup][127121][139667878192960][backup.py 56][start check cluster status]  
[2017-08-24 11:51:35,754][DEBUG][backup][127121][139667878192960][backup.py 73][The cluster status is Normal.]  
[2017-08-24 11:51:35,981][INFO][backup][127121][139667878192960][backup.py 472][/DWS/backup/data had been created.]  
[2017-08-24 11:51:36,209][INFO][backup][127121][139667878192960][backup.py 472][/DWS/backup/log had been created.]  
[2017-08-24 11:51:36,224][DEBUG][backup][127121][139667878192960][backup.py 617][End prepare backup.]  
[2017-08-24 11:53:04,254][DEBUG][backup][129754][140225321170752][backup.py 902][Start load backup JSON.]  
[2017-08-24 11:53:04,259][DEBUG][backup][129754][140225321170752][backup.py 911][Success to load backup JSON.]  
[2017-08-24 11:53:04,260][DEBUG][backup][129754][140225321170752][backup.py 627][Start backup DWS.]  
[2017-08-24 11:53:04,260][INFO][backup][129754][140225321170752][backup.py 632][cmd: touch /DWS/ backup/data/hostnode.ini.]  
[2017-08-24 11:53:04,502][INFO][backup][129754][140225321170752][backup.py 637][Success to create file hostnode.ini.]  
[2017-08-24 11:53:04,503][DEBUG][backup][129754][140225321170752][backup.py 400][Start stop cluster in smart mode.]  
[2017-08-24 11:53:22,411][INFO][backup][129754][140225321170752][backup.py 404][Authorized users only. All activities may be monitored and reported.  
cm_ctl: stop cluster.  
cm_ctl: stop nodeid:1  
cm_ctl: stop nodeid:2  
cm_ctl: stop nodeid:3  
.....  
cm_ctl: stop cluster successfully.  
cm_ctl: stopping the ETCD cluster.  
....  
cm_ctl: successfully done.]  
[2017-08-24 11:53:22,411][INFO][backup][129754][140225321170752][backup.py 409][Stop cluster successfully.]  
[2017-08-24 11:53:22,412][DEBUG][backup][129754][140225321170752][backup.py 336][Start set backup mode.]
```

```
[2017-08-24 11:53:22,412][INFO][backup][129754][140225321170752][backup.py 342][gs_guc set -Z  
datanode -N all -l all -c "default_transaction_read_only = on" && gs_guc set -Z coordinator -N all -l all -c  
"default_transaction_read_only = on"]  
[2017-08-24 11:53:23,576][DEBUG][backup][129754][140225321170752][backup.py 348][Success to set  
backup mode.]
```

- There are two steps in snapshot creation: Data in the entire database is backed up; snapshot files are uploaded to the OBS bucket. Troubleshoot related problems based on the error information in the logs.
- If the log prompts that the files failed to be uploaded to the bucket, check the network.
- If no current snapshot creation information exists in the logs and the problem cannot be located using logs, contact the developers.

----End

Verification

A snapshot can be created.

Related Information

None

1.3.4.3 Failed to Restore a Cluster Using Its Snapshot

Symptom

A message is displayed indicating a restoration failure after a user clicks **Restore**.

Priority

High

Impact

The cluster cannot be restored using a snapshot.

Possible Causes

- DWS Controller fails to connect to the cluster.
- The cluster fails to connect to OBS.
- Snapshots fail to be downloaded from OBS.
- Cluster restoration fails.

Estimated Processing Duration

30 min

Handling Method

Check the cluster status. Ensure that the communication from DWS Controller to the cluster and from the cluster to OBS is normal. Then, log in to DWS Controller and the cluster separately and view related logs for troubleshooting.

Emergency Handling Procedure

Step 1 Connect to database **rms** by referring to [Logging In to a Node in the Tenant Cluster](#). Search for the cluster ID in the **rds_cluster** table, and then search for **managelp** of all nodes in the cluster in the **rds_instance** table.

```
select id from rds_cluster where name='Cluster name';  
The select name,managelp from rds_instance where clusterId='Cluster ID';
```

Step 2 Check whether DWS Controller can ping the cluster.

On DWS Controller, ping **managelp** queried in [Step 1](#).

- If the operation fails, DWS Controller and the cluster are disconnected. Rectify the network fault.
- If OBS can be pinged, go to [Step 3](#).

Step 3 Log in to a cluster node by referring to [Logging In to a Node in the Tenant Cluster](#) and check whether the cluster can access OBS.

- If OBS cannot be pinged, the network from the cluster to OBS is faulty. Rectify the network fault.
- If OBS can be pinged, go to [Step 4](#).

Step 4 Log in to the node in the cluster and check the cluster recovery log.

```
[root@host-172-16-0-83 ~]# cd /home/Ruby/log  
[root@host-172-16-0-83 log]# vi cloud-dws-deploy.log
```

If an error message is reported, handle problems based on log prompts.

- If the log prompts that downloading the snapshot file to the local host fails, check the network.
- If the restoration fails, contact relevant personnel to locate the fault.

----End

Verification

The cluster can be restored using a snapshot.

Related Information

None

1.3.5 Upgrade

1.3.5.1 Cluster Upgrade Is Interrupted Due to Packet Delivery Errors

Symptom

When packets are sent to the cluster during the upgrade, an error message is displayed on Service OM, indicating that packet fails to be delivered.

Priority

High

Impact

The cluster upgrade fails.

Possible Causes

The plugin information of the cluster is incorrect in the database.

Estimated Processing Duration

30 min

Handling Method

1. Obtain the ID of the failed job on Service OM, log in to the dwscontroller container, and obtain the execution details of the packet delivery job based on the job ID.
The message indicating that plugin conf is empty is reported in the packet delivery job. The plugin information of the cluster may fail to be queried in the database.
2. Log in to database **rms**, search for plugin IDs of the cluster in the **cluster_plugin** table by cluster ID, and check whether the plugin information exists in the plugin info table.

Emergency Handling Procedure

- Step 1** Log in to ManageOne Maintenance Portal and click **Service OM** in the frequently used links area.
- Step 2** Choose **Service List > Data Warehouse Service**. In the navigation pane, choose **Upgrade Management > Upgrade**. Click **Details** on the right of the cluster name to obtain the jobId information about the packet delivery failure.
- Step 3** Obtain DWSController log files by referring to [Collecting dwscontroller Logs](#). You can download the log files from the ManageOne log platform or obtain them from the background.
- Step 4** You can view log information in different ways based on the log obtaining method.
- After obtaining logs on ManageOne, you can search for **jobId** in the log file to obtain the logs.

- After obtaining logs from the background, run the **cat** command and filter by **jobId** to obtain cluster creation logs.

```
cat ossres-dws.log | grep jobId | grep ERROR
```

 NOTE

Note that log files are randomly distributed on different management VMs. If log files are downloaded from the ManageOne platform, you need to decompress the ZIP packages of all logs to view the **var_log_dws_controller_ossres-dws** files in all folders. If log files are downloaded from the background and you cannot obtain the log files by running the **cat** command on a DWSController container, you need to log in to another container and run the **cat** command again.

Step 5 The message indicating that plugin conf is empty is reported in the packet delivery job. The plugin information of the cluster may fail to be queried in the database.

Step 6 Log in to the GaussDB(DWS) database on the management side by referring to [Logging In to the rms Database on the Management Side](#), search for plugin IDs of the cluster in the **cluster_plugin** table by cluster ID, and check whether the plugin information exists in the plugin info table.

```
The select pluginId from cluster_plugin where clusterId = 'Cluster ID';  
select * from plugin_info where id = '{Obtained pluginID}';
```

Step 7 In earlier versions of GaussDB(DWS), the PostGIS plugin is supported. It is possible that historical plugin information is not recorded in the database. Log in to the dwscontroller container by referring to [Logging In to a dwscontroller Pod](#) and query the name and ID of the plugin supported by the target version in the **/opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/dataStoreSpec/datastoreSpec_dws.xml** file.

```
cat /opt/cloud/3rdComponent/tomcat/webapps/rds/WEB-INF/classes/xml/  
dataStoreSpec/datastoreSpec_dws.xml | grep plugin
```

```
<PluginConfig>  
  <plugin type="postgis" id="42e50901-9ab2-419c-9c22-a4411a053d96" version="2.4.2.dws.3" />  
</PluginConfig>
```

Step 8 Modify the **cluster_plugin** table in the database and update the plugin information of the current cluster version to the plugin information supported by the target version in the **datastoreSpec_dws.xml** file.

```
update cluster_plugin set pluginId = 'Plugin ID' where clusterId = 'Cluster ID';
```

Step 9 On the Service OM page, reset the cluster status to **Waiting** and perform packet delivery and upgrade operations on the cluster again.

----End

Verification

On the Service OM page, reset the cluster status to perform the package delivery and upgrade again until the upgrade is complete.

Related Information

None

1.3.5.2 Failed to Upgrade the Cluster

Symptom

Failed to upgrade the cluster due to timeout.

Priority

High

Impact

The cluster cannot be upgraded.

Possible Causes

- There is a large amount of cluster metadata. As a result, it takes a long time to back up metadata before the upgrade.
- Services are accessed during the upgrade and the cluster restart takes a long time.

Estimated Processing Duration

30 min

Handling Method

1. On Service OM, check the job ID of the failed upgrade. Log in to DWS Controller by referring to [Logging In to a dwscontroller Pod](#) to obtain the job information.
2. Log in to a GaussDB(DWS) node by referring to [Logging In to a Node in the Tenant Cluster](#), go to the `/home/Ruby/log/dws_upgrade.log` file, and view the cluster upgrade logs. You can see that the rollback command is executed during the upgrade.
3. Switch to user **Ruby**, go to the `$GAUSSLOG/om` directory, and check the om upgrade logs.

Emergency Handling Procedure

- Step 1** If the amount of metadata to be backed up is large, perform **VACUUM FULL** on the cluster before the upgrade.
- Step 2** If the restart takes a long time during the upgrade, restart the cluster before the upgrade.
- Step 3** If the upgrade failure is caused by the upgrade timeout configuration on the management side, modify the timeout period and upgrade DWS Controller again. After that, upgrade the cluster.

----End

Verification

On Service OM, reset the upgrade status, deliver the package, and upgrade the cluster again. The fault is rectified if the upgrade is successful and the upgrade status is **completed**.

Related Information

None

1.3.5.3 Agent Upgrade Fails

Symptom

During cluster upgrade, a package delivery exception and an upgradeInstance exception are reported.

Priority

High

Impact

Agent fails to be upgraded, and the packet delivery and cluster upgrade fail.

Possible Causes

Errors exist in the upgrade package.

Estimated Processing Duration

20 min

Handling Method

1. On the Service OM page, obtain the ID of the packet delivery job that fails.
2. Log in to a **dwscontroller** pod by referring to [Logging In to a dwscontroller Pod](#) and obtain the job information based on the job ID.
3. Log in to a node by referring to [Logging In to a Node in the Tenant Cluster](#) and check the **upgradeInstance** and **upgrade** logs in the **/home/Ruby/log** directory. Check whether the Agent has been upgraded in the **/rds/datastore/dws/** and **/rds/mgmtAgent** directories.

Emergency Handling Procedure

- Step 1** If Agent upgrade failure is caused by concurrent execution of different nodes, go to the **/home/Ruby/log/channel.log** file, obtain the command delivered by the **upgradeInstance**, and run this command directly in the CLI.

Step 2 If Agent fails to be upgraded due to an upgrade package error, rectify the fault and perform the upgrade again.

----End

Verification

On Service OM, reset the upgrade status, distribute the package and upgrade the cluster again.

Related Information

None

1.3.5.4 Failed to Upgrade Microservices on the Management Side Because Other Cloud Services Occupy Resources of the CloudAutoDeploy-CDK Nodes

Symptom

For Huawei Cloud Stack GaussDB(DWS) 8.1.2, microservices on the management side fail to be upgraded using Huawei Cloud Stack Update. Log in to the CloudAutoDeploy-CDK master node to check the pod information. The microservice pods cannot be started due to insufficient resources.

Priority

High

Impact

Microservices fail to be upgraded when GaussDB(DWS) is upgraded to 8.1.2.

Possible Causes

In earlier versions of Huawei Cloud Stack, ECF, DWS, and MRS are deployed on the same CloudAutoDeploy-CDK cluster and share the same node resources. In the 8.1.2 version, microservices are deployed on the CloudAutoDeploy-CDK nodes of the corresponding cloud service. Therefore, when upgrading a single cloud service, pods of other cloud services occupy the CloudAutoDeploy-CDK nodes, which will lead to failure in microservice upgrade.

Estimated Processing Duration

20 min

Handling Method

Log in to the CloudAutoDeploy-CDK master node and delete the pods of other cloud services on the CloudAutoDeploy-CDK nodes where a cloud service is located. The CloudAutoDeploy-CDK node tags have been modified, and resources will be released after the pods are deleted and restarted. Then upgrade a single cloud service again.

Emergency Handling Procedure

- Step 1** Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#), run the **su - root** command to switch to root user, and run the **kubectl** command to check the pod information deployed on the CloudAutoDeploy-CDK nodes.

```
kubectl get pod --all-namespaces -owide|grep -v '^kube'|grep -E "(node_ip1|node_ip2|node_ip3)"
```

In the preceding command, *node_ip1*, *node_ip2*, and *node_ip3* indicate the IP addresses of all CloudAutoDeploy-CDK nodes where a cloud service needs to be upgraded. There may be more than three nodes.

In the following example, *172.xx.xx.228*, *172.xx.xx.229*, *172.xx.xx.225*, *172.xx.xx.230*, and *172.xx.xx.231* indicate the IP addresses of all ECF CloudAutoDeploy-CDK nodes.

```
[root@172.***.205 ~]# TMOUT=0
[root@172.***.205 ~]# su - root
Last login: Wed Oct 20 16:21:34 CST 2021 on pts/1
[root@172-***.205 ~]# kubectl get pod --all-namespaces -owide|grep -v '^kube'|grep -E "(172.***.228|172.***.229|172.***.225|172.***.230|172.***.231)*"
dws
  dms-collection-58c5d7dcf8-zst9j  1/1  Running   0      25h  172.***.151  172.***.230  <none>    <none>
dws
  dwscontroller-7668f788d4-k58fk  1/1  Running   0      25h  172.***.168  172.***.228  <none>    <none>
ecf
  dbsinsight-5bb89b6994-7dm8c    1/1  Running   0      25h  172.***.102  172.***.228  <none>    <none>
ecf
  ecfbusmanager-75f7b84c6c-7vw28  1/1  Running   0      25h  172.***.103  172.***.229  <none>    <none>
ecf
  ecfcuslernanager-75f7b84c6c-tr65h 1/1  Running   0      25h  172.***.101  172.***.229  <none>    <none>
mrs
  mrsapigw-8688dc8cf6-6m868    1/1  Running   0      25h  172.***.150  172.***.230  <none>    <none>
mrs
  mrsapigw-8688dc8cf6-b2d5s    1/1  Running   0      25h  172.***.103  172.***.229  <none>    <none>
mrs
  mrsdeployer-8d549788d-fwmhm   1/1  Running   0      25h  172.***.135  172.***.231  <none>    <none>
```

The pods of the DWS and MRS microservices are deployed on the CloudAutoDeploy-CDK nodes of ECF and these pods occupy the resources of ECF, as shown in the command output. Migrate these resources to other nodes.

- Step 2** Run the following command to delete and restart a pod. During the restart, the pod of the microservice is migrated to the CloudAutoDeploy-CDK nodes of other cloud services because the node tags of ECF have changed. In this way, the ECF CloudAutoDeploy-CDK node resources are released.

NOTICE

Delete the second pod when you have deleted and restarted the first pod successfully to ensure that microservices keep being available during the process.

```
kubectl delete pod microservice_pod -n service_name
```

```
[root@172-***.205 ~]# kubectl delete pod dwscontroller-7668f788d4-k58fk dms-collection-58c5d7dcf8-zst9j -ndws
pod "dwscontroller-7668f788d4-k58fk" deleted
pod "dms-collection-58c5d7dcf8-zst9j" deleted
[root@172-***.205 ~]# kubectl delete pod mrsapigw-8688dc8cf6-6m868 mrsdeployer-8d549788d-fwmhm -nmrs
pod "mrsapigw-8688dc8cf6-6m868" deleted
pod "mrsdeployer-8d549788d-fwmhm" deleted
[root@172-***.205 ~]#
[root@172-***.205 ~]# kubectl get pod -nmrs -owide|grep ^mrsapigw
mrsapigw-8688dc8cf6-b2d5s  1/1  Running   0      25h  172.***.103  172.***.229  <none>    <none>
mrsapigw-8688dc8cf6-clpp   1/1  Running   0      2m13s  172.***.54   172.***.213  <none>    <none>
[root@172-***.205 ~]# kubectl delete pod mrsapigw-8688dc8cf6-b2d5s -nmrs
pod "mrsapigw-8688dc8cf6-b2d5s" deleted
[root@172-***.205 ~]#
```

- Step 3** Perform **Step 1** again to check the microservices on the ECF CloudAutoDeploy-CDK nodes and ensure that only the ECF microservices are deployed on the ECF nodes.

```
[root@172-***.205 ~]# kubectl get pod --all-namespaces -owide|grep -v '^kube'|grep -E "(172.***.228|172.***.229|172.***.225|172.***.230|172.***.231)*"
ecf
  dbsinsight-5bb89b6994-7dm8c    1/1  Running   0      25h  172.***.102  172.***.228  <none>    <none>
ecf
  ecfcuslernanager-75f7b84c6c-7vw28 1/1  Running   0      25h  172.***.101  172.***.229  <none>    <none>
ecf
  ecfcuslernanager-75f7b84c6c-tr65h 1/1  Running   0      25h  172.***.101  172.***.229  <none>    <none>
[root@172-***.205 ~]#
```

Step 4 Return to the Huawei Cloud Stack Update page and retry the failed operations during microservice upgrade.

----End

1.3.6 Instance

1.3.6.1 EIP Is Unreachable After a Cluster Is Created

Symptom

After a BMS cluster is created, EIP cannot be used to access the data warehouse cluster.

Priority

High

Impact

Users cannot use the EIP to log in to the data warehouse cluster.

Possible Causes

CIDR information of the VPC is required when BMSs are deployed across tenants and NICs. Therefore, you need to set the CIDR before creating a BMS cluster.

Estimated Processing Duration

30 min

Handling Method

1. Create a BMS cluster, bind an EIP, and check whether EIP can be used to access this cluster.
2. Check whether a CIDR is allocated to the VPC to which the BMS cluster belongs.
3. Run the **ip rule show** command to check the route information of the node. Check whether the route table whose ID is **100** exists and run the **route -n** command to check the route information of the local host.

Emergency Handling Guide

Step 1 If the EIP bound to the BMS cannot be accessed, contact BMS engineers to check the BMS configuration.

Step 2 If no CIDR is allocated to the VPC to which the BMS belongs, allocate a CIDR to the VPC and create the BMS cluster again.

Step 3 If the route table whose ID is **100** does not exist on the BMS node, run the **sh /etc/init.d/addRoute** command to execute the **/etc/init.d/addRoute** script to add the route table configuration.

----End

Verification

After the cluster is created, you can access the cluster through the EIP.

Related Information

None

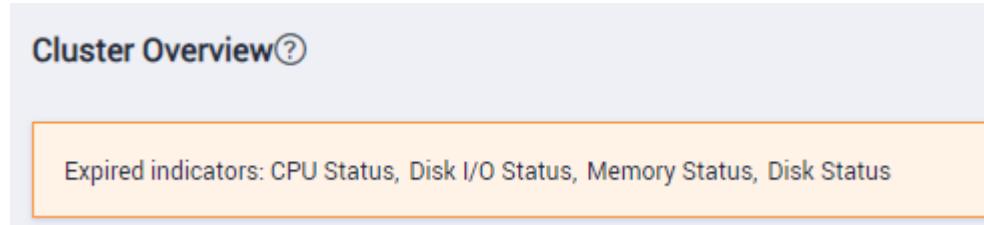
1.3.7 Monitoring

1.3.7.1 Monitoring Metrics Have Expired

Symptom

If an alarm indicating that some monitoring metrics have expired is displayed on the DMS monitoring page, the latest timestamp of these metrics is three collection periods later than the current system timestamp.

The following figure shows an example.



Possible Causes

- The collection of corresponding monitoring items is disabled.
- The DMS monitoring function is disabled.
- **dms-agent** stops reporting data.
- **dms-collection** has not imported monitoring data to the database.
- **dms-monitor** cannot obtain the latest timestamp.

Locating Method

Locate faults from easy ones to difficult ones:

1. Check whether the collection of DMS monitoring items is disabled.
2. Check whether the communication between the frontend and **dms-monitor** is normal.

3. Log in to the DMS metric database and check whether data is reported in the corresponding database.
4. Log in to the CCN on the tenant side and check whether **dms-agent** is running properly.

Procedure

- Step 1** Check whether the DMS collection function and monitoring item collection are enabled.
- If yes, go to **Step 2**.
 - If no, enable the collection. Then go to **Step 2**.

Name	Description	Collection Frequency (s)	Default Frequency
Circuit Breaking Queries	Real-time status collection of triggered circuit breaking query in a...	120	120
Cluster Host Status	Cluster host status indicator collection	60	60
Cluster Instance Status	Cluster instance status indicator collection	60	60
Slow Instance Detection	Locating and status collection of slow instances in a cluster	240	240
Cluster Status	Cluster status indicator collection	30	30
CN Availability	Indicator collection of CN abnormal status	60	60
CPU Status	CPU status indicator collection	30	30
Database Active Status	Database active status indicator collection	30	30
Database Capacity	Database capacity indicator collection	86400	86400
Database Status	Database status indicator collection	60	60

- Step 2** Press **F12** on the browser to invoke the browser debugging tool. Check whether the communication between the frontend and **dms-monitor** is normal.
- If yes, go to **Step 3**.
 - If no, contact technical support.

Name	Description	Collection Frequency (s)	Default Frequency
Circuit Breaking Queries	Real-time status collection of triggered circuit breaking query in a...	120	120
Cluster Host Status	Cluster host status indicator collection	60	60
Cluster Instance Status	Cluster instance status indicator collection	60	60
Slow Instance Detection	Locating and status collection of slow instances in a cluster	240	240
Cluster Status	Cluster status indicator collection	30	30
CN Availability	Indicator collection of CN abnormal status	60	60
CPU Status	CPU status indicator collection	30	30
Database Active Status	Database active status indicator collection	30	30
Database Capacity	Database capacity indicator collection	86400	86400
Database Status	Database status indicator collection	60	60

- Step 3** Log in to the DMS metric database by referring to [Logging In to the GaussDB Database of DMS](#) and check whether the latest data of the corresponding monitoring metrics is reported. Check whether the interval between the latest collection time and the current time is within three periods.

```
-- Get cluster ID by cluster name
select * from dms_meta_cluster where cluster_name = '<cluster_name>';
```

```
-- Get max ctime for all tables by cluster ID
select * from dms_meta_host where cluster_id = '<cluster_id>';
```

- If yes, go to **Step 4**.
- If no, contact technical support.

TC_MAX_CTIME						
ID : CLUSTER_ID	TABLE_NAME	HOST_ID : HOST_NAME	DNS_INSTANCE_ID	INST_ID	INST_NAME	MAX_CTIME :
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_CPU	59761 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_MEM	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_INST_STAT	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_CPU	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_INST_STAT	59764 host-25-213-2-7	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_INST_STAT	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_INSTANCE_SIZE_STATS	59764 host-25-213-2-7	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_HOST_STAT	59763 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_DISK_FS_SIZE	59763 host-25-213-2-7	c59b06c3-e138-427d-8d85-b7a0a3807290	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_HOST_STAT	59761 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_INSTANCE_SIZE_STATS	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_HOST_STAT	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_INSTANCE_SIZE_STATS	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_DB_SESSIONS	<null> <null>		5003	cn_5003	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_OPERATION_SYSTEM	59763 host-25-213-2-7	c59b06c3-e138-427d-8d85-b7a0a3807290	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_MEM	59763 host-25-213-2-7	c59b06c3-e138-427d-8d85-b7a0a3807290	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_CPU	<null> <null>		5003	cn_5003	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_INSTANCE_SIZE_STATS	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_STAT	59761 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_CPU	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_DB_SIZE	<null> <null>		5001	cn_5001	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_NET_IF	59764 host-25-213-2-7	c59b06c3-e138-427d-8d85-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_CLUSTER_HOST_STAT	59761 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_INSTANCE_SIZE_STATS	59763 host-25-213-2-7	c59b06c3-e138-427d-8d85-b7a0a3807290	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_MEM	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_NET_IF	59761 host-25-213-2-3	a39f025f-a828-42ab-a813-8f173d76c38a	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_OPERATION_SYSTEM	59763 host-25-213-2-7	c59b06c3-e138-427d-8d85-b7a0a3807290	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_DISKIO	59763 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_DISKIO	59762 host-25-213-2-2	c4ad029b-d2a3-4ced-88af-a1a71ccb0de3	<null>	<null>	1616587636000
68 4ca8c127-8bac-4237-9ccb-b733e791ab97	DNS_MTC_HARDWARE_DISKIO	59764 host-25-213-2-58	01e64507-b397-4c38-bd4e-cf1908decf3d	<null>	<null>	1616587636000

Step 4 Log in to a node on the tenant side and view the run logs of **dms-agent**. For details, see [Logging In to a Node in the Tenant Cluster](#). Analyze the run logs to check whether **dms-agent** is initialized and reports data properly.

su - Ruby

```
cd /var/chroot/DWS/manager/dmsagent/log
```

```
vi initial.log
```

```
vi agent_service.log
```

- If yes, check whether the data is properly displayed on the monitoring panel. If the fault persists, contact technical support.
- If no, data reporting errors are recorded in the run logs of **dms-agent**, and the value returned by the REST API is **500**. Go to **Step 6**.

Step 5 Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

Step 6 Run the following commands on the CloudAutoDeploy-CDK master node to log in to the **dms-collection** pod and check the logs.

```
kubectl get pods -n dws
```

```
kubectl exec -it <pod_name> -n dws bash
```

```
cd logs
```

```
vi dms-collection.log
```

----End

1.3.7.2 No Monitoring Information Is Displayed on the Monitoring Panel of the GaussDB(DWS) Cluster and an Interface Exception Is Reported

Symptom

No monitoring information is displayed on the monitoring panel of a GaussDB(DWS) cluster when you click **Monitoring Panel** of the target cluster, including the pages of **Cluster Overview**, **Monitoring > Node Monitoring**, and **Settings > Monitoring**.

Priority

High

Impact

The cluster monitoring information cannot be obtained.

Possible Causes

The DMS domain name cannot be resolved.

Estimated Processing Duration

30 min

Handling Method

Step 1 Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

Step 2 Run the following commands to log in to a monitoring pod and view the logs:

kubectl get pod -n dws

kubectl -ti exec dms-monitoring-xxxxxx -n dws bash

Step 3 Go to the **/opt/cloud/dms-monitoring/logs** directory and view the logs.

vi dms-monitoring.log

The following message is repeated many times in the logs: **ERROR com.huawei.dws.dms.monitoring.util.ResponseFactory - receive empty row data, failed to gen response**.

Step 4 Log in to a cluster node by referring to [Logging In to a Node in the Tenant Cluster](#) and view the DMS Agent logs. The logs are stored in the **/var/chroot/DWS/manager/dmsagent/log** directory outside the sandbox.

vi /var/chroot/DWS/manager/dmsagent/log

Error message **Name or service not known** is displayed when a domain name is used for access.

Step 5 The result **apiGatewayAddr** in **/home/Ruby/InitDms.json** corresponds to the domain name in **Step 4**. Therefore, this problem is caused by failed domain name resolution (CloudDNS is not deployed).

```
cat InitDms.json | grep apiGatewayAddr
```

```
[Ruby@host-2 ~]# cat InitDms.json | grep apiGatewayAddr
{"apiGatewayAddr": "dws.dms.cn-dwsglobal-1.externalregionacloud.com", "dmsVersion": "v1.0"}
```

----End

Emergency Handling Procedure

- Step 1** Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#) and run the following command to obtain the IP address corresponding to the domain name. Obtain the value of *Domain_name_configured_in_InitDms.json* from [Step 5](#).

```
ping Domain_name_configured_in_InitDms.json
```

For example, if you run **ping dws.dms.cn-dwsglobal-1.externalregionacloud.com**, **192.168.1.100** can be obtained.

```
exit
[root@EICCommon-Region-Master-01 ~]# ping dws.dms.cn-dwsglobal-1.externalregionacloud.com
PING dws.dms.cn-dwsglobal-1.externalregionacloud.com (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=1 ttl=64 time=0.338 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=2 ttl=64 time=0.157 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=3 ttl=64 time=0.120 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=4 ttl=64 time=0.178 ms
64 bytes from 192.168.1.100 (192.168.1.100): icmp_seq=5 ttl=64 time=0.240 ms
```

- Step 2** Go back to the cluster node by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to fix the OperationCenter monitoring issue:

```
apiGatewayAddr_ in_/home/Ruby/InitDms.json: 192.168.1.100
```

- Step 3** Restart DMS Agent.

```
ps aux|grep agent
```

```
kill -9 <agent_initial.py ProcessID>
```

- Step 4** Repeat [Step 2](#) to [Step 3](#) to log in to the remaining nodes in the cluster and perform corresponding operations.

- Step 5** Check whether the **/home/Ruby/dms_workdir/log/initial.log** logs contain information such as **Successfully send**. If yes, refresh the console page and wait for a period of time. The monitoring information will be displayed.

- Step 6** Perform the following steps to prevent this problem in clusters that are delivered later.

1. Log in to CloudScope using a browser as a system administrator.
 - URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
 - For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of deployment parameter table exported from HCC Turnkey (or HUAWEI CLOUD Stack Deploy in HUAWEI CLOUD Stack 8.1.1 and earlier versions) during Auto Change Platform installation.
 - Default account: **op_cdk_sso**
 - For details about the default password of the account, see the "CloudScopeLite" sheet in [Huawei Cloud Stack x.x.x Account List](#).

2. Choose **Services > CloudAutoDeploy-CDK**.
3. In the upper left corner of the page, select the corresponding region. In the navigation pane on the left, choose **Change Mgmt > Upgrade** and select the corresponding cluster. Then search for **dwscontroller** in the search box, select the corresponding **dwscontroller**, and click **Next**.
4. In the search box on the right, enter **dms.collection.apigateway.addr** and **cesGateway.endpoint** and change the parameter values to the IP address 192.168.1.100. Choose **Next > Upgrade** and wait until the upgrade is successful.

Parameter Name	Tag	Data Type	Template Parameter	Current Parameter	Description	Operation
dms.collection.apigateway.addr	global	string		dws.dms.cn-dwsglobal-1.externalregionacloud.com	The address of dms collection apigateway	Restore Defaults

Parameter Name	Tag	Data Type	Template Parameter	Current Parameter	Description	Operation
cesGateway.endpoint	global	string	100.125.0.218:443	imo-ces-cn-dwsglobal-1.externalregionacloud.com:443	..	Restore Defaults

5. Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).
6. List the **dwscontroller** pods.

kubectl get pods -n dws

```
Huawei's internal systems must only be used for conducting Huawei's business or for purposes authorized by Huawei management.
use is subject to audit at any time by Huawei management.
last login: Sun Jun 28 18:59:24 2028 from 24.65.15.235
[root@24-68-11-34 ~]# kubectl get pods -n dws
NAME           READY   STATUS    RESTARTS   AGE
dwscontroller-777f9567d-4qk8h  1/1     Running   0          7h51m
dwscontroller-777f9567d-zz9zc  1/1     Running   0          7h51m
[root@24-68-11-34 ~]#
```

7. Restart a **dwscontroller** pod.

kubectl delete pods {Pod_name} -n dws

{Pod_name} indicates the name of the first pod obtained in [Step 6.6](#), for example:

kubectl delete pods dwscontroller-777f9567d-4qk8h
dwscontroller-777f9567d-zz9zc -n dws

```
[root@24-68-11-34 ~]# kubectl delete pods dwscontroller-777f9567d-4qk8h dwscontroller-777f9567d-zz9zc -n dws
pod "dwscontroller-777f9567d-4qk8h" deleted
pod "dwscontroller-777f9567d-zz9zc" deleted
[root@24-68-11-34 ~]#
```

NOTE

When the preceding command is executed, the CloudAutoDeploy-CDK cluster automatically starts the new pod.

8. View the status of the new **dwscontroller** pod.

kubectl get pods -n dws

```
[root@24-68-11-34 ~]#
[root@24-68-11-34 ~]# kubectl get pods -n dws
NAME           READY   STATUS    RESTARTS   AGE
dwscontroller-777f9567d-5x9mc  1/1     Running   0          2m20s
dwscontroller-777f9567d-6rz6r  1/1     Running   0          2m20s
[root@24-68-11-34 ~]#
```

9. After the first pod is started in [Step 6.8](#), repeat [Step 6.7](#) to [Step 6.8](#) to restart another **dwscontroller** pod.

----End

Verification

The monitoring information is properly displayed on the monitoring panel.

Related Information

None

1.3.8 Others

1.3.8.1 Abnormal VM Resource Usage

Symptom

In scenarios where not many services are concurrently processed, alarms indicating abnormal system resource usage are displayed on the Service OM monitoring page. The alarms may include those indicating high memory or CPU usage, frequent disk read/write operations, and that the storage space is about to be used up.

Possible Causes

- The memory and CPU usage is high due to application bugs.
- An application is abnormal, generating a large number of logs and occupying much storage space.
- Programs on the server have vulnerabilities and are attacked by hackers. The server is used as a zombie, and most of its system resources are occupied.

Locating Method

Check abnormal processes and identify which processes occupy many resources. Inform the engineer responsible for it to fix the bugs.

If known processes are all normal, the fault is caused by hackers. Perform security hardening in a timely manner and fix program vulnerabilities.

Procedure

Step 1 Log in to the cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the **top** command to check system resource usage and identify which processes occupy many resources for a long time.

Pay attention to information in the **PID**, **%CPU**, **%MEM**, and **COMMAND** columns. The **COMMAND** column shows the process name. In the following figure, for example, the Java process uses 33.6% of the memory, and its PID is **29565**.

top - 14:34:25 up 23 days, 22:57, 2 users, load average: 0.00, 0.01, 0.05											
Tasks: 443 total, 2 running, 441 sleeping, 0 stopped, 0 zombie											
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st											
KiB Mem : 16230620 total, 8105476 free, 6046612 used, 2078532 buff/cache											
KiB Swap: 0 total, 0 free, 0 used. 9066792 avail Mem											
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
29565	rds	20	0	15.188g	5.202g	10520	S	1.0	33.6	13:15.49	java
126640	root	20	0	130332	2156	1260	R	0.3	0.0	0:00.04	top
1	root	20	0	58732	6784	3932	S	0.0	0.0	8:02.12	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.65	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.69	ksoftirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:0H
7	root	rt	0	0	0	0	S	0.0	0.0	0:03.92	migration/0
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/0
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/1
11	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/2
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/3
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/4
14	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/5
15	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/6
16	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/7
17	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/8
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/9
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/10
20	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcuob/11

Step 2 Run the **ps -ef |grep PID** command to view process information. The **PID** value is the abnormal PID obtained in **Step 1**.

Assume that you want to view the Tomcat process.

```
[root@service2 ~]# ps -ef |grep 29565
rds      29565     1  Oct27 ?        00:13:21 /var/rds/jdk1.8.0_102/jre/bin/java -Djava.util.logging.config.fil
gManager -Djdk.tls.ephemeralDHKeySize=2048 -Xms512m -Xmx12800m -Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true
r.ALLOW_BACKSLASH=false -Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=false -Dorg.apache.coyote.USE_CUS
mcat/bin/bootstrap.jar:/var/rds/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/var/rds/tomcat -Dcatalina.home=/var/rds
root    129335 126606  0 14:47 pts/1    00:00:00 grep --color=auto 29565
[root@service2 ~]#
```

Step 3 Go to the directory where the program is located, and check whether its configuration file is normal.

Assume that the content of the Tomcat process configuration file is as follows. Check whether the memory occupied by Tomcat startup is normal.

```
[root@insight1 tomcat]# pwd
/var/rds/tomcat
[root@insight1 tomcat]#grep "-Xmx" bin/catalina.sh
grep: invalid matcher mx
[root@insight1 tomcat]# grep "-Xmx" bin/catalina.sh
JAVA_OPTS="$JAVA_OPTS -Xms512m -Xmx2800m -
Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true -
Dorg.apache.catalina.connector.RECYCLE_FACADES=false -
Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=false -
Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=false -
Dorg.apache.coyote.USE_CUSTOM_STATUS_MSG_IN_HEADER=false"
```

If the configurations are proper, check whether Tomcat logs recording exceptions exist. If they exist, provide them for the R&D engineers responsible for it to locate problems and fix faults.

Step 4 If the storage space is used up, run the **df -h** command to check the space of which disk is used up.

In most cases, data disk space is used up.

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/xvda1	38G	3.4G	34G	10%	/
devtmpfs	7.8G	0	7.8G	0%	/dev
tmpfs	7.8G	0	7.8G	0%	/dev/shm
tmpfs	7.8G	777M	7.0G	10%	/run
tmpfs	7.8G	0	7.8G	0%	/sys/fs/cgroup
/dev/xvde1	296G	1.4G	279G	1%	/var/rds

- Step 5** Go to the directory to which data disks are mounted (directory corresponding to `/dev/xvde1`). Run the `du -sh /var/rds/*` command to find the directory occupying the most space.

Assume that the log directory occupies the most space (which is often the case). Check whether logs recording exceptions exist. If they exist, provide them for the R&D engineers responsible for it to locate the problem.

```
[root@service2 ~]# cd /var/rds
[root@service2 rds]# ll
total 44
drwx-----3 rdsrds4096 Oct 27 16:29 backup
drwx-----3 rootroot4096 Jul 12 15:57 elk-agent
drwx-----8 rdsrds4096 Jun 23 09:56 jdk1.8.0_102
drwx-----8 rdsrds4096 Dec 232015 jdk1.8.0_71
drwx-----3 rdsrds16384 Sep 1 14:40 lost+found
drwx-----9 rdsrds4096 Oct 27 16:41 RDS_Service
drwx-----9 rdsrds4096 Oct 27 16:38 tomcat
drwx----- 10 zabbix zabbix4096 Oct 25 20:08 zabbix
[root@service2 rds]# du -sh /var/rds/*
2.5M/var/rds/backup
182M/var/rds/elk-agent
355M/var/rds/jdk1.8.0_102
354M/var/rds/jdk1.8.0_71
24K /var/rds/lost+found
105M/var/rds/RDS_Service
197M/var/rds/tomcat
15M /var/rds/zabbix
```

----End

1.4 Faults on the Tenant Side

1.4.1 Storage

1.4.1.1 Skewed Data Is Detected During Routine Inspection and the Disk Usage of Some Nodes Is High

Symptom

Log in to a node in the cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to check the disk usage of the cluster. The disk usage of some nodes is higher than that of other nodes, and the disk usage exceeds 80%.

```
gs_ssh -c "df -h" | grep -iE 'data|manager'
```

```
[Ruby@host-172-20-18-58 ~]# gs_ssh -c "df -h" | grep -iE 'data|manager'  
/dev/vdb      100G  962M  100G  1% /DWS/manager  
/dev/vdb      100G  981M  99G   1% /DWS/manager  
/dev/vdb      100G  845M  100G  1% /DWS/manager
```

Priority

High

Impact

If the disk usage of a node exceeds 90%, the cluster becomes read-only.

Possible Causes

The disk usage of some nodes is higher than that of other nodes due to data skew.

Estimated Processing Duration

30 min

Handling Method

Find the table where data skew occurs based on the emergency guide and submit the table to the customer service side for rectification.

Emergency Handling Procedure

Scenario 1: Data skew caused by a full disk

- Step 1** First, use the **pg_stat_get_last_data_changed_time(oid)** function to query for the tables whose data is changed recently. The last change time of a table is recorded only on the CN where **INSERT**, **UPDATE**, and **DELETE** operations are performed. Therefore, you need to query for tables that are changed within the last day (the period can be changed in the function).

```
CREATE OR REPLACE FUNCTION get_last_changed_table(OUT schemaname text, OUT relname text)  
RETURNS setof record  
AS $$  
DECLARE  
row_data record;  
row_name record;  
query_str text;  
query_str_nodes text;  
BEGIN  
query_str_nodes := 'SELECT node_name FROM pgxc_node where node_type = "C"';  
FOR row_name IN EXECUTE(query_str_nodes) LOOP  
query_str := 'EXECUTE DIRECT ON (' || row_name.node_name || ') "SELECT b.nspname,a.relname FROM  
pg_class a INNER JOIN pg_namespace b on a.relnamespace = b.oid where  
pg_stat_get_last_data_changed_time(a.oid) BETWEEN current_timestamp - 1 AND current_timestamp"';  
FOR row_data IN EXECUTE(query_str) LOOP  
schemaname = row_data.nspname;  
relname = row_data.relname;  
return next;  
END LOOP;  
END LOOP;  
return;  
END; $$  
LANGUAGE plpgsql;
```

Step 2 Then, use the **table_distribution(schemaname text, tablename text)** function to query the storage space occupied by the table on each DN.

```
SELECT table_distribution(schemaname,relname) FROM get_last_changed_table();
```

Step 3 Confirm with the customer and delete tables with severe data skew.

----End

Scenario 2: Routine data skew inspection

- If the number of tables in the database is less than 10,000, use the skew view to query tables with data skew in the current database.

```
SELECT * FROM pgxc_get_table_skewness WHERE totalsize > 100*1024*1024 AND skewratio > 0.5  
ORDER BY totalsize DESC;
```

- If the number of tables in the database is more than 10,000, do not use the PGXC_GET_TABLE_SKEWNESS view because it takes a long time (hours) to query the entire database for skew columns. You are advised to use the **table_distribution()** function, and define the output based on PGXC_GET_TABLE_SKEWNESS, optimizing the calculation and reducing the output columns. Example:

```
SELECT schemaname,tablename,max(dnsizE) AS maxsize, min(dnsizE) AS minsize  
FROM pg_catalog.pg_class c  
INNER JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace  
INNER JOIN pg_catalog.table_distribution() s ON s.schemaname = n.nspname AND s.tablename =  
c.relname  
INNER JOIN pg_catalog.pgxc_class x ON c.oid = x.pcrelid AND x.pclocationtype = 'H'  
GROUP BY schemaname,tablename;
```

Verification

The difference among disk usages of different nodes does not exceed 5%.

Related Information

None

1.4.1.2 CN Cannot be Connected Because It Is in the down State

Symptom

A CN cannot be connected and its state displayed in the cluster backend is **down**.

Log in to a node by referring to [Logging In to a Node in the Tenant Cluster](#) and check the disk usage. The disk usage of the CN directory reaches 100% and a large number of temporary files exist in **/DWS/manager/coordinator/base/pgsql_tmp**.

```
gs_ssh -c "df -h" | grep -iE 'data|manager'
```

```
[Ruby@host-172-20-18-58 ~]# gs_ssh -c "df -h" | grep -iE 'data|manager'  
/dev/vdb      100G  962M 100G  1% /DWS/manager  
/dev/vdb      100G  981M  99G  1% /DWS/manager  
/dev/vdb      100G  845M 100G  1% /DWS/manager
```

Priority

High

Impact

The disk is full. As a result, the CN is in the **down** state and cannot be automatically started, affecting service running.

Possible Causes

There is no limit on the size of files that can be written to disks on CNs.

Estimated Processing Duration

1 min

Handling Method

Set limit on the size of files that can be written to disks on CNs and optimize SQL statements for writing files to disks.

Emergency Handling Procedure

Step 1 Log in to a node by referring to [Logging In to a Node in the Tenant Cluster](#).

Step 2 Run the following command to limit the size of files written to disks on the CN:

```
gs_guc reload -Z coordinator -Z datanode -N all -I all -c  
"temp_file_limit=10485760"
```

Step 3 Remove some log files to clear the disk space. The CN is automatically started.

Step 4 In the CN log (`/DWS/manager/log/Ruby/pg_log/cn_xxxx`), search for the keyword **LOG: SQL can't be shipped, reason**. The SQL statement pushdown performance is poor. Check whether the SQL statement can be optimized based on the reason why the SQL statement cannot be pushed down.

----End

Verification

The disk usage of the CN directory decreases. The CN is automatically started and restored to the normal state.

Related Information

None

1.4.1.3 Disk Usage Is High and Data Needs to Be Cleared

Symptom

Log in to a node in the cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to check the disk usage of the cluster. The overall disk usage of each node exceeds 80%.

```
gs_ssh -c "df -h" | grep -iE 'data|manager'
```

```
[Ruby@host-172-20-18-58 ~]# gs_ssh -c "df -h" | grep -iE 'data|manager'  
/dev/vdb      100G  962M  100G  1% /DWS/manager  
/dev/vdb      100G  981M  99G   1% /DWS/manager  
/dev/vdb      100G  845M  100G  1% /DWS/manager
```

Priority

High

Impact

If the disk usage of a node exceeds 90%, the cluster becomes read-only.

Possible Causes

1. Data is not cleared in a timely manner.
2. The cluster capacity needs to be expanded.

Estimated Processing Duration

10 min

Handling Method

Periodically check the disk usage and clear data in a timely manner.

Emergency Handling Procedure

Step 1 Ask the customer to determine the tables to be deleted or cleared. And execute the DROP TABLE or TRUNCATE TABLE statement.

Step 2 Check whether the cluster needs to be scaled out.

----End

Verification

The disk usage of each node is lower than 80%.

Related Information

None

1.4.1.4 CN Disk Is Full Because Audit Logs or Logs Are Not Compressed

Symptom

A CN cannot be connected and its state displayed in the cluster backend is **down**.

The disk usage of the **/DWS/manager** directory reaches 100%. The **/DWS/manager/log/Ruby/pg_audit** directory is too large.

Priority

High

Impact

The CN cannot be automatically started.

Possible Causes

The space priority policy is not used for audit logs.

Estimated Processing Duration

5 min

Handling Method

Apply the space priority policy to audit logs.

Emergency Handling Procedure

Step 1 Log in to a cluster node on the tenant side by referring to [Logging In to a Node in the Tenant Cluster](#). The CN directory is full and the `/DWS/manager/log/Ruby/pg_audit` directory occupies too much space.

Step 2 Run the following command in the sandbox:

```
gs_guc reload -Z coordinator -Z datanode -N all -I all -c "audit_resource_policy =on"
```

----End

Verification

The space of the `/DWS/manager` directory is released, and the CN automatically starts.

Related Information

For details, see "Configuring the Database Audit Logs" in [Data Warehouse Service \(DWS\) x.x.x User Guide \(for Huawei Cloud Stack x.x.x\)](#).

1.4.2 Cluster

1.4.2.1 Low Cluster Performance Displayed on the WebUI

Symptom

On the GaussDB(DWS) management console, the **Cluster Status** is **Low performance**.

Priority

High

Impact

The load on some nodes increases.

Possible Causes

Cluster switchover occurs.

Estimated Processing Duration

10 min

Handling Method

Perform the active/standby switchover.

Emergency Handling Procedure

Step 1 Connect to the cluster using gsql.

```
gsql -d <database name> -h <cluster address> -U <database user> -p <database port> -W <cluster password> -r
```

Step 2 Query the catch-up state in the cluster.

```
select * from pgxc_get_senders_catchup_time();
```

Step 3 Log in to a cluster node by referring to [Logging In to a Node in the Tenant Cluster](#) and perform an active/standby switchover.

```
gs_om -t switch --reset
```

----End

Verification

The cluster status becomes normal.

Related Information

None

1.4.2.2 Account Locked

Symptom

An account is locked and an error stating "The account has been locked" is reported when the account attempts to access a cluster.

Priority

High

Impact

The account cannot be used to access the database.

Possible Causes

When a user uses an account to access the database in a cluster, if the number of consecutive incorrect password attempts reaches the upper limit (10 by default), the account will be locked.

Estimated Processing Duration

5 min

Handling Method

For a common user, run the **alter user username account unlock** command as the administrator.

Emergency Handling Guide

Method for Unlocking the Administrator (**dbadmin** by Default)

- Step 1** Log in to the GaussDB(DWS) management console and go to the **Clusters > Dedicated Clusters** page.
- Step 2** Locate the target cluster and choose **More > Reset Password** in the **Operation** column.

----End

Method for Unlocking a Common User

Connect to the database as the administrator (**dbadmin** by default) and run the following command to unlock a database user (replace **user_name** with the name of the locked user):

```
gsql -d <Database name> -h <Cluster address> -U dbadmin -p <Database port> -W <Cluster password> -r  
ALTER USER user_name ACCOUNT UNLOCK;
```

Setting the Number of Login Failures

You can set the maximum number of incorrect password attempts by configuring the **failed_login_attempts** parameter on the **Parameter Modifications** tab of the cluster. When **failed_login_attempts** is set to **0**, the number of incorrect password attempts is unlimited. You are not advised to set **failed_login_attempts** to **0**.

Perform the following steps:

- Step 1** Log in to the GaussDB(DWS) management console.
- Step 2** In the navigation tree on the left, choose **Clusters > Dedicated Clusters**.
- Step 3** In the cluster list, find the target cluster and click the cluster name. The **Basic Information** page is displayed.

Step 4 Enter the **Parameter Modifications** tab page, locate the **failed_login_attempts** parameter, change its value, and click **Save**. After confirming the modification click **Save**.

----End

Verification

The account can be used to access the database.

Related Information

None

1.4.2.3 Viewing Audit Logs

Symptom

The customer wants to view audit logs.

Priority

High

Impact

None

Possible Causes

None

Estimated Processing Duration

10 min

Handling Method

None

Emergency Handling Guide

Step 1 Use an SQL client to connect to the database.

Step 2 Query audit logs:

```
SELECT * FROM pg_query_audit('2015-07-15 08:00:00','2015-07-15 09:47:33');
```

The query result is as follows:

time	type	result	username	database	client_conninfo	object_name
detail_info			node_name	thread_id	local_port	remote_port
2015-07-15 08:03:55+08	login_success	ok		postgres	gs_clean@::1	postgres
						login

```
db(postgres) success,the current user is: | cn_5003 | 139808902997776@490233835920483 | 9000 |  
55805
```

This record indicates that user **dbadmin** logged in to database **postgres** at 2015-07-15 08:03:55+08. After the host specified by **log_hostname** is started and a client is connected to its IP address, the host name found by reverse DNS resolution is displayed following the at sign (@) in the value of **client_conninfo**.

Step 3 To query the audit records of all CNs, run the following command:

```
SELECT * FROM pgxc_query_audit('2019-01-10 17:00:00','2019-01-10 19:00:00') where type =  
'login_success' and username = 'user1';
```

The query result is as follows:

time	type	result	username	database	client_conninfo	object_name
detail_info			node_name		thread_id	
local_port	remote_port					
2019-01-10 18:06:08+08	login_success	ok	user1	postgres	gsql@[local]	postgres
db(postgres)	success,the current user is:user1			coordinator1	139965149210368@600429968516954	
17560	null					
2019-01-10 18:06:22+08	login_success	ok	user1	postgres	gsql@[local]	postgres
db(postgres)	success,the current user is:user1			coordinator1	139965149210368@600429982697548	
17560	null					
2019-01-10 18:06:54+08	login_success	ok	user1	postgres	gsql@[local]	postgres
db(postgres)	success,the current user is:user1			coordinator2	140677694355200@600430014804280	
17562	null					
(3 rows)						

The query result shows the successful login records of **user1** on CN1 and CN2.

----End

Verification

None

Related Information

None

1.4.2.4 An Error Is Reported During Statement Execution, Indicating that the User Does Not Have the Permissions on the Table

Symptom

The following error is reported during statement execution:

```
ERROR: permission denied for xxx
```

Priority

High

Impact

The table or schema cannot be accessed.

Possible Causes

The user does not have the required permissions.

Estimated Processing Duration

5 min

Handling Method

Execute the **GRANT** statement to grant permissions.

Emergency Handling Procedure

Step 1 Grant permissions to tables or schemas using **GRANT**. If you want user **jerry** to have the query permission on all tables created by **tom** and the tables to be created, perform the following operations:

- Grant the schema permissions of user **tom** to user **jerry**.
`GRANT USAGE ON SCHEMA tom TO jerry;`
- Grant the **SELECT** permission on the tables created by user **tom** to user **jerry**.
`GRANT SELECT ON ALL TABLES IN SCHEMA tom TO jerry;`
- 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 TABLE TO jerry;`

----End

Verification

The operation is successful and no error is reported.

Related Information

See "GRANT" in [Data Warehouse Service \(DWS\) x.x.x Developer Guide \(for Huawei Cloud Stack x.x.x\)](#).

1.4.2.5 Querying Whether a User Has Permissions on a Table

Symptom

The customer wants to check whether a user has permissions on a table.

Priority

None

Impact

None

Possible Causes

None

Estimated Processing Duration

5 min

Handling Method

Query the **pg_class** system catalog.

Emergency Handling Guide

Step 1 Query the `pg_class` system catalog.

```
SELECT * FROM pg_class WHERE relname = 'tablename';
```

Check the **relacl** column. The command output is shown in the following figure. For details about the permission parameters, see [Table 1-4](#).

- *rolename=xxxx/yyyy*: indicates that *rolename* has the *xxxx* permission on the table and the permission is obtained from *yyyy*.
 - *=xxxx/yyyy*: indicates that **public** has the *xxxx* permission on the table and the permission is obtained from *yyyy*.

Take the following figure as an example:

joe=arwdDxtA: indicates that user **joe** has all permissions (**ALL PRIVILEGES**).

leo=arw/joe: indicates that user **leo** has the read, write, and modify permissions, which are granted by user **joe**.

Table 1-4 Permissions parameters

Parameter	Description
r	SELECT (read)
w	UPDATE (write)
a	INSERT (insert)
d	DELETE
D	TRUNCATE
x	REFERENCES
t	TRIGGER
X	EXECUTE

Parameter	Description
U	USAGE
C	CREATE
c	CONNECT
T	TEMPORARY
A	ANALYZE ANALYSE
arwdDxtA	ALL PRIVILEGES (for tables)
*	Actions for preceding permissions

Step 2 You can also use the **has_table_privilege** function to query user permissions on tables.

```
SELECT * FROM has_table_privilege('Username','Table_name','select');
```

For example, query whether user **joe** has the query permission on table **t1**.

```
SELECT * FROM has_table_privilege('joe','t1','select');
```

```
gaussdb=> select * from has_table_privilege('joe','t1','select');
 has_table_privilege
-----
 t
(1 row)
```

----End

Verification

None

Related Information

None

1.4.2.6 Node Is Faulty Because the Instance Directory Is Deleted

Symptom

The instance directory is deleted by mistake, and the instance status is abnormal. In this case, you need to manually restore the instance.

Priority

High

Impact

The cluster is in the degraded status and needs to be restored as soon as possible.

Possible Causes

The user deletes the data file by mistake.

Estimated Processing Duration

20 hours (depending on the data volume)

Handling Method

Run the **gs_replace** command to restore the instance.

Emergency Handling Procedure

Step 1 Log in to a node by referring to [Logging In to a Node in the Tenant Cluster](#) and perform the following operations in the sandbox.

Step 2 Disable the password-free mode.

```
gs_guc set -Z coordinator -Z datanode -N all -I all -h "local all all trust"
```

Step 3 Configure the instance node.

gs_replace -t config -h *hostname1* # *hostname1* indicates the node name to be restored.

The function is successfully configured if the following information is displayed:

```
Successfully upgraded standby instances.  
Configuring replacement instances.  
Successfully configured replacement instances.  
Deleting abnormal CN from pgxc_node on the normal CN.  
Successfully deleted abnormal CN from pgxc_node on the normal CN.  
Unlocking cluster.  
Successfully unlocked cluster.  
Locking cluster.  
Successfully locked cluster.  
Incremental building CN from the Normal CN.  
Successfully incremental built CN from the Normal CN.  
Creating fixed CN on the normal CN.  
Successfully created fixed CN on the normal CN.  
Starting the fixed cn.  
Successfully started the fixed cn.  
Creating fixed CN on the fixed CN.  
Successfully created fixed CN on the fixed CN.  
Unlocking cluster.  
Successfully unlocked cluster.  
Creating unfixed CN on the fixed and normal CN.  
No CN needs to be created.  
Configuration succeeded.
```

NOTE

If **gs_replace** fails, view the CN or DN logs and contact technical support. Log file path: `/var/chroot/DWS/manager/log/Ruby/pg_log`

Step 4 Start the instance node.

```
nohup gs_replace -t start -h hostname1 > /home/Ruby/gsreplace.log 2>&1 & #  
Prevent client sessions from being disconnected using nohup.
```

Run the **cat /home/Ruby/gsreplace.log** command to view logs. If information similar to the following is displayed, the startup is successful.

```
Starting.  
=====  
Successfully started instance process. Waiting to become Normal.  
=====  
=====  
Start succeeded.
```

NOTE

If **gs_replace** fails, view the CN or DN logs and contact technical support. Log file path: `/var/chroot/DWS/manager/log/Ruby/pg_log`

Step 5 After the node is restored, check the cluster status.

cm_ctl query -Cvd

- If the value of **balanced** is **Yes**, go to [Step 7](#).
- If the value of **balanced** is **No**, go to [Step 6](#) to perform a active/standby switchover for the cluster.

Step 6 Coordinate the service time window and run the following command to perform an active/standby switchover.

NOTE

The active/standby switchover can be performed only when there is no catch-up in the cluster.

cm_ctl switchover -a

The switchover is successful if information similar to the following is displayed:
switchover successfully.

Step 7 Enable the password-free mode.

```
gs_guc set -Z coordinator -Z datanode -N all -I all -h "local all all sha256"  
----End
```

Verification

The **gs_replace** command is executed successfully.

Related Information

None

1.4.2.7 Scale-out Fails on the Tenant Side After the Console on the Management Side Is Upgraded to 8.1.1

Symptom

After the console on the management side is upgraded from 8.1.0.x to 8.1.1, the newly created 8.1.0.101 or 8.1.1 cluster fails to be scaled out.

Priority

Medium

Impact

Existing clusters are not affected. Clusters created after the console upgrade cannot be scaled out.

Possible Causes

Browser cache

Estimated Processing Duration

5 min

Handling Method

Clear the browser cache.

Emergency Handling Procedure

Clear the browser cache.

Verification

The cluster can be scaled out.

Related Information

None

1.4.2.8 O&M Commands Occasionally Fail to Be Delivered When the Node Machine Is Restarted

Symptom

When the cluster machine is powered cycle, the O&M command fails to be delivered.

Priority

Medium

Impact

Cluster O&M operations are affected.

Possible Causes

The RPC communication is abnormal.

Estimated Processing Duration

15 min

Handling Method

- Step 1** Log in to the instance node and run the `cd /home/Ruby/log` command to view O&M logs and it is found that no new log is generated.
- Step 2** View the RPC channel logs, for example, `channel.log`. No log is generated since the time when the O&M command is delivered.
- Step 3** View the RPC process. Run `su - Ruby` and then `ps -ef | grep rpc` to check whether the RPC process exists.
- Step 4** If the RPC process does not exist, run the `/bin/python /rds/mgntAgent/workplace/rpc/monitorCtrl.py start` command to manually start the process and check whether an error message is displayed.
- Step 5** If the process fails to be started, check the error information. For example, if the error information indicates that the JAR package does not exist, check whether the `rpc-server-0.0.1-SNAPSHOT-jar-with-dependencies.jar` package exists in the `/rds/mgntAgent/workplace/rpc/` directory (8.1.0.3 or earlier) or the `/rds/rpc` directory (new version).
- Step 6** If the JAR package does not exist, the file is lost by mistake when an exception occurs in the system. To quickly recreate the instance and the channel on the management side and prevent O&M operations from being blocked, copy the file from another directory to the RPC directory as user **Ruby**.
 - In 8.1.0.3 or earlier, copy all files from the `/rds/mgntAgent/vx.x.x/rpc` directory to the startup directory `/rds/mgntAgent/workplace/rpc/`. `vx.x.x` indicates the workspace directory of the source version.
 - In the new version, copy all files from `/rds/mgntAgent/vx.x.x/rpc` to the startup directory `/rds/rpc`. `vx.x.x` indicates the workspace directory of the current version.
- Step 7** Perform **Step 4** again to start the RPC service. If the `channel.log` file contains the startup log `Server started, listening on 12017`, the RPC service has been started. Perform O&M again.

----End

Related Information

None

1.4.2.9 An Error Message Is Displayed When a Command Fails to Be Delivered During DMS Configuration

Symptom

When the DMS monitoring panel is configured (modifying/disabling monitoring collection), an error message is displayed indicating that the command fails to be delivered.

Priority

Medium

Impact

Users cannot configure the monitoring panel.

Possible Causes

The gRPC service is abnormal.

Estimated Processing Duration

20 min

Handling Method

Log in to Service OM and restart DMS Agent.

Emergency Handling Procedure

Step 1 Log in to Service OM, choose **Data Warehouse Service > Cluster Monitoring**, and find the cluster corresponding to the instance node.

Step 2 Restart DMS Agent. If the data can be updated normally, the fault is rectified.

Cluster Monitoring						
Region: cn-north-7						
Cluster Name	Cluster Status	Tenant Name	Created	Number of Nodes	Disk Usage (%)	Operation
Normal	09703a433200d3ee0fe6c007...	2021-06-18 19:07:05	3	6.08	Restart dms-agent	Details
Normal	0539cdee1800d9f10f9c008...	2021-06-19 01:28:41	3	0.05	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-19 16:18:24	8	8	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-07 10:32:03	3	5.56	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-07 11:11:05	3	4.76	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-22 19:01:05	3	4.12	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-22 21:25:13	3	4.08	Restart dms-agent	Details
Abnormal	06796105ea4c2c80c50bea7...	2021-06-22 16:48:05	8	3.89	Restart dms-agent	Details
Normal	09703a433200d3ee0fe6c007...	2021-06-18 16:21:22	4	3.86	Restart dms-agent	Details
Normal	06766105da0a4c2c80c50bea7...	2021-06-23 09:08:09	3	3.74	Restart dms-agent	Details

----End

Verification

The DMS monitoring panel can be configured.

Related Information

None

1.4.3 Communication

1.4.3.1 Failed to Connect to the Database of the Cluster

Symptom

Users fail to connect to the database by running gsql on the client.

Priority

High

Impact

The database cannot be connected.

Possible Causes

- The network connection fails.
- The password is incorrect.
- The connected database does not exist.
- The number of connections has reached the upper limit.

Estimated Processing Duration

30 min

Handling Method

Check whether the network connection is normal. Ensure that the entered password is correct, that the connected database exists, and that the number of CN connections does not reach the upper limit.

Emergency Handling Guide

Step 1 Rectify the network fault. Check the network connection between the client and the database server.

The network is faulty if the client fails to ping the database server. Contact the network administrator to rectify the fault.

Step 2 Ensure that the password is correct. If the password is incorrect, the following error information is displayed:

```
gaussdba@linux13:~/gaussdb> gsql -d human_resource -U gaussdba -W password -p 8000  
gsql: FATAL: Invalid username/password,login denied.
```

Step 3 Connect to the default database **postgres**. If **postgres** does not exist, the following error information is displayed:

```
gaussdba@linux13:~/gaussdb> gsql -d human_resource -p 8000  
gsql: FATAL: database "human_resource" does not exist
```

Step 4 If the number of CN connections exceeds the upper limit, the following error information is displayed:

```
gaussdba@plat1:~> gsql -d human_resource user1 -p 8000  
gsql: FATAL: sorry, too many clients already
```

Step 5 Increase **max_connections** based on scenarios and restart the database.

```
gaussdba@plat1:~/gaussdb> gs_guc set -Z coordinator -D /gaussdb/data/data_cn -c
"max_connections = 1200"
```

Table 1-5 Viewing the numbers of connections

Description	Command
View the maximum session number of a user.	Run the following command to view the upper limit of user user1 's connections. -1 indicates that no connection upper limit is set for user user1 . <pre>SELECT ROLNAME,ROLCONNLIMIT FROM PG_ROLES WHERE ROLNAME='Ruby'; rolname rolconnlimit -----+----- Ruby -1 (1 row)</pre>
View the number of connections that have been used by a specified user.	Run the following command to view the number of connections that have been used by user1 . 1 indicates the number of connections that have been used by user1 . <pre>SELECT COUNT(*) FROM V\$SESSION WHERE USERNAME='Ruby'; count ----- 1 (1 row)</pre>
View the upper limit of connections to database.	Run the following command to view the upper limit of connections used by postgres . -1 indicates that no upper limit is set for the number of connections that have been used by postgres . <pre>SELECT DATNAME,DATCONNLIMIT FROM PG_DATABASE WHERE DATNAME='postgres'; datname datconnlimit -----+----- postgres -1 (1 row)</pre>
View the number of connections that have been used by a database.	Run the following command to view the number of connections that have been used by postgres . 1 indicates the number of connections that have been used by postgres . <pre>SELECT COUNT(*) FROM PG_STAT_ACTIVITY WHERE DATNAME='postgres'; count ----- 1 (1 row)</pre>

Description	Command
View the total number of connections that have been used by all users.	Run the following command to view the number of connections that have been used by all users: SELECT COUNT(*) FROM V\$SESSION; count ----- 10 (1 row)

----End

Verification

The database can be connected.

Related Information

None

2 Alarm Handling

2.1 Alarms on the Management Side

2.1.1 DWS_00001 Script Execution Exception

Alarm Description

This alarm is generated when DWS Controller fails to manage clusters using an SSH or SFTP channel.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00001	Management plane alarm	Minor	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Script execution exception
	Type	QoS alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Cluster management operations will fail, resulting in service failures.

Possible Causes

- The network is disconnected.
- The network configuration is incorrect.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 View the exception alarm information and record the alarm generation time. Obtain the node ID according to **Possible Causes** in the alarm information.

The following is an example of **Possible Causes**:

```
[RdsRestartTask][execute]restart CloudAcurs error! instanceld:[82be434e-0f4a-4550-9fcf-6ba2d318e5a9]  
rdsChannel call [restart] exception:[82be434e-0f4a-4550-9fcf-6ba2d318e5a9]java.net.ConnectException:  
Connection timed out (Connection timed out)
```

82be434e-0f4a-4550-9fcf-6ba2d318e5a9 indicates the node ID.

Step 3 Run the following commands to connect to the O&M container, log in to the database node, and connect to the **rms** database:

kubectl exec -ti Container_name -n ecf bash

Floating IP address of the **mysql -h** database VM **-P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

use rms;

Step 4 Run the following command to query the node name according to the node ID obtained in **Step 2**.

```
SELECT name,id from rds_instance WHERE id='Node ID';
```

Step 5 In the GaussDB(DWS) O&M container, log in to the node queried in **Step 4**. For details, see [Logging In to a Node in the Tenant Cluster](#).

- If a login exception occurs, the node SSH is abnormal. Contact O&M engineers.
- If the login is successful, the network is in the normal state. Retry the failed service.
- If the fault persists after the retry, run the following commands to log in to the DWS Controller container and switch to the log path:

kubectl get pod -n dws. In the command output, **NAME** indicates the container name.

```
[root@10-63-90-40 ~]# kubectl get pod -n dws
NAME                      READY   STATUS    RESTARTS   AGE
dwscontroller-754fd8868b-lnlcr   1/1     Running   0          3d
dwscontroller-754fd8868b-w2m8h   1/1     Running   0          3d
```

kubectl exec -ti -n dws Container_name bash

```
[root@10-63-90-40 ~]# kubectl exec -ti -n dws dwscontroller-754fd8868b-w2m8h bash
[service@dwscontroller-754fd8868b-w2m8h logs]$
```

cd /opt/cloud/3rdComponent/tomcat/logs

- According to the alarm generation time obtained in [Step 2](#), use keyword **DWS_00001** to search for the alarm information in **ossres-dws**. For details, see [Querying Logs Based on the Alarm Generation Time](#).
- After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **alarmSwitch**. Collect information about logs containing keyword **alarmSwitch**.
- Collect the alarm information and DWS Controller logs and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-1 SSH error codes

Error Code	Description
1100 1	SESSION_CONNECT_ERROR: Session connection failed.
1100 2	SESSION_DISCONNECT_ERROR: Session disconnected.
1100 3	SHELL_CHANNEL_OPEN_ERROR: Opening shell channels failed.
1100 4	SHELL_CHANNEL_CONNECT_ERROR: Shell channel connection failed.

Error Code	Description
1100 5	SHELL_CHANNEL_DISCONNECT_ERROR: Shell channel disconnected.
1100 6	SHELL_CHANNEL_RUN_COMMAND_ERROR: Running shell channel commands failed.
1100 7	SFTP_CHANNEL_OPEN_ERROR: Opening SFTP channels failed.
1100 8	SFTP_CHANNEL_CONNECT_ERROR: SFTP channel connection failed.
1100 9	SFTP_CHANNEL_UPLOAD_ERROR: SFTP channel uploading failed.
1101 0	SFTP_CHANNEL_DOWNLOAD_ERROR: SFTP channel downloading failed.
1101 1	GENERATE_RSA_KEYPAIR_ERROR: Failed to generate RSA key pairs.
1101 2	INIT_CHANNEL_ERROR: Channel initialization failed.
1101 3	INSTANCE_UPGRADING: An SSH error occurs during cluster upgrade.

2.1.2 DWS_00002 Database Operation Exception

Alarm Description

This alarm is generated when database operations are performed on DWS Controller and an exception occurs.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00002	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Database Operation Exception
	Type	Operation alarm
	First Occurred At	Time when an alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Related services may fail to be executed.

Possible Causes

The database is incorrectly connected; The database service is abnormal; The data is deleted incorrectly.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

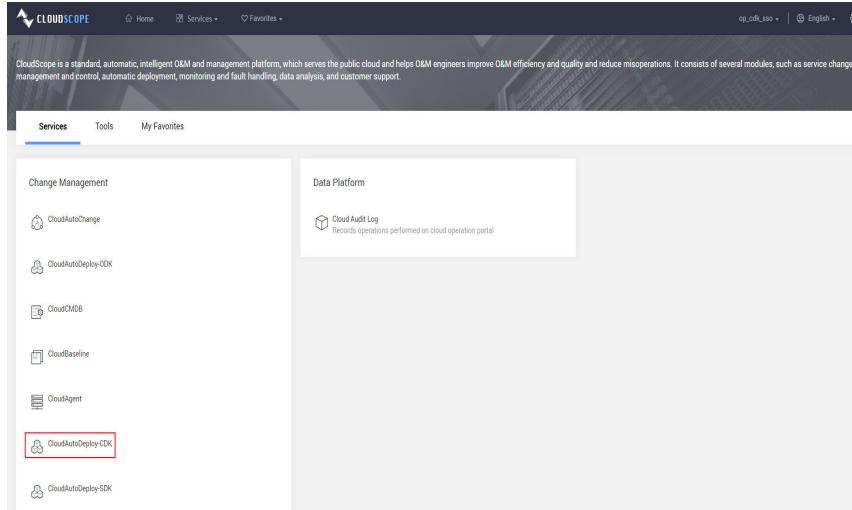
Step 2 Run the following commands to log in to a **dwscontroller** container and switch to the log path:

```
kubectl exec -ti -n Namespace Container_name bash  
cd /opt/cloud/3rdComponent/tomcat/logs
```

Step 3 Locate the **ossres-dws.log** log according to the alarm generation time on alarm platform. Then, use some characters in **Possible Causes** as the keyword and refer to the alarm generation time to locate the exception in the log.

Step 4 Preliminarily troubleshoot the exception based on the error information in the log. If the exception is caused by the failure to connect to the database node, perform the following steps:

- Log in to CloudScope and navigate to **CloudAutoDeploy-CDK**.



- Select the CDK cluster and namespace of dwscontroller.

This screenshot shows the 'Service Query' page in CloudScope. At the top, there are dropdown menus for 'CloudCDK_cdkClusterAdmin', 'Global', and 'bj-region-1'. Below that is a search bar with filters for 'ei-dbs-region' set to 'dws', 'All Status', and a search input 'Enter an instance name'. The main table lists a single instance: 'dwscontroller-x86_64' with 'Instance Name' 'dwscontroller-x86_64', 'Architecture' 'x86_64', 'Service Status' 'Running', 'Last Executed' 'Upgrade...', 'Template Name' 'dwscontroller...', 'Namespace' 'dws', 'Version' '1.0.0.202...', 'Creation Time' '2020-06-13 20:04:42 GMT+08:00', 'Update Time' '2020-06-14 20:59:58 GMT+08:00', and 'Operation' buttons for 'Upgrade' and 'Rollback'.

- Click **Upgrade** and use **db.** as the keyword for search to check whether the CDK parameters are consistent with those in the RDS instance information. If they are inconsistent, rectify the parameters. If the parameters are consistent, log in to the bearer tenant to check whether the RDS instance is normal. If the RDS instance is abnormal, manually restart it and try again.

This screenshot shows the 'Upgrade / Rollback' configuration page for the 'dwscontroller-x86_64' instance. It has tabs for 'Select Service', 'Configuration information', 'Information comparison', and 'Completed'. Under 'Installation Information', it shows 'Template Name: dwscontroller-x86_64(version: 1.0.0.20200611002405)' and a 'Description' field. Under 'Parameter Settings', there are 'Import JSON' and 'Export JSON' buttons, and a search bar with 'db.'. A table lists parameters: 'db.password' (string, value: 'd2NjX2NyXB0ATQzNDU1MzVGNDM0MjQzOzQ2NDM0N...'), 'db.username' (string, value: 'root'), 'db.driver' (string, value: 'com.mysql.jdbc.Driver'), and 'db.url' (string, value: 'jdbc:mysql://9.30.22.3:7306/rms?autoReconnect=true'). Buttons at the bottom include 'Previous', 'Next', and 'Cancel'.

Step 5 If the exception occurs during database import, for example, some fields do not exist or do not match, log in to the O&M container and connect to the database for troubleshooting based on the target table and target fields in the exception information. The procedure is as follows:

1. Run the following commands to connect to the O&M container, log in to the database node, connect to the **rms** database, and check the target fields:

kubectl exec -ti -n ecf Container_name bash

Floating IP address of the **mysql -h** database VM -P7306 -u database user;

Enter the user password as prompted and run the following command to switch to the rms database:

```
use rms;  
desc Target table name
```

2. Check whether the table fields are missing or the names do not match. Supplement the missing table fields based on the log information. If the database table cannot be recovered based on the log information, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.3 DWS_00003 Calling IAM Component Failed

Alarm Description

This alarm is generated when dwscontroller calls the IAM service and an exception occurs.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00003	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Calling IAM Component Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

An IAM exception, for example, a token obtaining or validation failure, will result in service execution failures.

Possible Causes

The IAM service is abnormal or the IAM configuration is incorrect.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

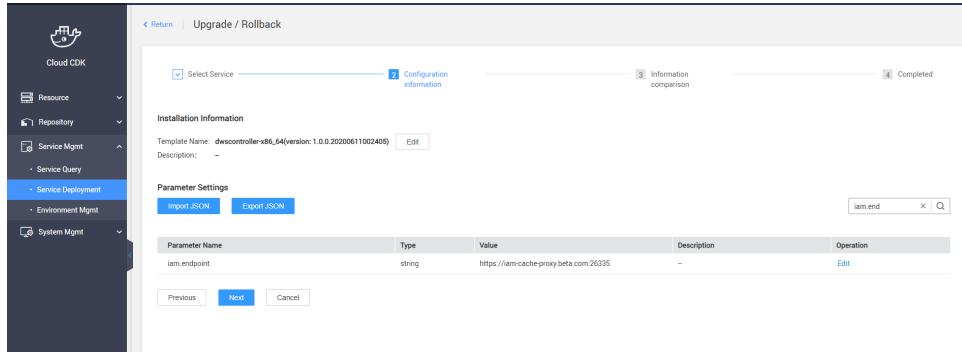
NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether the IAM component on DWS is correctly configured.

1. Log in to CloudScope and navigate to **CloudAutoDeploy-CDK**.
2. Choose **Service Query**, select the CDK cluster and namespace to which GaussDB(DWS) belongs, select the dwscontroller component, and click **Upgrade**. On the displayed page, all installation and deployment parameters of the dwscontroller component are displayed. Search for **iam.endpoint** to obtain the IAM parameter of the current environment.

Service Name	Instance Name	Architect..	Service St..	Last Exec..	Template Name	Namespa..	Version	Creation Time	Update Time	Operation
dwscontroller-	dwscontroller-x86_6...	x86_64	Runni...	Upgrade...	dwscontroller-	dws	1.0.0.202...	2020-09-13 20:04:42 GMT+08:00	2020-09-14 20:59:59 GMT+08:00	Upgrade Rollback More ▾



- Run the following command on the DWS O&M container. See the following figure.

ping iamdomain name

- If the ping operation succeeds, the IAM address is correct. Go to [Step 3](#).

```
[root@ecs-dws-maintain ~]# ping iam.cn-north-7.huaweicloud.com
PING iam.cn-north-7.huaweicloud.com (10.63.30.142) 56(84) bytes of data.
64 bytes from 10.63.30.142: icmp_seq=1 ttl=58 time=0.505 ms
64 bytes from 10.63.30.142: icmp_seq=2 ttl=58 time=0.304 ms
64 bytes from 10.63.30.142: icmp_seq=3 ttl=58 time=0.332 ms
64 bytes from 10.63.30.142: icmp_seq=4 ttl=58 time=0.309 ms
64 bytes from 10.63.30.142: icmp_seq=5 ttl=58 time=0.472 ms
64 bytes from 10.63.30.142: icmp_seq=6 ttl=58 time=0.344 ms
64 bytes from 10.63.30.142: icmp_seq=7 ttl=58 time=0.308 ms
^C
--- iam.cn-north-7.huaweicloud.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.304/0.367/0.505/0.081 ms
[root@ecs-dws-maintain ~]#
```

- If the ping operation fails, the IAM address is incorrect. Reconfigure the IAM address and retry previous services.

Step 3 If the IAM address is correct and can be successfully connected, search for and collect information about **Location Info** and **Possible Causes** of the alarm, and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-2 IAM error code

Error Code	Description
31001	IAM_GET_TOKEN_ERROR: Failed to obtain the token.
31002	IAM_RESOLVE_TOKEN_ERROR: Failed to parse the token.
31003	IAM_GET_RES_TENANT_ERROR: Failed to obtain the resource tenant.
31004	IAM_CREATE_RES_USER_ERROR: Failed to create the resource tenant.
31005	IAM_CREATE_GROUP_ERROR: Failed to create the group.

Error Code	Description
31006	IAM_CREATE_GROUPID_ERROR: Failed to create the group ID.
31007	IAM_QUERY_GROUPNAME_ERROR: Failed to query the group name.
31008	IAM_GET_ROLEID_FOR_TE_USER_ERROR: Failed to obtain the role ID of a tenant.
31009	IAM_GET_ROLEID_TO_IAM_ERROR: Failed to obtain the role ID of IAM.
31010	IAM_GET_PROJECTID_ERROR: Failed to obtain the project ID.
31011	IAM_BIND_ROLE_TO_GROUP_ERROR: Failed to bind a role to a group.
31012	IAM_ADD_USER_TO_GROUP_ERROR: Failed to add a user to a group.
31013	IAM_GET_AK_SK_FOR_TOKEN_ERROR: Failed to obtain the token AK/SK.
31014	IAM_GET_USERID_ERROR: Failed to obtain the user ID.

2.1.4 DWS_00004 Failed to Call the IaaS Component

Alarm Description

This alarm is generated when DWS Controller delivers tasks to the IaaS layer and a component on IaaS is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00004	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Call the IaaS Component
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Clusters may fail to be created, deleted, and expanded.

Possible Causes

Components on IaaS are abnormal or resources are insufficient.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Run the following commands to log in to a **dwscontroller** container and switch to the log path:

```
kubectl exec -ti -n Namespace Container_name bash  
cd /opt/cloud/3rdComponent/tomcat/logs
```

According to **First Occurred At** on OperationCenter, use keyword **DWS_00004** to search for the alarm information in **ossres-dws**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 3 After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **alarmSwitch**. Collect information about logs containing keyword **alarmSwitch**. View the error logs and locate the fault based on the error codes and messages returned by the IaaS components in the logs. The reference provides several common error codes for bottom-layer components and the corresponding solutions.

- If the error code or error message indicates that the flavor needs to be changed, run the following commands to connect to the O&M container, log in to the database node, and connect to the **rms** database to query the ECS

flavor used by the current cluster flavor. Then, switch to the ECS page to create a VM of the corresponding flavor and check whether the VM can be properly displayed and created.

Floating IP address of the **mysql -h** database VM -**P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the **rms** database:

use rms;

select * from rds_resspec where specCode= "DWS cluster flavor";

id	addedCodeInBill	bssProductId	comment	disabled	instanceType	regionCode	resTypeCode	specCode
f04f994c-81ae-4669-99dc-OTC_DWS_M3XLARGE	{"onHour": "92e86 CPU:4 ;Memor			0	master	cn-cmccl	otc.resource.type.dws.vm	dws.m3.xlarge

+ - × C ⌂

select * from rds_resspec where specCode= "dws.m3.xlarge"

Use the flavor ID obtained in the previous step to run the following command. The following figure shows the underlying flavor corresponding to the DWS flavor.

select * from rds_resspecattr where specId = 'flavor ID';

attrCode	specId	comment	value
cpu	f04f994c-81ae-4669-99dc-8392d6ad9c60		4
dataDisk	f04f994c-81ae-4669-99dc-8392d6ad9c60		160
dataVolumeNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	2
dnNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	2
flavor	f04f994c-81ae-4669-99dc-8392d6ad9c60		m3.xlarge.8
logDisk	f04f994c-81ae-4669-99dc-8392d6ad9c60		100
logVolumeNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	1
logVolumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	COMMON
mem	f04f994c-81ae-4669-99dc-8392d6ad9c60		32
osVolumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	COMMON
portNum	f04f994c-81ae-4669-99dc-8392d6ad9c60		4
volumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60		COMMON

+ - × C ⌂

select * from rds_resspecattr where specId = "f04f994c-81ae-4669-99dc-8392d6ad9c60"

If the ECS can be created but the DWS cluster flavor fails to be created, contact O&M engineers.

- If the error code or error message indicates that the disk type needs to be changed, connect to the O&M container, log in to the database node, and connect to the **rms** database to query the disk type used by the current cluster flavor. **Table 2-3** shows the disk mappings. Modify the disk type in the current environment based on the error message.

Table 2-3 Mappings between disks

DWS Disk Name	EVS Disk Name
ULTRAHIGH	SSD
COMMON	SATA
HIGH	SAS

attrCode	specId	comment	value
cpu	f04f994c-81ae-4669-99dc-8392d6ad9c60		4
dataDisk	f04f994c-81ae-4669-99dc-8392d6ad9c60		160
dataVolumeNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	2
dnNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	2
flavor	f04f994c-81ae-4669-99dc-8392d6ad9c60		m3.xlarge.8
logDisk	f04f994c-81ae-4669-99dc-8392d6ad9c60		100
logVolumeNum	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	1
logVolumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	COMMON
mem	f04f994c-81ae-4669-99dc-8392d6ad9c60		32
osVolumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60	(Null)	COMMON
portNum	f04f994c-81ae-4669-99dc-8392d6ad9c60		4
volumeType	f04f994c-81ae-4669-99dc-8392d6ad9c60		COMMON

```
+ - ✓ ✕ ⌂ ⌃
select * from rds_resspecattr where specId = "f04f994c-81ae-4669-99dc-8392d6ad9c60"
```

update rds_resspecattr set value = 'new flavor name' where specId = 'flavor ID' and attrcode = 'volumeType';

- If the error code or error message indicates that the exception is caused by NICs, that is, the current flavor does not support four NICs (by default, four NICs can be created for clusters of all flavors), contact O&M engineers to evaluate whether to change the flavor. For details, see the first case in [Step 3](#). If the NICs fail to be created, try again after a period of time. If the fault persists, contact O&M engineers.

Step 4 If the fault persists after the previous steps are performed, collect the alarm information on OperationCenter and dwscontroller logs, and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-4 IaaS error codes

Error Code	Description	Error Message	Solution
Ecs.0005	Invalid parameters.	request body is illegal.	Check whether the request body is of the correct JSON structure according to the API reference.
Ecs.0008	Invalid flavor attributes.	performancetype in extended flavor field [%s] is null.	Contact technical support to check whether the flavor registration is valid.
Ecs.0009	A flavor conflict occurred.	flavor[%s] could not support auto recovery.	Change the flavor when changing the ECS flavor.
Ecs.0010	The private IP address is already in use.	Private IP address %s is already in use.	Change the port.
Ecs.0011	The password does not meet the complexity requirement.	The password length must range from 8 to 26.	Check the password length and change the password.
Ecs.0012	The number of IP addresses is insufficient.	Insufficient IP addresses.	Check whether the floating IP addresses of the subnet are used up.
Ecs.0013	Insufficient EIP quota.	Insufficient EIP quota.	Apply for a higher EIP quota.
Ecs.0015	The disk of this type is not applicable to the ECS.	Flavor resource_type %s does not match volume_type %s.	Check whether the volume type matches the flavor.
Ecs.0019	Flavor abandoned.	Flavor %s is abandoned	Change another flavor.
Ecs.0027	Private flavor.	Flavor %s is private.	Change another flavor.
Ecs.0027	Private flavor, which cannot be used.	Flavor %s is private	Change another flavor.

Error Code	Description	Error Message	Solution
Ecs.0029	The flavor does not exist or has been abandoned.	the flavor[%s] does not exist.	Change another flavor.
Ecs.0031	The image does not exist.	image [%s] does not exist.	Change another image.
Ecs.0042	The number of attached data disks exceeds the maximum allowed limit.	The number of VBD volumes is %s, but KVM server supports up to 24.	Adjust the number of attached data disks.
Ecs.0043	The disk type does not exist.	volume type[%s] is not exist.	Change the disk type.
Ecs.0050	The number of NICs attached to the ECS exceeds the maximum value allowed.	The requested number of vif is bigger than the supplied.	Adjust the number of NICs.
Ecs.0101	Abnormal system disk status.	Status error of the system volume.	For details, contact technical support.
Ecs.0111	The disk is not in the attachment list.	volume %s is not in server %s attach volume list	Check whether the selected disk has been attached to the ECS, or replace the disk.
Ecs.0201	Failed to create a NIC.	Failed to create port in network %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0202	Failed to create the system disk.	Failed to create volume %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0203	Failed to create the data disk.	Failed to create volume %s because %s.	For details, see the returned error message or contact technical support.

Error Code	Description	Error Message	Solution
Ecs.0204	Failed to create the ECS.	Failed to add a tag to server %s: %s.	For details, see the returned error message or contact technical support.
Ecs.0205	Failed to attach the data disk.	Failed to call the Nova API to attach volume %s to ECS %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0212	Failed to allocate the private IP address.	Failed to call the Neutron API to view private IP addresses because the response is null or invalid.	For details, contact technical support.
Ecs.0214	Failed to create the network.	Failed to create VLAN network because %s.	For details, see the returned error message or contact technical support.
Ecs.0216	Failed to create the subnet.	Failed to create the subnet for vlan %s.	For details, see the returned error message or contact technical support.
Ecs.0217	Failed to attach the NIC.	attach server [%s] port [%s] fail ,reason is : %s	Contact technical support to locate the fault.
Ecs.0219	Failed to create the ECS.	Failed to quickly create server %s because the ECS status is error or %s.	For details, see the returned error message or contact technical support.
Ecs.0301	Failed to query the ECS.	The information, status, or metadata of server %s is null.	For details, see the returned error message or contact technical support.
Ecs.0302	Failed to query the ECS quota of the tenant.	Failed to view the quota usage of tenant %s because %s.	For details, see the returned error message or contact technical support.

Error Code	Description	Error Message	Solution
Ecs.0303	Failed to query the flavor.	Failed to view flavor %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0304	Failed to query the image.	Failed to view image %s because the image or image name is null.	Contact technical support to check whether the image has been correctly registered or to check other causes.
Ecs.0319	Insufficient flavor capacity.	check capacity: capacity is not enough.	Apply for expanding the flavor capacity.
Ecs.0501	Failed to delete the ECS.	ECS %s cannot be deleted because downloading the system volume data is in progress.	Try again later or contact technical support.
Ecs.0502	Failed to delete the private IP address.	Failed to roll back the EIP [%s] unbinding: %s.	For details, see the returned error message or contact technical support.
Ecs.0503	Failed to query the system volume.	Failed to view details about the volume because %s.	For details, see the returned error message or contact technical support.
Ecs.0507	Failed to delete the NIC.	Resource VLAN NICs cannot be deleted.	Check the NIC type.
Ecs.1100	Failed to access the IAM.	Failed to call the IAM API because %s.	For details, see the returned error message or contact technical support.
Ecs.1200	Failed to query the VPC.	Failed to view the EIP because %s.	For details, see the returned error message or contact technical support.

2.1.5 DWS_00006 Failed to Call the OBS Component

Alarm Description

This alarm is generated on dwscontroller when snapshots are being created, recovered, or deleted from a GaussDB(DWS) cluster and calling the OBS component is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00006	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Calling OBS Component Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The OBS component is abnormal. Operations, such as restoring a cluster or deleting a snapshot, will fail.

Possible Causes

- The network is disconnected.
- The network configuration is incorrect.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**.
Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Run the following commands to log in to the database node and connect to the **rms** database:

kubectl exec -ti Container_name -n ecf bash

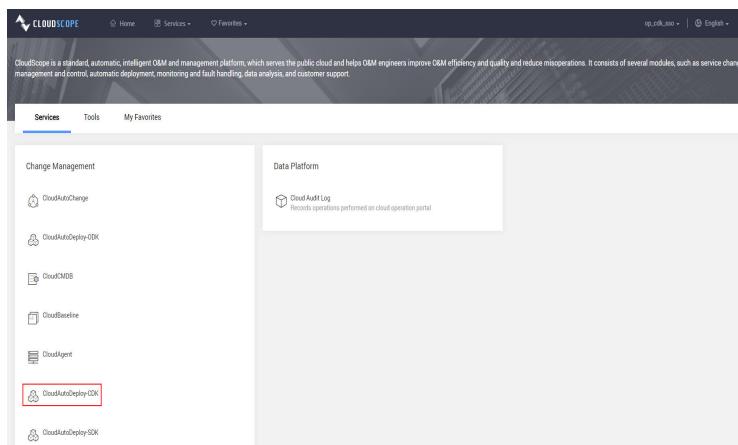
Floating IP address of the **mysql -h** database VM -P7306 -u database user;

Enter the user password as prompted and run the following command to switch to the **rms** database:

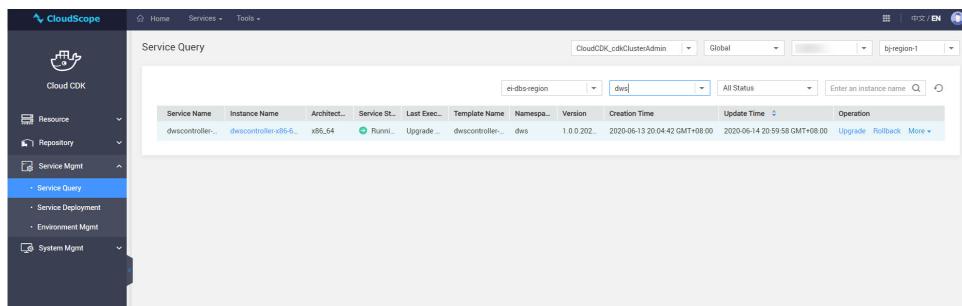
use rms;

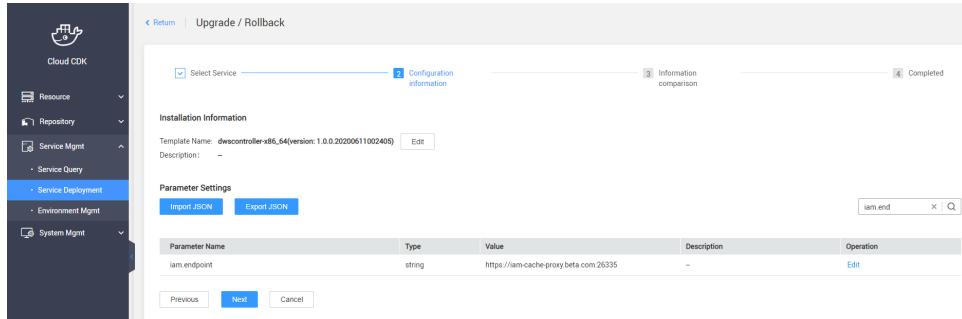
- Step 3** Check whether the OBS component of GaussDB(DWS) is correctly configured.

- Log in to CloudScope and navigate to **CloudAutoDeploy-CDK**.



- Choose **Service Query**, select the CDK cluster and namespace to which GaussDB(DWS) belongs, select the **dwscontroller** component, and click **Upgrade**. On the displayed page, all installation and deployment parameters of the **dwscontroller** component are displayed. Search for **obs.endpoint** to obtain the OBS parameter of the current environment.





- If the parameter is incorrect, modify it and retry.
- If the parameter is correct, go to **Step 4**.

Step 4 According to **instanceId** in the alarm, check whether **status** of the node is **200** and **monitorSwitch** is **1**. If the answers are yes, run the following command:

```
select status,monitorSwitch,managelp from rds_instance where id='InstanceId';
```

- If services on the node are in the normal state and you can ping **managelp** of the node by running the **ping managelp** command on the GaussDB(DWS) O&M container, go to **Step 5**.
- If services on the node are abnormal or you fail to ping **managelp** of the node, ignore the alarm and no further action is required.

Step 5 After confirming that you can log in to the node corresponding to **instanceId**, run the **connectTool.sh** command to log in to the node and run the **ping** command to check whether the node can connect to the OBS.

BOOK NOTE

- The address used in the **ping** command is the **obsEndpoint** address queried in **Step 3**.
- For details about how to log in to the node using SSH, see [Logging In to a Node in the Tenant Cluster](#).

ping obsEndPoint

- If the OBS can be pinged, go to **Step 6**.
- If the ping operation fails, ignore the alarm and contact O&M engineers to rectify the network fault.

Step 6 According to **First Occurred At** on OperationCenter, use keyword **DWS_00006** to search for the alarm information in **ossres-dws**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **alarmSwitch**. Collect information about logs containing keyword **alarmSwitch**.

Step 7 Collect OperationCenter alarm information and dwscontroller logs and contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-5 Error codes

Error Code	Description
61001	UPLOAD_BACKUP_FILE_FAILED: Failed to upload the backup file.
61002	UDSTOOL_DOWNLOAD_FAILED: Downloading failed.
61003	DELETE_BACKUP_FILE_FAILED: Failed to delete the backup file.
61004	OBS_ADDRESS_ILLEGAL_ERROR: Invalid OBS address.
61005	COPY_SNAPSHOT_FILE_FAILED: Failed to copy the snapshot.

2.1.6 DWS_00007 REST Component Call Exception

Alarm Description

This alarm is generated when dwscontroller calls the REST service and an exception occurs.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00007	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	REST Component Call Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If an exception occurs when REST is called, operations such as cluster creation and scale-out will fail.

Possible Causes

- The network is disconnected.
- The network configuration is incorrect.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 According to **First Occurred At** on OperationCenter, use keyword **DWS_00007** to search for the alarm information in **ossres-dws**. For details, see [Querying Logs Based on the Alarm Generation Time](#). After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **alarm**.

Step 3 Collect OperationCenter alarm information and dwscontroller logs and contact technical support.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.7 DWS_00008 Database Internal Exception

Alarm Description

This alarm is generated when service operations are performed on dwscontroller and bugs or unknown errors occur in the database.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00008	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Database Internal Exception
	Type	QoS alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Related services may fail to be executed.

Possible Causes

Unknown errors occur in the database.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If the error code is **SAFETYPARAM_APPLY_FAIL**, the security parameter setting fails.

Step 3 Obtain the node ID according to **Possible Causes**.

The following is an example of **Possible Causes**:

A DB internal error CloudOccurred when update safety params. configurationId: **4e0e4c15-fee4-6ec9-8d02-513b5ee9685b** instanceId:**1e0e4c15-cee4-4ec9-8d02-513b5ee9685b**

1e0e4c15-cee4-4ec9-8d02-513b5ee9685b indicates the node ID.

Step 4 Run the following commands to log in to the database node and connect to the **rms** database:

kubectl exec -ti Container_name -n ecf bash

Floating IP address of the **mysql -h** database VM -**P7306** -**u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

use rms;

select name from rds_instance where id='Node ID';

Step 5 On the GaussDB(DWS) O&M container, use SSH to log in to the cluster node ID queried in [Step 4](#).

For details about how to log in to cluster nodes using SSH commands, see [Logging In to a Node in the Tenant Cluster](#).

Step 6 Run the following commands to switch to user **Ruby** and check the node logs:

su - Ruby

vi /home/Ruby/log/cloud-dws-configureGuc.log

Step 7 Locate the exception in the log according to the alarm generation time, collect related information, and contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.8 DWS_00009 Failed to Call the DNS Component

Alarm Description

This alarm is generated when a user deletes a cluster to release the private network domain name and an error occurs.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00009	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Calling DNS Component Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The DNS information generated during cluster creation is retained.

Possible Causes

The DNS component is abnormal and cannot be properly accessed through the corresponding interface.

Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the node ID according to **Possible Causes**.

The following is an example of **Possible Causes**:

Delete record set failed, Response http status code is:400,Response Message body:
{"code":"DNS.0302","message":"This zone does not exist."}, clusterId is
6da32715-9974-4d3f-824a-4e0ff8d6993e

6da32715-9974-4d3f-824a-4e0ff8d6993e indicates the cluster ID.

Step 3 Run the following commands to log in to the database node and connect to the **rms** database:

Floating IP address of the **mysql -h** database VM -**P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

use rms;

Step 4 Check whether the domain name information exists in the **rds_zone_resource** table by using the cluster ID.

select * from rds_zone_resource where clusterId = 'cluster ID';



For details about how to obtain the cluster ID used in the preceding command, see [Step 2](#).

Step 5 Check whether the information contains domain names of the private and public networks.

If the domain names do not exist, they are successfully deleted, and no further action is required. If the domain names exist, go to [Step 6](#).

Step 6 Run the following commands to log in to a **dwscontroller** container and switch to the log path:

kubectl exec -ti -n Namespace Container_name bash

cd /opt/cloud/3rdComponent/tomcat/logs

Based on **First Occurred At** displayed on OperationCenter and the cluster ID, search for logs generated around the time when the alarm is reported in **ossres-dws.log**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 7 Collect log information and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.9 DWS_00010 Snapshot Operation Exception

Alarm Description

This alarm is generated when snapshot creation fails using DWS Controller.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00010	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	The snapshot operation of the GaussDB(DWS) cluster is abnormal.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Snapshot creation failed.

Possible Causes

The OBS is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 View the error code in **Location Info**.

If the error code is **CREATE_BACKUP_FAILED**, go to [Step 3](#).

Step 3 Obtain the node ID according to **Possible Causes**.

The following is an example of **Possible Causes**:

```
create backup failed! instanceId:[1e0e4c15-cee4-4ec9-8d02-513b5ee9685b] rdsChannel call  
[backupResult] failed. Message is cause:DO_BACKUP_FAILmessage:
```

1e0e4c15-cee4-4ec9-8d02-513b5ee9685b indicates the node ID.

Step 4 If keyword **Upload backup file to OBS failed** is displayed in **Possible Causes**, contact OBS technical personnel to check whether the OBS is faulty at the time when the alarm is reported.

- If OBS is faulty, contact the OBS technical support to rectify the fault. After the fault is rectified, you can create snapshots. No further action is required.
- If OBS is not faulty, run the following commands to log in to the database node and connect to the **rms** database:

Floating IP address of the **mysql -h** database VM **-P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the **rms** database:

use rms;

Log in to CDK and check whether the **obs.endpoint** parameter of the DWS Controller container is incorrectly configured.

- If the parameter is incorrect, modify the configuration and retry.
- If the parameter is correct, go to [Step 5](#).

Step 5 In the DWS O&M container, run the **connectTool.sh** command to log in to the node ID queried in [Step 3](#).

For details about how to log in to the node using the **connectTool.sh** command, see [Logging In to a Node in the Tenant Cluster](#).

Run the **ping** command to check whether the node can ping the OBS.

 NOTE

- The address in the **ping** command is the **obsEndpoint** address queried in step 3.
- For details about how to log in to cluster nodes using SSH commands, see [Logging In to a Node in the Tenant Cluster](#).

ping obsEndPoint

- If OBS can be pinged, go to the next step to collect logs.
- If the ping operation fails, ignore the alarm and contact O&M engineers to rectify the network fault.

Step 6 Run the following commands to switch to user **Ruby** and check the node logs:

su - Ruby

vi /home/Ruby/log/cloud-dws-deploy.log

Step 7 Locate the exception in the log according to the alarm generation time, collect related information, and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.10 DWS_00011 Upgrade Operation Exception

Alarm Description

This alarm is generated when the kernel upgrade or patch operation of DWS fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_00011	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Upgrade Operation Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

After the patch or upgrade task fails, a rollback is automatically performed. The cluster status may be affected in extreme cases.

Possible Causes

Possible causes are as follows:

1. The cluster status is abnormal.
2. The cluster operating status is abnormal.
3. The OS or the network environment of the node in the cluster is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain exception_code from the location Information and determine the cause of the upgrade failure. The following table describes the exception codes and corresponding upgrade operations.

Exception Code	Abnormal Upgrade Item
50001	Failed to upgrade the agent.
50002	Failed to upgrade the plug-in.
50003	Kernel upgrade failed.
50004	Failed to upgrade the cluster.
50005	Failed to roll back the kernel.
50006	Failed to roll back the cluster.
50007	Failed to submit the kernel.
50008	Failed to submit the cluster.
50009	Submission timed out.

Step 3 Obtain the cluster ID according to **Location Info**.

The following is an example of **Location Info**:

```
exception_code=UPDATE_AGENT_FAILURE, cluster_id=5791982f-c409-480a-9680-c56dc4083c95,
cluster_name=xwx700852_0417_813, datastore_type=dws, spec_code=dws.m3.xlarge, cluster_size=3,
failedReason=updateAgentFailure
```

In the preceding command, **cluster_id** indicates the cluster ID, for example, **5791982f-c409-480a-9680-c56dc4083c95**. **failedReason** indicates the failure cause. For example, **updateAgentFailure** indicates that the Agent fails to be upgraded.

- Step 4** Log in to Service CM, choose **Data Warehouse Service**, and choose **Upgrade Management**. Change the upgrade type based on the value of **failedReason**. If the Agent upgrade fails, set **Type** to **Agent**, search for the cluster information by cluster ID, and click **Details** to view the failure cause of the upgrade or patching.

No.	Type	Upgrade Procedure	JobID	Start Time	End Time	Error Information
1	agent	UpdatePrepareTask	2c908049879ccb4c01879dc97a3d02ed	2023/04/20 16:30:43 GMT+08:00	2023/04/20 16:30:53 GMT+08:00	--
2	agent	DeployAgentTask	2c908049879ccb4c01879dc97a3d02ed	2023/04/20 16:30:58 GMT+08:00	2023/04/20 16:31:05 GMT+08:00	Failed to execute task DeployAgentTask. Error ...
3	agent	UpdateInstanceTask	2c908049879ccb4c01879dc97a3d02ed	--	--	--
4	agent	SyncGULTask	2c908049879ccb4c01879dc97a3d02ed	--	--	--
5	agent	UpdateCompleteTask	2c908049879ccb4c01879dc97a3d02ed	--	--	--

- Step 5** In the DWS O&M container, log in to the cluster using the cluster ID.

For details about how to log in to the node using the **connectTool.sh** command, see [Logging In to a Node in the Tenant Cluster](#).

After logging in to the node, collect upgrade and patch logs stored in the **/home/Ruby/log** directory.

```
[root@host-192-168-3-44 Mike]# cd /home/Ruby/log/
[root@host-192-168-3-44 log]# ls
backup           cloud-dws-checkstatus.log      DataBaseEngineCollect.log.2018-01-18    dws_query_disk_volume.log  ps_set_log          updateDatastore.log
cloud-dws-setqueueparameter.log   connectTMS.log          dataReport.log        dws_upgrade_log  prepareConfigFile.log  updateInitialize.log
backup.log       connectTMS.log          dbs_mnton_backup.txt  get_variables.log  queryDiskVolume.log  updateInit.log
ces             DataBaseEngineCollect.log      deployPackage.log  haagent            restore.log         updatePrecheck.log
checkResult.log  DataBaseEngineCollect.log.2017-10-31  dws_base.log        haagentExtra.log  restore.txt        updateCommit.log
cloud-dws-checkstatus.log  DataBaseEngineCollect.log.2017-11-21  dws_base.log        initDb_log        setconfig.log
cloud-dws-deploy.log   DataBaseEngineCollect.log.2018-01-17  dws_check.log     netcardMonitor.log
```

- Step 6** Collect log information and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.11 DWS_00012 Service Node Overloaded

Alarm Description

This alarm is generated when the number of concurrent requests in seconds on a service node exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_0001 2	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Service Node Overloaded
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Some requests are intercepted and cannot produce results.

Possible Causes

1. For multi-pod nodes, consider concurrency skew caused by node exceptions.
2. The number of concurrent requests increases sharply due to attack behaviors.
3. The number of concurrent requests increases due to the normal increase of the demand of requests.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the **userId**, **remotelp**, **uri**, associated region, and overload type from **Location Info**, **Region**, and **Possible Causes**.

Step 3 The possible causes are as follows:

1. Check the service node status and check whether some nodes are faulty, causing concurrency to switch to other nodes.
2. View the logs of the corresponding service node, filter **olc** to obtain the URIs with a large number of concurrent requests, and analyze whether the increase of requests is normal.

Step 4 Perform the following operations based on the troubleshooting result in [Step 3](#):

1. If the first problem occurred, restore the service node.
2. If the second problem occurred, and the analysis conclusion is that the number of abnormal requests increases (for example, malicious attacks), manually handle malicious accounts.

If the analysis conclusion is that the number of requests increases within a normal range, you can increase the value of the cdk parameters **olc.custom.flow.rateLimit** and **olc.custom.admission.qps**. After the adjustment, check the running status of the service node. If the service is unstable, expand resources.

----End

Alarm Clearance

After the fault is rectified, clear the alarm in NMS alarm clearance mode.

Related Information

None

2.1.12 DWS_00013 Service Certificate Expiration

Alarm Description

Check the validity period of the management-plane certificate. This alarm is generated when the certificate is about to expire within 30 days. After the alarm is triggered, you need to upgrade the microservice certificate in a timely manner.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_0001 3	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Service Certificate Expiration
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the certificate is not replaced after it expires, the service authentication and startup will be abnormal.

Possible Causes

The certificate is not updated.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the container location, region, and possible alarm causes.

Step 3 Apply for a new certificate. To replace the certificate, decompress the [Data Warehouse Service \(DWS\) 8.1.3.331 Maintenance Guide \(for Huawei Cloud Stack 8.3.1\).zip](#) package to obtain the operation guide.

For details, see the section [Security Management > Certificate Management > Replacing Certificates](#) in [Data Warehouse Service \(DWS\) 8.1.3.331 Maintenance Guide \(for Huawei Cloud Stack 8.3.1\)](#).

----End

Alarm Clearance

After the fault is rectified, clear the alarm in NMS alarm clearance mode.

Related Information

None

2.1.13 DWS_01008 Node Status Fault

Alarm Description

This alarm is generated when DWS HAMonitor detects that the node status is abnormal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_01008	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Status Fault
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
	Other Information	Cluster details such as resourceId and domain_id.

Impact on the System

The node may be faulty.

Possible Causes

Some processes running on the node are unexpectedly stopped.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the OperationCenter and obtain the node name and ID according to **Location Info**.

The following is an example of **Location Info**:

```
instance_id: 08094ca2-0a1b-4848-a119-21cf70f95202,instance_name: dws-testTT-restore-2724-extension-extension-node-1-1,datastore_type: extension,spec_code: dws.d2.xlarge,node role: Standalone,private_ip: 192.168.0.115
```

In the preceding example, **dws-testTT-restore-2724-extension-extension-node-1-1** indicates the node name and **08094ca2-0a1b-4848-a119-21cf70f95202** indicates the node ID.

Step 3 In the DWS O&M container, run the **connectTool.sh** command to log in to the node queried in **Step 2**.

For details about how to log in to the node using the **connectTool.sh** command, see [Logging In to a Node in the Tenant Cluster](#).

Step 4 Run the following commands to switch to user **Ruby** and log in to the sandbox to view the status of all processes in the cluster:

```
su - Ruby
```

```
ssh `hostname -i`
```

```
cm_ctl query -C -v
```

The query result is as follows.

The process status can be either of the following:

- **normal**: indicates that the node is in the normal state. No further action is required.
 - Status except **normal**: indicates that the node is abnormal. Go to **Step 7**.

Step 5 Run the following commands to log in to the database node and connect to the **monitor** database:

Floating IP address of the mysql -h database VM -P7306 -u database user;

Enter the user password as prompted and run the following command to switch to the rms database:

use monitor;

Step 6 Run the following SQL statement to obtain the IP address of the DWSHAMonitor node from the **instance_monitor** and **monitor_info** tables:

SELECT

inst.id,inst.instance_orig_id,inst.cluster_id,inst.instance_name,inst.monitored,inst.monitor_switch,inst.STATUS,inst.manage_ip,inst.event_update_at,inst.is_cluster_status_reportor,

```
inst.instance_type,inst.monitor_id,mon.ip FROM instance_monitor inst,  
monitor_info mon WHERE instance_name LIKE "dws-nodelete%" AND  
inst.monitor_id = mon.id;
```

Step 7 Use the queried DWS HAMonitor node IP address to log in to the Monitor container and run the second command below to switch to the log path:

```
kubectl get pod -n ecf
```

```
[root@10-63-90-40 ~]# kubectl get pod -n ecf
NAME             READY   STATUS    RESTARTS   AGE
dbsevenet-b0b958554-pd5gg   1/1     Running   0          47d
dbsevenet-b0b958554-wn4l6   1/1     Running   0          47d
dbsinsight-7c897d5dc-rh9ds  1/1     Running   0          46d
dbsmonitor-7bfbdccfdc-mmwr7 1/1     Running   0          35d
dbsmonitor-7bfbdccfdc-pj6zg  1/1     Running   3          48d
ecfclustermanager-755958d57-2rdl2  0/1     CrashLoopBackOff  11014   38d
[root@10-63-90-40 ~]# kubectl exec -ti dbsmonitor-7bfbdccfdc-mmwr7 -n ecf bash
[service@dbsmonitor-7bfbdccfdc-mmwr7 bin]$ cd /opt/cloud/monitor/logs/
```

```
cd /opt/cloud/monitor/logs
```

According to **First Occurred At** on the alarm platform and the node ID obtained in **Step 2**, search for logs generated around the time when the alarm is reported in **hamonitor.log**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 8 Collect log information and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

In the DWS MHAMonitor log, if a message stating that the node status fault is reported for three consecutive times, the log information about the generated alarm is as follows:

```
[Fault Restore Thread: Instance(node ID), State(REPLICATE_STOPPED)] - begin save alarm.  
(AlarmMgr.java:59)  
[Fault Restore Thread: Instance(node ID), State(REPLICATE_STOPPED)] - save alarm success.  
(AlarmMgr.java:71)
```

2.1.14 DWS_01010 Cluster Status Is Abnormal

Alarm Description

This alarm is generated when DWS HAMonitor detects that the cluster status is abnormal for three consecutive times.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_01010	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Cluster Status Is Abnormal
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Service failures may occur in the cluster background.

Possible Causes

- The key nodes in the cluster are faulty.
- Network communication between nodes in a cluster is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the cluster ID according to the alarm generation time and **Location Info**.

The following is an example of **Location Info**:

```
cluster_id: b039030e-642f-4bf8-81cb-ef889bc2c75b,cluster_name: lxn7401,datastore_type: dws,cluster_size: 3,spec_code: dws.d2.xlarge,
```

08094ca2-0a1b-4848-a119-21cf70f95202 indicates the cluster ID.

Step 3 Run the following commands to log in to the database node and connect to the **rms** database:

Floating IP address of the **mysql -h** database VM **-P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

```
use rms;
```

Step 4 Run the following command to query the cluster status:

```
select status,name from rds_cluster where id='cluster ID';
```

 NOTE

For details about how to obtain the cluster ID used in the preceding command, see [Step 2](#).

- If **status** of the cluster is **300**, go to [Step 5](#).
- If **status** of the cluster is not **300**, no further action is required.

Step 5 Run the following commands to query the status of each node in the cluster and obtain the node name:

```
select i.id,i.name,i.status,t.execution_status,t.fail_reason,t.job_id  
from rds_instance as i join taskmgr_job as t  
where i.name like '%cluster name%' and i.jobId = t.job_id group by i.name;
```

- If the values of **status** of all nodes are not **300**, contact technical support.
- If the values of **status** of some nodes are **300**, go to [Step 6](#).

Step 6 In the DWS O&M container, run the **connectTool.sh** command to log in to the node whose **status** is **300**. Run the following commands to switch to user **Ruby** and log in to the sandbox to view the cluster status:

```
su - Ruby  
ssh `hostname -i`  
cm_ctl query -C -v
```

The query result is as follows.

```
[ Cluster State ]  
  
cluster_state : Normal  
redistributing : No  
balanced : Yes
```

 NOTE

For details about how to log in to the node using the **connectTool.sh** command, see [Logging In to a Node in the Tenant Cluster](#).

- If the values of **cluster_state** of all nodes are **normal** or **degraded**, no further action is required.
- If the values of **cluster_state** of nodes are not **normal** or **degraded**, exceptions occur on the node. Go to [Step 7](#).

Step 7 Run the following commands to log in to the database node and connect to the **monitor** database:

Floating IP address of the **mysql -h** database VM -P7306 -u database user;

Enter the user password as prompted and run the following command to switch to the rms database:

```
use monitor;
```

Run the following SQL statement to obtain the IP address of the DWSHAMonitor node from the **instance_monitor** and **monitor_info** tables:

```
SELECT  
inst.id,inst.instance_orig_id,inst.cluster_id,inst.instance_name,inst.monitored,inst.monitor_switch,inst.STATUS,i  
nst.manage_ip,inst.event_update_at,inst.is_cluster_status_reportor,
```

```
inst.instance_type,inst.monitor_id,mon.ip FROM instance_monitor inst, monitor_info mon WHERE instance_name LIKE "dws-nodelete%" AND inst.monitor_id = mon.id;
```

Step 8 Use the queried DWS Monitor node IP address to log in to the Monitor container and run the following command to check whether the HAMonitor process exists:

ps -ef | grep monitor

- If the following command output is displayed, the monitor process exists. Go to [Step 6](#).

```
[service@dbsmonitor-7bfbd6fdc-mmwr7 bin]$ ps -ef | grep monitor
root     13    7 0 Apr26 ?    00:00:00 su service -m -c /bin/sh /opt/cloud/monitor/bin/start.sh
service   14   13 0 Apr26 ?    00:00:00 /bin/sh /opt/cloud/monitor/bin/start.sh
service   18   14 40 Apr26 ?    13-14:00:50 java -jar -DPOD_NAMESPACE=ecf -DXmx=4096m
monitor-3.0.0-SNAPSHOT.jar
service 11154 10887 0 03:47 pts/0  00:00:00 grep --color=auto monitor
```

- If the following command output is displayed, the monitor process does not exist.

```
[rds@hamonitor1 logs]$ ps -ef | grep monitor
rds    116679 20241 0 05:28 pts/2  00:00:00 grep --color=auto monitor
```

Restart the POD of each Monitor. Wait for 3 to 4 minutes and check the POD startup status.

kubectl get pod -n ecf

kubectl delete pod [monitor container name] -n ecf

kubectl describe pod [monitor container name] -n ecf

After the container is started, the cluster status is updated in a certain period.

Run the following commands to switch to the log path and view logs to check whether the Monitor container is normal:

kubectl exec -ti [monitor container name] -n ecf bash

cd /opt/cloud/monitor/logs

According to **First Occurred At** on the alarm platform and the cluster ID, search for logs generated around the time when the alarm is reported in **hamonitor-ecf.log**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 9 Collect alarm information and logs and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.15 ECF_01015 Abnormal ECF Monitor Status

Alarm Description

This alarm is generated if DWSHAMonitor detects that the number of instance nodes exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
ECF_01015	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Abnormal ECF Monitor Status
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the monitor is abnormal, monitoring cannot be created for new nodes. As a result, cluster creation or scale-out may fail.

Possible Causes

The Monitor container monitors too many nodes. (Each container can monitor 1500 nodes.)

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Obtain the number of Monitor copies to be expanded based on the alarm generation time and **Other Information**.

An example of **Other Information** is as follows:

CloudService=DWS, resourceId: Monitor_Fault_Resource_Id, resourceIdName: Monitor_Fault_Resource_Name, Monitor instances capacity is exceed. It need more 1 monitors.

The preceding information indicates that a monitor container needs to be added.

- Step 3** Log in to CloudScope and switch to CloudAutoDeploy-CDK. Choose **Change Mgmt** and select the CloudAutoDeploy-CDK cluster and namespace to which the ecf service belongs. Select **dbsmonitor** and click **Next**. All installation and deployment parameters of all dbsmonitor components are displayed. Search for **REPLICATION** to obtain the monitor backup parameter of the current environment, add the value of this parameter to the number of containers to be added in the additional alarm information, update the parameter value, click **Next**, and click **Upgrade**.

- Step 4** If the alarm remains after the upgrade, collect alarm and log information and contact O&M engineers.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.16 DWS_01016 Failed to Update the Status

Alarm Description

Failed to synchronize the cluster or node status to the Controller.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_01016	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to update the status.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.
	status_pk_id	Domain ID for which the alarm is generated
	pod_name	Monitor container for which the alarm is generated.

Impact on the System

If this alarm is generated, the controller status fails to be synchronized, and the node status cannot be synchronized to the controller. More than 100 records are generated within two days.

Possible Causes

1. The controller domain name is unreachable.
2. The controller container is faulty.
3. The controller successfully sends the request. The request for invoking the controller /v2.0/insight/status-notification interface times out or an error is reported.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Scenario 1: The controller domain name is unreachable.

The domain name corresponding to controller_endpoint in the additional information may be unreachable. Log in to the monitor container corresponding to pod_name and run the curl -kv domain name corresponding to controller_endpoint command to check whether the domain name is correct. If the domain name is incorrect, contact O&M engineers.

```
[service@dbsmonitor-848bcb74bc-7wf62 bin]$ curl -kv dwscontroller.dws:18080
* Trying 10.247.50.101:18080...
* Connected to dwscontroller.dws (10.247.50.101) port 18080 (#0)
> GET / HTTP/1.1
> Host: dwscontroller.dws:18080
> User-Agent: curl/7.79.1
> Accept: /*/*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 400
< Content-Type: text/plain;charset=UTF-8
< Connection: close
<
Bad Request
This combination of host and port requires TLS.
* Closing connection 0
```

Step 3 Scenario 2: The controller container is faulty.

Log in to the background of the corresponding region and check whether the status of the DWS Controller container is Running and whether the value of READY is 1/1. If the value is 0/1, the container is faulty. If the container is faulty, contact O&M engineers.

```
[root@dws-test-master-1 ~]# kubectl get pod -ndws
NAME                  READY   STATUS    RESTARTS   AGE
dwscontroller-7fff577f74-xktvs   1/1     Running   0          23h
dwscontroller-7fff577f74-zmsfg   1/1     Running   0          1d
```

Step 4 Scenario 3: The controller successfully sends the notification, but an error is reported when the controller /v2.0/insight/status-notification interface is invoked.

1. Log in to the monitor container database,

```
select status_pk_id, cluster_orig_id, controller_endpoint, create_at from
status_change_event where controller_endpoint = 'controller_endpoint in
Additional Information' ORDER BY create_at desc;
```

Obtain status_pk_id and cluster_orig_id from the result.

2. Log in to the monitor container. You may need to log in to multiple containers to query logs. The logs are stored in the /opt/cloud/monitor/logs directory. Run the following command:

```
status_pk_id obtained by zgrep "[StatusEventDaemon]Send status change
event failed" hamonitor-ecf*|grep Step 4.1
```

```
hamonitor-ecf-49.log.gz:2023-05-26 04:11:44.389 [mon] [pool-2-thread-2] - IStatusChangeEventHandle statu... change event failed.event.StatusEvent{statusPkId="200007782859810105642<78348", clusterId="clustcfcf6-3b4e-47e6-a20a-cfb40
appType=0, clusterOrigId="42cf9570-d0fa-4de8-8879-972e2054fa6", instanceOrgId="5d91b1c7-0e0b-45dc-9e77-d7933908655", status=200, clusterStatus=200, groupStatus=mult, role="Standalone", clusterStatusDetails="Normal", logicalClusterStatus="Normal", logicalClusterName="elastic_group", logicalClusterType="Physical", activeMode=0, clusterType="Physical", instanceType="Physical", vnodeId=6, clusterCpu=24, "applications": [{"id": "0", "isRestoring": 0}], namespace="dws", controllerEndpoint="https://dwscontroller.dws:18080/rds", eventStatus="WAITING", createAt="2023-05-26 04:11:18"}[SendNotificationRunnable.java:93]
hamonitor-ecf-49.log.gz:2023-05-26 04:14:14.329 ERROR [pool-2-thread-8] - IStatusChangeEventHandle statu... change event failed.event.StatusEvent{statusPkId="200007782859810105642<78348", clusterId="clustcfcf6-3b4e-47e6-a20a-cfb40
appType=0, clusterOrigId="42cf9570-d0fa-4de8-8879-972e2054fa6", instanceOrgId="5d91b1c7-0e0b-45dc-9e77-d7933908655", status=200, clusterStatus=200, groupStatus=mult, role="Standalone", instanceType="Physical", clusterType="Physical", eventStatus="ERROR", createAt="2023-05-26 04:14:14"}[SendNotificationRunnable.java:93]
```

Obtain the result and the value of instanceOrgId.

3. Run the zgrep -C 5 **Step 4.2** Search result time **Step 4.2** Search result log file, as shown in the following figure.

If the value of `is Read time out`, no response is returned within 60 seconds after the interface is invoked. The operation may be successful or fail. You need to view logs on DWS Controller.

4. Log in to the DWSController container. You may need to log in to multiple DWSController containers to query logs. The logs are stored in the /opt/cloud/3rdComponent/install/MwTomcat-2.1.5/logs directory. Run the following command:

zgrep "Start changeStatus, req" internal-api-dws*|grep **Step 4.2** Obtained instanceOrigId|grep **Step 4.2** Obtained time, as shown in the following figure.

Run the following command to search for based on the ID in the red box that is closest to the search time:

```
zgrep c43c9bf869a54c0ebf952e99b039b01e ossres-dws.log*
```

```
[service@odwscontroller-ffff577f4-xktxs logs]$ zgrep c43c9bf869a54c0ebf952e99b039b01e ossres-dws.log*  
ossres-dws.log.37.gz:2023-05-26 04:12:59,309[https_jsse-nio-172.16.1.34-7443-exec-16][INFO]c43c9bf869a54c0ebf952e99b03  
insight/status-notification[com.huawei.hclouds.dbs.api.interceptor.InsightInterceptor.preHandle[InsightInterceptor].ja  
ossres-dws.log.37.gz:2023-05-26 04:12:59,310[https_jsse-nio-172.16.1.34-7443-exec-16][INFO]c43c9bf869a54c0ebf952e99b03
```

5. Check whether the log contains ERROR. As shown in the following figure, GaussDB(DWS).0000 is returned, indicating that the request is normal.

6. Log in to CloudScope and switch to CloudAutoDeploy-CDK. Choose Change Management and select the CloudAutoDeploy-CDK cluster and namespace to which the ecf service belongs. Select the dbsmonitor component and click Next. On the page that is displayed, all installation and deployment parameters of all dbsmonitor components are displayed. Search for sending.change.status.max.count to obtain the parameters of the current environment, increase the value of this parameter by 500, update the parameter value, click Next, and click Upgrade.
 7. If the alarm remains after the upgrade, collect alarm and log information and contact O&M engineers.

End

Alarm Clearance

The monitor sends the message for three times. If the message fails to be sent for three times, the synchronization status is SENDING. You need to manually clear the synchronization status.

Related Information

None

2.1.17 DWS_02002 Cluster Operations Are Abnormal

Alarm Description

Cluster operation exceptions belong to service exceptions. This alarm is generated when the network is faulty or the cluster is not running properly. A prompt is displayed asking for manual handling.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02002	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Cluster Operation Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

- Cluster creation fails.
- Clusters cannot be deleted and resources cannot be released.
- Clusters cannot be restarted, affecting user experience.
- The cluster cannot be scaled out by segment because the preparation for segment-based scale-out fails.

Possible Causes

- The network is disconnected.
- The cluster is abnormal.
- Services are abnormal.
- Failed to prepare for capacity expansion.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the error code and error location according to **Location Info**.

Step 3 If the error code is **CREATE_INSTANCE_EXCEPTION**, obtain the cluster ID from **Location Info**.

The following is an example of **Location Info**:

```
exception_code=CREATE_CLUSTER_EXCEPTION, cluster_id=a61114a1-6b6d-4405-92c0-3f2a351af987,  
cluster_name=dws-dttb2018-07-04-04-test, datastore_type=dws, spec_code=dws.d2.xlarge, cluster_size=3
```

a61114a1-6b6d-4405-92c0-3f2a351af987 indicates the cluster ID.

Step 4 Run the following commands to log in to the database node and connect to the **rms** database:

```
kubectl exec -ti Container_name -n ecf bash
```

```
mysql -h Floating_IP_address_of_the_database -u Database_username -P7306 -  
pDatabase_password;
```

```
use rms;
```

Step 5 Run the following command in the database to check the status of each node in the cluster:

```
select i.id,i.name,i.status,t.execution_status,t.fail_reason,t.job_id  
from rds_instance as i join taskmgr_job as t  
where i.name like '%cluster name%' and i.jobId = t.job_id group by i.name;
```

- If **status** of each node is not **300**, ignore the alarm and no further action is required.

- If the values of **status** of some nodes are **300**, go to [Step 6](#).

Step 6 Run the following command to log in to the dwscontroller container and switch to the log path:

```
kubectl get pod -n dws  
kubectl exec -ti [Container name] -n dws bash  
cd /opt/cloud/3rdComponent/tomcat/logs
```

Run the following command to filter information in the **ossres-dws.log** log:

```
grep "value of job_id obtained in Step 5" ossres-dws.log | grep "ERROR"
```

Collect log information according to **First Occurred At**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 7 Collect log files and alarm files and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-6 Error codes

Error Code	Description
02001	EARLY_WARNING: Early warning.
02002	BUSINESS_FAIL: Service failed. Exceptions that are hard to describe are classified into this group. The causes of service failures are detailed in Location Info and Possible Causes .
02003	CREATE_INSTANCE_EXCEPTION: An exception occurs during cluster creation.
02004	CREATE_READREPLICA_INSTANCE_EXCEPTION: An exception occurs when a read-only cluster is being created.
02005	RESTART_INSTANCE_EXCEPTION: Restart failed.
02006	REPAIR_INSTANCE_EXCEPTION: An exception occurs during cluster repair.

2.1.18 DWS_02020 Cluster Redistribution Failed

Alarm Description

This alarm is generated during cluster scale-out and sent to SRE for analysis of the root cause of the redistribution failure.

Symptom: Redistribution is always in progress, and redistribution cannot be suspended.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02020	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Cluster Redistribution Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Redistribution failure may cause the cluster to be unavailable.

Possible Causes

The network is faulty, the lock wait times out (services are being executed), or the disk space is insufficient during redistribution.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the first CN node in the cluster and view the **gs_expand** and **gd_redis logs** to locate the root cause.

gs_expand log path: **\$GAUSSLOG/om/**

gs_redis log path: **\$GAUSSLOG/bin/gs_redis/**

```
[root@host-172-16-40-18 Mike]# su Ruby
[Ruby@host-172-16-40-18 Mike]# cd $GAUSSLOG
[Ruby@host-172-16-40-18 Ruby]# ll
total 0
drwxr-x--- 10 Ruby Ruby 129 Nov 16 03:08 bin
drwxr-x--- 5 Ruby Ruby 57 Nov 16 03:05 cm
drwxr-x--- 2 Ruby Ruby 6 Nov 16 03:05 gs_obs
drwxr-x--- 9 Ruby Ruby 267 Nov 18 00:07 gs_profile
drwxr-x--- 2 Ruby Ruby 265 Nov 18 08:08 om
drwxr-x--- 9 Ruby Ruby 111 Nov 16 03:05 pg_audit
drwxr-x--- 9 Ruby Ruby 111 Nov 16 03:05 pg_log
[Ruby@host-172-16-40-18 Ruby]# pwd
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-40-18 Ruby]#
```

- Step 3** After the fault is rectified, run the redistribution command in the background or contact the customer to re-deliver the redistribution task on the GUI.

- Step 4** To restore redistribution on the page, you need to modify the mutual exclusion matrix on the management plane and the status in the Redis table. The operation procedures are as follows:

1. Run the following statement to query Quartz tasks and check whether any redistribution progress query task is being executed:

select * from qrtz_triggers where trigger_name = 'cluster ID';

If a task is found, run the following statement to suspend the task:

update qrtz_triggers set TRIGGER_STATE = 'PAUSED' where trigger_name = 'cluster ID';

If no task is found, perform steps **Step 4.2** to **Step 4.4**.

2. Log in to the database on the management plane, query the **rds_action** table, filter data based on the cluster ID (the filtering field is **objId**), and change the action field to **REDISTRIBUTION_PAUSED**. The statement is as follows:

update rds_action set action = 'REDISTRIBUTION_PAUSED' where objId = 'Cluster ID';

3. Query the **rds_redis_info** table, filter data based on the cluster ID (the filtering field is **cluster_id**), and change the status field to the **PAUSED**. The statement is: **update rds_redis_info set status = 'PAUSED' where cluster_id = 'cluster id';**

4. A message is displayed on the user page, indicating that the redistribution is suspended. Click **Restore**.

5. After a message is displayed indicating that the restoration is successful, check whether the **gs_expand** and **gs_redis** processes exist in the background. If they exist, the restoration is successful.
6. Restore the quartz task and query the progress again.
update qrtz_triggers set TRIGGER_STATE = 'WAITING' where trigger_name = 'cluster ID';

Step 5 On the page, check the cluster status and mutual exclusion matrix. If no exception is found, the rectification is complete.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.19 DWS_02021 Failed to Pause Cluster Redistribution

Alarm Description

The cluster attempts to pause redistribution during scale-out. However, the pause function does not take effect.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02021	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Pause Cluster Redistribution
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Redistribution failure may cause the cluster to be unavailable.

Possible Causes

The network is faulty, the lock wait times out (services are being executed), or the disk space is insufficient during redistribution.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the first CN node in the cluster and view the **gs_expand** and **gd_redis logs** to locate the root cause.

gs_expand log path: **\$GAUSSLOG/om/**

gs_redis log path: **\$GAUSSLOG/bin/gs_redis/**

```
[root@host-172-16-40-18 Mike]# su Ruby
[Ruby@host-172-16-40-18 Mike]# cd $GAUSSL0G
[Ruby@host-172-16-40-18 Ruby]# ll
total 0
drwxr-x---. 10 Ruby Ruby 129 Nov 16 03:08 bin
drwxr-x---. 5 Ruby Ruby 57 Nov 16 03:05 cm
drwxr-x---. 2 Ruby Ruby 6 Nov 16 03:05 gs_obs
drwxr-x---. 9 Ruby Ruby 267 Nov 18 00:07 gs_profile
drwxr-x---. 2 Ruby Ruby 265 Nov 18 08:08 om
drwxr-x---. 9 Ruby Ruby 111 Nov 16 03:05 pg_audit
drwxr-x---. 9 Ruby Ruby 111 Nov 16 03:05 pg_log
[Ruby@host-172-16-40-18 Ruby]# pwd
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-40-18 Ruby]#
```

Step 3 After the fault is rectified, run the redistribution command in the background or contact the customer to re-deliver the redistribution task on the GUI.

Step 4 To restore redistribution on the page, you need to modify the mutual exclusion matrix on the management plane and the status in the Redis table. The operation procedures are as follows:

1. Run the following statement to query Quartz tasks and check whether any redistribution progress query task is being executed:

```
select * from qrtz_triggers where trigger_name ='cluster ID';
```

If a task is found, run the following statement to suspend the task:

```
update qrtz_triggers set TRIGGER_STATE = 'PAUSED' where trigger_name = 'cluster ID';
```

If no task is found, perform steps [Step 4.2](#) to [Step 4.4](#).

2. Log in to the database on the management plane, query the **rds_action** table, filter data based on the cluster ID (the filtering field is **objId**), and change the action field to **REDISTRIBUTION_PAUSED**. The statement is as follows:

```
update rds_action set action = 'REDISTRIBUTION_PAUSED' where objId ='Cluster ID';
```

3. Query the **rds_redis_info** table, filter data based on the cluster ID (the filtering field is **cluster_id**), and change the status field to the **PAUSED**. The statement is: **update rds_redis_info set status = 'PAUSED' where cluster_id ='cluster id'**;

4. A message is displayed on the user page, indicating that the redistribution is suspended. Click **Restore**.

5. After a message is displayed indicating that the restoration is successful, check whether the **gs_expand** and **gs_redis** processes exist in the background. If they exist, the restoration is successful.

6. Restore the quartz task and query the progress again.

```
update qrtz_triggers set TRIGGER_STATE = 'WAITING' where trigger_name ='cluster ID';
```

Step 5 On the page, check the cluster status and mutual exclusion matrix. If no exception is found, the rectification is complete.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.20 DWS_02022 DMS Kafka Service Unavailable

Alarm Description

In GaussDB(DWS) 8.2.1 and later versions, the DMS message queue feature is enabled. After Kafka is enabled, the Kafka service is unavailable. This alarm is generated when the system detects that the Kafka service connection is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_0202 2	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	DMS Kafka Service Unavailable
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

In an environment where Kafka is enabled, there are a large number of nodes and the collection pressure is high. Once the Kafka is abnormal, DMS immediately switches to the memory processing mode. In this mode, the upper limit of the data processing capability is low and up to 2000 nodes can be supported. If there are too many nodes in the environment, the data collection service will be overloaded, data collection is slow and the system may break down.

Possible Causes

1. The environment parameter settings are incorrect. As a result, the client cannot connect to the server.
2. The network is disconnected.
3. The Kafka service is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Check whether the service interruption is caused by connection timeout or other network problems based on the alarm information. If yes, go to the next step. If no, contact R&D engineers.
- Step 3** Choose **Change Mgmt > Service List**. Select the region for which the alarm is generated, go to ei-dbs (tenant plane), and search for **collection**. Find the dms-collection service, view its details, and check whether the Kafka parameter settings are correct. If the Kafka service is purchased, check whether the service instance is running properly on the cloud console. If the instance is deployed independently, check the service running status on CDAS. If the Kafka service is abnormal, contact platform technical support.
- Step 4** After ensuring that the Kafka service is running, configure the correct Kafka configuration information in **DMS_Collection** and restart **DMS-Collection** through service upgrade on CloudScope for the change to take effect.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.21 DWS_02030 Inconsistent Agent Versions

Alarm Description

This alarm is generated when the guestAgentVersion of the DB instance after scaling is inconsistent with that of the original DB instance.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02030	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Inconsistent Agent Versions
	Type	QoS alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The guestAgentVersion of the DB instance after scaling is different from that of the original DB instance.

Possible Causes

The guestAgentVersion of the DB instance after scaling is different from that of the original DB instance.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the IP address and the error code and error location according to **Location Info**.

Step 3 Obtain the cluster's tenant information from **Other Information**, such as the tenant name, tenant ID, and resource tenant name.

Step 4 Obtain the cluster name, ID, flavor, and node quantity from **Location Info**.

The following is an example of **Location Info**:

```
exception_code=GrowCluster_Instance_Exception  
, cluster_id=a61114a1-6b6d-4405-92c0-3f2a351af987, cluster_name=dws-dttb2018-07-04-04-test,  
datastore_type=dws, spec_code=dws.d2.xlarge, cluster_size=3
```

a61114a1-6b6d-4405-92c0-3f2a351af987 indicates the cluster ID.

Step 5 Try checking possible causes.

The guestAgentVersion of the instance after scaling is different from that of the original instance. You need to upgrade the guestAgentVersion.

Step 6 If the exception cause cannot be found in the logs, collect related log information and alarm information and contact technical support.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.22 DWS_02040 Failed to Synchronize GUC Parameters

Alarm Description

This alarm is generated when the cluster fails to invoke the **sync_guc.py** script on the tenant side to synchronize GUC parameters to the database on the management plane.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02040	Management plane alarm	Minor	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Synchronize GUC Parameters
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

1. This problem does not affect services in the customer's cluster.
2. When you modify GUC parameters on the parameter modification page, a failure message may be displayed. However, the modification is successful. Customers may get a bad experience and submit consultation orders.

Possible Causes

1. The disk space is insufficient and the cluster is read-only. You need to expand the disk capacity or delete unnecessary data.
Run the following SQL statement using gsql:

```
select * from pg_settings;
```

Check whether the SQL statement is successfully executed.
2. The number of SQL connections in the cluster exceeds the upper limit.
Change the values of **max-connections** and **max_prepared_transactions**.
The following error message may be displayed for the service. After the number of connections decreases, the service and the parameter modification page return to normal.
Try 1 out of 1Exception:connection to server at "10.128.64.171", port 8000 failed: FATAL: Already too many clients, active/non-active/reserved: 11/808/3.
Try 1 out of 1Exception:pooler: failed to create 1 connections, Error Message: remote node cn_5001, detail: FATAL: cn_5001: Already too many clients, active/non-active/reserved: 10/809/3.FATAL: cn_5001: Already too many clients, active/non-active/reserved: 9/810/3.

Handling Procedure

- Step 1** Log in to the **cn-1-1** or **cn-2-1** node of the cluster and check whether the following log file exists. If the file does not exist, switch to another Coordinator node and search for **/home/Ruby/log/cloud-dws-syncguc.log**.
- Step 2** Run the **vi /home/Ruby/log/cloud-dws-syncguc.log** command to view the failure cause in the log.
- Step 3** Generally, this problem is not a code problem. If the number of connections is insufficient, you need to modify the GUC parameters. Go to the GUC configuration on the Service CM, select the corresponding cluster to modify the GUC configuration, and enter the parameter name and value.

Modify GUC Config

Cluster Name	test_gaoze
Parameter Name	Enter a parameter name.
Node Type	CN & DN
Parameter Value	Enter a parameter value.

OK Cancel

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.23 DWS_02070 DWS Failed to Automatically Update the External Data Source Configuration

Alarm Description

When the cluster fails to automatically update the external data source configuration, notify the SRE to locate the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_02070	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	DWS_02070 DWS Failed to Automatically Update the External Data Source Configuration

Type	Parameter	Description
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If an external data source is configured for the cluster and the failure alarm is generated for three times, the foreign table data associated with the data source cannot be accessed.

Possible Causes

Failed to request IAM to obtain the token or the cluster is faulty and the token update cannot be delivered.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 According to the IP address obtained in **Step 1**, run the following command to log in to dwscontroller and switch to the log path:

kubectl get pod -n dws. In the command output, **NAME** indicates the container name.

```
[root@10-63-90-40 ~]# kubectl get pod -n dws
NAME                      READY   STATUS    RESTARTS   AGE
dwscontroller-754fd8868b-lnlcr   1/1     Running   0          3d
dwscontroller-754fd8868b-w2m8h   1/1     Running   0          3d
```

kubectl exec -ti -n dws Container_name bash

```
[root@10-63-90-40 ~]# kubectl exec -ti -n dws dwscontroller-754fd8868b-w2m8h bash
[service@dwscontroller-754fd8868b-w2m8h logs]$
```

```
cd /opt/cloud/3rdComponent/tomcat/logs
```

According to **First Occurred At** on OperationCenter, use keyword **DWS_02070** to search for the alarm information in **ossres-dws.log**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 3 After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **ConfigExtDataSourceTask**. Collect information about logs containing keyword **ConfigExtDataSourceTask**.

Step 4 Collect OperationCenter alarm information and dwscontroller logs and contact O&M engineers.

----End

Alarm Clearance

After the fault is rectified, manually clear the alarm.

Related Information

None

2.1.24 DWS_10000 Internal System Exception

Alarm Description

This alarm is generated on the dwscontroller node when service operations are performed on dwscontroller and bugs or unknown errors occur.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_10000	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Internal System Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Service operations may fail.

Possible Causes

Unknown system errors exist.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** According to the IP address obtained in **Step 1**, run the following command to log in to dwscontroller and switch to the log path:

kubectl get pod -n dws

In the command output, **NAME** indicates the container name.

```
[root@10-63-90-40 ~]# kubectl get pod -n dws
NAME                  READY   STATUS    RESTARTS   AGE
dwscontroller-754fd8868b-lnlcr   1/1     Running   0          3d
dwscontroller-754fd8868b-w2m8h   1/1     Running   0          3d
```

kubectl exec -ti -n dws Container_name bash

```
[root@10-63-90-40 ~]# kubectl exec -ti -n dws dwscontroller-754fd8868b-w2m8h bash
[service@dwscontroller-754fd8868b-w2m8h logs]$
```

cd /opt/cloud/3rdComponent/tomcat/logs

According to **First Occurred At** on OperationCenter, use keyword **DWS_10000** to search for the alarm information in **ossres-dws.log**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

- Step 3** After locating the alarm, search for logs that are generated around the time when the alarm is reported and contain keyword **alarmSwitch**. Collect information about logs containing keyword **alarmSwitch**.

- Step 4** Collect OperationCenter alarm information and dwscontroller logs and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Table 2-7 Error codes

Error Code	Description
10001	ASSERT: Unknown error.
10003	INTERNAL_ERROR: Internal error.

2.1.25 DWS_20003 Cluster Creation Exception

Alarm Description

This alarm is generated when a cluster fails to be created.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_20003	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Cluster Creation Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Cluster creation fails.

Possible Causes

1. Underlying resources such as ECSs fail to be created.
2. The network between the management side and tenant side is disconnected.
3. GaussDB fails to be installed.
4. HAMonitor monitoring fails to be established.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the error code and error location according to **Location Info**.

Step 3 Obtain the cluster's tenant information from **Other Information**, such as the tenant name, tenant ID, and resource tenant name.

Step 4 Obtain the cluster name, ID, flavor, and node quantity from **Location Info**.

The following is an example of **Location Info**:

```
exception_code=CREATE_CLUSTER_EXCEPTION, cluster_id=a61114a1-6b6d-4405-92c0-3f2a351af987,  
cluster_name=dws-dttb2018-07-04-04-test, datastore_type=dws, spec_code=dws.d2.xlarge, cluster_size=3
```

a61114a1-6b6d-4405-92c0-3f2a351af987 indicates the cluster ID.

Step 5 Locate the fault based on the error code and error information in the log. The procedure is as follows:

1. Run the following commands to log in to the database node and connect to the **rms** database:

Floating IP address of the **mysql -h** database VM -**P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

use rms;

2. Run the following command in the database to check the status of each node in the cluster:

```
select name from rds_cluster where id = 'cluster ID';  
select i.id,i.name,i.status,t.execution_status,t.fail_reason,t.job_id  
from rds_instance as i join taskmgr_job as t  
where i.name like '%cluster name%' and i.jobId = t.job_id group by i.name;
```

3. Run the following command to log in to the dwscontroller container and switch to the log path:

```
cd /opt/cloud/3rdComponent/tomcat/logs
```

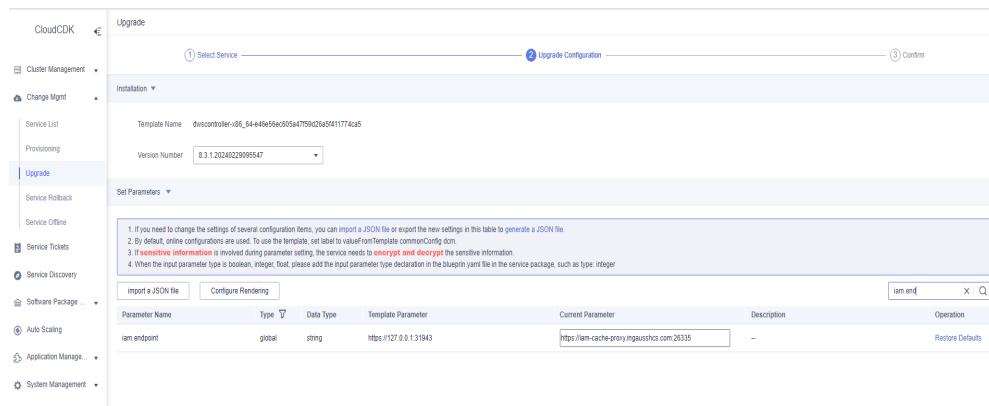
Run the following command to filter the **ossres-dws.log** log:

```
grep "job ID of any node obtained in step Step 5.2 ossres-dws.log |grep ERROR
```

Collect log information according to **First Occurred At**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

- Step 6** If the log indicates that the error is caused by the IAM service exception, check whether the IAM parameter is correct. If it is incorrect, correct it and try again.

1. Log in to CloudScope and navigate to **CloudAutoDeploy-CDK**.
2. In the navigation pane on the left, choose **Change Magmt & > Upgrade**, select the corresponding region. Search for **dwscontroller** in the search box, select the corresponding dwscontroller, and click **Next**.
3. On the displayed page, all installation and deployment parameters of the DWS Controller component are displayed. Search for **iam.endpoint** to obtain the IAM parameters of the current environment. If the parameters are incorrect, correct them and upgrade the CloudAutoDeploy-CDK.



4. After the upgrade, run the following commands to restart the POD:

```
kubectl get po -n dws
```

```
kubectl delete po [container name] -n dws
```

- Step 7** If the log contains ECS error code, view the detailed error information. The following lists ECS errors that may occur and the troubleshooting methods. Rectify the errors and try again.

Error Code	Description	Error Message	Solution
Ecs.0001	The number of ECSS has reached the maximum allowed.	the number of instance above quota limits	Apply for a higher quota of the corresponding resource according to the returned error message.

Error Code	Description	Error Message	Solution
Ecs.0012	The number of IP addresses is insufficient.	Insufficient IP addresses.	Check whether the floating IP addresses of the subnet are used up.
Ecs.0015	The disk of this type is not applicable to the ECS.	Flavor resource_type %s does not match volume_type %s.	Check whether the volume type matches the flavor.
Ecs.0019	Flavor abandoned.	Flavor %s is abandoned	Change another flavor.
Ecs.0027	Private flavor.	Flavor %s is private.	Change another flavor.
Ecs.0021	Insufficient EVS disk quota.	cinder quota check fail:volume count is over limits	Apply for a higher EVS disk quota.
Ecs.0022	The number of ECS groups has reached the maximum allowed.	the number of instance above server group quota limits	Apply for a higher ECS group quota.
Ecs.0025	EVS is not authorized to obtain KMS keys for encrypting EVS disks.	Failed to check the role of kms	Authorize EVS to obtain KMS keys for encrypting EVS disks.
Ecs.0027	Private flavor, which cannot be used.	Flavor %s is private	Change another flavor.
Ecs.0028	The blacklisted user configured in the flavor is not allowed to use the flavor.	The user is contained in %s and is not allowed use the flavor.	Change another flavor.
Ecs.0029	The flavor does not exist or has been abandoned.	the flavor[%s] does not exist.	Change another flavor.
Ecs.0030	The ECS has been frozen.	The server %s is freezed.	Check whether the account has been frozen or contact technical support.
Ecs.0031	The image does not exist.	image [%s] does not exist.	Change another image.

Error Code	Description	Error Message	Solution
Ecs.0042	The number of attached data disks exceeds the maximum allowed limit.	The number of VBD volumes is %s, but KVM server supports up to 24.	Adjust the number of attached data disks.
Ecs.0043	The disk type does not exist.	volume type[%s] is not exist.	Change the disk type.
Ecs.0057	The current disk has been attached to the ECS.	the volume has already been attached to this instance and you cannot repeatedly attach.	Attach a new disk to the ECS.
Ecs.0201	Failed to create a NIC.	Failed to create port in network %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0202	Failed to create the system disk.	Failed to create volume %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0203	Failed to create the data disk.	Failed to create volume %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0204	Failed to create the ECS.	Failed to add a tag to server %s: %s.	For details, see the returned error message or contact technical support.
Ecs.0205	Failed to attach the data disk.	Failed to call the Nova API to attach volume %s to ECS %s because %s.	For details, see the returned error message or contact technical support.
Ecs.0303	Failed to query the flavor.	Failed to view flavor %s because %s.	For details, see the returned error message or contact technical support.

Error Code	Description	Error Message	Solution
Ecs.0308	Failed to query the ECS quota of the tenant.	Failed to view limits because %s.	For details, see the returned error message or contact technical support.
Ecs.0319	Insufficient flavor capacity.	check capacity: capacity is not enough.	Apply for expanding the flavor capacity.

- Step 8** If the cluster failed to be created because of the **RdsPingInstanceManagerIpTask** failure, the network between the management and tenant sides is disconnected due to VPC component exceptions. In this case, try again later. If the fault persists, contact O&M engineers.

Step 9 If **RdsInitInstanceTask** fails, run the **connectTool.sh** command to log in to the O&M container or node. For details about how to use **connectTool.sh** to connect to a cluster node, see [Logging In to a Node in the Tenant Cluster](#).

Obtain related information from the **cloud-dws-deploy** log. To do so, log in to the instance node and run the following command to switch to the log directory:

```
cd /home/Ruby/log
```

- Step 10** If the failure is caused by the monitoring failure of HAMonitor, log in to the O&M container, run the **connectTool** script to connect to the database instance, and view the **haagent.log** log [w1] of the instance. After connecting to the instance node, run the following command to switch to the haagent directory and run the **tail** command to check whether the current log contains exception information. If no exception information is found, collect the logs.

```
cd /home/Ruby/log/haagent
```

```
tail -f haagent.log
```

```
[root@host-172-16-13-137 log]# cd haagent/
[root@host-172-16-13-137 haagent]# pwd
/home/Ruby/log/haagent
[root@host-172-16-13-137 haagent]# ll
total 2248
-rw----- 1 Ruby Ruby 2298973 Jun 1 10:57 haagent.log
[root@host-172-16-13-137 haagent]# █
```

Run the following commands to log in to the Monitor container and switch to the log path:

```
kubectl get po -n ecf
```

```
kubectl exec -ti [monitor container name] -n dws bash
```

```
cd /opt/cloud/monitor/logs/
```

```
[root@10-63-90-40 ~]# kubectl get pod -n ecf
NAME                      READY   STATUS    RESTARTS   AGE
dbsevent-b9b958554-pd5gg   1/1     Running   0          47d
dbsevent-b9b958554-wn4l6   1/1     Running   0          47d
dbsinsight-7c897d7d5c-rh9ds 1/1     Running   0          46d
dbsmonitor-7bfbd6fdc-mmwr7 1/1     Running   0          35d
dbsmonitor-7bfbd6fdc-pj6zg  1/1     Running   3          48d
ecfclustermanager-75595d8d57-2rdl2 0/1     CrashLoopBackoff 11014   38d
[root@10-63-90-40 ~]# kubectl exec -ti dbsmonitor-7bfbd6fdc-mmwr7 -n ecf bash
[service@dbsmonitor-7bfbd6fdc-mmwr7 bin]$ cd /opt/cloud/monitor/logs/
```

Run the following command to check whether the Monitor process is running properly:

```
ps -ef | grep monitor
```

If the following information is displayed, the monitor process exists. Run the **tail** command to view the error log. If no error is reported, collect the log and contact O&M personnel.

```
tail -f /opt/cloud/monitor/logs/hamonitor-ecf.log
```

```
[service@dbsmonitor-7bfbd6fdc-mmwr7 bin]$ ps -ef | grep monitor
root      13  7 0 Apr26 ?    00:00:00 su service -m -c /bin/sh /opt/cloud/monitor/bin/start.sh
service    14  13 0 Apr26 ?   00:00:00 /bin/sh /opt/cloud/monitor/bin/start.sh
service    18  14 40 Apr26 ?   13-14:00:50 java -jar -DPOD_NAMESPACE=ecf -DXmx=4096m
monitor-3.0.0-SNAPSHOT.jar
service  11154 10887 0 03:47 pts/0  00:00:00 grep --color=auto monitor
```

If the following command output is displayed, the monitor process does not exist.

```
[rds@hamonitor1 logs]$ ps -ef | grep monitor
rds    116679 20241 0 05:28 pts/2  00:00:00 grep --color=auto monitor
```

Run the following commands to start the monitor process. After the startup, query whether the monitor process exists. If the process is successfully started, try again.

```
cd /opt/cloud/monitor/bin
```

```
sh start.sh
```

If the process exists, query the monitor container log and run the **tail -f /opt/cloud/monitor/logs/hamonitor-ecf.log** command to check whether any exception information is recorded during the startup."

If no exception occurs, contact technical support.

Step 11 If the exception cause cannot be found in the log, collect related log information and alarm information and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.26 DWS_20100 Cluster Deletion Exception

Alarm Description

This alarm is generated when a cluster fails to be created.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_20100	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Cluster Deletion Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The cluster cannot be deleted.

Possible Causes

1. Authentication fails because the connection to IAM times out.
2. Deletion of the underlying resources such as VPC and ECS fails.

3. Notification to CBC fails.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Obtain the IP address and the error code and error location according to **Location Info**.
- Step 3** Obtain the cluster's tenant information from **Other Information**, such as the tenant name, tenant ID, and resource tenant name.
- Step 4** Obtain the cluster name, ID, flavor, and node quantity from **Location Info**.

The following is an example of **Location Info**:

```
exception_code=Delete_Cluster_Exception, cluster_id=a61114a1-6b6d-4405-92c0-3f2a351af987,  
cluster_name=dws-dttb2018-07-04-04-test, datastore_type=dws, spec_code=dws.d2.xlarge, cluster_size=3
```

a61114a1-6b6d-4405-92c0-3f2a351af987 indicates the cluster ID.

- Step 5** Check the possible causes. If the exception occurs because the ECS, VPC, or IAM is unavailable, contact the O&M personnel of the corresponding service.

If **multiengineDeleteVMTask** fails, log in to the controller container, obtain logs, and view related information in the **ossres-dws.log** file.

If the exception cause cannot be found in the logs, collect related log information and alarm information and contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.27 DWS_2020 Failed to Update the AK and SK of the Management Tenant of an Instance

Alarm Description

After CCMS is enabled, the system updates the AK and SK of the management tenant every **10** hours. This alarm is generated when the AK and SK on an instance fail to be updated.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2020 0	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Update the AK and SK of the Management Tenant of an Instance
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

AK/SK rotation depends on the agent. Since version 8.1.3.101, the agent obtains a temporary AK/SK from CCMS during cluster creation. The AK/SK becomes invalid 48 hours later. If the AK/SK of an instance fails to be updated, the AK/SK of the instance becomes invalid. As a result, the management plane cannot communicate with the instance.

Possible Causes

The instance status changes. As a result, the communication with the instance fails.

System Actions

None

Handling Procedure

1. Log in to the ManageOne alarm platform to obtain the alarm information.
 - a. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - b. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - c. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 - d. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

2. Obtain the instance IDs from **Location Info** and **Possible Causes**. Only three instance IDs are displayed. You need to search for **publish Ak and Sk to instance total** in the controller log file **ossres-dws.log** to obtain the IDs of all failed instances.
3. Call an API on the controller container to update the instance AK/SK.

Obtain the user token. To obtain the IAM domain name, search for **iam.endpoint** on CloudAutoDeploy-CDK.

```
curl -i -s -H "Content-Type: application/json" -X POST -d'{"auth":{"identity": {"methods":["password"],"password":{"user":{"name": "Username","password": "Password","domain":{"name": "Tenant_name }}}}, "scope": {"project":{"name": "region_name"}, "domain":{"name": "Tenant_name }}}}' https://iam**/v3/auth/tokens -k --tlsv1.2
```

Obtain the token value and fill it in the **IAM_TOKEN** variable in the following request:

```
curl -i -k -v POST "https://127.0.0.1:7443/rds/v1/instances/publish-ak-sk" -H 'Content-Type:application/json' -H 'X-Language:zh-cn' -H 'Accept:application/json' -H 'X-Auth-Token:${IAM_TOKEN}' -d '{"instance_ids":["b8fda39d-d0bf-4bbb-8017-d3472c7313a0"]}'
```

This API is used to update the AK/SK of an instance again.

4. If step 3 fails, log in to the tenant cluster instance that reports the alarm, go to the **/home/Ruby** directory, and open the **InitCes.json** file. Copy the AK and SK values in the file of the instance whose AK and SK are successfully updated and use them to replace the ones of the instance whose update failed.

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

2.1.28 DWS_20210 Failed to Deliver the Operator Spill Threshold After Disk Capacity Expansion

Alarm Description

After disk scale-out is successful for DWS 8.2.0 or later, you need to modify the alarm threshold of the operator data spilling rule on a single DN. This alarm is generated when the modification fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_20210	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Deliver the Operator Spill Threshold After Disk Capacity Expansion
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

After the disk capacity is expanded, if the exception rule modification fails, the previous alarm threshold for operator data spill will be used, causing a false alarm.

Possible Causes

The delivered disk capacity parameter after scale-out is incorrect.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the instance for which the alarm is generated based on **instance_name** in the alarm location information and run the following command to switch to user **Ruby**:

su - Ruby

Access the sandbox.

ssh `hostname -i`

- Step 3** Use gsql to connect to the database and run the following command to change the alarm threshold of the operator spill rule on a DN:

ALTER EXCEPT RULE default_spillsize WITH (spillsize=*totalSpace/10*);

Example:

```
ALTER EXCEPT RULE except_rule2 WITH (spillsize=5000);
```

The value of spillsize is half of the disk capacity (MB) after scale-out.

If the primary and standby nodes use different disks for capacity expansion, the value of **spillsize** is the disk capacity (MB) after expansion.

- Step 4** Rectify the fault and try again.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.29 DWS_20220 Scale-out Failed

Alarm Description

If the cluster scale-out fails, this alarm is sent to notify SRE to ascertain the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_20220	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Scale-out Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Cluster scale-out failure may cause the cluster to be unavailable.

Possible Causes

The network is faulty, the cluster scale-out fails to pass the inspection, or the GUC parameters are improper.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Locate the failed task in the RMS database based on the jobId in the alarm location information.
- Step 3** Log in to the tenant node and locate the root cause based on the log information.
- Step 4** Rectify the fault and try again.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.30 DWS_20221 Scheduling Task Failed After Resizing a Cluster

Alarm Description

After the resizing is successful or fails, a scheduled task is executed to clear the data after a period of time. This alarm is generated when the task fails to be executed.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_20221	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Scheduling Task Failed After Resizing a Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the scheduling fails, node resources may not be released.

Possible Causes

The network is faulty, the backup fails, the token becomes invalid due to tenant changes, or a dependent service is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the cluster ID from the alarm location information.

Step 3 Query the failed step in the **dws_cluster_resize_status** table based on the cluster ID.

Step 4 Locate the root cause based on logs, change the status of the **dws_cluster_resize_status** table, and try again.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

Table 2-8 Related Information

status	Description
0	Initializing
1	Backing up
2	Backed up

status	Description
3	Waiting for reservation period
5	Reservation period expired
6	Deleting the old node
7	Waiting for rollback (rollback after resizing failure)
8	Rolling back
20	Denotes success
21	Backup failed
23	Deletion failed
24	Rollback failed
25	Unknown error

2.1.31 DWS_21110 GaussDB(DWS) Data Migration Task Status Abnormal

Alarm Description

This alarm is generated when the data migration task process exits unexpectedly.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_21110	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	GaussDB(DWS) Data Migration Task Status Abnormal
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The data migration service created by the user is interrupted.

Possible Causes

The data migration application Gds-Kafka exits abnormally.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In **Location Info** and **Possible Causes**, obtain the cluster ID, cluster name, job ID, job name, and tenant information.

Step 3 In the instance list on the **Data Migration > Instances** page, locate the instance for which the alarm is generated and click **Manage Jobs** in the **Operation** column. Select the abnormal job task in the alarm information and click **Start** to restart the job task.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.32 DWS_22001 GaussDB(DWS) Audit Log Dump Exception

Alarm Description

After the log dump function is enabled in security settings, this alarm is generated when an exception occurs during periodic log dump.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_22001	Management plane alarm	Minor	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	An exception occurs when GaussDB (DWS) audit logs are dumped.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceld and domain_id.

Impact on the System

Database operation logs cannot be dumped to OBS in a timely manner. If you try again or dump logs again after the fault is rectified, the original logs can be saved to OBS without affecting cluster services.

Possible Causes

1. The network between the management side and tenant side is disconnected.
2. The network between the tenant side and OBS is disconnected.
3. The OBS is faulty.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the error code and error location according to **Location Info**.

Step 3 Obtain the cluster's tenant information from **Other Information**, such as the tenant name, tenant ID, and resource tenant name.

Step 4 Obtain the cluster name, ID, flavor, and node quantity from **Location Info**.

The following is an example of **Location Info**:

```
cluster_id=94a1ad37-1bde-4919-8e93-712577a9c3b2, cluster_name=dws_noss1_4autotest_nomodify,  
datastore_type=dws3.0, spec_code=dwsx3.4U16G.4DPU, cluster_size=3
```

In the preceding information, 94a1ad37-1bde-4919-8e93-712577a9c3b2 indicates the cluster ID.

Step 5 Locate the fault based on the error code and error information in the log. The procedure is as follows:

1. Run the following commands to log in to the database node and connect to the **rms** database:

Floating IP address of the **mysql -h** database VM -**P7306 -u** database user;

Enter the user password as prompted and run the following command to switch to the rms database:

```
use rms;
```

2. Run the following command in the database to obtain the status of the log dump task in the cluster:

```
select job_id, job_def_name, execution_status, begin_time, server_hostname from taskmgr_job where  
job_def_name='dumpAuditLogJob' and request like '%{ cluster ID }%';
```

3. Run the following command to log in to the dwscontroller container and switch to the log path:

```
cd /opt/cloud/3rdComponent/tomcat/logs
```

Run the following command to filter the **ossres-dws.log** log:

Failed job_id value obtained in **grep " 5.2 "ossres-dws.log**

Collect log information according to **First Occurred At**. For details, see [Querying Logs Based on the Alarm Generation Time](#).

Step 6 The ID of the instance where the error is reported is displayed in the log. Log in to the instance based on the instance ID and view the **logStorageOBS.log** file to locate the error cause.

Step 7 If the exception cause cannot be found in the log, collect related log information and alarm information and contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.33 DWS_23001 Inconsistent Resource (Abnormal Cluster) Status

Alarm Description

This alarm is triggered during check of the consistency between the resource and charging status. The trigger conditions are as follows:

```
rds_cluster.status in ('100', '300', '302', '303', '304', '400', '500', '800', '900', '910', '920') rds_resource.isBilling = 1
```

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_23001	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Inconsistent Resource (Abnormal Cluster) Status
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The **rds_cluster.status** and **rds_resource.isBilling** attributes are mandatory for SDR accounting, which may affect SDR accounting result. You are advised to rectify the fault in a timely manner.

Possible Causes

1. Defects of the service feature module: After the cluster resource status **rds_cluster.status** is modified, the status parameter in billing **rds_resource.isBilling** is not modified synchronously, or is incorrectly modified. The status change includes deleting, expanding, and adding nodes.
2. Defects of the status monitoring module: The cluster/node monitoring status module of the monitor component does not update the cluster resource status **rds_cluster.status** and cluster resource billing status **rds_resource.isBilling** synchronously.
3. Unauthorized modification of cluster information: O&M personnel directly change the database cluster status **rds_cluster.status** but do not change the resource billing status **rds_resource.isBilling**.
4. The cluster resource status **rds_cluster.status** is inconsistent with the cluster resource billing status **rds_resource.isBilling**, and the difference between the last modification time **rds_resource.updateAt** and the current time (UTC time) is greater than 1 hour.

Handling Procedure

Step 1 Log in to the dws-controller database in the region where the alarm is reported and query the resource information of the alarm. In the query command, **\${timestamp}** is the value of timestamp in the additional alarm information.

1. Query and check the details of the resource (abnormal cluster) for which the alarm is reported.

```
select tbl_cluster.id as id, tbl_cluster.name as name, tbl_cluster.status as status, 
tbl_cluster.namespace as namespace, tbl_cluster.datastoreType as datastoreType, 
tbl_cluster.datastoreVersion as datastoreVersion, tbl_tenant.realDomainName as tenant, 
tbl_instance.id as instanceId, tbl_instance.name as instanceName, tbl_instance.status as 
instanceStatus, tbl_resource.id as resource, tbl_resource.tag as tag, tbl_resource.isBilling as 
billing, tbl_resource.updateAt as updated from rds_cluster tbl_cluster join rds_instance tbl_instance 
on tbl_cluster.id = tbl_instance.clusterId join rds_resource tbl_resource on tbl_instance.id = 
tbl_resource.instId join rds_restanttbl_tenant on tbl_cluster.tenantId =tbl_tenant.realDomainId 
where tbl_cluster.status in ('100', '300', '302', '303', '304', '400', '500', '800', '900', '910', '920') and 
tbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') andtbl_resource.isBilling = 1 and 
(tbl_resource.updateAt <= ${timestamp} ortbl_resource.updateAt is null);
```

2. Query and check the total number of resources (abnormal clusters) for which the alarm is generated.

```
select count(tbl_resource.id) from rds_clustertbl_cluster join rds_instancetbl_instance on 
tbl_cluster.id =tbl_instance.clusterId join rds_resourcetbl_resource ontbl_instance.id = 
tbl_resource.instId join rds_restanttbl_tenant ontbl_cluster.tenantId =tbl_tenant.realDomainId 
wheretbl_cluster.status in ('100', '300', '302', '303', '304', '400', '500', '800', '900', '910', '920') and 
tbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') andtbl_resource.isBilling = 1 and 
(tbl_resource.updateAt <= ${timestamp} ortbl_resource.updateAt is null);
```

Step 2 Create a backup table to back up information about abnormal resources for audit and check. The format of **\${datetime}** is yyyyMMddHHmmss. For example: 20221127103045. Ensure that the target table to be created does not exist. If the target table exists, rename it with the timestamp.

```
create table rds_resource_alarm_23001_${datetime} as selecttbl_resource.* from rds_clustertbl_cluster join 
rds_instancetbl_instance ontbl_cluster.id =tbl_instance.clusterId join rds_resourcetbl_resource on 
tbl_instance.id =tbl_resource.instId join rds_restanttbl_tenant ontbl_cluster.tenantId = 
tbl_tenant.realDomainId wheretbl_cluster.status in ('100', '300', '302', '303', '304', '400', '500', '800', '900', 
'910', '920') andtbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') andtbl_resource.isBilling = 1 and 
(tbl_resource.updateAt <= ${timestamp} ortbl_resource.updateAt is null);
```

Step 3 Change the abnormal status **rds_resource.isBilling** to be the same as the cluster status. The variable **\${datetime}** is the name of the backup table created in [Step 2](#).

```
update rds_resource set isBilling = 0  
where id in (select id from rds_resource_alarm_23001_${datetime})  
and isBilling = 1;
```

Step 4 Confirm and clear current alarms.

----End

Alarm Clearance

After the fault is rectified, clear the alarm in NMS alarm clearance mode.

Related Information

None

2.1.34 DWS_23002 Inconsistent Resource (Normal Node) Status

Alarm Description

This alarm is triggered during check of the consistency between the resource and charging status. The trigger conditions are as follows:

```
rds_cluster.status in ('150', '200') rds_instance.status in ('199', '200') rds_resource.isBilling = 0
```

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_23002	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Inconsistent Resource (Normal Node) Status
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The **rds_cluster.status** and **rds_resource.isBilling** attributes are mandatory for SDR accounting, which may affect SDR accounting result. You are advised to rectify the fault in a timely manner.

Possible Causes

1. Defects of the service feature module: After the cluster resource status **rds_cluster.status** is modified, the status parameter in billing **rds_resource.isBilling** is not modified synchronously, or is incorrectly modified. The status change includes deleting, expanding, and adding nodes.
2. Defects of the status monitoring module: The cluster/node monitoring status module of the monitor component does not update the cluster resource status **rds_cluster.status** and cluster resource billing status **rds_resource.isBilling** synchronously.
3. Unauthorized modification of cluster information: O&M personnel directly change the database cluster status **rds_cluster.status** but do not change the resource billing status **rds_resource.isBilling**.
4. The cluster resource status **rds_cluster.status** is inconsistent with the cluster resource billing status **rds_resource.isBilling**, and the difference between the last modification time **rds_resource.updateAt** and the current time (UTC time) is greater than 1 hour.

Handling Procedure

Step 1 Log in to the dws-controller database in the region where the alarm is reported and query the resource information of the alarm. In the query command, **\${timestamp}** is the value of timestamp in the additional alarm information.

1. Query and check the details of the resource (normal node) for which the alarm is generated:

```
select tbl_cluster.id as id, tbl_cluster.name as name, tbl_cluster.status as status,
tbl_cluster.namespace as namespace, tbl_cluster.datastoreType as datastoreType,
tbl_cluster.datastoreVersion as datastoreVersion, tbl_tenant.realDomainName as tenant,
tbl_instance.id as instanceId, tbl_instance.name as instanceName, tbl_instance.status as
instanceStatus, tbl_resource.id as resource, tbl_resource.tag as tag, tbl_resource.isBilling as
billing, tbl_resource.updateAt as updated from rds_cluster tbl_cluster join rds_instance tbl_instance
on tbl_cluster.id = tbl_instance.clusterId join rds_resource tbl_resource on tbl_instance.id =
tbl_resource.instanceId join rds_restantant tbl_tenant on tbl_cluster.tenantId = tbl_tenant.realDomainId
where tbl_cluster.status in ('150', '200') and tbl_instance.status in ('199', '200') and
tbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') and tbl_resource.isBilling = 0 and
(tbl_resource.updateAt <= ${timestamp} or tbl_resource.updateAt is null);
```

2. Query and check the total number of resources (normal nodes) for which the alarm is generated:

```
select count(tbl_resource.id) from rds_cluster tbl_cluster join rds_instance tbl_instance on
tbl_cluster.id = tbl_instance.clusterId join rds_resource tbl_resource on tbl_instance.id =
tbl_resource.instanceId join rds_restantant tbl_tenant on tbl_cluster.tenantId = tbl_tenant.realDomainId
where tbl_cluster.status in ('150', '200') and tbl_instance.status in ('199', '200') and
tbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') and tbl_resource.isBilling = 0 and
(tbl_resource.updateAt <= ${timestamp} or tbl_resource.updateAt is null);
```

Step 2 Create a backup table to record the dirty data that triggers the alarm and use the table as the baseline for clearing dirty data in the **rds_resource** table. When you create a table, if the table already exists, the creation command is automatically ignored.

```
CREATE TABLE IF NOT EXISTS `rds_resource_alarm_backup` ( `alarm_id` varchar(64) NOT NULL,
`backup_time` datetime NOT NULL, `expired` varchar(32) NOT NULL, `id` varchar(64) NOT NULL, `hostId`
```

```
varchar(64) DEFAULT NULL, `volumeId` varchar(64) DEFAULT NULL, `physicalVolume` bigint(20) DEFAULT NULL, `application` varchar(64) DEFAULT NULL, `comment` longtext, `createAt` datetime DEFAULT NULL, `device` varchar(64) DEFAULT NULL, `endAt` datetime DEFAULT NULL, `extendFields` longtext, `instId` varchar(64) DEFAULT NULL, `isBilling` int(11) DEFAULT NULL, `orderId` varchar(255) DEFAULT NULL, `payModel` int(11) DEFAULT NULL, `period` int(11) DEFAULT NULL, `resType` varchar(64) DEFAULT NULL, `resModel` varchar(32) DEFAULT NULL, `dssPoolId` varchar(64) DEFAULT NULL, `shareable` int(11) DEFAULT NULL, `size` bigint(20) DEFAULT NULL, `specId` varchar(64) DEFAULT NULL, `tag` varchar(64) DEFAULT NULL, `updateAt` datetime DEFAULT NULL, `volumeUUID` varchar(64) DEFAULT NULL, `mountDir` varchar(64) DEFAULT NULL ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Step 3 Change the value of **expired** to **yes** for all historical data in the backup table.

```
update rds_resource_alarm_backup set expired = 'yes';
```

Step 4 Back up the dirty data in the **rds_resource** table that triggers the alarm. In the command, **\${timestamp}** is the value of timestamp in the additional alarm information.

```
insert into rds_resource_alarm_backup (alarm_id, backup_time, expired, id, hostId, volumeId, physicalVolume, application, comment, createAt, device, endAt, extendFields, instId, isBilling, orderId, payModel, period, resType, resModel, dssPoolId, shareable, size, specId, tag, updateAt, volumeUUID, mountDir) select '23002' as alarm_id, now() as backup_time, 'no' as expired, tbl_resource.id as id, tbl_resource.hostId as hostId, tbl_resource.volumeId as volumeId, tbl_resource.physicalVolume as physicalVolume, tbl_resource.application as application, tbl_resource.comment as comment, tbl_resource.createAt as createAt, tbl_resource.device as device, tbl_resource.endAt as endAt, tbl_resource.extendFields as extendFields, tbl_resource.instId as instId, tbl_resource.isBilling as isBilling, tbl_resource.orderId as orderId, tbl_resource.payModel as payModel, tbl_resource.period as period, tbl_resource.resType as resType, tbl_resource.resModel as resModel, tbl_resource.dssPoolId as dssPoolId, tbl_resource.shareable as shareable, tbl_resource.size as size, tbl_resource.specId as specId, tbl_resource.tag as tag, tbl_resource.updateAt as updateAt, tbl_resource.volumeUUID as volumeUUID, tbl_resource.mountDir as mountDir from rds_cluster tbl_cluster join rds_instance tbl_instance on tbl_cluster.id = tbl_instance.clusterId join rds_resource tbl_resource on tbl_instance.id = tbl_resource.instId join rds_restant tenant on tbl_cluster.tenantId = tenant.realDomainId where tbl_cluster.status in ('150', '200') and tbl_instance.status in ('199', '200') and tbl_cluster.datastoreType in ('dws', 'hybrid', 'stream') and tbl_resource.isBilling = 0 and (tbl_resource.updateAt <= ${timestamp} or tbl_resource.updateAt is null);
```

Step 5 Modify the abnormal status **rds_resource.isBilling**.

```
update rds_resource set isBilling = 1  
where id in (select id from rds_resource_alarm_backup where alarm_id = '23002' and expired = 'no')  
and isBilling = 0;
```

Step 6 Change **expired** to **yes** for all used data in the backup table.

```
update rds_resource_alarm_backup set expired = 'yes';
```

Step 7 Clear current alarms on the alarm platform.

----End

Alarm Clearance

After the fault is rectified, clear the alarm in NMS alarm clearance mode.

Related Information

None

2.1.35 DWS_23003 Inconsistent Resource (Abnormal Node) Status

Alarm Description

This alarm is triggered during check of the consistency between the resource and charging status. The trigger conditions are as follows:

```
rds_cluster.status in ('150', '200') rds_instance.status in ('100', '110', '300', '301', '302', '303', '304', '305', '400',  
'500', '600', '700', '701', '900') rds_resource.isBilling = 1
```

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_23003	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Inconsistent Resource (Abnormal Node) Status
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The **rds_cluster.status** and **rds_resource.isBilling** attributes are mandatory for SDR accounting, which may affect SDR accounting result. You are advised to rectify the fault in a timely manner.

Possible Causes

1. Defects of the service feature module: After the cluster resource status **rds_cluster.status** is modified, the status parameter in billing **rds_resource.isBilling** is not modified synchronously, or is incorrectly modified. The status change includes deleting, expanding, and adding nodes.
2. Defects of the status monitoring module: The cluster/node monitoring status module of the monitor component does not update the cluster resource status **rds_cluster.status** and cluster resource billing status **rds_resource.isBilling** synchronously.
3. Unauthorized modification of cluster information: O&M personnel directly change the database cluster status **rds_cluster.status** but do not change the resource billing status **rds_resource.isBilling**.
4. The cluster resource status **rds_cluster.status** is inconsistent with the cluster resource billing status **rds_resource.isBilling**, and the difference between the last modification time **rds_resource.updateAt** and the current time (UTC time) is greater than 1 hour.

Handling Procedure

Step 1 Log in to the dws-controller database in the region where the alarm is reported and query the resource information of the alarm. In the query command, **\${timestamp}** is the value of timestamp in the additional alarm information.

1. Query and check the details of the resource (abnormal cluster) for which the alarm is reported.

```
select tbl_cluster.id as id, tbl_cluster.name as name, tbl_cluster.status as status,
tbl_cluster.namespace as namespace, tbl_cluster.datastoreType as datastoreType,
tbl_cluster.datastoreVersion as datastoreVersion, tbl_tenant.realDomainName as tenant,
tbl_instance.id as instanceId, tbl_instance.name as instanceName, tbl_instance.status as
instanceStatus, tbl_resource.id as resource, tbl_resource.tag as tag, tbl_resource.isBilling as
billing, tbl_resource.updateAt as updated from rds_cluster tbl_cluster join rds_instance tbl_instance
on tbl_cluster.id = tbl_instance.clusterId join rds_resource tbl_resource on tbl_instance.id =
tbl_resource.instanceId join rds_restant(tbl_tenant on tbl_cluster.tenantId =tbl_tenant.realDomainId
where tbl_cluster.status in ('150', '200') and tbl_instance.status in ('100', '110', '300', '301', '302', '303',
'304', '305', '400', '500', '600', '700', '701', '900') and tbl_cluster.datastoreType in ('dws', 'hybrid',
'stream') and tbl_resource.isBilling = 1 and (tbl_resource.updateAt <= ${timestamp} or
tbl_resource.updateAt is null);
```

2. Query and check the total number of resources (abnormal clusters) for which the alarm is generated.

```
select count(tbl_resource.id) from rds_cluster tbl_cluster join rds_instance tbl_instance on
tbl_cluster.id =tbl_instance.clusterId join rds_resource tbl_resource ontbl_instance.id =
tbl_resource.instanceId join rds_restant(tbl_tenant ontbl_cluster.tenantId =tbl_tenant.realDomainId
wheretbl_cluster.status in ('150', '200') andtbl_instance.status in ('100', '110', '300', '301', '302', '303',
'304', '305', '400', '500', '600', '700', '701', '900') andtbl_cluster.datastoreType in ('dws', 'hybrid',
'stream') andtbl_resource.isBilling = 1 and (tbl_resource.updateAt <= ${timestamp} or
tbl_resource.updateAt is null);
```

Step 2 Create a backup table to back up information about abnormal resources for audit and check. The format of **\${datetime}** is yyyyMMddHHmmss. For example: 20221127103045. Ensure that the target table to be created does not exist. If the target table exists, rename it with the timestamp.

```
create table rds_resource_alarm_23003_${datetime} as select *from rds_clustertbl_cluster join
rds_instancetbl_instance ontbl_cluster.id =tbl_instance.clusterId join rds_resourcetbl_resource on
tbl_instance.id =tbl_resource.instanceId join rds_restanttbl_tenant ontbl_cluster.tenantId =
tbl_tenant.realDomainId wheretbl_cluster.status in ('150', '200') andtbl_instance.status in ('100', '110',
'300', '301', '302', '303', '304', '305', '400', '500', '600', '700', '701', '900') andtbl_cluster.datastoreType in
('dws', 'hybrid', 'stream') andtbl_resource.isBilling = 1 and (tbl_resource.updateAt <= ${timestamp} or
tbl_resource.updateAt is null);
```

Step 3 Change the abnormal status **rds_resource.isBilling** to be the same as the cluster status. The variable **\${datetime}** is the name of the backup table created in [Step 2](#).

```
update rds_resource set isBilling = 0
where id in (select id from rds_resource_alarm_23003_${datetime})
and isBilling = 1;
```

Step 4 Confirm and clear current alarms.

----End

Alarm Clearance

After the fault is rectified, clear the alarm in NMS alarm clearance mode.

Related Information

None

2.1.36 DWS_23052 GaussDB(DWS) Resource Tenant Bucket Freezing/Unfreezing Exception

Alarm Description

This alarm is generated when a bucket is frozen due to arrears or fails to be frozen or unfrozen.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_23052	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	The bucket of the GaussDB (DWS) resource tenant fails to be frozen or unfrozen.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Bucket ID.	Bucket ID and tenant project ID.

Impact on the System

- If the resource fails to be frozen, the user can continue to use the resource.
- If the bucket fails to be unfrozen, the user cannot use bucket resources properly.
- If the frozen resource fails to be deleted, the user can still use the resource, but the fee is borne by GaussDB (DWS).

Possible Causes

Frozen: Failed to invoke OBS to delete the bucket policy.

Failed to stop the OMS migration task.

Unfreezing: Failed to invoke OBS to set the bucket policy.

Frozen deletion: Failed to invoke OBS to delete the bucket.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In Location Information and Additional Information, you can obtain the bucket ID, resource tenant ID, and bucket name (which vary depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the bucket ID, resource tenant ID, and bucket name from Location Information and Additional Information.

Step 2 Check whether the location information in the alarm information contains OBS error information. If yes, the OBS API fails to be called to set the bucket policy or delete the bucket. Log in to the background and view Controller logs.

Obtain detailed log information and contact OBS engineers to locate the fault.

Step 3 For other error information, log in to the background and obtain the tenant ID or bucket ID based on the location information. For details to obtain detailed controller logs. Then, contact O M engineers for assistance.

----End

Alarm Clearance

You need to manually clear the alarm after the fault is rectified.

Related Information

None

2.1.37 DWS_23053 GaussDB(DWS) Resource Tenant Bucket Usage Synchronization Exception

Alarm Description

OBS bucket management periodically synchronizes charging information to obs_tablespace. This alarm is generated when the synchronization fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_23053	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	GaussDB (DWS) Resource Tenant Bucket Usage Synchronization Exception
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Bucket ID.	Detailed information about the bucket ID, bucket name, and resource tenant ID.

Impact on the System

Resource tenants or buckets that fail to be synchronized cannot be charged.

Possible Causes

The OBS system is abnormal. As a result, the bucket capacity cannot be queried.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In Location Information and Additional Information, you can obtain the bucket ID, resource tenant ID, and bucket name (which vary depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the bucket ID, resource tenant ID, and bucket name from Location Information and Additional Information.

Step 2 Check whether the location information in the alarm information contains OBS error information. If yes, an error is reported when the OBS API is called to obtain the bucket capacity. Log in to the background and view Controller logs.

Obtain detailed log information and contact OBS engineers to locate the fault.

Step 3 For other error information, log in to the background and obtain the tenant ID or bucket ID based on the location information. For details to obtain detailed controller logs. Then, contact O M engineers for assistance.

----End

Alarm Clearance

You need to manually clear the alarm after the fault is rectified.

Related Information

None

2.1.38 DWS_24001 Root Directory of the System Disk in the GaussDB(DWS) Cluster Is Not Automatically Expanded

Alarm Description

This alarm is generated when the root directory of the system disk in a data warehouse cluster is not expanded to the bare metal server flavor.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_24001	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Root Directory of the System Disk in the GaussDB(DWS) Cluster Is Not Automatically Expanded
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The root directory is not automatically expanded, which may affect the use of the cluster.

Possible Causes

The **Cloud-Init** plug-in is faulty. As a result, the system disk of the BMS instance is not automatically expanded.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the values of **instance_id** and **instance_name** from the alarm location information.

Step 3 Log in to the current instance and run the **lsblk** command to check whether the root directory is not expanded. As shown in the following figure, the total capacity of system disk **vda** is 850 GB, 50 GB is used by **vda1** and **vda2**, and 800 GB is idle.

```
[root@host-172-16-6-198 Mike]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda    253:0    0  850G  0 disk 
| -vda1 253:1    0    1G  0 part /boot/efi
`-vda2 253:2    0    49G  0 part /
vdb    253:16   0  100G  0 disk /var/chroot/DWS/data2
vdc    253:32   0  100G  0 disk /var/chroot/DWS/data1
vdd    253:48   0  105G  0 disk /var/chroot/DWS/manager
[root@host-172-16-6-198 Mike]#
```

Step 4 Run the **partprobe -s** command as the root user to update the system partition information.

```
[root@host-172-16-6-198 Mike]# partprobe -s
/dev/vdd: loop partitions 1
/dev/vdb: loop partitions 1
/dev/vdc: loop partitions 1
```

- Step 5** Run the **lsblk** command to check whether the root directory of the system disk has been expanded from 49 GB to 849 GB.

```
[root@host-172-16-6-198 Mike]# lsblk
NAME   MAJ:MIN RM  SIZE R0 TYPE MOUNTPOINT
vda    253:0    0  850G  0 disk
| -vda1 253:1    0    1G  0 part /boot/efi
` -vda2 253:2    0  849G  0 part /
vdb    253:16   0  110G  0 disk /var/chroot/DWS/data2
vdc    253:32   0  100G  0 disk /var/chroot/DWS/data1
vdd    253:48   0  105G  0 disk /var/chroot/DWS/manager
```

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.39 DWS_30000 GaussDB(DWS) License Is About to Exceed the Threshold

Description

The DWS license usage threshold can be configured in ManageOne. This alarm is generated when the usage exceeds the threshold.

Attribute

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_30000	Management plane alarm	Warning	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	GaussDB(DWS) License Is About to Exceed the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The usage of a license control item has reached the configured threshold, which has no impact so far. If the usage exceeds the threshold, cluster creation and scaling functions will be restricted.

Possible Causes

The license usage exceeds the threshold.

Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **License_Capacity_Exceeded_Threshold**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click  in the row of the alarm to view the alarm details. You can obtain the BBOM code of the license control item that triggers the alarm from the alarm location information.

Step 2 View the alarm information and record the alarm generation time. Obtain the BBOM code of the license control item from the alarm location information.

Example of alarm location information:

The following license control items whose usage exceeds the threshold exist:
Item Name|Item Code|Unit|Region|System|Used|Total|Alarm Threshold:
DWS,Data Warehouse Service, License,per vCPU|HCSEIBDDWSVU|vCPU|cn-global-3|DWS|12|18|60.0%

HCSEIBDDWSV indicates the BBOM code of the license control item.

Step 3 Log in to the ManageOne license management page and check the alarm thresholds of the license control item.

1. Log in to ManageOne Maintenance Portal and choose **System > System Settings > License Management**.
2. Choose **Control Items > Products and Cloud Services**. Check the usage and threshold of the control item of DWS.
3. To clear the alarm, modify the alarm threshold or import a new license file.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.40 DWS_30001 DWS License Exceeded Authorized Capacity

Description

This alarm is generated when the DWS license usage exceeds 120% of the authorized capacity.

Attribute

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_30001	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	The number of DWS licenses exceeds the authorized number.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the usage of the current license control item exceeds 120% of the authorized capacity, the cluster creation, repair, and capacity expansion functions will be restricted.

Possible Causes

The license usage exceeds the upper limit.

Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **License_Capacity_Exceeded_Alarm**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click  in the row of the alarm to view the alarm details. You can obtain the BBOM code of the license control item that triggers the alarm from the alarm location information.

Step 2 View the alarm information and record the alarm generation time. Obtain the BBOM code of the license control item from the alarm location information.

Example of alarm location information:

ManageOne has the following license control items:Item Name|Item Code|Unit|Region|System|Used|Total:
Cloud Service Configuration,Data Warehouse Service-per Year-per vCPU|HCSEIBDDWSV|vCPU|cn-global-2|
DWS|48|20

HCSEIBDDWSV indicates the BBOM code of the license control item.

Step 3 Log in to the ManageOne license management page and check the alarm thresholds of the license control item.

1. Log in to ManageOne Maintenance Portal and choose **System > System Settings > License Management**.
2. Choose **Control Items > Products and Cloud Services**. Check the usage of the control item of DWS.
3. To clear the alarm, import a new authorized license.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.41 DWS_30002 DWS License Charging Item Is Used but Not Registered

Alarm Description

This alarm is generated when the DWS license billing item is used but the corresponding billing item is not imported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_3000 2	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	The DWS license billing item is used but not registered.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Detailed information such as the used but unregistered billing item type and used amount.

Impact on the System

After the trial period of the current license billing item expires, creating, repairing, and expanding clusters, and enabling GUC parameters will be restricted.

Possible Causes

The license is registered, but the charging item is not imported.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set Operator to contains, set Value to used but do not register, used, click OK, and click OK again to filter DWS alarms.
4. Click  on the left of the row that contains the alarm to view the alarm details. In Additional Information, obtain the BBOM code of the license control item for which the alarm is generated. For example, in license item [item] used but do not register, used: 100, [item] is the charging item that is used but not imported.

Step 2 Log in to the ManageOne license management page and view the license control items.

1. Log in to ManageOne Maintenance Portal and choose **System > System Settings > License Management**.
2. Select the corresponding product mode or cloud service mode.
3. Import related billing items.

----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

2.1.42 DWS_4100 Failed to Scale In a GaussDB(DWS) Physical Cluster

Alarm Description

This alarm is generated when the scale-in of a physical cluster fails to be performed. This alarm is used to notify SRE of the root cause of the scale-in failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_4100 0	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Scale In a GaussDB(DWS) Physical Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceld and domain_id.

Impact on the System

The cluster may be unavailable.

Possible Causes

The network is faulty, the lock wait times out (services are being executed), or the disk space is insufficient during scale-in redistribution.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the first CN based on the cluster name in the alarm location information, view logs outside the sandbox, and view the **/home/Ruby/log/clusterShrink.log** file to check the scale-in status.

Step 3 View the **gs_shrink** and **gd_redis** logs to locate the root cause.

gs_shrink log path: **\$GAUSSLOG/om/**

gs_redis log path: **\$GAUSSLOG/bin/gs_redis/**

Step 4 After the fault is rectified, click retry scale-in on the console page.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.43 DWS_41001 Fine-grained Restoration Failed

Alarm Description

This alarm is generated when the fine-grained snapshot restoration of a cluster fails to be performed. This alarm is used to notify SRE to confirm the root cause of the failure.

The cluster task status is **Restoration failed**.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_41001	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Fine-grained Restoration Failed
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The fine-grained restoration of the cluster fails, and the tables selected by the customer cannot be restored.

Possible Causes

The backup file is damaged, the disk space is insufficient, the network is faulty, or the backup media is faulty.

Handling Procedure

Step 1 Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

1. Log in to the **rms** database and obtain the first instance node.
`select name from rds_instance where clusterId = 'xxx';`

2. Log in to the node.

```
kubectl get pod -n dws-maintain  
kubectlexec -it dwsmaintaintool-xxxx bash -n dws-maintain  
cd opsTool/  
sh connectTool.sh -uroot -drms -h192.168.1.1 -p3306 -n instance_name -tStandalone  
su - Ruby
```

3. View instance logs and Roach logs.

Instance log path: /home/Ruby/log/fine_grained_backup_restore.log

Roach log path: /var/chroot/DWS/manager/backup/log

4. Rectify the fault based on the logs.

The causes of fine-grained restoration failures are complex. If the SRE cannot locate the causes, contact R&D engineers.

----End

Alarm Clearance

The alarm will be automatically cleared after stopping fine-grained restoration or rectifying the fault.

Related Information

None

2.1.44 DWS_41002 Failed to Restore a Snapshot to the Original Cluster

Alarm Description

This alarm is generated when fine-grained snapshot restoration fails in a cluster to notify SRE to confirm the root cause of the failure. The cluster task status on the page shows that the restoration fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_41002	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Restore a Snapshot to the Original Cluster
	Type	Operation alarm

Type	Parameter	Description
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Failed Restore a snapshot to the original cluster. The cluster may be unavailable.

Possible Causes

The backup file is damaged, the disk space is insufficient, the network is faulty, or the backup media is faulty.

Handling Procedure

Step 1 Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

1. Log in to the rms database and obtain the first instance node.
`select name from rds_instance where clusterId = 'xxx';`

2. Log in to the instance node.

```
kubectl get pod -n dws-maintain  
kubectl exec -it dwsmaintaintool-xxxx bash -n dws-maintain  
cd opsTool/  
sh connectTool.sh -uroot -drms -h 192.168.1.1 -p3306 -n instance_name -tStandalone  
su - Ruby
```

3. View instance logs and Roach logs.

Instance log path: **/home/Ruby/log/inplaceRestore.log**

Roach log path: **/var/chroot/DWS/manager/backup/log**

4. Rectify the fault based on the logs.

The causes of fine-grained restoration failures are complex. If the SRE cannot locate the causes, contact R&D engineers.

----End

Alarm Clearance

The alarm will be automatically cleared after stopping fine-grained restoration or rectifying the fault.

Related Information

None

2.1.45 DWS_50000 Failed to Change Cluster Specifications

Alarm Description

This alarm is generated when the specifications of a cluster fail to be changed.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_50000	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Change Cluster Specifications
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The cluster may be unavailable.

Possible Causes

The memory and number of CPUs in the flavor do not meet the requirements.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Query the task information in the database corresponding to the dwscontroller microservice on the management plane based on the cluster ID in the alarm location information.

Query the task information in the **taskmgr_job** and **taskmgr_task** tables to check which task fails.

Task Name	Task name	Description
dwsStopClusterJob	dwsStopClusterTask	A job
dwsInstanceSpecResizeJob	dwsWaitClusterStopTask dwsShutDownServerTask dwsInstanceFlavorResizeTask dwsStartServerTask	The number of jobs is the same as the number of nodes.
dwsSpecResizeConfigGUCJob	dwsWaitSpecResizeJobTask dwsConfigureGUCTask dwsStartClusterTask	A job

Step 3 Check the failed job or task and locate the failure cause.

Failed Task	Possible Cause	Handling Method
Stopping the cluster	Cluster status exception	Log in to the node and run the cm_ctl query -Cvd command to check the cluster status.
Changing ECS specifications	1. If the ECS resource specifications are insufficient, error code ECS.0207 is displayed. 2. The ECS service fails to invoke the specification change interface, and the RestClient request failure is recorded in the log. 3. For other causes, locate the fault based on logs.	View the pod logs and contact R&D engineers to locate the fault. If some nodes are successfully changed, submit the task again and try again.
Configuring GUC	The cluster status or network is abnormal.	Log in to the tenant node and view dws_spec_resize.log .
Starting a cluster	The cluster status is abnormal.	Log in to the node and run the cm_ctl query -Cvd command to check the cluster status.

Step 4 After the fault is rectified, contact the customer to modify the specifications again.

----End

Alarm Clearance

Manually clear the alarm after the fault is rectified.

Related Information

None

2.1.46 DWS_6000 Failed to Create DR

Alarm Description

This alarm is generated when a DR fails to be created in a cluster to notify SRE to confirm the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_6000 0	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Create DR
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

None

Possible Causes

The network is faulty.

Handling Procedure

Cross-AZ DR:

- Step 1** Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: /home/Ruby/log/disaster_recovery.log outside the sandbox

----End

Cross-region DR:

- Step 1** Check whether the Direct Connect is implemented and normal between the two regions.

- Step 2** Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

- Step 3** Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'**.

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: /home/Ruby/log/disaster_recovery.log outside the sandbox

----End

Alarm Clearance

The alarm can be cleared after the DR creation is stopped or the fault is rectified.

Related Information

None

2.1.47 DWS_60001 Failed to Start DR

Alarm Description

This alarm is generated when DR fails to be started in the cluster to notify the SRE to confirm the root cause of the DR startup failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_6000 1	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to start DR
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The standby cluster is unavailable.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

Step 1 Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

Step 1 Check whether the Direct Connect is implemented and normal between the two regions.

Step 2 Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

Step 3 Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privateip from rds_instance where id = 'instance ID'.**

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.
- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log** outside the sandbox

----End

Alarm Clearance

The alarm is cleared after the DR is stopped or the fault is rectified.

Related Information

None

2.1.48 DWS_60002 Failed to Stop DR

Alarm Description

This alarm is generated when DR fails to be stopped in the cluster to instruct SRE to confirm the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60002	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Stop DR
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The standby cluster is unavailable.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

- Step 1** Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

- Step 1** Check whether the Direct Connect is implemented and normal between the two regions.

- Step 2** Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

- Step 3** Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'.**

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Alarm Clearance

The alarm is cleared after the DR is stopped or the fault is rectified.

Related Information

None

2.1.49 DWS_60003 Failed to Switch to the DR Cluster

Alarm Description

When the DR switchover fails, the cluster sends this alarm to notify the SRE to confirm the root cause of the DR switchover failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60003	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Switch to the DR Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The standby cluster is unavailable.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

Step 1 Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

Step 1 Check whether the Direct Connect is implemented and normal between the two regions.

Step 2 Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

Step 3 Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'.**

Step 4 Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

Step 5 After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Alarm Clearance

The alarm is cleared after the DR switchover is stopped or the fault is rectified.

Related Information

None

2.1.50 DWS_60004 Failed to Restore the DR Relationship

Alarm Description

When the cluster fails to restore the DR relationship, this alarm is sent to the SRE to confirm the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60004	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Restore the DR Relationship
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The standby cluster is unavailable.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

- Step 1** Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

- Step 1** Check whether the Direct Connect is implemented and normal between the two regions.

- Step 2** Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

- Step 3** Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'.**

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Alarm Clearance

The alarm is cleared after the DR relationship restoration is stopped or the fault is rectified.

Related Information

None

2.1.51 DWS_60005 Failed to Delete the DR Task

Alarm Description

When DR fails to be started in the cluster, this alarm is generated to notify the SRE to confirm the root cause of the failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60005	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Delete the DR Task
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The standby cluster is unavailable.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

- Step 1** Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

- Step 1** Check whether the Direct Connect is implemented and normal between the two regions.

- Step 2** Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

- Step 3** Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'**.

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Alarm Clearance

The alarm is cleared after the DR deletion is stopped or the fault is rectified.

Related Information

None

2.1.52 DWS_60006 DWS Logical Cluster Task Failed

Alarm Description

If a task fails during logical cluster operations, this alarm is generated to notify SRE of the root cause of the cgroup synchronization failure.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_6000 6	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	This alarm is generated when a DWS logical cluster task fails.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The availability of cluster services is not affected. However, the operation failure may cause customer assurance. Handle the problem as soon as possible.

Possible Causes

Product problems related to scale-out;

The product on the OM side of the logical cluster is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On the Task Management page, locate the information about the failed task based on the cluster ID.
- Step 3** In the dwscontroller microservice container, use the jobId to view the ossres-dws.log file and check the error information.
- Step 4** If the failure is caused by an agency or kernel problem, rectify the fault and click Retry next to the failed task.

----End

Alarm Clearance

The fault can be rectified.

Related Information

None

2.1.53 DWS_60007 Failed to Synchronize cgroup Information During DR

Alarm Description

This alarm is generated when the active cluster fails to synchronize cgroup information to the standby cluster during DR.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60007	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Synchronize cgroup Information During DR
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The normal DR process is not affected, but the cgroup information consistency between the standby cluster and the primary cluster is affected. If the cgroup information of the standby cluster does not match that of the primary cluster, cluster resource management and control may be affected.

Possible Causes

The network, disk, memory, or management plane is faulty.

Handling Procedure

Cross-AZ DR:

- Step 1** Log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Cross-region DR:

- Step 1** Check whether the Direct Connect is implemented and normal between the two regions.

- Step 2** Check in the security group whether port **22** and **ICMP** between the two cluster subnets are enabled.

- Step 3** Log in to the instance outside the sandbox and view **/etc/ssh/sshd_config** to check whether **ListenAddress** is added to **privatelvp**.

To query the private IP address, log in to the **rms** database on the management plane and run the following SQL statement: **select privatelvp from rds_instance where id = 'instance ID'**.

- Step 4** Log in outside the sandbox and check whether the CIDR of the peer cluster is added to the route. You can query the CIDR by choosing **Dedicated Clusters > Subnet Information** on the management plane.

- Step 5** After confirming that the preceding information is correct, log in to the first node in the cluster and view the instance and Roach logs to locate the root cause.

Instance log path: **/home/Ruby/log/disaster_recovery.log outside the sandbox**

----End

Alarm Clearance

The alarm is cleared after the DR deletion is stopped or the fault is rectified.

Related Information

None

2.1.54 DWS_60016 Failed to Invoke GaussDB(DWS) OpenAPI

Alarm Description

An unknown exception occurs when a user calls the DMS open API.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60016	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	An internal error occurred when invoking the GaussDB (DWS) OpenAPI.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Traceld	OpenAPI URL, request mode, traceld, and error information.

Impact on the System

Related OpenAPIs are unavailable.

Possible Causes

Internal server error.

Handling Procedure

Contact oncall to locate the fault based on Traceld.

Alarm Clearance

Automatic clear

Related Information

None

2.1.55 DWS_60017 GaussDB(DWS) DMS-AGENT Process Is Abnormal

Alarm Description

The DMS-AGENT process is abnormal. For example, the DMS-AGENT working directory is missing, the node process is not started, the pid file is missing, or the configuration files between nodes are inconsistent.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_60017	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	GaussDB (DWS) DMS-AGENT Process Is Abnormal
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster resourceId, domain_id, and process exception details.

Impact on the System

The dms-agent process is abnormal. As a result, user-defined metrics may fail to be delivered, and metrics of some nodes in the cluster are not reported.

Possible Causes

1. The pid file is missing.
2. The working directory is missing.
3. Node monitoring is not reported.
4. Configuration files are inconsistent between nodes.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Find the cluster ID in Additional Information. Log in to the tenant instance to check whether the dms-agent process exists and whether metrics are properly reported.

Step 3 Check whether the working directory exists and whether the pid file exists.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.56 DWS_89002 Failed to Obtain Managed Cluster Information Through the FIM Interface

Alarm Description

This alarm is generated when the FIM interface cannot obtain information about a managed cluster, including the alarm information, cluster status, and node flavor.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_89002	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Failed to Obtain Managed Cluster Information Through the FIM Interface
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The system may fail to obtain the dynamic information about a managed cluster, including the cluster status, creation time, and node flavor. In addition, the cluster's alarm information cannot be reported to the HCS alarm platform.

Possible Causes

1. The managed cluster is deleted. As a result, the FIM interface cannot obtain its information.
2. The FIM user information is modified or deleted. As a result, information authentication of the interface fails.
3. The network connection is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In **Possible Causes**, find the **floatIp** of FusionInsight Manager. Log in to the management plane of FusionInsight Manager and check whether the cluster still exists through <https://floatIp:28443/web/#!/app/homepage/detail>.

Step 3 On FusionInsight Manager, choose **System > Permission > User** to check whether the user of the managed cluster exists.

Username	User Type	Description	Created On
admin	Human-Machine	Administrator of FusionInsight Manager.	09/16/2020 17:00:30
test_xml	Machine-Machine		09/16/2020 19:20:53

Step 4 Use **telnet floatip 28443** to check whether the network connection is normal.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.57 1078919294 ECF Monitor Pod Status Alarm

Alarm Description

This alarm is generated when the ECF Monitor component is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919294	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	ECF Monitor Pod Status Alarm
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The cluster status monitoring of the EI cloud services that depend on the EI Common component may be abnormal. As a result, alarms on the tenant side cannot be reported.

Possible Causes

The ECF Monitor component is abnormal due to insufficient CloudAutoDeploy-CDK cluster memory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Connect to the CloudAutoDeploy-CDK master node, view the container status, and restart the container.

1. Run the **kubectl get pods -n ecf** command to check the status. The following figure shows the normal container status. If the status is not the same as that shown in the following figure, the container is abnormal.

```
[root@10-63-90-40 ~]# kubectl get po -n ecf
NAME                      READY   STATUS    RESTARTS   AGE
dbsevent-b9b958554-pd5gg   1/1    Running   0          55d
dbsevent-b9b958554-wn4l6   1/1    Running   0          54d
dbsinsight-7c897d7d5c-cszk7 1/1    Running   0          1d
dbsmonitor-7bfbdc6fdc-mmwr7 1/1    Running   0          43d
dbsmonitor-7bfbdc6fdc-pj6zg 1/1    Running   4          56d
ecfclustermanager-75595d8d57-kfkrt 0/1    Running   353       1d
```

2. Run the following command to restart the container based on the container name obtained in **Step 2.1**. If there are two containers, restart them one by one.

kubectl delete pod Pod_name -n ecf

Example: **kubectl delete pod dbsmonitor-7bfbdc6fdc-mmwr7-n ecf**

Step 3 After the restart, run the **kubectl get pods -n ecf** command to check the container status again. When the container status becomes normal, log in to the console and create a cluster for verification. If the cluster creation fails at 96% in progress, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.58 1078919295 ECF Insight Pod Status Alarm

Alarm Description

This alarm is generated when the ECF Insight component is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919295	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	ECF Insight Pod Status Alarm
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

All EI services that depend on the EI Common component may fail to connect to ManageOne Maintenance Portal.

Possible Causes

The ECF Insight component is abnormal due to insufficient CloudAutoDeploy-CDK cluster memory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Connect to the CloudAutoDeploy-CDK master node, view the container status, and restart the container.

1. Run the **kubectl get pods -n ecf** command to check the status. The following figure shows the normal container status. If the status is not the same as that shown in the following figure, the container is abnormal.

NAME	READY	STATUS	RESTARTS	AGE
dbsevent-b9b958554-pd5gg	1/1	Running	0	55d
dbsevent-b9b958554-wn4l6	1/1	Running	0	54d
dbsinsight-7c897d7d5c-cszk7	1/1	Running	0	1d
dbsmonitor-7bfbd6fdc-mmwr7	1/1	Running	0	43d
dbsmonitor-7bfbd6fdc-pj6zg	1/1	Running	4	56d
ecfclustermanager-75595d8d57-kfkrt	0/1	Running	353	1d

2. Run the following command to restart the container based on the container name obtained in **Step 2.1**. If there are two containers, restart them one by one.

kubectl delete pod Pod_name -n ecf

Example: **kubectl delete pod dbsinsight-7c897d7d5c-cszk7 -n ecf**

Step 3 After the restart, run the **kubectl get pods -n ecf** command to check the container status until it becomes normal. If there are two containers, restart them one by one. After the restart is successful, verify whether the O&M plane can be connected. If the fault persists, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.59 1078919297 ECF Event Pod Status Alarm

Alarm Description

This alarm is generated when the ECF Event component is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919297	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	ECF Event Pod Status Alarm
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Alarms of cloud services that depend on the EI Common component cannot be properly reported.

Possible Causes

The ECF Event component is abnormal due to insufficient CDK cluster memory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Connect to the CloudAutoDeploy-CDK master node, view the container status, and restart the container.

1. Run the **kubectl get pods -n ecf** command to check the status. The following figure shows the normal Event container status. If the status is not the same as that shown in the following figure, the container is abnormal.

NAME	READY	STATUS	RESTARTS	AGE
dbsevent-b9b958554-pd5gg	1/1	Running	0	55d
dbsevent-b9b958554-wn4l6	1/1	Running	0	54d
dbsinsight-7c897d7d5c-cszk7	1/1	Running	0	1d
dbsmonitor-7bfbdc6fdc-mmwr7	1/1	Running	0	43d
dbsmonitor-7bfbdc6fdc-pj6zg	1/1	Running	4	56d
ecfclustermanager-75595d8d57-kfkrt	0/1	Running	353	1d

2. Run the following command to restart the container based on the container name obtained in **Step 2.1**. If there are two containers, restart them one by one.

kubectl delete pod Pod_name -n ecf

Example: **kubectl delete pod dbsevent-b9b958554-pd5gg -n ecf**

Step 3 After the restart, run the **kubectl get pods -n ecf** command to check the container status again. When the container status becomes normal, log in to the DWS console and check whether the cluster can properly report events. If the fault persists, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.60 1078919298_ECF Cluster Manager Pod Status Alarm

Alarm Description

This alarm is generated when the ECF Cluster Manager component is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891929 8	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	ECF Cluster Manager Pod Status Alarm
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The management services of other EI services that depend on the EI Common component may be affected.

Possible Causes

The ECF Cluster Manager component is abnormal due to insufficient CDK cluster memory.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Connect to the CloudAutoDeploy-CDK master node, view the container status, and restart the container.

1. Run the **kubectl get pods -n ecf** command to check the status. The following figure shows an exception of the ECF Cluster Manager component.

```
[root@10-63-90-40 ~]# kubectl get po -n ecf
NAME                               READY   STATUS    RESTARTS   AGE
dbsevent-b9b958554-pd5gg          1/1     Running   0          55d
dbsevent-b9b958554-wn4l6          1/1     Running   0          54d
dbsinsight-7c897d7d5c-cszk7       1/1     Running   0          1d
dbsmonitor-7bfbd6fdc-mmwr7       1/1     Running   0          43d
dbsmonitor-7bfbd6fdc-pj6zg        1/1     Running   4          56d
ecfclustermanager-75595d8d57-kfkrt  0/1     Running   353        1d
[root@10-63-90-40 ~]#
```

2. Run the following command to restart the container based on the container name obtained in **Step 2.1**.

kubectl delete pod Pod_name -n ecf

Example: **kubectl delete pod ecfclustermanager-75595d8d57-kfkrt -n ecf**

Step 3 After the restart, run the **kubectl get pods -n ecf** command to check the container status again. After 2 to 3 minutes, the container status becomes normal. If the container fails to be restarted, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.61 1078919299 DWS Controller Pod Status Alarm

Alarm Description

This alarm is generated when exceptions on the GaussDB(DWS) management side occur.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919299	Management plane alarm	Critical	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	DWS Controller Pod Status Alarm
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Cluster management may be abnormal, and the corresponding management page becomes unavailable.

Possible Causes

The DWS Controller component works improperly.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Connect to the CloudAutoDeploy-CDK master node, view the container status, and restart the container.

1. Run the **kubectl get pods -n dws** command to check the container status. The following figure shows the normal container status. If the status is not the same as that shown in the following figure, the container is abnormal.

```
[root@9-30-25-209 ~]# kubectl get pods -n dws
NAME                  READY   STATUS    RESTARTS   AGE
dwscontroller-857c9c44ff-d47dw   1/1     Running   0          11h
[root@9-30-25-209 ~]# █
```

2. Run the following command to restart the container based on the container name obtained in **Step 2.1**. If there are two containers, restart them one by one.

kubectl delete pod [pod_name] -n dws

Example: **kubectl delete pod dwscontroller-857c9c44ff-d47dw -n dws**

- Step 3** After the restart, run the **kubectl get pods -n dws** command to check the container status. When the container status becomes normal, log in to the console and check whether DWS is normal. If the fault persists, contact O&M engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.62 Querying Logs Based on the Alarm Generation Time

Background

UTC time is used by each node on the management side while local time is used on the alarm platform, which causes time difference.

Before querying logs by **First Occurred At** on the alarm platform, calculate the UTC time based on the local time.

Procedure

For example, if the local time is GMT+02:00 and the alarm "Script Generation Exception" is generated, perform the following steps to query logs based on the alarm generation time.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** View the alarm information. Obtain the alarm IP address and alarm generation time, for example, **2020-10-19 16:56:57**.
- Step 3** If the local time is Beijing time, there is a difference of eight hours between the UTC time and Beijing time. Therefore, the UTC time is **2020-10-19 8:56:57**. If the local time is GMT+02:00, the UTC time is **2020-10-19 14:56:57**.
- Step 4** Log in to the O&M container of the IP address obtained in **Step 2**. Run the following command to switch to the log path:

```
cd /opt/cloud/3rdComponent/tomcat/logs
```

- Step 5** Query logs generated around the UTC time (for example, **2020-10-19 8:56:57**).

----End

2.1.63 DWS_200000001_OM Node CPU Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of CPU usage (system + user) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the CPU usage (system + user) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000001_OM	Management plane alarm	Urgent: > 90%	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node CPU Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the CPU usage of a node exceeds the threshold, the compute resources of the node are about to be used up, and related services may be executed slowly or fail.

Possible Causes

The database service load is too heavy or database CPU skew occurs.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

1. Choose **Monitoring > Node Monitoring**. View the CPU usage of all nodes on the node monitoring page. If the CPU usage of only one node is high, CPU skew occurs. If the CPU usage of all nodes is high, the service load is too high.
2. Choose **Monitoring**. Go to the **Real-Time** page. View the CPU execution durations of all SQL statements that are being executed and sort them in descending order. Find the query statement with the longest CPU execution time and analyze its resource usage.

Step 3 If the service load is heavy according to **Step 2**, check whether services are properly scheduled or workload queues are properly configured. If no, adjust related services. If the compute resources are insufficient, contact O&M personnel to scale out the cluster.

Step 4 If CPU skew occurs according to **Step 2**, choose **Monitoring > Query Monitoring > Real-Time** to sort the SQL statements by **CPU Time Skew** in descending order. In this way, you can locate the SQL statement with the most unbalanced CPU usage and decide whether to terminate the query or wait until the query is complete.

Step 5 If a single statement consumes excessive resources according to **Step 2**, locate the query statement with the longest CPU execution time and decide whether to terminate it.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.64 DWS_200000002_OM Node System CPU Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of system CPU usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the system CPU usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000002_OM	Management plane alarm	Urgent: > 50%	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node System CPU Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the system CPU usage of a node exceeds the threshold, a large number of the node compute resources are wasted in OS kernel operations (such as waiting for global resource locks and applying for/releasing memory). Related services may be executed slowly or fail.

Possible Causes

The database service load is too heavy or the OS is incorrectly configured.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

1. Choose **Monitoring > Node Monitoring**. View the CPU usage of all nodes on the node monitoring page. If the CPU usage of most nodes is high and the system CPU usage is also high, the service load is too heavy.
2. Choose **Monitoring**. Go to the **Real-Time** page. View the number of concurrent SQL statements that are being executed. If the number of concurrent statements reaches or approaches the upper limit, the cluster is overloaded.

Step 3 If the service load is heavy according to **Step 2**, check whether services are properly scheduled or workload queues are properly configured. If no, adjust related services. If the compute resources are insufficient, contact O&M personnel to scale out the cluster.

Step 4 If the OS is configured incorrectly according to **Step 2**, contact the vendor's O&M personnel to locate and rectify the fault.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.65 DWS_200000004_OM Node System Disk Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of system disk (/) usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the system disk (/) usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000004_OM	Management plane alarm	Urgent: > 85%; important: > 80%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node System Disk Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resource_id and domain_id.

Impact on the System

If the system disk usage of a node exceeds the threshold, the system disk (/) storage resources of the node are about to be used up, and the cluster is about to be read-only.

Possible Causes

Too many system logs are accumulated or the tools installed by the user occupies too much system disk space.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to scale out the cluster, log in to the corresponding node on the tenant side and clear the system logs.

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.66 DWS_200000005_OM Node Log Disk Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of log disk (/var/chroot/DWS/manager) usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the log disk (/var/chroot/DWS/manager) usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000005_OM	Management plane alarm	Urgent: > 85%; Important: > 80%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Log Disk Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the log disk usage of a node exceeds the threshold, the log disk (`/var/chroot/DWS/manager`) storage resources of the node are about to be used up, and the cluster is about to be read-only.

Possible Causes

Too many kernel logs are accumulated.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to scale out the cluster, log in to the corresponding node on the tenant side and clear the database kernel logs.

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.67 DWS_200000006_OM Node Data Disk Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of data disk (`/var/chroot/DWS/data[n]`) usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the data disk (`/var/chroot/DWS/data[n]`) usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000006_OM	Management plane alarm	Urgent: > 85%; important: > 80%	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Data Disk Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the data disk usage of a node exceeds the threshold, the data disk (`/var/chroot/DWS/data[n]`) storage resources of the node are about to be used up, and the cluster is about to be read-only.

Possible Causes

Storage resources of the database cluster are about to be used up.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to expand the capacity, you can delete unnecessary or expired historical data and perform the VACUUM FULL operation. For details, see *Data Warehouse Service (DWS) 8.1.3.331 User Guide (for Huawei Cloud Stack 8.3.1)* in the [**Data Warehouse Service \(DWS\) 8.1.3.331 User Guide \(for Huawei Cloud Stack 8.3.1\)**](#).

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.68 DWS_2000000007_OM Node System Disk I/O Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of system disk (/) I/O usage (**util**) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the system disk (/) I/O usage (**util**) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000 000007_O M	Management plane alarm	Urgent: > 90%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node System Disk I/O Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the system disk I/O usage of a node exceeds the threshold, the system disk (/) I/O resources of the node are about to be used up, and read/write performance bottlenecks occur in the cluster.

Possible Causes

System logs are frequently read and written, or tools installed by users frequently read and write the system disk.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the tenant node, check the system disk I/O, locate the processes with high I/O usage, and terminate the processes.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.69 DWS_200000008_OM Node Log Disk I/O Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of log disk (`/var/chroot/DWS/manager`) I/O usage (`util`) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the log disk (`/var/chroot/DWS/manager`) I/O usage (`util`) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000008_OM	Management plane alarm	Urgent: > 90%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Log Disk I/O Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the log disk I/O usage of a node exceeds the threshold, the log disk (**/var/chroot/DWS/manager**) I/O resources of the node are about to be used up, and read/write performance bottlenecks occur in the cluster.

Possible Causes

The database kernel logs are frequently read and written, or tools installed by users frequently read and write the log disk.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the tenant node, check the log disk I/O, locate the processes with high I/O usage, and terminate the processes.

Step 3 If kernel logs are frequently read and written, contact the vendor's O&M personnel as soon as possible.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.70 DWS_200000009_OM Node Data Disk I/O Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of data disk (`/var/chroot/DWS/data[n]`) I/O usage (**util**) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the data disk (`/var/chroot/DWS/data[n]`) I/O usage (**util**) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000009_OM	Management plane alarm	Urgent: > 90%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Data Disk I/O Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resource_id and domain_id.

Impact on the System

If the data disk I/O usage of a node exceeds the threshold, the data disk (`/var/chroot/DWS/data[n]`) I/O resources of the node are about to be used up, and read/write performance bottlenecks occur in the cluster.

Possible Causes

The service load is heavy or too many SQL statements are queried so that a large amount of data is flushed to disks.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

1. Choose **Monitoring > Node Monitoring > Disks**. View the disk I/O usage of all nodes on the disk monitoring page. If the disk I/O usage of a single node is high, disk I/O skew occurs. If the disk I/O usage of all nodes is high, the service load is too heavy.
2. Choose **Monitoring**. Go to the **Real-Time** page. View the peak I/O count of all SQL statements that are being executed and sort the list in descending order. Find the query statement that has the highest IOPS and analyze the resource usage of the query statement.

Step 3 If the service load is heavy according to **Step 2**, check whether services are properly scheduled or workload queues are properly configured. If no, adjust related services. If the compute resources are insufficient, contact O&M personnel to scale out the cluster.

Step 4 If CPU skew occurs according to **Step 2**, choose **Monitoring > Query Monitoring > Real-Time** and sort the SQL statements by highest IOPS in descending order. Locate the SQL statement that consumes the most I/O resources, and decide whether to terminate the query or wait until the query is complete.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.71 DWS_2000000010_OM Node System Disk Latency Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of system disk (/) I/O latency (**await**) of any node in the cluster is exceeded within the specified period and the constraint

is not met. The alarm will be cleared when the system disk (/) I/O latency (**await**) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000 000010_O M	Management plane alarm	Important: > 400 ms	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node System Disk Latency Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the system disk I/O latency of a node exceeds the threshold, the system disk (/) of the node responds slowly, and read/write performance bottlenecks occur in the cluster.

Possible Causes

System logs are frequently read and written, or tools installed by users frequently read and write the system disk, or the system disk is failing.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** View the historical information about the system disk I/O latency. If high latency persists for a long time, the disk may be faulty. Contact the vendor O&M personnel to replace the disk.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.72 DWS_2000000011_OM Node Log Disk Latency Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of log disk (`/var/chroot/DWS/manager`) I/O latency (`await`) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the log disk (`/var/chroot/DWS/manager`) I/O latency (`await`) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000011_OM	Management plane alarm	Important: > 400 ms	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Log Disk Latency Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated

Type	Parameter	Description
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the log disk I/O latency of a node exceeds the threshold, the log disk (`/var/chroot/DWS/manager`) of the node responds slowly, and read/write performance bottlenecks occur in the cluster.

Possible Causes

Kernel logs are frequently read and written, or tools installed by users frequently read and write the log disk, or the log disk is failing.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 View the historical information about the log disk I/O latency. If high latency persists for a long time, the disk may be faulty. Contact the vendor O&M personnel to replace the disk.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.73 DWS_2000000012_OM Node Data Disk Latency Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of data disk (`/var/chroot/DWS/data[n]`) I/O latency (`await`) of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the data disk (`/var/chroot/DWS/data[n]`) I/O latency (`await`) is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000012_OM	Management plane alarm	Important: > 400 ms	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Data Disk Latency Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the data disk I/O latency of a node exceeds the threshold, the data disk (`/var/chroot/DWS/data[n]`) of the node responds slowly, and read/write performance bottlenecks occur in the cluster.

Possible Causes

Data is frequently read and written, or tools installed by users frequently read and write the data disk, or the data disk is failing.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 View the historical information about the data disk I/O latency. If high latency persists for a long time, the disk may be faulty. Contact the vendor O&M personnel to replace the disk.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.74 DWS_2000000013_OM Node System Disk Inode Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of system disk (/) inode usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the system disk (/) inode usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000013_OM	Management plane alarm	Urgent: > 95%; important: > 90%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node System Disk Inode Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the system disk inode usage of a node exceeds the threshold, the system disk (/) capacity of the node is about to be used up, and the cluster is about to be read-only.

Possible Causes

Too many system logs are accumulated or the tools installed by the user occupies too much system disk space.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to scale out the cluster, log in to the corresponding node on the tenant side and clear the system logs.

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.75 DWS_200000014_OM Node Log Disk Inode Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of log disk (`/var/chroot/DWS/manager`) inode usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the log disk (`/var/chroot/DWS/manager`) inode usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000014_OM	Management plane alarm	Urgent: > 95%; important: > 90%	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Log Disk Inode Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the log disk inode usage of a node exceeds the threshold, the log disk (`/var/chroot/DWS/manager`) capacity of the node is about to be used up, and the cluster is about to be read-only.

Possible Causes

Too many kernel logs are accumulated.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to scale out the cluster, log in to the corresponding node on the tenant side and clear the database kernel logs.

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.76 DWS_2000000015_OM Node Data Disk Inode Usage Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of data disk (`/var/chroot/DWS/data[n]`) inode usage of any node in the cluster is exceeded within the specified period and the constraint is not met. The alarm will be cleared when the data disk (`/var/chroot/DWS/data[n]`) inode usage is lower than the threshold and the constraint is not met.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000 000015_O M	Management plane alarm	Urgent: > 95%; important: > 90%	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Node Data Disk Inode Usage Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the data disk inode usage of a node exceeds the threshold, the data disk (`/var/chroot/DWS/data/[n]`) capacity of the node is about to be used up, and the cluster is about to be read-only.

Possible Causes

Storage resources of the database cluster are about to be used up.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If you do not want to expand the capacity, you can delete unnecessary or expired historical data and perform the VACUUM FULL operation. For details, see *Data Warehouse Service (DWS) 8.1.3.331 User Guide (for Huawei Cloud Stack 8.3.1)* in the [Data Warehouse Service \(DWS\) 8.1.3.331 User Guide \(for Huawei Cloud Stack 8.3.1\)](#).

Step 3 Contact O&M personnel to scale out the cluster if you confirm that the storage resources are insufficient.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.77 DWS_2000000016_OM Data Spilled to Disks of the Query Statement Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of data flushed to disks of the SQL statement in the cluster is exceeded within the specified period and the constraint is not met. The alarm can be cleared only after you handle the SQL statement.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000016_OM	Management plane alarm	Urgent: > 5 GB	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Data Spilled to Disks of the Query Statement Exceeds the Threshold
	Type	Operation alarm

Type	Parameter	Description
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

This alarm indicates that the query statement is not optimized. As a result, database cluster features cannot be well utilized and batch processing is blocked, deteriorating the overall cluster performance.

Possible Causes

The user database is not optimized.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

Choose **Utilities > SQL Diagnosis**. View the SQL tuning suggestions for the query statement.

Step 3 Manually clear the alarm after the SQL statement is optimized.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.78 DWS_2000000017_OM Number of Queuing Query Statements Exceeds the Threshold

Alarm Description

This alarm is generated if the threshold of the number of queuing SQL statements is exceeded within the specified period. The alarm will be cleared when the number of queuing SQL statements is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000017_OM	Management plane alarm	Urgent: >10	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Number of Queuing Query Statements Exceeds the Threshold
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Batch processing is slow and ad hoc query does not respond.

Possible Causes

Workload queues are improperly configured, or database cluster is unable to process the services.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

1. Choose Load Analysis > Load Information Snapshot, and view the resource usage and the number of queuing tasks of workload queues. If the workload queue quota is not configured properly, modify the quota.
2. If all workload queues are fully loaded and the number of queuing query statements keeps increasing, modify the time for batch processing.
3. If the problem persists, contact the vendor O&M personnel to scale out the cluster.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.79 DWS_2000000018_OM Queue Congestion in the Default Cluster Resource Pool

Alarm Description

This alarm is generated if the number of queuing SQL statements exceeded the threshold within the specified period. The alarm will be cleared when the number of queuing SQL statements is less than the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000018_OM	Management plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Queue Congestion in the Default Cluster Resource Pool
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Tasks delivered by users cannot be executed properly. The resource pool queue is blocked, affecting service execution.

Possible Causes

The cluster breaks down or the cluster performance is abnormal due to lack of resources.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the DMS page to locate the fault.

1. Choose **Monitoring**. Go to the **Real-Time** page. Terminate the query statements that take a long time to execute.
2. Choose **Monitoring**. Go to the **Real-Time** page. Terminates idle sessions.
3. If the problem persists, contact the vendor O&M personnel to locate cluster performance issues.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.80 DWS_2000000019_OM High TCP Retransmission Rate After Packet Loss

Alarm Description

This alarm is generated if the DMS alarm module detects a high retransmission rate on a server and no alarm suppression conditions are met. If the retransmission rate decreases, the alarm will be automatically cleared.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000019_OM	Management plane alarm	Critical, Major, Minor, or Warning	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	High TCP Retransmission Rate After Packet Loss
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the packet loss retransmission rate of the cluster network exceeds the threshold, the SQL running performance of upper-layer services deteriorates and the performance of upper-layer applications deteriorates.

Possible Causes

The network is disconnected.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Locate the current cluster node based on the cluster ID and node ID, and check the network status. If the problem persists, contact the O&M personnel of the vendor to locate the cluster performance problem.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.81 DWS_200000020_OM Long SQL Probe Execution Duration in a Cluster

Alarm Description

This alarm is generated if the DMS alarm module detects a SQL probe execution duration on a server and no alarm suppression conditions are met. If no execution duration exceeds the threshold, the alarm will be automatically cleared.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000020_OM	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Long SQL Probe Execution Duration in a Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The cluster performance deteriorates or the cluster is faulty.

Possible Causes

1. The service load of the cluster is high or the cluster is faulty. As a result, the execution of the SQL probe becomes slow.

Handling Procedure

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

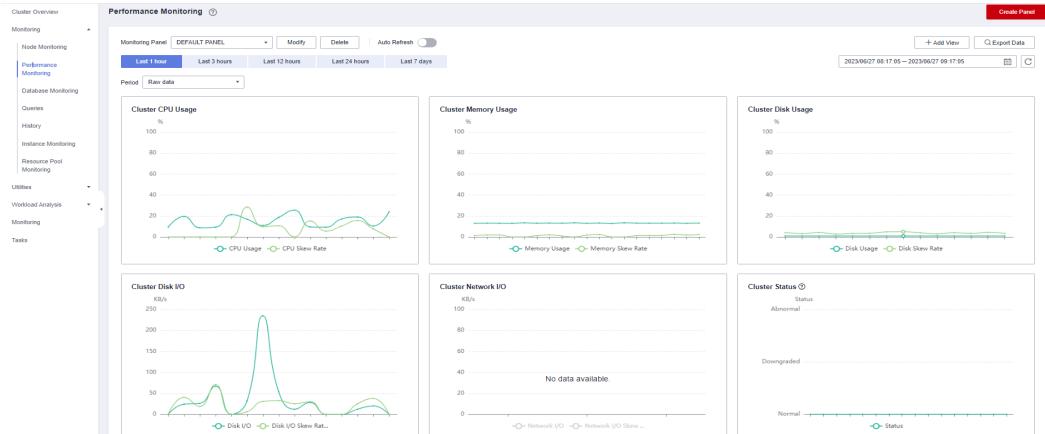
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

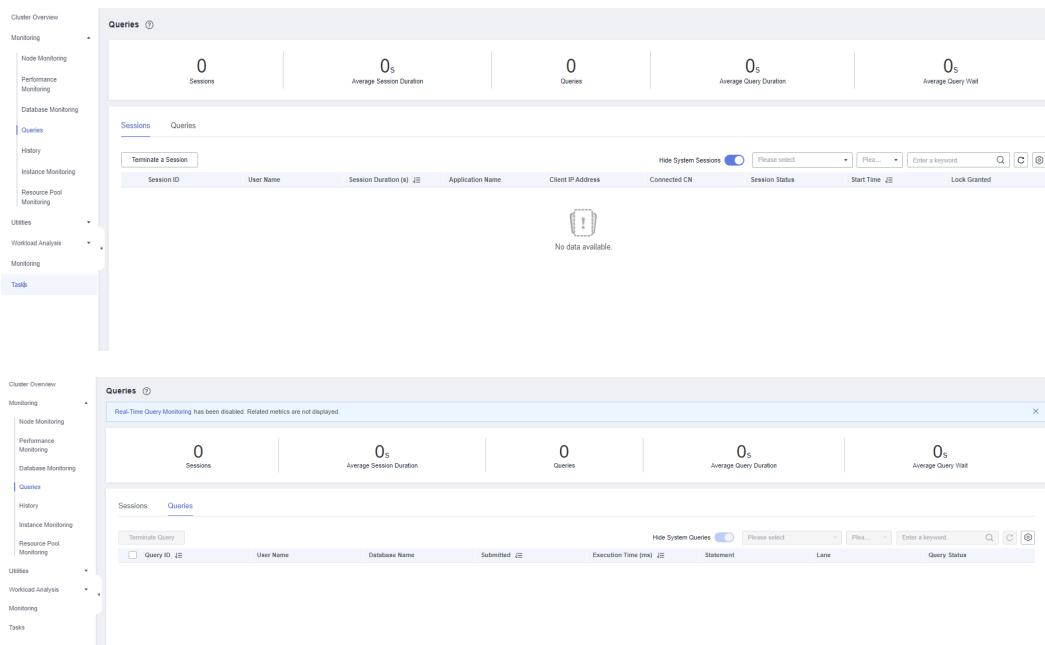
The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the cluster node and run the **cm_ctl query -Cvd** command to check the cluster status.

Step 3 Go to the monitoring module of the cluster for which the alarm is generated, choose **Performance Monitoring**, and view monitoring metrics such as the CPU usage, disk usage, and memory usage to determine whether the service load is high or the metrics are abnormal.



Step 4 Choose **Queries** and check whether there are queries or sessions that wait for a long time, causing the cluster broken down. If yes, terminate sessions or queries.



----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.82 DWS_2000000022_OM Monitoring Metric Is Not Reported for Too Many Periods

Alarm Description

This alarm is generated when a cluster metric is not reported for a certain number of periods by the DMS alarm module, for example, 10 periods and the metric is

not in suppression period. This alarm is cleared when the metric data is reported again.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000 000022_O M	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Monitoring Metric Is Not Reported for Too Many Periods
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Monitoring information is missing on the cluster monitoring panel.

Possible Causes

1. The dms-agent process exits due to some reasons. As a result, related metric data is not collected.
2. Metric data fails to be imported to the database due to some exceptions.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

5. The additional information contains the following monitoring metrics:

SchemaUsage: schema space usage; **InstanceResources**: instance information; **ClusterHostStatus**: cluster node status; **CpuStat**: CPU usage; **ClusterInstStatus**: cluster instance status; **IOStat**: cluster I/O usage; **MemStat**: memory usage; **DbStats**: database monitoring; **FileSystemStat**: disk usage; **OsStat**: operating system status; **SessionStats**: session usage; **NetIfStat**: network status; **FileSystemInodeStat**: inode usage; **ClusterStatus**: cluster status; **DbActiveStats**: database usage.

- Step 2** Log in to the cluster node and check whether the dms-agent thread (`agent_service.py --start`) is running properly.

If the thread does not exist, go to the `/rds/dms-agent/workplace` directory and manually run the `startup.sh` script to start the thread.

If the thread is running properly, go to the `/var/chroot/DWS/manager/dmsagent/log` directory and view the `initial.log` and `agent_service.log` files to check whether any error is reported.

- Step 3** Log in to the dms-collection container, view the log, search for the metric keyword found in the additional information, and check whether error information exists.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.83 DWS_2000000023_OM A Vacuum Full Operation That Holds a Table Lock for A Long Time Exists in the Cluster

Alarm Description

This alarm is generated when the DMS alarm module detects that a vacuum full operation holds a lock for too long and does not meet the constraints.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000000023_OM	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	A Vacuum Full Operation That Holds a Table Lock for A Long Time Exists in the Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

Subscriber services may fail to be executed.

Possible Causes

1. The user table occupies a large amount of space.
2. The I/O load of the current cluster is too high.
3. Other lock-holding services are running on the user table, and vacuum full is in the lock waiting state.

Handling Procedure

Step 1 Log in to GaussDB(DWS) console, and click **Monitoring Panel** of the cluster for which the alarm is generated.

Step 2 In the navigation tree on the left, choose **Queries**. On the **Sessions** tab, search for **vacuum full**.



Check whether the execution time of vacuum full exceeds the alarm threshold (20 minutes by default). You can evaluate whether the execution time of vacuum full is within the normal range based on the size of the user table.

If the real-time query does not contain the vacuum full operation or the execution time does not exceed the threshold, this alarm will be automatically cleared later.

Step 3 Check whether there are queries waiting for the lock held by the vacuum full operation.

On the **Sessions** tab, query the lock object for the same operation as vacuum full and check whether different sessions request the same lock object.



----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.1.84 DWS_200000024_OM Residual SQL Threads Exist in the Cluster

Alarm Description

By default, GaussDB(DWS) checks the **PG_STAT_ACTIVITY** view every 180 seconds to detect possible residual threads of the current user's query sessions on CNs and DNs. This alarm is generated when it is detected within 5 minutes (configurable) that residual SQL threads exist on CNs or DNs for more than 6 hours (configurable).

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000024_OM	Management plane alarm	Major	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Residual SQL Threads Exist in the Cluster
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceld and domain_id.

Impact on the System

Too many residual cluster threads may cause long lock waits and occupy system resources. As a result, the overall performance is slow.

Possible Causes

Some threads do not exit after the DN receives the cancel signal from the CN. As a result, residual transactions exist.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Query the residual thread information in the cluster based on the PID carried in the additional alarm information in step 1 and lock the thread information.

```
select * from pg_stat_activity where pid = 'pid';
```

Step 3 Connect to the CN or DN and run the following statement to terminate the session:

```
select pg_terminate_backend(pid);
```

----End

Alarm Clearance

This alarm cannot be automatically cleared. After the fault is rectified, you need to manually clear it on the alarm platform.

Related Information

None

2.1.85 DWS_200000025_OM GaussDB(DWS) Cluster Job Execution Duration Exceeds the Threshold

Alarm Description

This alarm is generated when the DMS alarm module detects that the job execution time of a cluster instance exceeds the threshold and the suppression conditions are not met in a specified period. This alarm is cleared when the DMS alarm module detects that the execution time of all query statements on the cluster instance is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_200000025_OM	Management plane alarm	Critical/Major	Service alarm	GaussDB(DWS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	The job execution duration of the GaussDB (DWS) cluster exceeds the threshold.
	Type	Service alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The current job execution or overall service running may be affected.

Possible Causes

- The CPU and memory resources in the cluster resource pool are insufficient. As a result, the job execution is slow.
- The queried table contains a large amount of data, or the table contains skew and dirty pages. As a result, the job execution is slow.
- A deadlock occurs in the cluster. As a result, the job execution is slow.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 The alarm information contains the statement ID and statement execution duration. If the execution duration exceeds the estimated duration, log in to Monitoring Panel and choose Monitoring > Real-Time Query in the navigation pane to stop the query statement.

Step 3 The alarm information contains the resource pool name. In the navigation pane, choose Dedicated Cluster, click the name of the cluster for which the alarm is generated, and choose Resource Management > Modify Resource Pool to adjust the resource ratio in the resource pool.

----End

Alarm Clearance

You need to clear this alarm manually after the fault is rectified.

Related Information

None

2.1.86 DWS_2000000026_OM Data Written by CNs in a DWS Cluster Exceeds the Threshold

Alarm Description

This alarm is generated when the DMS alarm module detects that the amount of data written to the CN exceeds the threshold in a specified period and the suppression conditions are not met. This alarm is cleared when the DMS alarm module detects that the amount of data written to the CN is lower than the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_2000 000026_O M	Management plane alarm	Critical	Service alarm	GaussDB(D WS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Cluster Name	Cluster for which the alarm is generated.
	Tenant Name	Name of the tenant to which the cluster belongs.
	Alarm Severity	Severity of the alarm.
Other Information	The disk ID.	ID of the cluster for which the alarm is generated
	Resource.	Cluster for which the alarm is generated.
	Instance name	Indicates the name of the CN for which the alarm is generated.
	First Reported	Indicates the first occurrence of an alarm, including the alarm threshold and current value.

Impact on the System

The SQL statement CN occupies disk space, which may cause the cluster to be read-only. When the SQL statement CN is flushed to disks, the memory space is insufficient, the statement execution is slow, and the lock is held for a long time, affecting service execution.

Possible Causes

1. The memory space used by the cluster is insufficient.
2. The SQL statement is not optimized, and the execution efficiency is low.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the query ID of the SQL statement whose data flushing exceeds the threshold based on the alarm information. You can log in to the database to scan and kill the SQL statement, or log in to Monitoring Panel and choose Monitoring > Real-Time Query in the navigation tree to stop the query statement.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.87 DWS_25xxxxxxxx User-Defined Threshold Alarms

Alarm Description

As the alarm source, DMS allows you to create personalized alarms, which start with **DWS_25**. Currently, only schema usage alarms can be customized. Select a database name and schema name to create an alarm for schema usage monitoring.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
DWS_25xxx xxxxx	Management plane alarm	<i>User-defined</i>	Operation alarm	GaussDB(DWS)	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	This parameter is user-defined.
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

If the schema space is insufficient, user table data fails to be written, affecting user services.

Possible Causes

The remaining space of the schema configured by the user is insufficient.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

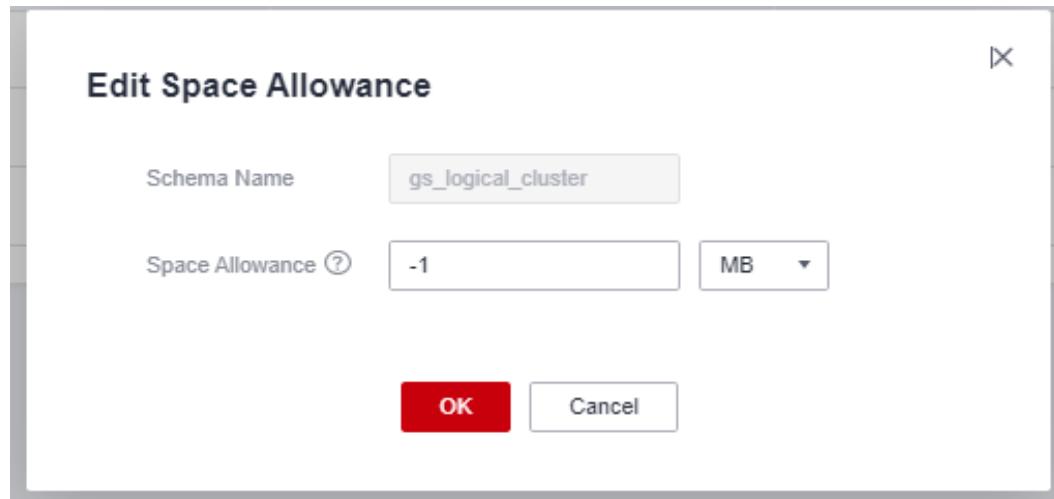
NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Go to the details page of the cluster for which the alarm is generated, click **Resource Management Configurations** to access the resource management module, and click **Schema Space Control**.

Schema Name	Used Space	Space Allowance	Used Percent	Max Value	Min Value	Operation
pt_logical_cluster	0	Unlimited	0	0	0	Exe
public	0	Unlimited	0	0	0	Exe
scheduler	0.02 MB	Unlimited	0	0.01 MB	0.01 MB	Exe

Click **Edit** on the right of the list to modify the space limit.



----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.1.88 TASKMGR_00001 Alarm Sending Failure

Alarm Description

If alarms on the tenant plane or management plane fail to be reported to the alarm platform, an alarm indicating that the alarm fails to be sent is also reported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
TASKMGR_00001	Management plane alarm	Major	Operation alarm	GaussDB(D WS)	No

Alarm Parameters

Type	Parameter	Description
Location Info	Alarm Name	Alarm sending failure
	Type	Operation alarm
	Occurred At	Time when the alarm is generated
Other Information	Cluster ID	Cluster details such as resourceId and domain_id.

Impact on the System

The reporting of real alarms is affected, and the fault locating of the cluster or management plane service is affected.

Possible Causes

The alarm platform interface is incorrectly configured, or the alarm platform service is unstable.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 The alarm information contains the ID of the alarm that fails to be sent. Query logs in the GaussDB (DWS) Event microservice based on the alarm ID to determine the cause of the alarm sending failure.

Step 3 You can also locate the problem that occurs in the current cluster or management plane service based on the alarm that fails to be sent.

----End

Alarm Clearance

You need to clear this alarm manually after the fault is rectified.

Related Information

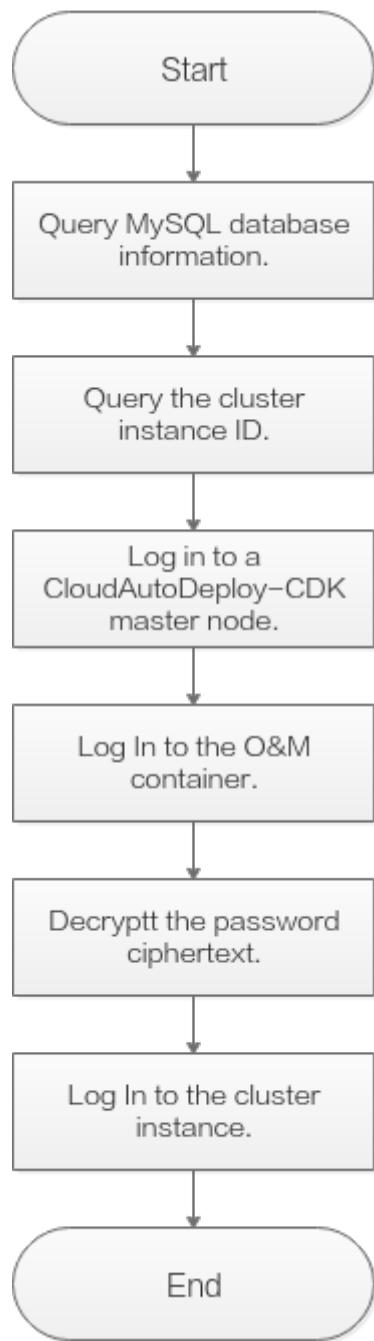
None

2.2 Alarms on the Tenant Side

2.2.1 Logging In to a Node in the Tenant Cluster

This section describes how to use O&M pods to log in to cluster nodes for troubleshooting on the tenant side. The following figure shows the login process.

Figure 2-1 Login process



Querying MySQL Database Information

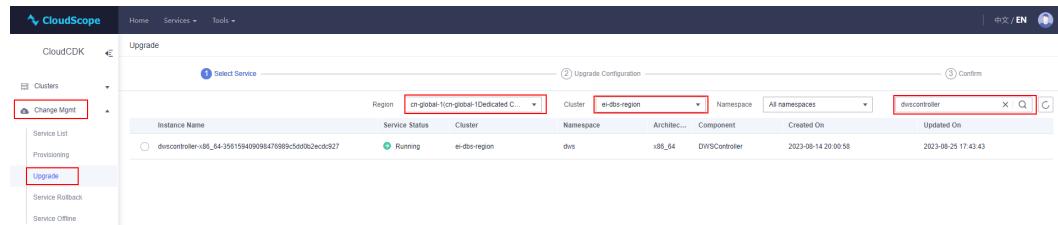
Step 1 Log in to CloudScope using a browser as a system administrator.

- URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op_cdk_sso**

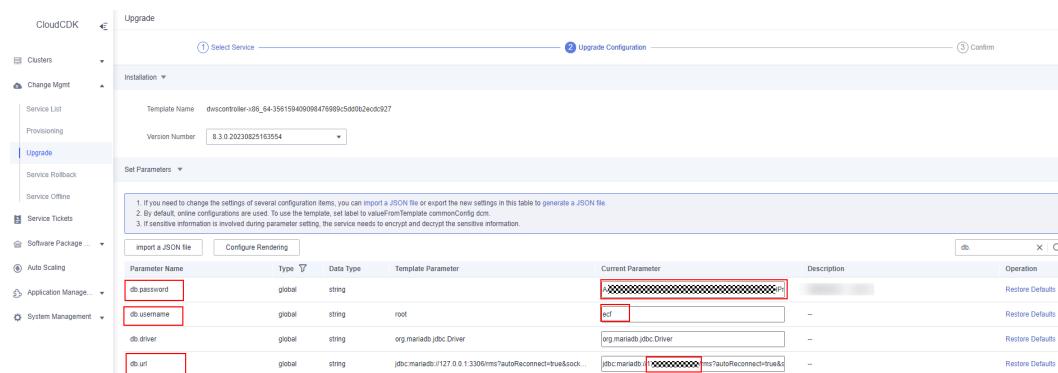
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

Step 2 Choose **Services > Change Mgmt > CloudAutoDeploy-CDK**.

Step 3 In the navigation pane on the left, choose **Change Magmt & > Upgrade**, select the corresponding region, and select the cluster **ei-dbs-region**. Search for **dwscontroller** in the search box, select the corresponding dwscontroller, and click **Next**.



Step 4 Enter the keyword **db.** in the search box on the right and record the password ciphertext corresponding to **db.password**, username corresponding to **db.username**, and database IP address and port number corresponding to **db.url**.



Step 5 After the recording is complete, click **Home** in the upper left corner to exit the current page to prevent misoperations.

----End

Querying the Cluster Instance ID

Step 1 Log in to CloudScope using a browser as a system administrator.

- URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op_cdk_sso**
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

- Step 2** In the **Common Links** area, click **Service CM**. Select your region and then access the **Service CM** page.
- Step 3** Choose **Service List > Data Warehouse Service** to switch to the corresponding namespace.
- Step 4** Choose **Sre OM Management > Clusters** on the left, click the cluster name to go to the node list page, and record the ID of a CN whose name contains **cn**.

Node ID	Node Name	Node Status	Recent Task Status	Latest Task Time
oce3249a-979f-496d-a20b-8fffa3e23c4	auto-default--ypr0G8Z9NrgzPQJc1O2LR1MIVSs-dws-c...	Normal	--	--
45890065-2042-45f7-8572-5839000c3271	auto-default--ypr0G8Z9NrgzPQJc1O2LR1MIVSs-dws-c...	Normal	--	--
5602290e2-2960-4833-89a1-254968526106	auto-default--ypr0G8Z9NrgzPQJc1O2LR1MIVSs-dws-c...	Normal	--	--

----End

Logging In to the CloudAutoDeploy-CDK Master Node

- Step 1** Log in to ManageOne Maintenance Portal via <https://ManageOne Maintenance Portal URL:31943>. Alternatively, log in to the unified portal and choose **OperationCenter**.

- Password login: Enter the username and password of the account.
 - Default account: **bss_admin**

NOTE

For ManageOne upgraded from 8.2.0 or earlier, the default username is **admin**.
For ManageOne 8.2.1 or later, the default username is **bss_admin**.

- Preset password: See the preset password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter the PIN.

Log in to ManageOne Maintenance Portal.

- Step 2** In the **Cloud O&M Management** navigation pane, click **Service_OM**. The Service OM page is displayed.

- Step 3** On the Service OM console page, click **VM**.

- Step 4** Query the IP address of the CloudAutoDeploy-CDK node. In the search box in the upper right corner, enter the keyword **EICCommon-Region-Master** to search for VMs. Generally, three VMs are available. You can record the IP address of any one of them.

- Step 5** Log in to the CloudAutoDeploy-CDK master node as user **opsadmin** using a remote login tool, and then switch to user **root**. The IP address is obtained in [Step 4](#).

su - root

- Default password of user **opsadmin**: Search for **EICommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).
- Default password of user **root**: Search for **EICommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

----End

Logging In to the O&M Container

Step 1 Run the following command on the CloudAutoDeploy-CDK master node to query the O&M pod names:

kubectl get pod -n ecf

Information similar to the following is displayed. Find the pod whose name starts with **dwsmaintaintool**. Any pod whose **STATUS** is **Running** can be used as an O&M pod.

NAME	READY	STATUS	RESTARTS	AGE
dbsevent-5995495644-6px4m	1/1	Running	0	47m
dbsevent-5995495644-hrt8l	1/1	Running	0	47m
dbsisight-79f5fdfc4d-8qcmp	1/1	Running	0	2d2h
dbsisight-79f5fdfc4d-kntp6	1/1	Running	0	2d2h
dbsmonitor-577696776c-j5cpt	1/1	Running	0	2d2h
dbsmonitor-577696776c-kwbzj	1/1	Running	0	2d2h
dwsmaintaintool-6849847c4b-9mxgf	1/1	Running	0	2d1h
dwsmaintaintool-6849847c4b-mdqz6	1/1	Running	0	2d1h
ecfclustermanager-85987598fd-pst2k	1/1	Running	0	40m
ecfclustermanager-85987598fd-x5jn9	1/1	Running	0	40m

Step 2 Log in to an O&M pod.

kubectl exec -it Pod_name -n ecf bash

Replace *Pod_name* with the name of a pod queried in **Step 1** whose **STATUS** is **Running**. The following shows an example.

kubectl exec -it dwsmaintaintool-ff99697f6-vtkcb -n ecf bash

----End

Decrypting the Password Ciphertext

Step 1 Run the following command on the O&M container to go to the **/opt/cloud/3rdComponent/opsTool** directory:

cd /opt/cloud/3rdComponent/opsTool

Step 2 Start the tool.

java -jar SccTool.jar

Step 3 Enter **3 {Password ciphertext}** as prompted to decrypt the password. For example, enter the ciphertext of the database user password queried in GeoGenius.

3 {Password ciphertext}

Press **Enter** to obtain the plaintext of the decrypted password.

Decrypt result:

Step 4 Press CTRL+C to exit the tool.

-----End

Logging In to a Cluster Instance

Step 1 Run the following command in the `/opt/cloud/3rdComponent/opsTool` directory of the O&M container to log in to the cluster instance: Obtain the username, host IP address, and port number from [Querying MySQL Database Information](#). Cluster instance ID is obtained from [Querying the Cluster Instance ID](#).

sh connectTool.sh -u Username -drms -hHost_IP -pPort_number -n Instance_ID -t Standalone

After the command is executed, enter the password as prompted. Obtain the password from [Decrypting the Password Ciphertext](#).

```
[serviceadm@mainaintool-7bbd4bb5-5f6f-opsTool]$ sh connectTool.sh -uXXXX -drms -hXXXX -pXXXX -n XXXXX -t Standard
Start connect DB server and query result.....
Query result complete.
```

```
[service@dwmswaintain tool-78bd4b855-b5f6g opsTool]$ sh connectTool.sh -u [REDACTED] -drms -h [REDACTED] -p [REDACTED] -n [REDACTED] -t Standalone
Start connect DB server and query result.....
Password:
Query result complete.
host is 192.168.0.239
start connect instance server.....
spawn /bin/rm -f /opt/cloud/3rdComponent/opsTool/tmp19605/connect_20230224033436_28179.exp >/dev/null 2>&1
spawn /bin/ssh -i /opt/cloud/3rdComponent/opsTool/tmp19605/ssh_key_Mike@[REDACTED] -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null
Warning: Permanently added '[REDACTED]' (ED25519) to the list of known hosts.

Authorized users only. All activities may be monitored and reported.
Enter passphrase for key /opt/cloud/3rdComponent/opsTool/tmp19605/ssh_key :

Authorized users only. All activities may be monitored and reported.
Last login: Fri Feb 24 03:31:27 2023 from [REDACTED]

Authorized users only. All activities may be monitored and reported.
[Mike@host-1 [REDACTED] ~]# su
Password:
[root@host-1 [REDACTED] ~]# Mike#
```

Step 2 Switch to user **Ruby** and log in to the cluster sandbox.

su - Ruby

```
ssh `hostname -i`
```



It takes some time to log in to the sandbox using `ssh $HOSTNAME`. Use `ssh `hostname -i`` or `ssh ip` instead.

Step 3 If you need to log in to another node in the cluster, run the following commands to query the IP address of the node (*node_ip* in the command output). Then run the corresponding command to enter the sandbox.

```
gs_om -t status --detail
```

ssh *node_ip*

Step 4 Perform O&M operations by referring to cases in this document.

----End

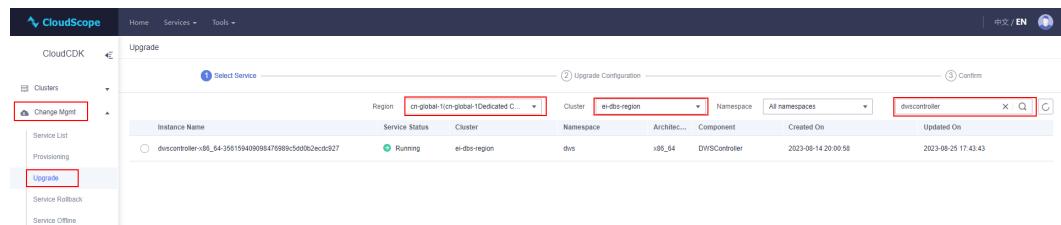
2.2.2 Querying MySQL Database Information

Step 1 Log in to CloudScope using a browser as a system administrator.

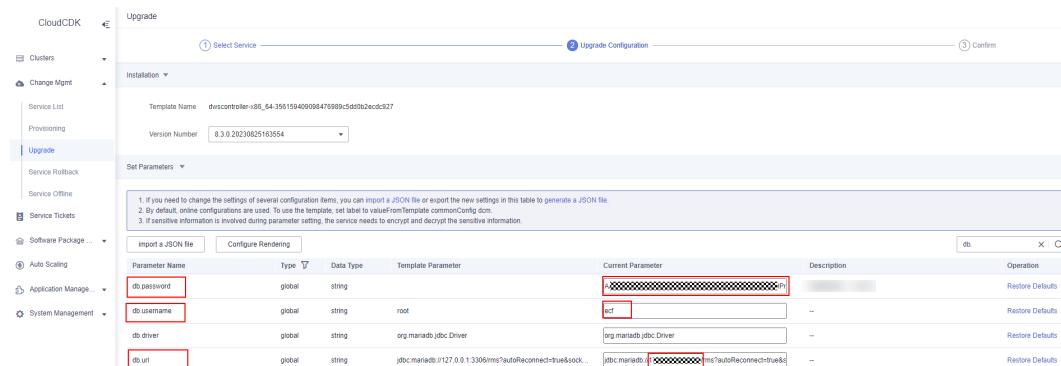
- URL: https://Address_for_accessing_CloudScope, for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op_cdk_sso**
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

Step 2 Choose **Services > Change Mgmt > CloudAutoDeploy-CDK**.

Step 3 In the navigation pane on the left, choose **Change Magmt & > Upgrade**, select the corresponding region, and select the cluster **ei-dbs-region**. Search for **dwscontroller** in the search box, select the corresponding dwscontroller, and click **Next**.



Step 4 Enter the keyword **db**. in the search box on the right and record the password ciphertext corresponding to **db.password**, username corresponding to **db.username**, and database IP address and port number corresponding to **db.url**.



Step 5 Decrypt the password ciphertext by referring to [Decrypting the Password Ciphertext](#) and record the decrypted password.

----End

2.2.3 1078853633 Missing Data Directory or Redo Log Directory on Data Instance (ALM_AI_MissingDataInstDataOrRedoDir)

Alarm Description

This alarm is generated when:

- The data directory on a data instance is deleted.
- The redo directory (`pg_xlog`) on a data instance is deleted.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078853633	Tenant Plane	Major	QoS alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, <code>cn_5001</code> .
Other Information	CloudService	Name of the cloud service for which the alarm is generated

Type	Parameter	Description
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When the data directory or redo directory on a data instance is missing, an alarm is reported and the data instance cannot be started. As a result, the cluster becomes abnormal after being started.

System Actions

- If the alarm is reported by a CN, the alarm will not be automatically handled.
- If the alarm is reported by a DN, handle it by referring to [1078919184 DN Process Abnormal \(ALM_AI_AbnormalDataNodeProcess\)](#).

Possible Causes

- The data directory on the data instance is deleted.
- The redo log directory (**pg_xlog**) on the data instance is deleted.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether the data directory or redo directory (**pg_xlog**) of the instance reporting the alarm is deleted.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

The following figure shows the query result. The **pg_xlog** directory in the data directory is the redo directory.

Step 3 Use the `gs_replace` script to recover a faulty CN or DataNode instance.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.4 1078919169 Data Instance Connections Exceed the Threshold (ALM_AI_TooManyDataInstConn)

Alarm Description

This alarm is generated when the number of client connections to a CN exceeds the threshold (specified by parameter **max_connections*connection_alarm_rate**) configured in the **postgresql.conf** file.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891916 9	Tenant plane	Major	QoS alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

New clients cannot connect to a CN.

System Actions

None

Possible Causes

The number of clients connected to a CN exceeds the threshold (specified by parameter **max_connections*connection_alarm_rate**) configured in the **postgresql.conf** file.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Increase the value of **max_connections** in the **postgresql.conf** configuration file of the CN instance reporting the alarm.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 dws]$ cm_ctl query -cvid
[ CMServer State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.181   1    /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2    /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
rebalancing : No
balanced : Yes

[ Coordinator State ]
node      node_ip      instance      state
1 host-10-0-16-47 10.0.16.67   5001 /DWS/data1/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
stance      state
-----
1 host-10-0-16-47 10.0.16.67   6001 /DWS/data1/hdnl/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /DWS/data1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
02 /DWS/data1/hdnl/dummy2 R Secondary Normal
1 host-10-0-16-38 10.0.16.70   6003 /DWS/data1/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6004 /DWS/data2/hdnl2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.108  30
03 /DWS/data2/hdnl2/dummy2 R Secondary Normal
2 host-10-0-16-38 10.0.16.70   6005 /DWS/data1/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6006 /DWS/data1/hdnl1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
04 /DWS/data1/hdnl1/dummy2 R Secondary Normal
2 host-10-0-16-47 10.0.16.67   6007 /DWS/data1/hdnl2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6008 /DWS/data2/hdnl2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
05 /DWS/data2/hdnl2/dummy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6009 /DWS/data1/hdnl1/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6010 /DWS/data1/hdnl1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
06 /DWS/data1/hdnl1/dummy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6011 /DWS/data2/hdnl2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70  6012 /DWS/data2/hdnl2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
07 /DWS/data2/hdnl2/dummy2 R Secondary Normal
```

For example, if the CN instance directory is **/DWS/data1/coordinator**, you can perform the following steps to modify the configuration:

vi /DWS/data1/coordinator/postgresql.conf

Find the **max_connections** parameter and increase its value based on the service scenario. The maximum value is **8388607**.

Run the following command to restart the instance (**node** indicates the host name of the faulty instance. Replace it with the actual host name):

gs_replace -t start -h node

Step 3 If the fault persists, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.5 1078919170 GTM Instance Abnormal (ALM_AI_AbnormalGTMInst)

Alarm Description

This alarm is generated when the primary GTM instance is disconnected from or asynchronous with the standby GTM instance.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919170	Tenant Plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the primary GTM instance is disconnected from the standby GTM instance and the primary GTM instance is working in synchronous mode, the system is unavailable for 120 seconds. After DWS detects the fault, it sets the mode of the primary GTM instance to HA. If the primary GTM instance is working in HA mode, the system works correctly.

NOTE

When the cluster is working correctly, the primary GTM instance works in synchronous mode and synchronizes received tasks to the standby instance in real time, ensuring consistency between the primary and standby instances. After the standby instance is faulty and cannot recover, the primary instance stops synchronizing tasks to the standby instance. The primary instance works in HA mode.

System Actions

In synchronous mode, if the primary GTM instance is disconnected from the standby GTM instance, DWS detects the fault within 120 seconds and automatically sends a command to set the primary GTM instance to the HA mode.

Possible Causes

The primary GTM instance is disconnected from the standby GTM instance.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether the primary and standby GTM instances of the cluster are faulty.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

The command output is displayed as follows:

Step 3 Check whether the network of the servers running the primary and standby GTM instances is normal. For example, the NIC used by the server running the primary or standby GTM instance is eth0, run the following command to observe packet loss and check whether the network is normal:

```
/sbin/ifconfig eth0
```

If the NIC is abnormal, rectify the fault.

Step 4 If the fault persists, contact technical support engineers.

-----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.6 1078919172 DN Abnormal (ALM_AI_AbnormalDatanodeInst)

Alarm Description

This alarm is generated when the primary DN is disconnected from the standby DN.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891917 2	Tenant Plane	Major	Environment alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The redo logs of the primary DataNode instance are automatically sent to the corresponding secondary DataNode instance, increasing the network pressure on the physical server running the secondary instance.

System Actions

When the primary DataNode instance is disconnected from the standby DataNode instance, the redo logs of the primary DataNode instance are automatically sent to the secondary DataNode instance, ensuring proper service operating.

Possible Causes

The primary DataNode instance is disconnected from the standby DataNode instance.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether the primary and standby DNs of the cluster are faulty.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 dws]$ cm_ctl query -cvid
[ CMServer State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.181    1   /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179    2   /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
rebalancing : No
balanced : Yes

[ Coordinator State ]
node      node_ip      instance      state
1 host-10-0-16-47 10.0.16.67    5001 /DWS/datal/coordinator Normal
2 host-10-0-16-38 10.0.16.70    5002 /DWS/datal/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.70    5002 /DWS/datal/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
3 host-10-0-16-57 10.0.16.108   1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70    1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
stance      state
-----
1 host-10-0-16-47 10.0.16.67    6001 /DWS/datal/hdnl/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70    6002 /DWS/datal/hdnl/standby1 S Standby Normal | 3 host-10-0-16-38 10.0.16.108   30
02 /DWS/datal/hdnl/dummy2 R Secondary Normal
host-10-0-16-47 10.0.16.67    6003 /DWS/datal/hdnl2/primary0 P Primary Normal | 3 host-10-0-16-38 10.0.16.108   6004 /DWS/datal/hdnl2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70    30
03 /DWS/datal/hdnl2/dummy1 R Secondary Normal
04 /DWS/datal/hdnl2/dummy2 R Secondary Normal
host-10-0-16-38 10.0.16.70    6005 /DWS/datal/hdnl1/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108   6006 /DWS/datal/hdnl1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67    30
05 /DWS/datal/hdnl1/dummy1 R Secondary Normal
06 /DWS/datal/hdnl1/dummy2 R Secondary Normal
host-10-0-16-57 10.0.16.108   6009 /DWS/datal/hdnl2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67   6008 /DWS/datal/hdnl2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108   30
07 /DWS/datal/hdnl2/dummy1 R Secondary Normal
3 host-10-0-16-57 10.0.16.108   6011 /DWS/datal/hdnl2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70    6010 /DWS/datal/hdnl1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70    30
07 /DWS/datal/hdnl1/dummy2 R Secondary Normal
3 host-10-0-16-47 10.0.16.67   6012 /DWS/datal/hdnl2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67    30
```

Step 3 Check whether the network of the servers running the primary and standby DataNode instances is normal. For example, the NIC used by the server running the primary or standby DataNode instance is eth0, run the following command to observe packet loss to check whether the network is normal:

```
/sbin/ifconfig eth0
```

If the NIC is abnormal, rectify the fault.

Step 4 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.7 1078919176 GTM Process Abnormal (ALM_AI_AbnormalGTMProcess)

Alarm Description

This alarm is generated when:

- The **gtm.conf** configuration file does not exist in the GTM instance data directory, or a parameter in the file is incorrectly configured.
- The GTM instance thread cannot monitor IP addresses or cannot be bound with a monitoring port.
- The GTM instance process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919176	Tenant Plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

- When the primary GTM instance fails to be started, DWS displays a startup failure message and the standby GTM instance becomes the primary one.
- When the standby GTM instance fails to be started, DWS displays a startup failure message but the system is still available. In this case, the primary GTM instance works in asynchronous mode.

System Actions

None

Possible Causes

- The **gtm.conf** configuration file does not exist in the GTM instance data directory, or a parameter in the file is incorrectly configured.
- The GTM instance thread cannot monitor IP addresses or cannot be bound with a monitoring port.
- The GTM instance process does not have the read or write permission on its data directory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If the GTM instance cannot be started, a log is recorded before the process exits. Go to the log directory to view the instance log, find the cause of the startup failure, and perform operations based on the log information.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance node in the tenant cluster based on the instance name. Perform this operation as user **Ruby**.

Run the following command to check the cluster status:

cm_ctl query -Cvd

As shown in the following figure, GTM 1002 is abnormal (the cluster has not been automatically downgraded).

```
[ CRServer State ]
node ..... instance ..... state
2 host-172-16-27-248 1 /DWS/data1/cm/cm_server Primary
3 host-172-16-49-123 2 /DWS/data1/cm/cm_server Standby

[ Cluster State ]
cluster_state : Unavailable
redistributing : No
balanced : Yes

[ Coordinator State ]
node ..... instance ..... state
1 host-172-16-57-242 5081 /DWS/data1/coordinator Normal
2 host-172-16-27-248 5082 /DWS/data1/coordinator Normal
3 host-172-16-49-123 5083 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node ..... instance ..... state
3 host-172-16-49-123 5083 /DWS/data1/coordinator Normal

[ GTM State ]
node ..... instance ..... state ..... sync_state
3 host-172-16-49-123 1001 /DWS/manager/gtm P Primary Connection bad Sync
2 host-172-16-27-248 1002 /DWS/manager/gtm S Down Disk damaged Sync

[ Datanode State ]
node ..... instance ..... state | node ..... instance ..... state | node ..... instance ..... state
1 host-172-16-57-248 5081 /DWS/data1/hdn01/primary0 P Primary Normal | 2 host-172-16-27-248 5082 /DWS/data2/hdn01/standby1 S Standby Normal | 3 host-172-16-49-123 3082 /DWS/data2/hdn01/dummy2 R Secondary Normal
2 host-172-16-27-248 5083 /DWS/data1/hdn01/primary0 P Primary Normal | 3 host-172-16-49-123 5083 /DWS/data2/hdn01/standby1 S Standby Normal | 1 host-172-16-57-242 3083 /DWS/data2/hdn01/dummy2 R Secondary Normal
3 host-172-16-49-123 3080 /DWS/data1/hdn01/secondary0 S Secondary Normal | 4 host-172-16-57-242 3081 /DWS/data2/hdn01/secondary0 S Secondary Normal
```

Go to the cluster log directory.

cd \$GAUSSLOG

View the structure of the current directory.

ls

Information similar to the following is displayed.

```
bin cm gs_obs gs_profile om pg_audit pg_log
```

Go to the **pg_log/gtm/** and **cm/cm_agent** directories and view logs to obtain more location information.

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.8 1078919177 CN Process Abnormal (ALM_AI_AbnormalCoordinatorProcess)

Alarm Description

This alarm is generated when:

- The **postgresql.conf** configuration file does not exist in the CN instance data directory, or a parameter in the file is incorrectly configured.
- The CN instance thread cannot monitor IP addresses or be bound with a monitoring port.

- The CN instance process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919177	Tenant Plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When the CN instance fails to be started, DWS displays a startup failure message and the database system cannot use the data definition language (DDL) statements anymore. However, the data manipulation language (DML) statements can be normally used.

System Actions

None

Possible Causes

- The **postgresql.conf** configuration file does not exist in the CN instance data directory, or a parameter in the file is incorrectly configured.
- The CN instance thread cannot monitor IP addresses or be bound with a monitoring port.
- The CN instance process does not have the read or write permission on its data directory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If the CN instance cannot be started, a log is recorded before the process exits. Go to the log directory to view the log of the CN instance, find the cause of the startup failure, and perform operations based on the log.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance node in the tenant cluster based on the instance name. Perform this operation as user **Ruby**.

Run the following command to check the cluster status:

cm_ctl query -Cvd

As shown in the following figure, Coordinator 5002 is abnormal (the cluster is in the degraded state).

```
[ CHServer State ]
node           instance          state
2 host-172-16-27-242 5001 /DWS/manager/cm/cm_server Primary
3 host-172-16-49-123 2 /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Degraded
redistributing : No
balanced : Yes

[ Coordinator State ]
node           instance          state
1 host-172-16-57-242 5001 /DWS/data1/coordinator Normal
2 host-172-16-27-240 5002 /DWS/data1/coordinator Down
3 host-172-16-49-123 5003 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node           instance          state
3 host-172-16-49-123 5003 /DWS/data1/coordinator Normal

[ GTM State ]
node           instance          state          sync_state
3 host-172-16-49-123 1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-172-16-27-240 1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node           instance          state | node           instance          state | node           instance          state | node           instance          state
1 host-172-16-57-242 6001 /DWS/data1/hdnn1/primary P Primary Normal | 2 host-172-16-27-240 6002 /DWS/data2/hdnn1/standby S Standby Normal | 3 host-172-16-49-123 3003 /DWS/data2/hdnn1/dummy2 R Secondary Normal
2 host-172-16-27-240 6003 /DWS/data2/hdnn1/primary P Primary Normal | 3 host-172-16-49-123 6004 /DWS/data2/hdnn1/standby S Standby Normal | 1 host-172-16-57-242 3002 /DWS/data2/hdnn1/dummy2 R Secondary Normal
3 host-172-16-49-123 6005 /DWS/data2/hdnn1/primary P Primary Normal | 1 host-172-16-57-242 6006 /DWS/data2/hdnn1/standby S Standby Normal | 2 host-172-16-27-240 6004 /DWS/data2/hdnn1/dummy2 R Secondary Normal
```

Go to the cluster log directory.

cd \$GAUSSLOG

View the structure of the current directory.

ls

Information similar to the following is displayed.

```
bin  cm  gs_obs  gs_profile  om  pg_audit  pg_log
```

Go to the **pg_log/cn_5002/** and **cm/cm_agent** directories and view logs to obtain more location information.

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.9 1078919184 DN Process Abnormal (ALM_AI_AbnormalDatanodeProcess)

Alarm Description

This alarm is generated when:

- The **postgresql.conf** configuration file does not exist in the DataNode instance data directory, or a parameter in the file is incorrectly configured.
- The DataNode instance thread cannot monitor IP addresses or be bound with a monitoring port.

- The DataNode instance process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919184	Tenant plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

- When the primary DataNode instance fails to be started, the system reports the failure. After 120 seconds, DWS switches the standby DataNode instance to the primary one, maintaining system availability.
- When the standby DataNode instance fails to be started, the system reports the failure but remains available.

System Actions

- When the primary DataNode instance fails to be started, DWS switches the standby DataNode instance to the primary one after 120 seconds, maintaining system availability.
- When the standby DataNode instance fails to be started, redo logs of the primary DataNode instance are automatically sent to the secondary DataNode instance.

Possible Causes

- The **postgresql.conf** configuration file does not exist in the DataNode instance data directory, or a parameter in the file is incorrectly configured.
- The DataNode instance thread cannot monitor IP addresses or be bound with a monitoring port.
- The DataNode instance process does not have the read or write permission on its data directory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If the DataNode instance cannot be started, a log is recorded before the process exits. Go to the log directory to view the log of the DataNode instance, find the cause of the startup failure, and perform operations based on the log.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance node in the tenant cluster based on the instance name. Perform this operation as user **Ruby**.

Run the following command to check the cluster status:

cm_ctl query -Cvd

As shown in the following figure, Datanode 6002 is abnormal (the cluster is in the degraded state).

Go to the cluster log directory.

cd \$GAUSSLOG

View the structure of the current directory.

ls

Information similar to the following is displayed.

```
bin  cm  gs_obs  gs_profile  om  pg_audit  pg_log
```

Go to the **pg_log/dn_6002** and **cm/cm_agent** directories and view logs to obtain more location information.

Step 3 If the fault persists, contact technical support engineers.

-----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.10 1078919221 Cluster Table Skew (ALM_AI_AbnormalTableSkewness)

Alarm Description

This alarm is generated when the data of the target DN is skewed after being imported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919221	Tenant plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the table is skewed, the disk usage of some DNs may increase sharply. As a result, the disk space is full and cluster functions are affected.

System Actions

None

Possible Causes

- Inappropriate distribution key
- Skewed data

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 If the fault is caused by an improper distribution key, reselect one based on the following principles:

1. **The values of the distribution key should be discrete so that data can be evenly distributed on each DN.**
2. **Do not select the column where a constant filter exists.** For example, if a constant constraint (for example, zqdh= '000001') exists on the **zqdh** column

in some queries on the **dwcjk** table, you are not advised to use **zqdh** as the distribution key.

3. **With the above principles met, you can select join conditions as distribution keys**, so that join tasks can be pushed down to DNs for execution, reducing the amount of data transferred between the DNs.

For a hash table, an inappropriate distribution key may cause data skew or poor I/O performance on certain DNs. Therefore, you need to check the table to ensure that data is evenly distributed on each DN. You can run the following SQL statements to check data skew:

```
select  
xc_node_id, count(1)  
from tablename  
group by xc_node_id  
order by xc_node_id desc;
```

xc_node_id corresponds to a DN. Generally, **over 5% difference between the amount of data on different DNs is regarded as data skew. If the difference is over 10%, choose another distribution column.**

4. You are not advised to add a column as a distribution key, especially not to add a column with sequence values as the distribution key. (Sequences may cause performance bottlenecks and unnecessary maintenance costs.)

Step 3 If data itself is skewed, increase the disk space.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.11 1078919224 Imbalanced Cluster Load (ALM_AI_UnbalancedCluster)

Alarm Description

This alarm is generated when the primary/standby relationship of instances in a cluster changes to be different from that during initial installation of the cluster.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919224	Tenant plane	Major	Environment	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the alarm is reported, the primary and standby GTMs or DataNodes switch over in the cluster, and the new primary/standby relationship is different from the initial status. In this case, primary instances in the cluster may be excessively switched over to a node, causing unbalanced cluster loads and deteriorating cluster performance.

System Actions

None

Possible Causes

The primary/standby relationship of the DataNode instances is abnormal.

- The primary DataNode instance is faulty and cannot provide services.
- The primary and standby DNs are disconnected.
- A DN switchover is manually performed.

The primary/standby relationship of the GTM instances is abnormal.

- The primary GTM instance is faulty and cannot provide services.
- The primary and standby GTM instances are disconnected.
- The primary and standby GTM instances are manually switched over.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the sandbox of any node in the cluster as user **Ruby** and run the following command to check the current cluster status:

cm_ctl query -Cvid

Step 3 If the values of **cluster_state** and **balanced** are **Normal** and **No** respectively, the cluster is in the **Normal** state, but the roles of the primary and standby instances have been switched. **P** in **Datanode State** indicates that the initial DataNode state is primary, and **Standby Normal** indicates that the current state of the DataNode is standby.

```
[ CMServer State ]  
node      node_ip     instance          state  
-----  
1 SZX1000071373 10.90.57.221 1 /opt/huawei/Bigdata/mppdb/cm/cm_server    Primary  
2 SZX1000071374 10.90.57.222 2 /opt/huawei/Bigdata/mppdb/cm/cm_server    Standby
```

```
[ Cluster State ]
```

```
cluster_state : Normal  
redistributing : No  
balanced       : No
```

```
[ Coordinator State ]
```

node	node_ip	instance	state				
1	SZX1000071373	10.90.57.221	5001 /srv/BigData/mppdb/data1/coordinator				
2	SZX1000071374	10.90.57.222	5002 /srv/BigData/mppdb/data1/coordinator				
3	SZX1000071375	10.90.57.223	5003 /srv/BigData/mppdb/data1/coordinator				
[Central Coordinator State]							
node	node_ip	instance	state				
2	SZX1000071374	10.90.57.222	5002 /srv/BigData/mppdb/data1/coordinator Normal				
[GTM State]							
node	node_ip	instance	state	sync_state			
2	SZX1000071374	10.90.57.222	1001 /opt/huawei/Bigdata/mppdb/gtm	P Primary Connection ok Sync			
1	SZX1000071373	10.90.57.221	1002 /opt/huawei/Bigdata/mppdb/gtm	S Standby Connection ok Sync			
[Datanode State]							
node	node_ip	instance	state	state	node	node_ip	node_ip
instance	state	state	node	node_ip	instance	node_ip	node_ip
1	SZX1000071373	10.90.57.221	6001 /srv/BigData/mppdb/data1/master1	P Primary	Normal	2	
SZX1000071374	10.90.57.222	6002 /srv/BigData/mppdb/data1/slave1	S Standby	Normal	3		
SZX1000071375	10.90.57.223	3002 /srv/BigData/mppdb/data1/dummyslave1	R Secondary	Normal			
1	SZX1000071373	10.90.57.221	6003 /srv/BigData/mppdb/data2/master2	P Primary	Normal	3	
SZX1000071375	10.90.57.223	6004 /srv/BigData/mppdb/data2/slave2	S Standby	Normal	2		
SZX1000071374	10.90.57.222	3003 /srv/BigData/mppdb/data2/dummyslave2	R Secondary	Normal			
1	SZX1000071373	10.90.57.221	6005 /srv/BigData/mppdb/data3/master3	P Primary	Normal	2	
SZX1000071374	10.90.57.222	6006 /srv/BigData/mppdb/data3/slave3	S Standby	Normal	3		
SZX1000071375	10.90.57.223	3004 /srv/BigData/mppdb/data3/dummyslave3	R Secondary	Normal			
1	SZX1000071373	10.90.57.221	6007 /srv/BigData/mppdb/data4/master4	P Primary	Normal	3	
SZX1000071375	10.90.57.223	6008 /srv/BigData/mppdb/data4/slave4	S Standby	Normal	2		
SZX1000071374	10.90.57.222	3005 /srv/BigData/mppdb/data4/dummyslave4	R Secondary	Normal			
2	SZX1000071374	10.90.57.222	6009 /srv/BigData/mppdb/data1/master1	P Primary	Normal	3	
SZX1000071375	10.90.57.223	6010 /srv/BigData/mppdb/data1/slave1	S Standby	Normal	1		
SZX1000071373	10.90.57.221	3006 /srv/BigData/mppdb/data1/dummyslave1	R Secondary	Normal			
2	SZX1000071374	10.90.57.222	6011 /srv/BigData/mppdb/data2/master2	P Standby Normal	1		
SZX1000071373	10.90.57.221	6012 /srv/BigData/mppdb/data2/slave2	S Standby	Normal	3		
SZX1000071375	10.90.57.223	3007 /srv/BigData/mppdb/data2/dummyslave2	R Secondary	Normal			
2	SZX1000071374	10.90.57.222	6013 /srv/BigData/mppdb/data3/master3	P Primary	Normal	3	
SZX1000071375	10.90.57.223	6014 /srv/BigData/mppdb/data3/slave3	S Standby	Normal	1		
SZX1000071373	10.90.57.221	3008 /srv/BigData/mppdb/data3/dummyslave3	R Secondary	Normal			
2	SZX1000071374	10.90.57.222	6015 /srv/BigData/mppdb/data4/master4	P Primary	Normal	1	
SZX1000071373	10.90.57.221	6016 /srv/BigData/mppdb/data4/slave4	S Standby	Normal	3		
SZX1000071375	10.90.57.223	3009 /srv/BigData/mppdb/data4/dummyslave4	R Secondary	Normal			
3	SZX1000071375	10.90.57.223	6017 /srv/BigData/mppdb/data1/master1	P Primary	Normal	1	
SZX1000071373	10.90.57.221	6018 /srv/BigData/mppdb/data1/slave1	S Standby	Normal	2		
SZX1000071374	10.90.57.222	3010 /srv/BigData/mppdb/data1/dummyslave1	R Secondary	Normal			
3	SZX1000071375	10.90.57.223	6019 /srv/BigData/mppdb/data2/master2	P Primary	Normal	2	
SZX1000071374	10.90.57.222	6020 /srv/BigData/mppdb/data2/slave2	S Standby	Normal	1		
SZX1000071373	10.90.57.221	3011 /srv/BigData/mppdb/data2/dummyslave2	R Secondary	Normal			
3	SZX1000071375	10.90.57.223	6021 /srv/BigData/mppdb/data3/master3	P Primary	Normal	1	
SZX1000071373	10.90.57.221	6022 /srv/BigData/mppdb/data3/slave3	S Standby	Normal	2		
SZX1000071374	10.90.57.222	3012 /srv/BigData/mppdb/data3/dummyslave3	R Secondary	Normal			
3	SZX1000071375	10.90.57.223	6023 /srv/BigData/mppdb/data4/master4	P Primary	Normal	2	
SZX1000071374	10.90.57.222	6024 /srv/BigData/mppdb/data4/slave4	S Standby	Normal	1		
SZX1000071373	10.90.57.221	3013 /srv/BigData/mppdb/data4/dummyslave4	R Secondary	Normal			

Switch the cluster to the balanced state after step **Step 5** during off-peak hours.

- Step 4** If the value of **cluster_state** is **Degraded** and the value of **balanced** is **No**, the cluster is not restored after the primary and standby instances are switched over.

```
[ CMServer State ]
node      node_ip    instance          state
-----1 SZX1000071373 10.90.57.221 1 /opt/huawei/Bigdata/mppdb/cm/cm_server Primary
2 SZX1000071374 10.90.57.222 2 /opt/huawei/Bigdata/mppdb/cm/cm_server Standby

[ Cluster State ]
cluster_state : Degraded
redistributing : No
balanced : No

[ Coordinator State ]
node      node_ip    instance          state
-----1 SZX1000071373 10.90.57.221 5001 /srv/BigData/mppdb/data1/coordinator Normal
2 SZX1000071374 10.90.57.222 5002 /srv/BigData/mppdb/data1/coordinator Normal
3 SZX1000071375 10.90.57.223 5003 /srv/BigData/mppdb/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip    instance          state
-----2 SZX1000071374 10.90.57.222 5002 /srv/BigData/mppdb/data1/coordinator Normal

[ GTM State ]
node      node_ip    instance          state      sync_state
-----2 SZX1000071374 10.90.57.222 1001 /opt/huawei/Bigdata/mppdb/gtm P Primary Connection ok Sync
1 SZX1000071373 10.90.57.221 1002 /opt/huawei/Bigdata/mppdb/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip    instance          state      | node      state      | node      node_ip
instance   state           | node      node_ip   instance
-----state
-----1 SZX1000071373 10.90.57.221 6001 /srv/BigData/mppdb/data1/master1 P Primary Normal | 2
SZX1000071374 10.90.57.222 6002 /srv/BigData/mppdb/data1/slave1 S Standby Normal | 3
SZX1000071375 10.90.57.223 3002 /srv/BigData/mppdb/data1/dummyslave1 R Secondary Normal
1 SZX1000071373 10.90.57.221 6003 /srv/BigData/mppdb/data2/master2 P Primary Normal | 3
SZX1000071375 10.90.57.223 6004 /srv/BigData/mppdb/data2/slave2 S Standby Normal | 2
SZX1000071374 10.90.57.222 3003 /srv/BigData/mppdb/data2/dummyslave2 R Secondary Normal
1 SZX1000071373 10.90.57.221 6005 /srv/BigData/mppdb/data3/master3 P Primary Normal | 2
SZX1000071374 10.90.57.222 6006 /srv/BigData/mppdb/data3/slave3 S Standby Normal | 3
SZX1000071375 10.90.57.223 3004 /srv/BigData/mppdb/data3/dummyslave3 R Secondary Normal
1 SZX1000071373 10.90.57.221 6007 /srv/BigData/mppdb/data4/master4 P Primary Normal | 3
SZX1000071375 10.90.57.223 6008 /srv/BigData/mppdb/data4/slave4 S Standby Normal | 2
SZX1000071374 10.90.57.222 3005 /srv/BigData/mppdb/data4/dummyslave4 R Secondary Normal
2 SZX1000071374 10.90.57.222 6009 /srv/BigData/mppdb/data1/master1 P Down Disk damaged /
3 SZX1000071375 10.90.57.223 6010 /srv/BigData/mppdb/data1/slave1 S Primary Normal | 1
SZX1000071373 10.90.57.221 3006 /srv/BigData/mppdb/data1/dummyslave1 R Secondary Normal
2 SZX1000071374 10.90.57.222 6011 /srv/BigData/mppdb/data2/master2 P Primary Normal | 1
SZX1000071373 10.90.57.221 6012 /srv/BigData/mppdb/data2/slave2 S Standby Normal | 3
SZX1000071375 10.90.57.223 3007 /srv/BigData/mppdb/data2/dummyslave2 R Secondary Normal
2 SZX1000071374 10.90.57.222 6013 /srv/BigData/mppdb/data3/master3 P Primary Normal | 3
SZX1000071375 10.90.57.223 6014 /srv/BigData/mppdb/data3/slave3 S Standby Normal | 1
SZX1000071373 10.90.57.221 3008 /srv/BigData/mppdb/data3/dummyslave3 R Secondary Normal
2 SZX1000071374 10.90.57.222 6015 /srv/BigData/mppdb/data4/master4 P Primary Normal | 1
SZX1000071373 10.90.57.221 6016 /srv/BigData/mppdb/data4/slave4 S Standby Normal | 3
SZX1000071375 10.90.57.223 3009 /srv/BigData/mppdb/data4/dummyslave4 R Secondary Normal
3 SZX1000071375 10.90.57.223 6017 /srv/BigData/mppdb/data1/master1 P Primary Normal | 1
SZX1000071373 10.90.57.221 6018 /srv/BigData/mppdb/data1/slave1 S Standby Normal | 2
SZX1000071374 10.90.57.222 3010 /srv/BigData/mppdb/data1/dummyslave1 R Secondary Normal
3 SZX1000071375 10.90.57.223 6019 /srv/BigData/mppdb/data2/master2 P Primary Normal | 2
```

```
SZX1000071374 10.90.57.222 6020 /srv/BigData/mppdb/data2/slave2 S Standby Normal | 1
S ZX1000071373 10.90.57.221 3011 /srv/BigData/mppdb/data2/dummyslave2 R Secondary Normal
3 SZX1000071375 10.90.57.223 6021 /srv/BigData/mppdb/data3/master3 P Primary Normal | 1
S ZX1000071373 10.90.57.221 6022 /srv/BigData/mppdb/data3/slave3 S Standby Normal | 2
S ZX1000071374 10.90.57.222 3012 /srv/BigData/mppdb/data3/dummyslave3 R Secondary Normal
3 SZX1000071375 10.90.57.223 6023 /srv/BigData/mppdb/data4/master4 P Primary Normal | 2
S ZX1000071374 10.90.57.222 6024 /srv/BigData/mppdb/data4/slave4 S Standby Normal | 1
S ZX1000071373 10.90.57.221 3013 /srv/BigData/mppdb/data4/dummyslave4 R Secondary Normal
```

The status of **dn_6009** is **Down Disk damaged**, and the status of standby **dn_6010** is **Primary Normal**. As a result, the number of primary DataNode increases on node **SZX1000071374**.

Run the **gs_replace** command to restore the damaged **dn_6009**. Note that the restoration consists of two steps: **config** and **start**. Specify the host name of the node where **dn_6009** resides after **-h**.

```
> gs_replace -t config -h SZX1000071374
Fixing all the CMAgents instances.
There are [0] CMAgents need to be repaired in cluster.
Configuring replacement instances.
Successfully configured replacement instances.
Successfully fixed all the CMAgents instances.
Configuring
Waiting for promote peer instances.
.
Successfully upgraded standby instances.
Deleting failed CN from pgxc_node.
No CN needs to be fixed.
Configuring replacement instances.
Successfully configured replacement instances.
Setting the SCTP.
Successfully set the SCTP.
Configuration succeeded.

> gs_replace -t start -h SZX1000071374
Starting.
=====
Successfully started instance process. Waiting to become Normal.
=====
.
=====
Start succeeded on all nodes.
Start succeeded.
```

Check the cluster status. The expected status is **Normal**.

cm_ctl query -Cv

```
[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced : No
```

Switch the cluster to the balanced state after step **Step 5** during off-peak hours.

NOTE

1. The DataNode switchover serves as an example. The handling method is the same for GTM instance switchover.
2. If instances on multiple nodes are abnormal, run the **gs_replace** command to rectify the fault one by one.

Step 5 Run the following command to check the CN port number of the cluster:

cm_ctl query -Cvp

```
[ Coordinator State ]  
node      instance state  
-----  
1 SZX1000071373 5001 8000 Normal  
2 SZX1000071374 5002 8000 Normal  
3 SZX1000071375 5003 8000 Normal
```

The preceding command output is used as an example. The port number of the CN is 8000.

Log in to the sandbox of any CN node as user **Ruby** and run the following command:

```
gsql postgresql://:8000/postgres?application_name='OM' -r -c "checkpoint;"
```

```
CHECKPOINT
```

Switch the cluster to the balanced state.

```
cm_ctl switchover -a
```

```
cm_ctl: cmserver is rebalancing the cluster automatically.
```

```
.....
```

```
cm_ctl: switchover successfully.
```

Check the cluster status again.

```
cm_ctl query -Cv
```

```
[ Cluster State ]
```

```
cluster_state : Normal  
redistributing : No  
balanced : Yes
```

Step 6 Wait for a while and check whether the alarm is automatically cleared. If the alarm persists, contact technical support for assistance.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.12 1078919226 CM_Agent Process Abnormal (ALM_AI_AbnormlCMAProcess)

Alarm Description

This alarm is generated when:

- The **cm.conf** configuration file does not exist in the CM_AGENT process.
- The CM_AGENT instance process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891922 6	Tenant plane alarm	Major	Environment alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When the CM_AGENT instance fails to be started, DWS displays a startup failure message. The database system functions properly if no other exceptions occur. However, users or the administrator cannot obtain accurate information about the cluster status.

System Actions

None

Possible Causes

- The **cm.conf** configuration file does not exist in the CM_AGENT process.
- The CM_AGENT instance process does not have the read or write permission on its data directory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance node in the tenant cluster based on the instance name. Perform this operation as user **Ruby**.

Run the following command to check the cluster status:

cm_ctl query -Cvd

The following figure shows the query result. If all instances on the **host-172-16-49-123** node are abnormal (the cluster is in the degraded state), the **cm_agent** process may be abnormal.

```
[ CMServer State ]
node           instance          state
2 host-172-16-27-240 1 /DWS/manager/cm/cm_server Primary
3 host-172-16-49-123 2 /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster state : Degraded
repartitioning : No
balanced      : No

[ Coordinator State ]
node           instance          state
1 host-172-16-57-242 5001 /DWS/data1/coordinator Normal
2 host-172-16-27-240 5002 /DWS/data1/coordinator Normal
3 host-172-16-49-123 5003 /DWS/data1/coordinator Down

[ Central Coordinator State ]
node           instance          state
2 host-172-16-27-240 5002 /DWS/data1/coordinator Normal

[ GTM State ]
node           instance          state      sync_state
3 host-172-16-49-123 1001 /DWS/manager/gtm P Down Unknown Sync
2 host-172-16-27-240 1002 /DWS/manager/gtm S Primary Connection bad Most available

[ Datanode State ]
node           instance          state      | node           instance          state      | node           instance          state
1 host-172-16-57-242 6003 /DWS/data2/h2dn1/primer0 P Primary Normal | host-172-16-27-240 6004 /DWS/data2/h2dn1/xstandby1 S Standby Normal | host-172-16-49-123 3003 /DWS/data2/h2dn1/dummy2 R Secondary Unknown
2 host-172-16-27-240 6003 /DWS/data2/h2dn1/primer0 P Primary Normal | 3 host-172-16-49-123 6004 /DWS/data2/h2dn1/xstandby1 S Down Unknown | 1 host-172-16-57-242 3003 /DWS/data2/h2dn1/dummy2 R Secondary Normal
3 host-172-16-49-123 6005 /DWS/data2/h2dn1/primer0 P Down Unknown | 1 host-172-16-57-242 6006 /DWS/data2/h2dn1/primer0 P Primary Normal | 2 host-172-16-27-240 3004 /DWS/data2/h2dn1/dummy2 R Secondary Normal
```

Replace **cm_server** at the end of the cm_server data directory with **cm_agent** to obtain the data directory of cm_agent, that is, **/DWS/manager/cm/cm_agent**.

- Step 3** Check whether user **Ruby** has the permission to access the cm_agent data directory **/DWS/manager/cm/cm_agent**. If user **Ruby** does not have the permission, run the **chmod** command to grant the permission to user **Ruby**. Check whether the **cm.conf** configuration file exists in the directory. If the file does not exist, run the **gs_replace** command to restore the instance.

```
gs_replace -t config -h host-172-16-49-123 && gs_replace -t start -h host-172-16-49-123
```

- Step 4** Check whether the cluster status is normal. If the fault is rectified, go to the cluster log directory.

```
cd $GAUSSLOG
```

View the structure of the current directory.

```
ls
```

Information similar to the following is displayed.

```
bin  cm  gs_obs  gs_profile  om  pg_audit  pg_log
```

Go to the **cm/cm_agent** and **cm/om_monitor** directories and view logs to obtain more location information.

- Step 5** If the fault persists, contact technical support.

```
----End
```

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.13 1078919227 CM_Server Process Abnormal (ALM_AI_AbnormalCMSProcess)

Alarm Description

This alarm is generated when:

- The **cm.conf** configuration file does not exist in the **CM_SERVER** process.
- The CM_SERVER instance process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919227	Tenant plane alarm	Major	Environment alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated

Type	Parameter	Description
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When the CM_SERVER instance fails to be started, DWS displays a startup failure message. The database system functions properly if no other exceptions occur. However, users or the administrator cannot obtain accurate information about the cluster status.

System Actions

None

Possible Causes

- The **cm.conf** configuration file does not exist in the **CM_SERVER** process.
- The **CM_SERVER** instance process does not have the read or write permission on its data directory.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance node in the tenant cluster based on the instance name. Perform this operation as user **Ruby**.

Run the following command to check the cluster status:

cm_ctl query -Cvd

The following figure shows the query result, indicating that all **cm_server** processes on the **host-172-16-49-123** node are abnormal (the cluster is still in the normal state).

```
[ CMServer State ]
node           instance      state
2 host-172-16-27-240 1 /DNS/manager/cm/cm_server Primary
3 host-172-16-49-123 2 /DNS/manager/cm/cm_server Down

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced       : Yes

[ Coordinator State ]
node           instance      state
1 host-172-16-57-242 5001 /DNS/data1/coordinator Normal
2 host-172-16-27-240 5002 /DNS/data1/coordinator Normal
3 host-172-16-49-123 5003 /DNS/data1/coordinator Normal

[ Central Coordinator State ]
node           instance      state
3 host-172-16-49-123 5003 /DNS/data1/coordinator Normal

[ GTM State ]
node           instance      state      sync_state
3 host-172-16-49-123 1001 /DNS/manager/gtm P Primary Connection ok Sync
2 host-172-16-27-240 1002 /DNS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node           instance      state      | node           instance      state      | node           instance      state
1 host-172-16-57-242 6001 /DNS/data1/hdn1/priary0 P Primary Normal | 2 host-172-16-27-240 6002 /DNS/data2/hdn1/standby1 S Standby Normal | 3 host-172-16-49-123 6002 /DNS/data2/hdn1/dummy2 R Secondary Normal
2 host-172-16-27-240 6002 /DNS/data1/hdn1/priary0 P Primary Normal | 3 host-172-16-49-123 6004 /DNS/data2/hdn1/standby1 S Standby Normal | 1 host-172-16-57-242 3002 /DNS/data2/hdn1/dummy2 R Secondary Normal
3 host-172-16-49-123 6005 /DNS/data2/hdn1/priary0 P Primary Normal | 1 host-172-16-57-242 6005 /DNS/data2/hdn1/standby1 S Standby Normal | 2 host-172-16-27-240 3004 /DNS/data2/hdn1/dummy2 R Secondary Normal
```

Replace **cm_server** at the end of the **cm_server** data directory with **cm_agent** to obtain the data directory of **cm_agent**, that is, **/DWS/manager/cm/cm_agent**.

Step 3 Check whether user **Ruby** has the permission to access the **cm_server** data directory (**/DWS/manager/cm/cm_server**) and **cm_agent** data directory (**/DWS/manager/cm/cm_agent**). If it does not, run the **chmod** command to modify the permission.

Check whether the **cm.conf** configuration file exists in the **cm_agent** directory (**cm_server** and **cm_agent** use the same configuration file). If the configuration file does not exist, run the **gs_replace** command to restore the instance.

gs_replace -t config -h host-172-16-49-123 && gs_replace -t start -h host-172-16-49-123

Step 4 Check whether the cluster status is normal. If the fault is rectified, go to the cluster log directory.

cd \$GAUSSLOG

View the structure of the current directory.

ls

Information similar to the following is displayed.

```
bin  cm  gs_obs  gs_profile  om  pg_audit  pg_log
```

Go to the **cm/cm_agent** and **cm/cm_server** directories and view logs to obtain more location information.

Step 5 If the fault persists, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.14 1078919231 Inconsistent MTU Values (ALM_AI_AbnormalMTUValue)

Alarm Description

This alarm is generated when the MTU values of NICs corresponding to nodes' service IP addresses in a cluster are inconsistent.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919231	Tenant plane alarm	Major	Environment alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated

Type	Parameter	Description
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When the MTU values are inconsistent, the communication between DWS nodes becomes abnormal, and the basic functions and O&M operations of the database cluster may fail or time out.

System Actions

None

Possible Causes

- After the OS is restarted, the MTU value of an instance is set to the default value, which is different from the MTU value of other nodes in the cluster.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 - Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Access the instance for which the alarm is reported and change its MTU value to be the same as the MTU value of other instances.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 data1]# cm_ctl query -Cvid
[ CMServer State ]
node      node_ip      instance      state
-----+
2 host-10-0-16-38 10.0.16.181 1    /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179 2    /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced      : Yes

[ Coordinator State ]
node      node_ip      instance      state
-----+
1 host-10-0-16-47 10.0.16.67 5001 /DWS/data1/coordinator Normal
2 host-10-0-16-38 10.0.16.70 5002 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
-----+
2 host-10-0-16-38 10.0.16.70 5002 /DWS/data1/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
-----+
3 host-10-0-16-57 10.0.16.108 1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70 1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
-----+
1 host-10-0-16-47 10.0.16.67 6001 /DWS/data1/hdn1/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70 6002 /DWS/data1/hdn1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108 6004 /DWS/data2/hdn2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70 6004 /DWS/data2/hdn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70 6005 /DWS/data1/hdn1/primary1 P Primary Normal | 3 host-10-0-16-57 10.0.16.108 6006 /DWS/data1/hdn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67 6006 /DWS/data1/hdn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67 6007 /DWS/data2/hdn2/primary1 P Primary Normal | 1 host-10-0-16-47 10.0.16.67 6008 /DWS/data2/hdn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108 6008 /DWS/data2/hdn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108 6009 /DWS/data1/hdn1/primary2 P Primary Normal | 1 host-10-0-16-47 10.0.16.67 6010 /DWS/data1/hdn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70 6010 /DWS/data1/hdn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70 6011 /DWS/data2/hdn2/primary2 P Primary Normal | 2 host-10-0-16-38 10.0.16.70 6012 /DWS/data2/hdn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67 6012 /DWS/data2/hdn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67 6013 /DWS/data1/hdn1/secondary2 R Secondary Normal
```

Run the following command to change the MTU value (assume that the NIC name is eth0 and the MTU value is 1500):

/sbin/ifconfig eth0 mtu 1500

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.15 1078919239 Abnormal DataNode Disk (ALM_AI_AbnormalDataInstDisk)

Alarm Description

This alarm is generated when the disk used by a DN instance is damaged.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919239	Tenant plane alarm	Major	Device alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The database can still be used, but its overall performance will be affected.

System Actions

The DN using the damaged disk will copy data from its backup node to restore data, but the restored data may still be written on the damaged disk page.

Possible Causes

The disk is faulty.

Handling Procedure

Replace the disk immediately.

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.16 1078919242 Failed to Create Connection for Database Service (ALM_AI_AbnormalPhonyDead)

Alarm Description

This alarm is generated when CM_AGENT fails to connect to the GTM, DN, or CN for multiple times.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891924 2	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The instance will be restarted and a primary/standby CN, DN, or GTM switchover will occur.

System Actions

None

Possible Causes

The memory and I/O of the node where the faulty instance resides are used up.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Go to the log directory where the instance generating the alarm resides, view the log, and perform operations instructed by the log.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 data1]# cm_ctl query -cvid
[ CMServer State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.181   1    /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2    /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
rebalancing : No
balanced : Yes

[ Coordinator State ]
node      node_ip      instance      state
1 host-10-0-16-47 10.0.16.67   5001 /DWS/data1/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
stance      state
-----
1 host-10-0-16-47 10.0.16.67   6001 /DWS/data1/hdnl/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /DWS/data1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
02 /DWS/data1/hdnl/dummy2 R Secondary Normal
1 host-10-0-16-38 10.0.16.70   6003 /DWS/data1/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6004 /DWS/data2/hdn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
03 /DWS/data2/hdn2/dummy2 R Secondary Normal
2 host-10-0-16-38 10.0.16.70   6005 /DWS/data1/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6006 /DWS/data1/hdn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
04 /DWS/data1/hdn1/dummy2 R Secondary Normal
2 host-10-0-16-47 10.0.16.67   6007 /DWS/data1/hdn1/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6008 /DWS/data2/hdn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
05 /DWS/data2/hdn2/dummy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6009 /DWS/data1/hdnl/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6010 /DWS/data1/hdn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
06 /DWS/data1/hdn1/dummy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6011 /DWS/data2/hdn2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70  6012 /DWS/data2/hdn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
07 /DWS/data2/hdn2/dummy2 R Secondary Normal
```

Go to the log path defined by the GAUSSLOG environment variable to view specific logs, such as DN instance logs, GTM instance logs, CN instance logs, and instance monitoring logs such as CM_AGENT and CM_SERVER. Run the following command to view the log path:

```
echo $GAUSSLOG
```

Information similar to the following is displayed.

```
[Ruby@host-172-16-38-100 ~]# echo $GAUSSLOG
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-38-100 ~]#
```

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.17 1078919243 CM_Agent Failed to Connect to the Database (ALM_AI_AbnormalCmaConnFail)

Alarm Description

This alarm is generated when CM_AGENT fails to create persistent connections when monitoring the GTM, DN, and CN.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891924 3	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When CM_AGENT fails to connect to the GTM, DN, or CN process to be monitored and the issue persists for a long time, a primary/standby switchover will occur if the GTMs and DNs are the primary nodes.

System Actions

None

Possible Causes

- The GTM, DN, and CN are not started.
- The CN and DN connection pools are full.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Go to the log directory where the instance generating the alarm resides, view the log, and perform operations instructed by the log.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 dws]|# cm_ctl query -cvid
[ CMServer State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.181   1    /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2    /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
reistributing : No
balanced : Yes

[ Coordinator State ]
node      node_ip      instance      state
1 host-10-0-16-47 10.0.16.67   5001 /DWS/datal/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /DWS/datal/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.70   5002 /DWS/datal/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
stance      state
-----
1 host-10-0-16-47 10.0.16.67   6001 /DWS/datal/hdnl/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /DWS/datal/hdnl1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
02 /DWS/datal/hdnl1/dumy2     R Secondary Normal
2 host-10-0-16-38 10.0.16.70   6003 /DWS/datal/hdnl2/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6004 /DWS/datal/hdnl2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
03 /DWS/datal/hdnl2/dumy2     R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6005 /DWS/datal/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6006 /DWS/datal/hdnl1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
04 /DWS/datal/hdnl1/dumy2     R Secondary Normal
4 host-10-0-16-38 10.0.16.70   6007 /DWS/datal/hdnl2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6008 /DWS/datal/hdnl2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
05 /DWS/datal/hdnl2/dumy2     R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6009 /DWS/datal/hdnl2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6010 /DWS/datal/hdnl1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
06 /DWS/datal/hdnl1/dumy2     R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6011 /DWS/datal/hdnl2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70  6012 /DWS/datal/hdnl2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
07 /DWS/datal/hdnl2/dumy2     R Secondary Normal
```

Go to the log path defined by the GAUSSLOG environment variable to view specific logs, such as DN instance logs, GTM instance logs, CN instance logs, and instance monitoring logs such as CM_AGENT and CM_SERVER. Run the following command to view the log path:

echo \$GAUSSLOG

Information similar to the following is displayed.

```
[Ruby@host-172-16-38-100 ~]# echo $GAUSSLOG
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-38-100 ~]#
```

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.18 1078919245 Failed to Recreate the DN (ALM_AI_AbnormalBuild)

Alarm Description

If the primary and standby data is different, the cluster automatically recreates the DN. This alarm is generated when the DN fails to be recreated.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891924 5	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the DN fails to be recreated, the DN cannot run properly. As a result, the cluster runs in the fault mode, deteriorating the performance and decreasing the availability.

System Actions

None

Possible Causes

- The hardware is faulty, the disk runs slowly, or the network is disconnected.
- Logs of the primary and standby DNs are inconsistent.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Go to the log directory where the instance generating the alarm resides, view the log, and perform operations instructed by the log.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 dws]|# cm_ctl query -cvid
[ CMServer State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.181   1    /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2    /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
rebalancing : No
balanced : Yes

[ Coordinator State ]
node      node_ip      instance      state
1 host-10-0-16-47 10.0.16.67   5001 /DWS/datal/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /DWS/datal/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
2 host-10-0-16-38 10.0.16.70   5002 /DWS/datal/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
stance      state
-----
1 host-10-0-16-47 10.0.16.67   6001 /DWS/datal/hdnl/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /DWS/datal/hdnl1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
02 /DWS/datal/hdnl1/dumy2 R Secondary Normal
1 host-10-0-16-38 10.0.16.108  6003 /DWS/datal/hdnl2/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6004 /DWS/datal/hdnl2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
03 /DWS/datal/hdnl2/dumy2 R Secondary Normal
2 host-10-0-16-38 10.0.16.70   6005 /DWS/datal/hdnl/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6006 /DWS/datal/hdnl1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
04 /DWS/datal/hdnl/dumy2 R Secondary Normal
2 host-10-0-16-47 10.0.16.67   6007 /DWS/datal/hdn2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6008 /DWS/datal/hdn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
05 /DWS/datal/hdn2/dumy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6009 /DWS/datal/hdnl/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6010 /DWS/datal/hdn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
06 /DWS/datal/hdnl/dumy2 R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6011 /DWS/datal/hdn2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70  6012 /DWS/datal/hdn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
07 /DWS/datal/hdn2/dumy2 R Secondary Normal
```

Go to the log path defined by the GAUSSLOG environment variable to view specific logs, such as DN instance logs, GTM instance logs, CN instance logs, and instance monitoring logs such as CM_AGENT and CM_SERVER. Run the following command to view the log path:

```
echo $GAUSSLOG
```

Information similar to the following is displayed.

```
[Ruby@host-172-16-38-100 ~]# echo $GAUSSLOG
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-38-100 ~]#
```

Step 3 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.19 1078919246 Process Restarts Abnormally (ALM_AI_INS_RESTART)

Alarm Description

This alarm is generated when an unexpected process is restarted of a CN, DN, or GTM in the cluster.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891924 6	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

This alarm indicates that a CN, DN, or GTM process has been restarted, which may temporarily affect services. Check the current cluster status and check whether other alarms are generated. Clear other alarms, if any, after you handle this alarm.

System Actions

None

Possible Causes

A core dump may occur in the instance process, CM Agent may be triggered to kill the instance process, two active DNs or GTMs may exist, or the instance may break down.

Other alarms, such as **ALM_AI_AbnormalGTMInst**, **ALM_AI_AbnormalDatanodeInst** and **ALM_AI_AbnormalCmaConnFail**, may also be reported.

This alarm will not be generated if the instance process cannot be started due to a damaged instance data directory or a manually stopped process after the process exits.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the following command to switch to the **Ruby** user:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 data]# cm_ctl query -Cvid
[ CMServer State ]
node      node_ip     instance          state
2 host-10-0-16-38 10.0.16.181   1 /DWS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2 /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced       : Yes

[ Coordinator State ]
node      node_ip     instance          state
1 host-10-0-16-47 10.0.16.67   5001 /DWS/data1/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip     instance          state
2 host-10-0-16-38 10.0.16.70   5002 /DWS/data1/coordinator Normal

[ GTM State ]
node      node_ip     instance          state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node      node_ip     instance          state | node      node_ip     instance          state | node      node_ip     in
stance          state
1 host-10-0-16-47 10.0.16.67   6001 /DWS/data1/hdnn1/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /DWS/data1/hdnn1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
02 /DWS/data1/hdnn1/dummy2   R Secondary Normal
03 /DWS/data2/hdnn2/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6004 /DWS/data2/hdnn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
04 /DWS/data2/hdnn2/dummy2   R Secondary Normal
2 host-10-0-16-38 10.0.16.70   6005 /DWS/data1/hdnn1/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6006 /DWS/data1/hdnn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
05 /DWS/data1/hdnn1/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6008 /DWS/data2/hdnn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  30
03 /DWS/data1/hdnn1/dummy2   R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6009 /DWS/data1/hdnn1/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6010 /DWS/data1/hdnn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70  30
06 /DWS/data1/hdnn1/dummy2   R Secondary Normal
3 host-10-0-16-57 10.0.16.108  6011 /DWS/data2/hdnn2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70  6012 /DWS/data2/hdnn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  30
07 /DWS/data2/hdnn2/dummy2   R Secondary Normal
```

Find the log path defined by the **GAUSSLOG** environment variable and go to the path to view the logs of the instance where process restart occurs. In addition, you can check the **cm_agent** and **cm_server** logs in the path to obtain more location information. Run the following command to view the log path:

echo \$GAUSSLOG

Information similar to the following is displayed.

```
[Ruby@host-172-16-38-100 ~]# echo $GAUSSLOG
/var/chroot/DWS/manager/log/Ruby
[Ruby@host-172-16-38-100 ~]#
```

Step 3 Clear other alarms if any.

Step 4 If the fault persists, contact technical support.

----End

Alarm Clearance

Event alarms do not need to be cleared manually.

Related Information

None

2.2.20 1078919256 Database Node Runs Too Slowly (ALM_AI_SLOWNODE)

Alarm Description

This alarm is generated when the number of waiting times of CN/DN instances in a cluster exceeds the preset threshold due to disk, memory, CPU, or network exceptions within a specified period, and the ratio of the number of waiting times

of instances to the total number of waiting times in the cluster exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
107891925 6	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated

Type	Parameter	Description
	domain_id	Domain ID for which the alarm is generated

Impact on the System

This alarm indicates that the node is running slowly and will become the performance bottleneck of the cluster.

System Actions

None

Possible Causes

- The disk of the node is faulty.
- The memory of the node is insufficient.
- The CPU usage of the node is too high.
- The network connection of the node is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Step 3 Isolate the slow node.

In the following command, *HOSTNAME* indicates the host name obtained in [Step 2](#), and *[-l LOGFILE]* indicates the log path. The log path is optional.

gs_om -t isolate_stop -h HOSTNAME [-l LOGFILE]

Step 4 Contact Huawei engineers to check the disk, memory, CPU, and network of the slow node and restore the node environment accordingly.

Step 5 Restore the slow node.

In the following command, *HOSTNAME* indicates the host name obtained in [Step 2](#), and *[-l LOGFILE]* indicates the log path. The log path is optional.

gs_om -t isolate_restore -h HOSTNAME [-l LOGFILE]

Step 6 Check whether the alarm is cleared.

- If yes, refer to "Log Reference" and contact technical support.
- If no, no further action is required.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.21 1078919257 gRPC Certificate File Does Not Exist (ALM_AI_AbnormalGrpcKey)

Alarm Description

This alarm is generated when the certificate is lost or the GAUSSHOME environment variable is incorrectly configured after authentication is enabled for the remote read function (**remote_read_mode = authentication**).

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919257	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If this alarm is generated, the remote read authentication is enabled, but the server certificate path is incorrect or the file does not exist during cluster startup. As a result, the primary or standby DN on the node cannot be started. After the cluster is started, if the client certificate path is incorrect or the file does not exist, the remote read function cannot work properly.

System Actions

None

Possible Causes

The certificate file is missing.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

Information similar to the following is displayed.

```
[Ruby@host-10-0-16-38 data1]# cm_ctl query -Cvid
[ OServer State ]
node      node_ip      instance      state
-----+-----+-----+-----+
2 host-10-0-16-38 10.0.16.181    1   /DWS/manager/cm/cm server Primary
3 host-10-0-16-57 10.0.16.179    2   /DWS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced       : Yes

[ Coordinator State ]
node      node_ip      instance      state
-----+-----+-----+-----+
1 host-10-0-16-47 10.0.16.67    5001 /DWS/data1/coordinator Normal
2 host-10-0-16-38 10.0.16.70    5002 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node      node_ip      instance      state
-----+-----+-----+-----+
2 host-10-0-16-38 10.0.16.70    5002 /DWS/data1/coordinator Normal

[ GTM State ]
node      node_ip      instance      state      sync_state
-----+-----+-----+-----+-----+
3 host-10-0-16-57 10.0.16.108   1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70    1002 /DWS/manager/gtm S Standby Connection ok Sync

[ DataNode State ]
node      node_ip      instance      state      | node      node_ip      instance      state      | node      node_ip      in
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 host-10-0-16-47 10.0.16.67    6001 /DWS/data1/h0dn1/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70    6002 /DWS/data1/h0dn1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108   36
02 /DWS/data1/h0dn1/dummy2     R Secondary Normal
2 host-10-0-16-47 10.0.16.67    6003 /DWS/data2/h0dn2/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108   6004 /DWS/data2/h0dn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70   36
03 /DWS/data2/h0dn2/dummy2     R Secondary Normal
2 host-10-0-16-38 10.0.16.70    6005 /DWS/data1/h1dn1/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108   6006 /DWS/data1/h1dn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67   36
04 /DWS/data1/h1dn1/dummy2     R Secondary Normal
2 host-10-0-16-38 10.0.16.70    6007 /DWS/data2/h1dn2/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67   6008 /DWS/data2/h1dn2/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108   36
05 /DWS/data2/h1dn2/dummy2     R Secondary Normal
3 host-10-0-16-57 10.0.16.108   6009 /DWS/data1/h2dn1/primary0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67   6010 /DWS/data1/h2dn1/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70   36
06 /DWS/data1/h2dn1/dummy2     R Secondary Normal
3 host-10-0-16-57 10.0.16.108   6011 /DWS/data2/h2dn2/primary0 P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6012 /DWS/data2/h2dn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67   36
07 /DWS/data2/h2dn2/dummy2     R Secondary Normal
```

Step 3 Determine whether to enable the encryption authentication of the remote read function based on service requirements.

- If you do not enable this function, go to step [Step 4](#) and the operation is complete.

- If yes, go to **Step 5**.

Step 4 Run the following commands to disable the authentication of the remote read function and restart the cluster:

```
gs_guc set -Z coordinator -Z datanode -N all -I all -c  
"remote_read_mode=non_authentication"  
  
cm_ctl stop; cm_ctl start
```

Step 5 Run the following command to check whether all of the five certificate files exist:

```
cd ${GAUSSHOMEROOT}/share/sslcert/grpc/
```

```
ll
```

The command output is displayed as follows:

```
[omm@host1 ~]$ cd ${GAUSSHOMEROOT}/share/sslcert/grpc  
[omm@host1 grpc]$ ll  
total 44  
-rw----- 1 omm wheel 4486 Jun  2 17:10 cacert.pem  
-rw----- 1 omm wheel 4486 Jun  2 17:10 client.crt  
-rw----- 1 omm wheel 1675 Jun  2 17:10 client.key  
-rw----- 1 omm wheel 9482 Jun  2 17:10 openssl.cnf  
-rw----- 1 omm wheel 4486 Jun  2 17:10 server.crt  
-rw----- 1 omm wheel 1675 Jun  2 17:10 server.key
```

- If no, go to **Step 6**.
- If yes, go to **Step 8**.

Step 6 Log in to the instance node where the certificate files exist and are not damaged, and run the following command to copy the missing files to the instance node where the alarm is generated:

```
scp -r ${GAUSSHOMEROOT}/share/sslcert/grpc/Host name of the node where the certificate is damaged or files are missing:${GAUSSHOMEROOT}/share/sslcert/grpc/
```

Change the file permission to **600**.

Step 7 Run the following command to restart the instance for which the alarm is generated (**node** indicates the host name of the faulty instance. Replace it with the actual host name):

```
gs_replace -t start -h node
```

Step 8 If the fault persists, contact technical support engineers.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.22 1078919258 Cluster Read-only (ALM_AI_ReadOnlyMode)

Alarm Description

This alarm is generated when the cluster status changes to read-only.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919258	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The cluster status is marked as read-only and data cannot be written to or modified in the cluster.

System Actions

None

Possible Causes

The cluster disk usage exceeds 90%. As a result, the cluster becomes read-only and data cannot be written to or modified in the cluster.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#) and run the following command to switch to user **Ruby**:

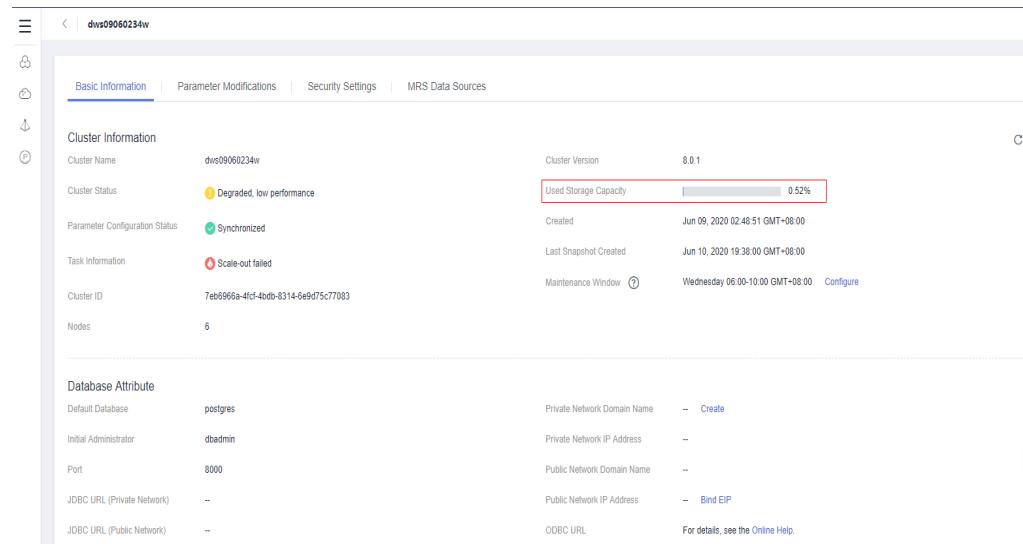
su - Ruby

Log in to any node in the cluster as user **Ruby** and run the following command:

cm_ctl query -Cvid

The command output is displayed as follows:

Step 3 Log in to the GaussDB(DWS) console, view the basic information of the target cluster, and check whether the used disk capacity exceeds 90%. If yes, capacity expansion is required. The following figure shows the details.



Step 4 If the cluster is still in the read-only state, choose **Cancel Readonly** for the cluster.

Step 5 If the fault persists, contact technical support.

-----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.2.23 1078919260 Disk Usage Is Too High (ALM_AI_DiskRatioHigh)

Alarm Description

This alarm is generated when the disk usage of each DN in the cluster exceeds 80%.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919260	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .

Type	Parameter	Description
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

System Actions

None

Impact on the System

This alarm indicates that the DN disk space in the current cluster is about to be used up. Expand the disk space as soon as possible.

Possible Causes

The disk usage of the DN exceeds 80% of the total disk space.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the environment information of the instance for which the alarm is generated.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

1. Run the following command to switch to the **Ruby** user:

su - Ruby

2. Access the sandbox.

ssh `hostname -i`

3. Check the disk usage of the cluster.

gs_ssh -c "df -h"

Step 3 If the disk usage of most instances exceeds 80%, contact the user to expand the disk capacity.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.24 1078919264 Remaining Database Disk Capacity Warning (ALM_AI_DiskUsageRisk)

Alarm Description

This alarm is generated when the disk or inode usage of a cluster instance is greater than or equal to 80%.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919264	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

This alarm is generated when the disk or inode usage of cluster instances is high. If the disk usage exceeds 90%, the cluster is marked as read-only.

System Actions

None

Possible Causes

Check whether the disk usage of some instances is too high due to data skew. If yes, contact the user to modify service tables. If no, contact the user to expand the disk capacity as soon as possible.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the disk usage of the data directory of the instance for which the alarm is generated.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

1. Run the following command to switch to the **Ruby** user:

su - Ruby

2. Access the sandbox.

ssh `hostname -i`

3. Check the disk usage of the cluster.

gs_ssh -c "df -h"

4. Check the inode usage of the cluster.

gs_ssh -c "df -i"

Step 3 If the disk usage of only some instances is high, data skew may occur in the service tables. In this case, contact the user to rectify the tables.

Step 4 If the disk usage of most instances is high, contact the user to expand the disk capacity.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.25 1078919265 Remaining Database Disk Capacity Is Insufficient (ALM_AI_DiskUsageReadOnly)

Alarm Description

This alarm is generated when the disk or inode usage reaches 90%, and the cluster is marked as read-only.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919265	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The cluster status is marked as read-only, and data cannot be written to or modified in the cluster.

System Actions

None

Possible Causes

The cluster disk or inode usage exceeds 90%. As a result, the cluster becomes read-only and data cannot be written to or modified in the cluster.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the disk usage of the data directory of the instance for which the alarm is generated.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the following command to switch to the **Ruby** user:

su - Ruby

Access the sandbox.

ssh `hostname -i`

Check the disk usage of the cluster.

gs_ssh -c "df -h"

Check the inode usage of the cluster.

gs_ssh -c "df -i"

Step 3 If the disk usage of only some instances is high, data skew may occur in the service tables. In this case, contact the user to rectify the tables.

Step 4 If the disk usage of most instances is high, contact the user to expand the disk capacity.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.26 1078919266 Remaining Database Disk Capacity Is Severely Insufficient (ALM_AI_DiskUsageDanger)

Alarm Description

This alarm is generated when the disk or inode usage of a cluster instance is greater than or equal to 95%.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919266	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the data disk or inode usage reaches 95%, the primary DN where the disk resides is restarted, and the standby and secondary DNs are forcibly stopped. If the log disk usage reaches 95%, DNs are not affected.

System Actions

None

Possible Causes

The cluster disk or inode usage exceeds 95%. As a result, the cluster becomes read-only and data cannot be written to or modified in the cluster.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the disk usage of the data directory of the instance for which the alarm is generated.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the following command to switch to the **Ruby** user:

su - Ruby

Access the sandbox.

ssh `hostname -i`

Check the disk usage of the cluster.

gs_ssh -c "df -h"

Check the inode usage of the cluster.

gs_ssh -c "df -i"

Step 3 If the disk usage of only some instances is high, data skew may occur in the service tables. In this case, contact the user to rectify the tables.

Step 4 If the disk usage of most instances is high, contact the user to expand the disk capacity.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.27 1078919267 Failed to Start DMS Agent

Alarm Description

After DMS Agent is installed and deployed, the DMS Agent startup script is registered with the crontab scheduled task list of the host machine. The crontab invokes the DMS Agent startup script every one minute to check whether the DMS Agent collection process exists. If no, the startup script attempts to restart the collection. This alarm is generated when the DMS Agent collection process fails to be restarted. This alarm is cleared when the collection process is started successfully.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919267	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .

Type	Parameter	Description
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If DMS Agent fails to be started, the main functions of DMS are affected. As a result, no data is displayed on the page or the metrics are in the expired state.

System Actions

None

Possible Causes

1. The host machine does not have sufficient resources. As a result, DMS Agent cannot be started.
2. The key initialization information on which DMS Agent depends cannot be obtained.
3. DMS Agent cannot connect to other DMS services due to cluster network problems.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the environment information of the instance for which the alarm is generated.

Locate the cluster by checking the fields **Location Info > cluster_id** or **cluster_name** in the alarm details. Then check **Other Information** to view the instance directory.

1. Log in to the instance for which the alarm is generated in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Then, switch to user **Ruby**.
`su - Ruby`
2. Check whether the DMS Agent process is running.
`ps aux | grep agent_service.py`
3. Access the DMS Agent log directory.
`cd /var/chroot/DWS/manager/dmsagent/log`
4. View the DMS Agent initialization and execution logs, analyze the cause, and rectify the fault.
`vi initial.log`
`vi agent_service.log`

Step 3 When the fault is rectified, the crontab automatically invokes the DMS Agent startup script to start the DMS Agent collection process and the alarm will be cleared.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.28 1078919270 Failed to Install the Plug-In (ALM_AI_InstallPluginFailed)

Alarm Description

When O&M operations such as installation, capacity expansion, warm backup, upgrade, and snapshot restoration are performed for a cluster on the tenant side, the plug-in is automatically installed on the new instance. If the plug-in fails to be installed, the O&M operation result is not affected, but this alarm is reported to prompt O&M personnel or users to manually install the plug-in.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919270	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If the plug-in fails to be installed, O&M operations and main functions of the database are not affected, but some additional functions are unavailable.

System Actions

None

Possible Causes

The plug-in fails to be installed due to intermittent network disconnection.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the environment information of the alarm reporting instance.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance as user **root**.

1. Go to the installation directory of the plug-in package.
`cd /opt/dws/download_package/ Plugin_name`

For example, go to the **dmsAgent** plug-in directory and run the **ls** command.

```
agent_initial.py arm check_giar.py comm giar_net_stat.sh giar_tcp_stat.sh install.py scheduler_operate.sh start_stop_inst_check.sh stop.sh update.py version  
agent_service.py cert collect common.sh giar_stat_check.sh install.log sched so startup.sh subhealthcheck util x86
```

2. View the installation logs, analyze the fault cause, and rectify the fault:
`view install.log`

Step 3 Log in to Service CM, choose **Services > Data Warehouse Service**, and choose **Upgrade Management**.

- Set **Type** to **aggregation**, **dmsAgent**, or **inspect** based on the name for which the alarm is generated.
- Do not specify a source version.

- Set **Target Version** to the current cluster version.

Step 4 Select the cluster to be upgraded and click **Allow Upgrade**. In the dialog box that is displayed, click **OK**. Wait until the cluster can be updated.

Step 5 Select the cluster and click **Upgrade**. Wait until the task is complete and the upgrade status changes to **completed**.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.29 1078919280 DN Log Redo Operations Are Slow (ALM_AI_DatanodeRedoSlow)

Alarm Description

This alarm is generated when the difference between the logs after a redo operation and the logs received exceeds the threshold (4 GB). Xlog redo operations are executed slowly due to improper services or disk, memory, or CPU faults of a standby DN in the cluster.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919280	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm

Type	Parameter	Description
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

When this alarm is generated, the redo log completion rate of the standby node is greatly different from that of the primary node. Although the current service is not affected, the alarm is potentially a major risk that affects the reliability of the cluster system. Therefore, the alarm must be handled as soon as possible. If the primary DN is abnormal and the standby DN needs to be promoted to primary, it may take a long time for the standby DN to complete the redo operation. The cluster will be unavailable for a long time.

Possible Causes

- The standby node is not running for a long time.
- Special DDL operations have been performed.
- The node disk is faulty.
- The node memory is insufficient.
- The node CPU usage is too high.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

Run the following command to view the instance path:

cm_ctl query -Cvid

The following figure shows the query result. The information following the instance ID (for example, 6003) is the instance path.

```
[rhel7-0-0-16-38 data]# cm_ctl query Cvid
[ CM Server State ]
node          node_ip           instance      state
2 host-10-0-16-38 10.0.16.181   1 /OVS/manager/cm/cm_server Primary
3 host-10-0-16-57 10.0.16.179   2 /OVS/manager/cm/cm_server Standby

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced       : Yes

[ Coordinator State ]
node          node_ip           instance      state
1 host-10-0-16-47 10.0.16.67   5001 /OVS/datal/coordinator Normal
2 host-10-0-16-38 10.0.16.70   5002 /OVS/datal/coordinator Normal

[ Central Coordinator State ]
node          node_ip           instance      state
2 host-10-0-16-38 10.0.16.70   5002 /OVS/datal/coordinator Normal

[ Gtm State ]
node          node_ip           instance      state      sync_state
3 host-10-0-16-57 10.0.16.108  1001 /OVS/manager/gtm P Primary Connection ok Sync
2 host-10-0-16-38 10.0.16.70   1002 /OVS/manager/gtm S Standby Connection ok Sync

[ DataNode State ]
node          node_ip           instance      state | node          node_ip           instance      state | node          node_ip           in
stance
-----
1 host-10-0-16-47 10.0.16.67   6001 /OVS/datal/hdnn1/primary P Primary Normal | 2 host-10-0-16-38 10.0.16.70   6002 /OVS/datal/hdnn1/standby1 S Standby Normal | 3 host-10-0-16-57 10.0.16.108  6004 /OVS/datal/hdn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70   6006 /OVS/datal/hdn1/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  6008 /OVS/datal/hdn2/primary0 P Primary Normal | 3 host-10-0-16-57 10.0.16.108  6010 /OVS/datal/hdn2/standby1 S Standby Normal | 2 host-10-0-16-38 10.0.16.70   6012 /OVS/datal/hdn2/standby1 S Standby Normal | 1 host-10-0-16-47 10.0.16.67  6014 /OVS/datal/hdn2/secondary0 R Secondary Normal
03 /OVS/datal/hdn2/secondary1 R Secondary Normal
04 /OVS/datal/hdn2/secondary2 R Secondary Normal
05 /OVS/datal/hdn2/secondary3 R Secondary Normal
3 host-10-0-16-57 10.0.16.108   6009 /OVS/datal/hdnn2/prIMARY0 P Primary Normal | 1 host-10-0-16-47 10.0.16.67  6011 /OVS/datal/hdnn2/secondary0 R Secondary Normal
4 host-10-0-16-38 10.0.16.108   6013 /OVS/datal/hdnn2/secondary1 R Secondary Normal
5 host-10-0-16-38 10.0.16.108   6015 /OVS/datal/hdnn2/secondary2 R Secondary Normal
6 host-10-0-16-38 10.0.16.108   6017 /OVS/datal/hdnn2/secondary3 R Secondary Normal
```

Step 3 Run the `gs_ctl query` command to check the difference between `receiver_replay_location` and `receiver_flush_location` of the xlog redo operation of the standby DN.

gs_ctl query -D *Instance_path*

Information similar to the following is displayed:

```
Receiver info:  
receiver_pid      : 24907  
local_role        : Standby  
peer_role         : Primary  
peer_state        : Normal  
state             : Streaming  
sender_sent_location : 1/70B93F0  
sender_write_location  : 1/70B93F0  
sender_flush_location   : 1/70B93F0  
sender_replay_location  : 1/70B93F0  
receiver_received_location : 1/70B93F0  
receiver_write_location   : 1/70B93F0  
receiver_flush_location    : 1/70B93F0  
receiver_replay_location   : 0/50AA003  
sync_percent        : 2%
```

Step 4 Check the startup time of the standby DN to determine whether the standby DN is not running for a long time.

- If yes, because xlogs are not synchronized between the primary and standby nodes for a long time, synchronization cannot be complete within a short period of time. In this case, evaluate the actual service status, temporarily reduce service access, and reduce the generation speed of xlogs. Then check whether the difference between **receiver_replay_location** and **receiver_flush_location** is narrowed. After the alarm is cleared, restore the jobs. Pay attention to the cluster monitoring status so that each node in the cluster can be restored to the normal status in a timely manner.
- If no, go to [Step 5](#).

Step 5 Find the redo log file based on **receiver_replay_location**, use the pg_xlogdump tool to parse and view the operations in the redo logs, and check whether a large number of DDL operations, such as **CREATE**, **DROP**, **TRUNCATE**, and **REINDEX**, are performed on database objects such as tables.

- If yes, evaluate the actual service status and adjust the services. If necessary, suspend the services to prevent DDL operations that take a long time to redo in batch processing jobs. On GaussDB(DWS), perform DDL operations (such as creating tables) in a unified manner and prevent DDL operations in batch processing jobs so that performance is not affected. Then check whether the difference between **receiver_replay_location** and **receiver_flush_location** is narrowed.
- If no, go to [Step 6](#).

Step 6 Contact the system administrator to check whether the node disk, memory, or CPU are faulty, or whether the resources are about to be used up.

NOTE

If the node hardware is faulty, rectify the fault by following the instructions provided in section "Replacing the Entire Server in the BMS Scenario" in *Data Warehouse Service (DWS) 8.1.3.331 Emergency Plan (for Huawei Cloud Stack 8.3.1)*.

- If yes, repair or replace the hardware components.
- If no, go to [Step 7](#).

Step 7 Check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, contact technical support.

----End

Alarm Clearance

This alarm is automatically cleared when the difference between the redo logs and the received logs decreases from more than 4 GB to less than 2 GB.

Related Information

None

2.2.30 1078919290 Cluster Instance OS Is Restarted (ALM_AI_OSReboot)

Description

This alarm is generated when the OS of a cluster instance has been restarted.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919290	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated

Type	Parameter	Description
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If a cluster instance is restarted, the database process on the instance will also be restarted, which may cause intermittent service interruption.

System Actions

None

Possible Causes

If the fault is not caused by a planned restart, contact the IaaS personnel for cause analysis.

Procedure

None

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.31 107891930 Failed to Create a Table (ALM_AI_CreateTableFail)

Alarm Description

This alarm is generated when the number of consecutive table creation failures in a cluster in a specified period exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919300	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

System Actions

None

Impact on the System

This alarm indicates that the current cluster is unavailable and the fault needs to be rectified as soon as possible.

Possible Causes

- A CN/DN/GTM instance is faulty due to disk, memory, CPU, or network faults, and cannot be automatically restored by a restart or an active/standby switchover.
- The cluster status is normal but the read-only attribute is enabled or a CN breaks down.
- Other exceptions

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Handle other alarms, if any, and check whether the alarm is automatically cleared.

Step 3 Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

Query the cluster status.

cm_ctl query -Cvidp

The following figure shows the query result of a normal cluster.

```
[Rubyhost-172-16-40-7]# cm_ctl query -Cvdp
[ CMServer State ]
node          node_ip           instance      state
-----+-----+-----+-----+
2 host-172-16-35-83 172.16.180.213 1 /DWS/manager/cm/_server Primary
3 host-172-16-20-115 172.16.161.36 2 /DWS/manager/cm/_server Standby

[ Cluster State ]
cluster_state : Normal
redistributing : No
balanced : Yes

[ Coordinator State ]
node          node_ip           instance      state
-----+-----+-----+-----+
1 host-172-16-40-7 172.16.67.139 5001 8900 /DWS/data1/coordinator Normal
2 host-172-16-35-83 172.16.85.11 5002 8900 /DWS/data1/coordinator Normal
3 host-172-16-20-115 172.16.98.128 5003 8900 /DWS/data1/coordinator Normal

[ Central Coordinator State ]
node          node_ip           instance      state
-----+-----+-----+-----+
3 host-172-16-20-115 172.16.98.128 5003 /DWS/data1/coordinator Normal

[ GTM State ]
node          node_ip           instance      state      sync_state
-----+-----+-----+-----+-----+
3 host-172-16-20-115 172.16.98.128 1001 /DWS/manager/gtm P Primary Connection ok Sync
2 host-172-16-35-83 172.16.85.11 1002 /DWS/manager/gtm S Standby Connection ok Sync

[ Datanode State ]
node          node_ip           instance      state      | node          node_ip           instance      state      | node
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 host-172-16-40-7 172.16.67.139 6001 49000 /DWS/data1/h0dn1/priary0 P Primary Normal | 2 host-172-16-35-83 172.16.85.11 6002 45000 /DWS/data2/h0dn1/standby1 S Standby Normal | 3 host-172-16-20-115 172.16.98.128 3002 /DWS/data2/h0dn1/dummy2 R Secondary Normal
1 host-172-16-40-7 172.16.67.139 6003 49000 /DWS/data2/h0dn2/priary0 P Primary Normal | 3 host-172-16-20-115 172.16.98.128 6004 45000 /DWS/data4/h0dn2/standby1 S Standby Normal | 2 host-172-16-35-83 172.16.85.11 3003 /DWS/data4/h0dn2/dummy2 R Secondary Normal
1 host-172-16-40-7 172.16.67.139 6005 49000 /DWS/data3/h0dn1/priary0 P Primary Normal | 3 host-172-16-20-115 172.16.98.128 6006 45000 /DWS/data2/h1dn1/standby1 S Standby Normal | 1 host-172-16-40-7 172.16.67.139 3004 /DWS/data2/h1dn1/dummy2 R Secondary Normal
2 host-172-16-35-83 172.16.85.11 6007 49002 /DWS/data3/h1dn2/priary0 P Primary Normal | 1 host-172-16-40-7 172.16.67.139 6008 45000 /DWS/data4/h1dn2/standby1 S Standby Normal | 3 host-172-16-20-115 172.16.98.128 3005 /DWS/data4/h1dn2/dummy2 R Secondary Normal
1 host-172-16-40-7 172.16.67.139 6009 49000 /DWS/data1/h2dn1/priary0 P Primary Normal | 1 host-172-16-40-7 172.16.67.139 6010 45000 /DWS/data2/h2dn1/standby1 S Standby Normal | 2 host-172-16-35-83 172.16.85.11 3006 /DWS/data2/h2dn1/dummy2 R Secondary Normal
3 host-172-16-40-7 172.16.67.139 6011 49002 /DWS/data3/h2dn1/priary0 P Primary Normal | 2 host-172-16-35-83 172.16.85.11 6012 45000 /DWS/data4/h2dn1/standby1 S Standby Normal | 1 host-172-16-40-7 172.16.67.139 3007 /DWS/data4/h2dn2/dummy2 R Secondary Normal
```

Check whether abnormal nodes or instances exist. If yes, handle the exception first. If the cluster nodes and instances are normal, run the following command to connect to a CN and create a table.

```
gsql postgresql://:8000/postgres?application_name='OM' -c "create table alarm_test(a int);"
```

Replace **8000** with a CN port number displayed when you query the cluster status. In the SQL statement, **alarm_test** can be replaced with another table name. Check the table creation result.

Step 4 If the fault persists, contact technical support.

-----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.2.32 1078919301 Failed to Start the Plug-in (ALM_AI_StartPluginFailed)

Alarm Description

Failed to start a plug-in after it is installed.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919301	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

System Actions

None

Impact on the System

The cluster fails to be deployed.

Possible Causes

The installed plug-in is missing.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check the environment information of the instance for which the alarm is generated.

Obtain the instance name by checking the **instance_name** field under the location information or other information in the alarm details.

Refer to [Logging In to a Node in the Tenant Cluster](#) to log in to the instance as user **root**.

1. Go to the installation directory of the plug-in package.
cd /var/chroot/opt/dws/download_package/ *Plugin_name*

For example, go to the **dmsAgent** plug-in directory and run the **ls** command.

```
agent_initial.py arm check_gsar.py comm gsar_net_stat.sh gsar_tcp_stat.sh install.py scheduler_operate.sh start_slow_inst_check.sh stop.sh subhealthcheck update.py version
agent_service.py cert collect common.sh gsar_stat_check.sh install.log sched so startup.sh util x86
```

2. View the installation logs, analyze the fault cause, and rectify the fault:
view install.log

Step 3 Log in to Service CM, choose **Services > Data Warehouse Service**, and choose **Upgrade Management**.

- Set **Type** to **aggregation**, **dmsAgent**, or **inspect** based on the name for which the alarm is generated.
- Do not specify a source version.
- Set **Target Version** to the current cluster version.

Step 4 Select the cluster to be upgraded and click **Allow Upgrade**. In the dialog box that is displayed, click **OK**. Wait until the cluster can be updated.

Step 5 Select the cluster and click **Upgrade**. Wait until the task is complete and the upgrade status changes to **completed**.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.2.33 1078919306 gs_scheduler Process Abnormal

Alarm Description

GaussDB(DWS) cm_agent checks whether the **gs_scheduler** process exists every second. If the **gs_scheduler** process does not exist, cm_agent attempts to start a new **gs_scheduler** process. If the **gs_scheduler** process cannot be started for three consecutive times, that is, the **gs_scheduler** process does not exist for three consecutive times, an alarm is reported indicating that the scheduler process of the node is abnormal. This alarm is automatically cleared when the **gs_scheduler** process exists.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919306	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The scheduler is started on the CCN. If the scheduler process cannot be started, jobs scheduled by the scheduler cannot be scheduled.

Possible Causes

- The database cannot be connected.
- The gs_scheduler executable file does not exist.
- External scripts frequently kill the scheduler.

- The scheduler cannot write logs.
- The certificate file is frequently replaced.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Extract required information based on the alarm details. You can obtain the **HOST_IP** and logical location of the abnormal host from the CMA alarm details, but you must have the permissions on the host.

Step 3 Check whether the **gs_scheduler** process exists on the CCN node.

1. Check whether the node under **Central Coordinator State** is the current node.
`cm_ctl query -Cv`
 - a. If yes, go to **Step 3.2**.
 - b. If no, log in to the CCN node in SSH mode and run the **Step 3.2** command.
2. Check whether the scheduler process exists.
`ps ux | grep gs_scheduler`
 - a. If yes, check whether the PID of the **gs_scheduler** process has changed. If yes, go to Step 4. If no, check whether the alarm is cleared.
 - b. If no, go to **4.3**.
3. Connect to the CN instance and check whether the connection is normal.
 - a. If yes, go to **Step 4**.
 - b. If no, check whether related alarms are generated on the CN. After the CN fault is rectified, check whether the scheduler process is started.

Step 4 Check whether the **gs_scheduler** executable file exists.

```
cd $GPHOME/script && ls -l | grep gs_scheduler
```

1. If yes, go to **Step 5**.
2. If no, copy the executable file from another node. Then, check whether the alarm is cleared.

Step 5 Check whether there are external scripts frequently killing the scheduler.

```
ps ux | grep kill
```

1. If yes, check whether the kill target is the gs_scheduler process.
2. If no, go to **Step 6**.

Step 6 Check whether scheduler logs are properly written. Check whether the disk where **\$GAUSSLOG** is located is full. Invoker logs are stored in **\$GAUSSLOG/om**.

```
df -h
```

1. If yes, clear the disk and check whether the scheduler process is started.
2. If no, go to **Step 7**.

Step 7 Check whether the certificate file is frequently replaced. The certificate file is stored in the **\$GAUSSHOME/share/sslcert/grpcio/** directory. Check for several times whether the certificate generation time changes frequently. If it changes frequently, an external user may be performing O&M operations, such as scale-out, upgrade, and resizing. Wait until the certificate time stay unchanged, check whether the scheduler process is started.

----End

Alarm Clearance

This alarm is automatically cleared when the scheduler process becomes normal.

Related Information

None

2.2.34 1078919307 Big Data Framework Process Abnormal

Alarm Description

GaussDB(DWS) cm_agent checks whether the big data framework process exists every second. If the process does not exist, cm_agent attempts to start a new big data framework process. If the big data framework process does not exist in three consecutive checks, the big data framework process on the node is abnormal. This alarm is automatically cleared when the big data framework process exists.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919307	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

The big data framework process is started on each instance. If the big data framework process cannot be started, big data services will be affected.

Possible Causes

- The Java environment is incorrect, and the JRE component is missing.
- The command lines of the big data framework are incorrect.
- Failed to obtain the PID file lock and a process already exists.
- The **unix domain socket** file fails to be created. As a result, the listener cannot be created and the system exits abnormally.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Extract required information based on the alarm details. You can obtain the **HOST_IP** and logical location of the abnormal host from the CMA alarm details, but you must have the permissions on the host.

Step 3 Check whether multiple big data processes exist on the node.

```
ps ux | grep dws-bigdata |grep -v grep
```

1. If yes, check whether the dws-bigdata process ID changes frequently. If no, check whether the alarm is cleared. If the value keeps changing, go to [Step 4](#).
2. If no, go to [Step 5](#).

Step 4 View the dws-bigdata log in the **\$GAUSSLOG/dws-bigdata/** directory.

```
vi $GAUSSLOG/dws-bigdata/dws-bigdata.log
```

1. If the error message indicates that the JRE environment is missing, go to [Step 5](#).
2. If the error message indicates that the **unix domain socket** file fails to be created, go to [Step 6](#).
3. If the error message indicates that the pid file lock fails to be obtained, go to [Step 7](#).

Step 5 The Java environment is incorrect, and the JRE component is missing.

1. Check whether the JAR package exists. If yes, perform [Step 3-2](#). If no, copy the executable file from another node. Wait for the **cm_agent** process to start.

```
cd $GAUSSHOME/dws-bigdata && ls -l | grep dws-bigdata
```
2. Reinstall the JRE. The installation package contains **GaussDB-*-*-JRE-64bit.bin**, for example, **GaussDB-8.x.x-REDHAT-JRE-64bit.bin**. Reinstall the CM Agent and wait for the CM Agent to start the process.

Step 6 The Unix domain socket file fails to be created, and the listener cannot be created.

Obtain the **unix_socket_directory** directory and check whether the **.gaussBigData.socket** file exists in the directory.

```
cmxpath=`cm_ctl query -Cvd | grep cm_server | awk '{print $4}'|head -n 1`&cd `echo ${cmxpath%/*}`&cd cm_agent
```

```
cat cm.conf | grep unix_socket_directory  
cd `cat cm.conf | grep unix_socket_directory | sed "s/'//g" | sed 's/'//g' | awk '{print $3}'`  
ls -a | grep .gaussBigData.socket
```

1. If the directory does not exist, check whether the **dws-bigdata** process user has the permission on the **unix_socket_directory** directory. If the user does not have the permission, grant the permission to the user and wait for **cm_agent** to start the processes.
2. If yes, delete **.gaussBigData.socket**, kill all **java -jar dws-bigdata** processes, and wait for **cm_agent** to start the processes.

Step 7 Check whether the **dws-bigdata.pid** process file exists.

Check the configuration of **dws_bigdata_directory** in **cm.conf**.

```
cmxpath=`cm_ctl query -Cvd | grep cm_server | awk '{print $4}'|head -n 1`;cd `echo ${cmxpath%/*}`  
cd cm_agent  
cat cm.conf | grep dws_bigdata_directory
```

1. If no command output is displayed, the PID file is in **\$HOME**.
2. If there is output, the PID file is in the **dws_bigdata_directory**.
3. If the pid file exists in the preceding directory, delete the **dws-bigdata.pid** file in the errored directory, kill all **java -jar dws-bigdata** processes, and wait for the CM to start again. If no, check whether the user has the permission to access the directory specified by **dws_bigdata_directory**. If not, grant the access permission to the user, and wait for **cm_agent** to start the process.

----End

Alarm Clearance

This alarm is automatically cleared when the big data framework process becomes normal.

Related Information

None

2.2.35 1078919309 Table Data Is Damaged in the GaussDB (DWS) Cluster During Data Verification

Alarm Description

After a data detection task is added to the scheduler, the scheduler periodically scans all user tables in the database based on the task period to check whether data in the tables is damaged. This alarm is generated when the scheduler detects that data in a table is damaged.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919309	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

- Awareness Dimension
 - a. Data damage is detected based on service errors and cannot be rectified before service awareness.
 - b. It takes a long time to detect non-hotspot data damage. During this period, if the hardware of the node where the backup resides is faulty, two copies will be damaged by means of build, causing data loss.
 - c. After a file is damaged, it takes a long time to scan the entire database.
 - d. Whether the all-zero pages are normal cannot be determined. Consequently, no error is reported when a service accesses the all-zero page. The current mechanism cannot detect this error, which may lead to data loss due to infection.
- Dimension
 - a. If a single backup is damaged, a large number of errors are reported, affecting services or change operations such as upgrade and scale-out.
 - b. If two copies are damaged, data will be lost.
 - c. In extreme cases, both the active and standby instances cannot be started, and the cluster is unavailable.
 - d. Backup and DR are based on file-level physical copy. Damaged files will be infected, reducing the reliability of backup and DR data.

Possible Causes

Hardware faults

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Extract required information based on the alarm details. You can obtain the **HOST_IP** and logical location of the abnormal host from the CMA alarm details, but you must have the permissions on the host.

Step 3 Connect to the database and run the SQL statement to view data in the table.

```
select * from scheduler.data_integrity_err_table_info;
```

In the preceding information, scheduler.data_integrity_err_table_info contains detailed information about the tables whose data is damaged. For details, see the following table.

Table 2-9 Detailed information about the table whose data is damaged

Parameter	Description
database_name	Name of the database where the damaged table is located
schema_name	Schema name of the damaged table
table_name	Name of the damaged table
primary_is_checked	Whether the primary DN is checked
standby_is_checked	Whether the standby DN is checked
primary_check_info	Primary DN Check Result
standby_check_info	Standby DN Check Result
primary_check_error	Primary DN Check Result
standby_check_error	Standby DN Check Result

Step 4 The O&M engineer contacts the development engineer of the database vendor to restore the data.

----End

2.2.36 1078919310 Table Data Is Damaged After Incremental Build of the GaussDB (DWS) Cluster

Alarm Description

Incremental build anti-infection verification, which is set by the guc parameter enable_incremental_build_check. When the enable_incremental_build_check parameter is enabled, data verification is performed after incremental build triggered by the CM. This alarm is generated when data verification fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
1078919310	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

- Awareness Dimension
 - a. Data damage is detected based on service errors and cannot be rectified before service awareness.
 - b. It takes a long time to detect non-hotspot data damage. During this period, if the hardware of the node where the backup backup resides is faulty, two copies will be damaged by means of build, causing data loss.
 - c. After a file is damaged, it takes a long time to scan the entire database.

- d. Whether the all-zero pages are normal cannot be determined. Consequently, no error is reported when a service accesses the all-zero page. The current mechanism cannot detect this error, which may lead to data loss due to infection.
- Dimension
 - a. If a single backup is damaged, a large number of errors are reported, affecting services or change operations such as upgrade and scale-out.
 - b. If two copies are damaged, data will be lost.
 - c. In extreme cases, both the active and standby instances cannot be started, and the cluster is unavailable.
 - d. Backup and DR are based on file-level physical copy. Damaged files will be infected, reducing the reliability of backup and DR data.

Possible Causes

Hardware faults

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Extract required information based on the alarm details. You can obtain the **HOST_IP** and logical location of the abnormal host from the CMA alarm details, but you must have the permissions on the host.

Step 3 Log in to the host, go to the directory of the instance specified by `instance_id`, go to the `pg_rewind_bak` directory, and view the `check_err_table_list` file.

Step 4 The O&M engineer contacts the development engineer of the database vendor to restore the data.

----End

2.2.37 2078918234 D (Dead) Processes or Z (Zombie) Processes Exist on DNs (ALM_AI_AbnormalProcess)

Alarm Description

The **Ruby** user process on the current node is in the D or Z state.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
2078918234	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated

Type	Parameter	Description
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If this alarm is generated, the CN, DN, CM, or GTM instance process is abnormal and is in the D or Z state.

System Actions

None

Possible Causes

The database I/O is high for a long time.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether the D or Z process exists on the node where the alarm is generated.

You can view the **instance_name** field in the **Location Info** or **Other Information** in the alarm details to locate the instance name and cluster name.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

1. Run the following command to switch to the **Ruby** user:
su - Ruby
2. Run the following command to check whether there are D or Z processes on the node:

```
ps -elf | grep -w /DWS/manager/app | awk '{if($3~"Ruby") {print $4,$15}}' | grep -E "Z|D"
```

Step 3 If a D or Z process is found, discuss with the customer for a time window to restart the host during off-peak hours or when no service is running.

Step 4 After the cluster is restarted, log in to the instance node of the tenant cluster and check whether the process is normal.

----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.2.38 2078918236 Intermittent Network Disconnection or Network Delay Between DWS Nodes (ALM_AI_AbnormalNetwork)

Alarm Description

In the results of 10 ping operations, there are three communication records in which the latency is greater than 1s or the intermittent disconnection rate is greater than 40%.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
2078918236	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceIdName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If this alarm is generated, the network between database nodes is abnormal. The network is intermittently disconnected or delayed.

System Actions

None

Possible Causes

The network is unstable.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Obtain the target IP address and peer IP address in the alarm information.

You can view the **instance_name** field in the **Location Info** or **Other Information** in the alarm details to locate the instance name and cluster name.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

1. Run the following command to switch to the **Ruby** user:

su - Ruby

2. Ping the two IP addresses to check whether delay and intermittent disconnection occur.

Step 3 If delay or intermittent disconnection occurs and service processing is affected, contact network engineers to rectify the fault.

----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.2.39 2078919291 Data Instance Generates Core Files (ALM_AI_CoreFile)

Alarm Description

CNs, DNs, or GTMs on the current node are abnormal, and core files are generated.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
207891929 1	Tenant plane alarm	Major	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If this alarm is generated, there are abnormal CN, DN, or GTM processes. Services are unavailable during the generation of a core dump.

System Actions

After a core dump occurs on a CN, DN, or GTM process, the instance will be restarted by the CM instance. Then, the cluster becomes normal.

Possible Causes

This problem is caused by an internal bug of the database. You need to locate and analyze the problem based on the core dump file.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Check whether core files are generated for the instance.

You can view the **instance_name** field in the **Location Info** or **Other Information** in the alarm details.

You can view the possible causes field in other information to locate the data instance directory corresponding to the core file.

Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#).

1. Run the following command to switch to the **Ruby** user:

su - Ruby

2. Run the following command to access the sandbox.

ssh `hostname -i`

3. Go to the data instance directory corresponding to the core file and check whether the core file is generated.

ls Data_instance_directory/core

Step 3 If core files exist and the SRE has the permission to run the **gdb** command, perform the following operations. Otherwise, skip this step.

 **NOTE**

The debug_tools plug-in is a built-in tool set, which can be used to debug and locate kernel problems.

1. Based on your instance name, log in to the instance node in the tenant cluster by referring to [Logging In to a Node in the Tenant Cluster](#). Run the following command to check whether the debug_tools plug-in has been deployed on the alarm reporting instance node outside the sandbox:

su - Ruby

gdb --version

2. If it is not deployed, perform the following operations to deploy it. Otherwise, skip this step.

1. Log in to Service CM and choose **Data Warehouse Service**.

2. Select **Upgrade Management** and perform aggregation upgrade for the cluster.

3. Log in to the instance node of the tenant cluster and run the following command outside the sandbox to obtain the core file information: The GaussDB process is used as an example.

su - Ruby

**gdb /var/chroot/DWS/manager/app/bin/gaussdb /var/chroot/
Data_instance_directory/core**

bt

4. Save the core file information and delete the core file.

5. O&M engineers contact R&D engineers of the database vendor to analyze and resolve the core dump problem.

Step 4 Collect logs of the instance node for which the alarm is generated.

1. Log in to Service CM and choose **Data Warehouse Service**.

2. Choose **Resource Management > Instance**, select the namespace based on the node where the instance is reported, and enter the name of the instance for which the alarm is generated. Select **Collect Log** from the **Operation** column. Collect logs generated in the corresponding period based on the alarm reporting time.

3. In the **Operation** column, select **More > View Log** to download and save the collected logs.

4. O&M engineers contact R&D engineers of the database vendor to analyze and resolve the core dump problem.

----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.2.40 6000000000 GDS-KAFKA Pipeline Abnormal

Description

After a user purchases a gds-kafka instance on the data migration page and creates a data migration job, a gds-kafka worker process is created in the background. The worker process generates the same number of consumer threads (pipeline threads) as that of the partitions of kafka topics, when the pipeline thread abnormally stops, an exception alarm is reported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
6000000000 0	Tenant plane alarm	Critical	Operation alarm	GaussDB(D WS)	Yes

Alarm Parameters



The number of parameters varies according to alarms.

Type	Parameter	Description
Location Info	instance_id	ID of the instance for which the alarm is generated
	instance_name	Name of the instance that reports the alarm
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated
	datastore_type	Type of the data storage for which the alarm is generated
	instance_role	Role of the instance for which the alarm is generated
	component_instance_name	Name of the component instance that reports the alarm, for example, cn_5001 .

Type	Parameter	Description
Other Information	CloudService	Name of the cloud service for which the alarm is generated
	resourceId	Resource ID for which the alarm is generated
	resourceName	Resource for which the alarm is generated
	domain_name	Domain name for which the alarm is generated
	domain_id	Domain ID for which the alarm is generated

Impact on the System

If this alarm is generated, the consumer thread corresponding to the gds-kafka data migration job stops consuming messages due to an exception. In this case, you need to locate the fault to prevent kafka.partition messages from being stacked and aged, causing message loss.

System Actions

None

Possible Causes

1. The Kafka server is abnormal. As a result, the pipeline thread of gds-kafka cannot connect to the Kafka server, and an alarm is generated.
2. The GaussDB(DWS) database is abnormal. For example, the connection times out. As a result, data cannot be imported to the database, the pipeline thread breaks down, and an alarm is generated.
3. There are other exceptions, such as performance exceptions (such as OOM), service logic bugs, and dirty data generated by Kafka.

Handling Procedure

Step 1 View the logs of the gds-kafka instance.

1. After you log in to an O&M pod, switch to the **opsTool** directory from the default directory **3rdComponent**.

```
cd opsTool
```
2. Run the following command to log in to the cluster instance: The username, host IP address, and port number are obtained in the [Querying MySQL Database Information](#). Cluster instance ID, which is obtained in [Querying the Cluster Instance ID](#).

```
sh connectTool.sh -u Username -drms -h Host_IP -p Port_number -n Instance_ID -t Standalone
```

3. Go to the working directory of the migration job.
`cd /var/chroot/DWS/data1`
4. Go to the target directory based on the migration job ID and view **logs/GDS-Kafka.log** to locate the exception cause.

Step 2 Rectify the fault and restart the migration job.

----End

Alarm Clearance

After the fault is rectified, the alarm is automatically cleared.

Related Information

None

2.3 Alarms of Managed Physic Machine Clusters

2.3.1 Description

The GaussDB(DWS) management console can manage GaussDB(DWS) PM clusters. Alarms of the PM clusters can be reported through ManageOne Maintenance Portal.

2.3.2 ALM-12001 Audit Log Dump 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 because 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12001	Tenant plane alarm	Minor	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	Source	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Specifies the name of the role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The system can only store a maximum of 50 dump files locally. If the fault persists on the dump server, the local audit log may be lost.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **Audit > Configuration**.

Step 3 Check whether the value of "SFTP IP" on the **Audit Dumping Configuration** page is valid.

Log in to a management node as user **root** and run the **ping** command to check whether the network connection between the SFTP server and the cluster is normal. The password is specified by users before the installation. Obtain it from the system administrator. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

- If yes, go to [Step 6](#).
- If no, go to [Step 4](#).

Step 4 Restore the network connection, reconfigure the SFTP server password, and click **OK** to deliver the configuration again.

Step 5 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 6](#).

Check whether the username, password, or dump directory are correct.

Step 6 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 9](#).
- If no, go to [Step 7](#).

Step 7 Change the user name, password, and dump directory, and click **OK** to deliver the configuration again.

Step 8 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 9](#).

Check whether the disk space of the dump directory is sufficient.

Step 9 Log in to the third-party server as user **root** based on the current dump directory on the dump configuration page. Run **df** to check whether the disk space of the dump directory on the third-party server is greater than 100 MB.

- If yes, go to [Step 12](#).
- If no, go to [Step 10](#).

Step 10 Expand the disk space of the third-party server, reconfigure the SFTP server password, and click **OK** to deliver the configuration again.

Step 11 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 12](#).

Reset the dump rule.

Step 12 On FusionInsight Manager, choose **Audit > Configuration**.

Step 13 Reset dump rules, set the parameters properly, and click **OK**.

Step 14 Wait for 2 minutes, view real-time alarms and check whether the alarm is cleared.

- If the service is normal, 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 OmmServer 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.3 ALM-12004 OLdap Resource Is 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 Manager recovers and the alarm handling is complete.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12004	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The Manager and component WebUI authentication services are unavailable and cannot provide security authentication and user management functions for web upper-layer services. Users may be unable to log in to the WebUIs of Manager and components.

Possible Causes

The LdapServer process in Manager is abnormal.

Handling Procedure

Check whether the LdapServer process in Manager is normal.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the active management node where FusionInsight Manager resides as user **omm**.

You can 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 view the current Manager HA information.

Step 3 Run `ps -ef | grep slapd` to check whether the LdapServer resource process in the `${BIGDATA_HOME}/om-server/om/` directory of the configuration file is running properly.

 NOTE

You can determine that the resource is normal as follows:

1. Run `sh ${BIGDATA_HOME}/om-server/om/sbin/status-oms.sh` and find that **ResHASatus** of the OLdap process is **Normal**.
2. Run `ps -ef | grep slapd` and find that the slapd process occupies port 21750.
 - If yes, go to [Step 4](#).
 - If no, go to [Step 5](#).

Step 4 Run the pid command of the `kill -2 ldap` process and wait for 20 seconds. HA automatically starts the oldap process. Check whether the status of the OLdap resource is normal.

- If yes, no further action is required.
- If no, go to [Step 5](#).

Collect fault information.

Step 5 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 6 Select **OmsLdapServer** and **OmmServer** for **Service**.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.4 ALM-12005 OKerberos Resource Is 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 alarm handling is complete and the Kerberos resource status recovers.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12005	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is 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 OKerberos depends is abnormal.

Handling Procedure

Check whether the OLDap resource on which OKerberos depends is abnormal in Manager.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the active management node where FusionInsight Manager resides 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` script to view the current Manager HA information.

Step 3 Run the `sh ${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh` command to check whether the status of the OLdap resource managed by HA is normal. In single-node system, the OLdap resource is in the **Active_normal** state. In dual-node system, 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 5](#).
- If no, go to [Step 4](#).

Step 4 Rectify the fault by following the instructions in [ALM-12004 OLdap Resource Is Abnormal](#). After the OLdap resource status is recovered, check whether the OKerberos resource status is recovered.

- If yes, no further action is required.
- If no, go to [Step 5](#).

Collect fault information.

Step 5 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 6 Select OmsKerberos and OmmServer for Service.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.5 ALM-12006 Node Fault

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12006	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Services on the node are unavailable.

Possible Causes

The network is disconnected, the hardware is faulty, or the operating system runs slowly.

Handling Procedure

Check whether the network is disconnected, whether the hardware is faulty, or whether the OS runs commands slowly.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 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 3 Log in to the active management node as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

Step 4 Run the **ping Faulty_host_IP_address** command to check whether the faulty node is reachable.

- If yes, go to [Step 13](#).
- If no, go to [Step 5](#).

Step 5 Contact the network administrator to check whether the network is faulty.

- If yes, go to [Step 6](#).
- If no, go to [Step 7](#).

Step 6 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If the service is normal, no further action is required.
- If no, go to [Step 7](#).

Step 7 Contact the system administrator to check whether the node hardware (CPU or memory) is faulty.

- If yes, go to [Step 8](#).
- If no, go to [Step 13](#).

Step 8 Repair or replace the faulty components and restart the node. Check whether the alarm is cleared.

 **NOTE**

If the node hardware is faulty, rectify the fault by following the instructions provided in "Emergency Handling > Common Emergency Faults > Replacing a Faulty Node" in Data Warehouse Service (DWS) 8.1.3.331 Troubleshooting (for Huawei Cloud Stack 8.3.1).

- If the service is normal, no further action is required.

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

Step 9 If a large number of node faults are reported in the cluster, the floating IP address resource may be abnormal. As a result, the controller cannot detect the agent heartbeat.

Log in to any faulty node and view the **/var/log/Bigdata/omm/oms/ha/scriptlog/floatip.log** file to check whether the logs generated one to two minutes before and after the fault occurs are complete.

- If yes, go to **Step 13**.
- If no, go to **Step 10**.

Step 10 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 11**.
- If no, go to **Step 13**.

Step 11 View the **/var/log/message** file of the OS to check whether sssd frequently restarts or nsqd exception information is displayed when the fault occurs. For Red Hat, check sssd information. For SUSE, check nsqd 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 of nsqd exception information

```
Feb 11 11:44:42 10-120-205-33 nsqd: 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 12**.
- If no, go to **Step 13**.

Step 12 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.

Collecting fault information

Step 13 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 14 In the **Services** area, select the following nodes:

- NodeAgent
- Controller
- OS

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.6 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 status is Bad for three consecutive times.

This alarm is cleared when the process can be connected.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12007	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The service provided by the process is unavailable.

Possible Causes

- The instance process is abnormal.
- The drive space is insufficient.



If a large number of process fault alarms are generated in the same period, files in the installation directory may be deleted by mistake or the permission on the files may be modified.

Handling Procedure

Check whether the instance process is abnormal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click to view the host name and service name for which the alarm is generated.

- Step 3** On the Alarms page, check whether the **ALM-12006 Node Fault** alarm is generated.

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

- Step 4** Handle the alarm by following the steps provided in **ALM-12006 Node Fault**.

- Step 5** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. Check in the installation directory whether the user, user group, and permission are normal. The correct user, user group, and the permission are **omm**, **ficommon**, and **750**, respectively.

- If yes, go to **Step 7**.
- If no, go to **Step 6**.

Step 6 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 7 Wait 5 minutes and check whether the ALM-12007 Process Fault alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to **Step 8**.

Check whether the disk space is insufficient.

Step 8 On FusionInsight Manager, check whether the alarm list contains ALM-12017 Insufficient Disk Capacity.

- If yes, go to **Step 9**.
- If no, go to **Step 12**.

Step 9 Rectify the fault by following the steps provided in [ALM-12017 Insufficient Disk Capacity](#).

Step 10 Wait 5 minutes and check whether the ALM-12017 Insufficient Disk Capacity alarm is cleared.

- If yes, go to **Step 11**.
- If no, go to **Step 12**.

Step 11 Wait for 5 minutes and check whether the alarm is cleared.

- If the service is normal, 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 Based on the service name obtained in **Step 2**, select the corresponding component and NodeAgent in the **Services** area.

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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.7 ALM-12010 Manager Heartbeat Interruption Between the Active and Standby Nodes

Alarm Description

This alarm is generated when the active Manager does not receive any 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12010	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is 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, an active/standby failover cannot be performed, and services are affected.

Possible Causes

- The link between the active and standby Manager servers is abnormal.

- The node name is incorrect.
- The port is disabled on the firewall.

Handling Procedure

Check whether the network between the active and standby Manager servers is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm, click , and view the IP address of the standby Manager server (Peer Manager).

- Step 3** Log in to the active Manager server. The password is specified by users before the installation. Obtain it from the system administrator as user **root**. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

- Step 4** Run the **ping standby Manager heartbeat IP address** command to check whether the standby Manager server can be pinged.

- If yes, go to [Step 7](#).
- If no, go to [Step 5](#).

- Step 5** Contact the network administrator to check whether the network is faulty.

- If yes, go to [Step 6](#).
- If no, go to [Step 7](#).

- Step 6** Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If the service is normal, no further action is required.
- If no, go to [Step 7](#).

Check whether the node name is correct.

- Step 7** Go to the software installation directory.

cd /opt

- Step 8** Search for the configuration file directories on the active and standby nodes.

find -name hacom_local.xml

Step 9 Go to the workspace directory.

cd \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/local/hacom/conf/

Step 10 Run the **vim** command to open the **hacom_local.xml** file and check whether the local and peer nodes are correctly configured. The local node is configured as the primary node, and the peer node is configured as the standby node.

- If yes, go to [Step 13](#).
- If no, go to [Step 11](#).

Step 11 Modify the configuration of the primary and standby nodes in **hacom_local.xml**. After the modification, press **Esc** to return to the CLI, and run **:wq** to save the modification and exit.

Step 12 Check whether the alarm is cleared automatically.

- If the service is normal, no further action is required.
- If no, go to [Step 13](#).

Check whether the port is disabled by the firewall.

Step 13 Run **lsof -i :20012** to check whether the heartbeat ports on the primary and standby nodes are enabled. If the ports are displayed in the command output, they are enabled. Otherwise, the ports are disabled by the firewall.

- If yes, go to [Step 14](#).
- If no, go to [Step 17](#).

Step 14 Run the **iptables -P INPUT ACCEPT** command to prevent disconnection from the server.

Step 15 Clear the firewall.

iptables -F

Step 16 Check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 17](#)

Collect fault information.

Step 17 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 18 In the **Services** area, select the following nodes:

- OmmServer
- Controller
- NodeAgent

Step 19 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 20 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.8 ALM-12011 Data Synchronization Exception Between the Active and Standby Manager 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 node fails to synchronize files with the active Manager node.

This alarm is cleared when the standby Manager synchronizes files with the active Manager.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12011	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.
	Local Manager HA Name	Local Manager HA.
	Peer Manager HA Name	Peer Manager HA.

Impact on the System

Because the configuration files on the standby Manager are not updated, some configurations will be lost after an active/standby switchover. Manager and some components may not run properly.

Possible Causes

The link between the active and standby Manager nodes is disconnected, and the storage space of the `/srv/BigData/LocalBackup` directory is full.

Handling Procedure

Check whether the network between the active and standby Manager servers is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click to obtain the IP address of the standby Manager (peer manager).
- Step 3** Log in to the active Manager server as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **ping Standby Manager IP address** command to check whether the standby Manager server is reachable.
- If yes, go to [Step 7](#).
 - If no, go to [Step 5](#).
- Step 5** Contact the network administrator to check whether the network is faulty.
- If yes, go to [Step 6](#).
 - If no, go to [Step 7](#).
- Step 6** Rectify the network fault and check whether the alarm is cleared from the alarm list.
- If the service is normal, no further action is required.
 - If no, go to [Step 7](#).

Check whether the storage space of the **/srv/BigData/LocalBackup** directory is full.

Step 7 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 8](#).
- If no, go to [Step 11](#).

Step 8 Run the following command to clear unnecessary backup files:

rm -rf Directory to be cleared

Examples are as follows:

rm -rf /srv/BigData/LocalBackup/0/default-oms_20191211143443

Step 9 On FusionInsight Manager, choose **O&M > Backup and Restore > 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 10 Wait about 1 minute and check whether the alarm is cleared.

- If the service is normal, 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 from **Services** and click **OK**.

- OmmServer
- Controller
- NodeAgent

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.9 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12012	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

The time on the node is inconsistent with the time on other nodes in the cluster. Therefore, some FusionInsight applications on the node may not run properly.

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 ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** to 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 in the command output, go to [Step 3](#).
- If **ntp** is displayed in the **ResName** column in the command output, go to [Step 21](#).

 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 2](#) again. If both **chrony** and **ntp** persist, contact text personnel.

Check whether the chrony service on the node is started properly.

- Step 3** Go to FusionInsight Manager. In the alarm list, click  in the row containing the alarm, and view the name of the host for which the alarm is generated in **Location Info**.

- Step 4** Check whether the **chronyd** process is running on the node using the following method. 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 information about the **chronyd** process.
- If yes, go to [Step 7](#).
 - If no, go to [Step 5](#).

- Step 5** Run the **systemctl chronyd start** command to start the NTP service. Currently, only CentOS/Red Hat 7.0 or later is supported.

- Step 6** Wait 10 minutes and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 7](#).

Check whether the current node can synchronize time properly with the chrony service on the active OMS node.

- Step 7** 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 8](#).
 - If no, go to [Step 18](#).

- Step 8** 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. For example:

```
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 9](#).
- If no, go to [Step 39](#).

- Step 9** 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 the UDP port 123 and port 323 are not disabled. (For details, see the firewall configuration policy of each system.)

- Step 10** Wait for 10 minutes and check whether the alarm is cleared.
- If yes, no further action is required.
 - If no, go to [Step 11](#).

- Step 11** 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 **1M**:

Run the **cat \${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys** command on the Red Hat system.

- Step 12** Run the following command to check whether the key value is the same as the value queried in [Step 11](#):

Run the **diff \${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/chrony.keys** command on the Red Hat system.

 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 M sdYbq;o^CzEAWo<U=Tw5  
host01:~ # diff ${BIGDATA_HOME}/om-server/OMS/workspace/conf/chrony.keys /etc/chrony.keys  
host01:~ #
```

- If yes, go to [Step 13](#).
- If no, go to [Step 39](#).

Step 13 Run the **cat \${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile** command to check whether the key value is the same as the value queried in [Step 11](#). (Compare it with the key value whose authentication key index is **1M** in the command output shown in [Step 11](#).)

- If yes, go to [Step 14](#).
- If no, go to [Step 16](#).

Step 14 Log in to the faulty node as user **root** and run the **cat /etc/chrony.keys** command in the Red Hat system to check whether the key value is the same as the value queried in [Step 13](#) (use the key value of the authentication key index field **1M** for comparison).

- If yes, go to [Step 39](#).
- If no, go to [Step 15](#).

Step 15 Run the **su - omm** command to switch to user **omm**, change the key value of the authentication key index field **1M** in **\${NODE_AGENT_HOME}/chrony.keys** to the key value of **ntpKeyFile** in [Step 13](#), and go to [Step 17](#).

Step 16 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 a Red Hat system):

```
cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf  
sed -i " `cat chrony.keys | grep -n '1 M' | awk -F ':' '{print $1}'` ``d" chrony.keys  
echo "1 M `cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/  
ntpKeyFile`" >> chrony.keys
```

Check whether the key value of the authentication key index being "1M" in "chrony.keys" is the same as the key value of "ntpKeyFile".

- If yes, go to [Step 17](#).
- If no, manually change the key value whose authentication key index field is **1M** in **chrony.keys** to the key value of **ntpKeyFile** and go to [Step 17](#).

Step 17 After 5 minutes, run the **systemctl chronyd restart** command to restart the **chrony** service on the active OMS node. After 15 minutes, check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 39](#).

Check whether the time deviation between the node and the chrony service on the active OMS node is large.

Step 18 Check whether the additional information of the NTP alarm indicates that the time offset is too large.

- If yes, go to [Step 19](#).
- If no, go to [Step 39](#).

Step 19 On the **Hosts** tab, 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 offset 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 20 Wait 10 minutes and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 39](#).

Check the NTP service on the current node.

Step 21 Go to FusionInsight Manager. In the alarm list, click  in the row containing the alarm, and view the name of the host for which the alarm is generated in **Location Info**.

Step 22 Check whether the ntpd process is running on the node using the following method. Log in to the The password is specified by users before the installation. Obtain it from the system administrator. node for which the alarm is generated as user **root** and run the **ps -ef | grep ntpd | grep -v grep** command to check whether the ntpd process information is displayed.

- If yes, go to [Step 25](#).
- If no, go to [Step 23](#).

Step 23 Run the "**service ntpd start**" command in RedHat OS to start the NTP service.

Step 24 Wait 10 minutes and check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 25](#).

Check whether the current node can synchronize time properly with the NTP service on the active OMS node.

Step 25 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 26](#).
- If no, go to [Step 36](#).

Step 26 Check whether the NTP service on the active OMS node is normal. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

Log in to the 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 27](#).
- If no, go to [Step 39](#).

Step 27 The NTP synchronization failure is usually related to 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 the UDP port 123 is not disabled. (For details, see the firewall configuration policy of each system.)

Step 28 Wait for 10 minutes and check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to [Step 29](#).

Step 29 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 **1M**:

SUSE: **cat \${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys**

Red Hat: **cat \${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys**

Step 30 Run the following command to check whether the key value is the same as the value queried in [Step 29](#):

SUSE: **diff \${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntp.keys /etc/ntp.keys**

Red Hat: **diff \${BIGDATA_HOME}/om-server/OMS/workspace/conf/ntpkeys /etc/ntp/ntpkeys**



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 31](#).

- If no, go to [Step 39](#).

Step 31 Run the `cat ${BIGDATA_HOME}/om-server/om/packaged-distributables/ntpKeyFile` command to check whether the key value is the same as the value queried in [Step 29](#). (Compare it with the key value whose authentication key index is **1M** in the command output shown in [Step 29](#).)

- If yes, go to [Step 32](#).
- If no, go to [Step 34](#).

Step 32 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 Linux) to check whether the key value is the same as the value queried in [Step 31](#) (use the key value of the authentication key index field **1M** for comparison).

- If yes, go to [Step 39](#).
- If no, go to [Step 33](#).

Step 33 Run the `su - omm` command to switch to user **omm**, change the key value of the authentication key index field **1M** in `${NODE_AGENT_HOME}/ntp.keys` (`${NODE_AGENT_HOME}/ntpkeys` in Red Hat Linux) to the key value of `ntpKeyFile` in [Step 31](#), and go to [Step 35](#).

Step 34 Run the following command as user **root** or **omm** to change the NTP key value on the active OMS node (change `ntp.keys` to `ntpkeys` in a Red Hat system):

```
cd ${BIGDATA_HOME}/om-server/OMS/workspace/conf  
sed -i "`cat ntp.keys | grep -n '1 M'|awk -F ':' '{print $1}`" 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 being **1M** in `ntp.keys` is the same as the key value of `ntpKeyFile`.

- If yes, go to [Step 35](#).
- If no, manually change the key value whose authentication key index field is **1M** in `ntp.keys` to the key value of `ntpKeyFile` and go to [Step 35](#).

Step 35 After 5 minutes, run the `service ntp restart` command to restart the NTP service on the active OMS node. After 15 minutes, check whether the alarm is cleared.

- If the service is normal, no further action is required.
- If no, go to [Step 39](#).

Check whether the time offset between the node and the NTP service on the active OMS node is large.

Step 36 Check whether the additional information of the NTP alarm indicates that the time offset is too large.

- If yes, go to [Step 37](#).
- If no, go to [Step 39](#).

Step 37 On the **Hosts** tab, 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 offset 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 38** Wait 10 minutes and check whether the alarm is cleared.
- If the service is normal, no further action is required.
 - If no, go to **Step 39**.

Collect fault information.

- Step 39** On the FusionInsight Manager portal, choose **O&M > Log > Download**.
- Step 40** In the **Services** area, select **NodeAgent** and **OmmServer**, and set **Host** to the node for which the alarm is generated and the active OMS node.
- Step 41** 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 42** Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.10 ALM-12014 Device Partition Lost

Alarm Description

The system scans the service directory every 60 seconds. 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 goes offline, or the partition is deleted). The system checks the partition status periodically.

This alarm needs to be cleared manually.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12014	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.
	DirName	Directory for which the alarm is generated.
	PartitionName	Device partition for which the alarm is generated.

Impact on the System

Service data fails to be written into the partition, and the service system runs abnormally.

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 the ManageOne alarm platform to obtain the alarm information.

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, click O&M > Alarm > Alarms, and click  in the row where the alarm is located.

Step 3 Obtain **HostName**, **PartitionName**, and **DirName** from **Location Info**.

Step 4 Check whether the disk of **PartitionName** on **HostName** is inserted to the correct server slot.

- If yes, go to [Step 5](#).
- If no, go to [Step 6](#).

Step 5 Contact hardware engineers to remove the faulty disk.

Step 6 Log in to the host for which the alarm is generated as user **root**, and check whether the file in the /etc/fstab directory contains **DirName**. The password is specified by users before the installation. Obtain it from the system administrator.

- If yes, go to [Step 7](#).
- If no, go to [Step 8](#).

Step 7 Run the **vi /etc/fstab** command to edit the file and delete the line containing **DirName**.

Step 8 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 9 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 **DirName** directory.

- If yes, manually clear the alarm. No further operation is required.
- If no, go to [Step 10](#).

Collect fault information.

Step 10 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 11 Select **OmmServer** 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 send 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

2.3.11 ALM-12015 Device Partition File System Read-Only

Alarm Description

The system scans the device partition 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12015	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.
	DirName	Directory for which the alarm is generated.
	PartitionName	Device partition for which the alarm is generated.

Impact on the System

Service data fails to be written into the partition, and the service system runs abnormally.

Possible Causes

The disk is faulty, for example, a bad sector exists.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, click O&M > Alarm > Alarms, and click  in the row where the alarm is located.

Step 3 In the **Alarm Details** area, obtain **HostName** and **PartitionName** from **Location Info**. **PartitionName** indicates the partition of the faulty disk.

Step 4 Contact hardware engineers to check whether the disk is faulty. If the disk is faulty, remove it from the server.

Step 5 After the disk is removed, the system reports ALM-12014 Partition Lost. Handle the alarm by following the instructions in [ALM-12014 Device Partition Lost](#). After the handling, the alarm is automatically cleared.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.12 ALM-12016 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. 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.

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12016	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

- The alarm threshold or alarm trigger count is improperly configured.
- The CPU configuration cannot meet service requirements. 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 the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

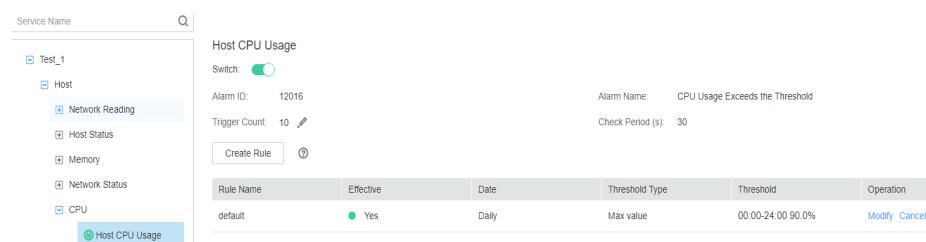
Step 2 Change the alarm threshold and alarm trigger count based on CPU usage.

Choose **O&M > Alarm > Thresholds > Name of the target cluster > Host > CPU > Host CPU Usage** to change the trigger count based on the actual service usage, as shown in [Figure 2-2](#).

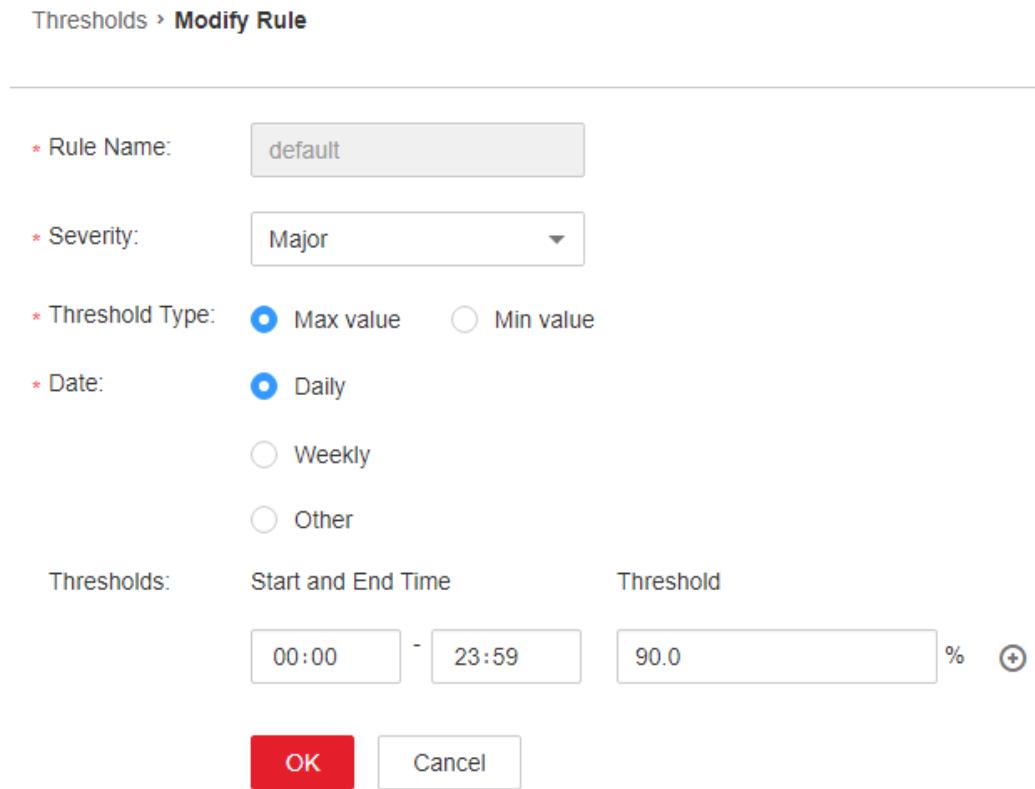
 **NOTE**

The alarm is generated when the process usage exceeds the threshold for the times specified by **Trigger Count**.

Figure 2-2 Setting alarm trigger count



Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > CPU > Host CPU Usage** to change the alarm threshold based on the actual service usage, as shown in [Figure 2-3](#).

Figure 2-3 Setting alarm threshold

Step 3 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 4**.

Check whether the CPU usage reaches the upper limit.

Step 4 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click to view the IP address of the node for which the alarm is generated.

Step 5 On the **Hosts** page, click the node 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 cluster administrator to increase the CPU threshold.

Step 7 Check whether the alarm is cleared.

- If yes, no further operation 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 OmmServer for 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.13 ALM-12017 Insufficient Disk Capacity

Alarm Description

The system checks the disk usage every 30 seconds and compares the actual disk usage with the threshold. There is a default threshold for the disk usage. This alarm is generated when the disk usage exceeds the 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12017	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	DirName	Directory for which the alarm is generated.
	PartitionName	Device partition for which the alarm is generated.

Impact on the System

Service processes become unavailable.

Possible Causes

- The alarm threshold is improperly configured.
- The disk configuration cannot meet service requirements. The disk usage reaches the upper limit.

Handling Procedure

Check whether the threshold is set properly.

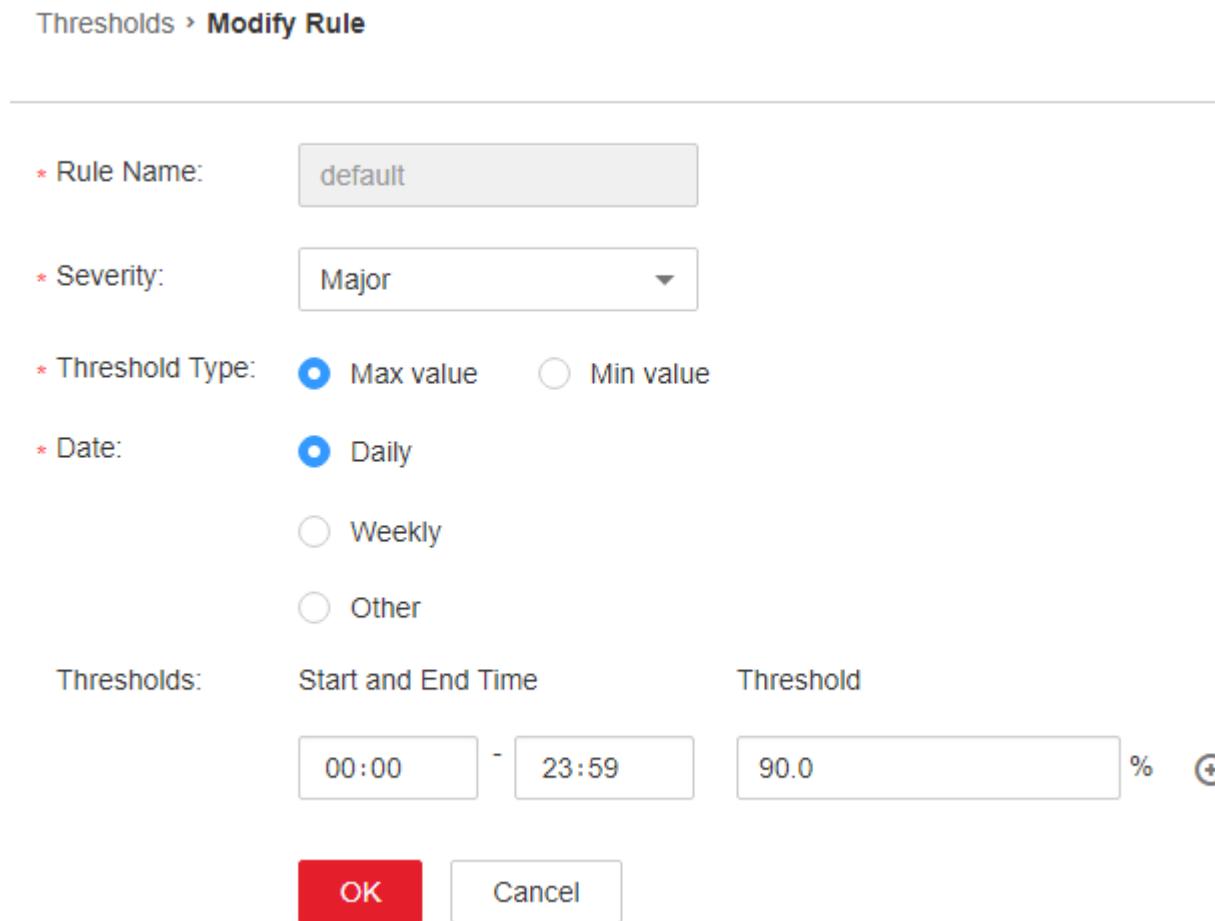
- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to FusionInsight Manager and check whether the threshold (configurable, 90% by default) is appropriate.
- If yes, go to [Step 3](#).
 - If no, go to [Step 5](#).

- Step 3** Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Disk > Disk Usage** and change the alarm threshold based on site requirements. See [Figure 2-4](#).

Figure 2-4 Setting alarm threshold

Step 4 Wait 2 minutes and check whether the alarm is cleared.

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

Check whether the disk space usage reaches the upper limit.

Step 5 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 6 Log in to the node for which the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 7 Run the `df -lmp | awk '$2 != "iso9660" | grep '^/dev/' | awk '{readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1` command to check the usage of disk partitions. Check whether the disk is mounted to the following directories based on the disk partition name obtained in **Step 5**: `/`, `/opt`, `/tmp`, `/var`, `/var/log`, and `/srv/BigData` (which can be customized).

- If yes, the disk is a system disk. Go to **Step 11**.
- If no, the disk is not a system disk. Then go to **Step 8**.

Step 8 Run the `df -lmp | awk '$2 != "iso9660" | grep '^/dev/' | awk '{readlink -m "$1 | getline real }{$1=real; print $0}' | sort -u -k 1,1` command to check the

usage of disk partitions. Determine the role of the disk based on the disk partition name obtained in [Step 5](#).

Step 9 Check the service to which the disk belongs.

If it is GaussDB(DWS) for MPPDB, adjust the capacity. Go to Step 9.

- If yes, adjust the capacity by following the instructions provided in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Capacity Adjustment Guide. Then go to [Step 10](#).
- If no, go to [Step 13](#).

Step 10 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 13](#).

Step 11 Run the `find / -xdev -size +500M -exec ls -l {} \;` command to view files larger than 500 MB on the node. Check whether such files are written to the disk.

- If yes, go to [Step 12](#).
- If no, go to [Step 13](#).

Step 12 Handle the large files and check whether the alarm is cleared 2 minutes later.

- If yes, no further action is required.
- If no, go to [Step 13](#).

Step 13 Contact the system administrator to expand the disk capacity.

Step 14 Wait 2 minutes and check whether the alarm is cleared.

- If yes, no further operation 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 OMS from the Services drop-down list.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.14 ALM-12018 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. The memory usage has a default threshold. This alarm is generated when 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.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12018	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Processes respond slowly or do not work.

Possible Causes

- Memory configuration cannot meet service requirements. The memory usage reaches the threshold.
- 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 the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to any node in the cluster as user **root** and run the **cat /etc/*-release** command to check whether the current OS is SUSE 12.X. The password is specified by users before the installation. Obtain it from the system administrator.
- If yes, go to [Step 3](#).
 - If no, go to [Step 5](#).

- Step 3** Run the **cat /proc/meminfo | grep Mem** command to check the actual memory usage of the current operating system.

```
MemTotal: 263576192 kB  
MemFree: 198283116 kB  
MemAvailable: 227641452 kB
```

- Step 4** Calculate the actual memory usage. Memory usage = 1 - (MemAvailable/MemTotal).

- If the actual memory usage is lower than 90%, manually disable the monitoring-to-alarm function. For details, see section "Configuring Thresholds" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide.
- If the actual memory usage is higher than 90%, go to [Step 5](#).

Perform capacity expansion for the system.

- Step 5** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address for which the alarm is generated.

- Step 6** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

- Step 7** If the memory usage exceeds the threshold, expand the memory capacity. For details, see Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Capacity Adjustment Guide.

- Step 8** Run **free -m | grep Mem\|: | awk '{printf("%s,", (\$3-\$6-\$7) * 100 / \$2)}'** to check the system memory usage.

Step 9 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- 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 **OmmServer** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.15 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 threshold. This alarm is generated when 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12027	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

No PID is available for new processes and service processes are unavailable.

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** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to obtain the IP address of the host for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 4 Run the `cat /proc/sys/kernel/pid_max` command to check the value of `pid_max`.

Step 5 If the PID usage exceeds the threshold, double the value of `pid_max` by running the `echo new value of pid_max > /proc/sys/kernel/pid_max` command.

Example: `echo 65536 > /proc/sys/kernel/pid_max`

Step 6 Wait 5 minutes and check whether the alarm is cleared.

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

Collect fault information.

Step 7 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 8 Select all services in the **Services** area.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.16 ALM-12028 Number of Processes in the D State on the Host Exceeds the Threshold

Alarm Description

The system periodically checks the number of D state processes of user **omm** on the host every 30 seconds and compares the number with the threshold. The number of D state processes has a default threshold. This alarm is generated when the number of host D state processes exceeds the threshold.

This alarm is cleared when the alarm trigger count is 1 and the total number of processes in the D state of user **omm** on the host does not exceed the threshold. This alarm is cleared when the alarm trigger count is greater than 1 and the total number of processes in the D state of user **omm** on the host is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12028	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Excessive system resources are used and the service process responds slowly.

Possible Causes

The host responds slowly to I/O (disk I/O and network I/O) requests and a process is in the D state.

Handling Procedure

Check the process that is in the D state.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address for which the alarm is generated.

Step 3 Log in to the host for which the alarm is generated as user **root** and run the **su - omm** command to switch to user **omm**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 4 Run the following command to view the PID of the process of user omm that is in the D state:

```
ps -elf | grep -v "\[thread_checkio\]" | awk 'NR!=1 {print $2, $3, $4}' | grep omm | awk -F ' ' '{print $1, $3}' | grep D | awk '{print $2}'
```

Step 5 Check whether no command output is empty.

- If yes, the service process is normal. Go to **Step 7**.
- If no, go to **Step 6**.

Step 6 Switch to the **root** user and run the **reboot** command to restart the host for which the alarm is generated. (Restarting the host is risky. Ensure that the service process is normal after the restart.)

Step 7 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation 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 **OMS** from the **Services** drop-down list.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.17 ALM-12029 Invalid License File

Alarm Description

After the cluster is installed, the system checks whether the license file is invalid every 5 minutes. This alarm is generated when the license file is invalid.

This alarm is cleared when the license file is valid.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12029	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The functions provided by the cluster cannot be used properly, and the system prompts the user to update the license.

Possible Causes

- The number of vCPUs in the GaussDB(DWS) cluster exceeds the upper limit allowed by the license.
- This alarm is generated when the license of the GaussDB(DWS) system expires.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **System > License > Cluster name**

Step 3 View the license information to obtain the license capacity and expiration time.

 **NOTE**

If the expiration time is **PERMANENT**, it never expires.

Step 4 For a GaussDB(DWS) cluster, compare the number of vCPUs used by the system with the license capacity, and compare the current system time with the license expiration time.

- If the system capacity exceeds the limit defined in the license file, go to [Step 5](#).
- If the license file expires, go to [Step 7](#).

Step 5 Contact frontline delivery personnel to apply for a new license file that meets the current system requirements, and import and activate the new license file.

Step 6 Check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 9](#).

Step 7 Contact frontline delivery personnel to apply for a new license file for the system, and import and activate the new license file.

Step 8 Check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 9](#).

Step 9 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 10 Select **Controller 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.18 ALM-12030 No Valid License

Alarm Description

After the cluster is installed, the system checks whether a valid license file exists in the system every 5 minutes. This alarm is generated when no valid license file exists.

This alarm is cleared when a valid license file is imported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12030	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The functions provided by the cluster cannot be used, and the system prompts you to import a valid license file.

Possible Causes

No valid license file is imported to the system.

Handling Procedure

Check whether a valid license file exists in the system.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

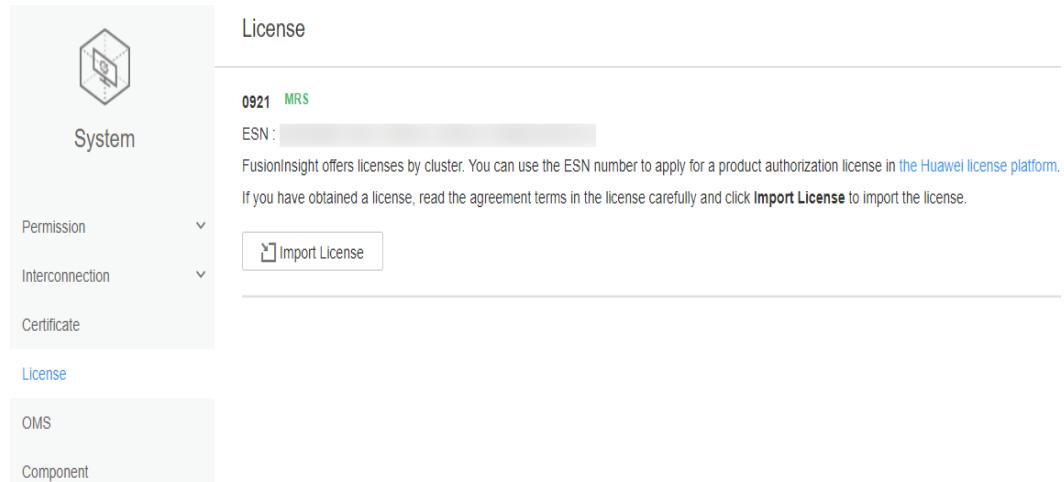
 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On the FusionInsight Manager portal, choose **System > License > Cluster name**.

Step 3 Check whether the page shown in [Figure 1 License page](#) is displayed.

Figure 2-5 License page



- If yes, go to [Step 4](#).
- If no, go to [Step 6](#).

Step 4 Contact frontline delivery personnel to apply for a new license file for the system and import the license file.

Step 5 Check whether the alarm is cleared.

- If yes, no further operation 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 **Controller** from the **Services** 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.19 ALM-12033 Slow Disk Fault

Alarm Description

The system runs the **iostat** command every second to monitor the disk I/O indicator. If the **svctm** value is greater than 100 ms in 300 seconds and 1.5 times greater than the value of **svctm_average**, the disk is faulty and the alarm is generated. If the number of slow periods is greater than 50% within 300s, the system considers that the disk is faulty and reports an alarm.

NOTE

The value of **svctm_average** is the average value of **svctm** of all disks on the current node.

This alarm is automatically cleared after the disk is replaced.

The alarm detecting principle is as follows:

On the Linux platform, run the **iostat -x -t 1** command to check whether the I/O is faulty. Specifically, check values of parameters in the red box in the following figure.

avg-cpu:	%user	%nice	%system	%iowait	steal	%idle						
Device:	rrqm/s	urqm/s	r/s	w/s	rsec/s	usec/s	avgrrq-sz	avgqu-sz	await	svctm	%util	
xvda	0.03	0.60	0.06	0.95	2.53	12.39	14.78	0.00	4.87	0.41	0.04	
xude	0.01	0.82	0.35	0.08	2.90	2.09	11.42	0.00	8.22	0.18	0.01	

- **%iowait**: indicates the percentage of the CPU I/O waiting time to the entire CPU cycle. If the value exceeds 50% or is obviously greater than **%system**, **%user**, or **%idle**, the I/O may be abnormal.
- **await**: indicates the sum of the disk I/O waiting time and I/O service time. Generally, the value does not exceed 20. For other DataNode disks, the value can be slightly greater than 40.
- **svctm**: indicates the disk I/O service time.

- %util: indicates whether the disk is busy. If the value is greater than 80%, the disk is busy.

If the value of **%util** is greater than 10 and the value of svctm is greater than 100, the I/O is recorded as faulty. This alarm is generated when the I/O is recorded as faulty for 30 times in the 60 times of checks.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12033	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	DiskName	Specifies the disk for which the alarm is generated.

Impact on the System

If a slow disk is faulty, the service performance deteriorates, the service processing capability is impeded, and even the service may be unavailable.

Possible Causes

The disk is aged or has bad sectors.

Handling Procedure

Check disk status.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**.

Step 3 View the detailed information about the alarm. Check the values of the **HostName** and **DiskName** fields in the location information to obtain the information about the faulty disk for which the alarm is generated.

Step 4 Check whether the node for which the alarm is generated is in the virtualization environment.

- If yes, go to [Step 5](#).
- If no, go to [Step 8](#).

Step 5 Check whether the storage performance provided by the virtualization environment meets the hardware requirements. Then go to [Step 6](#) after the check is complete.

Step 6 Log in to the node for which the alarm is generated as user **root** and run the **df -h** command to check whether the command output contains the value of the **DiskName** field. The password is specified by users before the installation. Obtain it from the system administrator.

- If yes, go to [Step 8](#).
- If no, go to [Step 7](#).

Step 7 Run the **lsblk** command to check whether the mapping between the values of **DiskName** and disks can be queried.

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 8](#).
- If no, go to [Step 23](#).

Step 8 Log in to the node for which the alarm is generated as user **root**. Run the **lsscsi | grep "/dev/sd[x]"** command to check the disk device information and determine whether RAID is created for the disk. The password is specified by users before the installation. Obtain it from the system administrator.

 NOTE

In the preceding command, `/dev/sd[x]` indicates the name of the disk for which the alarm is generated obtained in [Step 3](#).

Command 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, the disk may have been organized into a RAID group.

- If yes, go to [Step 13](#).
- If no, go to [Step 9](#).

Step 9 Run the `smartctl -i /dev/sd[x]` command to check whether the hardware supports SMART.

Command 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 is displayed, the hardware does not support SMART.

- If yes, go to [Step 10](#).
- If no, go to [Step 18](#).

Step 10 Run the `smartctl -H --all /dev/sd[x]` command to check basic SMART information and determine whether the disk is working correctly.

Command example:

```
smartctl -H --all /dev/sda
```

Check SMART overall-health self-assessment test result in the command output. If the result is FAILED, the disk is faulty and needs to be replaced. If the result is PASSED, check the count of Reallocated_Sector_Ct or Elements in grown defect list. If the count is greater than 100, the disk is faulty and needs to be replaced.

- If yes, go to [Step 11](#).
- If no, go to [Step 19](#).

Step 11 Run the `smartctl -l error -H /dev/sd[x]` command to check the Glist of the disk and determine whether the disk is working correctly.

Command 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 is faulty. The two types of errors indicate that the disk is abnormal and needs to be replaced.

If "No Errors Logged" is displayed, no error log exists. In this case, the disk SMART self-check can be triggered.

- If yes, go to [Step 12](#).
- If no, go to [Step 19](#).

Step 12 Run the **smartctl -t long /dev/sd[x]** command to trigger the disk SMART self-check. After the command is executed, the system displays the time when the self-check is complete. After the self-check is complete, perform [Step 10](#) and [Step 11](#) again to check whether the disk is normal.

Command example:

```
smartctl -t long /dev/sda
```

- If yes, go to [Step 18](#).
- If no, go to [Step 19](#).

Step 13 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** command to check whether the hardware supports SMART.

 NOTE

- **[sat|scsi]** indicates the disk type. The preceding two types need to be used.
- **[DID]** indicates the slot information. Slots 1 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
```

...

Run the commands that combine different disk types and slots. In a command output, if SMART support is: Enabled is displayed, the disk supports SMART. Record the parameters of the disk type and slot combination. If SMART support is: Enabled is not displayed in the outputs of all the preceding command combinations, the disk does not support SMART.

- If yes, go to [Step 14](#).
- If no, go to [Step 17](#).

Step 14 Run the **smartctl -d [sat|scsi]+megaraid,[DID] -H --all /dev/sd[x]** command recorded in [Step 13](#) to check basic SMART information and determine whether the disk is working correctly.

Command example:

```
smartctl -d sat+megaraid,2 -H --all /dev/sda
```

Check SMART overall-health self-assessment test result in the command output. If the result is FAILED, the disk is faulty and needs to be replaced. If the result is PASSED, check the count of Reallocated_Sector_Ct or Elements in grown defect list. If the count is greater than 100, the disk is faulty and needs to be replaced.

- If yes, go to [Step 15](#).
- If no, go to [Step 19](#).

Step 15 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 disk is working correctly.

Command example:

```
smartctl -d sat+megaraid,2 -l error -H /dev/sda
```

Check the Command/Feattrue_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 is faulty. The two types of errors indicate that the disk is abnormal and needs to be replaced.

If "No Errors Logged" is displayed, no error log exists. In this case, the disk SMART self-check can be triggered.

- If yes, go to [Step 16](#).
- If no, go to [Step 19](#).

Step 16 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 system displays the time when the self-check is complete. After the self-check is complete, perform [Step 14](#) and [Step 15](#) again to check whether the disk is normal.

Command example:

```
smartctl -d sat+megaraid,2 -t long /dev/sda
```

- If yes, go to [Step 18](#).
- If no, go to [Step 19](#).

Step 17 If the configured RAID card does not support SMART, the disk usually does not support SMART. In this case, use the check tool provided by the corresponding RAID card vendor to solve the problem. Then go to [Step 18](#).

For example, LSI is a MegaCLI tool.

Step 18 Delete the alarm and check whether such alarm is generated for the same disk continuously.

If the alarm is reported for three times for the current disk, you are advised to replace the disk.

- If yes, go to [Step 19](#).
- If no, no further action is required.

Replace the disk.

Step 19 On FusionInsight Manager, choose **O&M > Alarm > Alarm**.

Step 20 View the detailed information about the alarm to obtain the values of the HostName and the DiskName fields and the information about the faulty disk for which the alarm is generated.

Step 21 Replace the disk. For details, see Emergency Handling > Common Emergency Faults > Hard Disk Troubleshooting in the [Huawei Cloud Stack 8.x.x Data Warehouse Service \(DWS\) Fault Management](#).

Step 22 Check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to [Step 23](#).

Collect fault information.

Step 23 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 24 Select **OMS** from the **Services** drop-down list.

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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.20 ALM-12034 Periodic Backup Failure

Alarm Description

The system executes the periodic backup task every 60 minutes. This alarm is generated when the periodic backup task fails to be executed. This alarm is cleared when the next backup task is successfully executed.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12034	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	DiskName	Specifies the disk for which the alarm is generated.

Impact on the System

No backup package is available for a long time, so the system cannot be restored in case of exceptions.

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** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**.

Step 3 In the alarm list, click the of the alarm and obtain the **TaskName** from **Location Info**.

Step 4 On FusionInsight Manager, choose **O&M > Backup and Restoration > Backup Management**.

Step 5 Search for the backup task based on **TaskName** and click **More** in the **Operation** column. In the displayed dialog box, click **Query History** to view details about the backup task.

Step 6 In the log details window that is displayed, check whether "Failed to backup xx due to insufficient disk space, move the data in the /srv/BigData/LocalBackup directory to other directories." is displayed.

- If yes, go to **Step 7**.
- If no, go to **Step 14**.

Step 7 Click **View** under **Backup Directory** to obtain the directory path.

Step 8 Log in to the node as user **root** and run the following command to view the node mounting details. The password is specified by users before the installation. Obtain it from the system administrator.

df -h

Step 9 Check whether the available space of the node to which the backup path is mounted is less than 20 GB.

- If yes, go to **Step 10**.
- If no, go to **Step 14**.

Step 10 Check whether there are many backup packages in the backup directory.

- If yes, go to **Step 11**.
- If no, go to **Step 14**.

Step 11 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 12 Start the backup task again and check whether the backup task is successfully executed.

- If yes, go to **Step 13**.
- If no, go to **Step 14**.

Step 13 After 2 minutes, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 14**.

Collecting fault information

Step 14 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 15 Select Controller for Service.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.21 ALM-12035 Unknown Data Status After a Restoration Task Fails

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 is successfully executed.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12035	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	DiskName	Specifies the disk for which the alarm is generated.

Impact on the System

The data may be lost or the data status may be unknown, which may affect services.

Possible Causes

The possible cause of this alarm is that the component status does not meet the requirements before the restoration task is executed or an error occurs in a step during the restoration task. The error depends on the task details. You can obtain logs and task details to handle the alarm.

Handling Procedure

Check the component status.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **Cluster > Cluster name > Service** to check whether the current running status of components meets requirements. (OMS and DBService must be normal, and other components must be stopped.)
- If yes, go to [Step 10](#).
 - If no, go to [Step 3](#).

Step 3 Restore the component status as required and start the recovery task again.

Step 4 Log in to FusionInsight Manager and choose **O&M > Alarm > Alarm**.

Step 5 In the alarm list, locate the row that contains the alarm and click  to obtain the task name from **Location Info**.

Step 6 Choose **O&M > Backup and Restoration > Restoration Management**.

Step 7 Find the restoration task by **TaskName** and view the task details.

Step 8 Start the restoration task and check whether the restoration task is successfully executed.

- If yes, go to [Step 9](#).
- If no, go to [Step 10](#).

Step 9 After 2 minutes, 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 portal, choose **O&M > Log > Download**.

Step 11 Select **Controller** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.22 ALM-12036 License File About to Expire

Alarm Description

The system checks the license file in the system every 5 minutes. This alarm is generated when the license file is about to expire in less than 60 days.

This alarm is cleared when a normal license is imported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12036	Tenant plane alarm	Minor	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Users are notified that the license file is about to expire. If the license file expires, some functions are restricted and cannot be used.

Possible Causes

The license file is about to expire.

Handling Procedure

Check whether the license file is about to expire.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On the FusionInsight Manager portal, choose **System > License > Cluster name**.

- Step 3** View the license information to obtain the license expiration time.

 **NOTE**

If the expiration time is **PERMANENT**, it never expires.

- Step 4** Check whether the license expires within 60 days.

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

- Step 5** Contact frontline delivery personnel to apply for a new license file for the system, and import and activate the new license file.

- Step 6** Two minutes later, check whether the alarm is cleared.

- If yes, no further operation 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 **Controller** from the **Services** 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.23 ALM-12037 NTP Server Is Abnormal

Alarm Description

The system checks the NTP server status every 60 seconds. This alarm is generated when the system detects that the NTP server is abnormal for 10 consecutive times.

This alarm is cleared when the NTP server recovers.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12037	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host 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.

Possible Causes

- The NTP server network is faulty.

- The NTP server authentication fails.
- The time cannot be obtained from the NTP server.
- The time obtained from the NTP server is not continuously updated.

Handling Procedure

Check the NTP server network.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the real-time alarm list on FusionInsight Manager, locate the row that contains the alarm and click .

- Step 3** View the **Other Information** to check whether the IP address of the NTP server cannot be pinged.

- If yes, go to [Step 4](#).
- If no, go to [Step 5](#).

- Step 4** 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.
- If yes, no further operation is required.
 - If no, go to [Step 5](#).

Check whether the NTP server authentication fails.

- Step 5** Log in to the active OMS node as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

- Step 6** 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 in the command output, go to [Step 7](#).

- If **ntp** is displayed in the **ResName** column in the command output, go to [Step 8](#).

 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 6](#) again. If both **chrony** and **ntp** persist, contact text personnel.

Step 7 Run the **chronyc sources** command to check whether the authentication between the cluster and the NTP server fails.

If **0** is displayed in **Reach** column of the chrony service, the connection or authentication fails.

- If yes, go to [Step 13](#).
- If no, go to [Step 9](#).

Step 8 Run **ntpq -np** to check whether the NTP server authentication fails.

If the **refid** of the NTP service is **AUTH**, the authentication fails.

- If yes, go to [Step 13](#).
- If no, go to [Step 9](#).

Check whether the time can be obtained from the NTP server.

Step 9 View the **Other Information** to check whether the time cannot be obtained from the NTP server.

- If yes, go to [Step 10](#).
- If no, go to [Step 11](#).

Step 10 Contact the provider of the NTP server to rectify the NTP server fault. After the NTP server is in normal state, check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 11](#).

Check whether the time obtained from the NTP server fails to be updated.

Step 11 View the alarm additional information to check whether the time obtained from the NTP server fails to be updated.

- If yes, go to [Step 12](#).
- If no, go to [Step 13](#).

Step 12 Contact the provider of the NTP server to rectify the NTP server fault. After the NTP server is in normal state, check whether the alarm is cleared.

- If yes, no further operation 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 **NodeAgent** and **OmmServer** for **Services**.

Step 15 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 16 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.24 ALM-12038 Monitoring Indicator Dump 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12038	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The upper-layer management system fails to 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.

Handling Procedure

Check whether the server connection is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Check whether the network connection between FusionInsight Manager and the server is normal.
- 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 the alarm is cleared.
- If yes, no further action is required.
 - If no, go to [Step 4](#).

- Step 4** Choose **System > Interconnection > Upload Performance Data** and check whether the FTP username, password, port, dump mode, and public key are consistent with those on the server.
- If yes, go to [Step 6](#).
 - If no, go to [Step 5](#).

- Step 5** Enter the correct configuration, click **OK**, and check whether the alarm is cleared.
- If yes, no further action is required.
 - If no, go to [Step 6](#).

Check whether the permission on the save path on the server is correct.

Step 6 Choose **System > Interconnection > Upload Performance Data** and view the **FTP User Name, Save Path, and Dump Mode**.

- If the FTP mode is used, go to [Step 6](#).
- If the SFTP mode is used, go to [Step 8](#).

Step 7 Log in to the server in FTP mode. In the default directory, check whether the FTP user name has the read and write permissions on the relative save path.

- If yes, go to [Step 10](#).
- If no, go to [Step 9](#).

Step 8 Log in to the server in SFTP mode and check whether the FTP user name has the read and write permissions on the absolute save path.

- If yes, go to [Step 10](#).
- If no, go to [Step 9](#).

Step 9 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 10](#).

Check whether the save path on the server has sufficient disk space.

Step 10 Log in to the server and check whether the save path has sufficient disk space.

- If yes, go to [Step 12](#).
- If no, go to [Step 11](#).

Step 11 Delete unnecessary files or go to the monitoring indicator dumping configuration page to change the save path. 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 **OMS** from the **Services** drop-down list.

Step 14 Click  in the upper right corner, and set **Start Date** and **End Date** for log collection to 60 minutes ahead of and after the alarm generation time respectively. Then, click **Download**.

Step 15 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.25 ALM-12039 Data Inconsistency Between the Active and Standby OMS Databases

Alarm Description

The system checks the data synchronization status between the active and standby OMS nodes every 10 seconds. This alarm is generated when the synchronization status cannot be queried for 30 consecutive times or the synchronization status is abnormal.

This alarm is cleared when the data synchronization status is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12039	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Specifies the name of the role for which the alarm is generated.
	HostName	Specifies the name of the host for which the alarm is generated.
Other Information	Local GaussDB HA IP	HA IP address of the local GaussDB.
	Peer GaussDB HA IP	HA IP address of the peer GaussDB.
	SYNC_PERCENT	Synchronization percentage.

Impact on the System

The active and standby OMS databases are not synchronized. If the active instance is abnormal, data may be lost or abnormal.

Possible Causes

- The network between the active and standby nodes is unstable.
- The standby OMS database is abnormal.
- The disk space of the standby node is full.

Handling Procedure

Check whether the network between the active and standby nodes is normal.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the alarm list, locate the row that contains the alarm, click , and view the IP address of the standby OMS database node for which the alarm is generated.

Step 3 Log in to the active OMS database node as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 4 Run the **ping Heartbeat IP address of the standby OMS database** command to check whether the standby OMS database node is reachable.

- If yes, go to [Step 7](#).
- If no, go to [Step 5](#).

Step 5 Contact the network administrator to check whether the network is faulty.

- If yes, go to [Step 6](#).
- If no, go to [Step 7](#).

Step 6 Rectify the network fault and check whether the alarm is cleared from the alarm list.

- If yes, no further operation is required.
- If no, go to [Step 7](#).

Check whether the status of the standby OMS database is normal.

Step 7 Log in to the standby OMS database node as user **root**.

Step 8 Run the **su - omm** command to switch to user **omm**.

Step 9 Go to the `${BIGDATA_HOME}/om-server/om/sbin` directory and run the `./status-oms.sh` command to check whether the database resource status of the standby OMS is normal. In the command output, check whether the following information is displayed in the row where **ResName** is **gaussDB**:

Example:

```
10_10_10_231 gaussDB Standby_normal Normal Active_standby
```

- If yes, go to [Step 10](#).
- If no, go to [Step 17](#).

Check whether the disk space of the standby node is full.

Step 10 Log in to the standby OMS database node as user **root**.

Step 11 Run the `su - omm` command to switch to user **omm**.

Step 12 Run the `echo ${BIGDATA_DATA_HOME}/dbdata_om` command to obtain the data directory of the OMS database.

Step 13 Run the `df -h` command to check the system disk partition usage.

Step 14 Check whether the disk mounted to the OMS database data directory is full.

- If yes, go to [Step 15](#).
- If no, go to [Step 17](#).

Step 15 Expand the disk capacity by referring to Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Capacity Adjustment Guide.

Step 16 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 17](#).

Collect fault information.

Step 17 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 18 Select OmmServer for Service.

Step 19 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 20 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.26 ALM-12040 Insufficient System Entropy

Alarm Description

The system checks the entropy at 00:00:00 every day and performs five consecutive checks each time. First, the system checks whether the rng-tools or haveged tool is enabled and correctly configured. If not, the system checks the current entropy. This alarm is generated if the entropy is less than 100 in the five checks.

This alarm is cleared if the true random number mode is configured, random numbers are configured in pseudo-random number mode, or neither the true random number mode nor the pseudo-random number mode is configured but the entropy is greater than or equal to 100 in at least one check among the five checks.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12040	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The system cannot run properly.

Possible Causes

The **haveged** service or **rngd** service is abnormal.

Handling Procedure

Check and manually configure the system entropy.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**.

Step 3 Check the value of **HostName** in the **Location Info** to obtain the name of the host for which the alarm is generated.

Step 4 Log in to the node for which the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 5 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 8](#).
- If no, go to [Step 6](#).

Step 6 Run the **/sbin/service haveged status |grep "running"** command and check the command output.

- If the command is executed successfully, the haveged service is installed, correctly configured, and is running properly. Go to [Step 11](#).
- If the command is not executed successfully, the haveged service is not running properly. Then go to [Step 8](#).

Step 7 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, go to [Step 9](#).
- If no, go to [Step 8](#).

Step 8 Run the **ps -ef | grep -v "grep" | grep rngd | tr -d " " | grep "\-o/dev/random" | grep "\-r/dev/urandom"** command and check the command output.

- If the command is executed successfully, the rngd service is installed, correctly configured, and is running properly. Go to [Step 11](#).
- If the command fails to be executed, the **rngd** service is not running properly. Go to [Step 9](#).

Step 9 Manually configure the system entropy. For details, see [Related Information](#).

Step 10 Wait until 00:00:00 when the system checks the entropy again. Check whether the alarm is cleared automatically.

- 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 NodeAgent for 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

Manually check the system entropy.

Log in to the node as user root and run the cat /proc/sys/kernel/random/entropy_avail command to check whether the cluster entropy is 500 or greater. If the system entropy is less than 500, you can reset it by using one of the following methods:

- Using the haveged tool (true random number mode): Contact the OS supplier to install the tool and then start it.
- Using the rng-tools tool (pseudo-random number mode): Contact the OS supplier to install the tool and then configure the system entropy based on the OS type.
 - For Red Hat and CentOS, run the following commands:

```
echo 'EXTRAOPTIONS="-r /dev/urandom -o /dev/random -t 1 -i"'>> /etc/sysconfig/rngd
service rngd start
chkconfig rngd on
```
 - In SUSE, run the following command:

```
rngd -r /dev/urandom -o /dev/random
echo "rngd -r /dev/urandom -o /dev/random" >> /etc/rc.d/after.local
```

2.3.27 ALM-12041 Critical File Permission Is Abnormal

Alarm Description

Every 5 minutes, the system checks whether critical directories or file permissions, users, and user groups are normal. This alarm is generated when any of them are abnormal.

This alarm is cleared when the permissions, users, and user groups are normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12041	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	PathName	Specifies the path or name of the abnormal file.

Impact on the System

System functions are unavailable.

Possible Causes

The permission, user, and user group information about the file is modified manually or the system is powered off unexpectedly.

Handling Procedure

Check abnormal file permission.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarm**.
- Step 3** Check the value of **HostName** in **Location Info** of the alarm to obtain the name of the host for which the alarm is generated. Check the value of **PathName** in **Location Info** to obtain the path or name of the abnormal file.
- Step 4** Log in to the node for which the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 5** Run the **ll PathName** command to query the current user, permission, and user group of the file or path.
- Step 6** Go to **\${BIGDATA_HOME}/om-agent/nodeagent/etc/agent/autocheck**, run the **vi keyfile** command, and search for the name of the abnormal file to view the correct permission on the file.

 NOTE

In addition to the files and directories listed in keyfile, the files and directories, as well as the files and subdirectories thereof, configured in **\$OMS_RUN_PATH/workspace/ha/module/hasync/plugin/conf/filesync.xml** are also monitored to ensure normal configuration synchronization between the active and standby OMS nodes. User **omm** must have the read and write permissions on the files, and the read and execute permissions on the directories.

- Step 7** Compare the real-world permission of the file with the due permission obtained in **Step 6** and correct the permission, user, and user group information for the file.
- Step 8** Wait an hour and check whether the alarm is cleared.
- If yes, no further action is required.
 - If no, go to **Step 9**.

 NOTE

If the disk partition where the FusionInsight installation directory is located is full, some temporary files are generated in the installation directory due to the **sed** command execution failure in some programs, and the user does not have the read, write, and execute permissions. If these files are generated within the monitoring scope of this alarm, the system reports this alarm. The alarm cause indicates that the permissions on the temporary files are abnormal. You can clear the alarm by referring to the preceding alarm handling process, or delete the temporary files after confirming that the files with abnormal permission are temporary files. The temporary files generated by the **sed** command are similar to those shown in the following figure.

```
-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 9** On the FusionInsight Manager portal, choose **O&M > Log > Download**.
- Step 10** Select NodeAgent 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.28 ALM-12042 Critical File Configuration Is Abnormal

Alarm Description

The system checks whether key system configurations are correct every 5 minutes. This alarm is generated when a key system configuration is incorrect.

This alarm is cleared when all the key configurations are correct.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12042	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	PathName	Specifies the path or name of the abnormal file.

Impact on the System

Functions related to the file are abnormal.

Possible Causes

The file configuration is modified manually or the system is powered off unexpectedly.

Handling Procedure

Check abnormal file configurations.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**.

Step 3 Check the value of **HostName** in **Location Info** of the alarm to obtain the name of the host for which the alarm is generated. Check the value of **PathName** in **Location Info** to obtain the path or name of the abnormal file.

Step 4 Log in to the node for which the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 5 View the \$BIGDATA_LOG_HOME/nodeagent/scriptlog/checkfileconfig.log file and analyze the cause based on the error log. Manually check and modify the file configurations according to the criteria in **Related Information**.

Run the **vi file name** command to enter the editing mode, and then press **Insert** to start editing.

After the modification, press **Esc** to exit the editing mode and enter **:wq** to save the modification and exit.

Example:

vi /etc/ssh/sshd_config

Step 6 Wait an hour 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 8 Select **NodeAgent** for 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 technical support and send the collected logs.

----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 the **/proc/mounts** file.

Check whether the **swap** partitions configured in **fstab** corresponds to those in **/proc/swaps**.

- **Check standards of /etc/hosts**

Run the **cat /etc/hosts** command. If any of the following situations exists, the file configurations are abnormal.

- a. The **/etc/hosts** file does not exist.
- b. The host name is not configured in the file.
- c. The IP address corresponding to the host name is not unique.
- d. The IP address corresponding to the host name does not exist in the command output of the **ifconfig** command.
- e. In the file, one IP address corresponds to multiple host names.

- **Check standards of /etc/ssh/sshd_config**

Run the **vi /etc/ssh/sshd_config** command to check whether the following configuration items are correct:

- a. The value of **UseDNS** must be **no**.
- b. The value of **MaxStartups** must be greater than or equal to **1000**.
- c. At least one of **PasswordAuthentication** and **ChallengeResponseAuthentication** must be set to **yes**.

2.3.29 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 (the default threshold is 0.5%) 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12045	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The service performance deteriorates or some services time out.

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 customer network environment is of poor quality.

Handling Procedure

View the network packet dropped rate.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name and NIC name for which the alarm is generated.
- Step 3** Log in to the node for which the alarm is generated as user **omm** and run the **/sbin/ifconfig N/C name** command to check whether packet loss occurs on the network.

```
omm@8-5-192-4:~> /sbin/ifconfig eth2
eth2      Link encap:Ethernet  HWaddr E4:35:C8:7B:B5:48
          inet  addr:192.168.192.4  Broadcast:192.168.255.255  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 on the **Host** page of FusionInsight Manager based on the **HostName** in the alarm location information. Check the IP addresses of both the management plane and service plane.
- Packet loss rate = (Number of dropped packets/Total number of RX packets) x 100%. If the packet loss rate is greater than the threshold (0.5% by default), read packet loss occurs.
- If yes, go to [Step 12](#).
- If no, go to [Step 4](#).

Check the system environment.

Step 4 Log in to the active OMS node or the node for which the alarm is generated as user **omm**.

Step 5 Run the **cat /etc/*-release** command to check the OS type.

- For Red Hat, perform [Step 6](#).

```
# cat /etc/*-release  
Red Hat Enterprise Linux Server release 7.2 (Santiago)
```

- For SUSE, perform [Step 7](#).

```
# cat /etc/*-release  
SUSE Linux Enterprise Server 11 (x86_64)  
VERSION = 11  
PATCHLEVEL = 3
```

- In other cases, go to [Step 12](#).

Step 6 Run the **cat /etc/redhat-release** command to check whether the OS version is Red Hat 7.2 (x86) or Red Hat 7.4 (TaiShan).

```
# 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 8](#).
- If no, go to [Step 12](#).

Step 7 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 8](#).
- If no, go to [Step 12](#).

Step 8 Log in to FusionInsight Manager and choose **O&M > Alarm > Thresholds**.

Step 9 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 10](#).
- If no, the alarm sending function is disabled. Go to [Step 11](#).

Step 10 In the area on the right, toggle Switch off to disable the checking of **Network Read Packet Dropped Rate Exceeds the Threshold**.

Read Packet Dropped Rate

Switch:

- Step 11** 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.

Alarm

Export All **Clear Alarm** All Objects **Advanced Search** C T
Alarm ID: **12045** Alarm Name:
Start Time: End Time:
Alarm Status: All Alarm Types
Search Reset

NOTE

The ID of alarm **Network Read Packet Dropped Rate Exceeds the Threshold** is **12045**.

Check whether the NICs are bonded in active/standby mode.

- Step 12** Log in to the node for which the alarm is generated 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, as shown in the following figure, the bond mode is configured for the node. Go to [Step 13](#).

```
# ls -l /proc/net/bonding/
total 0
-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 15](#).

```
# ls -l /proc/net/bonding/
ls: cannot access /proc/net/bonding/: No such file or directory
```

- Step 13** 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 preceding command, **bond0** is the name of the bond configuration file. Use the file name obtained in [Step 12](#).

```
# 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 14](#).
- If no, go to [Step 15](#).

Step 14 Check whether the network adapter specified by the **NetworkCardName** parameter 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 15](#).

 **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.

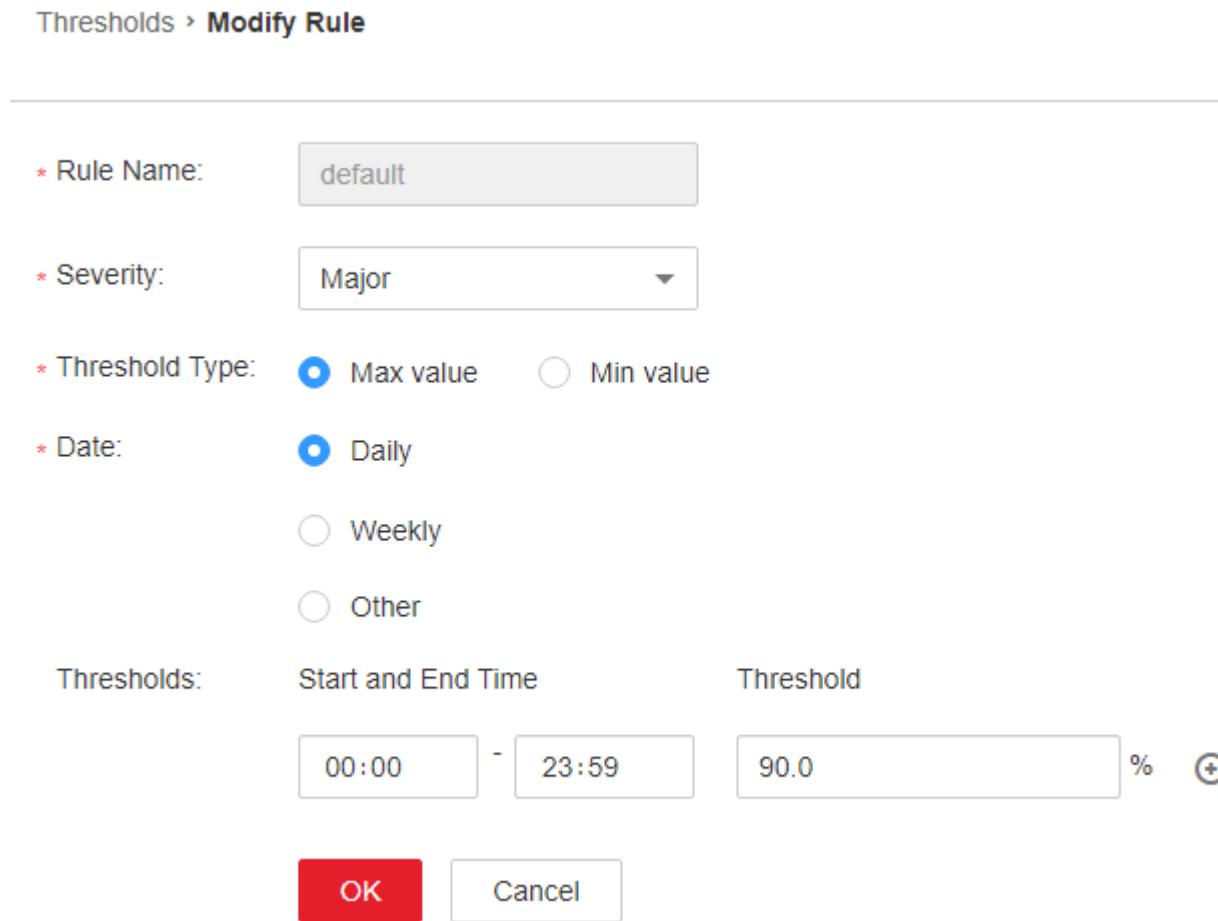
Check whether the threshold is set properly.

Step 15 Log in to FusionInsight Manager and check whether the threshold (configurable, 0.5% by default) is appropriate.

- If yes, go to [Step 18](#).
- If no, go to [Step 16](#).

Step 16 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Reading > Read Packet Dropped Rate** to change the alarm threshold based on the actual service usage, as shown in [Figure 2-6](#).

Figure 2-6 Setting alarm threshold



Step 17 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 18**.

Check whether the network is normal.

Step 18 Contact the system administrator to check whether the network is normal.

- If yes, rectify the network fault and go to **Step 19**.
- If no, go to **Step 20**.

Step 19 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 20**.

Collect fault information.

Step 20 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 21 Select **OMS** from the **Services** drop-down list.

Step 22 Set **Host** to the node for which the alarm is generated and the active OMS node.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.30 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 (the default threshold is 0.5%) 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**.

When the **Trigger Count** is **1**, this alarm is cleared when the network write packet dropped 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 packet dropped rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12046	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.

Type	Parameter	Description
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The service performance deteriorates or some services time out.

Possible Causes

- The alarm threshold is improperly configured.
- The customer network environment is of poor quality.

Handling Procedure

Check whether the threshold is set properly.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

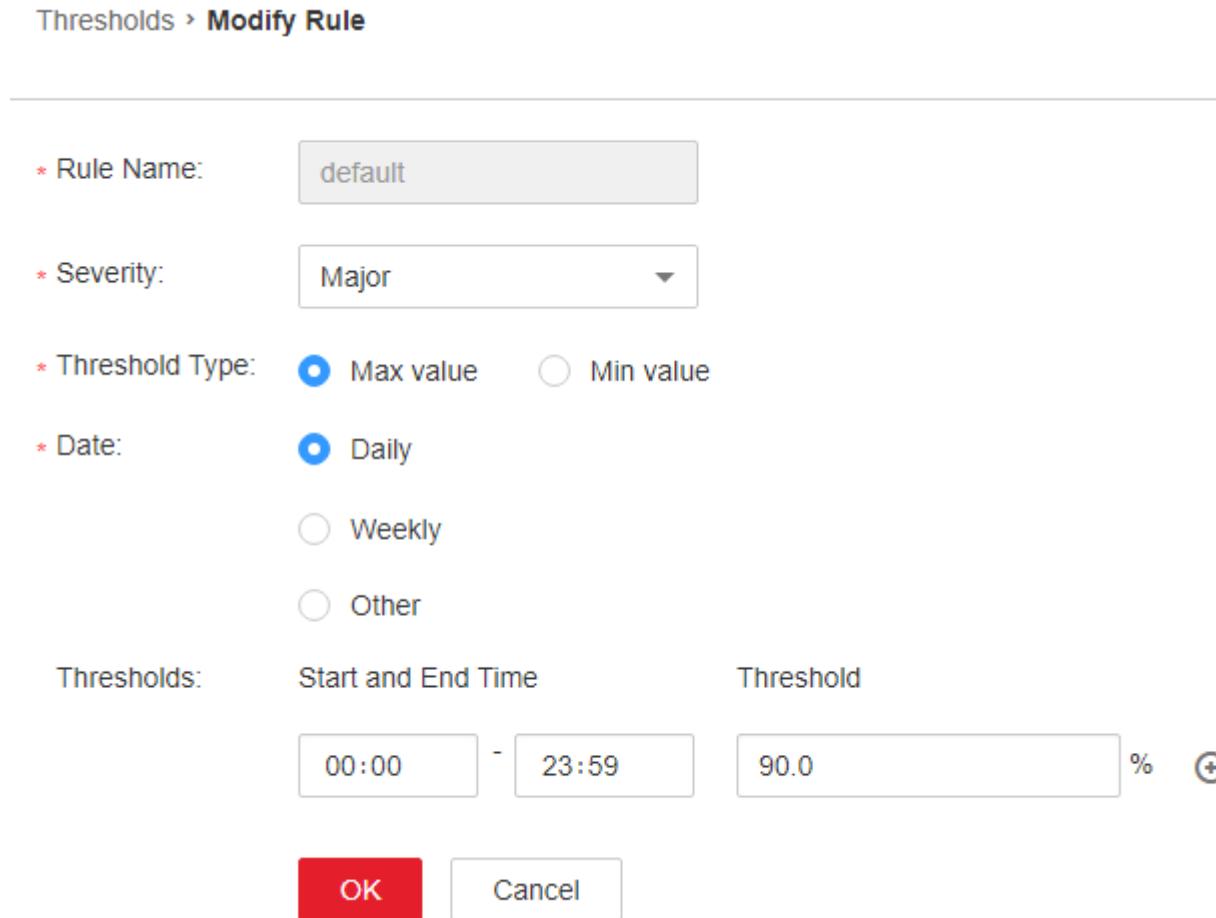
NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to FusionInsight Manager and check whether the threshold (configurable, 90% by default) is appropriate.
- If yes, go to [Step 5](#).
 - If no, go to [Step 3](#).

Step 3 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Writing > Write Packet Dropped Rate** to change the alarm threshold based on the actual service usage, as shown in [Figure 2-7](#).

Figure 2-7 Setting alarm threshold



Step 4 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 5](#).

Check whether the network is normal.

Step 5 Contact the system administrator to check whether the network is normal.

- If yes, rectify the network fault and 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 operation is required.
- If no, go to [Step 7](#).

Collect fault information.

Step 7 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 8 Select **OMS** from the **Services** drop-down list.

Step 9 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 10 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 11 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.31 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 (the default threshold is **0.5%**) 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 the **Trigger Count** is **1**, this alarm is cleared when the read packet error rate is less than or equal to the threshold. If the **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.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12047	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The communication is intermittently interrupted, and services time out.

Possible Causes

- The alarm threshold is improperly configured.
- The customer network environment is of poor quality.

Handling Procedure

Check whether the threshold is set properly.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to FusionInsight Manager and check whether the threshold (configurable, 90% by default) is appropriate.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Reading > Read Packet Error Rate** to change the alarm threshold based on the actual service usage, as shown in **Figure 2-8**.

Figure 2-8 Setting alarm threshold

Thresholds > **Modify Rule**

* Rule Name:	default	
* Severity:	Major	
* Threshold Type:	<input checked="" type="radio"/> Max value	<input type="radio"/> Min value
* Date:	<input checked="" type="radio"/> Daily	<input type="radio"/> Weekly
<input type="radio"/> Other		
Thresholds:	Start and End Time	Threshold
	00:00 - 23:59	90.0 %
OK Cancel		

Step 4 Wait 5 minutes and check whether the alarm is cleared.

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

Check whether the network is normal.

Step 5 Contact the system administrator to check whether the network is normal.

- If yes, rectify the network fault and 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 operation is required.

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

Collect fault information.

Step 7 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 8 Select **OMS** from the **Services** drop-down list.

Step 9 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 10 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 11 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.32 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 (the default threshold is **0.5%**) 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.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12048	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The communication is intermittently interrupted, and services time out.

Possible Causes

- The alarm threshold is improperly configured.
- The customer network environment is of poor quality.

Handling Procedure

Check whether the threshold is set properly.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to FusionInsight Manager and check whether the threshold (configurable, 90% by default) is appropriate.

- If yes, go to **Step 5**.
- If no, go to **Step 3**.

Step 3 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Writing > Write Packet Error Rate** to change the alarm threshold based on the actual service usage, as shown in **Figure 2-9**.

Figure 2-9 Setting alarm threshold

Thresholds > **Modify Rule**

* Rule Name:	default	
* Severity:	Major	
* Threshold Type:	<input checked="" type="radio"/> Max value	<input type="radio"/> Min value
* Date:	<input checked="" type="radio"/> Daily	<input type="radio"/> Weekly
<input type="radio"/> Other		
Thresholds:	Start and End Time	Threshold
	00:00 - 23:59	90.0 %
OK Cancel		

Step 4 Wait 5 minutes and check whether the alarm is cleared.

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

Check whether the network is normal.

Step 5 Contact the system administrator to check whether the network is normal.

- If yes, rectify the network fault and 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 operation is required.

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

Collect fault information.

Step 7 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 8 Select **OMS** from the **Services** drop-down list.

Step 9 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 10 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 11 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.33 ALM-12049 Read Throughput Rate Exceeds the Threshold

Alarm Description

The system checks the read throughput rate every 30 seconds. This alarm is generated when the read throughput rate exceeds the threshold (the default threshold is **80%**) 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 Throughput Rate**.

If the **Trigger Count** is **1**, this alarm is cleared when the read throughput rate is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the read throughput rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12049	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The service system runs abnormally or is unavailable.

Possible Causes

- The alarm threshold is improperly configured.
- The network port rate does not meet service requirements.

Handling Procedure

Check whether the threshold is set properly.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to FusionInsight Manager and check whether the threshold (configurable, 80% by default) is appropriate.

- If yes, go to **Step 3**.
- If no, go to **Step 5**.

Step 3 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Reading > Read Throughput Rate** to change the alarm threshold based on the actual service usage, as shown in **Figure 2-10**.

Figure 2-10 Setting alarm threshold

Thresholds > **Modify Rule**

The screenshot shows a configuration dialog for modifying a rule. At the top, it says "Thresholds > Modify Rule". The form includes fields for "Rule Name" (set to "default"), "Severity" (set to "Major"), "Threshold Type" (radio button selected for "Max value"), "Date" (radio button selected for "Daily"), and a section for "Thresholds" with "Start and End Time" set to "00:00 - 23:59" and "Threshold" set to "90.0 %". At the bottom are "OK" and "Cancel" buttons.

* Rule Name:	default	
* Severity:	Major	
* Threshold Type:	<input checked="" type="radio"/> Max value <input type="radio"/> Min value	
* Date:	<input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Other	
Thresholds:	Start and End Time	Threshold
	00:00 - 23:59	90.0 %
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Step 4 Wait 5 minutes and check whether the alarm is cleared.

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

Check whether the network port rate meets the requirements.

Step 5 In the real-time alarm list on FusionInsight Manager, click in the row that contains the alarm to obtain the IP address and network port name of the host for which the alarm is generated.

Step 6 Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 7 Run the **ethtool network port name** command to check the maximum network port rate **Speed**.

 **NOTE**

In a VM environment, you may fail to obtain the network port rate by running commands. You are advised to contact the system administrator to check whether the network port rate meets the requirements.

Step 8 If the read throughput rate exceeds the threshold, contact the system administrator to increase the network port rate.

Step 9 Check whether the alarm is cleared.

- If yes, no further operation is required.
- 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 **OMS** from the **Services** drop-down list.

Step 12 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 13 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 14 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.34 ALM-12050 Write Throughput Rate Exceeds the Threshold

Alarm Description

The system checks the write throughput rate every 30 seconds. This alarm is generated when the write throughput rate exceeds the threshold (the default threshold is **80%**) 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 Throughput Rate**.

If the **Trigger Count** is **1**, this alarm is cleared when the write throughput rate is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the write throughput rate is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12050	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The service system runs abnormally or is unavailable.

Possible Causes

- The alarm threshold is improperly configured.
- The network port rate does not meet service requirements.

Handling Procedure

Check whether the threshold is set properly.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to FusionInsight Manager and check whether the threshold (configurable, 80% by default) is appropriate.

- If yes, go to [Step 5](#).
- If no, go to [Step 3](#).

Step 3 Choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Writing > Write Throughput Rate** to change the alarm threshold based on the actual service usage,

as shown in [Figure 2-11](#).

Figure 2-11 Setting alarm threshold

Thresholds > **Modify Rule**

* Rule Name:	default	
* Severity:	Major	
* Threshold Type:	<input checked="" type="radio"/> Max value	<input type="radio"/> Min value
* Date:	<input checked="" type="radio"/> Daily	<input type="radio"/> Weekly
<input type="radio"/> Other		
Thresholds:	Start and End Time	Threshold
	00:00 - 23:59	90.0 %
OK Cancel		

Step 4 Wait 5 minutes and check whether the alarm is cleared.

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

Check whether the network port rate meets the requirements.

- Step 5** In the real-time alarm list on FusionInsight Manager, click in the row that contains the alarm to obtain the IP address and network port name of the host for which the alarm is generated.
- Step 6** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 7** Run the **ethtool** *network port name* command to check the maximum network port rate **Speed**.

NOTE

In a VM environment, you may fail to obtain the network port rate by running commands. You are advised to contact the system administrator to check whether the network port rate meets the requirements.

- Step 8** If the write throughput rate exceeds the threshold, contact the system administrator to increase the network port rate.

- Step 9** Check whether the alarm is cleared.

- If yes, no further operation is required.
- 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 **OMS** from the **Services** drop-down list.

- Step 12** Set **Host** to the node for which the alarm is generated and the active OMS node.

- Step 13** 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 14** Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.35 ALM-12051 Disk Inode Usage Exceeds the Threshold

Alarm Description

The system checks the disk inode usage every 30 seconds. This alarm is generated when the disk inode usage exceeds the threshold (the default threshold is 80%) for multiple times (the default value is 5).

To change the threshold, choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Disk > Disk Inode Usage**.

If the **Trigger Count** is 1, this alarm is cleared when the disk inode usage is less than or equal to the threshold. If 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12051	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	NetworkCard Name	Specifies the network port for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Data cannot be written to the file system.

Possible Causes

Too many small files are written to the disk.

Handling Procedure

Too many small files are written to the disk.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the real-time alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to obtain the IP address and disk partition of the host for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **df -i | grep -iE " Partition name | Filesystem"** command to check the current inode usage of the disk.

```
# df -i | grep -iE "xvda2|Filesystem"
Filesystem      Inodes   IUsed   IFree  IUse% Mounted on
/dev/xvda2    2359296  207420  2151876   9% /
```

- Step 5** If the inode usage exceeds the threshold, manually check whether the small files in the partition can be deleted.

 NOTE

You can run the **for i in /*; do echo \$i; find \$i|wc -l; done** command to view the number of files in a partition. Replace **/*** with the partition to be checked.

```
# for i in /srv/*; do echo $i; find $i|wc -l; done
/srv/BigData
4284
/srv/ftp
1
/srv/www
13
```

- If yes, delete the file and go to **Step 6**.
- If no, expand the disk capacity and go to **Step 6**.

- Step 6** Wait 5 minutes and check whether the alarm is cleared.
- If yes, no further operation is required.
 - If no, go to **Step 7**.

Collect fault information.

Step 7 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 8 Select **OMS** from the **Services** drop-down list.

Step 9 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 10 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 11 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.36 ALM-12052 Usage of Temporary TCP Ports Exceeds the Threshold

Alarm Description

The system checks the usage of temporary TCP ports every 30 seconds. This alarm is generated when the usage of temporary TCP ports exceeds the threshold (the default threshold is **80%**) for multiple times (the default value is 5).

To change the threshold, choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Network Status > Temporary TCP Port Usage**.

If the **Trigger Count** is **1**, this alarm is cleared when the usage of temporary TCP ports is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the usage of temporary TCP ports is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12052	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

Services on the host fail to establish connections with the external and services are interrupted.

Possible Causes

- The temporary ports do not meet service requirements.
- The system is abnormal.

Handling Procedure

Expand the range of temporary ports.

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

- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
- Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
- Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
- Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to obtain the IP address of the host for which the alarm is generated.

Step 3 Log in to the host for which the alarm is generated as user **omm**.

Step 4 Run the `cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 1` command to obtain the start port number. Run the `cat /proc/sys/net/ipv4/ip_local_port_range |cut -f 2` command to obtain the end port number. Subtract the start port number from the end port number to obtain the total number of temporary ports. If the total number of temporary ports is less than 28,232, the random port range of the OS is too small. In this case, contact the system administrator to expand the port range.

Step 5 Run the `ss -ant 2>/dev/null | grep -v LISTEN | awk 'NR > 2 {print $4}'|cut -d ':' -f 2 | awk '$1 >"start port number" {print $1}' | sort -u | wc -l` command to calculate the number of used temporary ports.

Step 6 Calculate the usage of temporary ports using the following formula: Usage of temporary ports = (Number of used temporary ports/Total number of temporary ports) x 100. Check whether the usage exceeds the threshold.

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

Step 7 Wait 5 minutes and check whether the alarm is cleared.

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

Check whether the system environment is normal.

Step 8 Run the following command to import the temporary file and view the frequently used ports in the `port_result.txt` file:

`netstat -tnp > $BIGDATA_HOME/tmp/port_result.txt`

```
netstat -tnp
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 9 Run the following command to check the processes that occupy a large number of ports:

`ps -ef |grep PID`



NOTE

- `PID` indicates the process ID of the port queried in **Step 8**.
- Run the following command to collect information about all processes in the system and check the processes that occupy a large number of ports:

`ps -ef > $BIGDATA_HOME/tmp/ps_result.txt`

Step 10 Contact the system administrator to clear the processes that occupy a large number of ports. Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 11**.

Collect fault information.

- Step 11** On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.
- Step 12** Select **OMS** from the **Services** drop-down list.
- Step 13** Set **Host** to the node for which the alarm is generated and the active OMS node.
- 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 to send the collected fault logs and the **port_result.txt** and **ps_result.txt** files, and delete the two temporary files in the environment.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.37 ALM-12053 Host File Handle Usage Exceeds the Threshold

Alarm Description

The system checks the handler usage every 30 seconds. This alarm is generated when the handle usage exceeds the threshold (the default threshold is **80%**) for multiple times (the default value is **5**).

To change the threshold, choose **O&M > Alarm > Thresholds > Name of the desired cluster > Host > Host Status > Host File Handle Usage**.

If the **Trigger Count** is **1**, this alarm is cleared when the file handle usage is less than or equal to the threshold. If the **Trigger Count** is greater than **1**, this alarm is cleared when the file handle usage is less than or equal to 90% of the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12053	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The system applications fail to open files, access networks, and perform other I/O operations. The applications are running improperly.

Possible Causes

- The application process is abnormal. For example, the opened file or socket is not closed.
- The number of file handles does not meet service requirements.
- The system is abnormal.

Handling Procedure

Check the files opened by the process.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to obtain the IP address of the host for which the alarm is generated.

Step 3 Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 4 Run the **lsof -n|awk '{print \$2}'|sort|uniq -c|sort -nr|more** command to check the processes that occupy a large number of file handles.

Step 5 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 6**.
- If no, go to **Step 8**.

Step 6 Release the abnormal processes that occupies too many file handles.

Step 7 Wait 5 minutes and check whether the alarm is cleared.

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

Increase the number of file handles.

Step 8 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click to obtain the IP address of the host for which the alarm is generated.

Step 9 Log in to the host for which the alarm is generated as user **root**.

Step 10 Contact the system administrator to increase the number of system file handles.

Step 11 Run the **cat /proc/sys/fs/file-nr** command to check the number of used handles and the maximum number of handles. The first value is the number of used handles, and the third value is the maximum number of handles. Check whether the usage exceeds the threshold.

```
# cat /proc/sys/fs/file-nr
12704 0 640000
```

- If yes, go to **Step 10**.
- If no, go to **Step 12**.

Step 12 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 13**.

Check whether the system environment is normal.

Step 13 Contact the system administrator to check whether the OS is abnormal.

- If yes, rectify the OS fault and go to **Step 14**.
- If no, go to **Step 15**.

Step 14 Wait 5 minutes and check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to **Step 15**.

Collect fault information.

Step 15 On the FusionInsight Manager portal of the active cluster, choose **O&M > Log > Download**.

Step 16 Select **OMS** from the **Services** drop-down list.

Step 17 Set **Host** to the node for which the alarm is generated and the active OMS node.

Step 18 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 19 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.38 ALM-12054 The Certificate File Is Invalid

Alarm Description

The system checks whether the certificate file is invalid (has expired or is not yet valid) on 23:00 every day. This alarm is generated when the certificate file is invalid.

This alarm is cleared when the status of the newly imported certificate is valid.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12054	Tenant plane alarm	Major	Security alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Type	Parameter	Description
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The system reminds users that the certificate file is invalid. If the certificate file is invalid, some functions are restricted and cannot be used properly.

Possible Causes

No certificate (CA certificate, HA root certificate, or HA user certificate) is imported to the system, certificates fail to be imported, or the certificate file is invalid.

Handling Procedure

Check the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In the real-time alarm list on FusionInsight Manager, locate the row that contains the alarm and click .

View **Other 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 3**.

You can view the IP addresses of the active and standby management nodes on the Host tab of FusionInsight Manager.

- If **HA root Certificate** is displayed in the additional information, check **Location Info** 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 **HA server Certificate** is displayed in the additional information, check **Location Info** to obtain the name of the host involved in this alarm. 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 3 Check whether the current system time is in the validity period of the CA certificate.

You can run the **bash \${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** command to view the effective time and expiration time of the CA root certificate.

- If yes, go to [Step 8](#).
- If no, go to [Step 6](#).

Step 4 Check whether the current system time is in 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 8](#).
- If no, go to [Step 7](#).

Step 5 Check whether the current system time is in 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 8](#).
- If no, go to [Step 7](#).

The following is an example of the effective time and expiration 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 //Expiration time

Import certificate files.

Step 6 Import a new CA certificate file.

Apply for or generate a new CA certificate file and import it. For details, see section "Replacing the CA Certificate" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide. The alarm is automatically cleared after the CA certificate is imported. 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 HA certificate file.

Apply for or generate a new HA certificate file and import it. For details, see section "Replacing the HA Certificate" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide. The alarm is automatically cleared after the CA certificate is imported. 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 9 In the **Services** area, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.39 ALM-12055 The Certificate File Is About to Expire

Alarm Description

The system checks the certificate file on 23:00 every day. This alarm is generated if the certificate file is about to expire with a validity period less than days set in the alarm threshold.

This alarm is generated if the status of the newly imported certificate is valid.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12055	Tenant plane alarm	Minor	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Trigger Condition	Specifies the threshold for triggering the alarm.

Impact on the System

The system reminds users that the license is about to expire. If the license expires, some functions are restricted and cannot be used properly.

Possible Causes

The remaining validity period of the CA certificate, HA root certificate, or HA user certificate is smaller than the alarm threshold.

Handling Procedure

Check the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In the real-time alarm list on FusionInsight Manager, locate the row that contains the alarm and click .

View **Other 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 3](#).

You can view the IP addresses of the active and standby management nodes on the Host tab of FusionInsight Manager.

- If **HA root Certificate** is displayed in the additional information, check **Location Info** 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 **HA server Certificate** is displayed in the additional information, check **Location Info** to obtain the name of the host involved in this alarm. 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 3** Check whether the remaining validity period of the CA certificate is smaller than the alarm threshold.

You can run the **bash \${CONTROLLER_HOME}/security/cert/conf/querycertvalidity.sh** command to view the effective time and expiration time of the CA root certificate.

- If yes, go to [Step 6](#).
- If no, go to [Step 8](#).

- Step 4** 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 7](#).
- If no, go to [Step 8](#).

- Step 5** 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 7](#).
- If no, go to [Step 8](#).

The following is an example of the effective time and expiration 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 //Expiration time
```

Import certificate files.

Step 6 Import a new CA certificate file.

Apply for or generate a new CA certificate file and import it. For details, see section "Replacing the CA Certificate" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide. 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 HA certificate file.

Apply for or generate a new HA certificate file and import it. For details, see section "Replacing the HA Certificate" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide. 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 In the **Services** area, select **Controller**, **OmmServer**, **OmmCore**, and **Tomcat**.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.40 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 exists every hour. If the task for periodically backing up metadata to a third-party server is not configured, a major alarm is generated.

This alarm is cleared when a user creates such a backup task.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12057	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If metadata is not backed up to a third-party server, metadata cannot be restored if both the active and standby management nodes of the cluster are faulty and local backup data is lost.

Possible Causes

Metadata is not configured with the task to periodically back up data to a third-party server.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarm**.
- Step 3** In the alarm list, click  of the alarm and obtain the data module for which the alarm is generated from **Other Information**.
- Step 4** Choose **O&M > Backup and Restoration > Backup Management**, and click **Create**.
- Step 5** Configure a backup task. The backup data to be configured must be consistent with the **Other Information** of this alarm.
- For details, see section "Creating a Backup Task" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide.
- Step 6** After the backup task is created successfully, wait for two minutes and check whether the alarm is cleared.
- If yes, no further operation is required.
 - If no, go to [Step 7](#).

Collecting fault information

- Step 7** On the FusionInsight Manager portal, choose **O&M > Log > Download**.
- Step 8** Select Controller for Service.
- Step 9** 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 10** Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.41 ALM-12058 License Is Not Bound to SnS

Alarm Description

The system checks whether the license is bound to the SnS service every 5 minutes (when the customer activates the license or installs the patch). If the license loaded and activated in the system is not bound to the SnS service, the system generates this alarm. This alarm is automatically cleared when the customer re-imports the activated license that contains SnS.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12058	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The customer system cannot use SnS.

Possible Causes

The license of the customer system is not bound to SnS.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

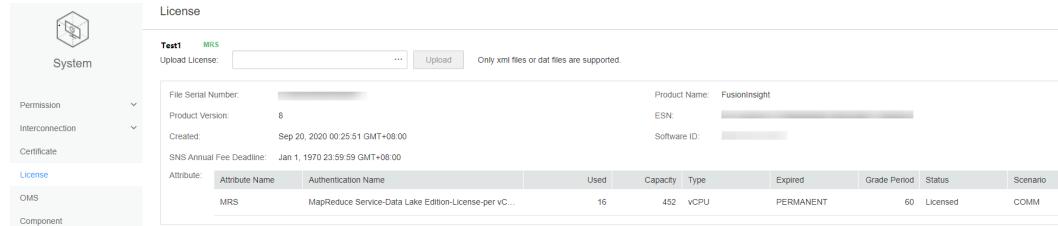
NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **System > License > Cluster name**

Step 3 View the license information.

Figure 2-12 License page



Step 4 Check whether the SNS alarm expiration date is 1970-01-01 23:59:59.

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

Step 5 Contact the frontline delivery personnel to bind the SNS authorization to the system license, import the license to FusionInsight Manager, and activate the license. For details, see Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) License Guide.

Step 6 Two minutes later, check whether the alarm is cleared.

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

Collecting fault information

Step 7 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 8 Select **Controller for Service**.

Step 9 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 10 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.42 ALM-12059 SNS of the License Is About to Expire

Alarm Description

The system checks whether the SNS of the current system license is about to expire every 5 minutes (when the customer activates the license or installs the

patch). This alarm is generated when the SnS expiration time of the current system license is less than 60 days from the current system time. This alarm is automatically cleared when the customer re-imports the activated license that contains SnS with extended effective period.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12059	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Specifies the cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Users are prompted to renew the license in a timely manner. Otherwise, the SnS service may be interrupted due to the expiration of the license.

Possible Causes

The SnS expiration time of the customer system license is less than 60 days from the system time.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

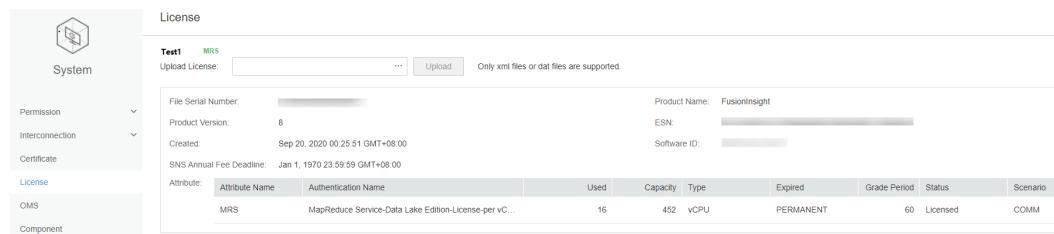
 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **System > License > Cluster name**

Step 3 View the license information.

Figure 2-13 License page



Step 4 Check whether the SNS expiration date is less than 60 days from the system time.

- If yes, go to [Step 5](#).
- If no, go to [Step 7](#).

Step 5 Contact the frontline delivery personnel to add the SNS authorization to the system license, import the license to FusionInsight Manager, and activate the license. For details, see [Huawei Cloud Stack 8.x.x Data Warehouse Service \(DWS\) License Guide](#).

Step 6 Two minutes later, check whether the alarm is cleared.

- If yes, no further operation is required.
- If no, go to [Step 7](#).

Collecting fault information

Step 7 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 8 Select Controller for Service.

Step 9 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 10 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.43 ALM-12060 SnS of the License Has Expired

Description

The system checks whether the SnS of the current system license has expired every 5 minutes (when the customer activates the license or installs the patch). This alarm is generated when the SnS expiration date of the current system license is earlier than the system time. This alarm is automatically cleared when customers import and activate license for renewing the SnS fee.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12060	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The customer system cannot use SnS.

Possible Causes

The SnS of the license system has expired.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

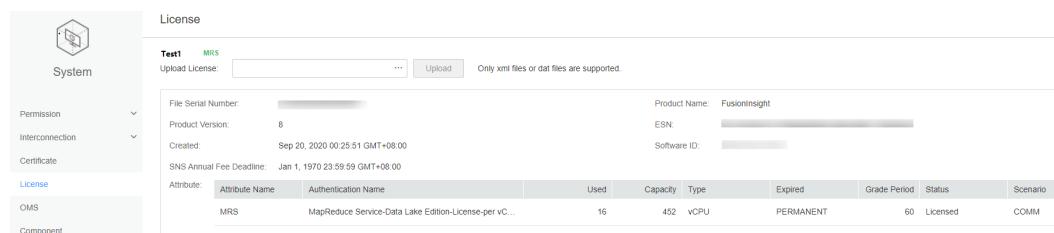
 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On the FusionInsight Manager portal, choose System > License > *Name of the desired cluster*.

Step 3 View the license information.

Figure 2-14 License page



Step 4 Check whether the SNS alarm expiration date is earlier than the current system time.

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

Step 5 Contact delivery personnel to add SNS entitlement to the system license, import the license to FusionInsight Manager, and activate the license.

Step 6 Two 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 the FusionInsight Manager portal, choose O&M > Log > Download.

Step 8 Select Controller 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 **Download**.

Step 10 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.44 ALM-12061 Process Usage Exceeds the Threshold

Description

The system checks the **omm** usage every 30 seconds. 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 concurrently opened by user **omm**. Divide the result of two processes. The division result is the **omm** process usage. The process usage has a default threshold. The 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12061	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.
	Trigger Condition	Generates an alarm when the actual indicator value exceeds the specified threshold.

Impact on the System

- Switch to user **omm** fails.
- New **omm** process cannot be created.

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.
- Too many processes are running at the same time.

Handling Procedure

Check whether the alarm threshold or alarm trigger count is properly configured.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

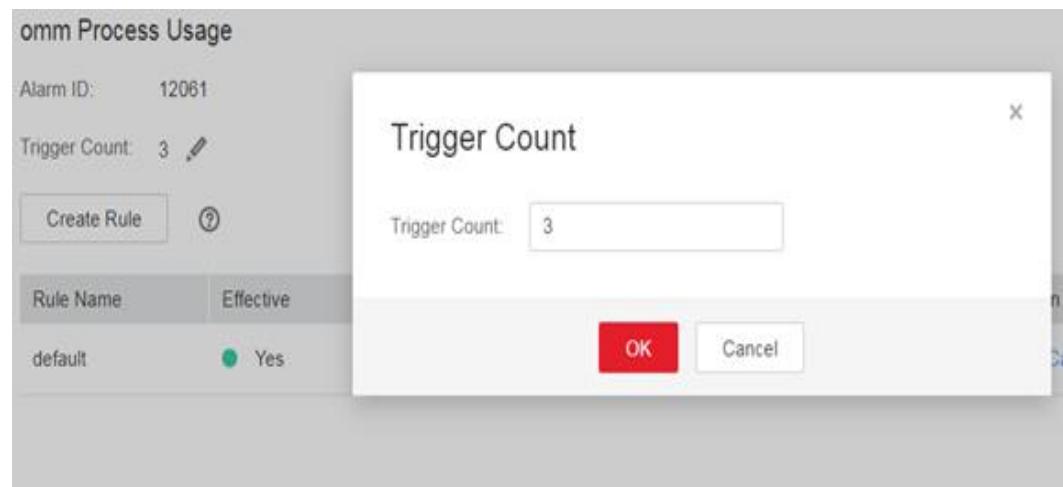
Step 2 On FusionInsight Manager, modify the alarm threshold and alarm trigger times based on the actual CPU usage.

Choose **O&M > Alarm > Threshold Configuration > Name of the target cluster > Host > Process > omm Process Usage** to change the alarm trigger times based on the actual service usage, as shown in [Figure 2-15](#).

 **NOTE**

The alarm is generated when the process usage exceeds the threshold for the times specified by **Trigger Count**.

Figure 2-15 Setting alarm trigger count



Choose **O&M > Alarm > Threshold Configuration > Name of the target cluster > Host > Process > omm Process Usage** to change the alarm threshold based on the actual service usage, as shown in [Figure 2-16](#).

Figure 2-16 Setting threshold alarms

The screenshot shows the 'Modify Rule' dialog for setting thresholds. It includes fields for 'Rule Name' (set to 'default'), 'Severity' (set to 'Major'), 'Threshold Type' (radio buttons for 'Max value' and 'Min value' with 'Max value' selected), 'Date' (radio buttons for 'Daily', 'Weekly', and 'Other' with 'Daily' selected), and a 'Thresholds' section. The 'Thresholds' section contains 'Start and End Time' fields set to '00:00' and '23:59', a 'Threshold' field set to '90.0 %', and a '+' button. At the bottom are 'OK' and 'Cancel' buttons.

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 maximum number of processes (including threads) that can be concurrently opened by user omm is properly configured.

- Step 4** 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 5** Log in to the host as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 6** Run the **su - omm** command to switch to the **omm** user.
- Step 7** Run the **ulimit -u** command to obtain the maximum number of threads that can be concurrently opened by user **omm** and check whether the value is greater than or equal to 60000.
- If yes, go to **Step 9**.
 - If no, go to **Step 8**.
- Step 8** Run the **ulimit -u 60000** command to change the value of this parameter for **omm** users to 60000. Wait 2 minutes and check whether the alarm is cleared.
- If yes, no further action is required.
 - If no, go to **Step 13**.

Check whether too many processes are started at the same time.

- Step 9** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click to view the host address for which the alarm is generated.
- Step 10** Log in to the host for which the alarm is generated as user **root**.
- Step 11** Run the **ps -o nlwp,pid,lwp,args, -u omm|sort -n** command to check the number of threads currently used by the system. The result is sorted based on the number of threads. Analyze the top 5 threads with the largest number of threads and check whether the threads are abnormal based on services. If yes, contact maintenance personnel to rectify the fault. If all threads are normal, run the **ulimit -u** command, change the value to a value greater than 60,000.
- Step 12** Wait 5 minutes 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 portal of the active cluster, choose **O&M > Log > Download**.
- Step 14** Select **OmmServer** and **NodeAgent** for **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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.45 ALM-12062 OMS Parameter Configurations Mismatch with the Cluster Scale

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12062	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

The OMS configuration is not modified when the cluster is installed or the system capacity is expanded.

Possible Causes

The OMS parameter configurations mismatch with the cluster scale.

Handling Procedure

Check whether the OMS configuration matches the cluster scale.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address for which the alarm is generated.

- Step 3** Log in to the host as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

- Step 4** Run the **su - omm** command to switch to user **omm**.

- Step 5** Run the **vi \$BIGDATA_LOG_HOME/controller/scriptlog/modify_manager_param.log** command to open the corresponding log and search for **Current oms configurations can not support xx nodes**. In the command, **xx** indicates the number of nodes in the current cluster.

- Step 6** Optimize the current cluster configuration by referring to [Optimizing Manager Configurations Based on the Number of Cluster Nodes](#).

- Step 7** One hour 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 **Controller for 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 technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

Optimizing manager configurations based on the number of cluster nodes

Step 1 log in to the active management node as user **omm**.

Step 2 Run the following command to switch to the specified 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**

For 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.node.heartbeat.error.threshold		30000	Controller => 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

2.3.46 ALM-12063 Unavailable Disk

Description

The system checks whether the data disk of the current host is available at the top of each hour. 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12063	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.
	DiskName	Disk for which the alarm is generated.

Impact on the System

Data read or write on the data disk fails, and services are abnormal.

Possible Causes

- The permission of the disk mount directory is abnormal.
- Bad sectors

Handling Procedure

Check whether the permission on the directory to which the disk is mounted is normal.

- Step 1** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click .
- Step 2** Log in to the ManageOne alarm platform to obtain the alarm information.
- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 - Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 3 View the IP address of the host and **DiskName** of the disk for which the alarm is generated.

Step 4 Log in to the host as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Step 5 Run the **df -h |grep DiskName** command to obtain the corresponding mount point and check whether the permission on the mount directory is unwritable or unreadable.

- If yes, go to [Step 6](#).
- If no, go to [Step 10](#).

 NOTE

If the permission of the mount directory is 000 or the owner is root, the mount directory is unreadable and unwritable.

Step 6 Modify the directory permission.

Step 7 One hour later, check whether this alarm is cleared.

- If yes, no further action is required.
- If no, go to [Step 8](#).

Step 8 Contact hardware engineers to rectify the disk.

Step 9 One hour later, check whether this 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 portal, choose **O&M > Log > Download**.

Step 11 Select **NodeAgent** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.47 ALM-12064 Host Random Port Range Conflicts with FusionInsight Used Port

Description

The system checks whether the random port range of the host conflicts with the port range used by FusionInsight every hour. This alarm is generated when a conflict occurs. The alarm is automatically cleared when the random port range of the host is changed to the normal range.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12064	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

The default port of the FusionInsight system is occupied. As a result, some processes fail to be started.

Possible Causes

The random port range is incorrectly configured.

Handling Procedure

Check the current random port range of the system.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address for which the alarm is generated.
- Step 3** Log in to the host as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** 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 yes, go to [Step 5](#).
 - If no, go to [Step 8](#).

- Step 5** Run the **vim /etc/sysctl.conf** command to change the value of **net.ipv4.ip_local_port_range** to **32768 61000**. If this configuration item does not exist, add **net.ipv4.ip_local_port_range = 32768 61000**.

- Step 6** Run the **sysctl -p /etc/sysctl.conf** command for the modification to take effect.

- Step 7** One hour 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 **NodeAgent** for 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.48 ALM-12066 Inter-Node Mutual Trust Fails

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 if this problem is resolved.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12066	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Some operations on the management plane may be abnormal.

Possible Causes

- The `/etc/ssh/sshd_config` configuration file is damaged.
- The password of user **omm** has expired.
- The private key encryption is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** 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 3** Log in to the active OMS management node as user **omm**. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.
- Step 4** Run the **ssh** command **ssh host2** (host2 is a node other than the OMS node in the alarm details) to check whether the password-free connection is successful.
- If yes, check other nodes in the alarm details by referring to [Step 4](#).
 - If no, go to [Step 9](#).
- Step 5** View the execution result of [Step 4](#) to check whether the connection fails (for example, **connection refused**).
- If yes, go to [Step 6](#).
 - If no, go to [Step 9](#).
- Step 6** Open the **/etc/ssh/sshd_config** configuration file on host2 and check whether the whitelist or blacklist such as **AllowUsers** and **DenyUsers** is configured.
- If yes, modify the whitelist or blacklist settings to ensure that the **omm** user is in the whitelist or not in the blacklist.
 - If no, contact OS experts.
- Step 7** Check the interaction information of the **ssh** command.
- If the **omm** user password is required, run the [Step 8](#) command.
 - If message "Enter passphrase for key '/home/omm/.ssh/id_rsa':" is displayed, run the [Step 9](#) command.
- Step 8** Check whether the trust list (**/home/omm/.ssh/authorized_keys**) of user **omm** on the OMS and host2 nodes 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** on the peer host to the trust list of the local host.

Collect fault information.

Step 9 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 10 Select **Controller for Service**.

Step 11 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 12 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.49 ALM-12067 Tomcat Resource Is Abnormal

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 the Tomcat resource is 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 FusionInsight 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12067	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- The Tomcat process repeatedly restarts.

Possible Causes

- The Tomcat directory permission is incorrect.
- The tomcat process is abnormal.

Handling Procedure

Check whether the Tomcat directory permission is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** 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 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** command to switch to the **omm** user.
- Step 5** Run the **vi \$BIGDATA_LOG_HOME/omm/oms/ha/scriptlog/tomcat.log** command to check whether the Tomcat resource log of HA contains the keyword "**Cannot find**". If yes, restore the file permission based on the keyword.
- Step 6** Wait for 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 8 Select **OmmServer** and **Tomcat** in the **Services** area.

Step 9 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 10 Contact technical support and send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.50 ALM-12068 ACS Resource Is Abnormal

Description

HA checks the ACS resources of the 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 the ACS resource is 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 FusionInsight 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12068	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.

Type	Parameter	Description
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- The ACS process repeatedly restarts, which may cause the FusionInsight Manager login failure.

Possible Causes

The ACS process is abnormal.

Handling Procedure

Check whether the ACS process is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** 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 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** commands to check whether the status of the ACS resources managed by the HA is normal. If the HA is deployed in a single-node system, the ACS resources are in normal state. If the HA is deployed in a two-node cluster, the ACS resources are in normal state on the active node and in 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/acs.log` command to view the ACS resource logs of the HA, analyze the logs, locate the cause of the resource exception, and rectify the fault.

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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 8 Select **Controller** and **OmmServer** for Service.

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 send the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.51 ALM-12069 AOS Resource Is Abnormal

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 the AOS resource is 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 FusionInsight 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12069	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- If the AOS process restarts continuously, you may fail to log in to FusionInsight Manager.

Possible Causes

The AOS process is abnormal.

Handling Procedure

Check whether the AOS process is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 - Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/omm/oms/ha/scriptlog/aos.log** commands to check whether the status of the AOS resource managed by HA is normal. In single-node mode, the AOS resource is in the normal state. In two-node cluster mode, 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 7**.
 - If no, go to **Step 5**.
- Step 5** Run the **vi \${BIGDATA_HOME}/omm/oms/ha/scriptlog/aos.log** command to view the AOS resource log of HA, analyze the log, locate the cause of the resource exception, and rectify the fault.
- 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.
- Step 8** Select **Controller** and **OmmServer** for Service.
- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.52 ALM-12070 Controller Resource Is Abnormal

Description

HA checks the controller resources of Manager every 80 seconds. This alarm is generated when HA detects that the controller resource is abnormal for two 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 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12070	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- If the controller process restarts continuously, you may fail to log in to FusionInsight Manager.

Possible Causes

The Controller process is abnormal.

Handling Procedure

Check whether the controller process is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.

- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** commands to check whether the status of the controller resource managed by HA is normal. (In single-node mode, the controller resource is in the normal state. In dual-node mode, the controller 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/controller.log** command to view the controller resource logs of HA. Run the **vi \${BIGDATA_LOG_HOME}/controller/controller.log** command to view the controller run logs, analyze the logs to identify the cause of the resource exception, and rectify the fault.

- Step 6** Five minutes later, check whether this 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 **Controller** and **OmmServer** for **Service**.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.53 ALM-12071 Httpd Resource Is Abnormal

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 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12071	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- 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 normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** command to switch to user **omm**.
- Step 5** 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 resource managed by HA is normal. In single-node mode, the httpd resource is in the normal state. In dual-node mode, the httpd resource is in the normal state on the active node and in the stopped state on the standby node.
- If yes, go to [Step 8](#).
 - If no, go to [Step 6](#).
- Step 6** Run the **vi \${BIGDATA_LOG_HOME}/omm/oms/ha/scriptlog/httpd.log** command to view the httpd resource log of HA, analyze the log, locate the cause of the resource exception, and rectify the fault.
- Step 7** Five minutes later, 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 9 Select **Controller** and **OmmServer** for Service.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.54 ALM-12072 Floating IP Address Resource Is Abnormal

Description

HA checks the floating IP address resource of Manager every 9 seconds. This alarm is generated when HA detects that the floating IP address resource is abnormal for three consecutive times.

This alarm is cleared when the floating IP address resource is normal.

Resource type of floating IP address is single-active. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new floating IP address 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12072	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- If the floating IP address process restarts continuously, the native UI of the service may fail to be accessed.

Possible Causes

The floating IP address is abnormal.

Check the floating IP address status of the primary management node.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address and resource name for which the alarm is generated.

Step 3 Log in to the active management node as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

Step 4 Run the following command to go to the **\${BIGDATA_HOME}/om-server/om/sbin/** directory:

```
cd ${BIGDATA_HOME}/om-server/om/sbin/
```

- Step 5** Run the **sh status-oms.sh** command to check whether the floating IP address of the active Manager is normal. In the command output, check whether the following information is displayed in the row where **ResName** of the active management node is **floatip**:

Example:

```
10-10-10-160 floatip Normal Normal Single_active
```

- If yes, go to [Step 9](#).
- If no, go to [Step 6](#).

- Step 6** Run the **ifconfig** command to check whether the network adapter of the floating IP address exists.
- If yes, go to [Step 9](#).
 - If no, go to [Step 7](#).

- Step 7** Run the **ifconfig** Network adapter name Floating IP address **netmask** Subnet mask command to reconfigure the network adapter of the floating IP address, for example, **ifconfig eth0 10.10.10.102 netmask 255.255.255.0**.

- 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](#).

Collect fault information.

- Step 9** On the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 10** Select **Controller** and **OmmServer** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.55 ALM-12073 CEP Resource Is Abnormal

Description

HA checks the CEP resource of Manager every 60 seconds. This alarm is generated when the HA detects that the CEP resource is abnormal for two consecutive times.

This alarm is cleared when the CEP resource is normal.

Resource type of CEP is single-active. Active/standby will be triggered upon resource exceptions. When this alarm is generated, the active/standby switchover is complete and new CEP 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12073	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- The CEP process repeatedly restarts, causing monitoring data to be abnormal.

Possible Causes

The CEP process is abnormal.

Check whether the CEP process is normal.

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

- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
- Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
- Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
- Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** commands to check whether the status of the CEP resource managed by HA is normal. (In single-node mode, the CEP resource is in the normal state. In two-node cluster mode, the CEP 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/cep/cep.log** and **vi \${BIGDATA_LOG_HOME}/omm/oms/cep/scriptlog/cep_ha.log** commands to view the CEP resource logs of HA, analyze the logs, locate the cause of the resource exception, and rectify the fault.
- Step 6** Five minutes later, check whether this 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 **Controller** and **OmmServer** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.56 ALM-12074 FMS Resource Is Abnormal

Description

HA checks the FMS resource of Manager every 60 seconds. This alarm is generated when HA detects that the FMS resources are abnormal for two 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 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12074	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- The FMS process repeatedly restarts. As a result, alarm information may fail to be reported.

Possible Causes

The FMS process is abnormal.

Handling Procedure

Check whether the FMS process is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** commands to check whether the status of the FMS resource managed by the HA is normal. In single-node mode, the FMS resource is in the normal state. In two-node cluster mode, the FMS 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/fms/fms.log** and **vi \${BIGDATA_LOG_HOME}/omm/oms/fms/scriptlog/fms_ha.log** commands to view the FMS resource logs of HA, analyze the logs, locate the cause of the resource exception, and rectify the fault.

- Step 6** Five minutes later, check whether this 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 **Controller** and **OmmServer** for **Service**.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.57 ALM-12075 PMS Resource Is Abnormal

Description

The HA checks the PMS resource of the 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 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12075	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

- The active/standby Manager switchover occurs.
- The PMS process repeatedly restarts, causing monitoring information to be abnormal.

Possible Causes

The PMS process is abnormal.

Handling Procedure

Check whether the PMS process is normal.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host name for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **su - omm** and **sh \${BIGDATA_HOME}/om-server/OMS/workspace0/ha/module/hacom/script/status_ha.sh** commands to check whether the status of the PMS resource managed by the HA is normal. In single-server mode, the PMS resource is in the normal state. In dual-server mode, the PMS 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/pms/pms.log** and **vi \${BIGDATA_LOG_HOME}/omm/oms/pms/scriptlog/pms_ha.log** commands to view the PMS resource logs of HA, analyze the logs, locate the cause of the resource exception, and rectify the fault.
- Step 6** Five minutes later, check whether this 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 **Controller** and **OmmServer** for Service.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.58 ALM-12076 GaussDB Resource Is Abnormal

Description

The HA software checks the Manager database every 10 seconds. This alarm is generated when HA detects that the database is abnormal for three consecutive times.

This alarm is cleared when the database is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12076	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If databases are abnormal, all core services and related service processes, such as alarms and monitoring functions, are affected.

Possible Causes

An error occurred in the database.

Handling Procedure

Check the database status of the active and standby management nodes.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the active and standby management nodes as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. Run the **su - ommdba** command to switch to user **ommdba**, and run the **gs_ctl query** command. Check whether the following information is displayed. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

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 yes, go to **Step 4**.
- If no, go to **Step 3**.

Step 3 Contact the network administrator to check whether a network fault occurs and rectifies the fault.

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

Step 4 Wait for 5 minutes and 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 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 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
ldap	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 no, go to **Step 6**.

Collect fault information.

Step 6 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 7 Select **OmmServer** 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 technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.59 ALM-12077 User Omm Expired

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12077	Tenant plane alarm	Major	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host 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 ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l omm** command to view the password of the current **omm** user.

- Step 3** View the value of **Account Expires** to check whether the user configurations have expired.

NOTE

If the parameter value is **never**, the password never expires.

- If yes, go to [Step 4](#).
- If no, go to [Step 5](#).

- Step 4** Run the **chage -E 'yyyy-MM-dd' omm** command to set the validity period of the **omm** user. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.60 ALM-12078 Password of User Omm Expired

Description

The system starts at 00:00 every day and checks whether the **omm** password expires every eight hours. This alarm is generated when the password expires.

This alarm is cleared when the **omm** password validity period is changed and the current status is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12078	Tenant plane alarm	Major	Security alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host 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 **omm** password has expired.

Handling Procedure

Check whether the password of user omm in the system has expired.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l omm** command to view the password of the current **omm** user.

- Step 3** Search for the value of **Password Expires** and check whether the password has expired.

 **NOTE**

If the parameter value is **never**, the password never expires.

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

- Step 4** Run the **chage -M 'days'omm** command to set the validity period of the **omm** password. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for **Service**.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.61 ALM-12079 User omm Is About to Expire

Description

The system starts at 00:00 every day and checks whether the **omm** user is about to expire every 8 hours. This alarm is generated when the difference between the current time and the user expiration time is less than 15 days.

This alarm is cleared when the validity period of the **omm** user is reset and the current status of the **omm** user is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12079	Tenant plane alarm	Minor	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host 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 in the system is about to expire.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l omm** command to view the password of the current **omm** user.

- Step 3** Search for the value of **Account Expires** and check whether the user settings 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

- Step 4** Run the **chage -E 'yyyy-MM-dd' omm** command to set the validity period of the **omm** user. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.62 ALM-12080 Password of User omm Is About to Expire

Description

The system starts at 00:00 every day and checks whether the **omm** password is about to expire every eight hours. This alarm is generated when the difference between the current time and the password expiration time is less than 15 days.

This alarm is cleared when the **omm** password validity period is reset and the current status is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12080	Tenant plane alarm	Minor	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

User **omm** has expired. The node trust relationship is unavailable, and Manager cannot manage the services.

Possible Causes

The **omm** password of the host 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 ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l omm** command to view the password of the current **omm** user.

- Step 3** Search for the value of **Password Expires** and check whether the password is 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

- Step 4** Run the **chage -M 'days' omm** command to set the validity period of the **omm** password. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.63 ALM-12081 User ommdba Expired

Description

The system starts at 00:00 every day and checks whether the **ommdba** user has expired every eight hours. This alarm is generated when the user has expired.

This alarm is cleared when the validity period of the **ommdba** user is reset and the current status of the **ommdba** user is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12081	Tenant plane alarm	Major	Security violation	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host 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 in the system has expired.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l ommdba** command to view the password of the current **ommdba** user.

- Step 3** 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

- Step 4** Run the **chage -E 'yyyy-MM-dd' ommdba** command to set the validity period of the **ommdba** user. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.64 ALM-12082 User ommdba Is About to Expire

Description

The system starts at 00:00 every day and checks whether the **ommdba** user is about to expire every 8 hours. This alarm is generated when the user is about to expire in 15 days.

This alarm is cleared when the validity period of the **ommdba** user is reset and the current status of the **ommdba** user is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12082	Tenant plane alarm	Minor	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

If the **ommdba** user expires, the OMS database cannot be managed and data cannot be accessed.

Possible Causes

The **ommdba** user of the host is about to expire.

Handling Procedure

Check whether user ommdba is about to expire.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l ommdba** command to view the settings of the current **ommdba** user.

- Step 3** Search for the value of **Account Expires** and check whether the user settings 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

- Step 4** Run the **chage -E 'yyyy-MM-dd' ommdba** command to set the validity period of the **ommdba** user. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.65 ALM-12083 Password of User ommdba Is About to Expire

Description

The system starts at 00:00 every day to check whether the password of user **ommdba** is about to expire every eight hours. This alarm is generated if the password is about to expire no less than 15 days later.

This alarm is cleared when the password validity period of user **ommdba** is reset and the current status is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12083	Tenant plane alarm	Major	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

The OMS database cannot be managed and data cannot be accessed.

Possible Causes

The **ommdba** password of the host is about to expire.

Handling Procedure

Check whether the ommdba password in the system is about to expire.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l ommdba** command to view the password of the current **ommdba** user.

Step 3 Search for the value of **Password Expires** and check whether the password is 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

Step 4 Run the **chage -M 'days' ommdba** command to set the validity period of the **ommdba** password. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 6 Select **NodeAgent** for Service.

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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.66 ALM-12084 Password of User **ommdba** Expired

Description

The system starts at 00:00 every day and checks whether the **ommdba** password has expired every eight hours. This alarm is generated when the password has expired.

This alarm is cleared when the **ommdba** password validity period is reset and the current status is normal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12084	Tenant plane alarm	Major	Security violation	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

If the password of user **ommdba** expires, the mutual trust relationship between Manager nodes is unavailable and Manager cannot manage services.

Possible Causes

The **ommdba** password of the host has expired.

Handling Procedure

Check whether the ommdba password in the system expires.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the faulty node in the cluster as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Run the **chage -l ommdba** command to view the password of the current **ommdba** user.

- Step 3** Search for the value of **Password Expires** and check whether the password has 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 yes, go to **Step 4**.
- If no, go to **Step 5**.

- Step 4** Run the **chage -M 'days' ommdba** command to set the validity period of the **ommdba** password. Wait for 8 hours 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 the FusionInsight Manager portal, choose **O&M > Log > Download**.

- Step 6** Select **NodeAgent** for Service.

- 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.67 ALM-12085 Service Audit Log Dump Failure

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12085	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

The service audit logs may be lost.

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 size of service audit logs is too large.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** In the alarm list on FusionInsight Manager, locate the row that contains the alarm and click  to view the host address for which the alarm is generated.
- Step 3** Log in to the host where the alarm is generated as user **root**. The password is specified by users before the installation. Obtain it from the system administrator.
- Step 4** Run the **vi \${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** command to search for the keyword "LOG SIZE is more than 5000MB". Indicates whether the keyword can be found.
- If yes, go to **Step 5**.
 - If no, go to **Step 6**.

- Step 5** Check whether the oversized service audit logs are caused by exceptions.

The storage space of the OMS backup path is insufficient.

- Step 6** Run the **vi \${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log** command to search for the keyword "Collect log failed, too many logs on". Indicates whether the keyword can be found.
- If yes, obtain the host IP address following the keyword Collect log failed, too many logs on and run the **Step 7** command.
 - If no, go to **Step 11**.

- Step 7** Log in to **Step 6** the host IP address as user **root**.

- Step 8** Run the **vi \${BIGDATA_LOG_HOME}/nodeagent/scriptlog/collectLog.log** command and search for the keyword log size exceeds.
- If yes, go to **Step 9**.
 - If no, go to **Step 11**.

Step 9 Expand the disk capacity of the OMS node by referring to section "Adding a New Disk to an Existing Node" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Capacity Adjustment Guide.

Step 10 In the next execution period, 03:00, check whether the alarm is cleared.

- If yes, no further action is required.
- If no, go to **Step 11**.

Check whether the space of a host where the service is located is insufficient.

Step 11 Run the `vi ${BIGDATA_LOG_HOME}/controller/scriptlog/getLogs.log` command to search for the keyword "Collect log failed, no enough space on *host/p*". Indicates whether the keyword can be found.

- If yes, obtain *host/p* as the IP address of the abnormal host and go to **Step 12**.
- If no, go to **Step 15**.

Step 12 Log in to the host as user **root** using the IP address. Run the `df -${BIGDATA_HOME}/tmp` command to obtain the remaining space of the log directory on the host. Check whether the value is less than 1000 MB.

- If yes, go to **Step 13**.
- If no, go to **Step 15**.

Step 13 Expand the disk capacity of the node by referring to section "Adding a New Disk to an Existing Node" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Capacity Adjustment Guide.

Step 14 In the next execution period, 03:00, 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 **Controller** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.68 ALM-12087 System Is in the Upgrade Observation Period

Description

The system checks whether it is in the upgrade observation period at 00:00 every day and checks whether the duration that it is 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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12087	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Upgrade Observation Period (Days)	Specifies the days that the system is in the upgrade observation period.

Impact on the System

The next upgrade or patch installation will fail.

Possible Causes

The upgrade is not submitted within a certain period (10 days by default) after the system is upgraded.

Handling Procedure

Check whether the system is in the upgrade observation period.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** Log in to the active management node as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. You can view the IP addresses of the active and standby management nodes on the Host tab page of FusionInsight Manager.

- Step 3** 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 4** Run the **select * from OM_CLUSTERS;** command to check the cluster information.

- Step 5** Check whether the value of **upgradObservationPeriod** isON is true, as shown in [Figure 2-17](#).

- If yes, the system is in the upgrade observation period. Use UpdateTool to submit the upgrade. For details, see the upgrade guide of the corresponding version.
- If no, go to [Step 7](#).

Figure 2-17 Cluster Information

CLUSTER_ID	CLUSTER_NAME	CLUSTER_DESCRIPTION	STACK_NAME	STACK_TYPE	PRESTACK_NAME	PRESTACK_TYPE	STACK_NODEL	OPENAPI_API_VERSION	IS_DETACHED	UPDATE_MODE	EXTEND_PWD
15801090310702000	test	upgrade	test	test	test	test	0	0	0	0	0

- Step 6** In the early morning of the next day, check whether this 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 Controller for Service.

Step 9 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 10 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.69 ALM-12089 Network Connection Between Nodes Is Abnormal

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12089	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

If the network health status between cluster nodes is poor, the functions of some components are affected.

Possible Causes

- Node shutdown
- The network is disconnected.

Handling Procedure

Check the network health status.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** 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 3** Log in to the node for which the alarm is generated. Run the ping command on the node to ping the target node to check whether the network between the two nodes is normal.
- If yes, go to [Step 7](#).
 - If no, go to [Step 4](#).
- Step 4** 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 [Step 6](#).
 - If no, go to [Step 5](#).
- Step 5** Check the running status of the faulty node to determine whether the node is shut down.
- If yes, start the faulty node and go to [Step 3](#).
 - If no, contact related personnel to locate the fault. If you need to remove the faulty node from the cluster, go to [Step 6](#). Otherwise, go to [Step 7](#).

Step 6 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 manually clear the alarm.

Step 7 Wait for 30 seconds and check whether the alarm is automatically cleared. If the alarm persists, manually clear it.

Collect fault information.

Step 8 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 9 Select **OmmAgent for Service**.

Step 10 Click  in the upper right corner to set the log collection time range. Generally, the time range is 10 seconds before and after the alarm generation time. Click **Download**.

Step 11 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.70 ALM-12099 Core Dump Occurs

Description

The GaussDB A provides the core file management to manage the life cycle of core files generated when applications crash and manage alarm notifications. This alarm is generated when a new core file is detected.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
12099	Tenant plane alarm	Minor	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.

Type	Parameter	Description
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

This alarm indicates that some processes crash. If a key process crashes, the cluster may be unavailable for a short period of time.

Possible Causes

Related processes crash.

Handling Procedure

CAUTION

- The following operations for parsing and viewing core file stack information may involve sensitive user data. Therefore, the technical support engineers can perform these operations only after being authorized by users.
- By default, the core file system where the alarm is generated is retained for 72 hours. If the file storage times out or the file size exceeds the preset value, the system automatically clears the file. If this alarm is generated, contact technical support engineers as soon as possible.

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

- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
- Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
- Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
- Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 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 file based on the **DumpedFilePath** attribute in the other information.

Step 3 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 run the **Step 4** command.
- If yes, go to **Step 4**.

Step 4 Use the GDB tool to view the detailed stack information about the core file.

1. Go to the **DumpedFilePath** directory and find the core file.
2. Run the following commands to obtain the symbol table of the core file (SUSE OS is used as an example):

```
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-SUSE11-64bit-symbol.tar.gz  
cd symbols/bin/
```

Find the symbol table file whose name is the same as the process for which the alarm is generated. For example, the symbol table corresponding to **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.

Step 5 Contact technical support and send 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

2.3.71 ALM-25000 LdapServer Service Unavailable

Description

The system checks the LdapServer service status every 30 seconds. This alarm is generated when both LdapServer services are abnormal.

This alarm is cleared when at least one LdapServer service is in the normal state.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
25000	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

When this alarm is generated, no operation can be performed for the KrbServer users and LdapServer users in the cluster. For example, users, user groups, or roles cannot be added, deleted, or modified, and user passwords cannot be changed on the FusionInsight Manager portal. The authentication for existing users in the cluster is not affected.

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 reside are faulty.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **Cluster > Name of the desired cluster > Service > LdapServer > Instance**. Go to the LdapServer instance page to obtain the host name of the node where the two SlapdServer instances reside.
- Step 3** Choose **O&M > Alarm > Alarm**. On the **Alarm** page of the FusionInsight Manager system, check whether the **Node Fault** alarm is generated.
- If yes, go to [Step 4](#).
 - If no, go to [Step 7](#).
- Step 4** Check whether the host name in the alarm information is the same as the [Step 7](#) host name.
- If yes, go to [Step 5](#).
 - If no, go to [Step 7](#).
- Step 5** Rectify the fault by following steps provided in [ALM-12006 Node Fault](#).
- Step 6** In the alarm list, check whether alarm **LdapServer Service Unavailable** is cleared.
- If yes, no further action is required.
 - If no, go to [Step 11](#).
- Check whether the LdapServer process is in normal state.**
- Step 7** Choose **O&M > Alarm > Alarm**. On the **Alarm** page of the FusionInsight Manager system, check whether the **Process Fault** alarm is generated.
- If yes, go to [Step 8](#).
 - If no, go to [Step 11](#).
- Step 8** Check whether the service name and host name in the alarm are consistent with the LdapServer service and host names.
- If yes, go to [Step 9](#).
 - If no, go to [Step 11](#).
- Step 9** Rectify the fault by following steps provided in [ALM-12007 Process Fault](#).
- Step 10** In the alarm list, check whether alarm **LdapServer Service Unavailable** 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** Expand the **Service** drop-down list, and select **LdapServer** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.72 ALM-25004 Abnormal LdapServer Data Synchronization

Description

The system checks LdapServer data every 30 seconds. This alarm is generated when LdapServer data on the active and standby Manager nodes is inconsistent for 12 consecutive times. This alarm is cleared when LdapServer data on the active and standby Manager nodes becomes consistent.

The system checks LdapServer data every 30 seconds. This alarm is generated when LdapServer data in the cluster is inconsistent with that on Manager for 12 consecutive times. This alarm is cleared when LdapServer data in the cluster and on Manager becomes consistent.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
25004	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

LdapServer data inconsistency occurs because LdapServer data on Manager or 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 of the node where LdapServer resides is faulty.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarm**. Record the IP address of **Host Name** in the alarm location information as IP1. If multiple alarms are generated, record the IP addresses as IP1, IP2, and IP3 respectively.
- Step 3** Contact technical support engineers to use to log in to the node corresponding to IP1. Run the **ping** command on the node to check whether the IP address of the management plane of the active OMS node can be pinged.
- If yes, go to **Step 5**.
 - If no, go to **Step 4**.
- Step 4** 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 5**.

Check whether the LdapServer process is normal.

Step 5 On the **Alarm** page of FusionInsight Manager, check whether **Abnormal OLDap Resource** is generated for the LdapServer service.

- If yes, go to [Step 6](#).
- If no, go to [Step 8](#).

Step 6 Rectify the fault by following steps provided in [ALM-12004 OLDap Resource Is Abnormal](#).

Step 7 In the alarm list, check whether **Abnormal LdapServer Data Synchronization** is cleared.

- If yes, no further action is required.
- If no, go to [Step 8](#).

Step 8 On the **Alarm** page of FusionInsight Manager, check whether **Process Fault** is generated for the LdapServer service.

- If yes, go to [Step 9](#).
- If no, go to [Step 11](#).

Step 9 Rectify the fault by following steps provided in [ALM-12007 Process Fault](#).

Step 10 In the alarm list, check whether **Abnormal LdapServer Data Synchronization** is cleared.

- If yes, no further action is required.
- If no, go to [Step 11](#).

Check whether the OS restart damages data on LdapServer.

Step 11 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. Record the IP address of **Host Name** in the alarm location information as IP1. If multiple alarms are generated, record the IP addresses as IP1, IP2, and IP3 respectively. Choose **Cluster > Name of the target cluster > Service > LdapServer > Configuration**, record the LdapServer port number as PORT (if the IP address in the alarm locating information is the IP address of the standby OMS node, choose **System > OMS > oldap > Modify Configuration**, and record the LdapServer service listening port number).

Step 12 Log in to the IP1 node as user **omm**.

Step 13 Run the following command to check whether the query result contains error information:

```
ldapsearch -H ldaps://IP1:PORT -LLL -x -D cn=root,dc=hadoop,dc=com -W -b ou=Peoples,dc=hadoop,dc=com
```

- If yes, go to [Step 14](#).
- If no, go to [Step 16](#).

Step 14 Use the backup files generated before the alarm generation date to restore the LdapServer and OMS. For details, see section "Creating a Restoration Task" in Huawei Cloud Stack 8.x.x Data Warehouse Service (DWS) Administrator Guide.

 NOTE

Use the OMS data and LdapServer data backed up at the same time to restore data. Otherwise, the service and operation may fail. To recover data when services run properly, you are advised to manually backup 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 15 In the alarm list, check whether **Abnormal LdapServer Data Synchronization** 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 Expand the **Service** drop-down list, and select **LdapServer** and **OmsLdapServer** for the target cluster.

Step 18 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 19 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.73 ALM-25005 Abnormal Nscd Service

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
25005	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If the nscd service is unavailable, the node may fail to synchronize data from the LdapServer. In this case, running the **id** command may fail to obtain LDAP data, affecting upper-layer services.

Possible Causes

- The nscd service is not started.
- The network is disconnected, and the LDAP server cannot be accessed.
- The Name Service is abnormal.
- The OS executes commands slowly, and users cannot be queried.

Handling Procedure

Check whether the nscd service is started.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. Record the IP address of **Host Name** in the alarm location information as IP1. If multiple alarms are generated, record the IP addresses as IP1, IP2, and IP3 respectively.

Step 3 Contact technical support engineers. Log in to the node with IP address 1 as user **root**. The password is specified by users before the installation. Obtain it from the system administrator. Run the **ps -ef | grep nscd** command on the node to check whether the **/usr/sbin/nscd** process is started.

```
root    6893 12764 0 20:20 pts/2  00:00:00 grep nscd
root    8480     1 0 Jun13 ?      00:31:49 /usr/sbin/nscd
```

- If yes, go to [Step 6](#).
- If no, go to [Step 4](#).

Step 4 Run the **service nscd restart** command as the **root** user to restart the nscd service. Run the **ps -ef | grep nscd** command to check whether the service is started.

- If yes, go to [Step 5](#).
- If no, go to [Step 16](#).

Step 5 Five minutes later, run the command again as the **root** user to check whether the service exists.

- If yes, go to [Step 12](#).
- If no, go to [Step 16](#).

Check whether the network is faulty, and whether the LDAP server can be accessed.

Step 6 Log in to the faulty node as user **root** and run the **ping** command to check whether the network between the node and the LdapServer node is normal.

- If yes, go to [Step 7](#).
- If no, contact the network administrator to rectify the network fault.

Check whether the Name Service is normal.

Step 7 Log in to the faulty node as user **root**. Run the **cat /etc/nsswitch.conf** command to check whether **passwd**, **group**, **services**, **netgroup**, and **aliases** are correctly configured.

The correct parameter configurations are as follows: **passwd: compat ldap**, **group: compat ldap**, **services: files ldap**, **netgroup: files ldap**, and **aliases: files ldap**.

- If yes, go to [Step 8](#).
- If no, go to [Step 10](#).

Step 8 Log in to the faulty node as user **root**. Run the **cat /etc/nscd.conf** command to check whether the values of **enable-cache passwd**, **positive-time-to-live passwd**, **enable-cache group**, and **positive-time-to-live group** in the configuration file are correct.

The correct parameter configurations are as follows: **enable-cache passwd yes**, **positive-time-to-live passwd yes**, **enable-cache group yes**, and **positive-time-to-live group yes**.

- If yes, go to [Step 9](#).
- If no, go to [Step 11](#).

Step 9 Run the **/usr/sbin/nscd -i group** and **/usr/sbin/nscd -i passwd** commands as the **root** user, wait for 2 minutes, and then run the **id admin** and **id backup/manager** commands to check whether the results can be queried.

```
host07:~ # id admin  
uid=20000(admin) gid=9998(ficommon) groups=9998(ficommon),8000(Manager_administrator_180)  
host07:~ # id backup/manager  
uid=20002(backup/manager) gid=10001(supergroup) groups=10001(supergroup)
```

- If yes, go to [Step 12](#).
- If no, go to [Step 16](#).

Step 10 Run the **vi /etc/nsswitch.conf** command as the **root** user, correct the settings of the five configuration items in the [Step 7](#) file, save the settings, and run the **service nscd restart** command to restart the nscd service. Wait for 2 minutes, run the **id admin** and **id backup/manager** commands, and check whether the results can be queried.

- If yes, go to [Step 12](#).
- If no, go to [Step 16](#).

Step 11 Run the **vi /etc/nscd.conf** command as the **root** user, correct the settings of the four configuration items in the [Step 8](#) file, save the settings, and run the **service nscd restart** command to restart the nscd service. Wait for 2 minutes, run the **id admin** and **id backup/manager** commands, and check whether the results can be queried.

- If yes, go to [Step 12](#).
- If no, go to [Step 16](#).

Step 12 Log in to FusionInsight Manager, wait for 5 minutes, and check whether the **Abnormal Nscd Service** alarm is cleared.

- If yes, no further action is required.
- If no, go to [Step 13](#).

Check whether the operating system responds slowly when a command is executed.

Step 13 Log in to the faulty node as user **root**, run the **id admin** command, and check whether the command execution is slow. If the command execution takes more than 3 seconds, the command execution is slow.

- If yes, go to [Step 14](#).
- If no, go to [Step 16](#).

Step 14 Run the **cat /var/log/messages** command to check whether the nscd restarts frequently or whether the exception information **Can't contact LDAP server** exists.

An example of nscd exception information is as follows:

```
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 15**.
- If no, go to **Step 16**.

Step 15 Run the `vi $BIGDATA_HOME/tmp/random_ldap_ip_order` command to change the number at the end. If the 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 exchange the first two IP addresses of the URI configuration item.

After the modification, press **Esc** to exit the editing mode and enter `:wq` to save the modification and exit.

Run the `service nscd restart` command to restart the nscd service. Wait for 5 minutes and run the `id admin` command again. Check whether the command execution is slow.

- If yes, go to **Step 16**.
- If no, log in to other faulty nodes and repeat **Step 13** to **Step 15** to check whether the first LdapServer node in the URL 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 fault information.

Step 16 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 17 Expand the **Service** drop-down list, and select **LdapClient** for the target cluster.

Step 18 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 19 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.74 ALM-25006 Abnormal Sssd Service

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 Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
25006	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If the sssd service is unavailable, the node may fail to synchronize data from the LdapServer. In this case, running the **id** command may fail to obtain LDAP data, affecting upper-layer services.

Possible Causes

- The sssd service is not started or is started incorrectly.
- The network is disconnected, and the LDAP server cannot be accessed.
- The Name Service is abnormal.
- The OS executes commands slowly, and users cannot be queried.

Handling Procedure

Check whether the sssd service is started or incorrectly started.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
- Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 - Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 - Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. Record the IP address of **Host Name** in the alarm location information as IP1. If multiple alarms are generated, record the IP addresses as IP1, IP2, and IP3 respectively.

Step 3 Contact technical support engineers. to log in to the node with IP address 1 The password is specified by users before the installation. Obtain it from the system administrator. as user **root**. Run the **ps -ef | grep sssd** command on the node to check whether the **/usr/sbin/sssd** process is started.

```
root    6893 12764 0 20:20 pts/2  00:00:00 grep sssd
root    8480  1 0 Jun13 ?  00:33:19 /usr/sbin/sssd
```

- If yes, go to [Step 4](#).
- If no, go to [Step 5](#).

Step 4 Check whether the sssd process queried in [Step 3](#) has three subprocesses.

- If yes, go to [Step 6](#).
- If no, go to [Step 5](#).

Step 5 Run the **service sssd restart** command as the **root** user to restart the sssd service, and run the **ps -ef | grep sssd** command to check whether the sssd process is normal.

In normal cases, the **/usr/sbin/sssd** process and three sub-processes **/usr/libexec/sssd/sssd_be**, **/usr/libexec/sssd/sssd_nss** and **/usr/libexec/sssd/sssd_pam** exist.

- If yes, go to [Step 10](#).
- If no, go to [Step 14](#).

Check whether the network is faulty and the LDAP server cannot be accessed.

Step 6 Log in to the faulty node as user **root** and run the **ping** command to check whether the network between the node and the LdapServer node is normal.

- If yes, go to [Step 7](#).
- If no, contact the network administrator to rectify the network fault.

Check whether the Name Service is normal.

Step 7 Log in to the faulty node as user **root** and run the **cat /etc/nsswitch.conf** command to check whether passwd and group in the NameService configuration are correct.

The correct parameter configurations are as follows: **passwd: files sss** and **group: files sss**.

- If yes, go to [Step 8](#).
- If no, go to [Step 9](#).

Step 8 Run the `/usr/sbin/ssss_cache -G` and `/usr/sbin/ssss_cache -U` commands as the **root** user, wait for 2 minutes, and then run the **id admin** and **id backup/manager** commands to check whether the results can be queried.

- If yes, go to [Step 10](#).
- If no, go to [Step 14](#).

Step 9 Run the `vi /etc/nsswitch.conf` command as the **root** user, correct the values of the two configuration items in the [Step 7](#) file, save the file, and run the `service sssd restart` command to restart the sssd service. Wait for 2 minutes, run the **id admin** and **id backup/manager** commands, and check whether the command output is correct.

```
host07:~ # id admin  
uid=20000(admin) gid=9998(ficommon) groups=9998(ficommon),8000(Manager_administrator_180)  
host07:~ # id backup/manager  
uid=20002(backup/manager) gid=10001(supergroup) groups=10001(supergroup)
```

- If yes, go to [Step 10](#).
- If no, go to [Step 14](#).

Step 10 Log in to FusionInsight Manager, wait for 5 minutes, and check whether the **Abnormal Sssd Service** alarm is cleared.

- If yes, no further action is required.
- If no, go to [Step 11](#).

Check whether the operating system responds slowly when a command is executed.

Step 11 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 12](#).
- If no, go to [Step 14](#).

Step 12 Run the `cat /var/log/messages` command to check whether the sssd restarts frequently or whether the exception 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 13](#).
- If no, go to [Step 14](#).

Step 13 Run the `vi $BIGDATA_HOME/tmp/random_ldap_ip_order` command to change the number at the end. If the 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 and kill the process. Run the **/usr/sbin/sssd -D -f** command to restart the sssd service. Wait for 5 minutes and run the **id admin** command again.

Check whether the command execution is slow.

- If yes, go to [Step 14](#).
- If no, log in to other faulty nodes and run [Step 11](#) to [Step 13](#). 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 14 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 15 Expand the **Service** drop-down list, and select **LdapClient** for the target cluster.

Step 16 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 17 Contact technical support and send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.75 ALM-25500 KrbServer Service Unavailable

Description

The system checks the KrbServer service status every 30 seconds. This alarm is generated when the KrbServer service is abnormal.

This alarm is cleared when the KrbServer service is in normal state.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
25500	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Host for which the alarm is generated.

Impact on the System

When this alarm is generated, no operation can be performed for the KrbServer component in the cluster. The authentication of KrbServer in other components will be affected. The running status of components that depend on KrbServer in the cluster is faulty.

Possible Causes

- The node where the KrbServer service resides is faulty.
- The OLDap service is unavailable.

Handling Procedure

Check whether the node where the KrbServer service resides is faulty.

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **Cluster > Name of the desired cluster > Service > KrbServer > Instance**. Go to the KrbServer instance page and view the host name of the node where the KrbServer service is deployed.
- Step 3** On the **Alarm** page of FusionInsight Manager, check whether the **Node Fault** alarm is generated.

- If yes, go to **Step 4**.
- If no, go to **Step 7**.

Step 4 Check whether the host name in the alarm information is the same as the **Step 2** host name.

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

Step 5 Rectify the fault by following steps provided in **ALM-12006 Node Fault**.

Step 6 In the alarm list, check whether alarm **KrbServer Service Unavailable** is cleared.

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

Check whether the OLdap service is unavailable.

Step 7 On the **Alarm** page of FusionInsight Manager, check whether the **Abnormal OLdap Resource** alarm is generated.

- If yes, go to **Step 8**.
- If no, go to **Step 10**.

Step 8 Rectify the fault by following steps provided in **ALM-12004 OLdap Resource Is Abnormal**.

Step 9 In the alarm list, check whether alarm **KrbServer Service Unavailable** is cleared.

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

Collect fault information.

Step 10 On the FusionInsight Manager portal, choose **O&M > Log > Download**.

Step 11 Expand the **Service** drop-down list, and select **KrbServer** 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 send the collected logs.

----End

Alarm Clearance

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.76 ALM-37000 MPPDBServer Data Directory or Redo Directory Is Missing

Description

This alarm is generated when the data directory or the redo directory (**pg_xlog**) of the data instance does not exist.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37000	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Instance for which the alarm is generated.

Impact on the System

When the data directory or redo directory on a data instance is missing, an alarm is reported and the data instance cannot be started. After this alarm is generated, the database instance cannot be started and the status is abnormal.

Possible Causes

The data directory or redo directory of the CN or DN is deleted.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource Id, instance name, and instance id of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the real-time alarm list, locate the row that contains the alarm and click  . Obtain the host name in the **HostName** value of **Location**.

Step 3 Check whether the data directory or redo directory (**pg_xlog**) of the instance reporting the alarm is deleted.

Run the **gs_om -t status --detail** command to obtain the data directory corresponding to each CN or DN in the cluster, and check whether the redo directory **pg_xlog** exists under the data directory.

1. Log in to the node for which the alarm is generated as user **omm**.
2. Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

3. Run the **gs_om -t status --detail** command. Information similar to the following is displayed:

```
[ CMServer State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  1 /opt/huawei/Bigdata/mppdb/cm/cm_server Primary  
  
[ Cluster State ]  
cluster_state : Normal  
redistributing : No  
balanced       : Yes  
  
[ Coordinator State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  5001 /srv/BigData/mppdb/data1/coordinator Normal  
  
[ Central Coordinator State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  5001 /srv/BigData/mppdb/data1/coordinator Normal  
  
[ GTM State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  1001 /opt/huawei/Bigdata/mppdb/gtm P Primary  
[ Datanode State ]
```

node	node_ip	instance	state
1	host0	10.0.0.1	6001 /srv/BigData/mppdb/data1/master1 P Primary Normal
1	host0	10.0.0.1	6002 /srv/BigData/mppdb/data2/master2 P Primary Normal
1	host0	10.0.0.1	6003 /srv/BigData/mppdb/data3/master3 P Primary Normal

Step 4 Recover the damaged data instance (CN/DN).

Step 5 On FusionInsight Manager, choose **Cluster > Name of the target cluster > Service > Instance**.

Step 6 Select the abnormal node, click **More**, and select **Restart Instance**. Restart the node, wait for 5 minutes, and check whether the alarm persists.

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

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 8 Select **MPPDB** from the **Service** list box.

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

After the fault is rectified, the system automatically clears this alarm.

Related Information

None

2.3.77 ALM-37001 Redo Logs of the MPPDBServer Instance Are Missing

Alarm Description

This alarm is generated when some Xlogs of the primary DataNode instance are deleted before being synchronized to the standby DataNode instance.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37001	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

After Xlogs in the **pg_xlog** directory of a primary DataNode are deleted, they cannot be synchronized from the primary DataNode to its standby. This triggers the rebuilding of the standby node, increasing the network pressure on the physical server running the standby node. If Xlogs being used by the primary DataNode are missing, some data is lost, and the primary DataNode is abnormal.

Possible Causes

- Xlogs under the **pg_xlog** directory of a primary DataNode are deleted when the primary DataNode is writing transactions.
- Xlogs under the **pg_xlog** directory of a primary DataNode are deleted when the corresponding standby DataNode is abnormal and the primary DataNode is writing transactions.

Handling Procedure

NOTE

- The cluster automatically triggers the rebuilding of the standby node. This alarm is automatically cleared after the rebuilding is successful.
- If the alarm persists for a long time, restart the node.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster name, host name, and instance name in **Location**.
- Step 3** Choose **Cluster**, click the name of the cluster for which the alarm is generated, and choose **Services > MPPDB > Instance**.
- Step 4** Select the abnormal node, click **More**, and select **Restart Instance**. Wait 5 minutes and check whether this alarm persists.
- If yes, go to **Step 5**.
 - If no, no further action is required.

Collect fault information.

- Step 5** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.
- Step 6** Select **MPPDB** 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 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

2.3.78 ALM-37002 Number of MPPDB Instance Connections Exceeds the Threshold

Alarm Description

This alarm is generated when the number of client connections to a Coordinator instance exceeds the upper limit (**max_connections*connection_alarm_rate**) configured in the **postgresql.conf** file.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37002	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

New clients cannot connect to the Coordinator instance.

Possible Causes

The number of clients connected to the Coordinator instance exceeds the upper limit (**max_connections*connection_alarm_rate**) specified in the **postgresql.conf** configuration file.

Handling Procedure

Increase the **max_connections** value.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster name and host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm** and run the command `source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profil` to initialize environment variables.

Step 4 Enlarge the maximum number of connections to the Coordinator node. For example, run the following command to change the number of node **plat1** to **3000**:

```
gs_guc set -Z coordinator -N plat1 -I all -c "max_connections = 3000"
```

Step 5 On FusionInsight Manager, choose **Cluster**, click the name of the cluster for which the alarm is generated, click **More**, and select **Restart Service**.

Step 6 Check whether this alarm is cleared.

- If yes, no further operation 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 Select **MPPDB** 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 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

2.3.79 ALM-37003 Asynchronous or Disconnected Primary and Standby GTM Instances

Alarm Description

This alarm is generated when the primary GTM instance is disconnected from or asynchronous with the standby GTM instance.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37003	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If the connection between the primary and standby GTM instances is abnormal and the primary GTM instance is in the synchronization state, the system is unavailable within 120 seconds. After detecting this fault, the system sets the primary GTM instance to the HA mode and then becomes normal. If the primary GTM instance is working in HA mode, the system works properly.

 NOTE

When the cluster is working properly, the primary GTM instance works in the synchronization state and synchronizes received tasks to the standby instance in real time, ensuring consistency between the primary and standby instances. If the standby instance becomes faulty and cannot recover, the primary instance stops synchronizing tasks to the standby instance. In this case, the primary instance works in HA mode.

Possible Causes

The connection between the primary and standby GTM instances is abnormal.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm** and run the following commands to check whether the primary and standby GTM instances in the cluster are faulty:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile  
gs_om -t status --detail
```

GTM State		node	node_ip	instance	state	sync_state

2	host2	10.7.66.183	1001	/opt/huawei/Bigdata/mppdb/gtm	P Primary	Connection ok Sync
3	host3	10.7.66.245	1002	/opt/huawei/Bigdata/mppdb/gtm	S Standby	Connection ok Sync

- If yes, fix the faulty instance. Then go to **Step 4**.
- If no, go to **Step 4**.

Step 4 Check whether the network of the hosts accommodating the primary and standby GTM instances is normal. For example, if the NIC used by the host of the primary

or standby GTM instance is eth0, run the following command to check whether the network is normal:

`/sbin/ifconfig eth0`

- If the network is normal, go to [Step 5](#).
- If the network is abnormal, contact the hardware engineer to repair the NIC, and then go to [Step 5](#).

Step 5 Check whether the alarm persists.

- 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 Select **MPPDB** 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 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

2.3.80 ALM-37004 Asynchronous or Disconnected Primary and Standby DataNode Instances

Alarm Description

This alarm is generated when the primary DataNode instance is disconnected from the standby DataNode instance.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37004	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The redo logs of the primary DataNode instance will be automatically sent to the standby DataNode instance, increasing the network pressure on the physical server running the standby DataNode instance.

System Actions

When the primary DataNode instance is disconnected from the standby DataNode instance, the redo logs of the primary DataNode instance are automatically sent to the standby DataNode instance, ensuring proper service operating.

Possible Causes

The primary DataNode instance is disconnected from the standby DataNode instance.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm** and run the following commands to check whether the primary and standby DataNode instances in the cluster are faulty:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile  
gs_om -t status --detail
```

- If yes, restore the faulty instance. Then go to **Step 4**.
- If no, go to **Step 4**.

Step 4 Check whether the network of the hosts accommodating the primary and standby DataNode instances is normal. For example, if the NIC used by the host of the primary or standby DataNode instance is `eth0`, run the following command to check whether the network is normal:

```
/sbin/ifconfig eth0
```

- If the network is normal, go to **Step 5**.
- If the network is abnormal, contact the hardware engineer to repair the NIC, and then go to **Step 5**.

Step 5 Check whether the alarm persists.

- 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 Select **MPPDB** 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 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

2.3.81 ALM-37005 GTM Process Is Abnormal

Alarm Description

This alarm is generated when the GTM instance process is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37005	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

- If the primary GTM instance fails to start, the cluster displays a startup failure message, and the standby GTM instance is promoted to the primary role.
- If the standby GTM instance fails to start, the cluster displays a startup failure message. However, the system is still available, and the primary GTM instance works in asynchronous mode.

Possible Causes

- The **gtm.conf** configuration file does not exist in the GTM instance data directory, or a parameter in the file is incorrectly configured.
- The GTM thread cannot listen on a certain IP address or cannot be bound to the listening port.

- The GTM instance process does not have the read or write permission on its data directory.

Handling Procedure

Check the alarm cause and collect fault information.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 3 Select **MPPDB** from the **Service** drop-down list.

Step 4 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 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

2.3.82 ALM-37006 Coordinator Node Process Is Abnormal

Alarm Description

This alarm is generated in either of the following scenarios:

- A hardware fault (such as power outage or hard disk damage) occurs on the server where the Coordinator node is located.
- The **postgresql.conf** configuration file does not exist in the Coordinator node data directory, or a parameter in the file is incorrectly configured.

- The Coordinator node thread cannot listen on a certain IP address or cannot be bound to the listening port.
- The Coordinator node process does not have the read or write permission on its data directory or the data directory is lost.
- The virtual IP address to which the Coordinator node instance is bound is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37006	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If a Coordinator node fails to start, the cluster displays a startup failure message. The database system will be unable to use DDL statements but can use DML statements.

After about 10 minutes, the system automatically deletes the faulty Coordinator node. You can query the Coordinator node status as **Deleted** by running the **gs_om -t status --detail** command. Both DDL and DML statements can be used.

NOTICE

Do not restart the MPPDB service directly. Perform operations by following the description in [Handling Procedure](#).

Possible Causes

- A hardware fault (such as power outage or hard disk damage) occurs on the server where the Coordinator node is located.
- The **postgresql.conf** configuration file does not exist in the Coordinator node data directory, or a parameter in the file is incorrectly configured.
- The Coordinator node thread cannot listen on a certain IP address or cannot be bound to the listening port.
- The Coordinator node process does not have the read or write permission on its data directory or the data directory is lost.
- The virtual IP address to which the Coordinator node instance is bound is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 If an alarm indicating that device partitions are lost is generated before or after this alarm is generated, rectify the fault by referring to "Hard Disk Troubleshooting" in the [**HUAWEI CLOUD Stack x.x.x Data Warehouse Service \(DWS\) Fault Management \(Physical Machine Clusters\)**](#).

Step 3 Wait 5 minutes after the alarm is generated. On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, check whether the alarm persists.

- If yes, go to **Step 4**.
- If no, no further action is required.

Step 4 In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location**.

Step 5 Choose **Cluster**, click the name of the cluster for which the alarm is generated, and choose **Services > MPPDB > Configuration > Basic Configurations**. Then, view the **mppdb.cms.active.ip** value to obtain the IP of the active CMS node.

Step 6 Log in to the active CMS node as user **omm** and run the **source \${BIGDATA_HOME}/mppdb/.mppdbgs_profile** command to start environment variables. Run the following command to check whether the status of the faulty Coordinator node is **Deleted**:

gs_om -t status --detail

- If yes, go to [Step 7](#).
- If no, go to [Step 13](#).

Step 7 On FusionInsight Manager, choose **Cluster**, click the name of the cluster for which the alarm is generated, and choose **Services > MPPDB**. Click **Instance** and click the MPPDBServer of the faulty node.

Step 8 Click **Configuration** and then **All Configurations**, and enter parameter **mppdb.coo.number** in the search box.

Step 9 Set the value of **mppdb.coo.number** to **0** and click **Save**.

Step 10 In the dialog box that is displayed, click **OK**. When the system displays **Operation succeeded**, click **Finish** to check whether the operation is successful.

- If yes, manually clear this alarm on the console after deleting the faulty Coordinator node.
- If no, go to [Step 13](#).

Step 11 Restore the faulty node. For details, see the [Huawei Cloud Stack x.x.x Data Warehouse Service \(DWS\) Fault Management \(Physical Machine Clusters\)](#).

Check whether the faulty node is successfully recovered.

- If yes, go to [Step 12](#).
- If no, replace the faulty node. For details, see "Replacing a GaussDB(DWS) Node" in the [Huawei Cloud Stack x.x.x Data Warehouse Service \(DWS\) Fault Management \(Physical Machine Clusters\)](#).

Step 12 Add the recovered Coordinator node.

1. Repeat [Step 7](#) to [Step 8](#), set the **mppdb.coo.number** parameter to **1**, and click **Save**.
2. In the dialog box that is displayed, click **OK**. A message indicating that the operation is successful is displayed. Click **Finish** and check whether the operation is successful.
 - If yes, the Coordinator node is added. No further action is required.
 - If no, go to [Step 13](#).

Step 13 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 14 Select **MPPDB** 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 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

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

Related Information

None

2.3.83 ALM-37007 DataNode Process Is Abnormal

Alarm Description

This alarm is generated in either of the following scenarios:

- The **postgresql.conf** configuration file does not exist in the DataNode data directory, or a parameter in the file is incorrectly configured.
- The DataNode thread cannot listen on a certain IP address or cannot be bound to the listening port.
- The DataNode process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37007	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

- If the primary DataNode instance fails to start, the system displays a failure message. After 120s, the cluster switches the standby DataNode instance to the primary one, maintaining system availability.
- If the standby DataNode instance fails to start, the system displays a failure message but remains available.

Possible Causes

- The **postgresql.conf** configuration file does not exist in the DataNode data directory, or a parameter in the file is incorrectly configured.
- The DataNode thread cannot listen on a certain IP address or cannot be bound to the listening port.
- The DataNode process does not have the read or write permission on its data directory.

Handling Procedure

Check the alarm cause and collect fault information.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 If an alarm indicating that device partitions are lost is generated before or after this alarm is generated, rectify the fault by referring to "Hard Disk Troubleshooting" in the [**HUAWEI CLOUD Stack x.x.x Data Warehouse Service \(DWS\) Fault Management \(Physical Machine Clusters\)**](#).

Step 3 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 4 Select **MPPDB** from the **Service** drop-down list.

Step 5 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 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

2.3.84 ALM-37008 MPPDB Service Unavailable

Alarm Description

The alarm module checks the MPPDB service health status every 30 seconds. This alarm is generated when the MPPDB service is faulty.

This alarm is cleared when the MPPDB becomes healthy.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37008	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Specifies the name of the service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the host for which the alarm is generated.

Impact on the System

GaussDB(DWS) cannot provide services for external systems.

Possible Causes

The MPPDB service is stopped.

Handling Procedure

Restart the MPPDB service.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location**.

Step 3 Choose **Cluster**, click the name of the cluster for which the alarm is generated, and choose **Services > MPPDB**.

Step 4 Click **More** and select **Restart Service**.

Step 5 Wait 5 minutes. On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, check whether the alarm persists.

- 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 Select **MPPDB** 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 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

2.3.85 ALM-37012 HA Listening Socket of MPPDBServer Instances Is Abnormal

Alarm Description

This alarm is generated when other processes of the OS occupy the HA listening port.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37012	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If the HA listening port is occupied for more than 120s, the system becomes unavailable.

System Actions

- If the HA port is occupied, the GaussDB process cannot be started. The cluster will try to restart the GaussDB process first. The system cannot be used during this period.

- If the process still cannot be started within 120s, the cluster promotes the standby DataNode instance to the primary role, and the system becomes available.

Possible Causes

Other processes in the OS occupy the HA listening port.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Locate the data directory of the DataNode instance for which the alarm is generated.

1. Log in to the node for which the alarm is generated as user **omm**.

2. Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile
```

3. Run the **gs_om -t status --detail** command. Information similar to the following is displayed:

```
[ CMServer State ]
```

node	node_ip	instance	state
1	host0	10.0.0.1	/opt/huawei/Bigdata/mppdb/cm/cm_server Primary

```
[ Cluster State ]
```

cluster_state	: Normal
redistributing	: No
balanced	: Yes

```
[ Coordinator State ]
```

node	node_ip	instance	state
------	---------	----------	-------

```
-----  
1 host0 10.0.0.1 5001 /srv/BigData/mppdb/data1/coordinator Normal  
[ Central Coordinator State ]  
node node_ip instance state  
-----  
1 host0 10.0.0.1 5001 /srv/BigData/mppdb/data1/coordinator Normal  
[ GTM State ]  
node node_ip instance state  
-----  
1 host0 10.0.0.1 1001 /opt/huawei/Bigdata/mppdb/gtm P Primary  
[ Datanode State ]  
node node_ip instance state  
-----  
1 host0 10.0.0.1 6001 /srv/BigData/mppdb/data1/master1 P Primary Normal  
1 host0 10.0.0.1 6002 /srv/BigData/mppdb/data2/master2 P Primary Normal  
1 host0 10.0.0.1 6003 /srv/BigData/mppdb/data3/master3 P Primary Normal
```

/srv/BigData/mppdb/data1/master1 is the DataNode instance data directory.

Step 4 Assume that the data directory of the instance is **/srv/BigData/mppdb/data1/master1**. Run the following command to open the **postgresql.conf** file:

```
vi /srv/BigData/mppdb/data1/master1/postgresql.conf
```

Locate the **repliconinfo1** parameter, and its **localport** value is the HA listening port. Run the following command to check whether the port is occupied by other processes (assume that the port is 10000):

```
netstat -anp | grep 10000
```

If the port is occupied, check whether it is occupied by a key process.

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

Step 5 Run the following command to stop the process:

```
kill -9 pid
```

Step 6 Check whether the alarm persists.

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

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 8 Select **MPPDB** 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 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

2.3.86 ALM-37013 MPPDBServer Instance Socket Is Abnormal

Alarm Description

This alarm is generated when other processes of the OS occupy the GTM or HA listening port.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37013	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

When the HA port is occupied for more than 120s, the system will automatically handle the fault and become available. However, the system is unavailable within that 120-second period.

System Actions

- If the listening or HA port is occupied, the GTM process cannot be started. The cluster will try to restart the process first. The system cannot be used during this period.
- If the process still cannot be started within 120s, the cluster promotes the standby GTM instance to the primary role, and the system becomes available.

Possible Causes

Other processes of the OS occupy the GTM listening or HA port.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Locate the data directory of the GTM instance for which the alarm is generated.

1. Log in to the node for which the alarm is generated as user **omm**.

2. Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

3. Run the **gs_om -t status --detail** command. Information similar to the following is displayed:

```
[ CMServer State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  1 /opt/huawei/Bigdata/mppdb/cm/cm_server Primary  
  
[ Cluster State ]  
cluster_state : Normal  
redistributing : No  
balanced       : Yes
```

```
[ Coordinator State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  5001 /srv/BigData/mppdb/data1/coordinator Normal  
  
[ Central Coordinator State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  5001 /srv/BigData/mppdb/data1/coordinator Normal  
  
[   GTM State   ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  1001 /opt/huawei/Bigdata/mppdb/gtm P Primary  
[ Datanode State ]  
node    node_ip      instance          state  
-----  
1 host0 10.0.0.1  6001 /srv/BigData/mppdb/data1/master1 P Primary Normal  
1 host0 10.0.0.1  6002 /srv/BigData/mppdb/data2/master2 P Primary Normal  
1 host0 10.0.0.1  6003 /srv/BigData/mppdb/data3/master3 P Primary Normal
```

`/opt/huawei/Bigdata/mppdb/gtm` is the data directory of the GTM instance.

Step 4 Assume that the data directory of the GTM instance is `/opt/huawei/Bigdata/mppdb/gtm/`. Run the following command to open the `gtm.conf` file:

```
vi /opt/huawei/Bigdata/mppdb/gtm/gtm.conf
```

Locate the listening port parameter `port` and the HA listening port parameter `local_port` of the GTM instance.

Step 5 Run the following command to check whether the port is occupied by other processes (assume that the port is 10000):

```
netstat -anp | grep 10000
```

If the listening port or HA port of the GTM instance is occupied, check whether it is occupied by a key process.

- If yes, go to [Step 6](#).
- If no, go to [Step 8](#).

Step 6 Run the following command to stop the process:

```
kill -9 pid
```

Step 7 Check whether the alarm persists.

- 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 Select **MPPDB** from the **Service** drop-down list.

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

2.3.87 ALM-37014 Lock File of the GaussDB Process Already Exists

Alarm Description

This alarm is generated when the lock file of a Coordinator or DataNode instance in the cluster fails to be created.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37014	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The instance that fails to create the lock file may fail to start, and the cluster cannot be started as well.

Possible Causes

System instances are terminated abnormally, leaving residual lock files in the system.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

Step 5 Run the following command to obtain the host for which the alarm is generated and its data directory (host at **10.252.153.218** and data directory **/srv/BigData/mppdb/data1/coordinator** in this example):

```
gs_om -t status --detail
```

```
[ CMServer State ]
```

node	node_ip	instance	state
------	---------	----------	-------

1	lfgphicprb09394	10.252.153.218	2 /opt/huawei/Bigdata/mppdb/cm/cm_server Primary
3	lfgphicprb09396	10.252.153.81	1 /opt/huawei/Bigdata/mppdb/cm/cm_server Standby

```
[ Cluster State ]
```

cluster_state : Normal
redistributing : No
balanced : No

[Coordinator State]				
node	node_ip	instance	state	
1	lfgphicprb09394	10.252.153.218	5001	/srv/BigData/mppdb/data1/coordinator Down
2	lfgphicprb09395	10.252.153.234	5002	/srv/BigData/mppdb/data1/coordinator Normal
3	lfgphicprb09396	10.252.153.81	5003	/srv/BigData/mppdb/data1/coordinator Normal

Step 6 Log in to the node in SSH mode, run the following commands to go to the data directory, and check whether there is a **postmaster.pid** file:

```
cd /srv/BigData/mppdb/data1/coordinator
```

```
ll
```

- If yes, go to [Step 7](#).
- If no, go to [Step 10](#).

Step 7 Run the following command to obtain the PID in the first line of the **postmaster.pid** file:

```
cat postmaster.pid
```

```
42883  
/srv/BigData/mppdb/data1/coordinator  
1541404937  
25308  
/opt/huawei/Bigdata/mppdb/mppdb_tmp  
localhost  
25308001 131076
```

Step 8 Run the following command to check whether there is a process with this PID:

```
ps -ef |grep 42883
```

```
omm 42883 1 4 Nov05 ? 17:25:59 /opt/huawei/Bigdata/mppdb/core/bin/gaussdb --  
coordinator -D /srv/BigData/mppdb/data1/coordinator  
omm 125791 55322 0 15:10 pts/0 00:00:00 grep --color=auto 42883
```

- If yes, go to [Step 9](#).
- If no, go to [Step 10](#).

Step 9 Run the following commands to stop the process and remove the **postmaster.pid** file, respectively. Then, check whether the alarm is cleared.

```
kill -9 42883
```

```
rm -f postmaster.pid
```

- If yes, no further action is required.
- If no, go to [Step 10](#).

Step 10 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 11 Select **MPPDB** from the **Service** drop-down 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 [Technical Support](#) and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.88 ALM-37015 Insufficient File Handles for the GaussDB Process

Alarm Description

This alarm is generated when the available file handles of the OS are insufficient.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37015	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If file handles are insufficient, some instances may fail to be started and the cluster cannot be started properly.

Possible Causes

File handles of the OS are insufficient.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

Step 5 Run the following command to connect to the database:

```
gsq1 -d postgres -p 25308
```

Step 6 Run the following command to check whether the value of **max_files_per_process** is less than the default value **3000**:

```
SHOW max_files_per_process;
```

Information similar to the following is displayed:

```
max_files_per_process
-----
2000
(1 row)
```

- If yes, go to **Step 7**.
- If no, go to **Step 9**.

Step 7 Run the following commands to change the value of **max_files_per_process** to **3000**:

```
\q
```

```
gs_guc set -Z coordinator -Z datanode -N all -I all -c  
'max_files_per_process=3000'
```

Step 8 Run the following commands to restart the cluster:

```
gs_om -t stop
```

```
gs_om -t start
```

Step 9 Check file handles of the OS. Stop the processes that occupy too many file handles but are irrelevant to the database.

 NOTE

You can run the following commands to check the number of file handles set for the OS and that of file handles occupied by each process. In the output of the second command, the numbers of occupied file handles are displayed in the first column, and the PIDs are displayed in the second column. You can stop some unimportant processes that occupy too many file handles.

```
# cat /proc/sys/fs/file-max  
782799
```

```
# lsof -n|awk '{print $2"\t"$1}'|sort|uniq -c|sort -nr|more  
  
131 24204 gaussdb  
57 24244 cleanup  
57 24231 cm_agent
```

Step 10 Wait for a while and check whether the alarm persists.

- If yes, go to [Step 11](#).
- If no, no further action is required.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 12 Select **MPPDB** from the **Service** drop-down 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 [Technical Support](#) and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.89 ALM-37016 Xlog Archive Command Fails to Be Executed on the MPPDBServer

Alarm Description

This alarm is generated when a Coordinator or DataNode instance in the cluster fails to execute the Xlog archive command.

This alarm is automatically cleared when the Xlog archive command is executed successfully.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37016	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

Some Xlogs may not be archived to the archive directory specified in the archive command. The number of Xlog files in the archive directory is increasing, leading to insufficient disk space.

Possible Causes

- The archive command is incorrect.
- The archive directory specified in the archive command does not support data write.
- The archive directory specified in the archive command does not exist.

- The archive directory specified in the archive command is full, and data cannot be written to the directory.

Handling Procedure

Modify the archiving configuration.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **root** or **omm**.

 **NOTE**

- User **root**: The password is specified by users before the installation. Obtain it from the system administrator.
- User **omm**:

Step 4 In the **postgresql.conf** file (for example, **/srv/BigData/mppdb/data1/master1/postgresql.conf**) of the Coordinator or primary DataNode instance, check whether the syntax of **archive_command** is incorrect.

For details about the **archive_command** syntax, see **archive_command** descriptions in **GUC Parameters > Write Ahead Logs > Archiving** in the *Developer Guide*.

- If yes, go to [Step 5](#).
- If no, go to [Step 6](#).

Step 5 Correct the syntax, wait 5 minutes, and check whether the alarm recurs.

- If yes, go to [Step 6](#).
- If no, no further action is required.

Step 6 Check whether the archive directory specified in the archive command does not exist, does not allow data write, or does not have sufficient space.

- If yes, go to [Step 7](#).
- If no, go to [Step 8](#).

Step 7 Rectify the fault based on the check result and ensure that data can be written into the specified archive directory. Wait 5 minutes and check whether the alarm recurs.

- 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 Select **MPPDB** from the **Service** drop-down list.

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

2.3.90 ALM-37017 Number of Database Connections Exceeds the Upper Limit

Alarm Description

This alarm is generated when the number of connections to a database on a Coordinator instance in the cluster exceeds the upper limit.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37017	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.
	databaseName	Specifies the name of the database to connect to.

Impact on the System

Common users cannot access the database on the Coordinator instance.

Possible Causes

The number of connections to the current database on the Coordinator instance exceeds the upper limit.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Access the Coordinator instance for which the alarm is generated as a database administrator who has the rights to create other database users, for example, **omm**. An example is as follows:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

```
gsql -d postgres -p 25308
```

Step 4 Check the upper limits of connections to all databases on the current Coordinator instance. The number of connections to database **abc** on the Coordinator instance is limited to **3**.

```
select * from pg_database;
```

datname	datdba	encoding	datcollate	datatype	datistemplate	datallowconn	datconnlimit	datacl
template1	10	0 C	C	t	t	-1	13506	1336
1663 {=c/xijie_trunk,xijie_trunk=CTc/xijie_trunk}								
template0	10	0 C	C	t	f	-1	13506	1335
1663 {=c/xijie_trunk,xijie_trunk=CTc/xijie_trunk}								
postgres	10	0 C	C	f	t	-1	13506	1337
1663								
abc	10	0 C	C	f	t	3	13506	1336
1663								

(4 rows)

Step 5 Close some connections or increase the maximum number of connections to the database.

- To close a connection, run the following command:

```
\q
```

- To increase the maximum number of connections, run the following command:

```
ALTER DATABASE dbname WITH connection limit 100;
```

Replace **dbname** with the actual database name, for example:

```
ALTER DATABASE abc WITH connection limit 100;
```

```
UPDATE 1
```

```
select * from pg_database;
```

datname	datdba	encoding	datcollate	datatype	datistemplate	datallowconn	datconnlimit	datacl
template1	10	0 C	C	t	t	-1	13506	1336
1663 {=c/xijie_trunk,xijie_trunk=CTc/xijie_trunk}								
template0	10	0 C	C	t	f	-1	13506	1335
1663 {=c/xijie_trunk,xijie_trunk=CTc/xijie_trunk}								
postgres	10	0 C	C	f	t	-1	13506	1337
1663								
abc	10	0 C	C	f	t	9	13506	1336
1663								

(4 rows)

Step 6 Connect to database **abc** and check whether the alarm persists.

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

Collect fault information.

- Step 7** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.
- Step 8** Select **MPPDB** 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 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

2.3.91 ALM-37018 User Is Connected to Excessive Databases

Alarm Description

This alarm is generated when the number of connections of a user on a Coordinator instance in the cluster exceeds the upper limit.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37018	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Type	Parameter	Description
	databaseName	Specifies the name of the database to connect to.

Impact on the System

The Coordinator instance cannot be accessed by this user.

Possible Causes

The number of connections of the database user to the current Coordinator instance exceeds the upper limit.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
 3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
 4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.
- Step 3** Access the Coordinator instance for which the alarm is generated as a database administrator who has the rights to create other database users, for example, **omm**. An example is as follows:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile
```

```
gsql -d postgres -p 25308
```

- Step 4** Check the upper limits of connections of all users on the current Coordinator instance. The number of connections of user **gaussdba** on the Coordinator instance is limited to **3**.

```
select * from pg_authid;  
rolname | rolsuper | rolinherit | rolcreaterole | rolcreatedb | rolcatupdate | rolcanlogin | rolreplication |  
rolauditadmin | rolsystemadmin | rolconnlimit |
```

```
rolpassword | rolvaliduntil
-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
+-----+
gaussdba | t | t | t | t | t | t | t | t | t | t
| 3 | sha2567cee5d311c1e21e84671a2f2e1d8023f1990b4fa7c5656e44277acd3087e2c7fc74
224dbb26375c88c91c9007af78fb1e5212656ec482957bf8fe8ce383b0f59d3ae6152aa0009ee46271d0446eb8c
d0d0e461b09c17f93449c14d4c75238b3d |
(1 row)
```

Step 5 Close some connections or increase the maximum number of connections to the database.

- To close a connection, run the following command:

```
\q
```

- To increase the maximum number of connections, run the following command:

```
alter role gaussdba CONNECTION LIMIT 9;
```

```
ALTER ROLE
```

```
select * from pg_authid;
```

```
rolname | rolsuper | rolinherit | rolcreaterole | rolcreatedb | rolcatupdate | rolcanlogin | rolreplication |
rolauditadmin | rolesystemadmin | rolconnlimit |
```

```
rolpassword |
```

```
rolvaliduntil
-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+
+-----+
gaussdba | t | t | t | t | t | t | t | t | t | t
| 9 | sha2567cee5d311c1e21e84671a2f2e1d8023f1990b4fa7c5656e44277acd3087e2c7fc74
224dbb26375c88c91c9007af78fb1e5212656ec482957bf8fe8ce383b0f59d3ae6152aa0009ee46271d0446
eb8cd0d0e461b09c17f93449c14d4c75238b3d |
(1 row)
```

Step 6 Connect to the database as user **gaussdba** and check whether the alarm persists.

- If yes, go to [Step 7](#).
- If no, no further action is required.

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 8 Select **MPPDB** 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 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

2.3.92 ALM-37019 Connection Between MPPDBServer Data Instances and GTM Is Abnormal

Alarm Description

This alarm is generated in either of the following scenarios:

- A GTM instance is faulty.
- The network of the server where the primary GTM instance is deployed is faulty.
- In synchronization mode, the network of the servers where primary and standby GTM instances are deployed is faulty.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37019	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

Before restoration of the primary GTM instance, the system remains unavailable for 120 seconds.

System Actions

- If the primary GTM instance is faulty for more than 120 seconds, the cluster will promote the standby GTM instance to primary and the system recovers.
- In synchronization mode, if the network of primary and standby GTM instances is faulty, the cluster sets the primary GTM instance to the HA mode 120 seconds later and the system recovers.

Possible Causes

- A GTM instance is faulty.
- The network of the server where the primary GTM instance is deployed is faulty.
- In synchronization mode, the network of the servers where primary and standby GTM instances are deployed is faulty.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location**.

Step 3 Choose **Cluster**, click the name of the cluster for which the alarm is generated, choose **Services > MPPDB > Instance**, and obtain the nodes where MPPDB is installed.

Step 4 Log in to any node where MPPDB is installed as user **omm**, run the **source** command to refresh environment variables, and run the **gs_om -t status --detail** command to check the cluster status (assume that the cluster installation directory is **/opt/huawei/Bigdata**).

```
source /opt/huawei/Bigdata/mppdb/.mppdbgs_profile
```

```
gs_om -t status --detail
```

In the command output, the instance whose state is **P** is the primary GTM instance.

[GTM State]					
node	node_ip	instance	state	sync_state	
2	SZX1000071374	10.90.57.222 1001	/opt/huawei/Bigdata/mppdb/gtm	P Primary	Connection ok Sync
1	SZX1000071373	10.90.57.221 1002	/opt/huawei/Bigdata/mppdb/gtm	S Standby	Connection ok Sync

- Step 5** Check whether the primary GTM instance is faulty. Log in to the node where the primary GTM instance is located as user **omm** and run the following commands to check whether the instance is normal:

```
source /opt/huawei/Bigdata/mppdb/.mppdbgs_profile  
gtm_ctl query -D /opt/huawei/Bigdata/mppdb/gtm
```

Assume that the data directory of the primary GTM instance is **/opt/huawei/Bigdata/mppdb/gtm**.

```
HA state:  
    server_mode      : Primary  
    connection_state : Connection ok  
    global_transaction_id : 16471  
    sync_mode        : Sync on  
Sync state:  
    message_send_count : 0  
    message_receive_count : 0
```

- If the query result is inconsistent with the preceding information, the primary GTM instance is faulty. Locate the cause by analyzing logs of the instance and other monitored instances. Then go to **Step 6**.
- If the query result shows that the connection to the standby instance fails, check the network connectivity and rectify the network faults in a timely manner. Then 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** Select **MPPDB** 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 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

2.3.93 ALM-37020 MPPDBServer Connection Authentication Is Abnormal

Alarm Description

This alarm is generated when a user remotely accesses a Coordinator or DataNode instance in the cluster in TRUST mode.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37020	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

TRUST authentication is not allowed for remote access to a data instance, and users cannot remotely access a Coordinator or DataNode instance in TRUST authentication mode.

Possible Causes

The authentication mode for remote access to a Coordinator or DataNode instance is incorrect.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Check whether remote access is configured with TRUST authentication in the **pg_hba.conf** file under the data directory of the instance for which the alarm is generated. If yes, change the authentication mode to non-TRUST. (Assume that the data directory of the instance is **/srv/BigData/mppdb/data1/coordinator/**. If **10.90.57.224** is the client IP address, change the authentication mode to **sha256**.)

 **NOTE**

Nodes within a cluster use the TRUST authentication mode, but nodes outside the cluster should use SHA256 authentication.

vim /srv/BigData/mppdb/data1/coordinator/pg_hba.conf

```
host all all 10.90.57.221/32 trust
host all all 10.90.57.222/32 trust
host all all 10.90.57.223/32 trust
host all all 10.90.57.224/32 sha256
```

Step 5 Set up the connection again and check whether the alarm persists.

- 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 Select **MPPDB** 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 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

2.3.94 ALM-37021 CM_SERVER Process Is Abnormal

Alarm Description

This alarm is generated in either of the following scenarios:

- The **cm.conf** configuration file does not exist in the CM_SERVER process.
- The CM_SERVER process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37021	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If the CM_SERVER process fails to start, the cluster displays a startup failure message. The database system functions properly if no other exception occurs.

However, users or the administrator cannot obtain accurate information about the cluster status.

Possible Causes

- The **cm.conf** file of the CM_SERVER process does not exist in the **cm_agent** data directory.
- The CM_SERVER process does not have the read or write permission on its data directory.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Assume that the data directory of the instance is **/opt/huawei/Bigdata/mppdb/cm/cm_server**. Check whether **cm.conf** exists in the **/opt/huawei/Bigdata/mppdb/cm/cm_agent** directory. If it does not, replace the instance. For details, see "Rectifying an MPPDBServer Instance" in the **HUAWEI CLOUD Stack x.x.x Data Warehouse Service (DWS) Fault Management (Physical Machine Clusters)**.

Step 5 Check whether the database administrator has the permission to access the **/opt/huawei/Bigdata/mppdb/cm/cm_server** and **/opt/huawei/Bigdata/mppdb/cm/cm_agent** data directories of the instance. If not, run the **chmod** command to change the permission.

Step 6 Wait 5 minutes and check whether the alarm persists.

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

Collect fault information.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 8 Select **MPPDB** 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 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

2.3.95 ALM-37022 CM_AGENT Process Is Abnormal

Alarm Description

This alarm is generated in either of the following scenarios:

- The **cm.conf** configuration file does not exist in the CM_AGENT process.
- The CM_AGENT process does not have the read or write permission on its data directory.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37022	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If the CM_AGENT process fails to start, the cluster displays a startup failure message. The database system functions properly if no other exception occurs. However, users or the administrator cannot obtain accurate information about the cluster status.

Possible Causes

- The **cm.conf** configuration file does not exist in the CM_AGENT process.
- The CM_AGENT process does not have the read or write permission on its data directory.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).



The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click **▼** in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Assume that the data directory of the instance is **/opt/huawei/Bigdata/mppdb/cm/cm_agent**. Check whether **cm.conf** exists in this directory. If it does not, replace the instance using **gs_replace**. For details, see "Rectifying an

MPPDBServer Instance" in the *HUAWEI CLOUD Stack x.x.x Data Warehouse Service (DWS) Fault Management (Physical Machine Clusters)*.

- Step 5** Check whether the database administrator has the permission to access the `/opt/huawei/Bigdata/mppdb/cm/cm_agent` data directory of the instance. If not, run the `chmod` command to change the permission.
- Step 6** Wait 5 minutes and check whether the alarm persists.
- If yes, go to **Step 7**.
 - If no, no further action is required.
- Collect fault information.
- Step 7** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.
- Step 8** Select **MPPDB** 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 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

2.3.96 ALM-37024 Clusters Are Unbalanced

Alarm Description

This alarm is generated when the primary/standby relationship of instances in a cluster changes to be different from that during initial installation of the cluster.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37024	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If the alarm is reported, the primary and standby GTMs or DataNodes switch over in the cluster, and the new primary/standby relationship is different from that during initial installation of the cluster. In this case, primary instances in the cluster may be excessively switched over to a node, causing unbalanced cluster loads and deteriorating cluster performance.

Possible Causes

Abnormal primary/standby relationship of DataNodes:

- A primary DataNode is faulty and cannot provide services.
- The primary and standby DataNodes are disconnected.
- The primary and standby DataNodes are manually switched over.

Abnormal primary/standby relationship of the GTM instances:

- The primary GTM instance is faulty and cannot provide services.
- The primary and standby GTM instances are disconnected.
- The primary and standby GTM instances are manually switched over.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** Choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**, and obtain the nodes where MPPDB is installed.
- Step 4** Log in to any MPPDB node as user **omm** and run the **source** command to configure environment variables and the **gs_om -t status --detail** command to check the cluster status. */opt/huawei/Bigdata* indicates the cluster installation directory.

```
source /opt/huawei/Bigdata/mppdb/.mppdbgs_profile
```

```
gs_om -t status --detail
```

- Step 5** If the values of **cluster_state** and **balanced** are **Normal** and **No** respectively, the primary and standby instances are switched over. **P** in **Datanode State** indicates that the initial DataNode state is primary, and **Standby Normal** indicates that the current state of the DataNode is standby. For details about how to complete the restoration, see "Resetting Instance Status" in the [HUAWEI CLOUD Stack 8.1.x Data Warehouse Service \(DWS\) Fault Management \(Physical Machine Clusters\)](#).

```
[ CMServer State ]
```

node	node_ip	instance	state
1	SZX1000071373	10.90.57.221	1 /opt/huawei/Bigdata/mppdb/cm/cm_server P Primary
2	SZX1000071374	10.90.57.222	2 /opt/huawei/Bigdata/mppdb/cm/cm_server Standby

```
[ Cluster State ]
```

```
cluster_state : Normal
redistributing : No
balanced : No
```

```
[ Coordinator State ]
```

node	node_ip	instance	state
1	SZX1000071373	10.90.57.221	5001 /srv/BigData/mppdb/data1/coordinator Normal
2	SZX1000071374	10.90.57.222	5002 /srv/BigData/mppdb/data1/coordinator Normal
3	SZX1000071375	10.90.57.223	5003 /srv/BigData/mppdb/data1/coordinator Normal

```
[ Central Coordinator State ]
```

node	node_ip	instance	state
2	SZX1000071374	10.90.57.222	5002 /srv/BigData/mppdb/data1/coordinator Normal

```
[ GTM State ]
```

node	node_ip	instance	state	sync_state
2	SZX1000071374	10.90.57.222	1001 /opt/huawei/Bigdata/mppdb/gtm P Primary Connection ok Sync	
1	SZX1000071373	10.90.57.221	1002 /opt/huawei/Bigdata/mppdb/gtm S Standby Connection ok Sync	

[Datanode State]		node	node_ip	instance	state	node	node_ip	node	node_ip
instance	state			state	node	node_ip	instance		
<hr/>									
1	SZX1000071373	10.90.57.221	6001	/srv/BigData/mppdb/data1/master1	P	Primary	Normal	2	
SZX1000071374	10.90.57.222	6002	/srv/BigData/mppdb/data1/slave1	S	Standby	Normal	3		
SZX1000071375	10.90.57.223	3002	/srv/BigData/mppdb/data1/dummyslave1	R	Secondary	Normal			
1	SZX1000071373	10.90.57.221	6003	/srv/BigData/mppdb/data2/master2	P	Primary	Normal	3	
SZX1000071375	10.90.57.223	6004	/srv/BigData/mppdb/data2/slave2	S	Standby	Normal	2		
SZX1000071374	10.90.57.222	3003	/srv/BigData/mppdb/data2/dummyslave2	R	Secondary	Normal			
1	SZX1000071373	10.90.57.221	6005	/srv/BigData/mppdb/data3/master3	P	Primary	Normal	2	
SZX1000071374	10.90.57.222	6006	/srv/BigData/mppdb/data3/slave3	S	Standby	Normal	3		
SZX1000071375	10.90.57.223	3004	/srv/BigData/mppdb/data3/dummyslave3	R	Secondary	Normal			
1	SZX1000071373	10.90.57.221	6007	/srv/BigData/mppdb/data4/master4	P	Primary	Normal	3	
SZX1000071375	10.90.57.223	6008	/srv/BigData/mppdb/data4/slave4	S	Standby	Normal	2		
SZX1000071374	10.90.57.222	3005	/srv/BigData/mppdb/data4/dummyslave4	R	Secondary	Normal			
2	SZX1000071374	10.90.57.222	6009	/srv/BigData/mppdb/data1/master1	P	Primary	Normal	3	
SZX1000071375	10.90.57.223	6010	/srv/BigData/mppdb/data1/slave1	S	Standby	Normal	1		
SZX1000071373	10.90.57.221	3006	/srv/BigData/mppdb/data1/dummyslave1	R	Secondary	Normal			
2	SZX1000071374	10.90.57.222	6011	/srv/BigData/mppdb/data2/master2	P	Standby	Normal	1	
SZX1000071373	10.90.57.221	6012	/srv/BigData/mppdb/data2/slave2	S	Standby	Normal	3		
SZX1000071375	10.90.57.223	3007	/srv/BigData/mppdb/data2/dummyslave2	R	Secondary	Normal			
2	SZX1000071374	10.90.57.222	6013	/srv/BigData/mppdb/data3/master3	P	Primary	Normal	3	
SZX1000071375	10.90.57.223	6014	/srv/BigData/mppdb/data3/slave3	S	Standby	Normal	1		
SZX1000071373	10.90.57.221	3008	/srv/BigData/mppdb/data3/dummyslave3	R	Secondary	Normal			
2	SZX1000071374	10.90.57.222	6015	/srv/BigData/mppdb/data4/master4	P	Primary	Normal	1	
SZX1000071373	10.90.57.221	6016	/srv/BigData/mppdb/data4/slave4	S	Standby	Normal	3		
SZX1000071375	10.90.57.223	3009	/srv/BigData/mppdb/data4/dummyslave4	R	Secondary	Normal			
3	SZX1000071375	10.90.57.223	6017	/srv/BigData/mppdb/data1/master1	P	Primary	Normal	1	
SZX1000071373	10.90.57.221	6018	/srv/BigData/mppdb/data1/slave1	S	Standby	Normal	2		
SZX1000071374	10.90.57.222	3010	/srv/BigData/mppdb/data1/dummyslave1	R	Secondary	Normal			
3	SZX1000071375	10.90.57.223	6019	/srv/BigData/mppdb/data2/master2	P	Primary	Normal	2	
SZX1000071374	10.90.57.222	6020	/srv/BigData/mppdb/data2/slave2	S	Standby	Normal	1		
SZX1000071373	10.90.57.221	3011	/srv/BigData/mppdb/data2/dummyslave2	R	Secondary	Normal			
3	SZX1000071375	10.90.57.223	6021	/srv/BigData/mppdb/data3/master3	P	Primary	Normal	1	
SZX1000071373	10.90.57.221	6022	/srv/BigData/mppdb/data3/slave3	S	Standby	Normal	2		
SZX1000071374	10.90.57.222	3012	/srv/BigData/mppdb/data3/dummyslave3	R	Secondary	Normal			
3	SZX1000071375	10.90.57.223	6023	/srv/BigData/mppdb/data4/master4	P	Primary	Normal	2	
SZX1000071374	10.90.57.222	6024	/srv/BigData/mppdb/data4/slave4	S	Standby	Normal	1		
SZX1000071373	10.90.57.221	3013	/srv/BigData/mppdb/data4/dummyslave4	R	Secondary	Normal			

Step 6 If the value of **cluster_state** is **Degraded**, go to [Step 7](#).

[CMServer State]		node	node_ip	instance	state
1	SZX1000071373	10.90.57.221	1	/opt/huawei/Bigdata/mppdb/cm/cm_server	Primary
2	SZX1000071374	10.90.57.222	2	/opt/huawei/Bigdata/mppdb/cm/cm_server	Standby

[Cluster State]

cluster_state : Degraded
redistributing : No
balanced : No

[Coordinator State]

node	node_ip	instance	state
1	SZX1000071373	10.90.57.221	5001 /srv/BigData/mppdb/data1/coordinator
2	SZX1000071374	10.90.57.222	5002 /srv/BigData/mppdb/data1/coordinator
3	SZX1000071375	10.90.57.223	5003 /srv/BigData/mppdb/data1/coordinator

[Central Coordinator State]

node	node_ip	instance	state
------	---------	----------	-------

```
-----
2 SZX1000071374 10.90.57.222 5002 /srv/BigData/mppdb/data1/coordinator Normal

[ GTM State ]
node      node_ip     instance          state      sync_state
-----
2 SZX1000071374 10.90.57.222 1001 /opt/huawei/Bigdata/mppdb/gtm   P Primary Connection ok Sync
1 SZX1000071373 10.90.57.221 1002 /opt/huawei/Bigdata/mppdb/gtm   S Standby Connection ok Sync

[ Datanode State ]
node      node_ip     instance          state      | node      node_ip     node_ip
instance           state           | node      node_ip     instance
state
-----
1 SZX1000071373 10.90.57.221 6001 /srv/BigData/mppdb/data1/master1   P Primary Normal | 2
SZX1000071374 10.90.57.222 6002 /srv/BigData/mppdb/data1/slave1   S Standby Normal | 3
SZX1000071375 10.90.57.223 3002 /srv/BigData/mppdb/data1/dummyslave1   R Secondary Normal
1 SZX1000071373 10.90.57.221 6003 /srv/BigData/mppdb/data2/master2   P Primary Normal | 3
SZX1000071375 10.90.57.223 6004 /srv/BigData/mppdb/data2/slave2   S Standby Normal | 2
SZX1000071374 10.90.57.222 3003 /srv/BigData/mppdb/data2/dummyslave2   R Secondary Normal
1 SZX1000071373 10.90.57.221 6005 /srv/BigData/mppdb/data3/master3   P Primary Normal | 2
SZX1000071374 10.90.57.222 6006 /srv/BigData/mppdb/data3/slave3   S Standby Normal | 3
SZX1000071375 10.90.57.223 3004 /srv/BigData/mppdb/data3/dummyslave3   R Secondary Normal
1 SZX1000071373 10.90.57.221 6007 /srv/BigData/mppdb/data4/master4   P Primary Normal | 3
SZX1000071375 10.90.57.223 6008 /srv/BigData/mppdb/data4/slave4   S Standby Normal | 2
SZX1000071374 10.90.57.222 3005 /srv/BigData/mppdb/data4/dummyslave4   R Secondary Normal
2 SZX1000071374 10.90.57.222 6009 /srv/BigData/mppdb/data1/master1   P Down Disk damaged /
3 SZX1000071375 10.90.57.223 6010 /srv/BigData/mppdb/data1/slave1   S Primary Normal / 1
SZX1000071373 10.90.57.221 3006 /srv/BigData/mppdb/data1/dummyslave1   R Secondary Normal
2 SZX1000071374 10.90.57.222 6011 /srv/BigData/mppdb/data2/master2   P Primary Normal | 1
SZX1000071373 10.90.57.221 6012 /srv/BigData/mppdb/data2/slave2   S Standby Normal | 3
SZX1000071375 10.90.57.223 3007 /srv/BigData/mppdb/data2/dummyslave2   R Secondary Normal
2 SZX1000071374 10.90.57.222 6013 /srv/BigData/mppdb/data3/master3   P Primary Normal | 3
SZX1000071375 10.90.57.223 6014 /srv/BigData/mppdb/data3/slave3   S Standby Normal | 1
SZX1000071373 10.90.57.221 3008 /srv/BigData/mppdb/data3/dummyslave3   R Secondary Normal
2 SZX1000071374 10.90.57.222 6015 /srv/BigData/mppdb/data4/master4   P Primary Normal | 1
SZX1000071373 10.90.57.221 6016 /srv/BigData/mppdb/data4/slave4   S Standby Normal | 3
SZX1000071375 10.90.57.223 3009 /srv/BigData/mppdb/data4/dummyslave4   R Secondary Normal
3 SZX1000071375 10.90.57.223 6017 /srv/BigData/mppdb/data1/master1   P Primary Normal | 1
SZX1000071373 10.90.57.221 6018 /srv/BigData/mppdb/data1/slave1   S Standby Normal | 2
SZX1000071374 10.90.57.222 3010 /srv/BigData/mppdb/data1/dummyslave1   R Secondary Normal
3 SZX1000071375 10.90.57.223 6019 /srv/BigData/mppdb/data2/master2   P Primary Normal | 2
SZX1000071374 10.90.57.222 6020 /srv/BigData/mppdb/data2/slave2   S Standby Normal | 1
SZX1000071373 10.90.57.221 3011 /srv/BigData/mppdb/data2/dummyslave2   R Secondary Normal
3 SZX1000071375 10.90.57.223 6021 /srv/BigData/mppdb/data3/master3   P Primary Normal | 1
SZX1000071373 10.90.57.221 6022 /srv/BigData/mppdb/data3/slave3   S Standby Normal | 2
SZX1000071374 10.90.57.222 3012 /srv/BigData/mppdb/data3/dummyslave3   R Secondary Normal
3 SZX1000071375 10.90.57.223 6023 /srv/BigData/mppdb/data4/master4   P Primary Normal | 2
SZX1000071374 10.90.57.222 6024 /srv/BigData/mppdb/data4/slave4   S Standby Normal | 1
SZX1000071373 10.90.57.221 3013 /srv/BigData/mppdb/data4/dummyslave4   R Secondary Normal
```

- Step 7** In the part in bold and italic in the preceding command output, the primary DataNode **6009** is in the **Down** state and the standby DataNode **6010** is promoted to primary. As a result, the number of primary DataNode increases on node **SZX1000071374**. In this case, you need to run the **gs_replace** command to rectify the faulty DataNode **6009**.

NOTE

The DataNode switchover serves as an example. The handling method is the same for GTM instance switchover.

```
omm@S ZX1000071374:/srv/BigData/mppdb/data2> gs_replace -t config -h SZX1000071374
```

Fixing all the CMAgents instances.

There are [0] CMAgents need to be repaired in cluster.

```
Configuring replacement instances.  
Successfully configured replacement instances.  
Successfully fixed all the CMAgents instances.  
Configuring  
Waiting for promote peer instances.  
.  
Successfully upgraded standby instances.  
Deleting failed CN from pgxc_node.  
No CN needs to be fixed.  
Configuring replacement instances.  
Successfully configured replacement instances.  
Setting the SCTP.  
Successfully set the SCTP.  
Configuration succeeded.
```

Step 8 Run the following commands to start the host where the instance needs to be replaced:

```
omm@SZX1000071374:/srv/BigData/mppdb/data2> gs_replace -t start -h SZX1000071374  
Starting.  
=====  
Successfully started instance process. Waiting to become Normal.  
=====  
.  
=====  
Start succeeded on all nodes.  
Start succeeded.
```

Step 9 Reset the instance status.

```
omm@SZX1000071374:/srv/BigData/mppdb/data2> gs_om -t switch --reset  
Operating: Switch reset.  
cm_ctl: cmserver is rebalancing the cluster automatically.  
....  
cm_ctl: switchover successfully.  
Operation succeeded: Switch reset.
```

Step 10 Wait for a while and check whether the alarm persists.

- If yes, go to **Step 11**.
- If no, no further action is required.

Collect fault information.

Step 11 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 12 Select **MPPDB** from the **Service** drop-down 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 **Technical Support** and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.97 ALM-37026 MTU Values Are Inconsistent

Alarm Description

This alarm is generated when:

The MTU values of the NICs corresponding to the service IP addresses of the nodes in the cluster are inconsistent.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37026	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If MTU values are inconsistent, communication among GaussDB(DWS) nodes is abnormal. The basic functions and O&M operations of the database cluster may fail or time out.

Possible Causes

After the OS is restarted, the MTU value of an instance is set to the default value, which is different from the MTU value of other nodes in the cluster.

Handling Procedure

- Step 1** Log in to the ManageOne alarm platform to obtain the alarm information.
1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
 2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** Choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**, and obtain the nodes where MPPDB is installed.
- Step 4** Log in to any node where MPPDB is installed as user **omm**.

- Step 5** Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

- Step 6** Use **gs_check** to check the MTU value of each node in the cluster and identify the node and the ID of the NIC whose MTU value is inconsistent with that of other nodes.

gs_check -i CheckMTU

You need to enter the username and password of user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Information similar to the following is displayed:

```
Check root password connection successfully
Warning: The MTU value is inconsistent on all node, maybe checking will be slower or hang.
1500: [host0-eth0,host1-eth0]
1000: [host2-eth0]
Distribute the context file to remote hosts successfully
Start to health check for the cluster. Total Items:1 Nodes:3

Checking...          [=====] 1/1
Start to analysis the check result
CheckMTU.....WARNING
The item run on 3 nodes. success: 2 (consistent) warning: 1
The warning[szvphicpra42317] value:
1000
The success[szvphicpra42315,szvphicpra42316] value:
1500

Analysis the check result successfully
Success. All check items run completed. Total:1 Warning:1
For more information please refer to /opt/huawei/Bigdata/mppdb/wisequery/script/inspection/output/
CheckReport_201808173599753199.tar.gz
```

In the preceding example, the MTU value of NIC eth0 of host2 is 1000, which is inconsistent with that of other nodes.

- Step 7** Log in to the node whose MTU value is inconsistent with that of other nodes as user **root** and change the MTU value of the corresponding NIC (for example, **eth0**)

to be the same as the MTU value of other nodes (for example, 1500). The password is specified by users before the installation. Obtain it from the system administrator.

ifconfig eth0 mtu 1500

Step 8 Run the following commands to add the commands in **Step 7** to the automatic startup file:

- SUSE:
cd /etc/init.d
vim boot.local
- Red Hat, CentOS, or EulerOS:
cd /etc/rc.d
vim rc.local

Step 9 Perform **Step 6** again.

- If the MTU values of all nodes are consistent, manually clear the alarm.
- If the MTU values are still inconsistent, contact the system administrator. If the problem persists, contact [Technical Support](#).

----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

2.3.98 ALM-37027 Feature Vector Training Encoding Service Platform Is Unavailable

Alarm Description

This alarm is generated when the feature vector training encoding process deployed on a Coordinator (CN) is abnormal.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37027	Tenant plane alarm	Critical	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If this alarm is generated, the encoding training platform that can convert long features to short features in the cluster is unavailable, and long features cannot be converted to short features in a timely manner. As a result, efficient short feature-based retrieval cannot be used. If you use the service, the retrieval efficiency of feature value matching in the database decreases.

Possible Causes

- The training platform process is not started or is terminated by other programs.
- The instance installation directory is lost.
- The CN where the SimsTrainserver instance is installed is faulty or cannot be found.
- The current database is abnormal and cannot provide data read or write capabilities.

Handling Procedure

Locate the alarm cause.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** On FusionInsight Manager, choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**, and obtain the node where SimsTrainserver is installed.
- Step 4** Log in to the SimsTrainserver node as user **omm** and run the **source** command to configure environment variables and the **gs_om -t status --detail** command to check the cluster status. **/opt/huawei/Bigdata** indicates the cluster installation directory.

```
source /opt/huawei/Bigdata/mppdb/.mppdbgs_profile  
gs_om -t status --detail
```

- Step 5** Check the command output.

- If the value of **cluster_state** is **Normal** or **Degrade**, go to **Step 6** to view the CN state.
- If the value of **cluster_state** is **Unavailable**, the current cluster is abnormal, go to **Step 10**.

```
[ CMServer State ]  
  
node      node_ip     instance          state  
-----  
1 SZX1000071373 10.90.57.221 1  /opt/huawei/Bigdata/mppdb/cm/cm_server    Primary  
2 SZX1000071374 10.90.57.222 2  /opt/huawei/Bigdata/mppdb/cm/cm_server    Standby  
  
[ Cluster State ]  
  
cluster_state : Normal  
redistributing : No  
balanced       : No
```

- Step 6** View the information about **Coordinator State** in the command output in **Step 4**. **/srv/BigData** indicates the cluster data directory.

- If the SimsTrainserver node does not exist in the displayed CN list, add a SimsTrainserver node. For details, see "Common Emergency Faults" in the **HUAWEI CLOUD Stack x.x.x Data Warehouse Service (DWS) Fault Management (Physical Machine Clusters)**. Then go to **Step 7**.
- If the CN where SimsTrainserver is installed is not in the **Normal** state, restore the CN. For details, see "Common Emergency Faults" in the **HUAWEI CLOUD Stack x.x.x Data Warehouse Service (DWS) Fault Management (Physical Machine Clusters)**. Then go to **Step 7**.
- If the CN is in the **Normal** state, go to **Step 7**.

```
[ Coordinator State ]  
  
node      node_ip     instance          state  
-----  
1 SZX1000071373 10.90.57.221 1 /srv/BigData/mppdb/data1/coordinator Normal  
2 SZX1000071374 10.90.57.222 2 /srv/BigData/mppdb/data1/coordinator Normal  
3 SZX1000071375 10.90.57.223 3 /srv/BigData/mppdb/data1/coordinator Normal
```

- Step 7** Go to the MPPDB installation directory and find the **simSearch/TrainServer/bin** directory. In the **simSearch/TrainServer/bin** directory, run the **sh monitor_trainServer.sh status** command.

- If "[monitor_trainServer.sh] process status normal" is displayed, no further action is required.
- If "[monitor_trainServer.sh] process status abnormal" is displayed, go to **Step 8**.

Step 8 Run script **start_trainServer.sh**, go to the MPPDB installation directory, and find the **simSearch/TrainServer/bin** directory. In the **simSearch/TrainServer/bin** directory, run the **sh monitor_trainServer.sh status** command.

- If "[monitor_trainServer.sh] process status normal" is displayed, go to **Step 9**.
- If "[monitor_trainServer.sh] process status abnormal" is displayed, go to **Step 10**.

Step 9 Wait for three minutes and check whether the alarm persists.

- 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 Select **MPPDB** from the **Service** drop-down 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 **Technical Support** and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.99 ALM-37028 NIC Multi-Queue Is Not Configured

Alarm Description

This alarm is generated when:

The NIC corresponding to the service IP address of the current node is not configured, or the NIC has not been bound to different CPU cores.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37028	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If NIC multi-queue is not bound, the database can still be used, but reliability and performance of the database cluster deteriorate.

Possible Causes

The irqbalance service is not stopped. In this case, the irqbalance service dynamically adjusts the interruption binding when load is high, invalidating the binding relationship.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** Choose **Cluster**, click the name of the cluster for which the alarm is generated, choose **Services > MPPDB > Instance**, and obtain the nodes where MPPDB is installed.
- Step 4** Log in to the alarmed node where MPPDB is installed as user **omm**.

- Step 5** Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile
```

- Step 6** Use **gs_check** to check the value bound to the NIC queue in the background and check whether the NIC queue value is unqualified.

Run the **python -V** command on the CLI. If the Python version is earlier than 2.7.0, log in to each node where the alarm is reported and run the **gs_check -i CheckMultiQueue -L** command. Otherwise, run the **gs_check -i CheckMultiQueue** command on any node where the alarm is reported.

You need to enter the username and password of user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Information similar to the following is displayed:

```
Check root password connection successfully
Distribute the context file to remote hosts successfully
Start to health check for the cluster. Total Items:1 Nodes:3

Checking... [=====] 1/1
Start to analysis the check result
CheckMultiQueue.....NG
The item run on 3 nodes. success: 2 ng: 1
The ng[host1] value:
Network card [eth0] multi-queue support is not enabled.

Analysis the check result successfully
Failed. All check items run completed. Total:1 NG:1
For more information please refer to /opt/huawei/Bigdata/mppdb/wisequery/script/gspylib/inspection/
output/CheckReport_20190225363008708.tar.gz
```

In this example, NG is reported for the value bound to the NIC queue on the host1 node, which means that this value is unqualified.

- Step 7** Log in to a node whose NIC queue value is inconsistent with that of other nodes as user **omm**.

- Step 8** Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile
```

Step 9 Run the following commands to change all unqualified values.

Run the **python -V** command on the CLI. If the Python version is earlier than 2.7.0, log in to each node where the alarm is reported and run the **gs_check -i CheckMultiQueue -L --set** command. Otherwise, run the **gs_check -i CheckMultiQueue --set** command on any node whose NIC queue value is inconsistent with that of other nodes.

You need to enter the username and password of user **root**. The password is specified by users before the installation. Obtain it from the system administrator.

Information similar to the following is displayed:

```
Check root password connection successfully
Distribute the context file to remote hosts successfully
Start to health check for the cluster. Total Items:1 Nodes:3

Checking... [=====] 1/1
Start to analysis the check result
CheckMultiQueue.....OK
The item run on 3 nodes. success: 3

Analysis the check result successfully
Success. All check items run completed. Total:1 Success:1
For more information please refer to /opt/huawei/Bigdata/mppdb/wisequery/script/gspylib/inspection/
output/CheckReport_201902253655522339.tar.gz
```

Step 10 Perform [Step 6](#) again.

- If the NIC queue values of all nodes are correct, manually clear the alarm.
- If the values are still unqualified, contact the system administrator. If the fault persists, contact [Technical Support](#).

----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

2.3.100 ALM-37029 MPPDB Service Is Unavailable

Alarm Description

The alarm module checks the MPPDBMonitor service health status every 30 seconds. This alarm is generated when the MPPDBMonitor service is faulty.

This alarm is cleared when MPPDBMonitor becomes healthy.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37029	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

The MPPDBMonitor component cannot provide services externally.

Possible Causes

The MPPDBMonitor service is stopped.

Handling Procedure

Restart the MPPDBMonitor service.

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** Choose **Cluster**, click the name of the cluster for which the alarm is generated, and choose **Services > MPPDBMonitor**.
- Step 4** Click **More** and select **Restart Service**. Restart the MPPDBMonitor service, wait for 5 minutes, and check whether the alarm persists.
- If yes, go to [Step 5](#).
 - If no, no further action is required.

Step 5 Contact [Technical Support](#).

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.101 ALM-37031 CM_AGENT Connecting to the Database Failed

Alarm Description

This alarm is generated when CM_AGENT fails to create persistent connections to monitor the GTM, DN, and CN.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37031	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.

Type	Parameter	Description
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

When CM_AGENT fails to connect to the GTM, DN, or CN process to be monitored and the issue persists for a long time, a primary/standby switchover will occur if the GTMs and DNs are the primary nodes.

Possible Causes

- The GTM, DN, and CN are not started.
- The CN and DN connection pools are full.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the alarm list, check whether alarm ALM-37005, ALM-37006, or ALM-37007 is generated.

- If yes, rectify the fault by the procedure provided for alarm ALM-37005, ALM-37006, or ALM-37007.
- If no, go to **Step 3**.

Step 3 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 4 Select **MPPDB** from the **Service** drop-down list.

Step 5 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 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

2.3.102 ALM-37032 Creating Connections for Database Service Failed

Alarm Description

This alarm is generated when the ALM-37031 alarm is not generated and CM_AGENT fails to connect to GTMs, DNs, and CNs for multiple times.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37032	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The instance will be restarted and a primary/standby CN, DN, or GTM switchover will occur.

Possible Causes

The memory and I/O of the node where the faulty instance resides are used up.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 3 Select **MPPDB** from the **Service** drop-down list.

Step 4 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**.

----End

Step 1 Contact [Technical Support](#) and provide the collected logs.

----End

2.3.103 ALM-37033 DN Disk Is Faulty

Alarm Description

This alarm is generated when the disk used by a DN instance is damaged.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37033	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The database can still be used, but its overall performance will be affected.

System Actions

The DN using the damaged disk will copy data from its backup node to restore data, but the restored data may still be written on the damaged disk page.

Possible Causes

The disk is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the information about the node and instance for which the alarm is generated from the location information area.

Step 3 Replace the disk. For details, see "Hard Disk Troubleshooting" in the [HUAWEI CLOUD Stack 8.1.x Data Warehouse Service \(DWS\) Fault Management \(Cluster Machine Clusters\)](#).

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.104 ALM-37034 Rebuilding DN Failed

Alarm Description

If the primary and standby data is different, the cluster automatically recreates the DN. This alarm is generated when the DN fails to be recreated.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37034	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If the DN fails to be recreated, the DN cannot run properly. As a result, the cluster runs in the faulty mode, deteriorating the performance and decreasing the availability.

Possible Causes

- The hardware is faulty, the disk runs slowly, or the network is disconnected.
- Logs of the primary and standby DNs are inconsistent.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 3 Select **MPPDB** from the **Service** drop-down list.

Step 4 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**.

----End

Step 1 Contact **Technical Support** and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.105 ALM-37035 Cluster Node Is Running Slowly

Alarm Description

This alarm is generated when the number of waiting times of CN/DN instances in a cluster exceeds the preset threshold due to disk, memory, CPU, or network exceptions within a specified period, and the ratio of the number of waiting times of instances to the total number of waiting times in the cluster exceeds the threshold.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37035	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

This alarm indicates that the node is running slowly and will become the performance bottleneck of the cluster.

Possible Causes

- The node disk is faulty.
- The node memory is insufficient.
- The node CPU usage is too high.
- The network connection of the node is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the host name in the **HostName** value of **Location**.

Step 3 Log in to the node for which the alarm is generated as user **omm**.

Step 4 Initialize environment variables.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile
```

Step 5 Isolate the slow node.

In the following command, *HOSTNAME* indicates the host name obtained in [Step 2](#), and *[-l LOGFILE]* indicates the log path. The log path is optional.

```
gs_om -t isolate_stop -h HOSTNAME [-l LOGFILE]
```

Step 6 Contact Huawei engineers to check the disk, memory, CPU, and network of the slow node and restore the node environment accordingly.

Step 7 Restore the slow node.

In the following command, *HOSTNAME* indicates the host name obtained in [Step 2](#), and *[-l LOGFILE]* indicates the log path. The log path is optional.

```
gs_om -t isolate_restore -h HOSTNAME [-l LOGFILE]
```

Step 8 Check whether the alarm persists.

- If yes, go to [Step 9](#).
- If no, no further action is required.

Collecting fault information

Step 9 On FusionInsight Manager, choose **System > Log Download**.

Step 10 Select **MPPDB** from the **Services** drop-down list box and click **OK**.

Step 11 Set **Start Time** for log collection to 1 hour ahead of the alarm generation time and **End Time** to 1 hour after the alarm generation time and 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

2.3.106 ALM-37036 Data Skew Occurs During MPPDBServer Data Import

Alarm Description

This alarm is generated when the data of the target DN is skewed after being imported.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37036	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Table Name	Specifies name of the data skew table for which the alarm is generated.

Impact on the System

If the table is skewed, the disk usage of some DNs may increase sharply. As a result, the disk space is full and cluster functions are affected.

Possible Causes

- Inappropriate distribution key
- Skewed data

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 3 Select **MPPDB** from the **Service** drop-down list.

Step 4 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**.

----End

Step 1 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

2.3.107 ALM-37037 Features Are Not Authorized by the License

Alarm Description

This alarm is generated when the used database features are not authorized by the activated cluster license.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37037	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.
	Feature name	Specifies the name of the feature that triggers the alarm

Impact on the System

Technical support cannot be provided for features beyond the authorization scope of the currently activated license.

Possible Causes

- The license is not activated for the cluster.
- Features in use are beyond the authorization scope of the activated license.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the name of the feature for which the alarm is generated and the corresponding license version from the additional information area. The feature name is also indicated by the **featureName** field in the location information area. For details about the features, see [Table 2-10](#).

Table 2-10 Feature details corresponding to the **featureName** field

Field	Feature	Description	License Version
GPU_Acceleration_In_Multidimensional_Collision_Analysis	Multidimensional collision and analysis (GPU acceleration) NOTE GaussDB(DWS) does not support this feature.	Feature vector retrieval engine	Advanced feature license (Feature computing engine license)
Cross_DC_Collaboration	Cross-DC collaboration	Collaborative analysis between homogeneous clusters across DCs	Advanced license
Row_Level_Security	Row-level security	Row-level security (RLS)	Advanced license
Transparent_Encryption	Transparent data encryption	Transparent Data Encryption (TDE) in clusters	Advanced license
Private_Table	Private table	Private attributes	Advanced license

- Step 3** Determine whether to replace license for the cluster based on the actual service requirements.
- To replace the license, contact [Technical Support](#).
 - If the alarm is triggered by misoperations, manually clear the alarm. If the feature is no longer used, the alarm will not be reported, no further action is required.
 - If no feature beyond the licensed scope is used, this alarm is generated. In this case, go to [Step 1](#).

----End

- Step 1** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

- Step 2** Select **MPPDB** from the **Service** drop-down list.

- Step 3** 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**.

----End

- Step 1** Contact [Technical Support](#) and provide the collected logs.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.108 ALM-37039 Connecting to the KMS Service Failed

Alarm Description

This alarm is generated when transparent encryption is enabled for the current database and the CNs or DNs cannot connect to the KMS server due to network or KMS server faults.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37039	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The cluster where transparent encryption is enabled cannot be started.

Possible Causes

- The KMS server is not started.
- The KMS server address is incorrectly configured.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.

Step 3 On FusionInsight Manager, choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Configurations > All Configurations**. In the navigation pane on the left, choose **MPPDB > Advanced**. Check whether **mppdb_transparent_encryption_url** is correctly set.

- If yes, go to **Step 5**.
- If no, set the parameters based on the site requirements, save the settings, restart the instance, and go to **Step 4**.

Step 4 Choose **O&M > Alarm > Alarm** and check whether the alarm persists.

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

Step 5 Choose **Cluster > KMS cluster name > Service > KMS > Instance**. Check whether the running status of the KMS instance in the value of **mppdb.TransparentEncryptionUrl** in **Step 3** is normal.

- If yes, go to **Step 8**.
- If no, restore the instance and go to **Step 6**.

Step 6 Choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**. Select the instance for which the alarm is generated, and click **More** and choose **Restart** to restart the instance.

Step 7 Choose **O&M > Alarm > Alarm** and check whether the alarm persists.

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

Step 8 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 9 Select **MPPDB** from the **Service** drop-down list.

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

2.3.109 ALM-37040 TDE Key File Is Damaged

Alarm Description

Transparent encryption is enabled for the current database, and the TDE key file used by the database is damaged.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37040	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The database cannot be started.

Possible Causes

- The key file is deleted by mistake.
- The key file is modified.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarms**. In the alarm list, click  in the row where the alarm is located. Obtain the cluster, host, and instance names from **Location Information**.

Step 3 Use PuTTY to log in to the node for which the alarm is generated as user **omm** and run the following commands to check whether file **gs_tde_keys.cipher** exists:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgbs_profile
```

```
cd $GAUSSHOME/bin/
```

```
ls -l
```

- If yes, go to [Step 7](#).
- If no, go to [Step 4](#).

Step 4 Use PuTTY to log in to other MPPDB instance nodes where the **gs_tde_keys.cipher** file is not damaged as user **omm** and run **source \${BIGDATA_HOME}/mppdb/.mppdbgbs_profile** to initialize environment variables, run the **scp** command to copy **\$GAUSSHOME/bin/gs_tde_keys.cipher** to the **\$GAUSSHOME/bin/** directory on the node for which the alarm is generated, and modify the permission of the **gs_tde_keys.cipher** file to 600.

Step 5 On FusionInsight Manager, choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**. Select the instance for which the alarm is generated and choose **More > Restart** to restart the instance.

Step 6 Choose **O&M > Alarm > Alarm** and check whether the alarm persists.

- If yes, go to [Step 7](#).
- If no, no further action is required.

Step 7 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 8 Select **MPPDB** from the **Services** drop-down list box 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

2.3.110 ALM-37041 TDE Key Verification Error Occurs

Alarm Description

The database in use uses the transparent encryption feature, and the key obtained from the KMS server is incorrect.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37041	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

The cluster cannot be started.

Possible Causes

The KMS service is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.

3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 3 Select **MPPDB** from the **Services** drop-down list box and click **OK**.

Step 4 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 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

2.3.111 ALM-37042 MPPDB Client Version Does Not Match the Kernel Version

Alarm Description

GaussDB(DWS) provides the client management feature to centrally manage information about clients connected to the MPPDB cluster and manage alarm notifications. This alarm is generated when the system detects that the client version is inconsistent with the kernel version.

 **NOTE**

If the application name, installation path, and driver type are configured or modified on the upgraded client, a new record is generated on the client management page of the upgraded client. The record of the earlier version is not overwritten, and the system continuously reports alarm ALM-37042. The historical records of the client are automatically deleted when the scheduled deletion task is executed. By default, a schedule deletion task deletes records in the previous 3 months.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37042	Tenant plane alarm	Warning	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If this alarm is generated, the version of the client connected with the MPPDB cluster is inconsistent with the kernel version. As a result, the cluster may be unavailable.

Possible Causes

After the MPPDB kernel is upgraded, the client driver is not upgraded.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 Go to the dashboard page, select *Name of the desired cluster*. On the page that is displayed, click **More** and choose **Download Client**. Select the corresponding client type, and set the save path.

Step 3 Choose **Cluster > Name of the desired cluster > Client**, query the information about the client whose version does not match the kernel version, and upgrade the client based on the query result (client IP address and client driver type).

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.112 ALM-37043 GaussDB AD Users Conflict with Each Other Or Are Invalid

Alarm Description

This alarm is generated when a database user with the same name as a third-party AD user (conflicting user) exists in the GaussDB(DWS) cluster, or a deleted third-party AD user is not cleared from the database (invalid user).

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37043	Tenant plane alarm	Minor	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.

Type	Parameter	Description
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Database users may perform unauthorized operations.

Possible Causes

If an AD user with the same name as an existing database user is created in the GaussDB(DWS) cluster during batch creation of AD users, the AD user conflicts with the database user; If an AD user that is successfully created in the GaussDB(DWS) cluster is deleted on the AD server but not deleted from the GaussDB(DWS) cluster, the user becomes an invalid user.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 Choose **Cluster > Name of the desired cluster > Service > MPPDB > Database User > AD Domain User**. In the search box, view all conflicting or invalid users. For conflicting users, determine whether to delete them from the AD or database based on service requirements. For invalid users, determine whether to delete them from the database based on service requirements.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.113 ALM-37044 GaussDB Failed to Connect to the AD Service

Alarm Description

This alarm is generated when connection to the third-party AD service fails.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37044	Tenant plane alarm	Minor	Operation alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

Users cannot be synchronized from the third-party AD service. AD users created in the GaussDB(DWS) cluster cannot be authenticated by the AD service.

Possible Causes

The third-party AD service is faulty.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.

2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 Check the AD service IP address in the additional alarm information and contact the AD service administrator to rectify the fault.

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.114 ALM-37045 GRPC Certificate File Does Not Exist

Alarm Description

This alarm is generated when the certificate is lost or the GAUSSHOME environment variable is incorrectly configured and the certificate cannot be accessed after the remote read function is enabled (`remote_read_mode = authentication`) in the primary/standby/secondary deployment.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37045	Tenant plane alarm	Major	Security	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

If this alarm is generated, the remote read authentication is enabled, but the server certificate path is incorrect or the file does not exist during cluster startup. As a result, the primary or standby DN on the node cannot be started. After the cluster is started, the client certificate path is incorrect or the file does not exist. As a result, the remote read function cannot work properly.

Possible Causes

The certificate file is lost.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the alarm list, click

-  in the row that contains the alarm. Obtain the cluster, host, and instance names from **Location Information**.

Step 3 Check whether the encryption authentication of the remote read function needs to be enabled.

- If no, go to **Step 4**. No further action is required.
- If yes, go to **Step 5**.

Step 4 Use PuTTY to log in to any MPPDB node as user **omm** and perform the following steps to disable the authentication function (the cluster needs to be restarted):

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile  
gs_guc set -Z coordinator -Z datanode -N all -I all -c  
"remote_read_mode=non_authentication"  
  
cm_ctl stop; cm_ctl start
```

Step 5 Use PuTTY to log in to the node for which the alarm is generated as user **omm** and run the following command to check whether all the five certificate files exist:

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile  
cd $GAUSSHOME/share/sslcert/grpc/  
  
ls -l
```

If no, go to **Step 6**.

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

Step 6 Use PuTTY to log in to the MPPDB instance node where the certificates are not damaged as user **omm**, run the **source \${BIGDATA_HOME}/mppdb/.mppdbgs_profile** command to initialize environment variables, run the **scp** command to copy the missing files to the **\$GAUSSHOME/share/sslcert/grpc/** directory on the node where this alarm is generated, and change the permissions of all files to 600.

Step 7 On FusionInsight Manager, choose **Cluster > Name of the cluster for which the alarm is generated > Service > MPPDB > Instance**. Select the instance for which the alarm is generated and choose **More > Restart** to restart the instance.

Step 8 Choose **O&M > Alarm > Alarm** and check whether the alarm persists.

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

Step 9 On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

Step 10 Select **MPPDB** from the **Services** drop-down list box and click **OK**.

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

2.3.115 ALM-37046 THP Is Running

Alarm Description

This alarm is generated when the THP service is enabled on a cluster node.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37046	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

Transparent Huge Pages (THP) defragments system memory, but it is unnecessary for large memory with the **hugepage** configured, because THP occupies a large amount of CPU resources, affecting database performance.

Possible Causes

The THP service is running.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the alarm list, click  in the row that contains the alarm. Obtain the cluster, host, and instance names from **Location Information**.

Step 3 Use PuTTY to log in to the node for which the alarm is generated as user **root**, and run the following command to add **never** to the THP file and disable the THP service:

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

Step 4 Run the following command to disable the THP service and write the disabling command to the **initFile**:

```
sed -i '/.*transparent_hugepage.*enabled.*echo never.*$/d' initFile && echo "echo never > /sys/kernel/mm/transparent_hugepage/enabled" >> initFile
```

The path of the **initFile** file varies depending on the operating system. Replace the path as follows:

- The path in SUSE OS: **/etc/init.d/boot.local**
- The path in Red Hat/CentOS/Euler OSs: **/etc/rc.d/rc.local**

----End

Alarm Clearance

This alarm is automatically cleared after the fault is rectified.

Related Information

None

2.3.116 ALM-37047 DN Log Redo Operations Are Slow

Alarm Description

This alarm is generated when the difference between the logs after a redo operation and the logs received exceeds the threshold (4 GB). Xlog redo operations are executed slowly due to improper services or disk, memory, or CPU faults of a standby DN in the cluster.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
37047	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.
	Instance	Specifies the instance for which the alarm is generated.

Impact on the System

When this alarm is generated, the redo log completion rate of the standby node is greatly different from that of the primary node. Although the current service is not affected, the alarm is potentially a major risk that affects the reliability of the cluster system. Therefore, the alarm must be handled as soon as possible. If the primary DN is abnormal and the standby DN needs to be promoted to primary, it may take a long time for the standby DN to complete the redo operation. The cluster will be unavailable for a long time.

Possible Causes

- The standby node is not running for a long time.
- Special DDL operations are performed.

- The node disk is faulty.
- The node memory is insufficient.
- The node CPU usage is too high.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.
4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

NOTE

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

Step 2 Use PuTTY to log in to the node for which the alarm is generated as user **omm**, run the **gs_ctl query** command to check the difference between **receiver_replay_location** and **receiver_flush_location** of the xlog redo operation of the standby DN.

```
source ${BIGDATA_HOME}/mppdb/.mppdbgs_profile  
gs_ctl query -D /instance path
```

Information similar to the following is displayed:

```
Receiver info:  
receiver_pid : 24907  
local_role : Standby  
peer_role : Primary  
peer_state : Normal  
state : Streaming  
sender_sent_location : 1/70B93F0  
sender_write_location : 1/70B93F0  
sender_flush_location : 1/70B93F0  
sender_replay_location : 1/70B93F0  
receiver_received_location : 1/70B93F0  
receiver_write_location : 1/70B93F0  
receiver_flush_location : 1/70B93F0  
receiver_replay_location : 0/50AA003  
sync_percent : 2%
```

Step 3 Check the startup time of the standby DN. Check whether the standby DN is not running for a long time and whether alarm ALM-37004 is generated.

- If yes, because xlogs are not synchronized between the primary and standby nodes for a long time, synchronization cannot be complete within a short period of time. In this case, evaluate the actual service status, temporarily reduce service access, and reduce the generation speed of xlogs. Then check whether the difference between **receiver_replay_location** and **receiver_flush_location** is narrowed. After the alarm is cleared, restore the

jobs. Pay attention to the cluster monitoring status so that each node in the cluster can be restored to the normal status in a timely manner.

- If no, go to [Step 4](#).

- Step 4** Find the redo log file based on **receiver_replay_location**, use the pg_xlogdump tool to parse and view the operations in the redo logs, and check whether a large number of DDL operations, such as **CREATE**, **DROP**, **TRUNCATE**, and **REINDEX**, are performed on database objects such as tables.
- If yes, evaluate the actual service status and adjust the services. If necessary, suspend the services to prevent DDL operations that take a long time to redo in batch processing jobs. On GaussDB(DWS), perform DDL operations (such as creating tables) in a unified manner and prevent DDL operations in batch processing jobs so that performance is not affected. Then check whether the difference between **receiver_replay_location** and **receiver_flush_location** is narrowed.
 - If no, go to [Step 5](#).

- Step 5** Contact the system administrator to check whether the node disk, memory, or CPU are faulty, or whether the resources are about to be used up.

NOTE

If the node hardware is faulty, rectify the fault by following the instructions provided in "Emergency Handling > Common Emergency Faults > Replacing a Faulty Node" in Data Warehouse Service (DWS) 8.1.3.331 Fault Management (for Huawei Cloud Stack 8.3.1).

- If yes, repair or replace the hardware components.
- If no, go to [Step 6](#).

- Step 6** Check whether the alarm persists.

- If yes, go to [Step 7](#).
- If no, no further action is required.

Collect fault information.

- Step 7** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.

- Step 8** Select **MPPDB** 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 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 when the difference between the redo logs and the received logs decreases from more than 4 GB to less than 2 GB.

Related Information

None

2.3.117 ALM-45170 DMSCollector Instance Is Abnormal

Alarm Description

This alarm is generated when DMSCollector is managed in a cluster and the DMSAgent process does not exist.

Alarm Attributes

Alarm ID	Alarm Category	Alarm Severity	Alarm Type	Service Type	Auto Cleared
45170	Tenant plane alarm	Major	QoS alarm	FusionInsight Manager	Yes

Alarm Parameters

Type	Parameter	Description
Location Info	ClusterName	Cluster or system for which the alarm is generated.
	ServiceName	Service for which the alarm is generated.
	RoleName	Role for which the alarm is generated.
Other Information	HostName	Specifies the name of the host for which the alarm is generated.

Impact on the System

If data reporting for DMSCollector managed in the cluster is abnormal, the cluster overview data on HCS may be abnormal.

Possible Causes

The DMSAgent process does not exist. As a result, the DMSCollector instance managed in the cluster is abnormal.

Handling Procedure

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

1. Log in to ManageOne Maintenance Portal and choose **Monitor > Alarms > Current Alarms**.
2. Click **Filter** in the upper left corner and click **Other Information**. The **Other Information** dialog box is displayed.
3. Set **Operator** to **contains** and **Value** to **CloudService=DWS**, and click **OK**. Click **OK** again to filter DWS alarms.

4. Click the alarm name to view the alarm details. In **Location Info** and **Other Information**, you can obtain the cluster ID, node ID, and cluster name (varying depending on the alarm).

 **NOTE**

The displayed information varies depending on the alarm. You may obtain the resource ID, instance name, and instance ID of the cluster from **Location Info** and **Other Information**.

- Step 2** On FusionInsight Manager, choose **O&M > Alarm > Alarm**. In the alarm list, click  in the row that contains the alarm. Obtain the cluster, host, and instance names from **Location Information**.
- Step 3** Log in to the server where the DMSCollector instance is abnormal as user **omm**.
- Step 4** Run the following command to check whether the DMSAgent process *agent_service.py* exists. If the process does not exist, go to **Step 5**.
- ```
ps -ef | grep "agent_service.py" | grep -v grep
```
- Step 5** On FusionInsight Manager, choose **O&M**. In the navigation pane on the left, choose **Log > Download**.
- Step 6** Select **DMSCollector** 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 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

### 2.3.118 Technical Support

Huawei Technologies Co., Ltd. provides customers with all-round technical support and services. If you encounter any problem during product use or maintenance, obtain information that can help you locate or solve your problem from the following channels:

- Cloud Computing & Big Data Information Service Platform: <http://support-it.huawei.com/cloud/#/home?lang=en>
- Intelligent Q&A robot: <https://support.huawei.com/iknow/?lang=en>
- Community: <http://forum.huawei.com/enterprise/en/forum.html>

If the problem persists, you can contact our local Huawei representative office or the company's headquarters.

- Call the service hotline of the local Huawei office.
- Visit the Huawei support website and provide feedback on the **Contact Us** page.
  - Enterprises: Visit <http://support.huawei.com/enterprise>.
  - Carriers: Visit <http://support.huawei.com>.

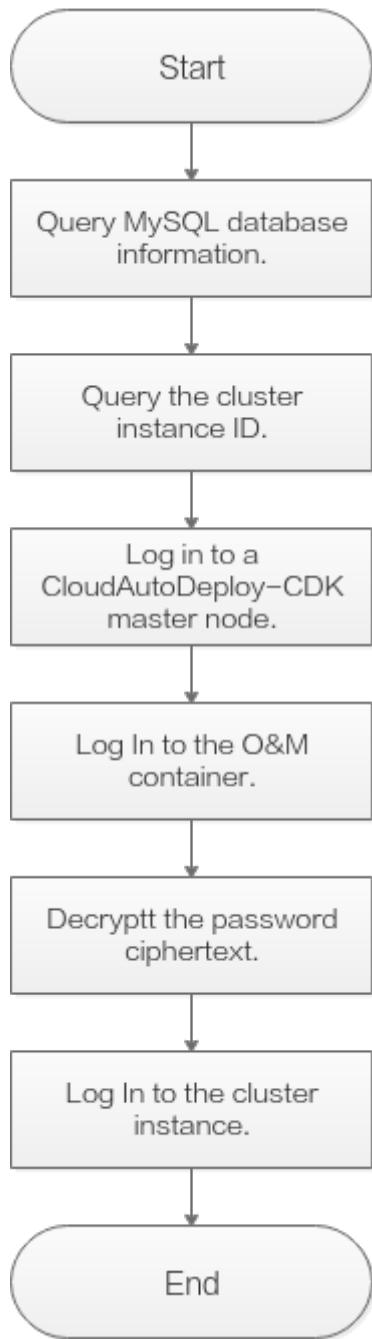
# 3 Appendixes

---

## 3.1 Logging In to a Node in the Tenant Cluster

This section describes how to use O&M pods to log in to cluster nodes for troubleshooting on the tenant side. The following figure shows the login process.

**Figure 3-1** Login process



## Querying MySQL Database Information

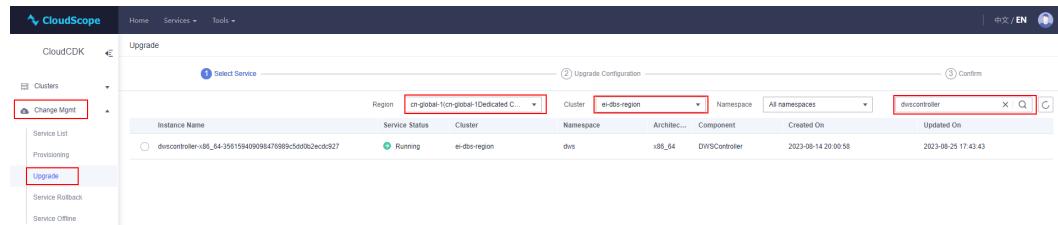
**Step 1** Log in to CloudScope using a browser as a system administrator.

- URL: [https://Address\\_for\\_accessing\\_CloudScope](https://Address_for_accessing_CloudScope), for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op\_cdk\_sso**

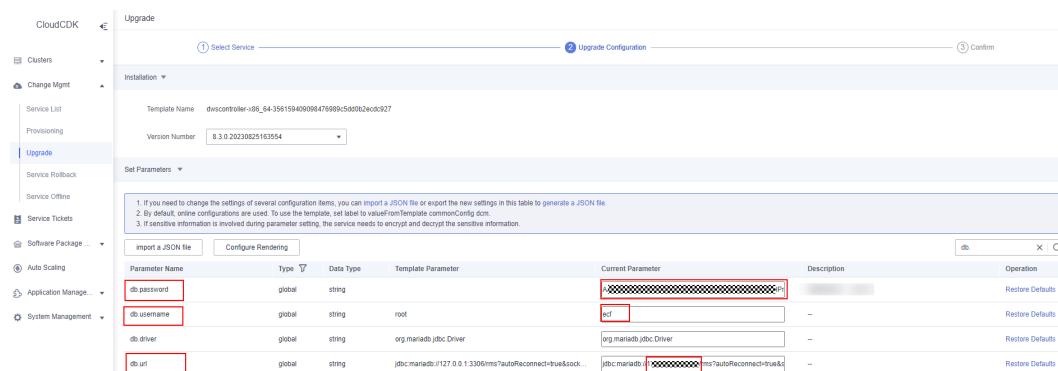
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

**Step 2** Choose **Services > Change Mgmt > CloudAutoDeploy-CDK**.

**Step 3** In the navigation pane on the left, choose **Change Magmt & > Upgrade**, select the corresponding region, and select the cluster **ei-dbs-region**. Search for **dwscontroller** in the search box, select the corresponding dwscontroller, and click **Next**.



**Step 4** Enter the keyword **db.** in the search box on the right and record the password ciphertext corresponding to **db.password**, username corresponding to **db.username**, and database IP address and port number corresponding to **db.url**.



**Step 5** After the recording is complete, click **Home** in the upper left corner to exit the current page to prevent misoperations.

----End

## Querying the Cluster Instance ID

**Step 1** Log in to CloudScope using a browser as a system administrator.

- URL: [https://Address\\_for\\_accessing\\_CloudScope](https://Address_for_accessing_CloudScope), for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op\_cdk\_sso**
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

- Step 2** In the **Common Links** area, click **Service CM**. Select your region and then access the **Service CM** page.
- Step 3** Choose **Service List > Data Warehouse Service** to switch to the corresponding namespace.
- Step 4** Choose **Sre OM Management > Clusters** on the left, click the cluster name to go to the node list page, and record the ID of a CN whose name contains **cn**.

| Node ID                               | Node Name                                         | Node Status | Recent Task Status | Latest Task Time |
|---------------------------------------|---------------------------------------------------|-------------|--------------------|------------------|
| oce3249a-979f-496d-a20b-8fffa3e23c4   | auto-default--ypr@G8Z9NrgzPQJc1O2LR1MIVS-dws-c... | Normal      | --                 | --               |
| 45890065-2042-45f7-8572-5839000c3271  | auto-default--ypr@G8Z9NrgzPQJc1O2LR1MIVS-dws-c... | Normal      | --                 | --               |
| 5602290e2-2960-4833-89a1-254968526106 | auto-default--ypr@G8Z9NrgzPQJc1O2LR1MIVS-dws-d... | Normal      | --                 | --               |

----End

## Logging In to the CloudAutoDeploy-CDK Master Node

- Step 1** Log in to ManageOne Maintenance Portal via <https://ManageOne Maintenance Portal URL:31943>. Alternatively, log in to the unified portal and choose **OperationCenter**.

- Password login: Enter the username and password of the account.
  - Default account: **bss\_admin**

### NOTE

For ManageOne upgraded from 8.2.0 or earlier, the default username is **admin**.  
For ManageOne 8.2.1 or later, the default username is **bss\_admin**.

- Preset password: See the preset password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in **Huawei Cloud Stack 8.3.1 Account List**.
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter the PIN.

Log in to ManageOne Maintenance Portal.

- Step 2** In the **Cloud O&M Management** navigation pane, click **Service\_OM**. The Service OM page is displayed.

- Step 3** On the Service OM console page, click **VM**.

- Step 4** Query the IP address of the CloudAutoDeploy-CDK node. In the search box in the upper right corner, enter the keyword **EICCommon-Region-Master** to search for VMs. Generally, three VMs are available. You can record the IP address of any one of them.

- Step 5** Log in to the CloudAutoDeploy-CDK master node as user **opsadmin** using a remote login tool, and then switch to user **root**. The IP address is obtained in **Step 4**.

**su - root**

- Default password of user **opsadmin**: Search for **EICommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).
- Default password of user **root**: Search for **EICommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

----End

## Logging In to the O&M Container

**Step 1** Run the following command on the CloudAutoDeploy-CDK master node to query the O&M pod names:

**kubectl get pod -n ecf**

Information similar to the following is displayed. Find the pod whose name starts with **dwsmaintaintool**. Any pod whose **STATUS** is **Running** can be used as an O&M pod.

| NAME                                    | READY | STATUS  | RESTARTS | AGE  |
|-----------------------------------------|-------|---------|----------|------|
| dbsevent-5995495644-6px4m               | 1/1   | Running | 0        | 47m  |
| dbsevent-5995495644-hrt8l               | 1/1   | Running | 0        | 47m  |
| dbsisight-79f5fdfc4d-8qcmp              | 1/1   | Running | 0        | 2d2h |
| dbsisight-79f5fdfc4d-kntp6              | 1/1   | Running | 0        | 2d2h |
| dbsmonitor-577696776c-j5cpt             | 1/1   | Running | 0        | 2d2h |
| dbsmonitor-577696776c-kwbzj             | 1/1   | Running | 0        | 2d2h |
| <b>dwsmaintaintool-6849847c4b-9mxgf</b> | 1/1   | Running | 0        | 2d1h |
| <b>dwsmaintaintool-6849847c4b-mdqz6</b> | 1/1   | Running | 0        | 2d1h |
| ecfclustermanager-85987598fd-pst2k      | 1/1   | Running | 0        | 40m  |
| ecfclustermanager-85987598fd-x5jn9      | 1/1   | Running | 0        | 40m  |

**Step 2** Log in to an O&M pod.

**kubectl exec -it Pod\_name -n ecf bash**

Replace *Pod\_name* with the name of a pod queried in **Step 1** whose **STATUS** is **Running**. The following shows an example.

**kubectl exec -it dwsmaintaintool-ff99697f6-vtkcb -n ecf bash**

----End

## Decrypting the Password Ciphertext

**Step 1** Run the following command on the O&M container to go to the **/opt/cloud/3rdComponent/opsTool** directory:

**cd /opt/cloud/3rdComponent/opsTool**

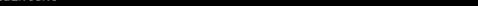
**Step 2** Start the tool.

**java -jar SccTool.jar**

**Step 3** Enter **3 {Password ciphertext}** as prompted to decrypt the password. For example, enter the ciphertext of the database user password queried in GeoGenius.

**3 {Password ciphertext}**

Press **Enter** to obtain the plaintext of the decrypted password.

```
international Encrypt, please input 1 and '' and password's plaintext
international Encrypt password in file, please input 2 and '' and absolute path of file
wcc,international,sm business Decrypt, please input 3 and '' and password's ciphertext
sm,international,sm business Decrypt password in file, please input 4 and '' and absolute path of file
sm business Encrypt, please input 5 and '' and password's plaintext
sm business Encrypt password in file, please input 6 and '' and absolute path of file
wcc Encrypt,please input 7 and '' and password's plaintext
wcc Encrypt password in file, please input 8 and '' and absolute path of file
wcc Decrypt and international Encrypt, please input 9 and '' and password's plaintext
wcc Decrypt and sm business Encrypt, please input 10 and '' and password's plaintext
international Decrypt and WCC Encrypt, please input 11 and '' and password's plaintext
sm business Decrypt and WCC Encrypt, please input 12 and '' and password's plaintext
international Decrypt and sm business Encrypt,please input 13 and '' and password's plaintext
sm business Decrypt and international Encrypt,please input 14 and '' and password's plaintext
3 BBBBAAAAAUAUAAAAAAAAAAHA/AB7D40U5P1+eBREgOVgLXNlcG3+jZG0yvBbaex4U7e8jY0X43AxxxxxAAAQTw
zuJ9vpKV80o/
```

Decrypt result:  
d000

**Step 4** Press CTRL+C to exit the tool.

----End

## Logging In to a Cluster Instance

**Step 1** Run the following command in the `/opt/cloud/3rdComponent/opsTool` directory of the O&M container to log in to the cluster instance: Obtain the username, host IP address, and port number from [Querying MySQL Database Information](#). Cluster instance ID is obtained from [Querying the Cluster Instance ID](#).

**sh connectTool.sh -u *Username* -drms -h*Host\_IP* -p*Port\_number* -n *Instance\_ID* -t Standalone**

After the command is executed, enter the password as prompted. Obtain the password from [Decrypting the Password Ciphertext](#).

```
[service@edvsmaintain tool:78db4bb55-b5f6g opstool]$ sh connectTool.sh -u@DB -drms -h192.168.1.100 -p7474 -n DB -c /tmp/conn -t Start
Start connect DB server and query result.....
Password:
Query result complete.
```

```
[service@dwmsaintain01 78b48b855-b5f6g opsTool]# sh connectTool.sh -u***** -drms -h***** -p***** -n ***** -t Standalone
Start connect DB server and query result.....
Password:
Query result complete.
```

```
spawn /bin/m -f /opt/cloud/3rdComponent/opsTool/tmp19605/connect 2023024033436 28179.exp >/dev/null 2>&1
spawn [root@host-1 ~]# /opt/cloud/3rdComponent/opsTool/tmp19605/ssh_key Mike@[REDACTED] -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null
Warning: Permanently added '[REDACTED]' (ED25519) to the list of known hosts.

Authorized users only. All activities may be monitored and reported.
Enter passphrase for key '/opt/cloud/3rdComponent/opsTool/tmp19605/ssh_key':
Authorized users only. All activities may be monitored and reported.
Last login: Fri Feb 24 03:31:27 2023 from [REDACTED]

Authorized users only. All activities may be monitored and reported.
[Mike@host-1 ~]# su
Password:
[root@host-1 ~]# Mike#
```

**Step 2** Switch to user **Ruby** and log in to the cluster sandbox.

## **su - Ruby**

```
ssh `hostname -i`
```



It takes some time to log in to the sandbox using `ssh $HOSTNAME`. Use `ssh `hostname -i`` or `ssh ip` instead.

**Step 3** If you need to log in to another node in the cluster, run the following commands to query the IP address of the node (*node\_ip* in the command output). Then run the corresponding command to enter the sandbox.

```
gs_om -t status --detail
```

**ssh** *node\_ip*

**Step 4** Perform O&M operations by referring to cases in this document.

----End

## 3.2 Logging In to the CloudAutoDeploy-CDK Master Node

**Step 1** Log in to ManageOne Maintenance Portal via <https://ManageOne Maintenance Portal URL:31943>. Alternatively, log in to the unified portal and choose **OperationCenter**.

- Password login: Enter the username and password of the account.
  - Default account: **bss\_admin**

 NOTE

For ManageOne upgraded from 8.2.0 or earlier, the default username is **admin**.  
For ManageOne 8.2.1 or later, the default username is **bss\_admin**.

- Preset password: See the preset password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).
- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter the PIN.

Log in to ManageOne Maintenance Portal.

**Step 2** In the **Cloud O&M Management** navigation pane, click **Service\_OM**. The Service OM page is displayed.

**Step 3** On the Service OM console page, click **VM**.

**Step 4** Query the IP address of the CloudAutoDeploy-CDK node. In the search box in the upper right corner, enter the keyword **EICCommon-Region-Master** to search for VMs. Generally, three VMs are available. You can record the IP address of any one of them.

**Step 5** Log in to the CloudAutoDeploy-CDK master node as user **opsadmin** using a remote login tool, and then switch to user **root**. The IP address is obtained in [Step 4](#).

**su - root**

- Default password of user **opsadmin**: Search for **EICCommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).
- Default password of user **root**: Search for **EICCommon-Region-Master-01** in the "Type A (Background)" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

----End

## 3.3 Querying MySQL Database Information

**Step 1** Log in to CloudScope using a browser as a system administrator.

- URL: [https://Address\\_for\\_accessing\\_CloudScope](https://Address_for_accessing_CloudScope), for example, <https://cloudscope.demo.com>
- For details about the URL for accessing CloudScope, see the COP information on the "Portal" sheet of the deployment parameter table exported from HCC Turnkey during Auto Change Platform installation.
- Default account: **op\_cdk\_sso**
- To obtain the default password of the account, search for the default password of the account on the "CloudScopeLite" sheet of [Huawei Cloud Stack 8.3.1 Account List](#).

**Step 2** Choose **Services > Change Mgmt > CloudAutoDeploy-CDK**.

**Step 3** In the navigation pane on the left, choose **Change Magmt & > Upgrade**, select the corresponding region, and select the cluster **ei-dbs-region**. Search for **dwscontroller** in the search box, select the corresponding dwscontroller, and click **Next**.

| Instance Name                                       | Service Status | Cluster       | Namespace | Architecture | Component     | Created On          | Updated On          |
|-----------------------------------------------------|----------------|---------------|-----------|--------------|---------------|---------------------|---------------------|
| dwscontroller-v08_04-35615940909847989c5d09b2ecd327 | Running        | ei-dbs-region | dws       | v8_04        | DWSController | 2023-08-14 20:00:58 | 2023-08-25 17:43:43 |

**Step 4** Enter the keyword **db**. in the search box on the right and record the password ciphertext corresponding to **db.password**, username corresponding to **db.username**, and database IP address and port number corresponding to **db.url**.

| Parameter Name | Type   | Data Type | Template Parameter                                       | Current Parameter | Description | Operation                        |
|----------------|--------|-----------|----------------------------------------------------------|-------------------|-------------|----------------------------------|
| db.password    | global | string    |                                                          | [REDACTED]        |             | <a href="#">Restore Defaults</a> |
| db.username    | global | string    | root                                                     | [REDACTED]        |             | <a href="#">Restore Defaults</a> |
| db.driver      | global | string    | org.mariadb.jdbc.Driver                                  | [REDACTED]        |             | <a href="#">Restore Defaults</a> |
| db.url         | global | string    | jdbc:mariadb://127.0.0.1:3306?autoReconnect=true&sock... | [REDACTED]        |             | <a href="#">Restore Defaults</a> |

**Step 5** Decrypt the password ciphertext by referring to [Decrypting the Password Ciphertext](#) and record the decrypted password.

----End

## 3.4 Logging In to the rms Database on the Management Side

**Step 1** Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

**Step 2** Log in to an O&M container by referring to [Logging In to the O&M Container](#).

**Step 3** Run the following command to connect to the MySQL database. The IP address of the database host can be obtained according to [Querying MySQL Database Information](#). For details about the password, see the [Type A \(Background\)](#) sheet in the [Huawei Cloud Stack 8.3.1 Account List](#). Select **DWS** for **Product Name** in column A, and search for **ecf**.

```
mysql -hDatabase_host_IP_address -P7306 -uecf;
```

Enter the password of user **ecf** as prompted and run the following command to switch to the **rms** database:

```
use rms;
```

----End

## 3.5 Logging In to a dwscontroller Pod

**Step 1** Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

**Step 2** Query the pods.

```
kubectl get pods -n dws -owide
```

Information similar to the following is displayed. **dwscontroller-xxx** indicates the pod names.

| NAME                                  | READY | STATUS  | RESTARTS | AGE   | IP            | NODE          | NOMINATED NODE  |
|---------------------------------------|-------|---------|----------|-------|---------------|---------------|-----------------|
|                                       |       |         |          |       |               |               | READINESS GATES |
| dms-collection-cbc7c6c-gx79t          | 1/1   | Running | 0        | 4d22h | 192.168.0.32  | 192.168.8.118 | <none>          |
| dms-collection-cbc7c6c-nt7sg          | 1/1   | Running | 0        | 4d22h | 192.168.0.107 | 192.168.8.127 | <none>          |
| dms-monitoring-5f44598478-njkv2       | 1/1   | Running | 0        | 4d22h | 192.168.0.128 | 192.168.8.120 | <none> <none>   |
| dms-monitoring-5f44598478-qwj4l       | 1/1   | Running | 0        | 4d22h | 192.168.0.144 | 192.168.8.119 | <none> <none>   |
| <b>dwscontroller-56864d578d-2kz5s</b> | 1/1   | Running | 0        | 26h   | 192.168.0.111 | 192.168.8.127 | <none> <none>   |
| <b>dwscontroller-56864d578d-wx8qr</b> | 1/1   | Running | 0        | 26h   | 192.168.0.75  | 192.168.8.125 | <none> <none>   |

**Step 3** Log in to a **dwscontroller** pod. In the following command, **dwscontroller\_pod\_name** indicates the name obtained in [Step 2](#).

```
kubectl exec -ti -n dws dwscontroller_pod_name bash
```

----End

## 3.6 Logging In to the GaussDB Database of DMS

**Step 1** Log in to ManageOne Maintenance Portal via <https://ManageOne Maintenance Portal URL:31943>. Alternatively, log in to the unified portal and choose **OperationCenter**.

- Password login: Enter the username and password of the account.
  - Default account: **bss\_admin**



For ManageOne upgraded from 8.2.0 or earlier, the default username is **admin**.  
For ManageOne 8.2.1 or later, the default username is **bss\_admin**.

- Preset password: See the preset password of the ManageOne Maintenance Portal account on the "Type A (Portal)" sheet in [Huawei Cloud Stack 8.3.1 Account List](#).

- Login using a USB key: Insert a USB key with preset user certificates, select the required device and certificate, and enter the PIN.

Log in to ManageOne Maintenance Portal.

**Step 2** In the **Cloud O&M Management** navigation pane, click **Service\_OM**. The Service OM page is displayed.

**Step 3** Choose **Services > Resource > Compute Resource**, click the **VMs** tab, search for **DWS-Gauss-DB** in the search box, and record the IP address of DWS-Gauss-DB01 or DWS-Gauss-DB02.

**Step 4** Use PuTTY to log in to any DWS-Gauss-DB node as user **opsadmin**, and run the **su - root** command to switch to user **root**.

- To obtain the default password of user **opsadmin**, search for **GaussDB(DWS)-Gauss-DB01** in the **Type A (Background)** sheet of the [Huawei Cloud Stack 8.3.1 Account List](#).
- To obtain the default password of user **root**, search for **GaussDB(DWS)-Gauss-DB01** in the **Type A (Background)** sheet of the [Huawei Cloud Stack 8.3.1 Account List](#).

**Step 5** Switch to user **dbadmin**.

**su - dbadmin**

**Step 6** Connect to the DMS database. For details about the password, see **Type B (EI Enterprise Intelligence)** in [Huawei Cloud Stack 8.3.1 Account List](#). Select **DWS for Cloud Service** in column A and search for **DMS database node** to obtain the password.

**gsql -Udbadmin -W Password**

**----End**

## 3.7 Collecting dwscontroller Logs

### Scenario

This section describes how to collect management logs. You are advised to collect logs on the ManageOne unified log platform. If ManageOne cannot provide services, manually collect logs by following the instructions provided in [Collecting dwscontroller Logs on the CDK Node](#).

### Collecting dwscontroller Logs Using ManageOne Maintenance Portal

**Step 1** Log in to ManageOne Maintenance Portal as an O&M administrator.

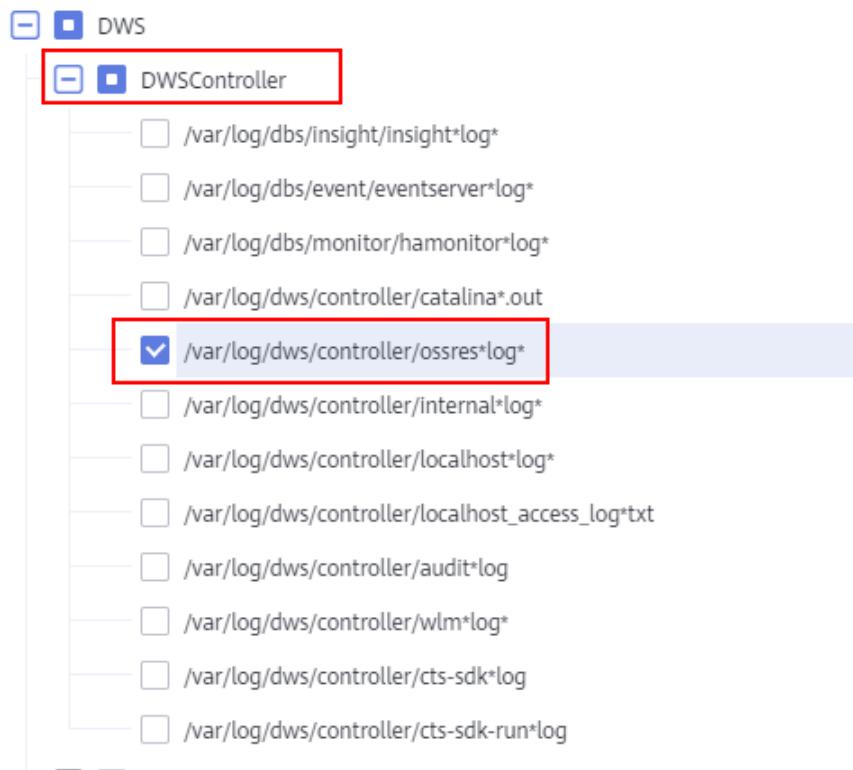
**Step 2** In the main menu, choose **O&M > Logs > Run Logs**.

**Step 3** In the navigation pane on the left, click **Management Run Log Download**.

**Step 4** Click **Add Download Log Task** to download log files.

1. Go to the **Custom** tab page and enter the task name.
2. Set the time segment for the log file. Click **Custom** next to **Time Segment** to set the time segment for the log to be downloaded.
3. In the log file list, search for **DWS** and select **DWS > DWSController > /var/log/dws/controller/ossres\*log\***.

**Figure 3-2** Configuring a log download task

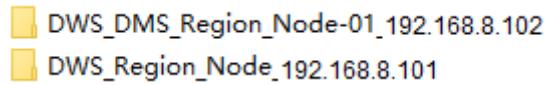


**Step 5** Click **OK**. After logs are collected, download them to the local PC.

 NOTE

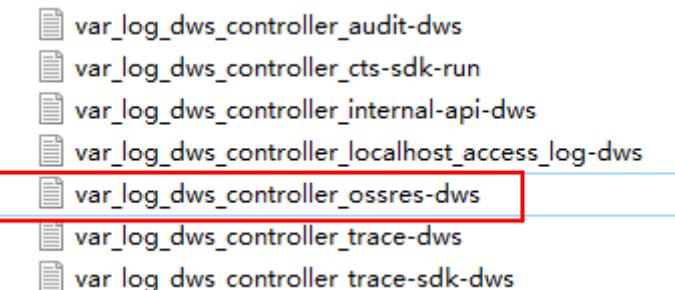
- Decompress the downloaded log file and you will get multiple .zip files. Each .zip file is the log package of a management-plane VM node. The name of each .zip file consists of the name of the VM of the management-plane microservice and the management IP address, as shown in the figure below. The log files of a container are randomly distributed on different management VMs. Therefore, you need to decompress all the .zip at a time. For example, if the **ossres-dws.log** files exist in the following two directories, you need to decompress the two files at the same time to obtain the complete log.

- ECF\_Region\_Node-02\_192.168.2.10.zip
- ECF\_Region\_Node-03\_192.168.2.15.zip
- DWS\_DMS\_Region\_Node-01\_192.168.2.30.zip



- The format of the log file is *Directory\_level\_of\_the\_host\_where\_the\_log\_file\_is\_located + Log\_name*. For example, if the path of the host where the dbsinsight component log file **ossres-dws.log** is located is **/var/log/dws/controller**, the log file name can be:

**var\_log\_dws\_controller\_ossres-dws.log**



----End

## Collecting dwscontroller Logs on the CDK Node

**Step 1** Log in to the CloudAutoDeploy-CDK master node by referring to [Logging In to the CloudAutoDeploy-CDK Master Node](#).

**Step 2** Obtain dwscontroller logs.

- Query the DWS Controller pod names.

**kubectl get pod -n dws -owide**

Information similar to the following is displayed. **dwscontroller-xxx** indicates the pod names.

| NAME                            | READY     | STATUS  | RESTARTS | AGE   | IP            | NODE          |
|---------------------------------|-----------|---------|----------|-------|---------------|---------------|
| NOMINATED NODE                  | READINESS | GATES   |          |       |               |               |
| dms-collection-cbc7c6c-gx79t    | 1/1       | Running | 0        | 4d22h | 192.168.0.32  | 192.168.8.118 |
| <none>                          | <none>    |         |          |       |               |               |
| dms-collection-cbc7c6c-nt7sg    | 1/1       | Running | 0        | 4d22h | 192.168.0.107 | 192.168.8.127 |
| <none>                          | <none>    |         |          |       |               |               |
| dms-monitoring-5f44598478-njkv2 | 1/1       | Running | 0        | 4d22h | 192.168.0.128 | 192.168.8.120 |
| <none>                          | <none>    |         |          |       |               |               |
| dms-monitoring-5f44598478-qwj4l | 1/1       | Running | 0        | 4d22h | 192.168.0.144 | 192.168.8.119 |
| <none>                          | <none>    |         |          |       |               |               |

```
dwscontroller-56864d578d-2kz5s 1/1 Running 0 26h 192.168.0.111 192.168.8.127
<none> <none>
dwscontroller-56864d578d-wx8qr 1/1 Running 0 26h 192.168.0.75 192.168.8.125
<none> <none>
```

2. Log in to a **dwscontroller** pod.

```
kubectl exec -it dwscontroller_container_name -n dws bash
```

3. Go to the log directory. Copy the **ossres-dws.log** file to the CDK Master node, enter **yes** as prompted, and enter the **root** password of the CloudAutoDeploy-CDK master node.

```
cd /opt/cloud/3rdComponent/tomcat/logs
```

```
scp ossres-dws.log root@CDK_Master_node_IP_address:/tmp
```

4. Log in to the CloudAutoDeploy-CDK master node as user **opsadmin** and run the following commands to switch to user **root** and change the owner of the log file to **opsadmin**:

```
su - root
```

```
chown -R opsadmin:wheel /tmp/ossres-dws.log
```

5. Use SFTP to log in to the CloudAutoDeploy-CDK master node as user **opsadmin** and download log files from the **/opt** directory.

6. Delete log files.

```
rm -rf /tmp/ossres-dws.log
```

----End