Abstract

This manual documents Continuent Tungsten, a high performance, High Availability and Disaster Recovery for MySQL clustering.

This manual includes information for 2.0, up to and including 2.0.5.

Build date: 2019-05-09 (3a7f04a)

Up to date builds of this document: Continuent Tungsten 2.0 Manual [Online], Continuent Tungsten 2.0 Manual [PDF]
# Table of Contents

Preface ........................................................................................................................... xvii  
1. Legal Notice .................................................................................................................. xvii  
2. Conventions .................................................................................................................. xvii  
3. Quickstart Guide ........................................................................................................... xviii  
1. Introduction ................................................................................................................... 19  
   1.1. Tungsten Replicator ................................................................................................. 19  
      1.1.1. Transaction History Log (THL) ..................................................................... 20  
   1.2. Tungsten Manager .................................................................................................. 20  
   1.3. Tungsten Connector ............................................................................................... 21  
2. Deployment .................................................................................................................... 23  
   2.1. Host Types ............................................................................................................ 23  
      2.1.1. Manager Hosts ............................................................................................... 23  
      2.1.2. Connector (Router) Hosts ............................................................................. 23  
      2.1.3. Replicator Hosts ........................................................................................... 24  
      2.1.4. Witness Hosts ............................................................................................... 24  
   2.2. Requirements ......................................................................................................... 26  
      2.2.1. Operating Systems Support .......................................................................... 26  
      2.2.2. Database Support ......................................................................................... 26  
      2.2.3. RAM Requirements ..................................................................................... 27  
      2.2.4. Disk Requirements ....................................................................................... 27  
      2.2.5. Java Requirements ....................................................................................... 27  
      2.2.6. Cloud Deployment Requirements ................................................................ 27  
   2.3. Deployment Sources ............................................................................................... 28  
      2.3.1. Using the TAR/GZipped files ....................................................................... 29  
      2.3.2. Using the RPM and DEB package files ......................................................... 29  
   2.4. Common tpm Options During Deployment ............................................................ 30  
   2.5. Best Practices ........................................................................................................ 30  
      2.5.1. Best Practices: Deployment .......................................................................... 30  
      2.5.2. Best Practices: Operations .......................................................................... 31  
      2.5.3. Best Practices: Maintenance ....................................................................... 31  
   2.6. Prepare Hosts .......................................................................................................... 31  
      2.6.1. Prepare MySQL Hosts .................................................................................. 31  
      2.6.2. Prepare Connector Hosts .............................................................................. 31  
      2.6.3. Prepare Active Witness Hosts ...................................................................... 32  
      2.6.4. Deploy SSH Keys ......................................................................................... 32  
   2.7. Deploying SSL Secured Replication and Administration ....................................... 33  
      2.7.1. Creating the Truststore and Keystore ............................................................. 33  
         2.7.1.1. Creating Your Own Client and Server Certificates ................................. 34  
         2.7.1.2. Creating a Custom Certificate and Getting it Signed .......................... 35  
         2.7.1.3. Using an existing Certificate .................................................................. 36  
         2.7.1.4. Converting SSL Certificates for keytool ............................................ 37  
      2.7.2. SSL and Administration Authentication ......................................................... 38  
      2.7.3. Configuring the Secure Service through tpm ................................................ 38  
      2.7.4. Configuring Connector SSL .......................................................................... 40  
      2.7.5. Connector SSL Example Procedure ............................................................. 41  
         2.7.5.1. Setup Environment and Paths ................................................................. 41  
         2.7.5.2. Configuring SSL for MySQL Server ..................................................... 41  
         2.7.5.3. Enable and Test SSL encryption from the Connector to the Database .... 43  
         2.7.5.4. Test SSL encryption from the Application to the Database .................. 45  
3. Deployment: MySQL Topologies .................................................................................. 46  
   3.1. Deploying a Master/Slave Cluster .......................................................................... 46  
      3.1.1. Prepare: Master/Slave Cluster .................................................................... 46  
      3.1.2. Install: Master/Slave Cluster ....................................................................... 47  
      3.1.3. Best Practices: Master/Slave Cluster ........................................................... 49  
   3.2. Deploying Multisite/Multimaster Clusters ............................................................... 49  
      3.2.1. Prepare: Multisite/Multimaster Clusters ......................................................... 51  
      3.2.2. Install: Multisite/Multimaster Clusters ............................................................ 51  
         3.2.2.1. Install: Multisite/Multimaster Clusters using Staging Configuration .... 51  
         3.2.2.2. Install: Multisite/Multimaster Clusters using INI Configuration ........... 56  
      3.2.3. Best Practices: Multisite/Multimaster Clusters ............................................. 59  
      3.2.4. Configuring Startup on Boot ........................................................................ 61  
      3.2.5. Resetting a single dataservice ..................................................................... 62  
      3.2.6. Resetting all dataservices ............................................................................ 62  
      3.2.7. Adding a new Cluster/Dataservice .............................................................. 63
3.2.8. Enabling SSL for Replicators Only ........................................ 64
3.2.9. Provisioning during live operations ................................. 65
3.2.10. Dataserver maintenance .............................................. 66
3.2.10.1. Fixing Replication Errors ............................................. 66
3.3. Deploying a Composite Cluster ........................................... 66
  3.3.1. Prepare: Composite Cluster ........................................... 67
  3.3.2. Install: Composite Cluster ........................................... 67
    3.3.2.1. Installing a Composite Configuration [Staging Use Case] ........ 67
    3.3.2.2. Installing a Composite Configuration [INI Use Case] .......... 70
  3.3.3. Best Practices: Composite Cluster .................................. 72
3.4. Deploying Tungsten Connector Only .................................... 72
3.5. Deploying Additional Datasources, Managers, or Connectors ......... 74
  3.5.1. Adding Datasources to an Existing Deployment .................. 74
  3.5.2. Adding Active Witnesses to an Existing Deployment ............. 75
  3.5.3. Adding Passive Witnesses to an Existing Deployment .......... 75
  3.5.4. Adding Connectors to an Existing Deployment ................... 76
  3.5.5. Adding a remote Composite Cluster ................................ 76
3.6. Replicating Data Into an Existing Dataservice .......................... 81
3.7. Replicating Data from a Cluster into MySQL .......................... 84
  3.7.1. Prepare: Replicating Data from a Cluster into MySQL .......... 85
  3.7.2. Deploy: Replicating Data from a Cluster into MySQL .......... 85
    3.7.2.1. Replicating Data from a Cluster to MySQL [Staging Use Case] 85
    3.7.2.2. Replicating Data from a Cluster to MySQL [INI Use Case] .... 87
  3.7.3. Best Practices: Replicating Data from a Cluster into MySQL 87
3.8. Migrating and Seeding Data ............................................. 90
  3.8.1. Migrating from MySQL Native Replication 'In-Place' .......... 90
  3.8.2. Migrating from MySQL Native Replication Using a New Service 91
  3.8.3. Seeding Data through MySQL ....................................... 93
4. Deployment: Advanced .................................................. 94
  4.1. Deploying Parallel Replication ...................................... 94
    4.1.1. Application Prerequisites for Parallel Replication .......... 94
    4.1.2. Enabling Parallel Apply During Install ......................... 94
    4.1.3. Channels .......................................................... 97
    4.1.4. Parallel Replication and Offline Operation .................. 98
      4.1.4.1. Clean Offline Operation ......................................... 98
      4.1.4.2. Tuning the Time to Go Offline Cleanly ......................... 98
      4.1.4.3. Unclean Offline ................................................ 98
    4.1.5. Adjusting Parallel Replication After Installation .......... 98
      4.1.5.1. How to Enable Parallel Apply After Installation .......... 98
      4.1.5.2. How to Change Channels Safely ................................ 100
      4.1.5.3. How to Disable Parallel Replication Safely ................. 100
      4.1.5.4. How to Switch Parallel Queue Types Safely ................. 101
    4.1.6. Monitoring Parallel Replication .................................. 101
      4.1.6.1. Useful Commands for Parallel Monitoring Replication ....... 101
      4.1.6.2. Parallel Replication and Applied Latency On Slaves ........ 101
      4.1.6.3. Relative Latency .............................................. 102
      4.1.6.4. Serialization Count ............................................ 102
      4.1.6.5. Maximum Offline Interval ..................................... 103
      4.1.6.6. Workload Distribution ........................................ 103
    4.1.7. Controlling Assignment of Shards to Channels ................. 104
    4.1.8. Disk vs. Memory Parallel Queues ................................ 105
4.2. Starting and Stopping Tungsten ....................................... 105
  4.2.1. Restarting the Replicator Service ................................ 106
  4.2.2. Restarting the Connector Service ................................ 106
  4.2.3. Restarting the Manager Service ................................... 106
  4.2.4. Restarting the Multisite/Multimaster Replicator Service ....... 107
4.3. Configuring Startup on Boot .......................................... 107
  4.3.1. Configuring Multisite/Multimaster Replicator Startup on Boot 107
4.4. Upgrading Tungsten ................................................... 108
  4.4.2. Upgrading when using INI-based configuration, or without ssh Access .... 108
    4.4.2.1. Upgrading Using the No-Switch Method ......................... 110
    4.4.2.2. Upgrading Using the Switch Method ............................. 111
    4.4.2.3. Upgrading a Single Host using rpn ............................. 111
  4.4.3. Upgrading from Continuent Tungsten 1.5.3/1.5.4 to Continuent Tungsten 2.0 111
  4.4.4. Installing an Upgraded JAR Patch ................................ 112
4.5. Downgrading to an Earlier Release .................................. 113
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.10. Connector Inline Command Interface</td>
<td>200</td>
</tr>
<tr>
<td>6.10.1. Connector tungsten cluster status Command</td>
<td>201</td>
</tr>
<tr>
<td>6.10.2. Connector tungsten connection count Command</td>
<td>201</td>
</tr>
<tr>
<td>6.10.3. Connector tungsten connection status Command</td>
<td>201</td>
</tr>
<tr>
<td>6.10.4. Connector tungsten flush privileges Command</td>
<td>202</td>
</tr>
<tr>
<td>6.10.5. Connector tungsten gc Command</td>
<td>202</td>
</tr>
<tr>
<td>6.10.6. Connector tungsten help Command</td>
<td>202</td>
</tr>
<tr>
<td>6.10.7. Connector tungsten mem info Command</td>
<td>203</td>
</tr>
<tr>
<td>6.10.8. Connector tungsten show [full] processlist Command</td>
<td>203</td>
</tr>
<tr>
<td>6.10.9. Connector show slave status Command</td>
<td>203</td>
</tr>
<tr>
<td>6.10.10. Connector tungsten show variables Command</td>
<td>204</td>
</tr>
<tr>
<td>6.11. Advanced Configuration</td>
<td>204</td>
</tr>
<tr>
<td>6.11.1. Using Multiple Dataservices</td>
<td>204</td>
</tr>
<tr>
<td>6.11.2. Connector Automatic Reconnect</td>
<td>205</td>
</tr>
<tr>
<td>6.11.3. Using the Connector with HA Proxy</td>
<td>205</td>
</tr>
<tr>
<td>6.11.3.1. Configuring HA Proxy using the native MySQL Check</td>
<td>206</td>
</tr>
<tr>
<td>6.11.3.2. Configuring HA Proxy with a Check Script</td>
<td>206</td>
</tr>
<tr>
<td>6.11.4. Using Fall-Back Bridge Mode</td>
<td>208</td>
</tr>
<tr>
<td>6.11.4.1. Using Fall-Back SSL To Bridge Mode</td>
<td>208</td>
</tr>
<tr>
<td>6.11.5. Using the Max Connections Feature</td>
<td>209</td>
</tr>
<tr>
<td>6.11.6. Adjusting the Client Disconnect Delay During Manual Switch</td>
<td>210</td>
</tr>
<tr>
<td>6.11.7. Adjusting the Bridge Mode Forced Client Disconnect Timeout</td>
<td>210</td>
</tr>
<tr>
<td>6.11.8. Adjusting the Connector Response to Resource Losses</td>
<td>210</td>
</tr>
<tr>
<td>6.11.8.1. Adjusting the Connector Response to Datasource Loss</td>
<td>210</td>
</tr>
<tr>
<td>6.11.8.2. Adjusting the Connector Response to Manager Loss</td>
<td>212</td>
</tr>
<tr>
<td>6.12. Connector General Limitations</td>
<td>213</td>
</tr>
<tr>
<td>7. Tungsten Manager</td>
<td>215</td>
</tr>
<tr>
<td>7.1. Tungsten Manager Introduction</td>
<td>215</td>
</tr>
<tr>
<td>7.2. Tungsten Manager Failover Tuning</td>
<td>215</td>
</tr>
<tr>
<td>7.3. Tungsten Manager Fault Detection, Fencing and Recovery</td>
<td>216</td>
</tr>
<tr>
<td>7.3.1. Tungsten Manager Definitions</td>
<td>216</td>
</tr>
<tr>
<td>7.3.2. Cluster Monitoring and Notification Events</td>
<td>216</td>
</tr>
<tr>
<td>7.3.3. Rule Organization - Detection, Investigation, Fencing, Recovery</td>
<td>217</td>
</tr>
<tr>
<td>8. Command-line Tools</td>
<td>221</td>
</tr>
<tr>
<td>8.1. The cctrl Command</td>
<td>221</td>
</tr>
<tr>
<td>8.1.11. cctrl Command-line Options</td>
<td>221</td>
</tr>
<tr>
<td>8.1.12. cctrl Modes</td>
<td>223</td>
</tr>
<tr>
<td>8.1.13. cctrl Commands</td>
<td>224</td>
</tr>
<tr>
<td>8.1.13.1. cctrl admin Command</td>
<td>224</td>
</tr>
<tr>
<td>8.1.13.2. cctrl cd Command</td>
<td>224</td>
</tr>
<tr>
<td>8.1.13.3. cctrl cluster Command</td>
<td>225</td>
</tr>
<tr>
<td>8.1.13.4. cctrl create composite Command</td>
<td>226</td>
</tr>
<tr>
<td>8.1.13.5. cctrl datasource Command</td>
<td>226</td>
</tr>
<tr>
<td>8.1.13.6. cctrl expert Command</td>
<td>228</td>
</tr>
<tr>
<td>8.1.13.7. cctrl fallover Command</td>
<td>228</td>
</tr>
<tr>
<td>8.1.13.8. cctrl help Command</td>
<td>228</td>
</tr>
<tr>
<td>8.1.13.9. cctrl ls Command</td>
<td>228</td>
</tr>
<tr>
<td>8.1.13.10. cctrl members Command</td>
<td>230</td>
</tr>
<tr>
<td>8.1.13.11. cctrl physical Command</td>
<td>230</td>
</tr>
<tr>
<td>8.1.13.12. cctrl ping Command</td>
<td>230</td>
</tr>
<tr>
<td>8.1.13.13. cctrl quit Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.14. cctrl recover Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.15. cctrl recover master using Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.16. cctrl recover relay using Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.17. cctrl recover using Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.18. cctrl replicator Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.19. cctrl rm Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.20. cctrl router Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.21. cctrl service Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.22. cctrl set Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.23. cctrl set force Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.24. cctrl set master Command</td>
<td>231</td>
</tr>
<tr>
<td>8.1.13.25. cctrl switch Command</td>
<td>231</td>
</tr>
<tr>
<td>8.2. The check_tungsten_latency Command</td>
<td>231</td>
</tr>
<tr>
<td>8.3. The check_tungsten_online Command</td>
<td>232</td>
</tr>
<tr>
<td>8.4. The check_tungsten_progress Command</td>
<td>233</td>
</tr>
<tr>
<td>8.5. The check_tungsten_services Command</td>
<td>233</td>
</tr>
</tbody>
</table>
8.6. The cluster_backup Command ........................................... 234
8.7. The connector Command .................................................. 234
8.8. The dsscan Command ....................................................... 236
8.8.1. Optional Arguments ................................................... 238
8.8.2. Supported Templates and Usage ..................................... 238

8.8.2.1. ddl-check-pkeys.vm ........................................... 238
8.8.2.2. ddl-mysql-hive-0.18.vm ....................................... 239
8.8.2.3. ddl-mysql-hive-0.18-staging.vm ............................... 240
8.8.2.4. ddl-mysql-hive-metadata.vm ................................. 241
8.8.2.5. ddl-mysql-oracle.vm ........................................... 241
8.8.2.6. ddl-mysql-oracle-cdc.vm ..................................... 242
8.8.2.7. ddl-mysql-vertica.vm .......................................... 242
8.8.2.8. ddl-mysql-vertica-staging.vm ............................... 243
8.8.2.9. ddl-oracle-mysql.vm ........................................... 243
8.8.2.10. ddl-oracle-mysql-pk-only.vm ................................. 244

8.9. The deployall Command ................................................ 245
8.10. env.sh Script ............................................................... 245
8.11. The manager Command ................................................ 245
8.12. The multi_trepcctl Command ....................................... 247
8.12.1. multi_trepcctl Options ............................................ 247
8.12.2. multi_trepcctl Commands ........................................ 249
8.12.2.1. multi_trepcctl list Command ............................... 250
8.12.2.2. multi_trepcctl run Command ............................... 250
8.13. The replicator Command .............................................. 250
8.14. The setupCDC.sh Command ........................................... 252
8.15. The startall Command ................................................ 255
8.16. The stopall Command .................................................. 255
8.17. The thl Command ....................................................... 255
8.17.1. the Position Commands ........................................... 256
8.17.2. the list Command .................................................. 257
8.17.3. the index Command ............................................... 258
8.17.4. the purge Command ............................................... 259
8.17.5. the info Command ................................................ 260
8.17.6. the help Command ................................................ 260
8.18. The trepcctl Command ................................................ 260
8.18.1. trepcctl Options .................................................. 261
8.18.2. trepcctl Global Commands ..................................... 262
8.18.2.1. trepcctl kill Command ..................................... 262
8.18.2.2. trepcctl services Command ................................ 262
8.18.2.3. trepcctl shutdown Command ................................ 264
8.18.2.4. trepcctl version Command .................................. 264
8.18.3. trepcctl Service Commands .................................... 264
8.18.3.1. trepcctl backup Command .................................. 265
8.18.3.2. trepcctl capabilities Command ............................ 266
8.18.3.3. trepcctl check Command .................................... 266
8.18.3.4. trepcctl clear Command ..................................... 267
8.18.3.5. trepcctl clients Command .................................. 267
8.18.3.6. trepcctl flush Command ..................................... 268
8.18.3.7. trepcctl heartbeat Command ................................ 268
8.18.3.8. trepcctl load Command ...................................... 269
8.18.3.9. trepcctl offline Command ................................... 270
8.18.3.10. trepcctl offline-deferred Command ....................... 270
8.18.3.11. trepcctl online Command ................................... 271
8.18.3.12. trepcctl properties Command ............................. 273
8.18.3.13. trepcctl purge Command ................................... 274
8.18.3.14. trepcctl reset Command .................................... 275
8.18.3.15. trepcctl restore Command ................................ 275
8.18.3.16. trepcctl setrole Command .................................. 276
8.18.3.17. trepcctl shard Command .................................... 276
8.18.3.18. trepcctl start Command .................................... 277
8.18.3.19. trepcctl status Command .................................. 277
8.18.3.20. trepcctl stop Command ...................................... 284
8.18.3.21. trepcctl unload Command ................................... 284
8.18.3.22. trepcctl wait Command ...................................... 284

8.19. The tpasswd Command ................................................ 285
8.20. The tungsten_health_check Script ................................ 285
8.21. The tungsten_monitor Script ........................................ 287
10.4.40.truncate.js Filter
10.4.41.zerosetnull.js Filter
10.5. JavaScript Filters
10.5.1. Writing JavaScript Filters
10.5.1.1. Implementable Functions
10.5.1.2. Getting Configuration Parameters
10.5.1.3. Logging Information and Exceptions
10.5.1.4. Exposed Data Structures

11. Performance and Tuning
11.1. Block Commit

A.2. Error/Cause/Solution
A.2.1. Lots of entries added to replicator log
A.2.2. Error: could not settle on encryption_client algorithm
A.2.3. The master replicator stopped with a JDBC error
A.2.4. ERROR backup.BackupTask Backup operation failed: null
A.2.5. Event application failed: seqno=20725782 fragno=0 message=java.sql.SQLDataException: Data too long for column 'eventid' at row 1
A.2.6. Unable to update the configuration of an installed directory
A.2.7. [S1000][unixODBC][MySQL][ODBC 5.3(w) Driver]SSL connection error: unknown error number
A.2.8. Connector shows errors with "java.net.SocketException: Broken pipe"
A.2.9. cctrl reports MANAGER[state=STOPPED]
A.2.10. Backup agent name not found: xtrabackup-full
A.2.11. Replicator runs out of memory
A.2.12. Replicator fails to connect after updating password
A.2.13. Attempt to write new log record with equal or lower fragno: seqno=3 previous stored fragno=32768 attempted new fragno=32768
A.2.14. ORA-00257: ARCHIVER ERROR. CONNECT INTERNAL ONLY, UNTIL FREED
A.2.15. ERROR 1010 [HY000] at line 5094506: Error dropping database [can't rmdir '/mysql-bin/'; errno: 17]
A.2.16. ERROR >> host >> can't alloc thread
A.2.17. ERROR 1580 [HY000] at line 5093787: You cannot 'DROP' a log table if logging is enabled
A.2.18. ERROR 2013 [HY000] at line 583: Lost connection to MySQL server during query
A.2.19. pendingExceptionMessage: "Unable to update last commit seqno: Incorrect datetime value: '2016-03-13 02:02:26' for column 'update_timestamp' at row 1
A.2.20. Too many open processes or files
A.2.21. WARN [KeepAliveTimerTask] - Error while sending a KEEP_ALIVE query to connection
A.2.22. Latency is high: master:ONLINE, progress=41331580333, THL latency=78849.733
A.2.23. Triggers not firing correctly on slave
A.2.24. cctrl hangs
A.2.25. Replication latency very high
A.2.26. Services requires a reset
A.2.27. trepctl status hangs
A.2.28. element 'mysq1_readonly' not found in path
A.2.29. Starting replication after performing a restore because of an invalid restart sequence number
A.2.30. MySQL is incorrectly configured
A.2.31. Replicator reports an Out of Memory error
A.2.32. Backup/Restore is not bringing my host back to normal

A.3. Known Issues
A.3.1. Triggers

A.4. Troubleshooting Timeouts
A.5. Troubleshooting Backups
A.6. Running Out of Diskspace
D.2.30. Terminology: Fields estimatedOfflineInterval
D.2.31. Terminology: Fields eventCount
D.2.32. Terminology: Fields extensions
D.2.33. Terminology: Fields extractTime
D.2.34. Terminology: Fields extractorClass
D.2.35. Terminology: Fields extractorName
D.2.36. Terminology: Fields filter.#.class
D.2.37. Terminology: Fields filter.#.name
D.2.38. Terminology: Fields filterTime
D.2.39. Terminology: Fields flushIntervalMillis
D.2.40. Terminology: Fields fsyncOnFlush
D.2.41. Terminology: Fields headSeqno
D.2.42. Terminology: Fields intervalguard
D.2.43. Terminology: Fields lastCommittedBlockSize
D.2.44. Terminology: Fields lastCommittedBlockTime
D.2.45. Terminology: Fields latestEpochNumber
D.2.46. Terminology: Fields logConnectionTimeout
D.2.47. Terminology: Fields logDir
D.2.48. Terminology: Fields logFileRetainMillis
D.2.49. Terminology: Fields logFileSize
D.2.50. Terminology: Fields MasterConnectURI
D.2.51. Terminology: Fields MasterListenURI
D.2.52. Terminology: Fields maxChannel
D.2.53. Terminology: Fields maxDelayInterval
D.2.54. Terminology: Fields maxOfflineInterval
D.2.55. Terminology: Fields maxSize
D.2.56. Terminology: Fields maximumStoredSeqno
D.2.57. Terminology: Fields minimumStoredSeqno
D.2.58. Terminology: Fields name
D.2.59. Terminology: Fields offlineRequests
D.2.60. Terminology: Fields otherTime
D.2.61. Terminology: Fields pendingError
D.2.63. Terminology: Fields pendingErrorEventId
D.2.64. Terminology: Fields pendingErrorSeqno
D.2.65. Terminology: Fields pendingExceptionMessage
D.2.66. Terminology: Fields pipelineSource
D.2.67. Terminology: Fields processedMinSeqno
D.2.68. Terminology: Fields queues
D.2.69. Terminology: Fields readOnly
D.2.70. Terminology: Fields relativeLatency
D.2.71. Terminology: Fields resourcePrecedence
D.2.72. Terminology: Fields rmiport
D.2.73. Terminology: Fields role
D.2.74. Terminology: Fields seqnoType
D.2.75. Terminology: Fields serializationCount
D.2.76. Terminology: Fields serialized
D.2.77. Terminology: Fields serviceName
D.2.78. Terminology: Fields serviceType
D.2.79. Terminology: Fields shardId
D.2.80. Terminology: Fields simpleServiceName
D.2.81. Terminology: Fields siteName
D.2.82. Terminology: Fields sourceId
D.2.83. Terminology: Fields stage
D.2.84. Terminology: Fields started
D.2.85. Terminology: Fields state
D.2.86. Terminology: Fields stopRequested
D.2.87. Terminology: Fields store.#
D.2.88. Terminology: Fields storeClass
D.2.89. Terminology: Fields syncInterval
D.2.90. Terminology: Fields taskCount
D.2.91. Terminology: Fields taskId
D.2.92. Terminology: Fields timeInStateSeconds
D.2.93. Terminology: Fields timeoutMillis
D.2.94. Terminology: Fields totalAssignments
D.2.95. Terminology: Fields transitioningTo
D.2.96. Terminology: Fields uptimeSeconds
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.</td>
<td>Witness: Active Service</td>
<td>25</td>
</tr>
<tr>
<td>2.2.</td>
<td>Witness: Inactive Service</td>
<td>26</td>
</tr>
<tr>
<td>3.1.</td>
<td>Topologies: Master/Slave Cluster</td>
<td>46</td>
</tr>
<tr>
<td>3.2.</td>
<td>Topologies: Multisite/Multimaster Clusters</td>
<td>50</td>
</tr>
<tr>
<td>3.3.</td>
<td>Topologies: Composite Cluster</td>
<td>67</td>
</tr>
<tr>
<td>3.4.</td>
<td>Topologies: Replicating into a Dataservice</td>
<td>81</td>
</tr>
<tr>
<td>3.5.</td>
<td>Topologies: Replicating Data from a Cluster into MySQL</td>
<td>84</td>
</tr>
<tr>
<td>3.6.</td>
<td>Migration: Migrating Native Replication using a New Service</td>
<td>92</td>
</tr>
<tr>
<td>5.1.</td>
<td>Sequence: Shunning a Datasource</td>
<td>130</td>
</tr>
<tr>
<td>5.2.</td>
<td>Migration: Migrating Native Replication using a New Service</td>
<td>161</td>
</tr>
<tr>
<td>5.3.</td>
<td>Cacti Monitoring: Example Graphs</td>
<td>173</td>
</tr>
<tr>
<td>6.1.</td>
<td>Tungsten Connector Basic Architecture</td>
<td>177</td>
</tr>
<tr>
<td>6.2.</td>
<td>Basic MySQL/Application Connectivity</td>
<td>178</td>
</tr>
<tr>
<td>6.3.</td>
<td>Advanced MySQL/Application Connectivity</td>
<td>179</td>
</tr>
<tr>
<td>6.4.</td>
<td>Using Tungsten Connector for MySQL/Application Connectivity</td>
<td>179</td>
</tr>
<tr>
<td>6.5.</td>
<td>Tungsten Connector during a failed datasource</td>
<td>180</td>
</tr>
<tr>
<td>6.6.</td>
<td>Tungsten Connector routing architecture</td>
<td>181</td>
</tr>
<tr>
<td>6.7.</td>
<td>Tungsten Connector Bridge Mode Architecture</td>
<td>191</td>
</tr>
<tr>
<td>6.8.</td>
<td>Tungsten Connector Authentication</td>
<td>193</td>
</tr>
<tr>
<td>9.1.</td>
<td>tpm INI Based Deployment</td>
<td>295</td>
</tr>
<tr>
<td>10.1.</td>
<td>Filters: Pipeline Stages on Masters</td>
<td>378</td>
</tr>
<tr>
<td>10.2.</td>
<td>Filters: Pipeline Stages on Slaves</td>
<td>379</td>
</tr>
<tr>
<td>C.1.</td>
<td>Tungsten Deployment</td>
<td>477</td>
</tr>
</tbody>
</table>
# List of Tables

1.1. Key Terminology ................................................................. 19  
2.1. Key Terminology ................................................................. 23  
6.1. Routing Method Selection .................................................. 182  
6.2. Connector Command Line Sub-Commands  ................................ 200  
6.3. Inline Interface Commands ................................................. 200  
8.1. ctrctl Command-line Options ............................................. 221  
8.2. ctrctl Command-line Options ............................................. 222  
8.3. ctrctl Command-line Options ............................................. 222  
8.4. ctrctl Command-line Options ............................................. 222  
8.5. ctrctl Command-line Options ............................................. 222  
8.6. ctrctl Command-line Options ............................................. 222  
8.7. ctrctl Command-line Options ............................................. 223  
8.8. ctrctl Command-line Options ............................................. 223  
8.9. ctrctl Command-line Options ............................................. 223  
8.10. ctrctl Command-line Options ............................................ 223  
8.11. ctrctl Commands ............................................................. 224  
8.12. ctrldatasource Commands ................................................ 227  
8.13. check_tungsten_latency Options ....................................... 231  
8.14. check_tungsten_online Options ....................................... 232  
8.15. check_tungsten_progress Options ..................................... 233  
8.16. check_tungsten_services Options ..................................... 233  
8.17. connector Commands ........................................................ 234  
8.18. ddlscan Command-line Options ........................................ 237  
8.19. ddlscan Supported Templates ......................................... 238  
8.20. manager Commands .......................................................... 245  
8.21. multi_trepctl Command-line Options ................................. 247  
8.22. multi_trepctl output Option ............................................ 248  
8.23. multi_trepctl Commands .................................................. 249  
8.24. replicator Commands ........................................................ 250  
8.25. replicator Commands Options for condrestart .................... 251  
8.26. replicator Commands Options for console ......................... 251  
8.27. replicator Commands Options for restart ......................... 251  
8.28. replicator Commands Options forf start ............................ 251  
8.29. setupCDC.conf Configuration Options ............................... 252  
8.30. tlh Options ................................................................. 255  
8.31. trepctl Command-line Options ......................................... 261  
8.32. trepctl Replicator Wide Commands ................................... 262  
8.33. trepctl Service Commands .............................................. 265  
8.34. trepctl backup Command Options ..................................... 265  
8.35. trepctl clients Command Options ..................................... 267  
8.36. trepctl offline-deferred Command Options .......................... 270  
8.37. trepctl online Command Options ...................................... 271  
8.38. trepctl purge Command Options ....................................... 274  
8.39. trepctl reset Command Options ....................................... 275  
8.40. trepctl setrole Command Options .................................... 276  
8.41. trepctl shard Command Options ....................................... 276  
8.42. trepctl status Command Options ..................................... 277  
8.43. trepctl wait Command Options ........................................ 284  
8.44. tpasswd Common Options ............................................... 285  
8.45. tungsten_health_check Command-line Options ..................... 285  
8.46. tungsten_monitor Command-line Options ............................ 287  
8.47. tungsten_provision_slave Command-line Options .................. 288  
8.48. tungsten_read_master_events Command-line Options .......... 289  
8.49. tungsten_set_position Command-line Options ..................... 290  
9.1. TPM Deployment Methods ................................................ 295  
9.2. tpm Core Options .......................................................... 304  
9.3. tpm Commands .............................................................. 305  
9.4. tpm Common Options ...................................................... 315  
9.5. tpm Validation Checks ..................................................... 318  
9.6. tpm Configuration Options .............................................. 336  
D.1. THL Event Format .......................................................... 492  
E.1. Continuent Tungsten Directory Structure ........................... 502  
E.2. Continuent Tungsten tungsten Sub-Directory Structure .......... 510
Preface

This manual documents Continuent Tungsten 2.0 up to and including 2.0.5 build 11. Differences between minor versions are highlighted stating the explicit minor release version, such as 2.0.5.x.

For other versions and products, please use the appropriate manual.

1. Legal Notice

The trademarks, logos, and service marks in this Document are the property of Continuent or other third parties. You are not permitted to use these Marks without the prior written consent of Continuent or such appropriate third party. Continuent, Tungsten, uni/cluster, m/cluster, p/cluster, uc/connector, and the Continuent logo are trademarks or registered trademarks of Continuent in the United States, France, Finland and other countries.

All Materials on this Document are [and shall continue to be] owned exclusively by Continuent or other respective third party owners and are protected under applicable copyrights, patents, trademarks, trade dress and/or other proprietary rights. Under no circumstances will you acquire any ownership rights or other interest in any Materials by or through your access or use of the Materials. All right, title and interest not expressly granted is reserved to Continuent.

All rights reserved.

2. Conventions

This documentation uses a number of text and style conventions to indicate and differentiate between different types of information:

- **Text in this style** is used to show an important element or piece of information. It may be used and combined with other text styles as appropriate to the context.

- Text in this style is used to show a section heading, table heading, or particularly important emphasis of some kind.

- Program or configuration options are formatted using **this style**. Options are also automatically linked to their respective documentation page when this is known. For example, `tpm` and `--hosts` both link automatically to the corresponding reference page.

- Parameters or information explicitly used to set values to commands or options is formatted using **this style**.

- Option values, for example on the command-line are formatted using **this style**. Parameters or information explicitly used to set values to commands or options is formatted using **this style**.

- Text in this style indicates literal or character sequence text used to show a specific value.

- Filenames, directories or paths are shown like this `/etc/passwd`. Filenames and paths are automatically linked to the corresponding reference page if available.

Bulleted lists are used to show lists, or detailed information for a list of items. Where this information is optional, a magnifying glass symbol enables you to expand, or collapse, the detailed instructions.

Code listings are used to show sample programs, code, configuration files and other elements. These can include both user input and replaceable values:

```shell
cd /opt/staging
unzip continuum-tungsten-2.0.5-11.zip
```

In the above example command-lines to be entered into a shell are prefixed using `shell`. This shell is typically `sh`, `ksh`, or `bash` on Linux and Unix platforms, or `Cmd.exe` or `PowerShell` on Windows.

If commands are to be executed using administrator privileges, each line will be prefixed with `root-shell`, for example:

```shell
vi /etc/passwd
```

To make the selection of text easier for copy/pasting, ignorable text, such as `shell>` are ignored during selection. This allows multi-line instructions to be copied without modification, for example:

```sql
create database test_selection;
drop database test_selection;
```

Lines prefixed with `mysql>` should be entered within the `mysql` command-line.
3. Quickstart Guide

- Are you planning on completing your first installation?
  - Do you know the Section 2.2, “Requirements”?
  - Have you followed the Appendix C, Prerequisites?
  - Have you decided which installation method you will use? INI or Staging?
  - Have you chosen your deployment type from Chapter 2, Deployment? Is this a Master/Slave deployment?

- Would you like to understand the different types of installation?
  There are two installation methods available in tpm, INI and Staging. A comparison of the two methods is at Section 9.1, “Comparing Staging and INI tpm Methods”.

- Do you want to upgrade to the latest version?
  See Section 9.5.18, “tpm update Command”.

- Are you trying to update or change the configuration of your system?
  See Section 9.5.18, “tpm update Command”.

- Has your system suffered a failure?
  For recovery methods and instructions, see Section 5.6, “Datasource Recovery Steps”.

- Would you like to perform database or operating system maintenance?
  See Section 5.14, “Performing Database or OS Maintenance”.

- Do you need to backup or restore your system?
  For backup instructions, see Section 5.9, “Creating a Backup”; and to restore a previously made backup, see Section 5.10, “Restoring a Backup”.
Chapter 1. Introduction

Continuent Tungsten™ provides a suite of tools to aid the deployment of database clusters using MySQL. Continuent Tungsten™ consists of three primary tools:

- **Tungsten Replicator**
  
  Tungsten Replicator supports replication between different databases. Tungsten Replicator acts as a direct replacement for the native MySQL replication, in addition to supporting connectivity to Oracle, MongoDB, Vertica and others.

- **Tungsten Manager**
  
  The Tungsten Manager is responsible for monitoring and managing a Continuent Tungsten dataservice. The manager has a number of control and supervisory roles for the operation of the cluster, and acts both as a control and a central information source for the status and health of the dataservice as a whole.

- **Tungsten Connector**
  
  The Tungsten Connector is a service that sits between your application server and your MySQL database. The connector routes connections from your application servers to the datasources within the cluster, automatically distributing and redirecting queries to each datasource according to load balancing and availability requirements.

Continuent Tungsten uses key terminology for different components in the system. These are used to distinguish specific elements of the overall system at the different levels of operations.

<table>
<thead>
<tr>
<th>Continuent Term</th>
<th>Traditional Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>composite dataservice</td>
<td>Multi-Site Cluster</td>
<td>A configured Continuent Tungsten service consisting of multiple dataservices, typically at different physical locations.</td>
</tr>
<tr>
<td>datasource</td>
<td>Cluster</td>
<td>The collection of machines that make up a single Tungsten Dataservice. Individual hosts within the dataservice are called datasources. Each dataservice is identified by a unique name, and multiple dataservices can be managed from one server.</td>
</tr>
<tr>
<td>dataserver</td>
<td>Database</td>
<td>The database on a host. Datasources include MySQL or Oracle.</td>
</tr>
<tr>
<td>datasource</td>
<td>Host or Node</td>
<td>One member of a datasource and the associated Tungsten components.</td>
</tr>
<tr>
<td>staging host</td>
<td>-</td>
<td>The machine [and directory] from which Continuent Tungsten™ is installed and configured. The machine does not need to be the same as any of the existing hosts in the dataservice.</td>
</tr>
<tr>
<td>active witness</td>
<td>-</td>
<td>A machine in the dataservice that runs the manager process but is not running a database server. This server will be used to establish quorum in the event that a datasource becomes unavailable.</td>
</tr>
<tr>
<td>passive witness</td>
<td>-</td>
<td>A witness host is a host that can be contacted using the ping protocol to act as a network check for the other nodes of the cluster. Witness hosts should be on the same network and segment as the other nodes in the dataservice.</td>
</tr>
<tr>
<td>coordinator</td>
<td></td>
<td>The datasource or active witness in a dataservice that is responsible for making decisions on the state of the dataservice. The coordinator is usually the member that has been running the longest. It will not always be the master. When the manager process on the coordinator is stopped, or no longer available, a new coordinator will be chosen from the remaining members.</td>
</tr>
</tbody>
</table>

### 1.1. Tungsten Replicator

Tungsten Replicator is an open source high performance replication engine that works with a number of different source and target databases to provide high-performance and improved replication functionality over the native solution. With MySQL replication, for example, the enhanced functionality and information provided by Tungsten Replicator allows for global transaction IDs, advanced topology support such as multi-master, star, and fan-in, and enhanced latency identification.

In addition to providing enhanced functionality Tungsten Replicator is also capable of heterogeneous replication by enabling the replicated information to be transformed after it has been read from the data server to match the functionality or structure in the target server. This functionality allows for replication between MySQL, Oracle, and Vertica, among others.

Understanding how Tungsten Replicator works requires looking at the overall replicator structure. There are three major components in the system that provide the core of the replication functionality:
**Extractor**

The extractor component reads data from a MySQL data server and writes that information into the Transaction History Log (THL). The role of the extractor is to read the information from a suitable source of change information and write it into the THL in the native or defined format, either as SQL statements or row-based information.

Information is always extracted from a source database and recorded within the THL in the form of a complete transaction. The full transaction information is recorded and logged against a single, unique, transaction ID used internally within the replicator to identify the data.

**Applier**

Appliers within Tungsten Replicator convert the THL information and apply it to a destination data server. The role of the applier is to read the THL information and apply that to the data server.

The applier works with a number of different target databases, and is responsible for writing the information to the database. Because the transactional data in the THL is stored either as SQL statements or row-based information, the applier has the flexibility to reformat the information to match the target data server. Row-based data can be reconstructed to match different database formats, for example, converting row-based information into an Oracle-specific table row, or a MongoDB document.

**Transaction History Log (THL)**

The THL contains the information extracted from a data server. Information within the THL is divided up by transactions, either implied or explicit, based on the data extracted from the data server. The THL structure, format, and content provides a significant proportion of the functionality and operational flexibility within Tungsten Replicator.

As the THL data is stored additional information, such as the metadata and options in place when the statement or row data was extracted are recorded. Each transaction is also recorded with an incremental global transaction ID. This ID enables individual transactions within the THL to be identified, for example to retrieve their content, or to determine whether different appliers within a replication topology have written a specific transaction to a data server.

These components will be examined in more detail as different aspects of the system are described with respect to the different systems, features, and functionality that each system provides.

From this basic overview and structure of Tungsten Replicator, the replicator allows for a number of different topologies and solutions that replicate information between different services. Straightforward replication topologies, such as master/slave are easy to understand with the basic concepts described above. More complex topologies use the same core components. For example, multi-master topologies make use of the global transaction ID to prevent the same statement or row data being applied to a data server multiple times. Fan-in topologies allow the data from multiple data servers to be combined into one data server.

### 1.1. Transaction History Log (THL)

Tungsten Replicator operates by reading information from the source database and transferring that information to the Transaction History Log (THL).

Each transaction within the THL includes the SQL statement or the row-based data written to the database. The information also includes, where possible, transaction specific options and metadata, such as character set data, SQL modes and other information that may affect how the information is written when the data is applied. The combination of the metadata and the global transaction ID also enable more complex data replication scenarios to be supported, such as multi-master, without fear of duplicating statement or row data application because the source and global transaction ID can be compared.

In addition to all this information, the THL also includes a timestamp and a record of when the information was written into the database before the change was extracted. Using a combination of the global transaction ID and this timing information provides information on the latency and how up to date a data server is compared to the original data source.

Depending on the underlying storage of the data, the information can be reformatted and applied to different data servers. When dealing with row-based data, this can be applied to a different type of data server, or completely reformatted and applied to non-table based services such as MongoDB.

THL information is stored for each replicator service, and can also be exchanged over the network between different replicator instances. This enables transaction data to be exchanged between different hosts within the same network or across wide-area-networks.

### 1.2. Tungsten Manager

The Tungsten Manager is responsible for monitoring and managing a Continuent Tungsten dataservice. The manager has a number of control and supervisory roles for the operation of the cluster, and acts both as a control and a central information source for the status and health of the dataservice as a whole.

Primarily, the Tungsten Manager handles the following tasks:
• Monitors the replication status of each datasource (node) within the cluster.

• Communicates and updates Tungsten Connector with information about the status of each datasource. In the event of a change of status, Tungsten Connectors are notified so that queries can be redirected accordingly.

• Manages all the individual components of the system. Using the Java JMX system the manager is able to directly control the different components to change status, control the replication process, and

• Checks to determine the availability of datasources by using either the Echo TCP/IP protocol on port 7 (default), or using the system ping protocol to determine whether a host is available. The configuration of the protocol to be used can be made by adjusting the manager properties. For more information, see Section C.2.2.3, “Host Availability Checks”.

• Includes an advanced rules engine. The rule engine is used to respond to different events within the cluster and perform the necessary operations to keep the dataservice in optimal working state. During any change in status, whether user-selected or automatically triggered due to a failure, the rules are used to make decisions about whether to restart services, swap masters, or reconfigure connectors.

Please see the Tungsten Manager documentation section Chapter 7, Tungsten Manager for more information.

1.3. Tungsten Connector

The Tungsten Connector is a service that sits between your application server and your MySQL database. The connector routes connections from your application servers to the datasources within the cluster, automatically distributing and redirecting queries to each datasource according to load balancing and availability requirements.

The primary goal of Tungsten Connector is to effectively route and redirect queries between the master and slave datasources within the cluster. Client applications talk to the connector, while the connector determines where the packets should really go, depending on the scaling and availability. Using a connector in this way effectively hides the complexities of the cluster size and configuration, allowing your cluster to grow and shrink without interrupting your client application connectivity. Client applications remain connected even though the number, configuration and orientation of the slaves within the cluster may change.

During failover or system maintenance Tungsten Connector takes information from Tungsten Manager to determine which hosts are up and available, and redirects queries only to those servers that are online within the cluster.

For load balancing, Tungsten Connector supports a number of different solutions for redirecting queries to the different datasources within the network. Solutions are either based on explicit routing, or an implied or automatic read/write splitting mode where data is automatically distributed between master hosts (writes) and slave hosts (reads).

Basic read/write splitting uses packet inspection to determine whether a query is a read operation (SELECT) or a write (INSERT, UPDATE, DELETE). The actual selection mechanism can be fine tuned using the different modes according to your application requirements.

The supported modes are:

• **Port Based Routing**
  
  Port based routing employs a second port on the connector host. All connections to this port are sent to an available slave.

• **Direct Reads**
  
  Direct reads uses the read/write splitting model, but directs read queries to dedicated read-only connections on the slave. No attempt is made to determine which host may have the most up to date version of the data. Connections are pooled between the connector and datasources, and this results in very fast execution.

• **SmartScale**
  
  With SmartScale, data is automatically distributed among the datasources using read/write splitting. Where possible, the connector selects read queries by determining how up to date the slave is, and using a specific session model to determine which host is up to date according to the session and replication status information. Session identification can be through predefined session types or user-defined session strings.

• **Host Based Routing**
  
  Explicit host based routing uses different IP addresses on datasources to identify whether the operation should be directed to a master or a slave. Each connector is configured with two IP addresses, connecting to one IP address triggers the connection to be routed to the current master, while connecting to the second IP routes queries to a slave.

• **SQL Based Routing**
  
  SQL based routing employs packet inspection to identify key strings within the query to determine where the packets should be routed. These core read/write splitting modes can also be explicitly overridden at a user or host level to allow your application maximum flexibility.
Internally, Tungsten Connector supports the native MySQL protocol, and accepts the raw packet data from the client and sends those packets directly to the datasource. Because it is the native network packets that are being forwarded between hosts the performance is kept high, without requiring any additional overhead or intelligence within the application.

The connector handles the distribution of packets between datasources, allowing clients to remain connected to Tungsten Connector even while the underlying datasources may become disconnected, or expanded as new datasources are added to the cluster.
Chapter 2. Deployment

Creating a Continuent Tungsten Dataservice using Continuent Tungsten requires careful preparation and configuration of the required components. This section provides guidance on these core operations, preparation and information such as licensing and best practice that should be used for all installations.

2.1. Host Types

Before covering the basics of creating different dataservice types, there are some key terms that will be used throughout the setup and installation process that identify different components of the system. These are summarised in Table 2.1, “Key Terminology”.

Table 2.1. Key Terminology

<table>
<thead>
<tr>
<th>Tungsten Term</th>
<th>Traditional Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>composite dataservice</td>
<td>Multi-Site Cluster</td>
<td>A configured Continuent Tungsten service consisting of multiple dataservices, typically at different physical locations.</td>
</tr>
<tr>
<td>dataservice</td>
<td>Cluster</td>
<td>A configured Continuent Tungsten service consisting of dataservers, datasources and connectors.</td>
</tr>
<tr>
<td>datasource</td>
<td>Database</td>
<td>The database on a host. Datasources include MySQL, PostgreSQL or Oracle.</td>
</tr>
<tr>
<td>dataserver</td>
<td>Host or Node</td>
<td>One member of a dataservice and the associated Tungsten components.</td>
</tr>
<tr>
<td>staging host</td>
<td>-</td>
<td>The machine from which Continuent Tungsten is installed and configured. The machine does not need to be the same as any of the existing hosts in the cluster.</td>
</tr>
<tr>
<td>staging directory</td>
<td>-</td>
<td>The directory where the installation files are located and the installer is executed. Further configuration and updates must be performed from this directory.</td>
</tr>
<tr>
<td>connector</td>
<td>-</td>
<td>A connector is a routing service that provides management for connectivity between application services and the underlying datasource.</td>
</tr>
<tr>
<td>Witness host</td>
<td>-</td>
<td>A witness host is a host that can be contacted using the ping protocol to act as a network check for the other nodes of the cluster. Witness hosts should be on the same network and segment as the other nodes in the dataservice.</td>
</tr>
</tbody>
</table>

2.1.1. Manager Hosts

The manager plays a key role within any dataservice, communicating between the replicator, connector and datasources to understand the current status, and controlling these components to handle failures, maintenance, and service availability.

The primary role of the manager is to monitor each of the services, identify problems, and react to those problems in the most effective way to keep the dataservice active. For example, in the case of a datasource failure, the datasource is temporarily removed from the cluster, the connector is updated to route queries to another available datasource, and the replication is disabled.

These decisions are driven by a rule-based system, which checks current status values, and performs different operations to achieve the correct result and return the dataservice to operational status.

In terms of control and management, the manager is capable of performing backup and restore information, automatically recovering from failure (including re-provisioning from backups), and is also able to individually control the configuration, service startup and shutdown, and overall control of the system.

Within a typical Continuent Tungsten deployment there are multiple managers and these keep in constant contact with each other, and the other services. When a failure occurs, multiple managers are involved in decisions. For example, if a host is no longer visible to one manager, it does not make the decision to disable the service on its own; only when a majority of managers identify the same result is the decision made. For this reason, there should be an odd number of managers [to prevent deadlock], or managers can be augmented through the use of witness hosts.

One manager is automatically installed for each configured datasource; that is, in a three-node system with a master and two slaves, three managers will be installed.

Checks to determine the availability of hosts are performed by using either the system ping protocol or the Echo TCP/IP protocol on port 7 to determine whether a host is available. ping protocol to determine whether a host is available. The configuration of the protocol to be used can be made by adjusting the manager properties. For more information, see Section C.2.1.1, “Host Availability Checks”.

2.1.2. Connector [Router] Hosts

Connectors (known as routers within the dataservice) provide a routing mechanism between client applications and the dataservice. The Tungsten Connector component automatically routes database operations to the master or slave, and takes account of the current cluster...
Deployment

status as communicated to it by the Tungsten Manager. This functionality solves three primary issues that might normally need to be handled by the client application layer:

• Datasource role redirection [i.e. master and slave]. This includes read/write splitting, and the ability to read data from a slave that is up to date with a corresponding write.

• Datasource failure [high-availability], including the ability to redirect client requests in the event of a failure or failover. This includes maintenance operations.

• Dataservice topology changes, for example when expanding the number of datasources within a dataservice

The primary role of the connector is to act as the connection point for applications that can remain open and active, while simultaneously supporting connectivity to the datasources. This allows for changes to the topology and active role of individual datasources without interrupting the client application. Because the operation is through one or more static connectors, the application also does not need to be modified or changed when the number of datasources is expanded or altered.

Depending on the deployment environment and client application requirements, the connector can be installed either on the client application servers, the database servers, or independent hosts. For more information, see Section 6.3, "Clients and Deployment".

Connectors can also be installed independently on specific hosts. The list of enabled connectors is defined by the --connectors option to tpm. A Continuent Tungsten dataservice can be installed with more connector servers than datasources or managers.

2.1.3. Replicator Hosts

The replicator provides the core replication of information between datasources and, in composite deployment, between dataservices. The replicator operates by extracting data from the ‘master’ datasource (for example, using the MySQL binary log), and then applies the data to one or more target datasources.

Different deployments use different replicators and configurations, but in a typical Continuent Tungsten deployment a master/slave or multi-master deployment model is used. For Continuent Tungsten deployments there will be one replicator instance installed on each datasource host.

Within the dataservice, the manager controls each replicator service and it able to alter the replicator operation and role, for example by switching between master and slave roles. The replicator also provides information to the manager about the latency of the replication operation, and uses this with the connectors to control client connectivity into the dataservice.

Replication within Continuent Tungsten is supported by Tungsten Replicator™ and this supports a wide range of additional deployment topologies, and heterogeneous deployments including MongoDB, Vertica, and Oracle. Replication to and from a dataservice are supported. For more information on replicating out of an existing dataservice, see:

• Section 3.7, "Replicating Data from a Cluster into MySQL"

Replicators are automatically configured according to the datasources and topology specified when the dataservice is created.

2.1.4. Witness Hosts

Continuent Tungsten operates through the rules built into the manager that make decisions about different configuration and status settings for all the services within the cluster. In the event of a communication failure within the system it is vital for the manager, in automatic policy mode, to perform a switch from a failed or unavailable master.

Within the network, the managers communicate with each other, in addition to the connectors and dataservers to determine their availability. The managers compare states and network connectivity. In the event of an issue, managers 'vote' on whether a failover or switch should occur.

The rules are designed to prevent unnecessary switches and failovers. Managers vote, and an odd number of managers helps to ensure that prevent split-brain scenarios when invalid failover decisions have been made.

Two types of witness are supported:

• Passive Witness — a passive witness is checked by the managers using a network ping to determine if the host is available. The witness host or hosts are used only as check to verify whether a failed host or failed network is the root cause.

• Active Witness — an active witness is an instance of Tungsten Manager running on a host that is otherwise not part of the dataservice. An active witness has full voting rights within the managers and can therefore make informed decisions about the dataservice state in the event of a failure. Active witnesses can only be a member of one cluster at a time.

All managers are active witnesses, and active witnesses are the recommended solution for deployments where network availability is less certain [i.e. cloud environments], and where you have two-node deployments.
Continuent Tungsten Quorum Requirements

- There should be at least three managers (including any active witnesses).
- There should be an odd number of managers and witnesses to prevent deadlocks.
- If the dataservice contains only two hosts, at least one active witness must be installed.
- Dataservices may contain either passive or active witnesses, but not both.

These rules apply for all Continuent Tungsten installations and must be adhered to. Deployment will fail if these conditions are not met.

The rules for witness selection are as follows:

1. Passive witnesses must be on the same network segment the managers. To prevent issues where a network switch or router failure would cause the managers to falsely identify a network failure, the managers must be able to connect to each other without having to route across networks or network segments.

   Active witnesses can be located beyond or across network segments, but all active witnesses must have clear communication channel to each other, and other managers. Difficulties in contacting other managers and services in the network could cause unwanted failover or shunning of datasources.

For example, consider the following scenario:

- Master dataserver on hostA, with slave dataservers on hostB and hostC
- Manager on hostA can see the dataserver on hostA and hostB, but not hostC
- Manager on hostB can see the dataserver on hostB and hostC, but not hostA
- Manager on hostC can see the dataserver on hostA, hostB and hostC
- Manager on hostA, hostB, and hostC can communicate with each other

Figure 2.1. Witness: Active Service

![Diagram of Tungsten deployment with hosts and managers]

The master will not be automatically switched, given that hostA is still available to two of the managers in the network.

If a second manager identifies hostA has failed:
Passive witnesses can be enabled when using `tpm` by using the `--witnesses` option:

```
shell> ./tools/tpm install alpha --witnesses=hostC,hostD
```

To enable active witnesses, the `--enable-active-witnesses=true` option must be specified and the hosts that will act as active witnesses must be added to the list of hosts provided to `--members`. This enables all specified witnesses to be enabled as active witnesses:

```
shell> ./tools/tpm install alpha --enable-active-witnesses=true
    --witnesses=hostC
    --members=hostA,hostB,hostC
```

### 2.2. Requirements

#### 2.2.1. Operating Systems Support

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Variant</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>RedHat/CentOS</td>
<td>Primary platform</td>
<td>RHEL 4, 5, and 6 as well as CentOS 5.x and 6.x versions are fully supported.</td>
</tr>
<tr>
<td>Linux</td>
<td>Ubuntu</td>
<td>Primary platform</td>
<td>Ubuntu 9.x-13.x versions are fully supported.</td>
</tr>
<tr>
<td>Linux</td>
<td>Debian/Suse/Other</td>
<td>Secondary Platform</td>
<td>Other Linux platforms are supported but are not regularly tested. We will fix any bugs reported by customers.</td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td>Secondary Platform</td>
<td>Solaris 10 is fully supported. OpenSolaris is not supported at this time.</td>
</tr>
<tr>
<td>Mac OS X</td>
<td></td>
<td>Secondary platform</td>
<td>Mac OS/X Leopard and Snow Leopard are used for development at Continuent but not certified. We will fix any bugs reported by customers.</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td>Limited Support</td>
<td>Tungsten 1.3 and above will support Windows platforms for connectivity [Tungsten Connector and SQL Router] but may require manual configuration. Tungsten clusters do not run on Windows.</td>
</tr>
<tr>
<td>BSD</td>
<td></td>
<td>Limited Support</td>
<td>Tungsten 1.3 and above will support BSD for connectivity [Tungsten Connector and SQL Router] but may require manual configuration. Tungsten clusters do not run on BSD.</td>
</tr>
</tbody>
</table>

#### 2.2.2. Database Support

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>Support Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>5.0, 5.1, 5.5, 5.6</td>
<td>Primary platform</td>
<td>Statement and row based replication is supported. MyISAM and InnoDB table types are fully supported; InnoDB tables are recommended.</td>
</tr>
</tbody>
</table>
2.2.3. RAM Requirements

RAM requirements are dependent on the workload being used and applied, but the following provide some guidance on the basic RAM requirements:

- Tungsten Replicator requires 2GB of VM space for the Java execution, including the shared libraries, with approximate 1GB of Java VM heapspace. This can be adjusted as required, for example, to handle larger transactions or bigger commit blocks and large packets.

  Performance can be improved within the Tungsten Replicator if there is a 2-3GB available in the OS Page Cache. Replicators work best when pages written to replicator log files remain memory-resident for a period of time, so that there is no file system I/O required to read that data back within the replicator. This is the biggest potential point of contention between replicators and DBMS servers.

- Tungsten Manager requires approximately 500MB of VM space for execution.

2.2.4. Disk Requirements

Disk space usage is based on the space used by the core application, the staging directory used for installation, and the space used for the THL files:

- The staging directory containing the core installation is approximately 150MB. When performing a staging-directory based installation, this space requirement will be used once. When using a INI-file based deployment, this space will be required on each server. For more information on the different methods, see Section 9.1, “Comparing Staging and INI tpm Methods”.

- Deployment of a live installation also requires approximately 150MB.

- The THL files required for installation are based on the size of the binary logs generated by MySQL. THL size is typically twice the size of the binary log. This space will be required on each machine in the cluster. The retention times and rotation of THL data can be controlled, see Section E.1.5, “The thl Directory” for more information, including how to change the retention time and move files during operation.

  When replicating from Oracle, the size of the THL will depend on the quantity of Change Data Capture (CDC) information generated. This can be managed by altering the intervals used to check for and extract the information.

A dedicated partition for THL or Continuent Tungsten is recommended to ensure that a full disk does not impact your OS or DBMS. Local disk, SAN, iSCSI and AWS EBS are suitable for storing THL. NFS is NOT recommended.

Because the replicator reads and writes information using buffered I/O in a serial fashion, there is no random-access or seeking.

2.2.5. Java Requirements

Tungsten Replicator is known to work with with the following Java versions and JVMs:

- Oracle JVM/JDK 6
- Oracle JVM/JDK 7
- OpenJDK 6
- OpenJDK 7

2.2.6. Cloud Deployment Requirements

Cloud deployments require a different set of considerations over and above the general requirements. The following is a guide only, and where specific cloud environment requirements are known, they are explicitly included:

Instance Types/Configuration

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>Support Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percona</td>
<td>5.5, 5.6, 5.7</td>
<td>Primary platform</td>
<td></td>
</tr>
<tr>
<td>MariaDB</td>
<td>5.5</td>
<td>Primary platform</td>
<td></td>
</tr>
<tr>
<td>Oracle [CDC]</td>
<td>10g Release 2</td>
<td>Primary Platform</td>
<td>Synchronous CDC is supported on Standard Edition only; Synchronous and Asynchronous are supported on Enterprise Editions</td>
</tr>
<tr>
<td>Drizzle</td>
<td></td>
<td>Secondary Platform</td>
<td>Experimental support for Drizzle is available. Drizzle replication is not tested.</td>
</tr>
</tbody>
</table>
Deployment

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Guidance</th>
<th>Amazon Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Type</td>
<td>Instance sizes and types are dependent on the workload, but larger instances are recommended for transactional databases.</td>
<td>m4.xlarge or better</td>
</tr>
<tr>
<td>Instance Boot Volume</td>
<td>Use block, not ephemeral storage.</td>
<td>EBS</td>
</tr>
<tr>
<td>Instance Deployment</td>
<td>Use standard Linux distributions and bases. For ease of deployment and configuration, use Puppet.</td>
<td>Amazon Linux AMIs</td>
</tr>
</tbody>
</table>

Development/QA nodes should always match the expected production environment.

AWS/EC2 Deployments

- Use Virtual Private Cloud (VPC) deployments, as these provide consistent IP address support.
- When using Active Witnesses, a micro instance can be used for a single cluster. For composite clusters, an instance size larger than micro must be used.
- Multiple EBS-optimized volumes for data, using Provisioned IOPS for the EBS volumes depending on workload:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>tpm Option</th>
<th>tpm Value</th>
<th>MySQL my.cnf Option</th>
<th>MySQL Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ (root)</td>
<td></td>
<td>/volumes/mysql/data</td>
<td>data dir</td>
<td>/volumes/mysql/data</td>
</tr>
<tr>
<td>MySQL Data</td>
<td>datasource-mysql-data-directory [353]</td>
<td>/volumes/mysql/data</td>
<td>data dir</td>
<td>/volumes/mysql/data</td>
</tr>
<tr>
<td>MySQL Binary Logs</td>
<td>datasource-log-directory [352]</td>
<td>/volumes/mysql/binlogs</td>
<td>log-bin</td>
<td>/volumes/mysql/binlogs/mysql-bin</td>
</tr>
<tr>
<td>Transaction History Logs (THL)</td>
<td>thl-directory [375]</td>
<td>/volumes/mysql/thl</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended Replication Formats

- MIXED is recommended for MySQL master/slave topologies [e.g., either single clusters or primary/data-recovery setups].
- ROW is strongly recommended for multi-master setups. Without ROW, data drift is a possible problem when using MIXED or STATEMENT. Even with ROW there are still cases where drift is possible but the window is far smaller.
- ROW is required for heterogeneous replication.

2.3. Deployment Sources

Continuent Tungsten is available in a number of different distribution types, and the methods for configuration available for these different packages differs. See Section 9.1, “Comparing Staging and INI tpm Methods” for more information on the available installation methods.

<table>
<thead>
<tr>
<th>Deployment Type/Package</th>
<th>TAR/GZip</th>
<th>RPM/DEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>tpm Command-line Configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>tpm INI File Configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy Entire Cluster</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Deploy Per Machine</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Two primary deployment sources are available:

- **Tar/GZip**
  
  Using the TAR/GZip package creates a local directory that enables you to perform installs and updates from the extracted ‘staging’ directory, or use the INI file format.

- **RPM/DEB Packages**
  
  Using the RPM/DEB package format is more suited to using the INI file format, as hosts can be installed and upgraded to the latest RPM/DEB package independently of each other.

All packages are named according to the product, version number, build release and extension. For example:
The version number is 2.0.5 and build number 11. Build numbers indicate which build a particular release version is based on, and may be useful when installing patches provided by support.

2.3.1. Using the TAR/GZipped files

To use the TAR/GZipped packages, download the files to your machine and unpack them:

```bash
shell> cd /opt/continuent/software
shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
```

This will create a directory matching the downloaded package name, version, and build number from which you can perform an install using either the INI file or command-line configuration. To use, you will need to use the `tpm` command within the `tools` directory of the extracted package:

```bash
shell> cd continuent-tungsten-2.0.5-11
```

2.3.2. Using the RPM and DEB package files

The RPM and DEB packages can be used for installation, but are primarily designed to be in combination with the INI configuration file.

Installation

Installing the RPM or DEB package will do the following:

1. Create the `tungsten` system user if it doesn't exist
2. Make the `tungsten` system user part of the `mysql` group if it exists
3. Create the `/opt/continuent/software` directory
4. Unpack the software into `/opt/continuent/software`
5. Define the `$CONTINUENT_PROFILES` and `$REPLICATOR_PROFILES` environment variables
6. Update the profile script to include the `/opt/continuent/share/env.sh` script
7. Create the `/etc/tungsten` directory
8. Run `tpm install` if the `/etc/tungsten.ini` or `/etc/tungsten/tungsten.ini` file exists

Although the RPM/DEB packages complete a number of the pre-requisite steps required to configure your cluster, there are additional steps, such as configuring `ssh`, that you still need to complete. For more information, see Appendix C, Prerequisites.

By using the package files you are able to setup a new server by creating the `/etc/tungsten.ini` file and then installing the package. Any output from the `tpm` command will go to `/opt/continuent/service_logs/rpm.output`.

**Note**

If you download the package files directly, you may need to add the signing key to your environment before the package will load properly.

For `yum` platforms [RHEL/CentOS/Amazon Linux], the `rpm` command is used:

```bash
root-shell> rpm --import http://www.continuent.com/RPM-GPG-KEY-continuent
```

For `Ubuntu/Debian` platforms, the `gpg` command is used:

```bash
root-shell> gpg --keyserver keyserver.ubuntu.com --recv-key 7206c924
```

Upgrades

If you upgrade to a new version of the RPM or DEB package it will do the following:

1. Unpack the software into `/opt/continuent/software`
2. Run `tpm update` if the `/etc/tungsten.ini` or `/etc/tungsten/tungsten.ini` file exists

The `tpm update` will restart all Continuent Tungsten services so you do not need to do anything after upgrading the package file.
2.4. Common tpm Options During Deployment

There are a variety of tpm options that can be used to alter some aspect of the deployment during configuration. Although they might not be provided within the example deployments, they may be used or required for different installation environments. These include options such as altering the ports used by different components, or the commands and utilities used to monitor or manage the installation once deployment has been completed. Some of the most common options are included within this section.

Changes to the configuration should be made with tpm update. This continues the procedure of using tpm install during installation. See Section 9.5.18, "tpm update Command" for more information on using tpm update.

- --datasource-systemctl-service

On some platforms and environments the command used to manage and control the MySQL or MariaDB service is handled by a tool other than the services or /etc/init.d/mysql commands.

Depending on the system or environment other commands using the same basic structure may be used. For example, within CentOS 7, the command is systemctl. You can explicitly set the command to be used by using the -datasource-systemctl-service to specify the name of the tool.

The format of the corresponding command that will be used is expected to follow the same format as previous commands, for example to start the database service:

```
shell> systemctl mysql stop
```

Different commands must follow the same basic structure, the command configured by --datasource-systemctl-service, the servicename, and the status (i.e. stop).

2.5. Best Practices

A successful deployment depends on being mindful during deployment, operations and ongoing maintenance.

2.5.1. Best Practices: Deployment

- Identify the best deployment method for your environment and use that in production and testing. See Section 9.1, “Comparing Staging and INI tpm Methods”.

- Standardize the OS and database prerequisites. There are Puppet and Chef modules available for immediate use or as a template for modifications.

- For security purposes you should ensure that you secure the following areas of your deployment:
  - Ensure that you create a unique installation and deployment user, such as tungsten, and set the correct file permissions on installed directories. See Section C.2.3, “Directory Locations and Configuration”.
  - When using ssh and/or SSL, ensure that the ssh key or certificates are suitably protected. See Section C.2.2.2, “SSH Configuration”.
  - Use a firewall, such as iptables to protect the network ports that you need to use. The best solution is to ensure that only known hosts can connect to the required ports for Continuent Tungsten. For more information on the network ports required for Continuent Tungsten operation, see Section C.2.2.1, “Network Ports”.
  - If possible, use authentication and SSL connectivity between hosts to protect your data and authorisation for the tools used in your deployment. See Section 2.7, “Deploying SSL Secured Replication and Administration” for more information.

- Choose your topology from the deployment section and verify the configuration matches the basic settings. Additional settings may be included for custom features but the basics are needed to ensure proper operation. If your configuration is not listed or does not match our documented settings; we cannot guarantee correct operation.

- If there are an even number of database servers in the cluster, configure the cluster with a witness host. An active witness is preferred but a passive one will ensure stability. See Section 2.1.4, “Witness Hosts” for an explanation of the differences and how to configure them.

- If you are using ROW replication, any triggers that run additional INSERT/UPDATE/DELETE operations must be updated so they do not run on the slave servers.

- Make sure you know the structure of the Continuent Tungsten home directory and how to initialize your environment for administration. See Section 5.1, “The Continuent Tungsten Home Directory” and Section 5.2, “Establishing the Shell Environment”.

- Prior to migrating applications to Continuent Tungsten test failover and recovery procedures from Chapter 5, Operations Guide. Be sure to try recovering a failed master and reprovisioning failed slaves.
2.5.2. Best Practices: Operations

- Setup proper monitoring for all servers as described in Section 5.16, “Monitoring Continuent Tungsten”.
- Configure the Continuent Tungsten services to startup and shutdown along with the server. See Section 4.3, “Configuring Startup on Boot”.
- Schedule the Section 8.6, “The cluster_backup Command” tool on each database server at least each night. The script will take a backup of at least one server. Skip this step if you have another backup method scheduled that takes consistent snapshots of your server.

2.5.3. Best Practices: Maintenance

- Schedule regular tests for local and DR failover. This should at least include switching the master server to another host in the local cluster. If possible, the DR cluster should be tested once per quarter.
- Disable any automatic operating system patching processes. The use of automatic patching will cause issues when all database servers automatically restart without coordination. See Section 5.14.3, “Performing Maintenance on an Entire Dataservice”.
- Regularly check for maintenance releases and upgrade your environment. Every version includes stability and usability fixes to ease the administrative process.

2.6. Prepare Hosts

Using Puppet is the fastest way to prepare a host for Continuent Tungsten. These instructions will show you how to install Puppet and prepare a host to run Continuent Tungsten. If you want to prepare the hosts without Puppet, follow the guidelines in Appendix C, Prerequisites.

- Make sure Puppet and all required packages are installed. See https://docs.puppetlabs.com/guides/puppetlabs_packagerepositories.html if you have any issues getting Puppet installed.

For RHEL/CentOS-based distributions:

```
shell > rpm -ivh http://yum.puppetlabs.com/puppetlabs-release-el-6.noarch.rpm
shell > yum install -y ruby rubygems ruby-devel puppet
```

For Ubuntu-based distributions:

```
shell > apt-get update
shell > apt-get install -y ruby ruby-dev puppet
```

- Install the Continuent Puppet module.

```
shell > mkdir -p /etc/puppet/modules
shell > puppet module install continuent/tungsten
```

- If you do not have DNS entries for the hosts in use, update the `/etc/hosts` file so that it reflects the proper IP addresses and complete hostname.

```
shell > puppet apply -e "
host { 'db1.west.example.com': ip => '192.168.11.101', }
host { 'db2.west.example.com': ip => '192.168.11.102', }
host { 'db3.west.example.com': ip => '192.168.11.103', }
"
```

2.6.1. Prepare MySQL Hosts

Use the Continuent Puppet module to install all prerequisites including MySQL. This will implement the prerequisites described in Section C.2, “Host Configuration” and Section C.3, “MySQL Database Setup”.

```
shell > puppet apply -e 'class { 'tungsten' :
  installMysql => true,
  replicationUser => 'tungsten',
  replicationPassword => 'secret',
  appUser => 'app_user',
  appPassword => 'secret',
}"
```

2.6.2. Prepare Connector Hosts

Use the Continuent Puppet module to install all common prerequisites. This will implement the prerequisites described in Section C.2, “Host Configuration”.

```
```
### Deployment

#### 2.6.3. Prepare Active Witness Hosts

Use the Continuent Puppet module to install all common prerequisites. This will implement the prerequisites described in Section C.2, “Host Configuration.”

```shell
puppet apply -e "class { 'tungsten' : }
```

#### 2.6.4. Deploy SSH Keys

The `tpm` script uses SSH to execute commands on each host. There are two simple ways to install these keys.

- Provide the SSH certificate and key to Puppet. In each of the examples below you may include an SSH certificate and key that will be assigned to the `tungsten` system user.

```shell
puppet apply -e "class { 'tungsten' : sshPublicKey => "-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAx
-----END RSA PRIVATE KEY-----",
```

- After unpacking the software package run the `tpm ssh-copy-cert` to output a set of commands that will setup the SSH certificate and authorized keys for a user. Run these commands as the `tungsten` system user on each host before proceeding with deployment.

```shell
mkdir -p ~/.ssh
```

```shell
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAx
-----END RSA PRIVATE KEY-----
```

After unpacking the software package run the `tpm ssh-copy-cert` to output a set of commands that will setup the SSH certificate and authorized keys for a user. Run these commands as the `tungsten` system user on each host before proceeding with deployment.
2.7. Deploying SSL Secured Replication and Administration

**Warning**

This procedure is for Continuent Tungsten Version 4.x and below ONLY!
For the correct procedures for Continuent Tungsten Version 5.0 and above, please see ???.

Continuent Tungsten supports encrypted communication between replication hosts. SSL can be employed at two different levels within the configuration, encryption of the THL communication channel used to transfer database events, and encryption (and implied authentication) of the JMX remote method invocation (RMI) used to administer services remotely within Continuent Tungsten.

To use SSL you must be using a Java Runtime Environment or Java Development Kit 1.5 or later. SSL is implemented through the `javax.net.ssl.SSLServerSocketFactory` socket interface class.

You will also need an SSL certificate. These can either be self-generated or obtained from an official signing authority. The certificates themselves must be stored within a Java key store and truststore. To create your certificates and add them to the keystore or truststore, see Section 2.7.1, "Creating the Truststore and Keystore". Instructions are provided for self-generated, self-signed, and officially signed versions of the necessary certificates.

For JMX RMI authentication, a password file and authentication definition must also be generated. This information is required by the JMX system to support the authentication and encryption process. See Section 2.7.2, "SSL and Administration Authentication" for more information.

Once the necessary files are available, you need to use `tpm` to install, or update an existing installation with the SSL configuration. See Section 2.7.3, "Configuring the Secure Service through `tpm`".

**Note**

Although not strictly required for installation, it may be useful to have the OpenSSL package installed. This contains a number of tools and utilities for dealing with certificate authority and general SSL certificates.

2.7.1. Creating the Truststore and Keystore

**Warning**

This procedure is for Continuent Tungsten Version 4.x and below ONLY!
For the correct procedures for Continuent Tungsten Version 5.0 and above, please see ???.

The SSL configuration works through two separate files that define the server and client side of the encryption configuration. Because individual hosts within a Continuent Tungsten configuration are both servers (when acting as a master, or when providing status information), and clients (when reading remote THL and managing nodes remotely), both the server and client side of the configuration must be configured.

Configuration for all systems relies on two files, the `truststore`, which contains the server certificate information (the certificates it will accept from clients), and the `keystore`, which manages the client certificate information (the certificates that will be provided to servers). The truststore and keystore hold SSL certificate information, and are password protected.

The keystores and truststores operate by holding one or more certificates that will be used for encrypting communication. The following certificate options are available:

- Create your own server and client certificates
- Create your own server certificates, get the server certificate signed by a Certificate Authority (CA), and use a corresponding signed client certificate
• Use a server and client certificate already signed by a CA. Care should be taken with these certificates, as they are associated with specific domains and/or hosts, and may cause problems in a dynamic environment.

In a multi-node environment such as Continuent Tungsten, all the hosts in the dataservice can use the same keystore and truststore certificates. The `tpm` command will distribute these files along with the configuration when a new installation is deployed, or when updating an existing deployment.

2.7.1. Creating Your Own Client and Server Certificates

Because the client and server components of the Continuent Tungsten configuration are the same, the same certificate can be used and add to both the keystore and truststore files.

The process is as follows:

1. Create the keystore and generate a certificate
2. Export the certificate
3. Import the certificate to the truststore

To start, use the supplied `keytool` to create a keystore and populate it with a certificate. The process asks for certain information. The alias is the name to use for the server and can be any identifier. When asked for the first and last name, use `localhost`, as this is used as the server identifier for the certificate. The other information should be entered accordingly.

Keystores (and truststores) also have their own passwords that are used to protect the store from updating the certificates. The password must be known as it is required in the configuration so that Continuent Tungsten can open the keystore and read the contents.

```
shell> keytool -genkey -alias replserver -keyalg RSA -keystore keystore.jks
```

```
Enter keystore password:
Re-enter new password:
```

```
What is your first and last name?
[Unknown]: localhost
```

```
What is the name of your organizational unit?
[Unknown]: My OU
```

```
What is the name of your city or locality?
[Unknown]: Mountain View
```

```
What is the name of your State or Province?
[Unknown]: CA
```

```
Is CN=localhost, OU=My OU, O=Continuent, L=Mountain View, ST=CA, C=US correct?
[no]: yes
```

```
Enter key password for <any>
```

```
The above process has created the keystore and the 'server' certificate, stored in the file keystore.jks.
```

Alternatively, you can create a new certificate in a keystore non-interactively by specifying the passwords and certificate contents on the command-line:

```
shell> keytool -genkey -alias replserver -keyalg RSA -keystore keystore.jks -dname "cn=localhost, ou=IT, o=Continuent, l=Mountain View, st=CA, c=US"
```

```
-verbose -trustcacerts -alias replserver -file client.cer -keystore truststore.ts
```

```
Enter keystore password:
```

```
Owner: CN=My Name, OU=My OU, O=Continuent, L=Mountain View, ST=CA, C=US
Issuer: CN=My Name, OU=My OU, O=Continuent, L=Mountain View, ST=CA, C=US
Serial number: 87db1e1
Valid from: Wed Jul 31 17:15:05 BST 2013 until: Tue Oct 29 16:15:05 GMT 2013
Certificate fingerprints:
```

This has created a certificate file in `client.cer` that can now be used to populate your truststore. When added the certificate to the truststore, it must be identified as a trusted certificate to be valid. The password for the truststore must be provided. It can be the same, or different, to the one for the keystore, but must be known so that it can be added to the Continuent Tungsten configuration.

```
shell> keytool -import -v -trustcacerts -alias replserver -file client.cer -keystore truststore.ts
```
Deployment

Signature algorithm name: SHA256withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier

KeyIdentifier [0000: E7 D1 DB 0B 42 AC 61 84   D4 2E 9A F1 80 00 88 44   .B..a........D]
0010: E4 69 C6 C7                                      .i..

Trust this certificate? [no]: yes
Certificate was added to keystore
[Storing truststore.ts]

This has created the truststore file, truststore.ts.

A non-interactive version is available by using the -noprompt option and supplying the truststore name:

```
shell> keytool -import -trustcacerts -alias replserver -file client.cer \\
-keystore truststore.ts -storepass password -noprompt
```

The two files, the keystore [keystore.jks], and truststore [truststore.ts], along with their corresponding passwords can be now be used with tpm to configure the cluster. See Section 2.7.3, “Configuring the Secure Service through tpm”.

2.7.1.2. Creating a Custom Certificate and Getting it Signed

You can create your own certificate and get it signed by an authority such as VeriSign or Thawte. To do this, the certificate must be created first, then you create a certificate signing request, send this to your signing authority, and then import the signed certificate and the certificate authority certificate into your keystore and truststore.

Create the certificate:

```
shell> keytool -genkey -alias replserver -keyalg RSA -keystore keystore.jks
```

Create a new signing request the certificate:

```
shell> keytool -certreq -alias replserver -file certrequest.pem \\
-keypass password -keystore keystore.jks -storepass password
```

This creates a certificate request, certrequest.pem. This must be sent to the signing authority to be signed.

- **Official Signing**

Send the certificate file to your signing authority. They will send a signed certificate back, and also include a root CA and/or intermediary CA certificate. Both these and the signed certificate must be included in the keystore and truststore files.

First, import the returned signed certificate:

```
shell> keytool -import -alias replserver -file signedcert.pem -keypass password \\
-keykeystore keystore.jks -storepass password
```

Now install the root CA certificate:

```
shell> keytool -import -alias careplserver -file cacert.pem -keypass password \\
-keykeystore keystore.jks -storepass password
```

35
Note

If the import of your certificate with `keytool` fails, it may be due to an incompatibility with some versions of OpenSSL, which fail to create suitable certificates for third-party tools. In this case, see Section 2.7.1.4, "Converting SSL Certificates for keytool" for more information.

And an intermediary certificate if you were sent one:

```shell
 keytool -import -alias interreplserver -file intercert.pem -keypass password -keystore keystore.jks -storepass password
```

Now export the signed certificate so that it can be added to the truststore. Although you can import the certificate supplied, by exporting the certificate in your keystore for inclusion into your truststore you can ensure that the two certificates will match:

```shell
 keytool -export -alias replserver -file client.cer -keystore keystore.jks
 Enter keystore password:
 Certificate stored in file <client.cer>
```

The exported certificate and CA root and/or intermediary certificates must now be imported to the truststore:

```shell
 keytool -import -trustcacerts -alias replserver -file client.cer -keystore truststore.ts -storepass password -noprompt
 keytool -import -trustcacerts -alias careplserver -file cacert.pem -keystore truststore.ts -storepass password -noprompt
 keytool -import -trustcacerts -alias interreplserver -file intercert.pem -keystore truststore.ts -storepass password -noprompt
```

**Self-Signing**

If you have setup your own certificate authority, you can self-sign the request using `openssl`:

```shell
 openssl ca -in certrequest.pem -out certificate.pem
```

Convert the certificate to a plain PEM certificate:

```shell
 openssl x509 -in certificate.pem -out certificate.pem -outform PEM
```

Finally, for a self-signed certificate, you must combine the signed certificate with the CA certificate:

```shell
 cat certificate.pem cacert.pem > certfull.pem
```

This certificate can be imported into your keystore and truststore.

To import your signed certificate into your keystore:

```shell
 keytool -import -alias replserver -file certfull.pem -keypass password -keystore keystore.jks -storepass password
```

Then export the certificate for use in your truststore:

```shell
 keytool -export -alias replserver -file client.cer -keystore keystore.jks
 Enter keystore password:
 Certificate stored in file <client.cer>
```

The same certificate must also be exported and added to the truststore:

```shell
 keytool -import -trustcacerts -alias replserver -file client.cer -keystore truststore.ts -storepass password -noprompt
```

This completes the setup of your truststore and keystore. The files created can be used in your `tpm` configuration. See Section 2.7.3, "Configuring the Secure Service through `tpm`".

### 2.7.1.3. Using an existing Certificate

If you have an existing certificate (for example with your MySQL, HTTP server or other configuration) that you want to use, you can import that certificate into your truststore and keystore. When using this method, you must import the signed certificate, and the certificate for the signing authority.

When importing the certificate into your keystore and truststore, the certificate supplied by the certificate authority can be used directly, but must be imported alongside the certificate authorities root and/or intermediary certificates. All the certificates must be imported for the SSL configuration to work.

The certificate should be in the PEM format if it is not already. You can convert to the PEM format by using the `openssl` tool:

```shell
 openssl x509 -in signedcert.crt -out certificate.pem -outform PEM
```
First, import the returned signed certificate:

```shell
keytool -import -file certificate.pem -keypass password \
-keystore keystore.jks -storepass password
```

**Note**

If the import of your certificate with `keytool` fails, it may be due to an incompatibility with some versions of OpenSSL, which fail to create suitable certificates for third-party tools. In this case, see Section 2.7.1.4, “Converting SSL Certificates for keytool” for more information.

Now install the root CA certificate:

```shell
keytool -import -file cacert.pem -keypass password \
-keystore keystore.jks -storepass password
```

And an intermediary certificate if you were sent one:

```shell
keytool -import -file intercert.pem -keypass password \
-keystore keystore.jks -storepass password
```

Now export the signed certificate so that it can be added to the truststore:

```shell
keytool -export -alias replserver -file client.cer -keystore keystore.jks
Enter keystore password:
Certificate stored in file <client.cer>
```

The exported certificate and CA root and/or intermediary certificates must now be imported to the truststore:

```shell
keytool -import -trustcacerts -alias replserver -file client.cer -keystore truststore.ts -storepass password -noprompt
keytool -import -trustcacerts -alias replserver -file cacert.pem -keystore truststore.ts -storepass password -noprompt
keytool -import -trustcacerts -alias replserver -file intercert.pem -keystore truststore.ts -storepass password -noprompt
```

### 2.7.1.4. Converting SSL Certificates for `keytool`

Some versions of the `openssl` toolkit generate certificates which are incompatible with the certificate mechanisms of third-party tools, even though the certificates themselves work fine with OpenSSL tools and libraries. This is due to a bug which affected certain releases of `openssl` 1.0.0 and later and the X.509 certificates that are created.

This problem only affects self-generated and/or self-signed certificates generated using the `openssl` command. Officially signed certificates from Thawte, VeriSign, or others should be compatible with `keytool` without conversion.

To get round this issue, the keys can be converted to a different format, and then imported into a keystore and truststore for use with Continuent Tungsten.

To convert a certificate, use `openssl` to convert the X.509 into PKCS12 format. You will be prompted to enter a password for the generated file which is required in the next step:

```shell
openssl pkcs12 -export -in client-cert.pem -inkey client-key.pem >client.p12
Enter Export Password:
Verifying - Enter Export Password:
```

To import the converted certificate into a keystore, specifying the destination keystore name, as well as the source PKCS12 password used in the previous step:

```shell
keytool -importkeystore -srcckeystore client.p12 -destkeystore keystore.jks -srcstoretype pkcs12
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

The same process can be used to import server certificates into truststore, by converting the server certificate and private key:

```shell
openssl pkcs12 -export -in server-cert.pem -inkey server-key.pem >server.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Then importing that into a truststore:

```shell
keytool -importkeystore -srcckeystore server.p12 -destkeystore truststore.ts -srcstoretype pkcs12
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 1 successfully imported.
```
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled

For official CA certificates, the generated certificate information should be valid for importing using keytool, and this file should not need conversion.

2.7.2. SSL and Administration Authentication

Warning

This procedure is for Continuent Tungsten Version 4.x and below ONLY!
For the correct procedures for Continuent Tungsten Version 5.0 and above, please see ???.

Continuent Tungsten uses JMX RMI to perform remote administration and obtain information from remote hosts within the dataservice. This communication can be encrypted and authenticated.

To configure this operation two files are required, one defines the authentication configuration, the other configures the username/password combinations used to authenticate. These files and configuration are used internally by the system to authenticate.

The authentication configuration defines the users and roles. The file should match the following:

```
monitorRole   readonly
controlRole   readwrite  
              create javax.management.monitor.*,javax.management.timer.*
              unregister

```

```
tungsten      readwrite  
              create javax.management.monitor.*,javax.management.timer.*
              unregister
```

The contents or description of this file must not be changed. Create a file containing this information in your configuration, for example jmxremote.access.

Now a corresponding password configuration must be created using the tpasswd tool. By default, plain-text passwords are generated:

```
shell> tpasswd -c tungsten password
      -t rmi_jmx
      -p ~/passwords.store
      -ts truststore.ts -tsp password
```

To use encrypted passwords, the truststore and truststore password must be supplied so that the certificate can be loaded and used to encrypt the supplied password. The -e must be specified to encrypt the password:

```
shell> tpasswd -c tungsten password 
      -t rmi_jmx
      -p ~/passwords.store
      -e
      -ts truststore.ts -tsp password
```

This creates a user, tungsten, with the password password in the file ~/passwords.store.

The password file, and the JMX security properties file will be needed during configuration. See Section 2.7.3, “Configuring the Secure Service through tpm”.

2.7.3. Configuring the Secure Service through tpm

Warning

This procedure is for Continuent Tungsten Version 4.x and below ONLY!
For the correct procedures for Continuent Tungsten Version 5.0 and above, please see ???.

To configure a basic SSL setup where the THL communication between, the keystore, truststore, and corresponding passwords must be configured in your installation.

Configuring SSL for THL Only

The configuration can be applied using tpm, either during the initial installation, or when performing an update of an existing installation. The same command-line options should be used for both. For the keystore and truststore, the pathnames supplied to tpm will be distributed to the other hosts during the update.

For example, to update an existing configuration, go to the staging directory for your installation:

```
shell> ./tools/tpm update 
      --thl-ssl=true
      --java-keystore-path=/keystore.jks
```
Deployment

Where:

- **--thl-ssl [358]**
  
  This enables SSL encryption on for THL when set to `true`.

- **--java-keystore-path [360]**
  
  Sets the location of the certificate keystore, the file will be copied to the installation directory during configuration.

- **--java-keystore-password [360]**
  
  The password for the keystore.

- **--java-truststore-path [360]**
  
  Sets the location of the certificate truststore, the file will be copied to the installation directory during configuration.

- **--java-truststore-password [360]**
  
  The password for the truststore.

**Note**

If you plan to update your configuration to use RMI authentication with SSL, the keystore and truststore must be the same as that used for THL SSL.

Once the installation or update has completed, the use of SSL can be confirmed by checking the THL URIs used to exchange information. For secure communication, the protocol is `thls`, as in the example output from `trepctl status`:

```
shell> trepctl status
Processing status command...
NAME                     VALUE
----                     -----...
appliedLastEventId     : mysql-bin.000011:0000000000003097:0
...  
masterConnectURI       : thls://localhost:/
masterListenURI        : thls://tr-ms1:2112/
maximumStoredSeqNo     : 15
minimumStoredSeqNo     : 0
...  
Finished status command...
```

**Configuring SSL for Administration**

Authentication and SSL encryption for administration controls the communication between administration tools such as `cctrl`. This prevents unknown tools from attempting to use the JMX remote invocation to perform different administration tasks.

The system works by encrypting communication, and then using explicit authentication (defined by the RMI user) to exchange authentication information.

To update your existing installation, go to the staging directory for your installation:

```
shell> ./tools/tpm update \  
   --java-keystore-path=/keystore.jks \   
   --java-keystore-password=password \   
   --java-truststore-path=/truststore.ts \   
   --java-truststore-password=password \   
   --rmi-ssl=true \   
   --rmi-authentication=true \   
   --rmi-user=tungsten \   
   --java-jmxremote-access-path=/jmxremote.access \   
   --java-passwordstore-path=/passwords.store
```

Where:

- **--rmi-ssl [357]**
  
  If set to `true`, enables RMI SSL encryption.

- **--rmi-authentication [357]**
  
  If set to `true`, enables authentication for the RMI service.
• **--rmi-user** [371]
  The user that will be used when performing administration. This should match the username used when creating the password file and security properties.

• **--java-jmxremote-access-path** [360]
  The path to the file containing the JMX RMI configuration, as configured in Section 2.7.2, “SSL and Administration Authentication”.

• **--java-passwordstore-path** [360]
  The location of the password file created when setting the password, as described in Section 2.7.2, “SSL and Administration Authentication”.

• **--java-keystore-path** [360]
  Sets the location of the certificate keystore, the file will be copied to the installation directory during configuration.

• **--java-keystore-password** [360]
  The password for the keystore.

• **--java-truststore-path** [360]
  Sets the location of the certificate truststore, the file will be copied to the installation directory during configuration.

• **--java-truststore-password** [360]
  The password for the truststore.

Once the update or installation has been completed, check that **trepctl** works and shows the status.

---

### 2.7.4. Configuring Connector SSL

SSL communication is supported for Tungsten Connector in three different possible combinations:

- SSL from the application to Tungsten Connector; Non-SSL connections from Tungsten Connector to MySQL
- Non-SSL from the application to Tungsten Connector; SSL connections from Tungsten Connector to MySQL
Deployment

- SSL from the application to Tungsten Connector; SSL connections from Tungsten Connector to MySQL

The connector also supports application connections using either SSL or Non-SSL communication on the same TCP/IP port. This allows you to choose SSL communication without changing your application ports.

To enable SSL communication with Tungsten Connector you must create suitable certificates keys and keystores, as described in Section 2.7.1, 'Creating the Truststore and Keystore'. The keystores used for Tungsten Connector can be the same, or different, to the keystores used for securing the manager and replication communication.

To enable connector SSL during installation or update, the `--connector-ssl=true` option must be set to true:

```
shell> ./tools/tpm update service_name --connector-ssl=true \
    --java-connector-keystore-path=/home/tungsten/keystore.jks \
    --java-connector-keystore-password=password \
    --java-connector-truststore-path=/home/tungsten/truststore.ts \
    --java-connector-truststore-password=password
```

This will update the connector configuration with the specified keystores, truststore and enable SSL on the connector connections.

### 2.7.5. Connector SSL Example Procedure

The below procedures accomplish the following objectives:

- Create, activate and test SSL keys for the MySQL server
- Enable and test SSL encrypted traffic between the MySQL server and the Connector
- Enable and test SSL encrypted traffic between the Application/Client and the Connector

#### 2.7.5.1. Setup Environment and Paths

Use these environment values on all Database & Connector nodes.

```
shell> export CONN_CERTS_PATH=~/connector-certs
shell> export MYSQL_CONFIG_PATH=/etc/mysql
shell> export MYSQL_CERTS_PATH=$MYSQL_CONFIG_PATH/certs
```

The `certs` directory is required on all Database nodes to hold the MySQL server certificates and keys.

```
shell> mkdir -p $CONN_CERTS_PATH
shell> sudo mkdir -p $MYSQL_CERTS_PATH
shell> sudo chown mysql: $MYSQL_CERTS_PATH
shell> sudo chmod 775 $MYSQL_CERTS_PATH
```

#### 2.7.5.2. Configuring SSL for MySQL Server

**Important**

The “Common Name” field for the Server and Client certificates MUST be different than the “Common Name” specified for the CA Cert.

1. Generate CA Cert

```
shell> openssl genrsa 2048 > $MYSQL_CERTS_PATH/ca-key.pem
shell> openssl req -new -x509 -nodes -days 3600 \
     -key $MYSQL_CERTS_PATH/ca-key.pem \
     -out $MYSQL_CERTS_PATH/ca-cert.pem
```

2. Generate Server Cert

```
shell> openssl req -newkey rsa:2048 -days 3600 -nodes \
     -keyout $MYSQL_CERTS_PATH/server-key.pem \
     -out $MYSQL_CERTS_PATH/server-cert.pem
shell> openssl rsa -in $MYSQL_CERTS_PATH/server-key.pem -out $MYSQL_CERTS_PATH/server-key.pem
shell> openssl x509 -req -in $MYSQL_CERTS_PATH/server-key.pem -days 3600 \n     -CA $MYSQL_CERTS_PATH/ca-cert.pem \n     -CAkey $MYSQL_CERTS_PATH/ca-key.pem \n     -set_serial 01 \n     -out $MYSQL_CERTS_PATH/server-cert.pem
```

3. Generate Client Cert

```
shell> openssl req -newkey rsa:2048 -days 3600 -nodes \
```

---

41
4. Verify All Certificates

```bash
shell> openssl verify -CAfile $MYSQL_CERTS_PATH/ca-cert.pem $MYSQL_CERTS_PATH/server-cert.pem $MYSQL_CERTS_PATH/client-cert.pem
```

5. Copy certs to all Database nodes (repeat as needed so that every Database node has the same certificates)

```bash
shell> rsync -av $MYSQL_CONFIG_PATH/ yourDBhost:$MYSQL_CONFIG_PATH/
```

6. Set proper ownership and permissions on ALL DB nodes

```bash
shell> sudo chown -R mysql: $MYSQL_CONFIG_PATH/
shell> sudo chmod -R g+w $MYSQL_CONFIG_PATH/
```

7. Update the `my.cnf` file to include the SSL certificates you just created (add three lines to the `[mysqld]` stanza)

```bash
shell> vi /etc/my.cnf
[mysqld]
... port=13306
# add three lines for SSL support
ssl-ca=/etc/mysql/certs/ca-cert.pem
ssl-cert=/etc/mysql/certs/server-cert.pem
ssl-key=/etc/mysql/certs/server-key.pem
...
```

8. Restart MySQL on all nodes using the standard rolling maintenance procedure - see Section 5.14.3, “Performing Maintenance on an Entire Datasetservice” for more information.

```bash
cctrl> ls
cctrl> datasource db3 shun
db3# service mysql restart
cctrl> recover
cctrl> datasource db2 shun
db2# service mysql restart
cctrl> recover
cctrl> switch to db2
cctrl> datasource db1 shun
db1# service mysql restart
cctrl> recover
cctrl> switch to db1
cctrl> ls
```

9. Add a new user to MySQL that requires SSL to connect. Do this just once on the current Master and let it propagate to the slaves.

```bash
shell> tpm mysql
mysql> DROP USER ssl_user;
mysql> CREATE USER ssl_user@'%' IDENTIFIED BY 'secret';
mysql> GRANT ALL ON *.* TO ssl_user@'%' REQUIRE SSL WITH GRANT OPTION;
mysql> flush privileges;
```

10. Verify that MySQL is working with SSL

   a. Expect this to fail, because the ssl_user is only allowed to connect to the database using SSL:

   ```bash
   shell> mysql -u ssl_user -psecret -h 127.0.0.1 -P 13306
   ```

   b. Expect this to pass, because we have supplied the proper SSL credentials:

   ```bash
   shell> mysql -u ssl_user -psecret -h 127.0.0.1 -P 13306 --ssl-ca=/etc/mysql/certs/ca-cert.pem
   ```

   c. Verify SSL:

   ```bash
   mysql> status
   ```
2.7.5.3. Enable and Test SSL encryption from the Connector to the Database

1. Convert MySQL Client Cert to pkcs12 format

```
shell> openssl pkcs12 -export \
    -inkey $MYSQL_CERTS_PATH/client-key.pem \
    -in $MYSQL_CERTS_PATH/client-cert.pem \
    -out $MYSQL_CERTS_PATH/client-cert.p12 \
    -passout pass:secret
```

2. Create tungsten_connector_keystore.jks

```
shell> keytool -importkeystore \
    -srckeystore $MYSQL_CERTS_PATH/client-cert.p12 \
    -srcstoretype PKCS12 \
    -destkeystore $CONN_CERTS_PATH/tungsten_connector_keystore.jks \
    -deststorepass secret \
    -srcstorepass secret
```

3. Import the CA Cert into the KeyStore

```
shell> keytool -import -alias mysqlServerCACert -file $MYSQL_CERTS_PATH/ca-cert.pem \
    -keystore $CONN_CERTS_PATH/tungsten_connector_keystore.jks \
    -storepass secret -noprompt
```

4. Import the CA Cert into the TrustStore

```
shell> keytool -import -alias mysqlServerCACert -file $MYSQL_CERTS_PATH/ca-cert.pem \
    -keystore $CONN_CERTS_PATH/tungsten_connector_truststore.ts \
    -storepass secret -noprompt
```

5. For INI-based deployments only, copy the certs to all Connector nodes [repeat as needed so that every Connector node has the same certificates]

```
shell> rsync -av $CONN_CERTS_PATH/ connectorHost:$CONN_CERTS_PATH/
```

6. Set proper ownership and permissions on ALL Connector nodes

```
shell> sudo chown tungsten: $CONN_CERTS_PATH/tungsten_connector_*
```

7. Add the new MySQL user to the Connector’s user.map config file.

See Section 6.6.1, “user.map File Format” for more information.

```
shell> vi /opt/continuent/tungsten/tungsten-connector/conf/user.map
ssl_user secret theSvcName
```

8. Update the Connector configuration to enable SSL

• Staging Method

Update all nodes (DB & Connector) in the cluster

```
shell> tpm query staging
shell> cd [STAGING_DIR]
shell> tools/tpm configure (yourServiceName) \
    --connector-ssl=true  \
    --java-connector-keystore-password=secret  \
    --java-connector-truststore-password=secret  \
    --java-connector-truststore-path=$CONN_CERTS_PATH/tungsten_connector_truststore.ts  \
    --java-connector-keystore-path=$CONN_CERTS_PATH/tungsten_connector_keystore.jks
```

```
shell> tools/tpm update
```

• INI Method

Repeat these two steps on each node (DB & Connector)

```
shell> vi /etc/tungsten/tungsten.ini
[defaults]
```
# enable SSL from the connector to the DB
connector-ssl=true
java-connector-keystore-password=secret
java-connector-truststore-password=secret
java-connector-truststore-path=$CONN_CERTS_PATH/tungsten_connector_truststore.ts
java-connector-keystore-path=$CONN_CERTS_PATH/tungsten_connector_keystore.jks

9. Test SSL connectivity through the connector
   a. Connect as the default application user

   ```
   shell> tpm connector
   ```
   b. Check the connection status

   **Note**
   Expecting "SSL.IN=false SSL.OUT=true"
   SSL.IN is false because the tpm connector command calls the mysql client in non-SSL mode.
   SSL.OUT is true because the connection to the database is encrypted, even if the connection from the mysql client is not.
   This can be verified with the “sudo tcpdump -X port 13306” command. Without the encryption, queries and responses are sent in plaintext and are visible in the output of tcpdump. When encryption is enabled, the queries and results are no longer visible.

   ```
   mysql> tungsten connection status;
   +-----------------------------------------------------------------------------+
   | Message                                                                     |
   +-----------------------------------------------------------------------------+
   | db1@east/master:ONLINE) STATUS(OK), QOS=RW_STRICT SSL.IN=false SSL.OUT=true | |
   +-----------------------------------------------------------------------------+
   1 row in set (0.00 sec)
   ```
   c. Check the SSL status

   **Note**
   Expecting “SSL: Not in use”
   SSL is not in use because the tpm connector command calls the mysql client in non-SSL mode.
   The connection to the database is encrypted, even if the connection from the mysql client is not.
   This can be verified with the “sudo tcpdump -X port 13306” command. Without the encryption, queries and responses are sent in plaintext and are visible in the output of tcpdump. When encryption is enabled, the queries and results are no longer visible.

   ```
   mysql> status
   +-----------------------------+
   | mysql Ver 14.14 Distrib 5.5.42-37.1, for Linux (x86_64) using readline 5.1 |
   +-----------------------------+
   | Connection id: 70           | |
   | Current database:           | |
   | Current user: app_user@app1 | |
   | SSL: Not in use             | |
   | Current pager: stdout       | |
   | Using outfile: ''           | |
   | Using delimiter: ;          | |
   | Server version: 5.5.42-37.1-log-tungsten Percona Server (GPL), Release 37.1, Revision 39ace0 | |
   | Protocol version: 10        | |
   | Connection: app1 via TCP/IP | |
   | Server characterset: latin1 | |
   | DB characterset: latin1     | |
   | Client characterset: latin1 | |
   | Conn. characterset: latin1  | |
   | TCP port: 3306              | |
   | Uptime: 2 hours 27 min 53 sec | |
   | Threads: 4 Questions: 41474 Slow queries: 0 Opens: 47 | |
   | Flush tables: 2 Open tables: 10 Queries per second avg: 4.674 | |
   +-----------------------------+
   ```
Deployment

Important

If you are able to login to MySQL and see that the "tungsten connection status;" is SSL.OUT=true, then you have successfully configured the communication between the Connector and MySQL to use SSL.

2.7.5.4. Test SSL encryption from the Application to the Database

1. Connect as the SSL-enabled application user through the Connector host

```
shell> mysql -u ssl_user -psecret -h 127.0.0.1 -P 3306 --ssl-ca=/etc/mysql/certs/ca-cert.pem
```

2. Check the connection status

Note

Expecting "SSL.IN=true SSL.OUT=true"

SSL.IN is true because the mysql client was invoked in SSL mode. Communications from the mysql client to the connector are encrypted.

SSL.out is true because the connection to the Database from the Connector is encrypted.

```
mysql>
```

3. Check the SSL status

Note

Expecting "Cipher in use is xxx-xxx-xxxxxx-xxx"

SSL is in use because the mysql client was invoked in SSL mode.

The connection from the mysql client to the database is encrypted.

```
mysql> status
```

```
mysql> Ver 14.14 Distrib 5.5.42-37.1, for Linux (x86_64) using readline 5.1
Connection id:      68
Current database:
Current user:      ssl_user@app1
SSL:         Cipher in use is DHE-RSA-AES256-SHA
Current pager:      stdout
Using outfile:      ''
Using delimiter:   ;
Server version:      5.5.42-37.1-log-tungsten Percona Server (GPL), Release 37.1, Revision 39acee0
Protocol version:   10
Connection:      app1 via TCP/IP
Server character set:   latin1
Db     character set:   latin1
Client character set:   latin1
Conn. character set:   latin1
TCP port:      3306
Uptime:         2 hours 33 min 32 sec
Threads: 4  Questions: 43065  Slow queries: 0  Opens: 47
Flush tables: 2  Open tables: 10  Queries per second avg: 4.674
```

Important

If you are able to login to MySQL and see that the "tungsten connection status;" is "SSL.IN=true SSL.OUT=true", and the "status;" contains "Cipher in use is xxx-xxx-xxxxxx-xxx", then you have successfully configured SSL-encrypted communication between the Application/Client and MySQL through the Connector.
Chapter 3. Deployment: MySQL Topologies

Creating a Continuent Tungsten Dataservice using Continuent Tungsten combines a number of different components, systems, and functionality, to support a running database dataservice that is capable of handling database failures, complex replication topologies, and management of the client/database connection for both load balancing and failover scenarios.

How you choose to deploy depends on your requirements and environment. All deployments operate through the `tpm` command. `tpm` operates in two different modes:

- **tpm staging configuration** — a `tpm` configuration is created by defining the command-line arguments that define the deployment type, structure and any additional parameters. `tpm` then installs all the software on all the required hosts by using `ssh` to distribute Continuent Tungsten and the configuration, and optionally automatically starts the services on each host. `tpm` manages the entire deployment, configuration and upgrade procedure.

- **tpm INI configuration** — `tpm` uses an `INI` to configure the service on the local host. The `INI` file must be create on each host that will be part of the cluster. `tpm` only manages the services on the local host; in a multi-host deployment, upgrades, updates, and configuration must be handled separately on each host.

The following sections provide guidance and instructions for creating a number of different deployment scenarios using Continuent Tungsten.

3.1. Deploying a Master/Slave Cluster

Within a master/slave service, there is a single master which replicates data to the slaves. The Tungsten Connector handles connectivity by the application and distributes the load to the datasources in the dataservice.

Figure 3.1. Topologies: Master/Slave Cluster

3.1.1. Prepare: Master/Slave Cluster

Before continuing with deployment you will need the following:

1. The name to use for the cluster.
2. The list of datasources in the cluster. These are the servers which will be running MySQL.
3. The list of servers that will run the connector.
4. The username and password of the MySQL replication user.
5. The username and password of the first application user. You may add more users after installation.

All servers must be prepared with the proper prerequisites. See Section 2.6, “Prepare Hosts” and Appendix C, Prerequisites for additional details.

### 3.1.2. Install: Master/Slave Cluster

1. Install the Continuent Tungsten package or download the Continuent Tungsten tarball, and unpack it:

   ```bash
   shell> cd /opt/continuent/software
   shell> tar zxf continuum-tungsten-2.0.5-11.tar.gz
   ```

2. Change to the Continuent Tungsten directory:

   ```bash
   shell> cd continuum-tungsten-2.0.5-11
   ```

3. Run `tpm` to perform the installation, using either the staging method or the INI method. Review Section 9.1, “Comparing Staging and INI Methods” for more details on these two methods.

   Click the link below to switch examples between Staging and INI methods
   
   **Show Staging**
   
   **Show INI**

   ```bash
   shell> ./tools/tpm configure defaults "
   --reset \n   --user=tungsten \n   --install-directory=/opt/continuent \n   --profile-script=~/.bash_profile \n   --replication-user=tungsten \n   --replication-password=password \n   --replication-port=13306 \n   --application-user=app_user \n   --application-password=secret \n   --application-port=3306 \n   --start-and-report=true
   ```

   ```bash
   shell> ./tools/tpm configure alpha "
   --topology=clustered \n   --master=host1 \n   --members=host1,host2,host3 \n   --connectors=host4
   ```

   ```bash
   shell> vi /etc/tungsten/tungsten.ini
   ```

   **[defaults]**
   user=tungsten
   install-directory=/opt/continuent
   profile-script=~/.bash_profile
   replication-user=tungsten
   replication-password=password
   replication-port=13306
   application-user=app_user
   application-password=secret
   application-port=3306
   start-and-report=true

   **[alpha]**
   topology=clustered
   master=host1
   members=host1,host2,host3
   connectors=host4

   Configuration group **defaults**
   The description of each of the options is shown below; click the icon to hide this detail:

   Click the icon to show a detailed description of each argument.

   - `--reset` [371]
Deployment: MySQL Topologies

reset

For staging configurations, deletes all pre-existing configuration information between updating with the new configuration values.

- --user=tungsten

user=tungsten

System User

- --install-directory=/opt/continuent

install-directory=/opt/continuent

Path to the directory where the active deployment will be installed. The configured directory will contain the software, THL and relay log information unless configured otherwise.

- --profile-script=~/.bash_profile

profile-script=~/.bash_profile

Append commands to include env.sh in this profile script

- --replication-user=tungsten

replication-user=tungsten

For databases that required authentication, the username to use when connecting to the database using the corresponding connection method (native, JDBC, etc.).

- --replication-password=password

replication-password=password

The password to be used when connecting to the database using the corresponding --replication-user.

- --replication-port=13306

replication-port=13306

The network port used to connect to the database server. The default port used depends on the database being configured.

- --application-user=app_user

application-user=app_user

Database username for the connector

- --application-password=secret

application-password=secret

Database password for the connector

- --application-port=3306

application-port=3306

Port for the connector to listen on

- --start-and-report=true

start-and-report=true

Start the services and report out the status after configuration

Configuration group alpha

The description of each of the options is shown below; click the icon to hide this detail:
• --topology=clustered

Replication topology for the dataservice. Valid values are star, cluster-slave, master-slave, fan-in, clustered, cluster-alias, all-masters, direct.

• --master=host1

The hostname of the master (extractor) within the current service. If the current host does not match this specification, then the deployment will by default be configured as a master/extractor.

• --members=host1,host2,host3

Hostnames for the dataservice members.

• --connectors=host4

Hostnames for the dataservice connectors.

Run `tpm` to install the software with the configuration.

```
shell > ./tools/tpm install
```

During the startup and installation, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

4. Initialize your `PATH` and environment.

```
shell > source /opt/continuent/share/env.sh
```

Important

Do not include `start-and-report` if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication ‘In-Place’” for next steps after completing installation.

3.1.3. Best Practices: Master/Slave Cluster

Follow the guidelines in Section 2.5, “Best Practices”.

3.2. Deploying Multisite/Multimaster Clusters

Warning

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

A Multisite/Multimaster topology provides all the benefits of a typical dataservice at a single location, but with the benefit of also replicating the information to another site. The underlying configuration within Continuent Tungsten uses the Tungsten Replicator System of Record (SOR) service, which enables multimaster operation between the two sites.

The configuration is in two separate parts:

• Continuent Tungsten dataservice that operates the main dataservice service within each site.

• Tungsten Replicator dataservice that provides replication between the two sites; one to replicate from site1 to site2, and one for site2 to site1.

A sample display of how this operates is provided in Figure 3.2, “Topologies: Multisite/Multimaster Clusters”.

49
The service can be described as follows:

- **Continuent Tungsten Service: east**
  
  Replicates data between east1, east2 and east3 (not shown).

- **Continuent Tungsten Service: west**

  Replicates data between west1, west2 and west3 (not shown).

- **Tungsten Replicator Service: east**

  Defines the replication of data within east as a replicator service using Tungsten Replicator. This service reads from all the hosts within the Continuent Tungsten service east and writes to west1, west2, and west3. The service name is the same to ensure that we do not duplicate writes from the clustered service already running.

  Data is read from the east Continuent Tungsten and replicated to the west Continuent Tungsten dataservice. The configuration allows for changes in the Continuent Tungsten dataservice (such as a switch or failover) without upsetting the site-to-site replication.

- **Tungsten Replicator Service: west**

  Defines the replication of data within west as a replicator service using Tungsten Replicator. This service reads from all the hosts within the Continuent Tungsten service west and writes to east1, east2, and east3. The service name is the same to ensure that we do not duplicate writes from the clustered service already running.

  Data is read from the west Continuent Tungsten and replicated to the east Continuent Tungsten dataservice. The configuration allows for changes in the Continuent Tungsten dataservice (such as a switch or failover) without upsetting the site-to-site replication.

- **Tungsten Replicator Service: east-west**
Replicates data from East to West, using Tungsten Replicator. This is a service alias that defines the reading from the dataservice (as a slave) to other servers within the destination cluster.

- Tungsten Replicator Service: west_east

Replicates data from West to East, using Tungsten Replicator. This is a service alias that defines the reading from the dataservice (as a slave) to other servers within the destination cluster.

**Requirements.** Recommended releases for Multisite/Multimaster deployments are Continuent Tungsten 4.0.x and Tungsten Replicator 4.0.0.

### 3.2.1. Prepare: Multisite/Multimaster Clusters

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Some considerations must be taken into account for any multimaster scenario:

- For tables that use auto-increment, collisions are possible if two hosts select the same auto-increment number. You can reduce the effects by configuring each MySQL host with a different auto-increment settings, changing the offset and the increment values. For example, adding the following lines to your `my.cnf` file:

```
auto-increment-offset = 1
auto-increment-increment = 4
```

In this way, the increments can be staggered on each machine and collisions are unlikely to occur.

- Use row-based replication. Update your configuration file to explicitly use row-based replication by adding the following to your `my.cnf` file:

```
binlog-format = row
```

- Beware of triggers. Triggers can cause problems during replication because if they are applied on the slave as well as the master you can get data corruption and invalid data. Continuent Tungsten cannot prevent triggers from executing on a slave, and in a multimaster topology there is no sensible way to disable triggers. Instead, check at the trigger level whether you are executing on a master or slave. For more information, see Section A.3.1, “Triggers”.

### 3.2.2. Install: Multisite/Multimaster Clusters

#### 3.2.2.1. Install: Multisite/Multimaster Clusters using Staging Configuration

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Creating the configuration requires two distinct steps, the first to create the two Continuent Tungsten deployments, and a second that creates the Tungsten Replicator configurations on different network ports, and different install directories.

1. Install the Continuent Tungsten package or download the Continuent Tungsten tarball, and unpack it:

   ```shell
   cd /opt/continuent/software
   tar zxf continuum-tungsten-2.0.5-11.tar.gz
   ```

2. Change to the Continuent Tungsten directory:

   ```shell
   cd continuum-tungsten2.0.5-11
   ```

3. Run `tpm` to configure the installation. This method assumes you are using the Section 9.3, “tpm Staging Configuration” method:

   ```shell
   ./tools/tpm configure defaults \\n   --user=tungsten \\n   --install-directory=/opt/continuent \\n   --replication-user=tungsten \\n   --replication-password=password \\n   --replication-port=13306 \\n   --application-user=app_user \\n   --application-password=secret
   ```
```
--application-port=3306 \
--start-and-report \
--profile-script=~/.bash_profile
```

```
shells ./tools/tpm configure east \
--topology=clustered \
--members=east1,east2,east3 \
--connectors=east1,east2,east3 \
--master=east1
```

```
shells ./tools/tpm configure west \
--topology=clustered \
--members=west1,west2,west3 \
--connectors=west1,west2,west3 \
--master=west1
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- **tpm configure defaults**
  
  This runs the `tpm` command. `configure defaults` indicates that we are setting options which will apply to all dataservices.

  - **--user=tungsten [377]**
    
    The operating system user name that you have created for the Tungsten service, `tungsten`.

  - **--install-directory=/opt/continuent [359]**
    
    The installation directory of the Tungsten service. This is where the service will be installed on each server in your dataservice.

  - **--replication-user=tungsten [370]**
    
    The MySQL user name to use when connecting to the MySQL database.

  - **--replication-password=password [370]**
    
    The MySQL password for the user that will connect to the MySQL database.

  - **--replication-port=13306 [370]**
    
    The TCP/IP port that the MySQL database is listening on for connections.

  - **--application-user=app_user [345]**
    
    The application user name.

  - **--application-password=secret [344]**
    
    The application password.

  - **--application-port=3306 [345]**
    
    The TCP/IP port on which to listen for incoming connections by the Tungsten connector service. To emulate the standard MySQL database service, port 3306 is used.

  - **--start-and-report [373]**
    
    Tells `tpm` to startup the service, and report the current configuration and status.

  - **--profile-script [368]**
    
    Tells `tpm` to add PATH information to the script to initialize the environment.

- **tpm configure east**
  
  This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `east` is the name and identity of the dataservice being created.

  - **--topology=clustered [377]**
    
    Tells `tpm` this is a clustered dataservice.

  - **--members=east1,east2,east3 [362]**
A comma separated list of all the hosts that are part of this dataservice.

- --connectors=east1,east2,east3

A comma separated list of the hosts that will have a connector service created on them.

- --master=east1

The hostname of the server that will be the default master MySQL server.

- tpm configure west

This runs the tpm command. configure indicates that we are creating a new dataservice, and west is the name and identity of the dataservice being created.

- --topology=clustered

Tells tpm this is a clustered dataservice.

- --members=west1,west2,west3

A comma separated list of all the hosts that are part of this dataservice.

- --connectors=west1,west2,west3

A comma separated list of the hosts that will have a connector service created on them.

- --master=west1

The hostname of the server that will be the default master MySQL server.

Note

Do not include --start-and-report if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication ‘In-Place’” for next steps after completing installation.

4. Run tpm to install the software with the configuration.

```
shell> ./tools/tpm install
```

During the startup and installation, tpm will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

5. Install the Tungsten Replicator package or download the Tungsten Replicator tarball, and unpack it:

```
shell> cd /opt/continuent/software
shell> tar zxf tungsten-replicator-3.0.0-524.tar.gz
```

6. Change to the Tungsten Replicator directory:

```
shell> cd tungsten-replicator-3.0.0-524
```

7. Run tpm to configure the installation. This method assumes you are using the Section 9.3, “tpm Staging Configuration” method:

```
shell> ./tools/tpm configure defaults
  --user=tungsten
  --install-directory=/opt/continuent
  --replication-user=tungsten
  --replication-password=password
  --replication-port=3306
  --application-user=app_user
  --application-password=secret
  --application-port=3306
  --start-and-report
  --profile-script=~/.bash_profile
shell> ./tools/tpm configure east
  --topology=clustered
  --members=east1,east2,east3
  --connectors=east1,east2,east3
```
Deployment: MySQL Topologies

```bash
tool> ./tools/tpm configure west
    --topology=clustered
    --members=west1,west2,west3
    --connectors=west1,west2,west3
    --master=west1

tool> ./tools/tpm configure west_east
    --topology=cluster-slave
    --master-dataservice=west
    --slave-dataservice=east

shell> ./tools/tpm configure west_east
    --topology=cluster-slave
    --master-dataservice=west
    --slave-dataservice=east
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- **tpm configure defaults**
  This runs the `tpm` command. `configure defaults` indicates that we are setting options which will apply to all dataservices.

- **--user=tungsten**
  The operating system user name that you have created for the Tungsten service, `tungsten`.

- **--install-directory=/opt/continuent**
  The installation directory of the Tungsten service. This is where the service will be installed on each server in your dataservice.

- **--replication-user=tungsten**
  The MySQL user name to use when connecting to the MySQL database.

- **--replication-password=password**
  The MySQL password for the user that will connect to the MySQL database.

- **--replication-port=13306**
  The TCP/IP port that the MySQL database is listening on for connections.

- **--application-user=app_user**
  The application user name.

- **--application-password=secret**
  The application password.

- **--application-port=3306**
  The TCP/IP port on which to listen for incoming connections by the Tungsten connector service. To emulate the standard MySQL database service, port 3306 is used.

- **--start-and-report**
  Tells `tpm` to startup the service, and report the current configuration and status.

- **--profile-script**
  Tells `tpm` to add PATH information to the script to initialize the environment.

- **tpm configure defaults**
  An additional set of defaults that are used to put the Tungsten Replicator in an independent directory.
- `--rmi-port=10002` [371]

Configure the second Tungsten Replicator to run on an additional port to avoid conflicts with Continuent Tungsten.

- `--executable-prefix=mm` [in [Tungsten Replicator 2.2 Manual]]

Configures the environment to create shell aliases for each of the commands shipped with Tungsten Replicator. Run the `aliases` command after initializing the environment to see a list of available aliases.

- `--thl-port=2113` [376]

Configure the second Tungsten Replicator to listen on an additional port to avoid conflicts with Continuent Tungsten.

- `tpm configure east`

This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `east` is the name and identity of the dataservice being created.

  - `--topology=clustered` [377]

  Tells `tpm` this is a clustered dataservice.

  - `--members=east1,east2,east3` [362]

  A comma separated list of all the hosts that are part of this dataservice.

  - `--connectors=east1,east2,east3` [351]

  A comma separated list of the hosts that will have a connector service created on them.

  - `--master=east1` [361]

  The hostname of the server that will be the default master MySQL server.

- `tpm configure west`

This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `west` is the name and identity of the dataservice being created.

  - `--topology=clustered` [377]

  Tells `tpm` this is a clustered dataservice.

  - `--members=west1,west2,west3` [362]

  A comma separated list of all the hosts that are part of this dataservice.

  - `--connectors=west1,west2,west3` [351]

  A comma separated list of the hosts that will have a connector service created on them.

  - `--master=west1` [361]

  The hostname of the server that will be the default master MySQL server.

- `tpm configure east_west`

This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `east_west` is the name and identity of the dataservice being created.

  - `--topology=cluster-slave` [377]

  Tells `tpm` this dataservice should replicate from a cluster to all datasources in `--slave-dataservice` [375].

  - `--master-dataservice=east` [370]

  Read replication information from any host in the `east` dataservice.

  - `--slave-dataservice=west` [375]

  Replicate information from `east` to every datasource in `west`.  

---

Replicate information from `east` to every datasource in `west`.  

---
Deployment: MySQL Topologies

- **tpm configure west_east**

  This runs the **tpm** command. **configure** indicates that we are creating a new dataservice, and **west_east** is the name and identity of the dataservice being created.

- **--topology=cluster-slave**

  Tells **tpm** this dataservice should replicate from a cluster to all datasources in **--slave-dataservice**.

- **--master-dataservice=west**

  Read replication information from any host in the **west** datasource.

- **--slave-dataservice=east**

  Replicate information from **west** to every datasource in **east**.

  **Note**

  Do not include **--start-and-report** if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication In-Place” for next steps after completing installation.

8. Run **tpm** to install the software with the configuration.

```
shell> ./tools/tpm install
```

During the startup and installation, **tpm** will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

9. Initialize your **PATH** and environment.

```
shell> source /opt/continuent/share/env.sh
shell> source /opt/replicator/share/env.sh
```

### 3.2.2.2. Install: Multisite/Multimaster Clusters using INI Configuration

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Creating the full topology requires two distinct install steps, the first creates the Continuent Tungsten cluster dataservices, and a second that creates the Tungsten Replicator services on different network ports and install directories.

1. Create the combined configuration file **/etc/tungsten/tungsten.ini** on all cluster hosts:

```
[defaults]
user=tungsten
install-directory=/opt/continuent
replication-user=tungsten
replication-password=secret
replication-port=3306
profile-script=~/.bashrc
start-and-report=true
application-user=app_user
application-password=secret
skip-validation-check=MySQLPermissionsCheck
start-and-report=true

[defaults.replicator]
home-directory=/opt/replicator
rmi-port=10002
executable-prefix=mm

[east]
topology=clustered
connectors=east1,east2,east3
master=east1
members=east1,east2,east3

[west]
topology=clustered
connectors=west1,west2,west3
```
Deployment: MySQL Topologies

```text
master=west1
members=west1,west2,west3

[east_west]
topology=cluster-slave
master-dataservice=east
slave-dataservice=west
thl-port=2113

[west_east]
topology=cluster-slave
master-dataservice=west
slave-dataservice=east
thl-port=2115
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `[defaults]`
  - `defaults` indicates that we are setting options which will apply to all cluster dataservices.
  - `user=tungsten [377]`
    The operating system user name that you have created for the Tungsten service, `tungsten`.
  - `install-directory=/opt/continuent [359]`
    The installation directory of the Continuent Tungsten service. This is where the cluster software will be installed on each server in your dataservice.
  - `replication-user=tungsten [370]`
    The MySQL user name to use when connecting to the MySQL database.
  - `replication-password=secret [370]`
    The MySQL password for the user that will connect to the MySQL database.
  - `replication-port=13306 [370]`
    The TCP/IP port that the MySQL database is listening on for connections.
  - `application-user=app_user [345]`
    The application user name.
  - `application-password=secret [344]`
    The application password.
  - `application-port=3306 [345]`
    The TCP/IP port on which to listen for incoming connections by the Tungsten connector service. To emulate the standard MySQL database service, port 3306 is used.
  - `start-and-report=true [373]`
    Tells `tpm` to startup the service, and report the current configuration and status.
  - `profile-script [368]`
    Tells `tpm` to add PATH information to the script to initialize the environment.
  - `[defaults.replicator]`
    - `defaults.replicator` indicates that we are setting options which will apply to all MSMM Tungsten Replicator services.
    - `install-directory=/opt/replicator [359]`
      The installation directory of the MSMM Tungsten Replicator.
  - `rmi-port=10002 [371]`
The MSMM Replication RMI listen port.

- **executable-prefix=mm** (in [Tungsten Replicator 2.2 Manual])

Declare aliases for all replication scripts that use mm_ as a prefix.

- **[east]**
  
  east is the name and identity of the cluster dataservice being created.

  - **topology=clustered** [377]
    
    Tells tpm this is a clustered dataservice.

  - **members=east1,east2,east3** [362]
    
    A comma separated list of all the hosts that are part of this cluster dataservice.

  - **connectors=east1,east2,east3** [351]
    
    A comma separated list of the hosts that will have a connector service created on them.

  - **master=east1** [361]
    
    The hostname of the server that will be the default master MySQL server.

- **[west]**
  
  west is the name and identity of the cluster dataservice being created.

  - **topology=clustered** [377]
    
    Tells tpm this is a clustered dataservice.

  - **members=west1,west2,west3** [362]
    
    A comma separated list of all the hosts that are part of this dataservice.

  - **connectors=west1,west2,west3** [351]
    
    A comma separated list of the hosts that will have a connector service created on them.

  - **master=west1** [361]
    
    The hostname of the server that will be the default master MySQL server.

- **[east_west]**
  
  east_west is the name and identity of the replication service that pulls data from the east cluster and applies to the west nodes.

  - **topology=cluster-slave** [377]
    
    Tells tpm this is a cluster-slave replication service which will have a list of all source cluster nodes available.

  - **master-dataservice=east** [370]
    
    The source cluster dataservice name.

  - **slave-dataservice=west** [375]
    
    The destination cluster dataservice name.

  - **thl-port=2113** [376]
    
    The network port for THL operations.

- **[west_east]**
  
  west_east is the name and identity of the replication service that pulls data from the west cluster and applies to the east nodes.

  - **topology=cluster-slave** [377]
Tells `tpm` this is a cluster-slave replication service which will have a list of all source cluster nodes available.

- `master-dataservice=west [370]`
  The source cluster dataservice name.

- `slave-dataservice=east [375]`
  The destination cluster dataservice name.

- `thl-port=2115 [376]`
  The network port for THL operations.

**Note**

Do not include `start-and-report=true [373]` if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication ‘In-Place’” for next steps after completing installation.

2. Create the two clusters:

   a. Install the Continuent Tungsten package `.rpm`, or download the compressed tarball and unpack it:

```
shell> cd /opt/continuent/software
shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
```

   b. Change to the Continuent Tungsten staging directory:

```
shell> cd continuent-tungsten-2.0.5-11
```

   c. Run `tpm` to install the Clustering software with the INI-based configuration:

```
shell> ./tools/tpm install
```

During the installation and startup, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

3. Install the cluster-to-cluster bi-directional replication:

   a. Install the Tungsten Replicator package or download the Tungsten Replicator tarball, and unpack it:

```
shell> cd /opt/continuent/software
shell> tar zxf tungsten-replicator-3.0.0-524.tar.gz
```

   b. Change to the Tungsten Replicator staging directory:

```
shell> cd tungsten-replicator-3.0.0-524
```

   c. Run `tpm` to install the Tungsten Replicator software with the INI-based configuration:

```
shell> ./tools/tpm install
```

During the installation and startup, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

4. Initialize your `PATH` and environment:

```
shell> source /opt/continuent/share/env.sh
shell> source /opt/replicator/share/env.sh
```

The MSMM clustering should be installed and ready to use.

**3.2.3. Best Practices: Multisite/Multimaster Clusters**

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.
When data is inserted on the master within the east Continuent Tungsten service and west Tungsten Replicator service (on east(1,2,3)), the sequence number of the east Continuent Tungsten service and west Tungsten Replicator service are relative to each other.

When data is inserted on east, the sequence number of the east Continuent Tungsten service and east Tungsten Replicator service (on east(1,2,3)) should be compared.

When data is inserted on west, the sequence number of the west Continuent Tungsten service and west Tungsten Replicator service (on east(1,2,3)) should be compared.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Continuent Tungsten Service Seqno</th>
<th>Tungsten Replicator Service Seqno</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert/update data on east</td>
<td>Seqno Increment</td>
<td>Seqno Increment</td>
</tr>
</tbody>
</table>

Note

In addition to this information, follow the guidelines in Section 2.5, “Best Practices”.

- Running a Multisite/Multimaster service uses many different components to keep data updated on all servers. Monitoring the dataservice is divided into monitoring the two different clusters. Be mindful when using commands that you have the correct path. You should either use the full path to the command under /opt/continuent and /opt/replicator, or use the aliases created by setting the --executable-prefix=mm in [Tungsten Replicator 2.2 Manual] option. Calling trepctl would become mm_trepctl.

- Configure your database servers with distinct auto_increment_increment and auto_increment_offset settings. Each location that may accept writes should have a unique offset value.

Using cctrl gives you the dataservice status individually for the east and west dataservice. For example, the east dataservice is shown below:

```
Continuent Tungsten 2.8.5 build 11
east: session established
[LOGICAL] /east > 1s
COORDINATOR[east1:AUTOMATIC:ONLINE]

ROUTERS:
[-1] connector@east1[17951](ONLINE, created=0, active=0)
[-1] connector@east2[17933](ONLINE, created=0, active=0)
[-1] connector@east3[17943](ONLINE, created=0, active=0)

DATASOURCES:
[-] east1(master:ONLINE, progress=29, THL latency=0.739)
[STATUS [OK] [2013/11/25 11:24:35 AM GMT]
  | MANAGER(state=ONLINE)
  | REPLICATOR(role=master, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)
  |]

[-] east2(slave:ONLINE, progress=29, latency=0.721)
[STATUS [OK] [2013/11/25 11:24:39 AM GMT]
  | MANAGER(state=ONLINE)
  | REPLICATOR(role=slave, master=east1, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)
  |]

[-] east3(slave:ONLINE, progress=29, latency=1.141)
[STATUS [OK] [2013/11/25 11:24:38 AM GMT]
  | MANAGER(state=ONLINE)
  | REPLICATOR(role=slave, master=east1, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)
```

When checking the current status, it is important to compare the sequence numbers from each service correctly. There are four services to monitor, the Continuent Tungsten service east, and a Tungsten Replicator service east that reads data from the west Continuent Tungsten service. A corresponding west Continuent Tungsten and east Tungsten Replicator service.

- When data is inserted on the master within the east Continuent Tungsten, use cctrl to determine the cluster status. Sequence numbers within the Continuent Tungsten east should match, and latency between hosts in the Continuent Tungsten service are relative to each other.

- When data is inserted on east, the sequence number of the east Continuent Tungsten service and east Tungsten Replicator service (on east(1,2,3)) should be compared.

- When data is inserted on the master within the east Continuent Tungsten, use cctrl to determine the cluster status. Sequence numbers within the Continuent Tungsten east should match, and latency between hosts in the Continuent Tungsten service are relative to each other.

- When data is inserted on west, the sequence number of the west Continuent Tungsten service and west Tungsten Replicator service (on east(1,2,3)) should be compared.
Deployment: MySQL Topologies

<table>
<thead>
<tr>
<th>Operation</th>
<th>Continenent Tungsten Service Seqno</th>
<th>Tungsten Replicator Service Seqno</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert/update data on west</td>
<td>east Seqno Increment</td>
<td>east Seqno Increment</td>
</tr>
</tbody>
</table>

Within each cluster, `cctrl` can be used to monitor the current status. For more information on checking the status and controlling operations, see Section 5.3, "Checking Dataservice Status".

**Note**

For convenience, the shell PATH can be updated with the tools and configuration. With two separate services, both environments must be updated. To update the shell with the Continenent Tungsten service and tools:

```
shell> source /opt/continuent/share/env.sh
```

To update the shell with the Tungsten Replicator service and tools:

```
shell> source /opt/replicator/share/env.sh
```

To monitor all services and the current status, you can also use the `multi_trepctl` command (part of the Tungsten Replicator installation). This generates a unified status report for all the hosts and services configured:

```
shell> multi_trepctl --by-service

<table>
<thead>
<tr>
<th>host</th>
<th>servicename</th>
<th>role</th>
<th>state</th>
<th>appliedlastseqno</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>east1</td>
<td>east</td>
<td>master</td>
<td>ONLINE</td>
<td>53</td>
<td>120.161</td>
</tr>
<tr>
<td>east3</td>
<td>east</td>
<td>master</td>
<td>ONLINE</td>
<td>44</td>
<td>6.697</td>
</tr>
<tr>
<td>east2</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>53</td>
<td>119.961</td>
</tr>
<tr>
<td>west1</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>53</td>
<td>119.834</td>
</tr>
<tr>
<td>west2</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>53</td>
<td>181.128</td>
</tr>
<tr>
<td>west3</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>53</td>
<td>204.790</td>
</tr>
<tr>
<td>west1</td>
<td>west</td>
<td>master</td>
<td>ONLINE</td>
<td>294327</td>
<td>0.285</td>
</tr>
<tr>
<td>west2</td>
<td>west</td>
<td>master</td>
<td>ONLINE</td>
<td>231595</td>
<td>0.316</td>
</tr>
<tr>
<td>east1</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>294327</td>
<td>0.879</td>
</tr>
<tr>
<td>east2</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>294327</td>
<td>0.567</td>
</tr>
<tr>
<td>east3</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>294327</td>
<td>1.046</td>
</tr>
<tr>
<td>west3</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>231595</td>
<td>22.895</td>
</tr>
</tbody>
</table>
```

In the above example, it can be seen that the west services have a much higher applied last sequence number than the east services, this is because all the writes have been applied within the west Cluster.

To monitor individual servers and/or services, use `trepctl`, using the correct port number and servicename. For example, on east1 to check the status of the replicator within the Continenent Tungsten service:

```
shell> trepctl status
```

To check the Tungsten Replicator service, explicitly specify the port and service:

```
shell> mm_trepctl -service west status
```

### 3.2.4. Configuring Startup on Boot

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Because there are two different Continenent services running, each must be individually configured to startup on boot:

- For the Continenent Tungsten service, use Section 4.3, "Configuring Startup on Boot".
- For the Tungsten Replicator service, a custom startup script must be created, otherwise the replicator will be unable to start as it has been configured in a different directory.

1. Create a link from the Tungsten Replicator service startup script in the operating system startup directory (`/etc/init.d`):
```
shell> sudo ln -s /opt/replicator/tungsten/tungsten-replicator/bin/replicator /etc/init.d/mmreplicator
```

2. Modify the `APP_NAME` variable within the startup script (`/etc/init.d/mmreplicator`) to `mmreplicator`:
```
APP_NAME="mmreplicator"
```

3. Update the operating system startup configuration to use the updated script.
On Debian/Ubuntu:

shell> sudo update-rc.d mmreplicator defaults

On RedHat/CentOS:

shell> sudo checkconfig --add mmreplicator

3.2.5. Resetting a single dataservice

Warning

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Under certain conditions, dataservices in a multimaster configuration may drift and/or become inconsistent with the data in another dataservice. If this occurs, you may need to re-provision the data on one or more of the dataservices after first determining the definitive source of the information.

In the following example the west service has been determined to be the definitive copy of the data. To fix the issue, all the datasources in the east service will be reprovisioned from one of the datasources in the west service.

The following is a guide to the steps that should be followed. In the example procedure it is the east Service that has failed:

1. Put the dataservice into MAINTENANCE mode. This ensures that Continuent Tungsten will not attempt to automatically recover the service.
   
   cctrl [east]> set policy maintenance

2. On the east, failed, Continuent Tungsten service, put each Tungsten Connector offline:
   
   cctrl [east]> router * offline

3. Reset the failed Tungsten Replicator service on all servers connected to the failed Continuent Tungsten service. For example, on west{1,2,3} reset the east Tungsten Replicator service:

   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east offline
   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east reset -all -y

4. Reset the Continuent Tungsten service on each server within the failed region [east{1,2,3}]:

   shell east> /opt/continuent/tungsten/tungsten-replicator/bin/replicator stop
   shell east> /opt/continuent/tungsten/tools/tpm reset east
   shell east> /opt/continuent/tungsten/tungsten-replicator/bin/replicator start

5. Restore a backup on each host [east{1,2,3}] in the failed east service from a host in the west service:

   shell east> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave
   --direct --source=west1
   shell east> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave
   --direct --source=west1 --force

6. Place all the Tungsten Replicator services on west{1,2,3} back online:

   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east online

7. On the east, failed, Continuent Tungsten service, put each Tungsten Connector online:
   
   cctrl [east]> router * online

8. Set the policy back to automatic:
   
   cctrl> set policy automatic

3.2.6. Resetting all dataservices

Warning

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.
For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

To reset all of the dataservices and restart the Continuent Tungsten and Tungsten Replicator services:

On all hosts (e.g. east{1,2,3} and west{1,2,3}):

```
shell> /opt/replicator/tungsten/tungsten-replicator/bin/replicator stop
shell> /opt/replicator/tungsten/tools/tpm reset
shell> /opt/continuent/tungsten/tools/tpm reset
shell> /opt/replicator/tungsten/tungsten-replicator/bin/replicator start
```

---

### 3.2.7. Adding a new Cluster/Dataservice

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

To add an entirely new cluster (dataservice) to the mesh, follow the below simple procedure.

**Note**

There is no need to set the Replicator starting points, and no downtime/maintenance window is required!

1. Choose a cluster to take a node backup from:
   - Choose a cluster and slave node to take a backup from.
   - Enable maintenance mode for the cluster:
     ```
     shell> cctrl
cctrl> set policy maintenance
     ```
   - Shun the selected slave node and stop both local and cross-site replicator services:
     ```
     shell> cctrl
cctrl> datasource {slave_hostname_here} shun
     slave shell> trepctl offline
     slave shell> replicator stop
     slave shell> mm_trepctl offline
     slave shell> mm_replicator stop
     ```
   - Take a backup of the shunned node, then copy to/restore on all nodes in the new cluster.
   - Recover the slave node and put cluster back into automatic mode:
     ```
     slave shell> replicator start
     slave shell> trepctl online
     slave shell> mm_repl start
     slave shell> mm_trepctl online
     shell> cctrl
cctrl> datasource {slave_hostname_here} online
cctrl> set policy automatic
     ```

2. On ALL nodes in all three (3) clusters, ensure the `/etc/tungsten/tungsten.ini` has all three clusters defined and all the correct cross-site combinations.

3. Install the Tungsten Clustering software on new cluster nodes to create a single standalone cluster and check the `cctrl` command to be sure the new cluster is fully online.

4. Install the Tungsten Replicator software on all new cluster nodes and start it.

Replication will now be flowing INTO the new cluster from the original two.

5. On the original two clusters, run `tools/tpm update` from the cross-site replicator staging software path:

```
shell> mm_tpm query staging
shell> cd {replicator_staging_directory}
shell> tools/tpm update --replace-release
shell> mm_trepctl online
shell> mm_trepctl services
```

Check the output from the `mm_trepctl services` command output above to confirm the new service appears and is online.
Note

There is no need to set the cross-site replicators at a starting position because:

- Replicator feeds from the new cluster to the old clusters start at seqno 0.
- The tungsten_olda and tungsten_oldb database schemas will contain the correct starting points for the INBOUND feed into the new cluster, so when the cross-site replicators are started and brought online they will read from the tracking table and carry on correctly from the stored position.

3.2.8. Enabling SSL for Replicators Only

Warning

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

It is possible to enable secure communications for just the Replicator layer in a MSMM topology. This would include both the Cluster Replicators and the Cross-Site Replicators because they cannot be SSL-enabled independently.

1. Create a certificate and load it into a java keystore, and then load it into a truststore and place all files into the /etc/tungsten/ directory. For detailed instructions, see Section 2.7.1.1, “Creating Your Own Client and Server Certificates”

2. Update /etc/tungsten/tungsten.ini to include these additional lines in the both the defaults section and the defaults.replicator section:

```ini
[defaults]
... java-keystore-path=/etc/tungsten/keystore.jks
java-keystore-password=secret
java-truststore-path=/etc/tungsten/truststore.ts
java-truststore-password=secret
thl-ssl=true

[defaults.replicator]
... java-keystore-path=/etc/tungsten/keystore.jks
java-keystore-password=secret
java-truststore-path=/etc/tungsten/truststore.ts
java-truststore-password=secret
thl-ssl=true
```

3. Put all clusters into maintenance mode.

```
shell> cctrl
cctrl> set policy maintenance
```

4. On all hosts, update the cluster configuration:

```
shell> tpm query staging
cshell> cd {cluster_staging_directory}
cshell> tools/tpm update
cshell> trepctl online
cshell> trepctl status | grep thl
```

On all hosts, update the cross-site replicator configuration:

```
shell> mm_tpm query staging
cshell> cd {replicator_staging_directory}
cshell> tools/tpm update
cshell> mm_trepctl online
cshell> mm_trepctl status | grep thl
```

Important

Please note that all replication will effectively be down until all nodes/services are SSL-enabled and online.

5. Once all the updates are done and the Replicators are back up and running, use the various commands to check that secure communications have been enabled.

Each datasource will show [SSL] when enabled:

```
shell> cctrl
cctrl> ls
```
Both the local cluster replicator status command `trepctl status` and the cross-site replicator status command `mm_trepctl status` will show **thls** instead of **thl** in the values for `masterConnectUri`, `masterListenUri` and `pipelineSource`.

```
shell> trepctl status | grep thl
masterConnectUri       : thls://db1:2112/
masterListenUri        : thls://db5:2112/
pipelineSource         : thls://db1:2112/
```

### 3.2.9. Provisioning during live operations

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

In the event of a failure within one host in the service where you need to reprovision the host from another running slave:

- Identify the servers that are failed. All servers that are not the master for their region can be re-provisioned using a backup/restore of the master (see Section 5.9, "Creating a Backup" or using the `tungsten_provision_slave` script.
- To re-provision an entire region, follow the steps below. The **east** region is used in the example statements below:

1. To prevent application servers from reading and writing to the failed service, place the Tungsten Connector offline within the failed region:
   ```
cctrl [east]> router * offline
```

2. On all servers in other regions (**west{1,2,3}**):
   ```
shell> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east offline
shell> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east reset -all -y
```

3. On all servers in the failed region (**east{1,2,3}**):
   ```
shell> /opt/replicator/tungsten/tungsten-replicator/bin/replicator stop
shell> /opt/replicator/tungsten/tools/tpm reset
shell> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave --direct --source=west1
```

4. Check that Continuent Tungsten is working correctly and all hosts are up to date:
   ```
cctrl [east]> ls
```

5. Restart the Tungsten Replicator service:
6. On all servers in other regions (west1,2,3):
   - shell> /opt/replicator/tungsten/tungsten-replicator/bin/replicator start

3.2.10. Dataserver maintenance

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

To perform maintenance on the dataservice, for example to update the MySQL configuration file, can be achieved in a similar sequence to that shown in Section 5.14, “Performing Database or OS Maintenance”, except that you must also restart the corresponding Tungsten Replicator service after the main Continuent Tungsten service has been placed back online.

For example, to perform maintenance on the **east** service:

1. Put the dataservice into **MAINTENANCE** mode. This ensures that Continuent Tungsten will not attempt to automatically recover the service.
   - cctrl [east]> set policy maintenance

2. Shun the first slave datasource so that maintenance can be performed on the host.
   - cctrl [east]> datasource east1 shun

3. Perform the updates, such as updating **my.cnf**, changing schemas, or performing other maintenance.

4. If MySQL configuration has been modified, restart the MySQL service:
   - cctrl [east]> service host/mysql restart

5. Bring the host back into the dataservice:
   - cctrl [east]> datasource host recover

6. Perform a switch so that the master becomes a slave and can then be shunned and have the necessary maintenance performed:
   - cctrl [east]> switch

7. Repeat the previous steps to shun the host, perform maintenance, and then switch again until all the hosts have been updated.

8. Set the policy back to automatic:
   - cctrl> set policy automatic

9. On each host in the other region, manually restart the Tungsten Replicator service, which will have gone offline when MySQL was restarted:
   - shell> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -host host -service east online

### 3.2.10.1. Fixing Replication Errors

In the event of a replication fault, the standard `cctrl`, `trepctl` and other utility commands in Chapter 8, Command-line Tools can be used to bring the dataservice back into operation. All the tools are safe to use.

If you have to perform any updates or modifications to the stored MySQL data, ensure binary logging has been disabled using:

```sql
mysql> SET SESSION SQL_LOG_BIN=0;
```

Before running any commands. This prevents statements and operations reaching the binary log so that the operations will not be replicated to other hosts.

### 3.3. Deploying a Composite Cluster

Continuent Tungsten supports the creation of composite clusters. This includes multiple master/slave dataservices tied together. One of the dataservices is identified as the master and all other dataservices replicate from it.
3.3.1. Prepare: Composite Cluster

Before continuing with deployment you will need the following:

1. The cluster name for each Master/Slave Cluster and a composite cluster name to group them.
2. The list of datasources in each cluster. These are the servers which will be running MySQL.
3. The list of servers that will run the connector. Each connector will be associated with a preferred cluster but will have access to the master regardless of location.
4. The username and password of the MySQL replication user.
5. The username and password of the first application user. You may add more users after installation.

All servers must be prepared with the proper prerequisites. See Section 2.6, "Prepare Hosts" and Appendix C, Prerequisites for additional details.

3.3.2. Install: Composite Cluster

- Staging Configuration - Section 3.3.2.1, "Installing a Composite Configuration (Staging Use Case)"
- INI Configuration - Section 3.3.2.2, "Installing a Composite Configuration (INI Use Case)"

3.3.2.1. Installing a Composite Configuration (Staging Use Case)

1. Install the Continuent Tungsten package or download the Continuent Tungsten tarball, and unpack it:

```
shell> cd /opt/continuent/software
shell> tar xzf continent-tungsten-2.0.5-11.tar.gz
```

2. Change to the Continuent Tungsten directory:
3. Run `tpm` to perform the installation. This method assumes you are using the Section 9.3, "tpm Staging Configuration" method:

```
sh> cd continuent-tungsten2.0.5-11

sh> ./tools/tpm configure defaults \
   --user=tungsten \ 
   --install-directory=/opt/continuent \ 
   --replication-user=tungsten \ 
   --replication-password=secret \ 
   --replication-port=13306 \ 
   --application-user=app_user \ 
   --application-password=password \ 
   --application-port=3306 \ 
   --replication-port=13306 \ 
   --profile-script="/opt/continuent/.bashrc" \ 
   --start-and-report

sh> ./tools/tpm configure alpha \
   --topology=clustered \ 
   --members=host1.alpha,host2.alpha,host3.alpha \ 
   --connectors=host1.alpha,host2.alpha,host3.alpha \ 
   --master=host1.alpha

sh> ./tools/tpm configure beta \
   --topology=clustered \ 
   --members=host1.beta,host2.beta,host3.beta \ 
   --connectors=host1.beta,host2.beta,host3.beta \ 
   --master=host1.beta \ 
   --relay-source=alpha

sh> ./tools/tpm configure gamma \
   --composite-datasources=alpha,beta
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- **tpm configure defaults**

  This runs the `tpm` command. `configure defaults` indicates that we are setting options which will apply to all dataservices.

  - **--user=tungsten [377]**

    The operating system user name that you have created for the Tungsten service, `tungsten`.

  - **--install-directory=/opt/continuent [359]**

    The installation directory of the Tungsten service. This is where the service will be installed on each server in your dataservice.

  - **--replication-user=tungsten [370]**

    The MySQL user name to use when connecting to the MySQL database.

  - **--replication-password=secret [370]**

    The MySQL password for the user that will connect to the MySQL database.

  - **--replication-port=13306 [370]**

    The TCP/IP port that the MySQL database is listening on for connections.

  - **--application-user=app_user [345]**

    The application user name.

  - **--application-password=password [344]**

    The application password.

  - **--application-port=3306 [345]**

    The TCP/IP port on which to listen for incoming connections by the Tungsten connector service. To emulate the standard MySQL database service, port 3306 is used.

  - **--start-and-report [373]**

    Tells `tpm` to startup the service, and report the current configuration and status.
Deployment: MySQL Topologies

- `--profile-script` [368]
  Tells `tpm` to add PATH information to the script to initialize the environment.

- `tpm configure alpha`
  This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `alpha` is the name and identity of the dataservice being created.

- `--topology=clustered` [377]
  Tells `tpm` this is a clustered dataservice.

- `--members=host1.alpha,host2.alpha,host3.alpha` [362]
  A comma separated list of all the hosts that are part of this dataservice.

- `--connectors=host1.alpha,host2.alpha,host3.alpha` [351]
  A comma separated list of the hosts that will have a connector service created on them.

- `--master=host1.alpha` [361]
  The hostname of the server that will be the default master MySQL server.

- `tpm configure beta`
  This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `beta` is the name and identity of the dataservice being created.

- `--topology=clustered` [377]
  Tells `tpm` this is a clustered dataservice.

- `--members=host1.beta,host2.beta,host3.beta` [362]
  A comma separated list of all the hosts that are part of this dataservice.

- `--connectors=host1.beta,host2.beta,host3.beta` [351]
  A comma separated list of the hosts that will have a connector service created on them.

- `--relay=host1.beta` [361]
  The hostname of the server that will be the default master MySQL server.

- `--relay-source=alpha` [370]
  The dataservice that should be the master by default after installation.

- `tpm configure gamma`
  This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `gamma` is the name and identity of the dataservice being created.

- `--composite-datasources=alpha,beta` [348]
  A comma separated list of the dataservices to be linked together.

Note

Do not include `--start-and-report` [373] if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication ‘In-Place’” for next steps after completing installation.

### 4. Run `tpm` to install the software with the configuration.

```bash
shell $ ./tools/tpm install
```

During the startup and installation, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

### 5. Initialize your `PATH` and environment.
3.3.2.2. Installing a Composite Configuration [INI Use Case]

1. Install the Continuent Tungsten™ package [.rpm], or download the compressed tarball and unpack it:

   ```
   shell> cd /opt/continuent/software
   shell> tar zxf continuum-tungsten-2.0.5-11.tar.gz
   ```

2. Change to the Continuent Tungsten directory:

   ```
   shell> cd continuum-tungsten2.0.5-11
   ```

3. Create `/etc/tungsten/tungsten.ini` with the appropriate configuration:

   ```
   [defaults]
   user=tungsten
   install-directory=/opt/continuent
   replication-user=tungsten
   replication-password=secret
   replication-port=13306
   application-user=app_user
   application-password=password
   application-port=3306
   profile-script="~/.bashrc"
   start-and-report
   [alpha]
   topology=clustered
   members=host1.alpha,host2.alpha,host3.alpha
   connectors=host1.alpha,host2.alpha,host3.alpha
   master=host1.alpha
   [beta]
   topology=clustered
   members=host1.beta,host2.beta,host3.beta
   connectors=host1.beta,host2.beta,host3.beta
   relay=host1.beta
   relay-source=alpha
   [gamma]
   composite-datasources=alpha,beta
   ```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument:

- **[defaults]**
  - `defaults` indicates that we are setting options which will apply to all dataservices.
  - `user=tungsten` [377]
    - The operating system user name that you have created for the Tungsten service, `tungsten`.
  - `install-directory=/opt/continuent` [359]
    - The installation directory of the Tungsten service. This is where the service will be installed on each server in your dataservice.
  - `replication-user=tungsten` [370]
    - The MySQL user name to use when connecting to the MySQL database.
  - `replication-password=secret` [370]
    - The MySQL password for the user that will connect to the MySQL database.
  - `replication-port=13306` [370]
    - The TCP/IP port that the MySQL database is listening on for connections.
  - `application-user=app_user` [345]
    - The application user name.
  - `application-password=password` [344]
The application password.

- **application-port=3306**
  The TCP/IP port on which to listen for incoming connections by the Tungsten connector service. To emulate the standard MySQL database service, port 3306 is used.

- **start-and-report**
  Tells tpm to startup the service, and report the current configuration and status.

- **profile-script**
  Tells tpm to add PATH information to the script to initialize the environment.

- ![alpha]
  alpha is the name and identity of the dataservice being created.

- **topology=clustered**
  Tells tpm this is a clustered dataservice.

- **members=host1.alpha,host2.alpha,host3.alpha**
  A comma separated list of all the hosts that are part of this dataservice.

- **connectors=host1.alpha,host2.alpha,host3.alpha**
  A comma separated list of the hosts that will have a connector service created on them.

- **master=host1.alpha**
  The hostname of the server that will be the default master MySQL server.

- ![beta]
  beta is the name and identity of the dataservice being created.

- **topology=clustered**
  Tells tpm this is a clustered dataservice.

- **members=host1.beta,host2.beta,host3.beta**
  A comma separated list of all the hosts that are part of this dataservice.

- **connectors=host1.beta,host2.beta,host3.beta**
  A comma separated list of the hosts that will have a connector service created on them.

- **relay=host1.beta**
  The hostname of the server that will be the default master MySQL server.

- **relay-source=alpha**
  The dataservice that should be the master by default after installation.

- ![gamma]
  gamma is the name and identity of the dataservice being created.

- **composite-datasources=alpha,beta**
  A comma separated list of the dataservices to be linked together.

**Note**

Do not include **start-and-report** if you are taking over for MySQL native replication. See Section 3.8.1, “Migrating from MySQL Native Replication In-Place” for next steps after completing installation.
4. Run `tpm` to install the software with the INI-based configuration:

```
shell> ./tools/tpm install
```

During the startup and installation, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

5. Initialize your `PATH` and environment.

```
shell> source /opt/continuent/share/env.sh
```

The Composite cluster should be installed and ready to use.

### 3.3.3. Best Practices: Composite Cluster

Follow the guidelines in Section 2.5, “Best Practices”.

### 3.4. Deploying Tungsten Connector Only

An independent Tungsten Connector installation can be useful when you want to create a connector service that provides HA and load balancing, but which operates independently of the main cluster. Specifically, this solution is used within disaster recovery and multi-site operations where the connector may be operating across site-boundaries independently of the dataservice at each site.

The independent nature is in terms of the configuration of the overall service through `tpm`: an independent connector configured to communicate with existing cluster hosts will be managed by the managers of the cluster. But, the connector will not be updated when performing a `tpm update` operation within the configured cluster. This allows the connector to work through upgrade procedures to minimize downtime.

To create an independent connector, `tpm` is used to create a definition for a cluster including the datasources, and specifying only a single connector host, then installing Continuent Tungsten on only the connector host. Failure to configure in this way, and `tpm` will install a full Continuent Tungsten service across all the implied members of the cluster.

Installation can be configured using the staging directory method of `tpm` as follows:

1. On your staging server, download the release package.

2. Unpack the release package:

```
shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
```

3. Change to the unpackaged directory:

```
shell> cd continuent-tungsten-2.0.5-11
```

4. Configure Continuent Tungsten using the staging directory method:

```
shell> ./tools/tpm configure alpha
--user=tungsten
--install-directory=/opt/continuent
--replication-port=13306
--application-port=3306
--application-user=app_user
--application-password=password
--mysql-connectorj-path=/usr/share/java/mysql-connector-java-bin.jar
--members=host1,host2,host3
--connectors=`hostname`
```

The above creates a configuration specifying the datasources, `host{1,2,3}`, and a single connector host based on the hostname of the installation host. Note that the application and datasource port configuration are the same as required by a typical Continuent Tungsten configuration. The values above are identical to those used in Section 3.1, “Deploying a Master/Slave Cluster” deployment.

**Warning**

As of Continuent Tungsten v4.0.0, the parameter `--mysql-connectorj-path` is no longer required because the Drizzle driver is the new default.

5. Now execute the installation, only installing the service on the current host, again using `hostname`:

```
shell> ./tools/tpm install --hosts=`hostname`
```

---

72
Deployment: MySQL Topologies

```bash
tools/tpm start --hosts=connector2
```

Wait a minute for the services to start up and configure themselves. After that you may proceed.

Once your services start successfully you may begin to use the cluster. To look at services and perform administration, run the following command from any database server.

```
$CONTINUENT_ROOT/tungsten/tungsten-manager/bin/cctrl
```

Configuration is now complete. For further information, please consult Tungsten documentation, which is available at docs.continuent.com.

**NOTE** >> Command successfully completed

If the installation process fails, check the output of the `/tmp/tungsten-configure.log` file for more information about the root cause.

6. Start the connector service:

```bash
shell> ./tools/tpm start alpha --hosts=connector
```

When using the INI file method of deployment, create a file containing the list of members, listing the current host as the only connector:

1. Download and extract the Continuent Tungsten distribution, and change into the distribution directory. See Section 2.3, “Deployment Sources” for more information.

2. Create the INI file `/etc/tungsten/tungsten.ini` with the following contents:

```ini
[defaults]
application-password=password
application-user=app_user
install-directory=/opt/continuent
replication-port=13306
user=tungsten

[alpha]
connectors=connector
master=host1
members=host2,host2,host3
```

3. Install the connector:

```bash
shell> ./tools/tpm install
```

4. Start the connector:

```bash
shell> ./tools/tpm start
```

Once started:

- The connector will appear, and be managed by, any manager host using the `cctrl` tool. For example:

```bash
[LOGICAL] /dsone > ls
COORDINATOR[host1:AUTOMATIC:ONLINE]

ROUTERS:
+----------------------------------------------------------------------------+
|connector@connector2[16019](ONLINE, created=0, active=0)                    |
|connector@host1[18450](ONLINE, created=19638, active=0)                     |
|connector@host2[1995](ONLINE, created=0, active=0)                          |
|connector@host3[8895](ONLINE, created=0, active=0)                          |
+----------------------------------------------------------------------------+
```

- The active status of the connector can be monitored using `cctrl` as normal.

- Updates to the main cluster will not update the Continuent Tungsten of the standalone connector. The standalone must be updated independently of the remainder of the Continuent Tungsten dataservice.

- Connector can be accessed using the connector host and specified port:

```bash
shell> mysql -utungsten -p -hconnector -P3306
```

- The `user.map` authorization file must be created and managed separately on standalone connectors. For more information, see Section 6.6, “User Authentication”
3.5. Deploying Additional Datasources, Managers, or Connectors

3.5.1. Adding Datasources to an Existing Deployment

1. Ensure the new host that is being added has been configured following the Appendix C, Prerequisites.

2. Update the configuration using `tpm`, adding the new host to the list of `--members [362]` and `--hosts [358]` using `+=`, which appends the host to the Existing Deployment:

   ```shell
   ./tools/tpm update alpha --members+=host6 --hosts+=host6
   ```

   If the host will also act as a connector, also add it to the list of connectors:

   ```shell
   ./tools/tpm update alpha --members+=host6 --hosts=host6 --connectors+=host6
   ```

3. Initially, the newly added host will attempt to read the information from the existing THL. If the full THL is not available from the master, the new slave will need to be reprovisioned:
   a. Log into the new host.
   b. Execute `tungsten_provision_slave` to read the information from an existing existing and overwrite the data within the new host:

   ```shell
   shell> tungsten_provision_slave --source=host2
   NOTE >>Put alpha replication service offline
   NOTE >>Create a mysqldump backup of host2 in /opt/continuent/backups/provision_mysqldump_2014-01-17-17-27_96
   NOTE >>host2>>Create mysqldump in /opt/continuent/backups/provision_mysqldump_2014-01-17-17-27_96/provision.sql.gz
   NOTE >>Load the mysqldump file
   NOTE >>Put the alpha replication service online
   NOTE >>Clear THL and relay logs for the alpha replication service
   ```

   Once the new host has been added and re-provision, check the status in `cctr`:
3.5.2. Adding Active Witnesses to an Existing Deployment

To add active witnesses to an Existing Deployment, use `tpm` to update the configuration, adding the list of active witnesses and the list of all members within the updated dataservice configuration.

Active Witness hosts must have been prepared using the notes provided in Appendix C, Prerequisites. Active witnesses must be able to resolve the hostnames of the other managers and hosts in the dataservice. Installation will fail if prerequisites and host availability and stability cannot be confirmed.

To update the configuration:

```
shell> ./tools/tpm update alpha --witnesses=host4 --members+=host4 --enable-active-witnesses=true
```

Once installation has completed successfully, and the manager service has started on each configured active witness, the status can be determined using `ls` within `cctrl`:

```
[LOGICAL] /alpha > ls
COORDINATOR[host1:AUTOMATIC:ONLINE]

ROUTERS:
- connector@host1[20446](ONLINE, created=0, active=0)
- connector@host2[21698](ONLINE, created=0, active=0)
- connector@host3[30354](ONLINE, created=0, active=0)

DATASOURCES:
- host1(slave:ONLINE, progress=8946, latency=0.000)
  | STATUS [OK] [2013/12/05 04:27:47 PM GMT]
  | MANAGER(state=ONLINE)
  | REPLICA(role=slave, master=host3, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)

- host2(slave:ONLINE, progress=8946, latency=0.334)
  | STATUS [OK] [2013/12/05 04:06:59 PM GMT]
  | MANAGER(state=ONLINE)
  | REPLICA(role=slave, master=host3, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)

- host3(master:ONLINE, progress=8946, THL latency=0.331)
  | STATUS [OK] [2013/11/20 05:39:14 PM GMT]
  | MANAGER(state=ONLINE)
  | REPLICA(role=master, state=ONLINE)
  | DATASERVER(state=ONLINE)
  | CONNECTIONS(created=0, active=0)

WITNESSES:
- host4(witness:ONLINE)
  | MANAGER(state=ONLINE)
```

Validation of the cluster with the new witnesses can be verified by using the `cluster validate` command within `cctrl`.

3.5.3. Adding Passive Witnesses to an Existing Deployment

To add passive witness to an existing installation, use `tpm` to update the active configuration.
3.5.4. Adding Connectors to an Existing Deployment

Adding more connectors to an existing installation allows for increased routing capacity. The new connectors will form part of the cluster and be fully aware and communicate with existing managers and datasources within the cluster.

To add more connectors to an existing deployment:

1. On the new host, ensure the Appendix C, Prerequisites have been followed.

2. On the staging host, update the configuration to include the connector host you are adding. For example, to update the list of connector hosts to include host4 on the service alpha:

   ```bash
   shell> ./tools/tpm configure alpha --connectors+=host4
   ``

   The `+=` appends the new host to the list of supported hosts.

3. Update the configuration, which will install the connector on the new host:

   ```bash
   shell> ./tools/tpm update --no-connectors
   ``

   Using the `--no-connectors` option updates the current deployment without restarting the existing connectors.

4. During a period when it is safe to restart the connectors:

   ```bash
   shell> ./tools/tpm promote-connector
   ``

   The status of all the connectors can be monitored using `cctr`.  

3.5.5. Adding a remote Composite Cluster

Adding an entire new cluster provides significant level of availability and capacity. The new cluster nodes that form the cluster will be fully aware of the original cluster(s) and communicate with existing managers and datasources within the cluster.

SUMMARY: On the staging host, update the configuration to include the new hosts, services and optionally a new composite service you are adding. For example, you could have a simple non-composite service you wish to convert to composite, or you could be adding another cluster to an existing composite dataservice.

To add an additional cluster to an existing composite cluster:

1. On the new host(s), ensure the Appendix C, Prerequisites have been followed.

2. Let's assume that we have a composite cluster dataservice called `global` with two clusters, `east` and `west`, with three nodes each, defined as follows:
shell> ./tools/tpm configure defaults \
--application-password=secret \ 
--application-port=3306 \ 
--application-user=app_user \ 
--install-directory=/opt/continuent \ 
--replication-password=secret \ 
--replication-user=tungsten \ 
--skip-validation-check=MySQLPermissionsCheck \ 
--start-and-report=true \ 
--user=tungsten

shell> ./tools/tpm configure east \
--connectors=db1,db2,db3 \ 
--master=db1 \ 
--slaves=db2,db3 \ 
--topology=clustered

shell> ./tools/tpm configure west \
--connectors=db4,db5,db6 \ 
--relay-source=east \ 
--relay=db4 \ 
--slaves=db5,db6 \ 
--topology=clustered

shell> ./tools/tpm configure global \
--composite-datasources=east,west

3. Locate the staging host and directory and go to it

shell> tpm query staging
shell> ssh {staging_host_from_above}
shell> cd {staging_directory_from_above}

4. Set the cluster to maintenance mode using cctrl:

shell> cctrl
[LOGICAL] / > set policy maintenance

5. Add the definition for the new slave cluster service north:

shell> ./tools/tpm configure north \
--connectors=db7,db8,db9 \ 
--relay-source=east \ 
--relay=db7 \ 
--slaves=db8,db9 \ 
--topology=clustered

6. Finally, add the definition for new cluster north to the composite cluster service global:

shell> ./tools/tpm configure global \
--composite-datasources=east,west,north

7. Update the configuration, which will install Tungsten on any new nodes:

shell> ./tools/tpm update --no-connectors -i

Using the --no-connectors option updates the current deployment without restarting the existing connectors.

8. On every node in the original clusters, make sure all replicators are online:

shell> trepctl online; trepctl services

9. Update the old cluster via cctrl to recognize the new cluster (i.e. north):

shell> cctrl -multi
shell> use global
cctrl> create composite datasource north
cctrl> ls

Continuent Tungsten 4.0.5 build 3194890
east: session established
[LOGICAL] / > set policy maintenance
[LOGICAL] /global > ls
COORDINATOR[db1:MAINTENANCE:ONLINE]
DATASOURCES:

Using the --no-connectors option updates the current deployment without restarting the existing connectors.
10. Go to the relay (master) node of the new cluster (i.e. db7) and provision it from a slave of the original cluster (i.e. db2):

```
shell> tungsten_provision_slave --source db2
```

```
tungsten@db7:~  $  tungsten_provision_slave --source db2
NOTE  >> Put north replication service offline
NOTE  >> Create a backup of db2 in /opt/continuent/backups/provision_xtrabackup_2017-01-07_13-53_58
NOTE  >> db2 >> Run innobackupex sending the output to db7:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-53_58
NOTE  >> db2 >> Transfer extra files to db7:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-53_58
NOTE  >> Prepare the files for MySQL to run
NOTE  >> Stop MySQL and empty all data directories
NOTE  >> Stop the MySQL service
NOTE  >> Transfer data files to the MySQL data directory
NOTE  >> Start the MySQL service
NOTE  >> Backup and restore complete
NOTE  >> Put the north replication service online
NOTE  >> Clear THL and relay logs for the north replication service
```

11. Go to a slave node of the new cluster (i.e. db8) and provision it from the relay node of the new cluster (i.e. db7):

```
shell> tungsten_provision_slave --source db7
```

```
tungsten@db8:~  $  tungsten_provision_slave --source db7
NOTE  >> Put north replication service offline
NOTE  >> Create a backup of db7 in /opt/continuent/backups/provision_xtrabackup_2017-01-07_13-54_71
NOTE  >> db7 >> Run innobackupex sending the output to db7:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-54_71
NOTE  >> db7 >> Transfer extra files to db7:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-54_71
NOTE  >> Prepare the files for MySQL to run
NOTE  >> Stop MySQL and empty all data directories
NOTE  >> Stop the MySQL service
NOTE  >> Transfer data files to the MySQL data directory
NOTE  >> Start the MySQL service
NOTE  >> Backup and restore complete
NOTE  >> Put the north replication service online
NOTE  >> Clear THL and relay logs for the north replication service
```

12. Go to a slave node (i.e. db9) of the new cluster and provision it from the newly-provisioned slave node of the new cluster (i.e. db8):

```
shell> tungsten_provision_slave --source db8
```

```
tungsten@db9:~  $  tungsten_provision_slave --source db8
NOTE  >> Put north replication service offline
NOTE  >> Create a backup of db8 in /opt/continuent/backups/provision_xtrabackup_2017-01-07_13-55_78
NOTE  >> db8 >> Run innobackupex sending the output to db8:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-55_78
NOTE  >> db8 >> Transfer extra files to db8:/opt/continuent/backups/provision_xtrabackup_2017-01-07_13-55_78
NOTE  >> Prepare the files for MySQL to run
NOTE  >> Stop MySQL and empty all data directories
NOTE  >> Stop the MySQL service
NOTE  >> Transfer data files to the MySQL data directory
NOTE  >> Clear THL and relay logs for the north replication service
```
Deployment: MySQL Topologies

13. Set the composite cluster to automatic mode using `cctrl`:

```
shell> cctrl -multi
[LOGICAL] / > set policy automatic
```

14. During a period when it is safe to restart the connectors:

```
shell> ./tools/tpm promote-connector
```

To convert from a single cluster to a composite cluster:

1. On the new host(s), ensure the Appendix C, Prerequisites have been followed.

2. Let's assume that we have a single cluster dataservice called `east` with three nodes, defined as follows:

```
shell> ./tools/tpm configure east
 --connectors=db1,db2,db3
 --master=db1
 --slaves=db2,db3
 --topology=clustered
```

3. Locate the staging host and directory and go to it

```
shell> tpm query staging
shell> ssh {staging_host_from_above}
shell> cd {staging_directory_from_above}
```

4. Set the cluster to maintenance mode using `cctrl`:

```
shell> cctrl
[LOGICAL] / > set policy maintenance
```

5. Add the definition for the new slave cluster service `west`:

```
shell> ./tools/tpm configure west
 --connectors=db4,db5,db6
 --relay-source=east
 --relay=db4
 --slaves=db5,db6
 --topology=clustered
```

6. Finally, add the definition for the composite cluster service `global`:

```
shell> ./tools/tpm configure global
 --composite-datasources=east,west
```

7. Update the configuration, which will install Tungsten on any new nodes:

```
shell> ./tools/tpm update --no-connectors -i
```

Using the `--no-connectors` option updates the current deployment without restarting the existing connectors.

8. On every node in the original cluster, make sure all replicators are online:

```
shell> trepctl online; trepctl services
```

9. Update the old cluster via `cctrl` to create the new composite cluster (i.e. `global`):

```
shell> cctrl -multi
 cctrl> create composite dataservice global
 cctrl> use global
 cctrl> create composite datasource east
 cctrl> create composite datasource west
 cctrl> ls
```

```
tungsten@db1:~  $ cctrl -multi
```

79
10. Go to the relay (master) node of the new cluster (i.e. db4) and provision it from a slave of the original cluster (i.e. db2):

```
shell> tungsten_provision_slave --source db2
```

```
tungsten@db4:~ $ tungsten_provision_slave --source db2
NOTE >> Put west replication service offline
NOTE >> Create a backup of db2 in /opt/continuent/backups/provision_xtrabackup_2017-01-06_21-47_55
NOTE >> db2 >> Run innobackupex sending the output to db4:/opt/continuent/backups/provision_xtrabackup_2017-01-06_21-47_55
NOTE >> db2 >> Transfer extra files to db4:/opt/continuent/backups/provision_xtrabackup_2017-01-06_21-47_55
NOTE >> Prepare the files for MySQL to run
NOTE >> Stop MySQL and empty all data directories
NOTE >> Stop the MySQL service
NOTE >> Transfer data files to the MySQL data directory
NOTE >> Start the MySQL service
NOTE >> Backup and restore complete
NOTE >> Put the west replication service online
NOTE >> Clear THL and relay logs for the west replication service
```

11. Go to a slave node of the new cluster (i.e. db5) and provision it from the relay node of the new cluster (i.e. db4):

```
shell> tungsten_provision_slave --source db4
```

```
tungsten@db5:~ $ tungsten_provision_slave --source db4
NOTE >> Put west replication service offline
NOTE >> Create a backup of db4 in /opt/continuent/backups/provision_xtrabackup_2017-01-06_21-54_94
NOTE >> db4 >> Run innobackupex sending the output to db5:/opt/continuent/backups/provision_xtrabackup_2017-01-06_21-54_94
```
12. Go to a slave node (i.e. db6) of the new cluster and provision it from the newly-provisioned slave node of the new cluster [i.e. db5]:

```
shell> tungsten_provision_slave --source db5
```

13. Set the composite cluster to automatic mode using cctrl:

```
shell> cctrl -multi
[LOGICAL] / > set policy automatic
```

14. During a period when it is safe to restart the connectors:

```
shell> ./tools/tpm promote-connector
```

### 3.6. Replicating Data Into an Existing Dataservice

If you have an existing dataservice, data can be replicated from a standalone MySQL server into the service. The replication is configured by creating a service that reads from the standalone MySQL server and writes into the cluster through a connector attached to your dataservice. By writing through the connector, changes to the underlying dataservice topology can be handled.

Additionally, using a replicator that writes data into an existing data service can be used when migrating from an existing service into a new Continuent Tungsten service. For more information on initially provisioning the data for this type of operation, see Section 5.11.2, “Migrating from MySQL Native Replication Using a New Service”.

![Figure 3.4. Topologies: Replicating into a Dataservice](image)

In order to configure this deployment, there are two steps:

1. Create a new replicator on the source server that extracts the data.
2. Create a new replicator that reads the binary logs directly from the external MySQL service through the connector.
There are also the following requirements:

- The host on which you want to replicate to must have Tungsten Replicator 5.3.0 or later.
- Hosts on both the replicator and cluster must be able to communicate with each other.
- The replication user on the source host must have the `RELOAD`, `REPLICATION SLAVE`, and `REPLICATION CLIENT GRANT` privileges.
- Replicator must be able to connect as the `tungsten` user to the databases within the cluster.
- When writing into the master through the connector, the user must be given the correct privileges to write and update the MySQL server. For this reason, the easiest method is to use the `tungsten` user, and ensure that that user has been added to the `user.map`:

```
tungsten secret alpha
```

Install the Tungsten Replicator package (see Section 2.3.2, “Using the RPM and DEB package files”), or download the compressed tarball and unpack it on `host1`:

```
shell> cd /opt/replicator/software
shell> tar zxf tungsten-replicator-2.0.5-11.tar.gz
```

Change to the Tungsten Replicator staging directory:

```
shell> cd tungsten-replicator-2.0.5-11
```

Configure the replicator on `host1`:

First we configure the defaults and a cluster alias that points to the masters and slaves within the current Continuent Tungsten service that you are replicating from:

Click the link below to switch examples between Staging and INI methods

Show Staging

Show INI

```
shell> ./tools/tpm configure alpha
   --master=host1
   --install-directory=/opt/continuent
   --replication-user=tungsten
   --replication-password=password
   --enable-batch-service=true

shell> vi /etc/tungsten/tungsten.ini
```

Configuration group `alpha`

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `--master=host1` [361]
  `master=host1` [361]
  The hostname of the master (extractor) within the current service. If the current host does not match this specification, then the deployment will by default be configured as a master/extractor.

- `--install-directory=/opt/continuent` [359]
  `install-directory=/opt/continuent` [359]
  Path to the directory where the active deployment will be installed. The configured directory will contain the software, THL and relay log information unless configured otherwise.

- `--replication-user=tungsten` [370]
  `replication-user=tungsten` [370]
  For databases that required authentication, the username to use when connecting to the database using the corresponding connection method (native, JDBC, etc.).
• --replication-password=password

replication-password=password

The password to be used when connecting to the database using the corresponding --replication-user.

• --enable-batch-service=true [in [Tungsten Replicator 2.2 Manual]]

enable-batch-service=true [in [Tungsten Replicator 2.2 Manual]]

This option enables batch mode for a service, which ensures that replication services that are writing to a target database using batch mode in heterogeneous deployments (for example Hadoop, Amazon Redshift or Vertica). Setting this option enables the following settings on each host:

• On a Master
  • mysql-use-bytes-for-string is set to false.
  • colnames filter is enabled (in the binlog-to-q stage to add column names to the THL information.
  • pkey filter is enabled (in the binlog-to-q and q-to-dbms stage), with the addPkeyToInserts and addColumnsToDelete filter options set to true. This ensures that rows have the right primary key information.
  • enumtostring filter is enabled (in the q-to-thl stage), to translate ENUM values to their string equivalents.
  • settostring filter is enabled (in the q-to-thl stage), to translate SET values to their string equivalents.

• On a Slave
  • mysql-use-bytes-for-string is set to true.
  • pkey filter is enabled (q-to-dbms stage).

This creates a configuration that specifies that the topology should read directly from the source host, host3, writing directly to host1. An alternative THL port is provided to ensure that the THL listener is not operating on the same network port as the original.

Now install the service, which will create the replicator reading direct from host3 into host1:

```shell>
./tools/tpm install
```

If the installation process fails, check the output of the `/tmp/tungsten-configure.log` file for more information about the root cause.

Once the installation has been completed, you must update the position of the replicator so that it points to the correct position within the source database to prevent errors during replication. If the replication is being created as part of a migration process, determine the position of the binary log from the external replicator service used when the backup was taken. For example:

```shell>
mysql> show master status;
*************************** 1. row ***************************
File: mysql-bin.000026
Position: 1311
Binlog_Do_DB:
Binlog_Ignore_DB:
1 row in set (0.00 sec)
```

Use `tungsten_set_position` to update the replicator position to point to the master log position:

```shell>
./opt/replicator/scripts/tungsten_set_position \
 --seqno=0 --epoch=0 --service=beta \
 --source-id=host3 --event-id=mysql-bin.000026:1311
```

Now start the replicator:

```shell>
./opt/replicator/tungsten/tungsten-replicator/bin/replicator start
```

Replication status should be checked by explicitly using the servicename and/or RMI port:
3.7. Replicating Data from a Cluster into MySQL

If you have an existing cluster and you want to replicate the data out to a separate standalone MySQL server using Tungsten Replicator then you can create a cluster alias, and use a master/slave topology to replicate from the cluster. This allows for THL events from the cluster to be applied to a separate server for the purposes of backup or separate analysis.

Figure 3.5. Topologies: Replicating Data from a Cluster into MySQL

During the installation process a cluster-alias and cluster-slave are declared. The cluster-alias describes all of the servers in the cluster and how they may be reached. The cluster-slave defines one or more servers that will replicate from the cluster.

The Tungsten Replicator will be installed on the cluster-slave server. That server will download THL data and apply them to the local server. If the cluster-slave has more than one server; one of them will be declared the relay (or master). The other members of the cluster-slave may also download THL data from that server.

If the relay for the cluster-slave fails; the other nodes will automatically start downloading THL data from a server in the cluster. If a non-relay server fails; it will not have any impact on the other members.
3.7.1. Prepare: Replicating Data from a Cluster into MySQL

1. Identify the cluster to replicate from. You will need the master, slaves and THL port (if specified). Use `tpm reverse` from a cluster member to find the correct values.

2. Identify all servers that will replicate from the cluster. If there is more than one, a relay server should be identified to replicate from the cluster and provide THL data to other servers.

3. Prepare each server according to the prerequisites for the DBMS platform it is serving. If you are working with multiple DBMS platforms; treat each platform as a different cluster-slave during deployment.

4. Make sure the THL port for the cluster is open between all servers.

3.7.2. Deploy: Replicating Data from a Cluster into MySQL

3.7.2.1. Replicating Data from a Cluster to MySQL (Staging Use Case)

The following Staging-method procedure will install the Tungsten Replicator software onto target node `host6`, extracting from a cluster consisting of three (3) nodes (`host1`, `host2` and `host3`) and applying into the target database on `host6`.

Important

If you are replicating to a non-MySQL target, please see ??? for more information.

1. On your staging server, go to the software directory.
   ```shell
cd /opt/continuent/software
   ```

2. Download the latest Tungsten Replicator version.

3. Unpack the release package
   ```shell
tar xvzf tungsten-replicator-6.0.3-599.tar.gz
   ```

4. Change to the unpackaged directory:
   ```shell
cd tungsten-replicator-6.0.3-599
   ```

5. Execute the `tpm` command to configure defaults for the installation.
   ```shell
   ./tools/tpm configure defaults \\
   --install-directory=/opt/replicator \\
   --profile-script=~/.bashrc \\
   --replication-password=secret \\
   --replication-port=13306 \\
   --replication-user=tungsten \\
   --start-and-report=true \\
   --user=tungsten
   ```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `tpm configure defaults`  
  This runs the `tpm` command. `configure defaults` indicates that we are setting options which will apply to all dataservices.

- `--install-directory=/opt/replicator` [359]
  The installation directory of the Tungsten service. This is where the service will be installed on each server in your dataservice.

- `--profile-script="~/.bashrc"` [368]
  The profile script used when your shell starts. Using this line modifies your profile script to add a path to the Tungsten tools so that managing Continenent Tungsten™ are easier to use.

- `--user=tungsten` [377]
  The operating system user name that you have created for the Tungsten service, `tungsten`.  

---

85
Deployment: MySQL Topologies

- `--replication-user=tungsten`
  The user name that will be used to apply replication changes to the database on slaves.

- `--replication-password=password`
  The password that will be used to apply replication changes to the database on slaves.

- `--replication-port=13306`
  Set the port number to use when connecting to the MySQL server.

- `--start-and-report`
  Tells `tpm` to startup the service, and report the current configuration and status.

6. Configure a cluster alias that points to the masters and slaves within the current Continuent Tungsten service that you are replicating from:

```bash
shell> ./tools/tpm configure alpha \
   --master=host1 \
   --slaves=host2,host3 \
   --thl-port=2112 \
   --topology=cluster-alias
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `tpm configure alpha`
  This runs the `tpm` command. `configure` indicates that we are creating a new dataservice, and `alpha` is the name of the dataservice being created.
  
  This definition is for a dataservice alias, not an actual dataservice because `--topology=cluster-alias` has been specified. This alias is used in the cluster-slave section to define the source hosts for replication.

- `--master=host1`
  Specifies the hostname of the default master in the cluster.

- `--slaves=host2,host3`
  Specifies the name of any other servers in the cluster that may be replicated from.

- `--thl-port=2112`
  The THL port for the cluster. The default value is 2112 but any other value must be specified.

- `--topology=cluster-alias`
  Define this as a cluster dataservice alias so `tpm` does not try to install cluster software to the hosts.

Important

This dataservice `cluster-alias` name MUST be the same as the cluster dataservice name that you are replicating from.

7. Create the configuration that will replicate from cluster dataservice `alpha` into the database on the host specified by `--relay=host6`:

```bash
shell> ./tools/tpm configure omega \
   --relay=host6 \
   --relay-source=alpha \
   --topology=cluster-slave
```

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `tpm configure omega`
  This runs the `tpm` command. `configure` indicates that we are creating a new replication service, and `omega` is the unique service name for the replication stream from the cluster.
Deployment: MySQL Topologies

- `--relay=host6 [361]`
  Specifies the hostname of the destination database into which data will be replicated.

- `--relay-source=alpha [370]`
  Specifies the name of the source cluster dataservice alias (defined above) that will be used to read events to be replicated.

- `--topology=cluster-slave [377]`
  Read source replication data from any host in the `alpha` dataservice.

8. If you are using a non-standard, possibly offboard, MySQL target like AWS RDS or Google CloudSQL use the following examples to configure the needed additional options for the `omega` replicator service to run in Offboard mode.

   Important
   If you are replicating to a non-MySQL target, please see ??? for more information.

- AWS RDS MySQL/MariaDB Offboard Target

  ```shell
  ./tools/tpm configure omega \
  --replication-host=RDS_ENDPOINT_FQDN_HERE \
  --replication-password=RDS_PASSWORD_HERE \
  --replication-port=3306 \
  --replication-user=tungsten \
  --privileged-slave=false \
  --skip-validation-check=InstallerMasterSlaveCheck \
  --skip-validation-check=MySQLPermissionsCheck \
  --skip-validation-check=MySQLBinaryLogsEnabledCheck
  ```

  Please see Prepare Amazon RDS/Amazon Aurora [in [Tungsten Replicator 2.2 Manual]] for more information.

- Google CloudSQL Offboard Target

  ```shell
  ./tools/tpm configure omega \
  --datasource-type=mysql \
  --privileged-slave=false \
  --replication-host=CLOUDSQL_ENDPOINT_FQDN_HERE \
  --replication-password=CLOUDSQL_PASSWORD_HERE \
  --replication-port=3306 \
  --replication-user=tungsten \
  --skip-validation-check=MySQLPermissionsCheck
  ```

9. Once the configuration has been completed, you can perform the installation to set up the Tungsten Replicator services using the `tpm` command run from the staging directory:

   ```shell
   ./tools/tpm install
   ```

   If the installation process fails, check the output of the `/tmp/tungsten-configure.log` file for more information about the root cause.

   The cluster-slave replicator should now be installed and ready to use.

3.7.2.2. Replicating Data from a Cluster to MySQL (INI Use Case)

   The following INI-based procedure will install the Tungsten Replicator software onto target node `host6`, extracting from a cluster consisting of three (3) nodes (`host1`, `host2` and `host3`) and applying into the target database on `host6`.

   Important
   If you are replicating to a non-MySQL target, please see ??? for more information.

1. Create the configuration file `/etc/tungsten/tungsten.ini` on the destination DBMS host, i.e. `host6`:

   ```ini
   [defaults]
   user=tungsten
   install-directory=/opt/replicator
   replication-user=tungsten
   replication-password=secret
   replication-port=3306
   profile-script=~/.bashrc
   start-and-report=true
   
   [alpha]
   topology=cluster-alias
   master=host1
   members=host1,host2,host3
   ```
Deployment: MySQL Topologies

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

• [defaults]
  
  defaults indicates that we are setting options which will apply to all cluster dataservices.

• user=tungsten
  
  The operating system user name that you have created for the Tungsten service, tungsten.

• install-directory=/opt/replicator
  
  The installation directory of the Tungsten Replicator service. This is where the replicator software will be installed on the destination DBMS server.

• replication-user=tungsten
  
  The MySQL user name to use when connecting to the MySQL database.

• replication-password=secret
  
  The MySQL password for the user that will connect to the MySQL database.

• replication-port=3306
  
  The TCP/IP port on the destination DBMS server that is listening for connections.

• start-and-report=true
  
  Tells tpm to startup the service, and report the current configuration and status.

• profile-script=~/.bashrc
  
  Tells tpm to add PATH information to the specified script to initialize the Tungsten Replicator environment.

• [alpha]
  
  alpha is the name and identity of the source cluster alias being created.

  This definition is for a dataservice alias, not an actual dataservice because topology=cluster-alias has been specified. This alias is used in the cluster-slave section to define the source hosts for replication.

• topology=cluster-alias
  
  Define this as a cluster dataservice alias so tpm does not try to install cluster software to the hosts.

• members=host1,host2,host3
  
  A comma separated list of all the hosts that are part of this cluster dataservice.

• master=host1
  
  The hostname of the server that is the current cluster master MySQL server.

• thl-port=2112
  
  The THL port for the cluster. The default value is 2112 but any other value must be specified.

• [omega]
  
  omega is is the unique service name for the replication stream from the cluster.

This replication service will extract data from cluster dataservice alpha and apply into the database on the DBMS server specified by relay=host6.
Deployment: MySQL Topologies

- **topology=cluster-slave [377]**
  
  Tells `tpm` this is a cluster-slave replication service which will have a list of all source cluster nodes available.

- **relay=host6 [361]**
  
  The hostname of the destination DBMS server.

- **relay-source=alpha [370]**
  
  Specifies the name of the source cluster dataservice alias (defined above) that will be used to read events to be replicated.

  **Important**

  The `cluster-alias` name [i.e. *alpha*] MUST be the same as the cluster dataservice name that you are replicating from.

  **Note**

  Do not include `start-and-report=true [373]` if you are taking over for MySQL native replication. See Section 5.11.1, “Migrating from MySQL Native Replication In-Place” for next steps after completing installation.

2. If you are using a non-standard MySQL target like AWS RDS or Google CloudSQL use the following examples to configure the needed additional options for the replicator service `omega` to run in Offboard mode.

  **Important**

  If you are replicating to a non-MySQL target, please see ??? for more information.

  Append the appropriate code snippet below to the bottom of the existing `[omega]` stanza:

  - **AWS RDS MySQL/MariaDB Offboard Target**

    ```
    replication-host=RDS_ENDPOINT_FQDN_HERE
    replication-password=RDS_PASSWORD_HERE
    replication-port=3306
    replication-user=tungsten
    privileged-slave=false
    skip-validation-check=InstallerMasterSlaveCheck
    skip-validation-check=MySQLPermissionsCheck
    skip-validation-check=MySQLBinaryLogsEnabledCheck
    ```

    Please see Prepare Amazon RDS/Amazon Aurora [in [Tungsten Replicator 2.2 Manual]] for more information.

  - **Google CloudSQL Offboard Target**

    ```
    datasource-type=mysql
    privileged-slave=false
    replication-host=CLOUDSQL_ENDPOINT_FQDN_HERE
    replication-password=CLOUDSQL_PASSWORD_HERE
    replication-port=3306
    replication-user=tungsten
    skip-validation-check=MySQLPermissionsCheck
    ```

  3. Download and install the latest Tungsten Replicator package [.rpm], or download the compressed tarball and unpack it on `host6`:

    ```
    shell> cd /opt/continuent/software
    shell> tar xzvf tungsten-replicator-6.0.3-599.tar.gz
    ```

  4. Change to the Tungsten Replicator staging directory:

    ```
    shell> cd tungsten-replicator-6.0.3-599
    ```

  5. Run `tpm` to install the Tungsten Replicator software with the INI-based configuration:

    ```
    shell> ./tools/tpm install
    ```

    During the installation and startup, `tpm` will notify you of any problems that need to be fixed before the service can be correctly installed and started. If the service starts correctly, you should see the configuration and current status of the service.

    If the installation process fails, check the output of the `/tmp/tungsten-configure.log` file for more information about the root cause.

    The cluster-slave replicator should now be installed and ready to use.
3.7.3. Best Practices: Replicating Data from a Cluster into MySQL

- Setup proper monitoring for all servers in the cluster-slave as described in Section 5.16, “Monitoring Continuent Tungsten”.

3.8. Migrating and Seeding Data

3.8.1. Migrating from MySQL Native Replication 'In-Place'

If you are migrating an existing MySQL native replication deployment to use Continuent Tungsten the configuration of the Continuent Tungsten replication must be updated to match the status of the slave.

1. Deploy Continuent Tungsten using the model or system appropriate according to Chapter 2, Deployment. Ensure that the Continuent Tungsten is not started automatically by excluding the `--start` or `--start-and-report` options from the `tpm` commands.

2. On each slave

   Confirm that native replication is working on all slave nodes:

   ```bash
   shell> echo 'SHOW SLAVE STATUS;' | tpm mysql | \
   egrep ' Master_Host| Last_Error| Slave_SQL_Running'
   Master_HOST: tr-ssl1
   Slave_SQL_Running: Yes
   Last_Error:
   ```

3. On the master and each slave

   Reset the Tungsten Replicator position on all servers:

   ```bash
   shell> replicator start offline
   shell> trepctl -service alpha reset -all -y
   ```

4. On the master

   Login and start Continuent Tungsten services and put the Tungsten Replicator online:

   ```bash
   shell> startall
   shell> trepctl online
   ```

5. On the master

   Put the cluster into maintenance mode using `cctrl` to prevent Continuent Tungsten automatically reconfiguring services:

   ```bash
   cctrl > set policy maintenance
   ```

6. On each slave

   Record the current slave log position (as reported by the `Master_Log_File` and `Exec_Master_Log_Pos` output from `SHOW SLAVE STATUS`). Ideally, each slave should be stopped at the same position:

   ```bash
   shell> echo 'SHOW SLAVE STATUS;' | tpm mysql | \
   egrep ' Master_Host| Last_Error| Master_Log_File| Exec_Master_Log_Pos'
   Master_HOST: tr-ssl1
   Master_Log_File: mysql-bin.000025
   Last_Error: Error executing row event: 'Table 'tungsten_alpha.heartbeat' doesn't exist'
   Exec_Master_Log_Pos: 181268
   ```

   If you have multiple slaves configured to read from this master, record the slave position individually for each host. Once you have the information for all the hosts, determine the earliest log file and log position across all the slaves, as this information will be needed when starting Continuent Tungsten replication. If one of the servers does not show an error, it may be replicating from an intermediate server. If so, you can proceed normally and assume this server stopped at the same position as the host is replicating from.

7. On the master

   Take the replicator offline and clear the THL:

   ```bash
   shell> trepctl offline
   shell> trepctl -service alpha reset -all -y
   ```

8. On the master

   Start replication, using the lowest binary log file and log position from the slave information determined in step 6.
Deployment: MySQL Topologies

9. On each slave
   a. Disable native replication to prevent native replication being accidentally started on the slave.
      
      *On MySQL 5.0 or MySQL 5.1:*
      
      ```shell```
      echo "STOP SLAVE; CHANGE MASTER TO MASTER_HOST='';" | tpm mysql
      ```
      
      *On MySQL 5.5 or later:*
      
      ```shell```
      echo "STOP SLAVE; RESET SLAVE ALL;" | tpm mysql
      ```

   b. If the final position of MySQL replication matches the lowest across all slaves, start Continuent Tungsten services:
      
      ```shell```
      trepctl online
      startall
      ```
      The slave will start reading from the binary log position configured on the master.
      
      If the position on this slave is different, use `trepctl online -from-event` to set the online position according to the recorded position when native MySQL was disabled. Then start all remaining services with `startall`.
      
      ```shell```
      trepctl online -from-event 000025:188249
      startall
      ```

10. Use `cctrl` to confirm that replication is operating correctly across the dataservice on all hosts.

11. Put the cluster back into automatic mode:
    
    ```cctrl```
    set policy automatic
    ```

12. Update your applications to use the installed connector services rather than a direct connection.

13. Remove the `master.info` file on each slave to ensure that when a slave restarts, it does not connect up to the master MySQL server again.

Once these steps have been completed, Continuent Tungsten should be operating as the replication service for your MySQL servers. Use the information in Chapter 5, Operations Guide to monitor and administer the service.

3.8.2. Migrating from MySQL Native Replication Using a New Service

When running an existing MySQL native replication service that needs to be migrated to a Continuent Tungsten service, one solution is to create the new Continuent Tungsten service, synchronize the content, and then install a service that migrates data from the existing native service to the new service while applications are reconfigured to use the new service. The two can then be executed in parallel until applications have been migrated.

The basic structure is shown in Figure 3.6, “Migration: Migrating Native Replication using a New Service”. The migration consists of two steps:

- Initializing the new service with the current database state.
- Creating a Tungsten Replicator deployment that continues to replicate data from the native MySQL service to the new service.

Once the application has been switched and is executing against the new service, the secondary replication can be disabled by shutting down the Tungsten Replicator in `/opt/replicator`. 
Deployment: MySQL Topologies

Figure 3.6. Migration: Migrating Native Replication using a New Service

To configure the service:

1. Stop replication on a slave for the existing native replication installation:

   ```mysql
   STOP SLAVE;
   ```

2. Obtain the current slave position within the master binary log:

   ```mysql
   SHOW SLAVE STATUS;
   ```

3. Create a backup using any method that provides a consistent snapshot. The MySQL master may be used if you do not have a slave to
   backup from. Be sure to get the binary log position as part of your back. This is included in the output to Xtrabackup or using the
   --master-data=2 option with mysqldump.

4. Restart the slave using native replication:

   ```mysql
   START SLAVE;
   ```

5. On the master and each slave within the new service, restore the backup data and start the database service

6. Setup the new Continuent Tungsten deployment using the MySQL servers on which the data has been restored. For clarity, this will be
called newalpha.

7. Configure a second replication service, beta to apply data using the existing MySQL native replication server as the master, and the
   master of newalpha. The information provided in Section 3.6, "Replicating Data Into an Existing Dataservice" will help. Do not start the new
   service.

8. Set the replication position for beta using tungsten_set_position to set the position to the point within the binary logs where the backup
   was taken:

   ```sh
   /opt/replicator/tungsten/tungsten-replicator/bin/tungsten_set_position
   --source-id=host3 --event-id=mysql-bin.000002:559
   ```

9. Start replicator service beta:

   ```sh
   /opt/replicator/tungsten/tungsten-replicator/bin/replicator start
   ```

Once replication has been started, use trepcpl to check the status and ensure that replication is operating correctly.

The original native MySQL replication master can continue to be used for reading and writing from within your application, and changes will
be replicated into the new service on the new hardware. Once the applications have been updated to use the new service, the old servers
can be decommissioned and replicator service beta stopped and removed.
3.8.3. Seeding Data through MySQL

Once the Tungsten Replicator is installed, it can be used to provision all slaves with the master data. The slaves will need enough information in order for the installation to succeed and for Tungsten Replicator to start. The provisioning process requires dumping all data on the master and reloading it back into the master server. This will create a full set of THL entries for the slave replicators to apply. There may be no other applications accessing the master server while this process is running. Every table will be emptied out and repopulated so other applications would get an inconsistent view of the database. If the master is a MySQL slave, then the slave process may be stopped and started to prevent any changes without affecting other servers.

1. If you are using a MySQL slave as the master, stop the replication thread:

   ```
   mysql> STOP SLAVE;
   ```

2. Check Tungsten Replicator status on all servers to make sure it is ONLINE and that the appliedLastSeqno values are matching:

   ```
   shell> trepctl status
   ```

Starting the process before all servers are consistent could cause inconsistencies. If you are trying to completely reprovision the server then you may consider running trepctl reset before proceeding. That will reset the replication position and ignore any previous events on the master.

3. Use mysqldump to output all of the schemas that need to be provisioned:

   ```
   shell> mysqldump --opt --skip-extended-insert -h host3 -u tungsten -P13306 -p \
   --databases db1,db2 > ~/dump.sql
   ```

   Optionally, you can just dump a set of tables to be provisioned:

   ```
   shell> mysqldump --opt --skip-extended-insert -h host3 -u tungsten -P13306 -p \
   db1 table1 table2 > ~/dump.sql
   ```

4. If you are using heterogeneous replication all tables on the slave must be empty before proceeding. The Tungsten Replicator does not replicate DDL statements such as DROP TABLE and CREATE TABLE. You may either truncate the tables on the slave or use ddlscan to recreate them.

5. Load the dump file back into the master to recreate all data:

   ```
   shell> cat ~/dump.sql | tpm mysql
   ```

   The Tungsten Replicator will read the binary log as the dump file is loaded into MySQL. The slaves will automatically apply these statements through normal replication.

6. If you are using a MySQL slave as the master, restart the replication thread after the dump file as completed loading:

   ```
   mysql> START SLAVE;
   ```

7. Monitor replication status on the master and slaves:

   ```
   shell> trepctl status
   ```
Chapter 4. Deployment: Advanced

The following sections provide guidance and instructions for creating advanced deployments, including configuration automatic startup and shutdown during boot procedures, upgrades, downgrades, and removal of Continuent Tungsten.

4.1. Deploying Parallel Replication

Parallel apply is an important technique for achieving high speed replication and curing slave lag. It works by spreading updates to slaves over multiple threads that split transactions on each schema into separate processing streams. This in turn spreads I/O activity across many threads, which results in faster overall updates on the slave. In ideal cases throughput on slaves may improve by up to 5 times over single-threaded MySQL native replication.

4.1.1. Application Prerequisites for Parallel Replication

Parallel replication works best on workloads that meet the following criteria:

- Data are stored in independent schemas. If you have 100 customers per server with a separate schema for each customer, your application is a good candidate.
- Transactions do not span schemas. Tungsten serializes such transactions, which is to say it stops parallel apply and runs them by themselves. If more than 2-3% of transactions are serialized in this way, most of the benefits of parallelization are lost.
- Workload is well-balanced across schemas.
- The slave host(s) are capable and have free memory in the OS page cache.
- The host on which the slave runs has a sufficient number of cores to operate a large number of Java threads.
- Not all workloads meet these requirements. If your transactions are within a single schema only, you may need to consider different approaches, such as slave prefetch. Contact Continuent for other suggestions.

Parallel replication does not work well on underpowered hosts, such as Amazon m1.small instances. In fact, any host that is already I/O bound under single-threaded replication will typically will not show much improvement with parallel apply.

4.1.2. Enabling Parallel Apply During Install

Parallel apply is enabled using the `--svc-parallelization-type` and `--channels` options of `tpm`. The parallelization type defaults to `none` which is to say that parallel apply is disabled. You should set it to `disk`. The `--channels` option sets the number of channels (i.e., threads) you propose to use for applying data. Here is a code example of a MySQL Applier installation with parallel apply enabled. The slave will apply transactions using 30 channels.

Show Staging

Show INI

```
shell> ./tools/tpm configure defaults
  --reset
  --install-directory=/opt/continuent
  --user=tungsten
  --mysql-allow-intensive-checks=true
  --profile-script=~/.bash_profile
  --application-port=3306
  --application-user=app_user
  --application-password=secret
  --replication-port=13306
  --replication-user=tungsten
  --replication-password=secret
  --svc-parallelization-type=disk
  --channels=10
  --start-and-report=true

shell> ./tools/tpm configure alpha
  --master=host1
  --members=host1,host2,host3
  --connectors=host1,host2,host3
```
Deployment: Advanced

```shell
vi /etc/tungsten/tungsten.ini
```

```ini
[defaults]
install-directory=/opt/continuent
user=tungsten
mysql-allow-intensive-checks=true
profile-script=~/.bash_profile
application-port=3306
application-user=app_user
application-password=secret
replication-port=13306
replication-user=tungsten
replication-password=secret
svc-parallelization-type=disk
channels=10
start-and-report=true

[alpha]
master=host1
members=host1,host2,host3
connectors=host1,host2,host3
topology=clustered
```

Configuration group **defaults**

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- **--reset** [371]
  
  reset [371]

  For staging configurations, deletes all pre-existing configuration information between updating with the new configuration values.

- **--install-directory=/opt/continuent** [359]
  
  install-directory=/opt/continuent [359]

  Path to the directory where the active deployment will be installed. The configured directory will contain the software, THL and relay log information unless configured otherwise.

- **--user=tungsten** [377]
  
  user=tungsten [377]

  System User

- **--mysql-allow-intensive-checks=true**
  
  mysql-allow-intensive-checks=true

  For MySQL installation, enables detailed checks on the supported data types within the MySQL database to confirm compatibility. This includes checking each table definition individually for any unsupported data types.

- **--profile-script=~/.bash_profile** [368]
  
  profile-script=~/.bash_profile [368]

  Append commands to include env.sh in this profile script

- **--application-port=3306** [345]
  
  application-port=3306 [345]

  Port for the connector to listen on

- **--application-user=app_user** [345]
  
  application-user=app_user [345]

  Database username for the connector

- **--application-password=secret** [344]

  Database password for the connector
**Database password for the connector**

- **--replication-port=13306**
  
  The network port used to connect to the database server. The default port used depends on the database being configured.

- **--replication-user=tungsten**
  
  For databases that required authentication, the username to use when connecting to the database using the corresponding connection method [native, JDBC, etc.].

- **--replication-password=secret**
  
  The password to be used when connecting to the database using the corresponding **--replication-user**.

- **--svc-parallelization-type=disk**
  
  Method for implementing parallel apply

- **--channels=10**
  
  Number of replication channels to use for services

- **--start-and-report=true**
  
  Start the services and report out the status after configuration

**Configuration group alpha**

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- **--master=host1**
  
  The hostname of the master (extractor) within the current service. If the current host does not match this specification, then the deployment will by default be configured as a master/extractor.

- **--members=host1,host2,host3**
  
  Hostnames for the dataservice members

- **--connectors=host1,host2,host3**
  
  Hostnames for the dataservice connectors

- **--topology=clustered**
  
  Replication topology for the dataservice Valid values are star, cluster-slave, master-slave, fan-in, clustered, cluster-alias, all-masters, direct

If the installation process fails, check the output of the `~/tmp/tungsten-configure.log` file for more information about the root cause.
There are several additional options that default to reasonable values. You may wish to change them in special cases.

- `--buffer-size [347]` — Sets the replicator block commit size, which is the number of transactions to commit at once on slaves. Values up to 100 are normally fine.

- `--native-slave-takeover [366]` — Used to allow Tungsten to take over from native MySQL replication and parallelize it. See here for more.

You can check the number of active channels on a slave by looking at the "channels" property once the replicator restarts.

```
slave shell> trepctl -service alpha status| grep channels
channels               : 10
```

**Important**

The channel count for a Master will ALWAYS be 1 because extraction is single-threaded:

```
master shell> trepctl -service alpha status| grep channels
channels               : 1
```

**Warning**

Enabling parallel apply will dramatically increase the number of connections to the database server.

Typically the calculation on a slave would be: Connections = Channel_Count x Service_Count x 2, so for a 4-way Composite Multimaster topology with 30 channels there would be 30 x 4 x 2 = 240 connections required for the replicator alone, not counting application traffic.

You may display the currently used number of connections in MySQL:

```
mysql> SHOW STATUS LIKE 'max_used_connections';
```

```
+----------------------+
| Variable_name        | Value |
|----------------------|
| Max_used_connections | 190   |
+----------------------+
1 row in set (0.00 sec)
```

Below are suggestions for how to change the maximum connections setting in MySQL both for the running instance as well as at startup:

```
mysql> SET GLOBAL max_connections = 512;
```

```
mysql> SHOW VARIABLES LIKE 'max_connections';
```

```
+-----------------+-------+
| Variable_name   | Value |
|-----------------+-------|
| max_connections | 512   |
+-----------------+-------+
1 row in set (0.00 sec)
```

```
shell> vi /etc/my.cnf
max_connections = 512
```

### 4.1.3. Channels

**Channels and Parallel Apply**

Parallel apply works by using multiple threads for the final stage of the replication pipeline. These threads are known as channels. Restart points for each channel are stored as individual rows in table `trep_commit_seqno` if you are applying to a relational DBMS server, including MySQL, Oracle, and data warehouse products like Vertica.

When you set the `--channels [348]` argument, the `tpm` program configures the replication service to enable the requested number of channels. A value of 1 results in single-threaded operation.

Do not change the number of channels without setting the replicator offline cleanly. See the procedure later in this page for more information.

**How Many Channels Are Enough?**

Pick the smallest number of channels that loads the slave fully. For evenly distributed workloads this means that you should increase channels so that more threads are simultaneously applying updates and soaking up I/O capacity. As long as each shard receives roughly the same number of updates, this is a good approach.

For unevenly distributed workloads, you may want to decrease channels to spread the workload more evenly across them. This ensures that each channel has productive work and minimizes the overhead of updating the channel position in the DBMS.
Once you have maximized I/O on the DBMS server leave the number of channels alone. Note that adding more channels than you have shards does not help performance as it will lead to idle channels that must update their positions in the DBMS even though they are not doing useful work. This actually slows down performance a little bit.

Affect of Channels on Backups

If you back up a slave that operates with more than one channel, say 30, you can only restore that backup on another slave that operates with the same number of channels. Otherwise, reloading the backup is the same as changing the number of channels without a clean offline.

When operating Tungsten Replicator in a Tungsten cluster, you should always set the number of channels to be the same for all replicators. Otherwise you may run into problems if you try to restore backups across MySQL instances that load with different locations.

If the replicator has only a single channel enabled, you can restore the backup anywhere. The same applies if you run the backup after the replicator has been taken offline cleanly.

4.1.4. Parallel Replication and Offline Operation

4.1.4.1. Clean Offline Operation

When you issue a trepctl offline command, Tungsten Replicator will bring all channels to the same point in the log and then go offline. This is known as going offline cleanly. When a slave has been taken offline cleanly the following are true:

- The `trep_commit_seqno` table contains a single row
- The `trep_shard_channel` table is empty

When parallel replication is not enabled, you can take the replicator offline by stopping the replicator process. There is no need to issue a `trepctl offline` command first.

4.1.4.2. Tuning the Time to Go Offline Cleanly

Putting a replicator offline may take a while if the slowest and fastest channels are far apart, i.e., if one channel gets far ahead of another. The separation between channels is controlled by the `maxOfflineInterval` parameter, which defaults to 5 seconds. This sets the allowable distance between commit timestamps processed on different channels. You can adjust this value at installation or later. The following example shows how to change it after installation. This can be done at any time and does not require the replicator to go offline cleanly.

```
shell> ./tools/tpm update alpha \
   --property=replicator.store.parallel-queue.maxOfflineInterval=30
```

The offline interval is only the the approximate time that Tungsten Replicator will take to go offline. Up to a point, larger values (say 60 or 120 seconds) allow the replicator to parallelize in spite of a few operations that are relatively slow. However, the down side is that going offline cleanly can become quite slow.

4.1.4.3. Unclean Offline

If you need to take a replicator offline quickly, you can either stop the replicator process or issue the following command:

```
shell> trepctl offline -immediate
```

Both of these result in an unclean shutdown. However, parallel replication is completely crash-safe provided you use transactional table types like InnoDB, so you will be able to restart without causing slave consistency problems.

**Warning**

You must take the replicator offline cleanly to change the number of channels or when reverting to MySQL native replication. Failing to do so can result in errors when you restart replication.

4.1.5. Adjusting Parallel Replication After Installation

4.1.5.1. How to Enable Parallel Apply After Installation

**Warning**

Be sure to place the cluster into MAINTENANCE mode first so the Manager does not attempt to automatically bring the replicator online.

```
 Ctrl> set policy maintenance
```

To enable parallel replication after installation, take the replicator offline cleanly using the following command:
Modify the configuration to add two parameters:

Show Staging

Show INI

```
shell> ./tools/tpm configure defaults \
   --svc-parallelization-type=disk \
   --channels=10
```

```
shell> vi /etc/tungsten/tungsten.ini
```

```
[defaults]
svc-parallelization-type=disk
channels=10
```

Configuration group `defaults`

The description of each of the options is shown below; click the icon to hide this detail:

Click the icon to show a detailed description of each argument.

- `--svc-parallelization-type=disk` [374]
  
  `svc-parallelization-type=disk` [374]

  Method for implementing parallel apply

- `--channels=10` [348]
  
  `channels=10` [348]

  Number of replication channels to use for services

  **Note**

  You make use an actual data service name in place of the keyword `defaults`.

Signal the changes by running an update followed by a complete restart of the Replicator process:

```
shell> tpm update
shell> replicator restart
```

**Warning**

Be sure to place the cluster into AUTOMATIC mode as soon as all replicators are updated and back online.

```
cctrl> set policy automatic
```

You can check the number of active channels on a slave by looking at the "channels" property once the replicator restarts.

```
slave shell> trepctl -service alpha status| grep channels
channels               : 10
```

**Important**

The channel count for a Master will ALWAYS be 1 because extraction is single-threaded:

```
mast shell> trepctl -service alpha status| grep channels
channels               : 1
```

**Warning**

Enabling parallel apply will dramatically increase the number of connections to the database server.

Typically the calculation on a slave would be: Connections = Channel_Count x Service_Count x 2, so for a 4-way Composite Multimaster topology with 30 channels there would be 30 x 4 x 2 = 240 connections required for the replicator alone, not counting application traffic.

You may display the currently used number of connections in MySQL:

```
mysql> SHOW STATUS LIKE 'max_used_connections';
```
4.1.5.2. How to Change Channels Safely

To change the number of channels you must take the replicator offline cleanly using the following command:

```shell
trepctl offline
```

This command brings all channels up the same transaction in the log, then goes offline. If you look in the `trep_commit_seqno` table, you will notice only a single row, which shows that updates to the slave have been completely serialized to a single point. At this point you may safely reconfigure the number of channels on the replicator, for example using the following command:

```shell
tpm update alpha --channels=5
```

You can check the number of active channels on a slave by looking at the "channels" property once the replicator restarts.

If you attempt to reconfigure channels without going offline cleanly, Tungsten Replicator will signal an error when you attempt to go online with the new channel configuration. The cure is to revert to the previous number of channels, go online, and then go offline cleanly. Note that attempting to clean up the `trep_commit_seqno` and `trep_shard_channel` tables manually can result in your slaves becoming inconsistent and requiring full resynchronization. You should only do such cleanup under direction from Continuent support.

**Warning**

Failing to follow the channel reconfiguration procedure carefully may result in your slaves becoming inconsistent or failing. The cure is usually full resynchronization, so it is best to avoid this if possible.

4.1.5.3. How to Disable Parallel Replication Safely

The following steps describe how to gracefully disable parallel apply replication.

**Replication Graceful Offline (critical first step)**

To disable parallel apply, you must first take the replicator offline cleanly using the following command:

```shell
trepctl offline
```

This command brings all channels up the same transaction in the log, then goes offline. If you look in the `trep_commit_seqno` table, you will notice only a single row, which shows that updates to the slave have been completely serialized to a single point. At this point you may safely disable parallel apply on the replicator, for example using the following command:

```shell
tools/tpm configure alpha --channels=1 --svc-parallelization-type=none
```

Disable Parallel Replication using the INI Method

For INI deployments, simply remove both `svc-parallelization-type` and `channels` options from the `/etc/tungsten/tungsten.ini` file, then execute `tpm update`.
Verification

You can check the number of active channels on a slave by looking at the "channels" property once the replicator restarts.

```
thsh> trepctl -service alpha status| grep channels
channels               : 1
```

Notes and Warnings

If you attempt to reconfigure channels without going offline cleanly, Tungsten Replicator will signal an error when you attempt to go online with the new channel configuration. The cure is to revert to the previous number of channels, go online, and then go offline cleanly. Note that attempting to clean up the `trep_commit_seqno` and `trep_shard_channel` tables manually can result in your slaves becoming inconsistent and requiring full resynchronization. You should only do such cleanup under direction from Continuent support.

**Warning**

Failing to follow the channel reconfiguration procedure carefully may result in your slaves becoming inconsistent or failing. The cure is usually full resynchronization, so it is best to avoid this if possible.

### 4.1.5.4. How to Switch Parallel Queue Types Safely

As with channels you should only change the parallel queue type after the replicator has gone offline cleanly. The following example shows how to update the parallel queue type after installation:

```
thsh> tpm update alpha --svc-parallelization-type=disk --channels=5
thsh> replicator restart
```

### 4.1.6. Monitoring Parallel Replication

Basic monitoring of a parallel deployment can be performed using the techniques in Chapter 5, *Operations Guide*. Specific operations for parallel replication are provided in the following sections.

#### 4.1.6.1. Useful Commands for Parallel Monitoring Replication

The replicator has several helpful commands for tracking replication performance:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trepctl status</td>
<td>Shows basic variables including overall latency of slave and number of apply channels</td>
</tr>
<tr>
<td>trepctl status -name shards</td>
<td>Shows the number of transactions for each shard</td>
</tr>
<tr>
<td>trepctl status -name stores</td>
<td>Shows the configuration and internal counters for stores between tasks</td>
</tr>
<tr>
<td>trepctl status -name tasks</td>
<td>Shows the number of transactions (events) and latency for each independent task in the replicator pipeline</td>
</tr>
</tbody>
</table>

#### 4.1.6.2. Parallel Replication and Applied Latency On Slaves

The `trepctl status appliedLastSeqno` parameter shows the sequence number of the last transaction committed. Here is an example from a slave with 5 channels enabled.

```
thsh> trepctl status
Processing status command...
NAME                     VALUE
appliedLastEventId        mysql-bin.000211:0000000020094456;0
appliedLastSeqno          78021
appliedLatency            0.216
channels                  5
```

When parallel apply is enabled, the meaning of `appliedLastSeqno` changes. It is the minimum recovery position across apply channels, which means it is the position where channels restart in the event of a failure. This number is quite conservative and may make replication appear to be further behind than it actually is.

- Busy channels mark their position in table `trep_commit_seqno` as they commit. These are up-to-date with the traffic on that channel, but channels have latency between those that have a lot of big transactions and those that are more lightly loaded.
• Inactive channels do not get any transactions, hence do not mark their position. Tungsten sends a control event across all channels so that they mark their commit position in `trep_commit_channel`. It is possible to see a delay of many seconds or even minutes in unloaded systems from the true state of the slave because of idle channels not marking their position yet.

For systems with few transactions it is useful to lower the synchronization interval to a smaller number of transactions, for example 500. The following command shows how to adjust the synchronization interval after installation:

```shell
shell> tpm update alpha \\
   --property=replicator.store.parallel-queue.syncInterval=500
```

Note that there is a trade-off between the synchronization interval value and writes on the DBMS server. With the foregoing setting, all channels will write to the `trep_commit_seqno` table every 500 transactions. If there were 50 channels configured, this could lead to an increase in writes of up to 10%—each channel could end up adding an extra write to mark its position every 10 transactions. In busy systems it is therefore better to use a higher synchronization interval for this reason.

You can check the current synchronization interval by running the `trepctl status -name stores` command, as shown in the following example:

```shell
shell> trepctl status -name stores
```

You can also force all channels to mark their current position by sending a heartbeat through using the `trepctl heartbeat` command.

### 4.1.6.3. Relative Latency

Relative latency is a `trepctl status` parameter. It indicates the latency since the last time the appliedSeqno advanced; for example:

```shell
shell> trepctl status
```

In this example the last transaction had a latency of .571 seconds from the time it committed on the master and committed 8.944 seconds ago. If relative latency increases significantly in a busy system, it may be a sign that replication is stalled. This is a good parameter to check in monitoring scripts.

### 4.1.6.4. Serialization Count

Serialization count refers to the number of transactions that the replicator has handled that cannot be applied in parallel because they involve dependencies across shards. For example, a transaction that spans multiple shards must serialize because it might cause an out-of-order update with respect to transactions that update a single shard only.

You can detect the number of transactions that have been serialized by looking at the `serializationCount` parameter using the `trepctl status -name stores` command. The following example shows a replicator that has processed 1512 transactions with 26 serialized.

```shell
shell> trepctl status -name stores
```
In this case 1.7% of transactions are serialized. Generally speaking you will lose benefits of parallel apply if more than 1-2% of transactions are serialized.

### 4.1.6.5. Maximum Offline Interval

The maximum offline interval \([\text{maxOfflineInterval}]\) parameter controls the “distance” between the fastest and slowest channels when parallel apply is enabled. The replicator measures distance using the seconds between commit times of the last transaction processed on each channel. This time is roughly equivalent to the amount of time a replicator will require to go offline cleanly.

You can change the \(\text{maxOfflineInterval}\) as shown in the following example, the value is defined in seconds.

```shell
tpm update alpha --property=replicator.store.parallel-queue.maxOfflineInterval=15
```

You can view the configured value as well as the estimate current value using the `trepctl status -name stores` command, as shown in yet another example:

```shell
trepctl status -name stores
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>estimatedOfflineInterval:</td>
<td>1.3</td>
</tr>
<tr>
<td>maxOfflineInterval      :</td>
<td>15</td>
</tr>
</tbody>
</table>

### 4.1.6.6. Workload Distribution

Parallel apply works best when transactions are distributed evenly across shards and those shards are distributed evenly across available channels. You can monitor the distribution of transactions over shards using the `trepctl status -name shards` command. This command lists transaction counts for all shards, as shown in the following example.

```shell
trepctl status -name shards
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>appliedLastEventId:</td>
<td>mysql-bin.000211:0000000020095529;0</td>
</tr>
<tr>
<td>appliedLastSeqno  :</td>
<td>78026</td>
</tr>
<tr>
<td>appliedLatency    :</td>
<td>0.558</td>
</tr>
<tr>
<td>eventCount        :</td>
<td>26</td>
</tr>
<tr>
<td>shardId           :</td>
<td>#UNKNOWN</td>
</tr>
<tr>
<td>stage             :</td>
<td>q-to-dbms</td>
</tr>
</tbody>
</table>

If one or more shards have a very large `eventCount` value compared to the others, this is a sign that your transaction workload is poorly distributed across shards.

The listing of shards also offers a useful trick for finding serialized transactions. Shards that Tungsten Replicator cannot safely parallelize are assigned the dummy shard ID `#UNKNOWN`. Look for this shard to find the count of serialized transactions. The `appliedLastSeqno` for this shard gives the sequence number of the most recent serialized transaction. As the following example shows, you can then list the contents of the transaction to see why it serialized. In this case, the transaction affected tables in different schemas.

```shell
trepctl status -name shards
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>appliedLastEventId:</td>
<td>mysql-bin.000211:0000000020095529;0</td>
</tr>
<tr>
<td>appliedLastSeqno  :</td>
<td>78026</td>
</tr>
<tr>
<td>appliedLatency    :</td>
<td>0.558</td>
</tr>
<tr>
<td>eventCount        :</td>
<td>26</td>
</tr>
<tr>
<td>shardId           :</td>
<td>#UNKNOWN</td>
</tr>
<tr>
<td>stage             :</td>
<td>q-to-dbms</td>
</tr>
</tbody>
</table>

```shell
thl list -seqno 78026
```

<table>
<thead>
<tr>
<th>SEQ# = 78026 / FRAG# = 0 (last frag)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- TIME = 2013-01-17 22:29:42.0</td>
</tr>
<tr>
<td>- EVENTID = mysql-bin.000211:0000000020095529;0</td>
</tr>
<tr>
<td>- SOUCREID = logos1</td>
</tr>
<tr>
<td>- METADATA = [mysql_server_id=1;service=percona;shard=#UNKNOWN]</td>
</tr>
<tr>
<td>- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent</td>
</tr>
<tr>
<td>- OPTIONS =</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

103
The replicator normally distributes shards evenly across channels. As each new shard appears, it is assigned to the next channel number, which then rotates back to 0 once the maximum number has been assigned. If the shards have uneven transaction distributions, this may lead to an uneven number of transactions on the channels. To check, use the `trepctl status -name tasks` and look for tasks belonging to the `q-to-dbms` stage.

If you see one or more channels that have a very high `eventCount`, consider either assigning shards explicitly to channels or redistributing the workload in your application to get better performance.

### 4.1.7. Controlling Assignment of Shards to Channels

Tungsten Replicator by default assigns channels using a round robin algorithm that assigns each new shard to the next available channel. The current shard assignments are tracked in table `trep_shard_channel` in the Tungsten catalog schema for the replication service.

For example, if you have 2 channels enabled and Tungsten processes three different shards, you might end up with a shard assignment like the following:

```
Foo => channel 0
bar => channel 1
foobar => channel 0
```

This algorithm generally gives the best results for most installations and is crash-safe, since the contents of the `trep_shard_channel` table persist if either the DBMS or the replicator fails.

It is possible to override the default assignment by updating the `shard.list` file found in the `tungsten-replicator/conf` directory. This file normally looks like the following:

```sh
# SHARD MAP FILE.
# This file contains shard handling rules used in the ShardListPartitioner
# class for parallel replication. If unchanged shards will be hashed across
# available partitions.
# You can assign shards explicitly using a shard name match, where the form
# is <db>=<partition>.
#common1=0
#common2=0
db1=1
#db2=2
db3=3
default partition for shards that do not match explicit name.
# permissible values are either a partition number or -1, in which
# case values are hashed across available partitions. (-1 is the
# default. 
#(*)=-1
# comma-separated list of shards that require critical section to run.
# critical section" means that these events are single-threaded to
# ensure that all dependencies are met.
```

104
Deployment: Advanced

You can update the shard.list file to do three types of custom overrides.

1. **Change the hashing method for channel assignments.** Round-robin uses the `trep_shard_channel` table. The string-hash method just hashes the shard name.

2. **Assign shards to explicit channels.** Add lines of the form `shard=channel` to the file as shown by the commented-out entries.

3. **Define critical shards.** These are shards that must be processed in serial fashion. For example, if you have a sharded application that has a single global shard with reference information, you can declare the global shard to be critical. This helps avoid applications seeing out of order information.

Changes to shard.list must be made with care. The same cautions apply here as for changing the number of channels or the parallelization type. For subscription customers we strongly recommend conferring with Continuent Support before making changes.

### 4.1.8. Disk vs. Memory Parallel Queues

Channels receive transactions through a special type of queue, known as a parallel queue. Tungsten offers two implementations of parallel queues, which vary in their performance as well as the requirements they may place on hosts that operate parallel apply. You choose the type of queue to enable using the `--svc-parallelization-type` option.

**Warning**

Do not change the parallel queue type without setting the replicator offline cleanly. See the procedure later in this page for more information.

#### Disk Parallel Queue (`disk` option)

A disk parallel queue uses a set of independent threads to read from the Transaction History Log and feed short in-memory queues used by channels. Disk queues have the advantage that they minimize memory required by Java. They also allow channels to operate some distance apart, which improves throughput. For instance, one channel may apply a transaction that committed 2 minutes before the transaction another channel is applying. This separation keeps a single slow transaction from blocking all channels.

Disk queues minimize memory consumption of the Java VM but to function efficiently they do require pages from the Operating System page cache. This is because the channels each independently read from the Transaction History Log. As long as the channels are close together the storage pages tend to be present in the Operating System page cache for all threads but the first, resulting in very fast reads. If channels become widely separated, for example due to a high `maxOfflineInterval` value, or the host has insufficient free memory, disk queues may operate slowly or impact other processes that require memory.

#### Memory Parallel Queue (`memory` option)

A memory parallel queue uses a set of in-memory queues to hold transactions. One stage reads from the Transaction History Log and distributes transactions across the queues. The channels each read from one of the queues. In-memory queues have the advantage that they do not need extra threads to operate, hence reduce the amount of CPU processing required by the replicator.

When you use in-memory queues you must set the `maxSize` property on the queue to a relatively large value. This value sets the total number of transaction fragments that may be in the parallel queue at any given time. If the queue hits this value, it does not accept further transaction fragments until existing fragments are processed. For best performance it is often necessary to use a relatively large number, for example 10,000 or greater.

The following example shows how to set the `maxSize` property after installation. This value can be changed at any time and does not require the replicator to go offline cleanly:

```
$ tpm update alpha
   --property=replicator.store.parallel-queue.maxSize=10000
```

You may need to increase the Java VM heap size when you increase the parallel queue maximum size. Use the `--java-mem-size` option on the `tpm` command for this purpose or edit the Replicator `wrapper.conf` file directly.

**Warning**

Memory queues are not recommended for production use at this time. Use disk queues.

### 4.2. Starting and Stopping Continuent Tungsten

To stop all of the services associated with a dataservice node, use the `stopall` script:

```
$ stopall
```
4.2.1. Restarting the Replicator Service

Warning

Restarting a running replicator temporarily stops and restarts replication. Either set \texttt{MAINTENANCE} mode within \texttt{cctrl} [see \texttt{Section 5.14, \textbf{Performing Database or OS Maintenance}} or shun the datasource before restarting the replicator [\texttt{Section 5.3.5.1, \textbf{Shunning a Datasource}}].

To shutdown a running Tungsten Replicator you must switch off the replicator:

\begin{verbatim}
shell> replicator stop
Stopping Tungsten Replicator Service...
Stopped Tungsten Replicator Service.
\end{verbatim}

To start the replicator service if it is not already running:

\begin{verbatim}
shell> replicator start
Starting Tungsten Replicator Service...
\end{verbatim}

4.2.2. Restarting the Connector Service

Warning

Restarting the connector service will interrupt the communication of any running application or client connecting through the connector to MySQL.

To shutdown a running Tungsten Connector you must switch off the replicator:

\begin{verbatim}
shell> connector stop
Stopping Tungsten Connector Service...
Stopped Tungsten Connector Service.
\end{verbatim}

To start the replicator service if it is not already running:

\begin{verbatim}
shell> connector start
Starting Tungsten Connector Service...
\end{verbatim}

If the cluster was configured with \texttt{auto-enable=false} \texttt{[345]} then you will need to put each node online individually.

4.2.3. Restarting the Manager Service

The manager service is designed to monitor the status and operation of the each of the datasources within the dataservice. In the event that the manager has become confused with the current configuration, for example due to a network or node failure, the managers can be restarted. This forces the managers to update their current status and topology information.

Before restarting managers, the dataservice should be placed in maintenance policy mode. In maintenance mode, the connectors will continue to service requests and the manager restart will not be treated as a failure.

To restart the managers across an entire dataservice, each manager will need to be restarted. The dataservice must be placed in maintenance policy mode first, then:

1. To set the maintenance policy mode:

\begin{verbatim}
[LOGICAL:EXPERT] /dsone > set policy maintenance
\end{verbatim}

2. On each datasource in the dataservice:
a. Stop the service:

```
shell> manager stop
```

b. Then start the manager service:

```
shell> manager start
```

3. Once all the managers have been restarted, set the policy mode back to the automatic:

```
[LOGICAL:EXPORT] /alpha > set policy automatic
Policy mode is now AUTOMATIC
```

### 4.2.4. Restarting the Multisite/Multimaster Replicator Service

**Warning**

Restarting a running replicator temporarily stops and restarts replication. When using Multisite/Multimaster, restarting the additional replicator will stop replication between sites.

These instructions assume you have installed the additional replicator with the `--executable-prefix=mm` (in Tungsten Replicator 2.2 Manual) option. If not, you should go to `/opt/replicator/tungsten/tungsten-replicator/bin` and run the `replicator` command directly.

To shutdown a running Tungsten Replicator you must switch off the replicator:

```
shell> mm_replicator stop
Stopping Tungsten Replicator Service...
Stopped Tungsten Replicator Service.
```

To start the replicator service if it is not already running:

```
shell> mm_replicator start
Starting Tungsten Replicator Service...
```

### 4.3. Configuring Startup on Boot

By default, Continuent Tungsten does not start automatically on boot. To enable Continuent Tungsten to start at boot time, use the `deployall` script provided in the installation directory to create the necessary boot scripts:

```
shell> sudo /opt/continuent/tungsten/cluster-home/bin/deployall
Adding system startup for /etc/init.d/tmanager ...
  /etc/rc0.d/K80tmanager -> ../init.d/tmanager
  /etc/rc1.d/K80tmanager -> ../init.d/tmanager
  /etc/rc2.d/S80tmanager -> ../init.d/tmanager
  /etc/rc3.d/S80tmanager -> ../init.d/tmanager
  /etc/rc4.d/S80tmanager -> ../init.d/tmanager
  /etc/rc5.d/S80tmanager -> ../init.d/tmanager
  /etc/rc6.d/K80tmanager -> ../init.d/tmanager
Adding system startup for /etc/init.d/treplicator ...
  /etc/rc0.d/K81treplicator -> ../init.d/treplicator
  /etc/rc1.d/K81treplicator -> ../init.d/treplicator
  /etc/rc2.d/S81treplicator -> ../init.d/treplicator
  /etc/rc3.d/S81treplicator -> ../init.d/treplicator
  /etc/rc4.d/S81treplicator -> ../init.d/treplicator
  /etc/rc5.d/S81treplicator -> ../init.d/treplicator
  /etc/rc6.d/K81treplicator -> ../init.d/treplicator
Adding system startup for /etc/init.d/tconnector ...
  /etc/rc0.d/K82tconnector -> ../init.d/tconnector
  /etc/rc1.d/K82tconnector -> ../init.d/tconnector
  /etc/rc2.d/S82tconnector -> ../init.d/tconnector
  /etc/rc3.d/S82tconnector -> ../init.d/tconnector
  /etc/rc4.d/S82tconnector -> ../init.d/tconnector
  /etc/rc5.d/S82tconnector -> ../init.d/tconnector
  /etc/rc6.d/K82tconnector -> ../init.d/tconnector
```

To disable automatic startup at boot time, use the `undeployall` command:

```
shell> sudo /opt/continuent/tungsten/cluster-home/bin/undeployall
```

### 4.3.1. Configuring Multisite/Multimaster Replicator Startup on Boot

Because there is an additional Tungsten Replicator running, each must be individually configured to startup on boot:

- For the Continuent Tungsten service, use Section 4.3, "Configuring Startup on Boot".
• For the Tungsten Replicator service, a custom startup script must be created, otherwise the replicator will be unable to start as it has been configured in a different directory.

1. Create a link from the Tungsten Replicator service startup script in the operating system startup directory (`/etc/init.d`):

```sh
sudo ln -s /opt/replicator/tungsten/tungsten-replicator/bin/replicator /etc/init.d/mmreplicator
```

2. Stop the Tungsten Replicator process. Failure to do this will cause issues because the service will no longer recognize the existing PID file and report it is not running.

```sh
/etc/init.d/mmreplicator stop
```

3. Modify the `APP_NAME` variable within the startup script (`/etc/init.d/mmreplicator`) to `mmreplicator`:

```sh
APP_NAME="mmreplicator"
```

4. Start the Tungsten Replicator process.

```sh
/etc/init.d/mmreplicator start
```

5. Update the operating system startup configuration to use the updated script.

On Debian/Ubuntu:

```sh
sudo update-rc.d mmreplicator defaults
```

On RedHat/CentOS:

```sh
sudo chkconfig --add mmreplicator
```

### 4.4. Upgrading Continuent Tungsten

To upgrade an existing installation on Continuent Tungsten, the new distribution must be downloaded and unpacked, and the included `tpm` command used to update the installation. The upgrade process implies a small period of downtime for the cluster as the updated versions of the tools are restarted, but downtime is deliberately kept to a minimum, and the cluster should be in the same operation state once the upgrade has finished as it was when the upgrade was started.

#### 4.4.1. Upgrading using the Staging Method (with ssh Access)

**Note**

For INI file upgrades, see Section 4.4.2, “Upgrading when using INI-based configuration, or without ssh Access”

**Warning**

Before performing and upgrade, please ensure that you have checked the Appendix C, Prerequisites, as software and system requirements may have changed between versions and releases.

To perform an upgrade of an entire cluster from a staging directory installation, where you have ssh access to the other hosts in the cluster:

1. On your staging server, download the release package.

2. Unpack the release package:

```sh
shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
```

3. Change to the extracted directory:

```sh
shell> cd continuent-tungsten2.0.5-11
```

4. The next step depends on your existing deployment:

- If you are upgrading a Multi-Site, Multi-Master deployment:

  If you installed the original service by making use of the `$CONTINUENT_PROFILES` and `$REPLICATOR_PROFILES` environment variables, no further action needs to be taken to update the configuration information. Confirm that these variables are set before performing the validation and update.

  If you did not use these environment variables when deploying the solution, you must load the existing configuration from the current hosts in the cluster before continuing by using `tpm fetch`:

```sh
shell> /tools/tpm fetch --hosts=west1,east2,east3,west1,west2,west3 | --user=tungsten --directory=/opt/continuent
```
**Important**

You must specify ALL the hosts within both clusters within the current deployment when fetching the configuration; use of the `autodetect` keyword will not collect the correct information.

- If you are upgrading any other deployment:

  If you are upgrading any other deployment:

  If you are using the `$CONTINUENT_PROFILES` variable to specify a location for your configuration, make sure that the variable has been set correctly.

  If you are not using `$CONTINUENT_PROFILES`, a copy of the existing configuration must be fetched from the installed Continuent Tungsten installation:

  ```
  shell> ./tools/tpm fetch --hosts=host1,host2,host3,autodetect 
  --user=tungsten --directory=/opt/continuent
  ```

  **Important**

  You must use the version of `tpm` from within the staging directory `./tools/tpm` of the new release, not the `tpm` installed with the current release.

  The current configuration information will be retrieved to be used for the upgrade:

  ```
  shell> ./tools/tpm fetch --hosts=host1,host2,host3 --user=tungsten --directory=/opt/continuent
  ```

  **5.** Check that the update configuration matches what you expect by using `tpm reverse`:

  ```
  shell> ./tools/tpm reverse 
  ```

  ```
  # Options for the dsone data service 
  tools/tpm configure dsone 
  --application-password=password 
  --application-port=3306 
  --application-user=app_user 
  --connectors=host1,host2,host3 
  --datasource-log-directory=/var/log/mysql 
  --install-directory=/opt/continuent 
  --master=host1 
  --members=host1,host2,host3 
  --profile-script=~/.bashrc 
  --replication-password=password 
  --replication-port=13306 
  --replication-user=tungsten 
  --start-and-report=true 
  --user=tungsten 
  --witnesses=192.168.0.1
  ```

  **6.** Run the upgrade process:

  ```
  shell> ./tools/tpm update
  ```

  **Note**

  During the update process, `tpm` may report errors or warnings that were not previously reported as problems. This is due to new features or functionality in different MySQL releases and Continuent Tungsten updates. These issues should be addressed and the `tpm update` command re-executed.

  The following additional options are available when updating:

  - `--no-connectors` (optional)

    By default, an update process will restart all services, including the connector. Adding this option prevents the connectors from being restarted. If this option is used, the connectors must be manually updated to the new version during a quieter period. This can be achieved by running on each host the command:

    ```
    shell> tpm promote-connector
    ```

    This will result in a short period of downtime (couple of seconds) only on the host concerned, while the other connectors in your configuration keep running. During the upgrade, the Connector is restarted using the updated software and/or configuration.

    A successful update will report the cluster status as determined from each host in the cluster:
The update process should now be complete. The current version can be confirmed by starting `cctrl`.

### 4.4.2. Upgrading when using INI-based configuration, or without ssh Access

To perform an upgrade of an individual node, `tpm` can be used on the individual host. The same method can be used to upgrade an entire cluster without requiring `tpm` to have ssh access to the other hosts in the dataservice.

**Warning**

Before performing and upgrade, please ensure that you have checked the Appendix C, Prerequisites, as software and system requirements may have changed between versions and releases.

**Important**

Application traffic to the nodes will be disconnected when the connector restarts. Use the `--no-connectors` `tpm` option when you upgrade to prevent the connectors from restarting until later when you want them to.

To upgrade a cluster using this method there are two methods, switch and no-switch. The switch method employs a manual cluster failover to a new master, the no-switch method does not. Which method you choose depends upon your needs.

#### 4.4.2.1. Upgrading Using the No-Switch Method

To use the no-switch method of upgrading:

1. Place the cluster into maintenance mode
2. Upgrade the slaves in the dataservice. Be sure to shun and welcome each slave.
3. Upgrade the master node

**Important**

Replication traffic to the slaves will be delayed while the replicator restarts. The delays will increase if there are a large number of stored events in the THL. Old THL may be removed to decrease the delay. Do NOT delete THL that has not been received on all slave nodes or events will be lost.

4. Upgrade the connectors in the dataservice one-by-one

**Important**

Application traffic to the nodes will be disconnected when the connector restarts.

5. Place the cluster into automatic mode
4.4.2.2. Upgrading Using the Switch Method

To use the switch method of upgrading:

1. Upgrade the slaves in the dataservice. Be sure to shun and welcome each slave.
2. Switch the current master to one of the upgraded slaves

   Important
   Application and replication traffic will be delayed while the switch occurs.

3. Upgrade the original master node which is now a slave. Be sure to shun and welcome it.
4. Upgrade the connectors in the dataservice one-by-one

   Important
   Application traffic to the nodes will be disconnected when the connector restarts.

4.4.2.3. Upgrading a Single Host using **tpm**

Note
For more information on performing maintenance across a cluster, see Section 5.14.3, “Performing Maintenance on an Entire Datasevice”.

To upgrade a single host using the **tpm** command:

1. Download the release package.
2. Unpack the release package:

   ```shell
tar zxf continuum-tungsten-2.0.5-11.tar.gz
   ```
3. Change to the extracted directory:

   ```shell
cd continuum-tungsten-2.0.5-11
   ```
4. Execute **tpm update**, specifying the installation directory. This will update only this host:

   ```shell
   ./.tools/tpm update --directory=/opt/continuent
   ```

   Configuration loaded from host1

   Getting cluster status on host1
   connect to ‘dsone@host1’
   dsone: session established
   [LOGICAL] /dsone > ls
   
   COORDINATOR[host2:AUTOMATIC:ONLINE]
   ..............................
   Completed: 1 host
   
   Next Steps
   We have added Tungsten environment variables to ~/.bashrc.
   Run ‘source ~/.bashrc’ to rebuild your environment.

   Once your services start successfully you may begin to use the cluster.
   To look at services and perform administration, run the following command from any database server:

   `cctrl`

   Configuration is now complete. For further information, please consult Tungsten documentation, which is available at docs.continuent.com.

   NOTE >> Command successfully completed

To update all of the nodes within a cluster, the steps above will need to be performed individually on each host.

4.4.3. Upgrading from Continuent Tungsten 1.5.3/1.5.4 to Continuent Tungsten 2.0

You can upgrade directly from Continuent Tungsten 1.5.3 or Continuent Tungsten 1.5.4 to Continuent Tungsten 2.0 using the standard update procedures.
When upgrading to Continuent Tungsten 2.0 from Continuent Tungsten 1.5.3/1.5.4, changes to the way witness hosts are used and identified mean that you should modify your configuration before completing the upgrade process.

The witness changes that affect the upgrade are as follows:

1. Witnesses must be on the same network subnet as the existing managers.
2. Dataservices must have at least three managers to provide status check during failure.
3. Active witnesses can be created; these install only the manager on target hosts to act witnesses to check network connectivity to the configured dataserver and connectors configured within the service.

If you are upgrading a host which satisfies conditions [1] and/or [2] in the above list, you can perform an upgrade using `tpm update`.

If your current witness host is not on the same network segment as the rest of your dataservice, the witness host must be removed from the configuration. Alternatively, you can add or update an existing witness host to be an active host witness within the cluster.

To upgrade a cluster and add the required active witnesses to the cluster, or to add additional active witnesses to a cluster which already has the required number of implied witness hosts, the configuration must be upgraded first before deploying the service.

### Note

Active witnesses must have the prerequisites for hosts (Section C.2, "Host Configuration" configured before the update and deployment is completed.

1. On your staging server, download the release package.
2. Unpack the release package:
   ```
   shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
   ```
3. Change into the directory:
   ```
   shell> cd continuent-tungsten-2.0.5-11
   ```
4. Fetch a copy of the existing configuration information:
   ```
   shell> ./tools/tpm fetch --hosts=host1,host2,host3,autodetect --user=tungsten --directory=/opt/continuent
   ```
5. Update the configuration with additional witness hosts:
   ```
   shell> ./tools/tpm configure service_name --enable-active-witnesses=true --witnesses=hostname --members+=hostname
   ```
6. Run the update and installation process:
   ```
   shell> ./tools/tpm update service_name
   ```

If you have multiple services configured that require active witnesses, you must update each service with additional witness hosts.

### 4.4.4. Installing an Upgraded JAR Patch

**Warning**

The following instructions should only be used if Continuent Support have explicitly provided you with a customer JAR file designed to address a problem with your deployment.

If a custom JAR has been provided by Continuent Support, the following instructions can be used to install the JAR into your installation.

1. Determine your staging directory or unarred installation directory:
   ```
   shell> tpm query staging
   ```
   Go to the appropriate host (if necessary) and the staging directory.
   ```
   shell> cd continuent-tungsten-2.0.5-11
   ```
2. Change to the correct directory. For example, to update Tungsten Replicator change to `tungsten-replicator/lib`; for Tungsten Manager use `tungsten-manager/lib`; for Tungsten Connector use `tungsten-connector/lib`:
   ```
   shell> cd tungsten-replicator/lib
   ```
3. Copy the existing JAR to a backup file:

```shell
cp tungsten-replicator.jar tungsten-replicator.jar.orig
```

4. Copy the replacement JAR into the directory:

```shell
cp /tmp/tungsten-replicator.jar ...
```

5. Change back to the root directory of the staging directory:

```shell
cd ../..
```

6. Update the release:

```shell
./tools/tpm update --replace-release
```

### 4.5. Downgrading to an Earlier Release

If after upgrading Continuent Tungsten you are experiencing problems, and Continuent Support have suggested that you downgrade to an earlier version of Continuent Tungsten, follow these steps to revert your existing Continuent Tungsten installation.

1. Redirect all users directly to the MySQL server on the master. This may require changing applications and clients to point directly to the MySQL servers. You cannot use Tungsten Connector to handle this for you, since the entire cluster, including the Tungsten Connector services, will be removed.

2. Stop Tungsten services on all servers:

```shell
stopall
```

3. Downgrading to Continuent Tungsten 2.0.x

   For Continuent Tungsten 2.0.x, the information stored in the database schema for the service, for example `tungsten_alpha`, can remain in place, unless you are changing the service name.

Downgrading to Continuent Tungsten 1.5.x

When downgrading to a release earlier than Continuent Tungsten 2.0, the schema used to hold information must be updated. You must rebuild the `tungsten` schema on all database servers in the updated cluster. This requires a number of different steps:

First, disable logging the statements to the binary log; this information does not need to be replicated around the cluster, even after restart:

```sql
SET SESSION SQL_LOG_BIN=0;
```

Now delete the `tungsten` schema in preparation for it to be recreated. Within Continuent Tungsten 1.5.4, information about the replication state is stored in the `tungsten` schema; within Continuent Tungsten 2.0.1 the information is stored within a schema matching the service name, for example the service `alpha` would be stored in the schema `tungsten_alpha`.

```sql
DROP SCHEMA IF EXISTS `tungsten`;
CREATE SCHEMA `tungsten`;
USE tungsten;
```

Now create the tables to store the status information:

```sql
CREATE TABLE `consistency` (
  `db` char(64) NOT NULL DEFAULT '',
  `tbl` char(64) NOT NULL DEFAULT '',
  `id` int(11) NOT NULL DEFAULT '0',
  `row_offset` int(11) NOT NULL,
  `row_limit` int(11) NOT NULL,
  `this_crc` char(40) DEFAULT NULL,
  `this_cnt` int(11) DEFAULT NULL,
  `master_crc` char(40) DEFAULT NULL,
  `master_cnt` int(11) DEFAULT NULL,
  `ts` timestamp NULL DEFAULT NULL,
  `method` char(32) DEFAULT NULL,
  PRIMARY KEY (`db`,`tbl`,`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```sql
CREATE TABLE `heartbeat` (
  `id` bigint(20) NOT NULL DEFAULT '0',
  `seqno` bigint(20) DEFAULT NULL,
  `eventid` varchar(32) DEFAULT NULL,
  `source_tstamp` timestamp NULL DEFAULT NULL,
  `target_tstamp` timestamp NULL DEFAULT NULL,
  `lag_millis` bigint(20) DEFAULT NULL,
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```
Now import the current sequence number from the existing Continuent Tungsten `trep_commit_seqno` table:

```sql
mysql> INSERT INTO tungsten.trep_commit_seqno
    
    (seqno, fragno, last_frag, source_id, epoch_number,
    eventid, applied_latency, update_timestamp)
    SELECT seqno, fragno, last_frag, source_id, epoch_number,
    eventid, applied_latency, update_timestamp
    FROM TUNGSTEN_SERVICE_SCHEMA.trep_commit_seqno;
```

Check the sequence number:

```sql
mysql> SELECT * FROM tungsten.trep_commit_seqno;
```

If the sequence number doesn’t match on all servers, update the tungsten schema on the master with the earliest information (i.e. lowest sequence number):

```sql
mysql> SET SQL_LOG_BIN=0;
mysql> UPDATE tungsten.trep_commit_seqno SET seqno=###,epoch_number=###,eventid=SSSSS;
```

4. Extract the release of Continuent Tungsten that should be installed instead, and then using `tpm fetch` to retrieve the current configuration.

```bash
shell> ./tools/tpm fetch --user=tungsten --hosts=host1,host2,host3,host4
    --release-directory=/opt/continuent
```

Note

In the event that the `tpm fetch` operation fails to detect the current configuration, run `tpm reverse` on one of the machines in the configured service. This will output the current configuration. If necessary, execute `tpm reverse` on multiple hosts to determine whether the information matches.

If you execute the returned text from `tpm reverse`, it will configure the service within the local directory, and the installation can then be updated.

Ensure that the current master is listed as the master within the configuration.

Now update Continuent Tungsten to deploy the new release:

```bash
shell> ./tools/tpm update
```

5. Start all the services on the master:

```bash
shell> startall
```

Confirm that the current master is correct within `trepctl` and `cctrl`. 

---

**Deployment: Advanced**

```sql
CREATE TABLE `history` (  
    `seqno` bigint(20) NOT NULL DEFAULT '0',  
    `fragno` smallint(6) NOT NULL DEFAULT '0',  
    `last_frag` char(1) DEFAULT NULL,  
    `source_id` varchar(128) DEFAULT NULL,  
    `type` tinyint(4) DEFAULT NULL,  
    `epoch_number` bigint(20) DEFAULT NULL,  
    `source_tstamp` timestamp NULL DEFAULT NULL,  
    `local_enqueue_tstamp` timestamp NULL DEFAULT NULL,  
    `processed_tstamp` timestamp NULL DEFAULT NULL,  
    `status` tinyint(4) DEFAULT NULL,  
    `comments` varchar(128) DEFAULT NULL,  
    `eventid` varchar(128) DEFAULT NULL,  
    `event` longblob,  
    PRIMARY KEY (`seqno`,`fragno`),  
    KEY `eventid` (`eventid`)  
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```sql
CREATE TABLE `trep_commit_seqno` (  
    `seqno` bigint(20) DEFAULT NULL,  
    `fragno` smallint(6) DEFAULT NULL,  
    `last_frag` char(1) DEFAULT NULL,  
    `source_id` varchar(128) DEFAULT NULL,  
    `epoch_number` bigint(20) DEFAULT NULL,  
    `eventid` varchar(128) DEFAULT NULL,  
    `applied_latency` int(11) DEFAULT NULL,  
    `update_timestamp` timestamp NULL DEFAULT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

---

114
6. Start the services on remaining servers:

   ```shell
   startall
   ```

7. If you were using a composite data service, you must recreate the composite dataservice configuration manually.

8. Once all the services are back up and running, it is safe to point users and applications at Tungsten Connector and return to normal operations.

### 4.6. Converting to a Different Topology

In this chapter we will provide procedures to convert one type of topology to another.

**Important**

Most, if not all, of the following conversion procedures will require a maintenance window and application downtime because the entire cluster is affected.

#### 4.6.1. Converting from Standalone to Composite Primary/DR for INI-based Deployments

This procedure will convert a standard, standalone cluster into a Composite Primary/DR cluster for a deployment that uses INI files for configuration.

Our example starting cluster has 5 nodes (1 master and 4 slaves) and uses service name `alpha`. Our target cluster will have 6 nodes (3 per cluster) in 2 member clusters `alpha_east` and `alpha_west` in composite service `alpha`.

This means that we will reuse the existing service name `alpha` as the name of the new composite service, and create two new service names, one for each cluster (`alpha_east` and `alpha_west`).

Below is an INI file extract example for our starting standalone cluster with 5 nodes:

```ini
[defaults] ...
[alpha]
connectors=db1,db2,db3,db4,db5
master=db1
members=db1,db2,db3,db4,db5
topology=clustered
```

To convert the above configuration to a Composite Primary/DR:

1. First you must stop all services on all existing nodes.

   ```shell
   stopall
   ```

2. Update `tungsten.ini` on all nodes.

   Create the two new services and put the correct information into all three stanzas.

   For example, below is an INI file extract example for our target composite cluster with 6 nodes:

   ```ini
   [defaults]
   start-and-report=false
   start=false ...
   [alpha_east]
   connectors=db1,db2,db3
   master=db1
   members=db1,db2,db3
topology=clustered
   [alpha_west]
   connectors=db4,db6
   master=db4
   members=db4,db5,db6
topology=clustered
   relay-source=alpha_east
   [alpha]
   composite-datasources=alpha_east,alpha_west
   ```

3. Invoke the conversion using the `tpm` command from the software extraction directory:

   ```shell
   tpm query staging
   ```
4. Finally, start all services on all existing nodes.

```shell
shell> startall
```

### 4.7. Removing Datasources, Managers or Connectors

Removing components from a datasevice is quite straightforward, usually involved both modifying the running service and changing the configuration. Changing the configuration is necessary to ensure that the host is not re-configured and installed when the installation is next updated.

In this section:

- Section 4.7.1, “Removing a Datasource from an Existing Deployment”
- Section 4.7.3, “Removing a Connector from an Existing Deployment”

#### 4.7.1. Removing a Datasource from an Existing Deployment

To remove a datasource from an existing deployment there are two primary stages, removing it from the active service, and then removing it from the active configuration.

For example, to remove `host6` from a service:

1. Check the current service state:

```shell
[LOGICAL]/alpha > ls

COORDINATOR[host1:AUTOMATIC:ONLINE]

ROUTERS:
+----------------------------------------------------------------------------+
| connector@host1[11401](ONLINE, created=17, active=0)                        |
| connector@host2[7998](ONLINE, created=0, active=0)                          |
| connector@host3[31540](ONLINE, created=0, active=0)                         |
| connector@host4[26829](ONLINE, created=27, active=1)                        |
+----------------------------------------------------------------------------+

DATASOURCES:
+----------------------------------------------------------------------------+
| host1(slave:ONLINE, progress=373, latency=0.000)                            |
| STATUS [OK] [2014/02/12 12:48:14 PM GMT]                                    |
| MANAGER(state=ONLINE)                                                      |
| REPLICATOR(role=slave, master=host6, state=ONLINE)                         |
| DATASERVER(state=ONLINE)                                                   |
| CONNECTIONS(created=30, active=0)                                          |
+----------------------------------------------------------------------------+
+----------------------------------------------------------------------------+
| host2(slave:ONLINE, progress=373, latency=1.000)                            |
| STATUS [OK] [2014/01/24 05:02:34 PM GMT]                                    |
| MANAGER(state=ONLINE)                                                      |
| REPLICATOR(role=slave, master=host6, state=ONLINE)                         |
| DATASERVER(state=ONLINE)                                                   |
| CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
+----------------------------------------------------------------------------+
| host3(slave:ONLINE, progress=373, latency=1.000)                            |
| STATUS [OK] [2014/02/11 03:17:08 PM GMT]                                    |
| MANAGER(state=ONLINE)                                                      |
| REPLICATOR(role=slave, master=host6, state=ONLINE)                         |
| DATASERVER(state=ONLINE)                                                   |
| CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
+----------------------------------------------------------------------------+
| host6(master:ONLINE, progress=373, THL latency=0.936)                      |
| STATUS [OK] [2014/02/12 12:39:52 PM GMT]                                    |
| MANAGER(state=ONLINE)                                                      |
| REPLICATOR(role=master, state=ONLINE)                                      |
```

2. Remove the datasource:

```shell
cd {software_staging_dir_from_tpm_query}
./tools/tpm update --replace-release
rm /opt/cont/tung/cluster-home/conf/cluster/*/datasource/*
```
2. Switch to **MAINTENANCE** policy mode:

```
[LOGICAL] /alpha > set policy maintenance
policy mode is now MAINTENANCE
```

3. Switch to administration mode:

```
[LOGICAL] /alpha > admin
```

4. Remove the node from the active service using the `rm` command. You will be warned that this is an expert command and to confirm the operation:

```
[ADMIN] /alpha > rm host6
WARNING: This is an expert-level command:
Incorrect use may cause data corruption
or make the cluster unavailable.
Do you want to continue? (y/n)> y
```

5. Switch back to logical mode:

```
[ADMIN] /alpha > logical
```

6. Switch to **AUTOMATIC** policy mode:

```
[LOGICAL] /alpha > set policy automatic
policy mode is now AUTOMATIC
```

Now the node has been removed from the active dataservice, the services must be stopped and then removed from the configuration.

1. Stop the running services:

```
shell> stopall
```

2. Now you must remove the node from the configuration, although the exact method depends on which installation method used with `tpm`:

- If you are using staging directory method with `tpm`:
  a. Change to the staging directory. The current staging directory can be located using `tpm query staging`:

```
shell> tpm query staging
```

```
tungsten@host1:/home/tungsten/continuent-tungsten-2.0.5-11
```

```
shell> cd /home/tungsten/continuent-tungsten-2.0.5-11
```

  b. Update the configuration, omitting the host from the list of members of the dataservice:

```
shell> tpm update alpha
--connectors=host1,host2,host3,host4
--members=host1,host2,host3
```

- If you are using the INI file method with `tpm`:

  • Remove the INI configuration file:

```
shell> rm /etc/tungsten/tungsten.ini
```

3. Stop the replicator/manager from being started again.

- If this all the services on the this node, replicator, manager and connector are being removed, remove the Continuent Tungsten installation entirely:

  • Remove the startup scripts from your server:

```
shell> sudo /opt/continuent/tungsten/cluster-home/bin/undeployall
```

  • Remove the installation directory:

```
shell> rm -rf /opt/continuent
```

- If the replicator/manager has been installed on a host but the connector is not being removed, remove the start scripts to prevent the services from being automatically started:
4.7.2. Removing a Composite Datasource/Cluster from an Existing Deployment

To remove an entire composite datasource [cluster] from an existing deployment there are two primary stages, removing it from the active service, and then removing it from the active configuration.

For example, to remove cluster `west` from a composite dataservice:

1. Check the current service state:

```
[shell] > cctrl -multi
DATA SERVICES:
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>east</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>west</td>
</tr>
</tbody>
</table>
```

2. Switch to `MAINTENANCE` policy mode:

```
[LOGICAL] / > use global
[LOGICAL] /global > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]
DATASOURCES:
|east(composite master:ONLINE) |
|STATUS [OK] [2017/05/16 01:25:30 PM UTC] |

[LOGICAL] /global > set policy maintenance
policy mode is now MAINTENANCE
```

3. Remove the composite member cluster from the composite service using the `drop` command.

```
[LOGICAL] /global > drop composite datasource west
COMPOSITE DATA SOURCE 'west@global' WAS REMOVED
[LOGICAL] / > ls
```

4. If the removed composite datasource still appears in the top-level listing, then you will need to clean up by hand. For example:

```
[LOGICAL] / > ls
```

Stop all managers on all nodes at the same time
Before:
east=db1,db2,db3
west=db4,db5,db6

After:
east=db1,db2,db3

Start all managers one-by-one, starting with the current master

Once all managers are running, check the list again:

5. Switch to AUTOMATIC policy mode:

Now the cluster has been removed from the composite dataservice, the services on the old nodes must be stopped and then removed from the configuration.

1. Stop the running services on all nodes in the removed cluster:

2. Now you must remove the node from the configuration, although the exact method depends on which installation method used with tpm:
   
   • If you are using staging directory method with tpm:
     
     a. Change to the staging directory. The current staging directory can be located using tpm query staging:

     b. Update the configuration, omitting the cluster datasource name from the list of members of the dataservice:

   • If you are using the INI file method with tpm:
     
     • Remove the INI configuration file:

3. Stop the replicator/manager from being started again.
   
   • If this all the services on the this node, replicator, manager and connector are being removed, remove the Continuent Tungsten installation entirely:
     
     • Remove the startup scripts from your server:

     • Remove the installation directory:

     • If the replicator/manager has been installed on a host but the connector is not being removed, remove the start scripts to prevent the services from being automatically started:
4.7.3. Removing a Connector from an Existing Deployment

Removing a connector involves only stopping the connector and removing the configuration. When the connector is stopped, the manager will automatically remove it from the dataservice. Note that applications that have been configured to talk to the connector must be updated to point to another connector.

For example, to remove host4 from the current dataservice:

1. Login to the host running the connector.
2. Stop the connector service:

```shell
template
```

3. Remove the connector from the configuration, the exact method depends on which installation method used with `tpm`:

   a. Change to the staging directory. The current staging directory can be located using `tpm query staging`:

```shell
template
```

   b. Update the configuration, omitting the host from the list of members of the dataservice:

```shell
template
```

   • If you are using the INI file method with `tpm`:

```shell
template
```

4. Stop the connector from being started again. If the connector is restarted, it will connect to the previously configured masters and begin operating again.

   • If this is a standalone Connector installation, remove the Continuent Tungsten installation entirely:

```shell
template
```

   • Remove the startup scripts from your server:

```shell
template
```

   • Remove the installation directory:

```shell
template
```

   • If the connector has been installed on a host with replicator and/or managers, remove the start script to prevent the connector from being automatically started:

```shell
template
```
Chapter 5. Operations Guide

Continuent Tungsten™ has a wide range of tools and functionality available for checking and managing the status of a dataservice. The majority of the management and information structure is based around a small number of command-line utilities that provide a complete range of tools and information, either through a direct command-line, or secondary shell like interface.

When installing the dataservice using `tpm`, if requested, the login script for the staging user (for example `.bashrc`) will have been updated to execute a script within the installation directory called `env.sh`. This configures the location of the installation, configuration, and adds the script and binary directories to the `PATH` so that the commands can be executed without having to use the full path to the tools.

If the script was not added to the login script automatically, or needs to be added to the current session, the script is located within the `share` directory of the installation directory. For example, `/opt/continuent/share/env.sh`. To load into the current session use `source`. See Section 5.2, "Establishing the Shell Environment" for more information.

```
shell> source /opt/continuent/share/env.sh
```

The main tool for controlling dataservices is `cctrl`. This provides a shell like interface for querying and managing the dataservice and includes shell-like features such as command history and editing. Commands can be executed using `cctrl` either interactively:

```
shell> cctrl
ctrl
connect to 'alpha@host1'
alpha: session established
[LOGICAL:EXPERT] /alpha >
ls
```

Or by supplying a command and piping that as input to the `cctrl` shell:

```
shell> echo 'ls' | cctrl
```

5.1. The Continuent Tungsten Home Directory

After installing Continuent Tungsten the home directory will be filled with a set of new directories. The home directory is specified by `--home-directory` or `--install-directory`. If you have multiple installations on a single server; each directory will include the same entries.

- `tungsten` - A symlink to the most recent version of the software. The symlink points into the `releases` directory. You should always use the symlink to ensure the most recent configuration and software is used.
- `releases` - Storage for the current and previous versions of the software. During an upgrade the new software will be copied into this directory and the `tungsten` symlink will be updated. See Section E.1.2, "The releases Directory" for more information.
- `service_logs` - Includes symlinks to the primary log for the replicator, manager and connector. This directory also includes logs for other tools distributed for Continuent Tungsten.
- `backups` - Storage for backup files created through `trepctl` or `cctrl`. See Section E.1.1, "The backups Directory" for more information.
- `thl` - Storage for THL files created by the replicator. Each replication service gets a dedicated sub-directory for storing THL files. See Section E.1.5, "The thl Directory" for more information.
- `relay` - Temporary storage for downloaded MySQL binary logs before they are converted into THL files.
- `share` - Storage for files that must persist between different software versions. The `env.sh` script will setup your shell environment to allow easy access to Continuent Tungsten tools.

5.2. Establishing the Shell Environment

The tools required to operate Continuent Tungsten are located in many directories around the home directory. The best way to access them is by setting up your shell environment.

The `env.sh` file will automatically be included if you specify the `--profile-script` during installation. This option may be included during a configuration change with `tpm update`.

If the `env.sh` file hasn't been included you may do so by hand with `source`.

```
shell> source /opt/continuent/share/env.sh
```

Important

Special consideration must be taken if you have multiple installations on a single server. That applies for clustering and replication or multiple replicators.

Include the `--executable-prefix` [in [Tungsten Replicator 2.2 Manual]] and `--profile-script` options in your configuration. Instead of extending the `PATH` variable; the `env.sh` script will define aliases for each command. If you
specified --executable-prefix=mm [in Tungsten Replicator 2.2 Manual] the trepctl command would be accessed as mm_trepctl.

5.3. Checking Dataservice Status

The `cctrl` command provides the main interface to the dataservice information and control. The current status and configuration of the dataservice can be determined by using the `ls` command within the `cctrl` shell:

```
shell> cctrl
Continuent Tungsten 2.0.5 build 11
connect to alpha@host1
alpha: session established
[LOGICAL:EXPERT] /alpha > ls
COORDINATOR[host1:AUTOMATIC:ONLINE]

RUTERS:
[connector@host1[8805](ONLINE, created=0, active=0)
[connector@host2[12039](ONLINE, created=0, active=0)
[connector@host3[12712](ONLINE, created=0, active=0)

DATASOURCES:
[host1(master:ONLINE, progress=3, THL latency=0.561]
[STATUS [OK] [2013/05/03 09:11:10 PM BST]
| MANAGER(state=ONLINE]
| REPLICATOR(role=master, state=ONLINE]
| DATASERVER(state=ONLINE]
| CONNECTIONS(created=0, active=0]

[host2(slave:ONLINE, progress=3, latency=1.243]
[STATUS [OK] [2013/05/04 05:40:43 AM BST]
| MANAGER(state=ONLINE]
| REPLICATOR(role=slave, master=host1, state=ONLINE]
| DATASERVER(state=ONLINE]
| CONNECTIONS(created=0, active=0]

[host3(slave:ONLINE, progress=3, latency=0.000]
[STATUS [OK] [2013/05/04 07:40:12 AM BST]
| MANAGER(state=ONLINE]
| REPLICATOR(role=slave, master=host1, state=ONLINE]
| DATASERVER(state=ONLINE]
| CONNECTIONS(created=0, active=0]
```

The output consists of the following major sections:

- **COORDINATOR**

  The coordinator is the node in the dataservice that is acting as the manager for the dataservice. The coordinator is decided upon within the dataservice by a consensus agreement, and the coordinator can change in the event of a failure of the existing coordinator. The coordinator is always the oldest datasource within the group that manages the dataservice, and does not need to be the same host as the master.

  The information about the coordinator is described in the following square brackets as `HOSTNAME:POLICY:STATUS`, where:

  - **HOSTNAME**
    
    The hostname of the current coordinator.

  - **POLICY**
    
    The current policy manager mode, which describes how the manager will respond to certain events. For example, in *AUTOMATIC* mode the manager will respond to issues and problems automatically, for example by performing an automatic master switch during a failover event.

    For more information on policy modes, see Section 5.4, "Policy Modes".

  - **STATUS**
The current status of the coordinator host.

- **ROUTERS**

A list of the currently configured SQL routers (using Tungsten Connector™) that are directing queries to the datasources. In the example, the dataservice consists of three routers, each connected to all of the configured data sources. The information output includes a summary of the number of connections made through the router, and the number of active connections to each router.

- **DATASOURCES**

The DATASOURCES section lists detailed information providing one block for each configured datasource. The header block of the datasource output describes the overall status of the datasource:

```
+----------------------------------------------------------------------------+
| host1(master:ONLINE, progress=3, THL latency=0.561)                     |
| STATUS [OK] [2013/05/03 09:11:10 PM BST]                             |
+----------------------------------------------------------------------------+
```

The first line describes the host and status information:

- Hostname of the datasource (host1)
- Current role within the dataservice and status of the datasource. For more information on roles, see Section 5.3.3, "Understanding Datasource Roles". For information on datasource states, see Section 5.3.4, "Understanding Datasource States".
- The `progress` indicates the current sequence number from the THL for the datasource.
- The `THL latency` shows the current latency of the datasource. For a master datasource using MySQL, this is the latency between the data being written to the MySQL binary log and being processed in the THL. For a slave, it shows the latency between the original commit (from the master) and the application on the slave.

The second line provides a more detailed current status, and the time since the status was last changed. In the event of a change of status, for example to the SHUNNED or OFFLINE state, the time will indicate how long the node has been in that status.

- The remaining lines of the datasource description provide detailed information about each of the remaining services on the datasource and their status. The list will depend on the assigned roles and parameters for each datasource. It is important to note that each service has a status that is independent of the overall datasource status.

- `| MANAGER(state=ONLINE) |
- The Manager service, and the current status of the manager. If a configured datasource is down, has recently been restarted, or the manager has been stopped, the status may be offline.

- `| REPLICATOR(role=slave, master=host1, state=ONLINE) |
- The Tungsten Replicator service, which replicates data between hosts. The status shows the current role (slave), the master host, and the current status of the replicator.

- `| DATASERVER(state=ONLINE) |
- The status of the dataserver service, which indicates the status of the underlying database service.

- `| CONNECTIONS(created=0, active=0) |
- The Tungsten Connector service, showing the number of connections have been created on this service, and the number that are currently active.

The main service status output, as provided by `ls` at the top level, provides a quick overview of the overall status of the dataservice. More detailed information on each service, and the current status of the individual services can be monitored and managed through `cctrl`.

### 5.3.1. Latency or Relative Latency Display

Continuent Tungsten can operate using either absolute or relative latency. The two are distinguished according to how the difference between transaction commit times are handled:

- **Absolute latency** — [default] is the difference between when a transaction was applied to a slave and when the transaction was originally applied to the master.
- **Relative latency** — is the difference between now and when the last transaction was written to the slave.

Absolute latency indicates the difference between transaction times, but, may also provide a misleading impression of the cluster state if there are large transactions being applied, or if the slave has stopped or become ‘stuck’ due to a transient failure. This is because absolute la-
tency shows the time difference between transactions. If a transaction takes 5 or 10 seconds to apply, the absolute latency will only display the difference between when the transaction was written, and only after this has occurred on both the master and the slave. The actual time difference between these may be less than a second, even though the transaction took 10 seconds to succeed.

Relative latency shows the time difference between the last transaction committed and the current time, hence if the transaction takes a considerable time to be applied, the relative latency will increase up until the transaction has finally been committed. If the relative latency increases and continues to increase, it may indicate a lagging or even failed slave.

To enable relative latency, the cluster must have been deployed, or updated, using the `--use-relative-latency=true` option to `tpm`. Once enabled, the following operational activities change:

- The output of `show slave status` when connected to MySQL through a connector will be updated so that the `Seconds_Behind_Master` field shows the relative, rather than absolute, latency. For example, in a cluster where relative latency is enabled, but no transactions are occurring, the output will show an increasing value:

  ```
  mysql> show slave status
  +-----------------------+-------------+
  | Seconds_Behind_Master | 0           |
  +-----------------------+-------------+
  1 row in set (0.01 sec)
  mysql> show slave status
  +-----------------------+-------------+
  | Seconds_Behind_Master | 7           |
  +-----------------------+-------------+
  1 row in set (0.01 sec)
  mysql> show slave status
  +-----------------------+-------------+
  | Seconds_Behind_Master | 38          |
  +-----------------------+-------------+
  1 row in set (0.01 sec)
  ```

- `cctrl` will output an additional field, `relative`, showing the relative latency value against the standard latency value. This can be seen in the example below:

  ```
  [LOGICAL] /alpha > ls
  COORDINATOR[host1:automatic:online]
  ROUTERS:
  +----------------------------------------------------------------------------+
  | connector@host1[6189](online, created=1, active=6)                     |
  +----------------------------------------------------------------------------+
  DATASOURCES:
  +----------------------------------------------------------------------------+
  | host1(master:online, progress=5, THL latency=1.008, relative=144.636) |
  | STATUS [OK] [2014/09/07 02:28:54 PM BST]                               |
  | MANAGER(state=online)                                                   |
  | REPLICATOR(role=master, state=online)                                   |
  | DATASERVER(state=online)                                                |
  | CONNECTIONS(created=4, active=1)                                        |
  +----------------------------------------------------------------------------+
  +----------------------------------------------------------------------------+
  | host2(slave:online, progress=5, latency=0.000, relative=144.638)       |
  | STATUS [OK] [2014/09/07 02:28:58 PM BST]                               |
  | MANAGER(state=online)                                                   |
  | REPLICATOR(role=slave, master=host1, state=online)                     |
  | DATASERVER(state=online)                                                |
  | CONNECTIONS(created=1, active=1)                                        |
  +----------------------------------------------------------------------------+
  +----------------------------------------------------------------------------+
  | host3(slave:online, progress=5, latency=5.938, relative=144.620)        |
  | STATUS [OK] [2014/09/07 02:29:13 PM BST]                               |
  | MANAGER(state=online)                                                   |
  | REPLICATOR(role=slave, master=host1, state=online)                     |
  | DATASERVER(state=online)                                                |
  | CONNECTIONS(created=0, active=0)                                        |
  +----------------------------------------------------------------------------+
  ```

- The Tungsten Connector will use the value when the `maxAppliedLatency` option is used in the connection string to determine whether to route a connection to a master or a slave.
For example, when running a script that sends a heartbeat, and then connects through a connector, the connection will be routed first to the slave, and then to the master:

```bash
echo "cluster heartbeat" | cctrl
sleep 1
mysql -utungsten_testing -pprivate --port=9999 --host=`hostname`
mysql@maxAppliedLatency=20?qos=RO_RELAXED -e"select 1;tungsten connection status;"
sleep 21
mysql -utungsten_testing -pprivate --port=9999 --host=`hostname`
mysql@maxAppliedLatency=20?qos=RO_RELAXED -e"select 1;tungsten connection status;"
```

The output of the execution of the script shows the slave and then master connections:

```
[LOGICAL] /alpha > cluster heartbeat
HEARTBEAT 'DEFAULT' INSERTED
[LOGICAL] /alpha >
Exiting...
```

5.3.2. Getting Detailed Information

Detailed information about the individual nodes, datasources and services within the dataservice can be obtained by using the hierarchical structure of the dataservice as presented through `cctrl`. By using the `-l` command-line option detailed information can be obtained about any object. For example, getting the detailed listing of a specific host produces the following:

```
[LOGICAL:EXPERT] /alpha > ls -l host1
COORDINATOR[host1:AUTOMATIC:ONLINE]
ROUTERS:
+----------------------------------------------------------------------------+
| connector@host1[18348](ONLINE, created=403, active=0)                       |
| host1(master:ONLINE, created=195, active=0)                               |
| host2(slave:ONLINE, created=0, active=0, latency=146.000)                 |
| host3(slave:ONLINE, created=208, active=0, latency=31.000)                |
| gateway:host2                                                             |
+----------------------------------------------------------------------------+
DATASOURCES:
+----------------------------------------------------------------------------+
| host1(master:ONLINE, progress=154146, THL latency=0.390)                    |
| activeConnectionsCount: 8                                                  |
| alertMessage:                                                             |
| alertStatus: OK                                                           |
| alertTime: 1368209428766                                                    |
| appliedLatency: 0.0                                                        |
| callableStatementsCreatedCount: 8                                        |
| connectionsCreatedCount: 193                                               |
```

125
5.3.3. Understanding Datasource Roles

All datasources within a dataservice have a specific role within the dataservice. The **master** role is one that provides a source of replication information, and a slave one that receives that information.

<table>
<thead>
<tr>
<th>Role</th>
<th>Supplies Replication Data</th>
<th>Receives Replication Data</th>
<th>Load Balancing</th>
<th>Failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Slave</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The information output is very detailed and provides a summary of all the configuration and status information for the given host. The connector information shows connectors made to each configureddataserver by each connector service. The datasource section shows detailed information on the dataserver and replicator services. The output from the replicator service is equivalent to that output by `trepctl`.

---

```java
null:REPLICATOR(role=master, state=ONLINE)
```

---

The information output is very detailed and provides a summary of all the configuration and status information for the given host. The connector information shows connectors made to each configured dataserver by each connector service. The datasource section shows detailed information on the dataserver and replicator services. The output from the replicator service is equivalent to that output by `trepctl`.

### 5.3.3. Understanding Datasource Roles

All datasources within a dataservice have a specific role within the dataservice. The **master** role is one that provides a source of replication information, and a slave one that receives that information.
Roles | Supplies Replication Data | Receives Replication Data | Load Balancing | Failover
---|---|---|---|---
Slave | No | Yes | Yes | Yes
Standby | No | Yes | No | Yes
Archive | No | Yes | Yes | No

More detailed information for each role:

- **master**
  A datasource in a master role is providing a source for replication information to other datasources in the dataservice and is able to provide both read and write connections for applications.

- **slave**
  A slave datasource is receiving data from a master and having that replicated data applied by Continuent Tungsten. Slaves are used for read-only operations by applications.

- **standby**
  A standby datasource receives replication data, but is never chosen by the connector to act as a read source by application clients. Standby datasources are therefore kept up to date with replication, but not used for load balancing.

  When a failover occurs, a standby datasource can be enabled as a standard slave and included in load-balanced operations.

- **archive**
  An archive datasource can be used to provide an active (up to date) copy of the data, without the datasource being used in the event of a failover. This can be useful for providing backup support, offline querying outside of the normal dataservice operations, or auditing purposes.

### 5.3.4. Understanding Datasource States

All datasources will be in one of a number of states that indicate their current operational status.

#### 5.3.4.1. ONLINE State

A datasource in the ONLINE state is considered to be operating normally, with replication, connector and other traffic being handled as normal.

#### 5.3.4.2. SHUNNED State

A SHUNNED datasource implies that the datasource is OFFLINE. Unlike the OFFLINE state, a SHUNNED datasource is not automatically recovered.

A datasource in a SHUNNED state is not connected or actively part of the dataservice. Individual services can be reconfigured and restarted. The operating system and any other maintenance to be performed can be carried out while a host is in the SHUNNED state without affecting the other members of the dataservice.

Datasources can be manually or automatically shunned. The current reason for the SHUNNED state is indicated in the status output. For example, in the sample below, the node host3 was manually shunned for maintenance reasons:

```plaintext
+----------------------------------------------------------------------------+
|host3(slave:SHUNNED(MANUALLY-SHUNNED), progress=157454, latency=1.000)     |
|STATUS [SHUNNED] [2013/05/14 05:12:52 PM BST]                             |
+----------------------------------------------------------------------------+
```

#### 5.3.4.3. OFFLINE State

A datasource in the OFFLINE does not accept connections through the connector for either reads or writes.

When the dataservice is in the AUTOMATIC policy mode, a datasource in the OFFLINE state is automatically recovered and placed into the ONLINE state. If this operation fails, the datasource remains in the OFFLINE state.

When the dataservice is in the MAINTENANCE or MANUAL policy mode, the datasource will remain in the OFFLINE state until the datasource is explicitly switched to the ONLINE state.

#### 5.3.4.4. FAILED State

When a datasource fails, for example when a failure in one of the services for the datasource stops responding or fails, the datasource will be placed into the FAILED state. In the example below, the underlying dataserver has failed:

```plaintext
+----------------------------------------------------------------------------+
|host3(slave:FAILED)                                                        |
|STATUS [FAILED] [2013/05/14 05:12:52 PM BST]                              |
+----------------------------------------------------------------------------+
```
For a **FAILED** datasource, the **recover** command within **cctrl** can be used to attempt to recover the datasource to the operational state. If this fails, the underlying fault must be identified and addressed before the datasource is recovered.

### 5.3.5. Changing Datasource States

Changing the status of a service is required either when the dataservice needs to be reconfigured, the topology altered, or when performing system maintenance.

The datasource status can be changed by using the **datasource** command, which accepts the datasource name and a sub-command:

```
datasource DATASOURCENAME SUBCOMMAND
```

For example, to shun the node **host1**:  
```
[LOGICAL:EXPERT] /alpha > datasource host1 shun
```

For detailed operations for different subcommands, see the following sections.

#### 5.3.5.1. Shunning a Datasource

Shunning a datasource identifies the source as unavailable; a shunned slave will not be used during a failover or switch operation.

Datasources can be automatically or manually shunned:

- **Automatic** shunning occurs when the dataservice is in **automatic** policy mode, and the datasource has become unresponsive or fails. For example, when a master fails, an automatic switch to a new master is performed, and the old master is shunned.

- **Manual** shunning occurs when the **shun** command is given to a datasource. Manual shunning can be used to set a datasource into a state that allows for maintenance and management operations to be performed on the datasource.

To manually shun the datasource:

```
[LOGICAL:EXPERT] /alpha > datasource host3 shun
```

DataSource 'host3' set to **SHUNNED**

Once shunned, the connector will stop using the datasource. The status can be checked using **ls**:

```
+----------------------------------------------------------------------------+
|host3(slave:SHUNNED(MANUALLY-SHUNNED), progress=157454, latency=1.000)      |
|STATUS [SHUNNED] [2013/05/14 05:24:41 PM BST]                               |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=slave, master=host2, state=ONLINE)                        |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
```

**Important**

Shunning a datasource does not stop the replicator; replication will continue on a shunned datasource until the replication service is explicitly placed into the offline state.

The level of the shunning is reported in the status as a manual operation. A manually shunned datasource can be enabled using the **datasource recover** command, see Section 5.3.5.2, “Recover a Datasource”.

#### 5.3.5.2. Recover a Datasource

The **datasource recover** command is a deeper operation that performs a number of operations to get the datasource back into the operational state. When used, the **datasource recover** command performs the following operations:

- Restarts failed or stopped services
- Changes the datasource configuration so that it is configured as a master or slave. For example, an automatically failed master will be reconfigured to operate as a slave to the current master.
- Restarts the replicator service in the slave or master role as appropriate
In all cases, the `datasource recover` command should be used if a datasource is offline or shunned, and it can be used at all times to get a datasource back in to operational state within the cluster. In essence, `recover` performs the same operations automatically as would be performed manually to get the node into the right state.

During the recovery process, the node will be checked, replication reconfigured, and the node brought back in to active service. If this process fails because the databases and replication states are out of sync and cannot be recovered, Continuent Tungsten may advise that a backup of another datasource and recovery to this datasource is performed. For more information on restoring from backups, see Section 5.10, “Restoring a Backup”.

### 5.3.5.3. Offline a Datasource

A datasource can be explicitly placed into offline mode. In offline mode, client applications connections to datasources are paused. When switching to OFFLINE mode existing connections are given a five-second grace period to complete their operations before being forced to disconnect. Replicator operation is not affected.

To set a datasource offline:

```
[LOGICAL:EXPERT] /alpha > datasource host3 offline
```

If the dataservice is in AUTOMATIC policy mode, and there are no other faults in the datasource, it will automatically be placed into ONLINE mode.

To set a datasource offline the dataservice must be in MAINTENANCE or MANUAL policy modes.

### 5.3.5.4. Mark a Datasource as Standby

`standby` datasources receive replication data, but are not part of the load-balancing provided by Tungsten Connector. In the event of a failover situation, a standby datasource will be enabled within the cluster as a slave. Because the standby datasource is up to date with respect to the replication of data, this process is instantaneous. The connector will be updated, and the new slave will operate as a read-only datasource.

To configure a datasource as a standby:

```
[LOGICAL:EXPERT] /alpha > datasource host3 standby
```

To clear the standby state:

```
[LOGICAL:EXPERT] /alpha > datasource host3 clear standby
```

**Note**

When a slave goes into standby mode, it will finish running any SQL queries that were started before it went into standby mode. New queries, even on the same connection, will not be directed to a slave that has just gone into standby

### 5.3.5.5. Mark a Datasource as Archive

An `archive` datasource receives replication data and is included as part of the load-balancing provided by Tungsten Connector. It is excluded from failover switches and will not be used as a master in the event of a failure. To mark a datasource as an archive datasource:

```
[LOGICAL:EXPERT] /alpha > datasource host3 set archive
```

To remove the archive role:

```
[LOGICAL:EXPERT] /alpha > datasource host3 clear archive
```

The archive role is a temporary requirement, and will not survive a re-install or upgrade.

### 5.3.6. Datasource Statuses

In addition to the overall state, all datasources have a specific status that indicates the current health and operation, rather than the configured state for that datasource. For example, a datasource can be in the online state, but have a DIMINISHED status if there is a recoverable problem with one of the datasource components.

- **OK**

  The OK status indicates that the datasource is currently operating correctly.
• **DIMINISHED**

A **DIMINISHED** status indicates that there is a problem with one of the dataservice services which is causing a reduced level of expected service. For example, in the sample output below, the reason is indicated as a stopped replicator service.

```
+----------------------------------------------------------------------------+
|host1(master:ONLINE)                                                        |
|STATUS [DIMINISHED] [2013/05/11 12:38:33 AM BST]                            |
|REASON[REPLICATOR STOPPED]                                                  |
+----------------------------------------------------------------------------+
```

The underlying service fault should be fixed and the status rechecked.

If all the services are **ONLINE**, but one node is in the **DIMINISHED** state, you should let the auto-recovery process complete. To do this:

1. Place the cluster into automatic mode:
   ```
   [LOGICAL] /alpha > set policy automatic
   ```

2. Set the status of the node in the **DIMINISHED** state to **OFFLINE**:
   ```
   [LOGICAL:EXPERT] /alpha > replicator host1 offline
   ```

Automatic recovery will then recover the node for you.

### 5.3.7. Datasource States and Policy Mode Interactions

States can be explicit set through `cctrl` command, however, depending on the current policy mode, the actual status set may be different from that initially set. For example, when shunning a datasource, the datasource will immediately go into **SHUNNED** state.

```
[LOGICAL:EXPERT] /alpha > datasource host3 shun
Datasource 'host3' set to SHUNNED
```

Figure 5.1. Sequence: Shunning a Datasource

```
cctrl> datasource host1 shun
```

```
Online
Shunned
```
To bring the datasource back into operation, it must be brought back using the recover command:

```
[LOGICAL:EXPERT] /alpha > datasource host3 recover
DataSource 'host3' is now OFFLINE
```

The `datasource recover` command performs whatever steps are necessary to bring the datasource back into operation within the dataservice. Even for manually shunned datasources, there may be additional configuration or recovery steps required.

If the dataservice policy mode is `MANUAL` or `MAINTENANCE` modes, the datasource remains in the OFFLINE state until manually put ONLINE.

### 5.4. Policy Modes

The dataservice operates using a policy mode, which configure how the dataservice management system responds to different events and operations within the dataservice. The policy mode can be set at will and enables maintenance and administration to be carried out without triggering the automatic failure and recovery procedures for operations that would otherwise trigger an automated response.

The procedure for how these operations are carried out are defined through a series of rules, with different policies applying different sets of the individual rules. The setting of the policy mode is dataservice-wide and instantaneous.

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Automatic</th>
<th>Manual</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fault Detection</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Failure Fencing</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Failure Recovery</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

The individual policy modes are described below:

- **AUTOMATIC Policy Mode**
  
  In automatic mode, the following operations and status changes happen automatically, managed by the coordinator:
  
  - Failed slave datasources are automatically marked as failed, temporarily removed from the dataservice, with application connections redirect to the other nodes in the dataservice. When the datasource becomes available, the node is automatically recovered to the dataservice.
  
  - Failed master datasources are automatically shunned and switched to the most up to date slave within the dataservice, which becomes the master and remaining slaves point to the newly promoted master.

  **Note**

  Automatic policy mode operates within a single dataservice only. Within a composite dataservice there is no automatic failover.

- **MANUAL Policy Mode**
  
  In the **MANUAL** policy mode, the dataservice identifies and isolates datasources when they fail, but automatic failover (for master datasources) and recovery is disabled.

- **MAINTENANCE Policy Mode**
  
  In **MAINTENANCE** policy mode all rules are disabled. Maintenance mode should be used when performing datasource or host maintenance that would otherwise trigger an automated fencing or recovery process.

  Maintenance mode should be used when administration or maintenance is required on the datasource, software, or operating system.

### 5.4.1. Setting Policy Modes

To set the policy, use the `set` command with the policy option. For example, to switch the current dataservice policy mode to manual:

```
[LOGICAL:EXPERT] /alpha > set policy manual
policy mode is now MANUAL
```

Policy mode changes are global, affecting the operation of all the members of the dataservice.

The current policy mode is shown when running `ls` within `cctrl`, see Section 5.3, “Checking Dataservice Status”.
5.5. Switching Master Hosts

The master host within a dataservice can be switched, either automatically, or manually. Automatic switching occurs when the dataservice is in the **AUTOMATIC** policy mode, and a failure in the underlying datasource has been identified. The automatic process is designed to keep the dataservice running without requiring manual intervention.

Manual switching of the master can be performed during maintenance operations, for example during an upgrade or dataserver modification. In this situation, the master must be manually taken out of service, but without affecting the rest of the dataservice. By switching the master to another datasource in the dataservice, the original master can be put offline, or shunned, while maintenance occurs. Once the maintenance has been completed, the datasource can be re-enabled, and either remain as the a slave, or switched back as the master datasource.

Switching a datasource, whether automatically or manually, occurs while the dataservice is running, and without affecting the operation of the dataservice as a whole. Client application connections through Tungsten Connector are automatically reassigned to the datasources in the dataservice, and application operation will be unaffected by the change. Switching the datasource manually requires a single command that performs all of the required steps, monitoring and managing the switch process.

Switching the master, manually or automatically, performs the following steps within the dataservice:

1. Set the master node to offline state. New connections to the master are rejected, and writes to the master are stopped.
2. On the slave that will be promoted, switch the datasource offline. New connections are rejected, stopping reads on this slave.
3. Kill any outstanding client connections to the master data source, except those belonging to the **tungsten** account.
4. Send a heartbeat transaction between the master and the slave, and wait until this transaction has been received. Once received, the THL on master and slave are up to date.
5. Perform the switch:
   - Configure all remaining replicators offline
   - Configure the selected slave as the new master.
   - Set the new master to the online state.
   - New connections to the master are permitted.
6. Configure the remaining slaves to use the new master as the master datasource.
7. Update the connector configurations and enable client connections to connect to the masters and slaves.

The switching process is monitored by Continuent Tungsten, and if the process fails, either due to a timeout or a recoverable error occurs, the switch operation is rolled back, returning the dataservice to the original configuration. This ensures that the dataservice remains operational. In some circumstances, when performing a manual switch, the command may need to be repeated to ensure the requested switch operation completes.

The process takes a finite amount of time to complete, and the exact timing and duration will depend on the state, health, and database activity on the dataservice. The actual time taken will depend on how up to date the slave being promoted is compared to the master. The switch will take place regardless of the current status after a delay period.

5.5.1. Automatic Master Failover

When the dataservice policy mode is **AUTOMATIC**, the dataservice will automatically failover the master host when the existing master is identified as having failed or become unavailable.

For example, when the master host host1 becomes unavailable because of a network problem, the dataservice automatically switches to host2. The dataservice status is updated accordingly, showing the automatically shunned host1:

```
[LOGICAL:EXPERT] /alpha > ls
COORDINATOR[host3:AUTOMATIC:ONLINE]

ROUTERS:
+----------------------------------------------------------------------------+
|connector@host2[28116](ONLINE, created=0, active=0)                         |
|connector@host3[1533](ONLINE, created=0, active=0)                          |
+----------------------------------------------------------------------------+

DATASOURCES:
+----------------------------------------------------------------------------+
|host1(master:SHUNNED(FAILED-OVER-TO-host2))                                 |
|STATUS [SHUNNED] [2013/05/14 12:18:54 PM BST]                               |
+----------------------------------------------------------------------------+
```
The status for the original master (host1) identifies the datasource as shunned, and indicates which datasource was promoted to the master in the FAILED-OVER-TO-host2.

A automatic failover can be triggered by using the datasource fail command:

```
[LOGICAL:EXPERT] /alpha > datasource host1 fail
```

This triggers the automatic failover sequence, and simulates what would happen if the specified host failed.

If host1 becomes available again, the datasource is not automatically added back to the dataservice, but must be explicitly re-added to the dataservice. The status of the dataservice once host1 returns is shown below:

```
[LOGICAL:EXPERT] /alpha > ls
COORDINATOR[host3:AUTOMATIC:ONLINE]
ROUTERS:
+----------------------------------------------------------------------------+
|connector@host1[19869](ONLINE, created=0, active=0)                         |
|connector@host2[28116](ONLINE, created=0, active=0)                         |
|connector@host3[1533](ONLINE, created=0, active=0)                          |
+----------------------------------------------------------------------------+
DATASOURCES:
+----------------------------------------------------------------------------+
|host1(master:SHUNNED(FAILED-OVER-TO-host2), progress=156323, THL latency=0.317) |
|STATUS [SHUNNED] [2013/05/14 12:38:21 PM BST]                                |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=master, state=ONLINE)                                     |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
```

Because host1 was previously the master, the datasource recover command verifies that the server is available, configures the node as a slave of the newly promoted master, and re-enables the services:

```
[LOGICAL:EXPERT] /alpha > datasource host1 recover
```

If the command is successful, then the node should be up and running as a slave of the new master.

The recovery process can fail if the THL data and dataserver contents do not match, for example when statements have been executed on a slave. For information on recovering from failures that recover cannot fix, see Section 5.6.1.3, “Slave Datasource Extended Recovery”.

### 5.5.2. Manual Master Switch

In a single data service dataservice configuration, the master can be switched between nodes within the dataservice manually using cctrl. The switch command performs the switch operation, annotating the progress.

```
[LOGICAL:EXPERT] /alpha > switch
SELECTED SLAVE: host2@alpha
PURGE REMAINING ACTIVE SESSIONS ON CURRENT MASTER 'host1@alpha'
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON MASTER 'host1@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host1@alpha'
PURGE THE NEW MASTER 'host2@alpha' ONLINE
PUT THE PRIOR MASTER 'host1@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host2@alpha' TO POINT TO NEW MASTER 'host2@alpha'
SWITCH TO 'host2@alpha' WAS SUCCESSFUL
```
By default, `switch` chooses the most up to date slave within the dataservice (`host2` in the above example), but an explicit slave can also be selected:

```
[LOGICAL:EXPERT] /alpha > switch to host3
SELECTED SLAVE: host3@alpha
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON CURRENT MASTER 'host2@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host2@alpha'
PUT THE PRIOR MASTER 'host2@alpha' ONLINE
PUT THE NEW MASTER 'host3@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host3@alpha' TO POINT TO NEW MASTER 'host3@alpha'
SWITCH TO 'host3@alpha' WAS SUCCESSFUL
```

With the previous example, the switch occurred specifically to the node `host3`.

### 5.6. Datasource Recovery Steps

When a datasource within the dataservice fails, the exact response by the dataservice is dependent on the dataservice policy mode. Different policy modes either cope with the failure or recovery process automatically, or a prescribed sequence must be followed.

Recovery can normally be achieved by following these basic steps:

- **Use the `recover` command**
  The `recover` command performs a number of steps to try and return the dataservice to the operational state, but works only if there is an existing master within the current configuration. Operations conducted automatically include slave recovery, and reconfiguring roles. For example:

```
[LOGICAL] /alpha > recover
FOUND PHYSICAL DATASOURCE TO RECOVER: 'host2@alpha'
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host2'
DATA SERVER 'host2' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host2@alpha' TO A SLAVE USING 'host3@alpha' AS THE MASTER
DataSource 'host2' is now OFFLINE
RECOVERY OF DATA SERVICE 'alpha' SUCCEEDED
FOUND PHYSICAL DATASOURCE TO RECOVER: 'host1@alpha'
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host1'
DATA SERVER 'host1' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host1@alpha' TO A SLAVE USING 'host3@alpha' AS THE MASTER
DataSource 'host1' is now OFFLINE
RECOVERY OF DATA SERVICE 'alpha' SUCCEEDED
RECOVERED 2 DATA SOURCES IN SERVICE 'alpha'
```

- **Slave failure, Master still available**
  Use the `recover` to bring all slaves back into operation. To bring a single slave, use the `datasource recover`:

```
[LOGICAL:EXPERT] /alpha > datasource host1 recover
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host1'
DATA SERVER 'host1' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host1@alpha' TO A SLAVE USING 'host2@alpha' AS THE MASTER
RECOVERY OF 'host1@alpha' WAS SUCCESSFUL
```

If recovery of the slave fails with this method, you can try more advanced solutions for getting your slave(s) working, including reprovisioning from another slave.

For more info, see Section 5.6.1, “Recover a failed slave”.

- **Master failure**
  If the most up to date master can be identified, use the `recover using` command to set the new master and recover the remaining slaves. If this does not work, use the `set master` command and then use the `recover` command to bring back as many possible slaves, and then use a backup/restore operation to bring any other slaves back into operation, or use the `tungsten_provision_slave` command. For more information, see Section 5.6.2, “Recover a failed master”.

A summary of these different scenarios and steps is provided in the following table:

<table>
<thead>
<tr>
<th>Policy Mode</th>
<th>Scenario</th>
<th>Datasource State</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOMATIC</td>
<td>Master Failure</td>
<td>master:SHUNNED[FAILED-OVER-TO-host2]</td>
<td>Automatic</td>
</tr>
<tr>
<td>AUTOMATIC</td>
<td>Master Recovery</td>
<td>master:SHUNNED[FAILED-OVER-TO-host2]</td>
<td>Section 5.6.2, “Recover a failed master”</td>
</tr>
<tr>
<td>AUTOMATIC</td>
<td>Slave Failure</td>
<td></td>
<td>Automatic</td>
</tr>
</tbody>
</table>
5.6.2.4, “Failing over a master”

5.6.2.2, “Recover a shunned master”

5.6.1, “Recover a failed slave”

5.6.2.3, “Manually Failing over a Master in MAINTENANCE policy mode”

5.6.1, “Recover when there are no masters”
In this case, the datasource can be manually shunned, which will then enable the `recover` command to operate and bring the node back into operation.

### 5.6.1.1. Provision or Reprovision a Slave

In the event that you cannot get the slave to recover using the `datasource recover` command, you can re-provision the slave from another slave within your dataservice.

The command performs three operations automatically:

1. Performs a backup of a remote slave
2. Copies the backup to the current host
3. Restores the backup

**Warning**

When using `tungsten_provision_slave` you must be logged in to the slave that has failed or that you want to reprovision. You cannot reprovision a slave remotely.

To use `tungsten_provision_slave`:

1. Log in to the failed slave.
2. Select the active slave within the dataservice that you want to use to reprovision the failed slave. You may use the master but this will impact performance on that host. If you use MyISAM tables the operation will create some locking in order to get a consistent snapshot.
3. Run `tungsten_provision_slave` specifying the source you have selected:

   ```shell
   shell> tungsten_provision_slave --source=host2
   NOTE >> Put alpha replication service offline
   NOTE >> Create a mysqldump backup of host2
   NOTE >> Put the alpha replication service offline
   NOTE >> Clear THL and relay logs for the alpha replication service
   ```

   The default backup service for the host will be used; `mysqldump` can be used by specifying the `--mysqldump` option.

   `tungsten_provision_slave` handles the cluster status, backup, restore, and repositioning of the replication stream so that restored slave is ready to start operating again.

**Important**

When using a Multisite/Multimaster topology the additional replicator must be put offline before restoring data and put online after completion.

```shell
shell> mm_trepctl offline
shell> tungsten_provision_slave --source=host2
shell> mm_trepctl online
shell> mm_trepctl status
```

For more information on using `tungsten_provision_slave` see Section 8.24, “The `tungsten_provision_slave` Script”.

### 5.6.1.2. Recover a slave from manually shunned state

A slave that has been manually shunned can be added back to the dataservice using the `datasource recover` command:

```shell
[LOGICAL:EXPERT] /alpha > datasource host3 recover
DataSource 'host3' is now OFFLINE
```

In **AUTOMATIC** policy mode, the slave will automatically be recovered from **OFFLINE** to **ONLINE** mode.

In **MANUAL** or **MAINTENANCE** policy mode, the datasource must be manually switched to the online state:

```shell
[LOGICAL:EXPERT] /alpha > datasource host3 online
Setting server for data source 'host3' to READ-ONLY
+----------------------------------------------------------------------------+
|host3                                                                       |
+----------------------------------------------------------------------------+
|Variable_name  Value                                                        |
|read_only  ON                                                               |
+----------------------------------------------------------------------------+
DataSource 'host3@alpha' is now ONLINE
```

136
5.6.1.3. Slave Datasource Extended Recovery

If the current slave will not recover, but the replicator state and sequence number are valid, the slave is pointing to the wrong master, or still mistakenly has the master role when it should be a slave, then the slave can be forced back into the slave state.

For example, in the output from `ls` in `cctrl` below, `host2` is mistakenly identified as the master, even though `host1` is correctly operating as the master.

```plaintext
COORDINATOR[host1:AUTOMATIC:ONLINE]

DATASOURCES:
+----------------------------------------------------------------------------+
| host1(master:ONLINE, progress=23, THL latency=0.198)                  |
| STATUS [OK] [2013/05/30 11:29:44 AM BST]                             |
| | MANAGER(state=ONLINE)                                               |
| | REPLICATOR(role=master, state=ONLINE)                               |
| | DATASERVER(state=ONLINE)                                            |
| | CONNECTIONS(created=0, active=0)                                    |
+----------------------------------------------------------------------------+

+----------------------------------------------------------------------------+
| host2(slave:SHUNNED(MANUALLY-SHUNNED), progress=-1, latency=-1.000)  |
| STATUS [SHUNNED] [2013/05/30 11:23:15 AM BST]                        |
| | MANAGER(state=ONLINE)                                               |
| | REPLICATOR(role=master, state=OFFLINE)                             |
| | DATASERVER(state=ONLINE)                                            |
| | CONNECTIONS(created=0, active=0)                                    |
+----------------------------------------------------------------------------+

+----------------------------------------------------------------------------+
| host3(slave:ONLINE, progress=23, latency=178877.000)                 |
| STATUS [OK] [2013/05/30 11:33:15 AM BST]                             |
| | MANAGER(state=ONLINE)                                               |
| | REPLICATOR(role=slave, master=host1, state=ONLINE)                 |
| | DATASERVER(state=ONLINE)                                            |
| | CONNECTIONS(created=0, active=0)                                    |
+----------------------------------------------------------------------------+
```

The datasource `host2` can be brought back online using this sequence:

1. Enable set `force` mode:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > set force true
   FORCE: true
   ```

2. Shun the datasource:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > datasource host2 shun
   DataSource 'host2' set to SHUNNED
   ```

3. Switch the replicator offline:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > replicator host2 offline
   Replicator 'host2' is now OFFLINE
   ```

4. Set the replicator to `slave` operation:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > replicator host2 slave
   Replicator 'host2' is now a slave of replicator 'host1'
   ```

   In some instances you may need to explicitly specify which node is your master when you configure the slave; appending the master hostname to the command specifies the master host to use:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > replicator host2 slave host1
   Replicator 'host2' is now a slave of replicator 'host1'
   ```

5. Switch the replicator service online:
   ```plaintext
   [LOGICAL:EXPERT] /alpha > replicator host2 online
   Replicator 'host2' is now ONLINE
   ```
6. Ensure the datasource is correctly configured as a slave:

```
[LOGICAL:EXPERT] /alpha > datasource host2 slave
Datasource 'host2' now has role 'slave'
```

7. Recover the slave back to the dataservice:

```
[LOGICAL:EXPERT] /alpha > datasource host2 recover
Datasource 'host2' is now offline
```

Datasource `host2` should now be back in the dataservice as a working datasource.

Similar processes can be used to force a datasource back into the master role if a switch or recover operation failed to set the role properly.

If the `recover` command fails, there are a number of solutions that may bring the dataservice back to the normal operational state. The exact method will depend on whether there are other active slaves (from which a backup can be taken) or recent backups of the slave are available, and the reasons for the original failure. Some potential solutions include:

- If there is a recent backup of the failed slave, restore the slave using that backup. The latest backup can be restored using Section 5.10, “Restoring a Backup”.  
- If there is no recent backup, but have another slave from which you can recover the slave, the node should be rebuilt using the backup from another slave. See Section 5.10.3, “Restoring from Another Slave”.

5.6.2. Recover a failed master

When a master datasource is automatically failed over in AUTOMATIC policy mode, the datasource can be brought back into the dataservice as a slave by using the recover command:

```
[LOGICAL:EXPERT] /alpha > datasource host1 recover
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host1'
DATA SERVER 'host1' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host1@alpha' TO A SLAVE USING 'host2@alpha' AS THE MASTER
SETTING THE ROLE OF DATASOURCE 'host1@alpha' FROM 'master' TO 'slave'
RECOVERY OF 'host1@alpha' WAS SUCCESSFUL
```

The recovered datasource will be added back to the dataservice as a slave.

5.6.2.1. Recover when there are no masters

When there are no masters available, due to a failover of a master, or multiple host failure there are two options available. The first is to use the `recover master using` command, which sets the master to the specified host, and tries to automatically recover all the remaining nodes in the dataservice. The second is to manually set the master host, and recover the remainder of the datasources manually.

- Using `recover master using`

  **Warning**

  This command should only be used in urgent scenarios where the most up to date master can be identified. If there are multiple failures or mismatches between masters and slaves, the command may not be able to recover all services, but will always result in an active master being configured.

  This command performs two distinct actions, first it calls `set master` to select the new master, and then it calls `datasource recover` on each of the remaining slaves. This attempts to recover the entire dataservice by switching the master and reconfiguring the slaves to work with the new master.

  To use, first you should examine the state of the dataservice and choose which datasource is the most up to date or canonical. For example, within the following output, each datasource has the same sequence number, so any datasource could potentially be used as the master:

```
[LOGICAL] /alpha > ls
COORDINATOR[host1:AUTO\(\em{MATIC:ONLINE}\)]
ROUTERS:
+----------------------------------------------------------------------------+
|connector@host1[18450](ONLINE, created=0, active=0)                         |
|connector@host2[8877](ONLINE, created=0, active=0)                          |
|connector@host3[8895](ONLINE, created=0, active=0)                          |
+----------------------------------------------------------------------------+
DATASOURCES:
+----------------------------------------------------------------------------+
|host1(master:SHUNNED(FAILSAFE AFTER Shunned by fail-safe procedure),        |
|progress=17, THL latency=8.565)                                             |
|STATUS [OK] [2013/11/04 04:39:28 PM GMT]                                     |
```
Once a host has been chosen, call the `recover master using` command specifying the full servicename and hostname of the chosen data-source:

```
[LOGICAL] /alpha > recover master using alpha/host1
```

This command is generally meant to help in the recovery of a data service that has data sources shunned due to a fail-safe shutdown of the service or under other circumstances where you wish to force a specific data source to become the primary. Be forewarned that if you do not exercise care when using this command you may lose data permanently or otherwise make your data service unusable.

Do you want to continue? (y/n) > y

DATA SERVICE 'alpha' DOES NOT HAVE AN ACTIVE PRIMARY. CAN PROCEED WITH 'RECOVER USING'

VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host1'
DATA SERVER 'host1' IS NOW AVAILABLE FOR CONNECTIONS
DataSource 'host1@alpha' IS NOW OFFLINE
FOUND PHYSICAL DATASOURCE TO RECOVER: 'host2@alpha'
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host2'
DATA SERVER 'host2' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host2@alpha' TO A SLAVE USING 'host1@alpha' AS THE MASTER
DataSource 'host2' is now OFFLINE
RECOVERY OF DATA SERVICE 'alpha' SUCCEEDED
FOUND PHYSICAL DATASOURCE TO RECOVER: 'host3@alpha'
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host3'
DATA SERVER 'host3' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host3@alpha' TO A SLAVE USING 'host1@alpha' AS THE MASTER
DataSource 'host3' is now OFFLINE
RECOVERY OF DATA SERVICE 'alpha' SUCCEEDED
RECOVERED 2 DATA SOURCES IN SERVICE 'alpha'

You will be prompted to ensure that you wish to choose the selected host as the new master. `cctrl` then proceeds to set the new master, and recover the remaining slaves.

If this operation fails, you can try the manual process, using `set master` and proceeding to recover each slave manually.

**Using `set master`**

The `set master` command forcibly sets the master to the specified host. It should only be used in the situation where no master is currently available within the dataservice, and recovery has failed. This command performs only one operation, and that is to explicitly set the new master to the specified host.

**Warning**

Using `set master` is an expert level command and may lead to data loss if the wrong master is used. Because of this, the `cctrl` must be forced to execute the command by using `set force true`. The command will not be executed otherwise.

To use the command, pick the most up to date master, or the host that you want to use as the master within your dataservice, then issue the command:

```
[LOGICAL] /alpha > set master host3
```
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host3'
DATA SERVER 'host3' IS NOW AVAILABLE FOR CONNECTIONS
DataSource 'host3' is now OFFLINE
DATASOURCE 'host3@alpha' IS NOW A MASTER

This does not recover the remaining slaves within the cluster, these must be manually recovered. This can be achieved either by using Section 5.6.1, “Recover a failed slave”, or if this is not possible, using Section 5.6.11, “Provision or Reprovision a Slave”.

5.6.2.2. Recover a shunned master

When a master datasource fails in MANUAL policy mode, and the node has been failed over, once the datasource becomes available, the node can be added back to the datasync by using the recover command, which enables the host as a slave:

```
[LOGICAL:EXPERT] /alpha > datasource host1 recover
VERIFYING THAT WE CAN CONNECT TO DATA SERVER 'host1'
DATA SERVER 'host1' IS NOW AVAILABLE FOR CONNECTIONS
RECOVERING 'host1@alpha' TO A SLAVE USING 'host2@alpha' AS THE MASTER
SETTING THE ROLE OF DATASOURCE 'host1@alpha' FROM 'master' TO 'slave'
RECOVERY OF 'host1@alpha' WAS SUCCESSFUL
```

The recovered master will be added back to the datasync as a slave.

5.6.2.3. Manually Failing over a Master in MAINTENANCE policy mode

If the datasync is in MAINTENANCE mode when the master fails, automatic recovery cannot sensibly make the decision about which node should be used as the master. In that case, the datasource service must be manually reconfigured.

In the sample below, host1 is the current master, and host2 is a slave. To manually update and switch host1 to be the slave and host2 to be the master:

1. Shun the failed master (host1) and set the replicator offline:

```
[LOGICAL:EXPERT] /alpha > datasource host1 shun
DataSource 'host1' set to SHUNNED
[LOGICAL:EXPERT] /alpha > replicator host1 offline
Replicator 'host1' is now OFFLINE
```

2. Shun the slave host2 and set the replicator to the offline state:

```
[LOGICAL:EXPERT] /alpha > datasource host2 shun
DataSource 'host2' set to SHUNNED
[LOGICAL:EXPERT] /alpha > replicator host2 offline
Replicator 'host2' is now OFFLINE
```

3. Configure host2 as the master within the replicator service:

```
[LOGICAL:EXPERT] /alpha > replicator host2 master
```

4. Set the replicator on host2 online:

```
[LOGICAL:EXPERT] /alpha > replicator host2 online
```

5. Recover host2 online and then set it online:

```
[LOGICAL:EXPERT] /alpha > datasource host2 welcome
[LOGICAL:EXPERT] /alpha > datasource host2 online
```

6. Switch the replicator to be in slave mode:

```
[LOGICAL:EXPERT] /alpha > replicator host1 slave host2
Replicator 'host1' is now a slave of replicator 'host2'
```

7. Switch the replicator online:

```
[LOGICAL:EXPERT] /alpha > replicator host1 online
Replicator 'host1' is now ONLINE
```

8. Switch the datasource role for host1 to be in slave mode:

```
[LOGICAL:EXPERT] /alpha > datasource host1 slave
Datasource 'host1' now has role 'slave'
```

9. The configuration and roles for the host have been updated, the datasource can be added back to the datasync and then put online:

```
[LOGICAL:EXPERT] /alpha > datasource host1 recover
```

140
**DataSource 'host1' is now OFFLINE**

```plaintext
[LOGICAL:EXPERT] /alpha > datasource host1 online
Setting server for data source 'host1' to READ-ONLY
```

<table>
<thead>
<tr>
<th>Variable_name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>read_only</td>
<td>ON</td>
</tr>
</tbody>
</table>

**DataSource 'host1@alpha' is now ONLINE**

10. With the dataservice in automatic policy mode, the datasource will be placed online, which can be verified with `ls`:

```plaintext
[LOGICAL:EXPERT] /alpha > ls
```

**5.6.2.4. Failing over a master**

When a master datasource fails in **MANUAL** policy mode, the datasource must be manually failed over to an active datasource, either by selecting the most up to date slave automatically:

```plaintext
[LOGICAL:EXPERT] /alpha > failover
```

Or to an explicit host:

```plaintext
[LOGICAL:EXPERT] /alpha > failover to host2
```

For the `failover` command to work, the following conditions must be met:

- There must be a master or relay in the **SHUNNED** or **FAILED** state.
- There must be at least one slave in the **ONLINE** state.

If there is not already a **SHUNNED** or **FAILED** master and a failover must be forced, use `datasource shun` on the master, or failover to a specific slave.
5.7. Composite Cluster Switching, Failover and Recovery

Switching of a datasource is done to transfer the Master role from one cluster to another, usually in another datacenter site. This also has the effect of turning the original Master into a Relay. The master datasource within a composite cluster can be forced to failover to the slave datasource in the event the master datasource is offline.

Switching the master datasource performs the following steps:

1. Set the master node to offline state. New connections to the master are rejected, and writes to the master are stopped.
2. On the relay in the target cluster, switch the datasource offline. New connections are rejected, stopping reads on this master.
3. Kill any outstanding client connections to the master data source, except those belonging to the tungsten account.
4. Send a heartbeat transaction between the old master and the new master, and wait until this transaction has been received. Once received, the THL on master and slave are up to date.
5. Perform the switch:
   - Configure all remaining replicators offline
   - Configure the target cluster relay node as the new master.
   - Set the new master to the online state.
   - New connections to the master are permitted.
6. Configure the old master to be a relay datasource.
7. Configure the slaves in the primary site to use the new master datasource.
8. Configure the slaves in the slave site to use the new relay datasource.
9. Update the connector configurations and enable client connections to connect to the masters and slaves.

The switching process is monitored by Continuent Tungsten, and if the process fails, either due to a timeout or a recoverable error occurs, the switch operation is rolled back, returning the datasource to the original configuration. This ensures that the datasource remains operational. In some circumstances, when performing a manual switch, the command may need to be repeated to ensure the requested switch operation completes.

The process takes a finite amount of time to complete, and the exact timing and duration will depend on the state, health, and database activity on the datasource. The actual time taken will depend on how up to date the slave being promoted is compared to the master. The switch will take place regardless of the current status after a delay period.

5.7.1. Composite Cluster Site Switch

Our example cluster has two sites, east and west. They are both members of composite cluster global. Site east has hosts db1, db2 and db3. Site west has hosts db4, db5 and db6.

Important

When working with composite clusters, you should use the -multi [222] option to cctrl. With this option enabled the prompt and information provided will be different. You can perform operations both on individual parts of the cluster, and on the entire composite cluster. This can be achieved by using the use COMPOSITESERVICE command. Tab completion is also available within cctrl when using this mode.
Composite Master Dataservice (Primary) - east

```plaintext
[LOGICAL] /global > use east
[LOGICAL] /east > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]

ROUTERS:
+----------------------------------------------------------------------------+
|connector@db1[9745](ONLINE, created=1, active=0)              |
|connector@db2[9911](ONLINE, created=1, active=0)              |
|connector@db3[9775](ONLINE, created=1, active=0)              |
|connector@db4[9757](ONLINE, created=1, active=0)              |
|connector@db5[9781](ONLINE, created=1, active=0)              |
|connector@db6[9944](ONLINE, created=1, active=0)              |
+----------------------------------------------------------------------------+

DATASOURCES:
+----------------------------------------------------------------------------+
|db1(master:ONLINE, progress=6, THL latency=0.814)                           |
|STATUS [OK] [2015/04/14 01:46:54 AM UTC]                                    |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=master, state=ONLINE)                                     |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=6, active=0)                                          |
+----------------------------------------------------------------------------+

|db2(slave:ONLINE, progress=6, latency=0.857)                                |
|STATUS [OK] [2015/04/14 01:46:59 AM UTC]                                    |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=slave, master=db1, state=ONLINE)                          |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+

|db3(slave:ONLINE, progress=6, latency=0.887)                                |
|STATUS [OK] [2015/04/14 01:46:59 AM UTC]                                    |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=slave, master=db1, state=ONLINE)                          |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
```

Composite Slave Dataservice [DR] - west

```plaintext
[LOGICAL] /east > use west
[LOGICAL] /west > ls
COORDINATOR[db4:AUTOMATIC:ONLINE]

ROUTERS:
+----------------------------------------------------------------------------+
|connector@db1[9745](ONLINE, created=8, active=0)              |
|connector@db2[9911](ONLINE, created=8, active=0)              |
|connector@db3[9775](ONLINE, created=8, active=0)              |
|connector@db4[9757](ONLINE, created=8, active=0)              |
|connector@db5[9781](ONLINE, created=8, active=0)              |
|connector@db6[9944](ONLINE, created=8, active=0)              |
+----------------------------------------------------------------------------+

DATASOURCES:
+----------------------------------------------------------------------------+
|db4(relay:ONLINE, progress=6, latency=5.050)                                |
|STATUS [OK] [2015/04/14 01:46:59 AM UTC]                                    |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=relay, master=db1, state=ONLINE)                          |
|  DATASERVER(state=ONLINE)                                                  |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
```
Manually switch the composite master role to the other site:

```
[LOGICAL] / > use global
[LOGICAL] /global > switch
SELECTED SLAVE: 'west@global'
FLUSHING TRANSACTIONS THROUGH 'db1@east'
REPLICATOR 'db1' IS NOW USING MASTER CONNECT URI 'thl://db4:2112/'
composite data source 'west@global' is now OFFLINE
PUT THE NEW MASTER 'west@global' ONLINE
PUT THE PRIOR MASTER 'east@global' ONLINE AS A SLAVE
REVERT POLICY: MAINTENANCE => AUTOMATIC
SWITCH TO 'west@global' WAS SUCCESSFUL
```

```
[LOGICAL] /global > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]
DATASOURCES:
```
```
[LOGICAL] /global = use east
[LOGICAL] /east > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]
```

Composite Slave Dataservice [DR] - east

```
[LOGICAL] /global = use east
[LOGICAL] /east > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]
```

```
ROUTERS:
```
```
DATASOURCES:
```
```
[LOGICAL] /east > ls
COORDINATOR[db1:AUTOMATIC:ONLINE]
```

```
ROUTERS:
```
```
DATASOURCES:
```
5.7.2. Composite Cluster Site Failover [Forced Switch]

In the event the Primary site goes down, and a graceful manual switch is not possible, the composite master role can be failed over to the Disaster Recovery cluster using `cctrl`. The `failover` command performs the forced switch operation. It will try to update the configuration of the east data service but will not fail if not successful.

In this example, hosts db1 [the composite master], db2 and db3 in cluster east have been shut down. To force dataservice `west` to become the primary, login to a node in that cluster and get into `cctrl`:

```
shell> cctrl -multi
Continuent Tungsten 2.0.5 build 11
west: session established
[LOGICAL] / > use global
[LOGICAL] /global >
COORDINATOR[db4:AUTOMATIC:ONLINE]
DATASOURCES:
```

```
| db4(slave:ONLINE, progress=3, THL latency=0.671) |
| STATUS [OK] [2015/04/14 01:45:42 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=master, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |
```

```
| db5(slave:ONLINE, progress=3, latency=1.581) |
| STATUS [OK] [2015/04/14 01:45:48 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=slave, master=db4, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |
```

```
| db6(slave:ONLINE, progress=3, latency=1.559) |
| STATUS [OK] [2015/04/14 01:45:47 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=slave, master=db4, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |
```

```
DATASOURCES:    
```
Mark the east data service as failed to prevent further actions:

```
[LOGICAL] /global > datasource east fail
WARNING: This is an expert-level command:
Incorrect use may cause data corruption
or make the cluster unavailable.
Do you want to continue? (y/A)> y
WARNING: UNABLE TO REACH PHYSICAL DATA SERVICE 'east' AT THIS TIME.
EXCEPTION: Unable to unable to continue with command because no manager is available in service 'east'.
CONTINUING WITH COMMAND
COMPOSITE DATA SOURCE 'east' IS NOW IN THE FAILED STATE
```

Issue the failover command to force the west dataservice to become the composite master:

```
[LOGICAL] /global > failover
WARNING: DATA SERVICE 'east' IS NOT AVAILABLE. CANNOT GET STATE
WARNING: CAN'T SET POLICY MODE 'maintenance' FOR SERVICE 'east'. CONTINUING.
SELECTED SLAVE: 'west@global'
WARNING: UNABLE TO REACH PHYSICAL DATA SERVICE 'east' AT THIS TIME.
EXCEPTION: Unable to unable to continue with command because no manager is available in service 'east'.
CONTINUING WITH COMMAND
ENSURING THAT WE CATCH UP WITH THE MOST ADVANCED RELAY
composite data source 'west@global' is now OFFLINE
WARNING: UNABLE TO REACH PHYSICAL DATA SERVICE 'west' AT THIS TIME.
EXCEPTION: Unable to unable to continue with command because no manager is available in service 'east'.
CONTINUING WITH COMMAND
PUT THE NEW MASTER 'west@global' ONLINE
REVERT POLICY: MAINTENANCE => AUTOMATIC
FAILOVER TO 'west@global' WAS SUCCESSFUL
```

Composite Master Dataservice [Primary] - west

```
[LOGICAL] /global > use west
[LOGICAL] /west > ls
COORDINATOR[db4:AUTOMATIC:ONLINE]
```
5.7.3. Composite Cluster Site Recovery

The first step in recovering the SHUNNED datasync is to re-provision the nodes if the data has gotten out of sync. See Section 5.6.1.1, "Provision or Reprovision a Slave" for more information.

Once the failed site has been restored, the shunned/superseded datasync can be brought back online using `cctrl`. The `recover` command performs this operation, annotating the progress.

```
shelles> cctrl -nul
Continuent Tungsten 2.0.5 build 11
west: session established
[LOGICAL] / > use global
[LOGICAL] /global > Is
COORDINATOR[db4:AUTOMATIC:ONLINE]

DATASOURCES:
|db4(master:ONLINE, progress=7, THL latency=0.110) |
|STATUS [OK] [2015/04/14 02:13:23 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=master, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |

|db5(slave:ONLINE, progress=7, latency=0.172) |
|STATUS [OK] [2015/04/14 02:13:23 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=slave, master=db4, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |

|db6(slave:ONLINE, progress=7, latency=0.173) |
|STATUS [OK] [2015/04/14 02:13:23 AM UTC] |
| MANAGER(state=ONLINE) |
| REPLICATOR(role=slave, master=db4, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |

SHUNNED(SUPERSEDED) Composite Master Dataservice - east

[LOGICAL] / > use east
[LOGICAL] /east > Is
COORDINATOR[db2:AUTOMATIC:ONLINE]

ROUTERS:
|connector@db1[10051](ONLINE, created=0, active=0) |
|connector@db2[16111](ONLINE, created=0, active=0) |
|connector@db3[16036](ONLINE, created=0, active=0) |
|connector@db4[9757](ONLINE, created=1, active=0) |
|connector@db5[9781](ONLINE, created=1, active=0) |
|connector@db6[9944](ONLINE, created=1, active=0) |
```
Use the `recover` command to bring the SHUNNED dataservice back online as a composite slave:

```
[LOGICAL] /global > recover
IDENTIFIED DATASOURCE 'east@global' FOR RECOVERY
COULD NOT IDENTIFY ACTIVE PRIMARY FOR SERVICE 'east'
ATTEMPTING TO IDENTIFY A FAILED PRIMARY FOR 'east'
PHYSICAL DATA SERVICE 'east' DOES NOT HAVE AN ACTIVE RELAY
FORCING THE PHYSICAL RELAY TO BE 'db1'
DATASERVICE 'db1:east' IS NOW A RELAY
RECOVERED 2 DATA SOURCES IN SERVICE 'east'
RECOVERED DATASERVICE 'east@global' ROLE IS NOW SLAVE
COMPOSITE DATA SOURCE 'east@global' IS NOW OFFLINE
REVERT SET POLICY AUTOMATIC
RECOVERY OF COMPOSITE SERVICE 'global' IS COMPLETE
```

Recovered Composite Slave Dataservice (DR) - east

```
[LOGICAL] /global > use east
[LOGICAL] /east > ls
```

DATASOURCES:
```
db1(relay:ONLINE, progress=7, latency=0.000)
| STATUS [OK] [2015/04/14 04:11:52 AM UTC]
+----------------------------------------------------------------------------+
| MANAGER(state=ONLINE) |
| REPLICATOR(role=relay, master=db1, state=ONLINE) |
| DATASERVER(state=ONLINE) |
| CONNECTIONS(created=0, active=0) |
+----------------------------------------------------------------------------+
```

**Operations Guide**
5.7.4. Composite Cluster Relay Recovery

If the Relay node in a Composite cluster should ever point to the incorrect Master node, you can perform the following procedure to re-point the replicator to the desired Master node.

For example, say we have a composite cluster **global**, with nodes db1, db2 and db3 in **east** and db4, db5 and db6 in **west**. db1 is the Master and db4 is the Relay.

In the output below, the Relay node db4 shows that its replicator is using db2 as the Master instead of db1:

```
+----------------------------------------------------------------------------+
|db4(relay:ONLINE, progress=2034642966, latency=2.456) |                  |
|STATUS [OK] [2017/03/20 05:57:49 AM GMT+00:00] |                  |
+----------------------------------------------------------------------------+

| MANAGER(state=ONLINE) |                  |
| REPLICATOR(role=relay, master=db2, state=ONLINE) |                  |
| DATASERVER(state=ONLINE) |                  |
| CONNECTIONS(created=8108, active=0) |                  |
+----------------------------------------------------------------------------+
```

Use the `cctrl replicator` command to adjust the relay source:

```
shell> cctrl -multi
Continuent Tungsten 2.0.5 build 11
west: session established
[LOGICAL] / > use west
[LOGICAL] /west > set policy maintenance
[LOGICAL] /west > replicator db4 offline
[LOGICAL] /west > replicator db4 relay east/db1
[LOGICAL] /west > set policy automatic
[LOGICAL] /west > is
+----------------------------------------------------------------------------+
|db4(relay:ONLINE, progress=2834642966, latency=2.456) |                  |
|STATUS [OK] [2017/03/20 05:57:49 AM GMT+00:00] |                  |
+----------------------------------------------------------------------------+

| MANAGER(state=ONLINE) |                  |
| REPLICATOR(role=relay, master=db1, state=ONLINE) |                  |
| DATASERVER(state=ONLINE) |                  |
| CONNECTIONS(created=8108, active=0) |                  |
+----------------------------------------------------------------------------+
```

5.8. Managing Transaction Failures

Inconsistencies between a master and slave dataserver can occur for a number of reasons, including:

- An update or insertion has occurred on the slave independently of the master. This situation can occur if updates are allowed on a slave that is acting as a read-only slave for scale out, or in the event of running management or administration scripts on the slave
- A switch or failover operation has lead to inconsistencies. This can happen if client applications are still writing to the slave or master at the point of the switch.
- A database failure causes a database or table to become corrupted.
When a failure to apply transactions occurs, the problem must be resolved, either by skipping or ignoring the transaction, or fixing and updating the underlying database so that the transaction can be applied.

When a failure occurs, replication is stopped immediately at the first transaction that caused the problem, but it may not be the only transaction and this may require extensive examination of the pending transactions to determine what caused the original database failure and then to fix and address the error and restart replication.

### 5.8.1. Identifying a Transaction Mismatch

When a mismatch occurs, the replicator service will indicate that there was a problem applying a transaction on the slave. The replication process stops applying changes to the slave when the first transaction fails to be applied to the slave. This prevents multiple-statements from failing.

Within `cctrl` the status of the datasource will be marked as `DIMINISHED [130]`, and the replicator state as `SUSPECT`.

```plaintext
[LOGICAL] /alpha > ls

[COORDINATOR] [host3: AUTOMATIC: ONLINE]
...

[REPLICATOR] [host2: SLAVE: ONLINE, progress: 1, latency: 1.800]
[REASON] [FAILED TO RECOVER REPLICATOR 'host2']

[MANAGER] [state: ONLINE]
[REPLICATOR] [role: slave, master=host1, state=SUSPECT]
[DATASERVER] [state: ONLINE]
[CONNECTIONS] [created=0, active=0]
...
```

More detailed information about the status and the statement that failed can be obtained within `cctrl` using the `replicator` command:

```plaintext
[LOGICAL] /alpha > replicator host2 status

[REPLICATOR] host2 status

appliedLastEventId: NONE
appliedLastSeqno: 1
appliedAtency: 1.0
channels: 1
clusterName: firstcluster
currentEventId: NONE
currentTimeMillis: 1372238640023

dataServerHost: host2
extensions: 
latestEpochNumber: 1
masterConnection: thl://host1/
masterListener: thl://host1:2112/
maxUnstartedSeqno: 1
minUnstartedSeqno: 1
offlineRequests: NONE
pendingError: Event application failed: seqno=120, frame=0
message=java.sql.SQLException: Statement failed on slave but succeeded on master
pendingErrorCode: NONE
pendingErrorEventId: mysql-bin.000012:0000000000012967:0
pendingErrorSeqno: 120
pendingExceptionMessage= java.sql.SQLException: Statement failed on slave but succeeded on master
Insert into messages values (("Trial message", 'Jack', 'Jill', now())
pipeLineSource: UNKNOWN
relativeLatency: 1.0
resourcePrecedence: 99
rmiPort: 10000
role: slave
sequenceType: java.lang.Long
serviceName: firstcluster
serviceType: unknown
simpleServiceName: firstcluster
siteName: default
source: host2
state: OFFLINE:ERROR
timeInStateSeconds: 587.806
transmissionTo: 
uptimeSeconds: 61371.957
version: Continenent Tungsten 2.8.5 build 11
```

The `trepsvc.log` log file will also contain the error information about the failed statement. For example:
Once the error or problem has been found, the exact nature of the error should be determined so that a resolution can be identified:

1. **Identify the reason for the failure by examining the full error message.** Common causes are:

   - **Duplicate primary key**

   A row or statement is being inserted or updated that already has the same insert ID or would generate the same insert ID for tables that have auto increment enabled. The insert ID can be identified from the output of the transaction using `thl`. Check the slave to identify the faulty row. To correct this problem you will either need to skip the transaction or delete the offending row from the slave dataserver.

   The error will normally be identified due to the following error message when viewing the current replicator status, for example:

   ```
   [LOGICAL] /alpha >replicator host3 status
   ...
   pendingError           : Event application failed: seqno=10 fragno=0 »
   message=java.sql.SQLException: Statement failed on slave but succeeded on master
   pendingErrorCode       : NONE
   pendingErrorEventId    : mysql-bin.000032:0000000000001872;0
   pendingErrorSeqno      : 10
   pendingExceptionMessage: java.sql.SQLException: Statement failed on slave but succeeded on master
   insert into myent values (0,'Test Message')
   ...
   ```

   The error can be generated when an insert or update has taken place on the slave rather than on the master.

   To resolve this issue, check the full THL for the statement that failed. The information is provided in the error message, but full examination of the THL can help with identification of the full issue. For example, to view the THL for the sequence number:

   ```
   shell> thl list -seqno 10
   SQL = 18 / FRAG# = 0 (Last Frag)
   TIME = 2014-01-09 16:47:40.0
   EPOCH = 1
   EVENTID = mysql-bin.000032:0000000000001872;0
   SOURCEID = host1
   METADATA = [mysql_server_id=1;dbms_type=mysql;service=firstcluster;shard=test]
   TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
   SQL(0) = SET INSERT_ID = 2
   OPTIONS = [##charset = UTF-8, autocommit = 1, sql_auto_is_null = 0, foreign_key_checks = 1, 
              unique_checks = 1, sql_mode = '1', character_set_client = 33, collation_connection = 33, 
              collation_server = 8]
   SCHEMA = test
   SQL(1) = insert into myent values (0,'Test Message')
   ```

   In this example, an `INSERT` operation is inserting a new row. The generated insert ID is also shown (in line 9, `SQL(0)`). Check the destination database and determine the what the current value of the corresponding row:

   ```
   mysql> select * from myent where id = 2;
   +----+---------------+
   | id | msg           |
   +----+---------------+
   |  2 | Other Message |
   +----+---------------+
   1 row in set (0.00 sec)
   ```

   The actual row values are different, which means that either value may be correct. In complex data structures, there may be multiple statements or rows that trigger this error if following data also relies on this value.

   For example, if multiple rows have been inserted on the slave, multiple transactions may be affected. In this scenario, checking multiple sequence numbers from the THL will highlight this information.
• Missing table or schema

If a table or database is missing, this should be reported in the detailed error message. For example:

```
Caused by: java.sql.SQLSyntaxErrorException: Unable to switch to database »
  'contacts' Error was: Unknown database 'contacts'
```

This error can be caused when maintenance has occurred, a table has failed to be initialized properly, or the

• Incompatible table or schema

A modified table structure on the slave can cause application of the transaction to fail if there are missing or different column specifications for the table data.

This particular error can be generated when changes to the table definition have been made, perhaps during a maintenance window. Check the table definition on the master and slave and ensure they match.

2. Choose a resolution method:

Depending on the data structure and environment, resolution can take one of the following forms:

• Skip the transaction on the slave

If the data on the slave is considered correct, or the data in both tables is the same or similar, the transaction from the master to the slave can be skipped. This process involves placing the replicator online and specifying one or more transactions to be skipped or ignored. At the end of this process, the replicator should be in the `ONLINE` state.

For more information on skipping single or multiple transactions, see Section 5.8.2, "Skipping Transactions".

• Delete the offending row or rows on the slave

If the data on the master is considered canonical, then the data on the slave can be removed, and the replicator placed online.

```
Warning
Deleting data on the slave may cause additional problems if the data is used by other areas of your application, relations to foreign tables.
```

For example:

```
mysql> delete from myent where id = 2;
Query OK, 1 row affected (0.01 sec)
```

Now place the replicator online and check the status:

```
[LOGICAL] /alpha > replicator host3 online
```

• Restore or reprovision the slave

If the transaction cannot be skipped, or the data safely deleted or modified, and only a single slave is affected, a backup of an existing, working slave can be taken and restored to the broken slave.

To perform a backup and restore, see Section 5.9, "Creating a Backup", or Section 5.10, "Restoring a Backup". To reprovision a slave from the master or another slave, see `tungsten_provision_slave`.

5.8.2. Skipping Transactions

When a failure caused by a mismatch or failure to apply one or more transactions, the transaction(s) can be skipped. Transactions can either be skipped one at a time, through a specific range, or a list of single and range specifications.

```
Warning
Skipping over events can easily lead to slave inconsistencies and later replication errors. Care should be taken to ensure that the transaction(s) can be safely skipped without causing problems. See Section 5.8.1, "Identifying a Transaction Mismatch".
```

• Skipping a Single Transaction

If the error was caused by only a single statement or transaction, the transaction can be skipped using `trepctl online`:

```
shell> trepctl online -skip-seqno 10
```
The individual transaction will be skipped, and the next transaction (11), will be applied to the destination database.

- Skipping a Transaction Range

If there is a range of statements that need to be skipped, specify a range by defining the lower and upper limits:

```bash
trepctl online -skip-seqno 10-20
```

This skips all of the transactions within the specified range, and then applies the next transaction (21) to the destination database.

- Skipping Multiple Transactions

If there are transactions mixed in with others that need to be skipped, the specification can include single transactions and ranges by separating each element with a comma:

```bash
trepctl online -skip-seqno 10,12-14,16,19-20
```

In this example, only the transactions 11, 15, 17 and 18 would be applied to the target database. Replication would then continue from transaction 21.

Regardless of the method used to skip single or multiple transactions, the status of the replicator should be checked to ensure that replication is online.

5.9. Creating a Backup

The `datasource backup` command for a datasource within `cctrl` backs up a datasource using the default backup tool. During installation, `xtrabackup-full` will be used if `xtrabackup` has been installed. Otherwise, the default backup tool used is `mysqldump`.

**Important**

For consistency, all backups should include a copy of all `tungsten_SERVICE` schemas. This ensures that when the Tungsten Replicator service is restarted, the correct start points for restarting replication are recorded with the corresponding backup data. Failure to include the `tungsten_SERVICE` schemas may prevent replication from being restart effectively.

Backing up a datasource can occur while the replicator is online:

```
[LOGICAL:EXPERT] /alpha > datasource host3 backup
Using the 'mysqldump' backup agent.
Replicator 'host3' starting backup
Backup of datasource 'host3' succeeded; uri=storage://file-system/store-0000000001.properties
```

By default, the backup is created on the local filesystem of the host that is backed up in the `backups` directory of the installation directory. For example, using the standard installation, the directory would be `/opt/continuent/backups`. An example of the directory content is shown below:

```
total 130788
drwxrwxr-x 2 tungsten tungsten 4096 Apr  4 16:09 .
drwxrwxr-x 3 tungsten tungsten 4096 Apr  4 11:53 ..
-rw-r--r-- 1 tungsten tungsten 4896 Apr  4 16:09 .
drwxr-xr-x 1 tungsten tungsten 4896 Apr  4 11:53 ..
-rw-r--r-- 1 tungsten tungsten 71 Apr  4 16:09 storage.index
-rw-r--r-- 1 tungsten tungsten 133907646 Apr  4 16:09 store-0000000001-mysqldump_2013-04-04_16-08_42.sql.gz
-rw-r--r-- 1 tungsten tungsten 317 Apr  4 16:09 store-0000000001.properties
```

For information on managing backup files within your environment, see Section E.1.1, “The backups Directory”.

The `storage.index` contains the backup file index information. The actual backup data is stored in the GZipped file. The properties of the backup file, including the tool used to create the backup, and the checksum information, are located in the corresponding `properties` file. Note that each backup and property file is uniquely numbered so that it can be identified when restoring a specific backup.

A backup can also be initiated and run in the background by adding the & (ampersand) to the command:

```
[LOGICAL:EXPERT] /alpha > datasource host3 backup &
[1] datasource host3 backup - RUNNING
```

**YOU MUST BE USING A DATA SERVICE TO EXECUTE THIS COMMAND EXECUTE 'use <data service name> ' TO SET YOUR CONTEXT.**

```
[1] datasource host3 backup - SUCCESS
```

5.9.1. Using a Different Backup Tool

If `xtrabackup` is installed when the dataservice is first created, `xtrabackup` will be used as the default backup method. Four built-in backup methods are provided:

- `mysqldump` — SQL dump to a single file. This is the easiest backup method but it is not appropriate for large data sets.
• `xtrabackup` — Full backup. This will take longer to take the backup and to restore.
• `xtrabackup-full` — Full backup to a directory [this is the default if `xtrabackup` is available and the backup method is not explicitly stated].
• `xtrabackup-incremental` — Incremental backup from the last `xtrabackup-full` or `xtrabackup-incremental` backup.

The default backup tool can be changed, and different tools can be used explicitly when the backup command is executed. The Percona `xtrabackup` tool can be used to perform both full and incremental backups. Use of this tool is optional and can be configured during installation, or afterwards by updating the configuration using `tpm`.

To update the configuration to use `xtrabackup`, install the tool and then follow the directions for `tpm update` to apply the `--repl-backup-method=xtrabackup-full [546]` setting.

To use `xtrabackup-full` without changing the configuration, specify the backup agent to the `datasource backup` command within `cctrl`:

```
[LOGICAL:EXPERT] /alpha >
  datasource host2 backup xtrabackup-full
Replicator 'host2' starting backup
Backup of dataSource 'host2' succeeded; uri=storage://file-system/store-0000000006.properties
```

### 5.9.2. Automating Backups

Backups cannot be automated within Continuent Tungsten, instead a `cron` job should be used to automate the backup process. `cluster_backup` is packaged with Continuent Tungsten to provide a convenient interface with `cron`. The `cron` entry should be added to every datasource or active witness in the cluster. The command includes logic to ensure that it will only take one backup per cluster by only running on the current coordinator. See Section 8.6, “The `cluster_backup` Command” for more information.

```
shell> /opt/continuent/tungsten/cluster-home/bin/cluster_backup -v >> /opt/continuent/service_logs/cluster_backup.log
```

The command output will be appended to `/opt/continuent/service_logs/cluster_backup.log` for later review. Use your preferred mechanism to configure `cron` to execute this command on the desired schedule.

An example `cron` entry:

```
shell> crontab -l
00 00 * * * /opt/continuent/tungsten/cluster-home/bin/cluster_backup >> /opt/continuent/service_logs/cluster_backup.log 2>&1
```

All output will be appended to `/opt/continuent/service_logs/cluster_backup.log`.

Alternatively, you can call the backup command directly through `cctrl`. This method does not ensure the named datasource is `ONLINE` or even available to be backed up.

```
shell> echo "datasource host2 backup" | /opt/continuent/tungsten/tungsten-manager/bin/cctrl -expert
```

### 5.9.3. Using a Different Directory Location

The default backup location the `backups` directory of the Continuent Tungsten installation directory. For example, using the recommended installation location, backups are stored in `/opt/continuent/backups`.

See Section E.1.1.4, “Relocating Backup Storage” for details on changing the location where backups are stored.

### 5.9.4. Creating an External Backup

There are several considerations to take into account when you are using a tool other than Continuent Tungsten to take a backup. We have taken great care to build all of these into our tools. If the options provided do not meet your needs, take these factors into account when taking your own backup.

- **How big is your data set?**
  
  The `mysqldump` tool is easy to use but will be very slow once your data gets too large. We find this happens around 1GB. The `xtrabackup` tool works on large data sets but requires more expertise. Choose a backup mechanism that is right for your data set.

- **Is all of your data in transaction-safe tables?**
  
  If all of your data is transaction-safe then you will not need to do anything special. If not then you need to take care to lock tables as part of the backup. Both `mysqldump` and `xtrabackup` take care of this. If you are using other mechanisms you will need to look at stopping the replicator, stopping the database. If you are taking a backup of the master then you may need to stop all access to the database.

- **Are you taking a backup of the master?**
  
  The Tungsten Replicator stores information in a schema to indicate the restart position for replication. On the master there can be a slight lag between this position and the actual position of the master. This is because the database must write the logs to disk before Tungsten Replicator can read them and update the current position in the schema.
When taking a backup from the master, you must track the actual binary log position of the master and start replication from that point after restoring it. See Section 5.10.2, “Restoring an External Backup” for more details on how to do that. When using mysqldump use the --master-data=2 option. The xtrabackup tool will print the binary log position in the command output.

Using mysqldump can be a very simple way to take consistent backup. Be aware that it can cause locking on MyISAM tables so running it against your master will cause application delays. The example below shows the bare minimum for arguments you should provide:

```shell
mysqldump --opt --single-transaction --all-databases --add-drop-database --master-data=2
```

### 5.10. Restoring a Backup

If a restore is being performed as part of the recovery procedure, consider using the tungsten_provision_slave tool. This will work for restoring from the master or a slave and is faster when you do not already have a backup ready to be restored. For more information, see Section 5.6.1.1, “Provision or Reprovision a Slave”.

To restore a backup, use the restore command to a datasource within cctrl:

1. Shun the datasource to be restored, and put the replicator service offline using cctrl:

   ```shell
   [LOGICAL] /alpha > datasource host2 shun
   [LOGICAL] /alpha > replicator host2 offline
   ```

2. Restore the backup using cctrl:

   ```shell
   [LOGICAL] /alpha > datasource host2 restore
   ```

   By default, the restore process takes the latest backup available for the host being restored. Continuent Tungsten does not automatically locate the latest backup within the dataservice across all datasources.

#### 5.10.1. Restoring a Specific Backup

To restore a specific backup, specify the location of the corresponding properties file using the format:

```
storage://storage-type/location
```

For example, to restore the backup from the filesystem using the information in the properties file `store-0000000004.properties`, login to the failed host:

1. Shun the datasource to be restored, and put the replicator service offline using cctrl:

   ```shell
   [LOGICAL] /alpha > datasource host2 shun
   [LOGICAL] /alpha > replicator host2 offline
   ```

2. Restore the backup using cctrl:

   ```shell
   [LOGICAL] /alpha > datasource host2 restore storage://file-system/store-0000000004.properties
   ```

   The supplied location is identical to that returned when a backup is performed.

#### 5.10.2. Restoring an External Backup

If a backup has been performed outside of Continuent Tungsten, for example from filesystem snapshot or a backup performed outside of the dataservice, follow these steps:

1. Shun the datasource to be restored, and put the replicator service offline using cctrl:

   ```shell
   [LOGICAL:EXPERT] /alpha > datasource host2 shun
   [LOGICAL:EXPERT] /alpha > replicator host2 offline
   ```

2. Reset the THL, either using thl or by deleting the files directly:

   ```shell
   shell> thl -service alpha purge
   ```

3. Restore the data or files using the external tool. This may require the database server to be stopped. If so, you should restart the database server before moving to the next step.

   **Note**

   The backup must be complete and the tungsten specific schemas must be part of the recovered data, as they are required to restart replication at the correct point. See Section 5.9.4, “Creating an External Backup” for more information on creating backups.
4. There is some additional work if the backup was taken of the master server. There may be a difference between the binary log position of the master and what is represented in the `trep_commit_seqno`. If these values are the same, you may proceed without further work. If not, the content of `trep_commit_seqno` must be updated.

   - Retrieve the contents of `trep_commit_seqno`:

     ```
     shell> echo "select seqno,source_id, eventid from tungsten_alpha.trep_commit_seqno" | tpm mysql
     seqno source_id eventid
     32033674 host1 mysql-bin.000032:0000000473860407; -1
     ```

   - Compare the results to the binary log position of the restored backup. For this example we will assume the backup was taken at `mysql-bin.000032:473863524`. Return to the master and find the correct sequence number for that position:

     ```
     shell> ssh host1
     shell> thl list -service alpha -low 32033674 -headers | grep 473863524
     32033678 32030709 0 true 2014-10-17 16:58:11.0 mysql-bin.000032:0000000473863524; -1 db1-east.continuent.com
     shell> exit
     ```

   - Return to the slave node and run `tungsten_set_position` to update the `trep_commit_seqno` table:

     ```
     shell> tungsten_set_position --service=alpha --source=host1 --seqno=32033678
     ```

5. Recover the datasource using `cctrl`:

   ```
   [LOGICAL] /alpha > datasource host2 recover
   ```

   The `recover` command will start the dataserver if it was left running and then bring the replicator and other operations online.

5.10.3. Restoring from Another Slave

If a restore is being performed as part of the recovery procedure, consider using the `tungsten_provision_slave` tool. This is will work for restoring from the master or a slave and is faster if you do not already have a backup ready to be restored. For more information, see Section 5.6.1.1, " Provision or Reprovision a Slave".

Data can be restored to a slave by performing a backup on a different slave, transferring the backup information to the slave you want to restore, and then running restore process.

For example, to restore the `host3` from a backup performed on `host2`:

1. Run the backup operation on `host2`:

   ```
   [LOGICAL:EXPERT] /alpha > datasource host2 backup
   Using the 'xtrabackup' backup agent.
   Replicator 'host2' starting backup
   Backup of dataSource 'host2' succeeded; uri=storage://file-system/store-0000000006.properties
   ```

2. Copy the backup information from `host2` to `host3`. See Section E.1.1.3, "Copying Backup Files" for more information on copying backup information between hosts. If you are using `xtrabackup` there will be additional files needed before the next step. The example below uses `scp` to copy a `mysqldump` backup:

   ```
   shell> cd /opt/continuent/backups
   shell> scp store-0000000006-mysqldump-812096863445699665.sql host3:$PWD/
   100%  234MB  18.0MB/s   00:13
   shell> scp store-0000000006.properties host3:$PWD/
   100%  314     0.3KB/s   00:00
   ```

   If you are using `xtrabackup`:

   ```
   shell> cd /opt/continuent/backups/xtrabackup
   shell> rsync -aze ssh full_xtrabackup_2014-08-16_15-44_86 host3:$PWD/
   ```

3. Shun the datasource to be restored, and put the replicator service offline using `cctrl`:

   ```
   [LOGICAL] /alpha > datasource host2 shun
   [LOGICAL] /alpha > replicator host2 offline
   ```

4. Restore the backup using `cctrl`:

   ```
   [LOGICAL] /alpha > datasource host2 restore
   ```

Once the restore operation has completed, the datasource will be placed into the online state.

**Note**

Check the ownership of files if you have trouble transferring files or restoring the backup. They should be owned by the Tungsten system user to ensure proper operation.
5.10.4. Manually Recovering from Another Slave

In the event that a restore operation fails, or due to a significant failure in the dataserver, an alternative option is to seed the failed dataserver directly from an existing running slave.

For example, on the host `host2`, the data directory for MySQL has been corrupted, and `mysqld` will no longer start. This status can be seen from examining the MySQL error log in `/var/log/mysql/error.log`:

```
130520 14:37:08 [Note] Recovering after a crash using /var/log/mysql/mysql-bin
130520 14:37:08 [Note] Starting crash recovery...
130520 14:37:08 [Note] Crash recovery finished.
130520 14:37:08 [Note] Server hostname (bind-address): '0.0.0.0'; port: 13306
130520 14:37:08 [Note] '0.0.0.0' resolves to '0.0.0.0'.
130520 14:37:08 [ERROR] Fatal error: Can't open and lock privilege tables: Table 'mysql.host' doesn't exist
130520 14:37:08 [ERROR] /usr/sbin/mysqld: File '/var/run/mysqld/mysqld.pid' not found (Errcode: 13)
130520 14:37:08 [ERROR] /usr/sbin/mysqld: Error reading file 'UNKNOWN' (Errcode: 9)
130520 14:37:08 [ERROR] /usr/sbin/mysqld: Error on close of 'UNKNOWN' (Errcode: 9)
```

Performing a restore operation on this slave may not work. To recover from another running slave, `host3`, the MySQL data files can be copied over to `host2` directly using the following steps:

1. Shun the `host2` datasource to be restored, and put the replicator service offline using `cctrl`:
   ```
   [LOGICAL] /alpha > datasource host2 shun
   [LOGICAL] /alpha > replicator host2 offline
   ```
2. Shun the `host3` datasource to be restored, and put the replicator service offline using `cctrl`:
   ```
   [LOGICAL] /alpha > datasource host3 shun
   [LOGICAL] /alpha > replicator host3 offline
   ```
3. Stop the `mysqld` service on `host2`:
   ```
   shell> sudo /etc/init.d/mysql stop
   ```
4. Stop the `mysqld` service on `host3`:
   ```
   shell> sudo /etc/init.d/mysql stop
   ```
5. Delete the `mysqld` data directory on `host2`:
   ```
   shell> sudo rm -rf /var/lib/mysql/*
   ```
6. If necessary, ensure the `tungsten` user can write to the MySQL directory:
   ```
   shell> sudo chown -R mysql:mysql /var/lib/mysql
   shell> sudo chmod 777 /var/lib/mysql
   ```
7. Use `rsync` on `host3` to send the data files for MySQL to `host2`:
   ```
   shell> rsync -aE ssh /var/lib/mysql/* host3:/var/lib/mysql/
   ``
   You should synchronize all locations that contain data. This includes additional folders such as `innodb_data_home_dir` or `innodb_log_group_home_dir`. Check the `my.cnf` file to ensure you have the correct paths.

   Once the files have been copied, the files should be updated to have the correct ownership and permissions so that the Tungsten service can read them.

8. Recover `host3` back to the dataservice:
   ```
   [LOGICAL:EXPERT] /alpha > dataservice host3 recover
   ```
9. Update the ownership and permissions on the data files on `host2`:
   ```
   host2 shell> sudo chown -R mysql:mysql /var/lib/mysql
   host2 shell> sudo chmod 770 /var/lib/mysql
   ```
10. Clear out the THL files on the target node `host2` so the slave replicator service may start cleanly:
    ```
    host2 shell> thl purge
    ```
11. Recover `host2` back to the dataservice:
    ```
    [LOGICAL:EXPERT] /alpha > dataservice host2 recover
    ```

    The `recover` command will start MySQL and ensure that the server is accessible before restarting replication. If the MySQL instance does not start; correct any issues and attempt the `recover` command again.
5.10.5. Rebuilding a Lost Datasource

If a datasource has been lost within the dataservice, for example, a complete hardware failure or disk crash, the datasource can be added back to the cluster once the operating system and other configuration have been completed. Essentially, the process is the same as when initially setting up your node, with the node being re-confirmed as part of the running service, installing and configuring only the returning node to the cluster.

In the following steps, the host host3 is being recovered into the cluster:

1. Setup the host with the pre-requisites, as described in Appendix C, Prerequisites.

2. Restore a snapshot of the data taken from another slave into the dataserver. If you have existing backups of this slave or another, they should be used. If not, take a snapshot of an existing slave and use this to apply the data to the slave. This will need to be performed outside of the Continuent Tungsten service using the native restore method for the backup method you have chosen. The backup must include the entire schema of your database, including the tungsten schemas for your services.

3. The next steps depend on the availability of the hostname. If the hostname of the datasource that was lost can be reused, then the host can be reconfigured within the existing service. If the hostname is not available, the service must be reconfigured to remove the old host, and add the new host.

Reusing an Existing Hostname

a. Login in to the server used for staging your Continuent Tungsten installation, and change to the staging directory. To determine the staging directory, use:

```
shell> tpm query staging
```

b. Repeat the installation of the service on the host being brought back:

```
shell> ./tools/tpm update svc_name --hosts=host3
```

The update process will re-install Continuent Tungsten on the host specified without reacting to the existence of the tungsten schema in the database.

Removing and Adding a new Host

a. Remove the existing (lost) datasource from the cluster using cctrl. First switch to administrative mode:

```
[LOGICAL] /alpha > admin
```

Remove the host from the dataservice:

```
[ADMIN] /alpha > rm host3
```

WARNING: This is an expert-level command:
Incorrect use may cause data corruption or make the cluster unavailable.

Do you want to continue? (y/n)>

b. Login in to the server used for staging your Continuent Tungsten installation, and change to the staging directory. To determine the staging directory, use:

```
shell> tpm query staging
```

c. Update the dataservice configuration with the new datasource, the example below uses host4 as the replacement datasource. The --dataservice-master-host should be used to specify the current master in the cluster:

```
shell> ./tools/tpm configure svc_name --dataservice-hosts=host1,host2,host4 \  

--dataservice-connectors=host1,host2,host4 \  

--dataservice-master-host=host4
```

d. Update the installation across all the hosts:

```
shell> ./tools/tpm update svc_name
```

4. Use cctrl to check and confirm the operation of the restore datasource.

The restored host should be part of the cluster and accepting events from the master as configured.

5.10.6. Resetting an Entire Dataservice from Filesystem Snapshots

To restore an entire dataservice from filesystem snapshots, the steps below should be followed. The same snapshot should be used on each host so that data on each host is the same. The following steps should be followed:
1. Set the dataservice into the `MAINTENANCE` policy mode:

```bash
[LOGICAL:EXPERT] /alpha > set policy maintenance
```

2. The following steps must be completed on each server before completing the next step:
   a. Stop the Continuent Tungsten services:
      ```bash
      shell> stopall
      ```
   b. Stop MySQL:
      ```bash
      shell> sudo /etc/init.d/mysql stop
      ```
   c. Replace the MySQL data files with the filesystem or snapshot data.
   d. Delete the THL files for each of the services that need to be reset:
      ```bash
      shell> rm /opt/continuent/thl/alpha/*
      ```
   e. Start MySQL to perform maintenance on the Tungsten schemas:
      ```bash
      shell> sudo /etc/init.d/mysql start
      ```
   f. Delete any Tungsten service schemas:
      ```bash
      mysql> DROP DATABASE tungsten_alpha;
      ```

   Once these steps have been executed on all the servers in the cluster, the services can be restarted.

3. On the current master, start the Continuent Tungsten services:

```bash
shell> startall
```

Now start the services using the same command on each of the remaining servers.

### 5.11. Migrating and Seeding Data

#### 5.11.1. Migrating from MySQL Native Replication 'In-Place'

If you are migrating an existing MySQL native replication deployment to use Continuent Tungsten the configuration of the Continuent Tungsten replication must be updated to match the status of the slave.

1. Deploy Continuent Tungsten using the model or system appropriate according to Chapter 2, *Deployment*. Ensure that the Continuent Tungsten is not started automatically by excluding the `--start` or `--start-and-report` options from the `tpm` commands.

2. On each slave
   Confirm that native replication is working on all slave nodes:
   ```bash
   shell> echo 'SHOW SLAVE STATUS;' | tpm mysql | \
   egrep ' Master_Host| Last_Error| Slave_SQL_Running'
   Master_Host: tr-ssl1
   Slave_SQL_Running: Yes
   Last_Error:
   ```

3. On the master and each slave
   Reset the Tungsten Replicator position on all servers:
   ```bash
   shell> replicator start offline
   shell> trepctl -service alpha reset -all -y
   ```

4. On the master
   Login and start Continuent Tungsten services and put the Tungsten Replicator online:
   ```bash
   shell> startall
   shell> trepctl online
   ```

5. On the master
   Put the cluster into maintenance mode using `cctrl` to prevent Continuent Tungsten automatically reconfiguring services:
   ```bash
   cctrl > set policy maintenance
   ```
6. On each slave

Record the current slave log position (as reported by the `Master_Log_File` and `Exec_Master_Log_Pos` output from `SHOW SLAVE STATUS`). Ideally, each slave should be stopped at the same position:

```shell
echo 'SHOW SLAVE STATUS\G' | tpm mysql | \
egrep "\^Master_Host| Last_Error| Master_Log_File| Exec_Master_Log_Pos\n   Master_Host: tr-ssl1
   Master_Log_File: mysql-bin.000025
   Last_Error: Error executing row event: 'Table 'tungsten_alpha.heartbeat' doesn't exist'
   Exec_Master_Log_Pos: 181268
```

If you have multiple slaves configured to read from this master, record the slave position individually for each host. Once you have the information for all the hosts, determine the earliest log file and log position across all the slaves, as this information will be needed when starting Continuent Tungsten replication. If one of the servers does not show an error, it may be replicating from an intermediate server. If so, you can proceed normally and assume this server stopped at the same position as the host is replicating from.

7. On the master

Take the replicator offline and clear the THL:

```shell
trepctl offline
trepctl -service alpha reset -all -y
```

8. On the master

Start replication, using the lowest binary log file and log position from the slave information determined in step 6.

```shell
trepctl online -from-event 000025:181268
```

Tungsten Replicator will start reading the MySQL binary log from this position, creating the corresponding THL event data.

9. On each slave

a. Disable native replication to prevent native replication being accidentally started on the slave.

   On MySQL 5.0 or MySQL 5.1:
   ```shell
echo "STOP SLAVE; CHANGE MASTER TO MASTER_HOST='';" | tpm mysql
   ```

   On MySQL 5.5 or later:
   ```shell
echo "STOP SLAVE; RESET SLAVE ALL;" | tpm mysql
   ```

b. If the final position of MySQL replication matches the lowest across all slaves, start Continuent Tungsten services:

   ```shell
trepctl online
trepctl startall
   ```

   The slave will start reading from the binary log position configured on the master.

   If the position on this slave is different, use `trepctl online -from-event` to set the online position according to the recorded position when native MySQL was disabled. Then start all remaining services with `startall`.

   ```shell
trepctl online -from-event 000025:188249
trepctl startall
   ```

10. Use `cctrl` to confirm that replication is operating correctly across the data service on all hosts.

11. Put the cluster back into automatic mode:

    ```cctrl> set policy automatic
    ```

12. Update your applications to use the installed connector services rather than a direct connection.

13. Remove the `master.info` file on each slave to ensure that when a slave restarts, it does not connect up to the master MySQL server again.

Once these steps have been completed, Continuent Tungsten should be operating as the replication service for your MySQL servers. Use the information in Chapter 5, *Operations Guide* to monitor and administer the service.

### 5.11.2. Migrating from MySQL Native Replication Using a New Service

When running an existing MySQL native replication service that needs to be migrated to a Continuent Tungsten service, one solution is to create the new Continuent Tungsten service, synchronize the content, and then install a service that migrates data from the existing native
service to the new service while applications are reconfigured to use the new service. The two can then be executed in parallel until applica-
tions have been migrated.

The basic structure is shown in Figure 5.2, “Migration: Migrating Native Replication using a New Service”. The migration consists of two steps:

- Initializing the new service with the current database state.
- Creating a Tungsten Replicator deployment that continues to replicate data from the native MySQL service to the new service.

Once the application has been switched and is executing against the new service, the secondary replication can be disabled by shutting
down the Tungsten Replicator in /opt/replicator.

Figure 5.2. Migration: Migrating Native Replication using a New Service

To configure the service:

1. Stop replication on a slave for the existing native replication installation:

   ```
   mysql> STOP SLAVE;
   ```

2. Create a backup using any method that provides a consistent snapshot. The MySQL master may be used if you do not have a slave to
   backup from. Be sure to get the binary log position as part of your back. This is included in the output to Xtrabackup or using the --mas-
   ter-data=2 option with mysqldump.

3. Restart the slave using native replication:

   ```
   mysql> START SLAVE;
   ```

4. On the master and each slave within the new service, restore the backup data and start the database service

5. Setup the new Continuent Tungsten deployment using the MySQL servers on which the data has been restored. For clarity, this will be
called newalpha.

6. Configure a second replication service, beta to apply data using the existing MySQL native replication server as the master, and the mas-
ter of newalpha.

   For more information, see Section 3.6, “Replicating Data Into an Existing Dataservice”.

   Do not start the new service.

7. Set the replication position for beta using tungsten_set_position to set the position to the point within the binary logs where the backup
   was taken:
8. Start replicator service beta:

```bash
grep /opt/replicator/tungsten/tungsten-replicator/bin/replicator start
```

Once replication has been started, use trepctl to check the status and ensure that replication is operating correctly.

The original native MySQL replication master can continue to be used for reading and writing from within your application, and changes will be replicated into the new service on the new hardware. Once the applications have been updated to use the new service, the old servers can be decommissioned and replicator service beta stopped and removed.

### 5.11.3. Seeding Data through MySQL

Once the Tungsten Replicator is installed, it can be used to provision all slaves with the master data. The slaves will need enough information in order for the installation to succeed and for Tungsten Replicator to start. The provisioning process requires dumping all data on the master and reloading it back into the master server. This will create a full set of THL entries for the slave replicators to apply. There may be no other applications accessing the master server while this process is running. Every table will be emptied out and repopulated so other applications would get an inconsistent view of the database. If the master is a MySQL slave, then the slave process may be stopped and started to prevent any changes without affecting other servers.

1. If you are using a MySQL slave as the master, stop the replication thread:

```bash
mysql> STOP SLAVE;
```

2. Check Tungsten Replicator status on all servers to make sure it is ONLINE and that the appliedLastSeqno Values are matching:

```bash
shell> trepctl status
```

Starting the process before all servers are consistent could cause inconsistencies. If you are trying to completely reprovision the server then you may consider running trepctl reset before proceeding. That will reset the replication position and ignore any previous events on the master.

3. Use mysqldump to output all of the schemas that need to be provisioned:

```bash
shell> mysqldump --opt --skip-extended-insert -h host3 -u tungsten -P13306 -p --databases db1,db2 > ~/dump.sql
```

Optionally, you can just dump a set of tables to be provisioned:

```bash
shell> mysqldump --opt --skip-extended-insert -h host3 -u tungsten -P13306 -p db1 table1 table2 > ~/dump.sql
```

4. If you are using heterogeneous replication all tables on the slave must be empty before proceeding. The Tungsten Replicator does not replicate DDL statements such as DROP TABLE and CREATE TABLE. You may either truncate the tables on the slave or use ddlscan to recreate them.

5. Load the dump file back into the master to recreate all data:

```bash
shell> cat ~/dump.sql | tpm mysql
```

The Tungsten Replicator will read the binary log as the dump file is loaded into MySQL. The slaves will automatically apply these statements through normal replication.

6. If you are using a MySQL slave as the master, restart the replication thread after the dump file as completed loading:

```bash
mysql> START SLAVE;
```

7. Monitor replication status on the master and slaves:

```bash
shell> trepctl status
```

### 5.12. Resetting a Continuent TungstenDataservice

Follow these steps to reset replication for an entire dataservice. The current master will remain the master. Use the switch after completion to change the master.

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.
For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

See Section 5.10.6, “Resetting an Entire Dataservice from Filesystem Snapshots” if you would like to restore a file system snapshot to every server as part of this process.

1. Put the dataservice into MAINTENANCE mode. This ensures that Continuent Tungsten will not attempt to automatically recover the service.
   ```
   cctrl> set policy maintenance
   ```

2. Enable force mode:
   ```
   cctrl> set force true
   ```

3. Shun each datasource:
   ```
   cctrl> datasource master shun
   cctrl> datasource slave1 shun
   cctrl> datasource slave2 shun
   ```

4. Put each Tungsten Connector offline:
   ```
   cctrl> router * offline
   ```

5. On each datasource, reset the service:
   ```
   shell> trepctl -service east offline
   shell> trepctl -service east reset -all -y
   ```

6. Reconfigure the replicator and datasource configuration on each host, starting with the master:
   ```
   cctrl> set force true
   cctrl> replicator new-master master
   cctrl> replicator new-master online
   cctrl> replicator slave1 slave new-master
   cctrl> replicator slave1 slave online
   cctrl> replicator slave2 slave new-master
   cctrl> replicator slave2 slave online
   cctrl> datasource slave1 slave
   cctrl> datasource slave2 slave
   cctrl> datasource slave1 slave online
   cctrl> datasource slave2 slave online
   ```

7. The connector can now be re-enabled and the cluster returned to operational state:
   ```
   cctrl> router * online
   cctrl> set policy automatic
   cctrl> cluster heartbeat
   ```

Any servers not matching the master must be reprovisioned. Use the `tungsten_provision_slave` tool to reprovision from the master or valid slave server.

### 5.12.1. Reset a Single Site in a Multisite/Multimaster Topology

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

Under certain conditions, dataservices in a multimaster configuration may drift and/or become inconsistent with the data in another dataservice. If this occurs, you may need to re-provision the data on one or more of the dataservices after first determining the definitive source of the information.

In the following example the `west` service has been determined to be the definitive copy of the data. To fix the issue, all the datasources in the `east` service will be reprovisioned from one of the datasources in the `west` service.

The following is a guide to the steps that should be followed. In the example procedure it is the `east` service that has failed:

1. Put the dataservice into MAINTENANCE mode. This ensures that Continuent Tungsten will not attempt to automatically recover the service.
   ```
   ctrl [east]> set policy maintenance
   ```
2. Put the Tungsten Connector for the dataservice offline:
   ```bash
   cctrl [east]> router * offline
   ```

3. Stop all services running in `east`:
   ```bash
   shell east> /opt/continuent/tungsten/cluster-home/bin/stopall
   shell east> /opt/replicator/tungsten/cluster-home/bin/stopall
   ```

4. Disable cross-site replication and reset the replication position:
   ```bash
   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east offline
   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east reset -all -y
   ```

5. Reprovision the master node in `east`:
   ```bash
   shell east[master]> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave --source west{slave}
   ```

6. Restart the services in `east`:
   ```bash
   shell east> /opt/continuent/tungsten/cluster-home/bin/startall
   shell east> /opt/continuent/tungsten/tungsten-replicator/bin/trepctl online
   shell east> /opt/replicator/tungsten/cluster-home/bin/startall
   ```

7. Ensure that the new service is functioning normally:
   ```bash
   shell east> echo ls | /opt/continuent/tungsten/tungsten-manager/bin/cctrl
   shell east> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl status
   ```

8. Bring the remote replicators back ONLINE
   ```bash
   shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east online
   ```

   Set the cluster to normal operational state:
   ```bash
   cctrl> router * online
   cctrl> set policy automatic
   ```

9. Reprovision the remaining nodes in the `east` cluster
   ```bash
   shell east{slave1}> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave \
   --source east{master}
   shell east{slave1}> /opt/continuent/tungsten/cluster-home/bin/startall
   shell east{slave1}> /opt/replicator/tungsten/cluster-home/bin/startall
   shell east{slave2}> /opt/continuent/tungsten/tungsten-replicator/scripts/tungsten_provision_slave \
   --source east{slave1}
   shell east{slave2}> /opt/continuent/tungsten/cluster-home/bin/startall
   shell east{slave2}> /opt/replicator/tungsten/cluster-home/bin/startall
   ```

### 5.12.2. Reset All Sites in a Multisite/Multimaster topology

**Warning**

The procedures in this section are designed for the pre-v6.x Multisite/Multimaster topology ONLY. Do NOT use these procedures with version 6.x Multisite Clusters.

For version 6.x Multisite Clustering, please refer to Deploying Composite Multimaster Clustering.

To reset all of the dataservices and restart the Continuent Tungsten and Tungsten Replicator services:

1. Put the both dataservices into `MAINTENANCE` mode. This ensures that Continuent Tungsten will not attempt to automatically recover the service.
   ```bash
   cctrl [east]> set policy maintenance
   cctrl [west]> set policy maintenance
   ```

2. Put the Tungsten Connector for both dataservices offline:
   ```bash
   cctrl [east]> router * offline
   cctrl [west]> router * offline
   ```

3. Stop the services on each server in the `east` region `east[1,2,3]`:
   ```bash
   shell east[1,2,3] /opt/continuent/tungsten/cluster-home/bin/stopall
   ```
4. Stop the services on each server in the west region (`west{1,2,3}`):

```shell
east>
shell east> /opt/continuent/tungsten/cluster-home/bin/stopall
east>
```

5. Reset the cluster on `east{1,2,3}`:

```shell
east>
shell east> /opt/continuent/tungsten/tools/tpm reset
east>
shell east> /opt/replicator/tungsten/tools/tpm reset
east>
```

6. Reset the cluster on `west{1,2,3}`:

```shell
west>
shell west> /opt/continuent/tungsten/tools/tpm reset
shell west> /opt/replicator/tungsten/tools/tpm reset
```

7. Reset the replication services on `east{1,2,3}`:

```shell
east>
shell east> /opt/continuent/tungsten/tungsten-replicator/bin/replicator start offline
east>
shell east> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east reset -all -y
```

8. Reset the replication services on `west{1,2,3}`:

```shell
west>
shell west> /opt/continuent/tungsten/tungsten-replicator/bin/replicator start offline
shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service west reset -all -y
```

9. Restart the services on each server in the east region (`east{1,2,3}`):

```shell
shell east> /opt/continuent/tungsten/cluster-home/bin/startall
```

10. Restart the services on each server in the west region (`west{1,2,3}`):

```shell
shell west> /opt/continuent/tungsten/cluster-home/bin/startall
```

11. Place all the Tungsten Replicator services on `east{1,2,3}` back online:

```shell
shell east> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service west online
```

12. Place all the Tungsten Replicator services on `west{1,2,3}` back online:

```shell
shell west> /opt/replicator/tungsten/tungsten-replicator/bin/trepctl -service east online
```

## 5.13. Replicator Fencing

Continuent Tungsten can be configured to handle failures during replication automatically and to fence the failure so that the issues do not lead to issues with the rest of the cluster, which may lead to problems with applications operating against the cluster. By default, the cluster is designed to take no specific action aside from indicating and registering the replicator so that the node will be identified as being within the **DIMINISHED** or **CRITICAL** state.

This behavior can be changed so that the failed replicator failure is fenced, with configuration operating on either the master, or slave replicators. When fencing has been enabled, the node will be placed into either the **OFFLINE** state if the node is a slave or a failover will occur if the node is a master.

### 5.13.1. Fencing a Slave Node Due to a Replication Fault

If the replicator should be placed into the **OFFLINE** state when replicator stops or raises an error, the following option can be set through `tpm` on the cluster configuration to set the `policy.fence.slaveReplicator` to true:

```shell
shell> tpm update alpha --property=policy.fence.slaveReplicator=true
```

The delay before the fencing operation takes place can be configured using the `policy.fence.slaveReplicator.threshold` parameter, which figures the delay before taking action, with the value multiplied by 10. For example, a setting of 6 implies a delay of 60 seconds. The delay enables transient errors, such as network failures, to be effectively managed without automatically fencing the slave.

```shell
shell> tpm update alpha --property=policy.fence.slaveReplicator.threshold=6
```

Once a slave has been fenced, the state will automatically be cleared when the replicator returns to the **ONLINE** state. Once this has been identified, the node will be placed in the **ONLINE** state.
5.13.2. Fencing Master Replicators

In the event of a master replicator failure, the fencing operation places the datasource into the **FAILED** state, triggering an automatic failover (see Section 5.5.1, “Automatic Master Failover”. Because this triggers a failover in the event of fencing the replicator, the configuration should only be enabled if it critical for your business that replication errors/stops should trigger a significant operation as failover.

To enable fencing of the master node due to replication faults, use the `policy.fence.masterReplicator` configuration property when configuring the cluster:

```
shell> tpm update alpha --property=policy.fence.masterReplicator=true
```

The delay before the fencing operation takes place can be configured using the `policy.fence.masterReplicator.threshold` property. The default value is 3, or 30 seconds.

```
shell> tpm update alpha --property=policy.fence.masterReplicator.threshold=6
```

When the replicator is identified as available, the master datasource is not placed back into the online state. Instead, the failed datasource must be explicitly recovered using the **recover** or **datasource host recover** commands.

5.14. Performing Database or OS Maintenance

When performing database or operating system maintenance, datasources should be temporarily removed from the dataservice and the replicator should be disabled. Follow these rules for the best results. Detailed steps are provided below for different scenarios.

- For maintenance operations on a master, the current master should be switched, the required maintenance steps performed, and then the master switched back.
- Disable a datasource using the **datasource shun** command.
- Put the replicator offline using **trepctl offline**.
- If you are using the Multisite/Multimaster topology, put the extra replicator offline using **mm_trepctl offline**. The **mm_trepctl alias** will only work if you configured Tungsten Replicator with the **--executable-prefix=mm** (in Tungsten Replicator 2.2 Manual) option.
- When making changes to a MySQL system the binary log should be disabled for your session. This will prevent corrective actions from replicating to other servers. Ignore this suggestion if you are making changes to a master that should be replicated.

```
mysql> SET SESSION SQL_LOG_BIN=0;
```

- Restart replication and recover the datasource after maintenance is complete using **datasource recover**, **trepctl online** and optionally **mm_trepctl online**.

5.14.1. Performing Maintenance on a Single Slave

Performing maintenance on a single slave can be achieved by temporarily shunning the slave (while in **AUTOMATIC** policy mode) and doing the necessary maintenance. Shunning a datasource in this way will temporarily remove it from the dataservice, and prevent active and new connections from using the datasource for operations.

The steps are:

1. Shun the slave:

```
[LOGICAL:EXPERT] /alpha > datasource host2 shun
```

Shunning a datasource does not put the replicator offline, so the replicator should also be put in the offline state to prevent replication and changes being applied to the database:

```
[LOGICAL:EXPERT] /alpha > replicator host2 offline
```

2. Perform the required maintenance, including updating the operating system, software or hardware changes.

3. Validate the server configuration:

```
shell> tpm validate
```

4. Recover the slave back to the dataservice:

```
[LOGICAL:EXPERT] /alpha > datasource host2 recover
```

Once the datasource is added back to the dataservice, the status of the node should be checked to ensure that the datasource has been correctly added back, and the node is **ONLINE** and up to date.
While the datasource is shunned, the node can be shutdown, restarted, upgraded, or any other maintenance. Throughout the process, the slave should be monitored to ensure that the datasource is correctly added back into the dataservice, and has caught up with the master. Any problems should be addressed immediately.

5.14.2. Performing Maintenance on a Master

Master maintenance must be carried out when the master has been switched to a slave, and then shunned. The master can be temporarily switched to a slave, taken out of the dataservice through shunning, and then added back to the dataservice and then switched back again to be the master.

**Important**

Maintenance on the dataserver should be performed directly on the corresponding server, not through the connector.

The complete sequence and commands required to perform maintenance on an active master are shown in the table below. The table assumes a datasource with three datasources:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
<th>host1</th>
<th>host2</th>
<th>host3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial state</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>2</td>
<td>Set the maintenance policy</td>
<td>set policy maintenance</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>3</td>
<td>Switch master</td>
<td>switch to host2</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>4</td>
<td>Shun host1</td>
<td>datasource host1 shun</td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>5</td>
<td>Perform maintenance</td>
<td></td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>6</td>
<td>Validate the host1 server configuration</td>
<td>tpm validate</td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>7</td>
<td>Recover the slave (host1) back</td>
<td>datasource host1 recover</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>8</td>
<td>Ensure the slave has caught up</td>
<td></td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>9</td>
<td>Switch master back to host1</td>
<td>switch to host1</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>10</td>
<td>Set automatic policy</td>
<td>set policy automatic</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
</tbody>
</table>

5.14.3. Performing Maintenance on an Entire Dataservice

To perform maintenance on all of the machines within a dataservice, a rolling sequence of maintenance must be performed carefully on each machine in a structured way. In brief, the sequence is as follows

1. Perform maintenance on each of the current slaves
2. Switch the master to one of the already maintained slaves
3. Perform maintenance on the old master [now in slave state]
4. Switch the old master back to be the master again

A more detailed sequence of steps, including the status of each datasource in the dataservice, and the commands to be performed, is shown in the table below. The table assumes a three-node datasource [one master, two slaves], but the same principles can be applied to any master/slave datasource:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
<th>host1</th>
<th>host2</th>
<th>host3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial state</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>2</td>
<td>Set maintenance policy</td>
<td>set policy maintenance</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>3</td>
<td>Shun slave host2</td>
<td>datasource host2 shun</td>
<td>Master</td>
<td>Shunned</td>
<td>Slave</td>
</tr>
<tr>
<td>4</td>
<td>Perform maintenance</td>
<td></td>
<td>Master</td>
<td>Shunned</td>
<td>Slave</td>
</tr>
<tr>
<td>5</td>
<td>Validate the host2 server configuration</td>
<td>tpm validate</td>
<td>Master</td>
<td>Shunned</td>
<td>Slave</td>
</tr>
<tr>
<td>6</td>
<td>Recover the slave host2 back</td>
<td>datasource host2 recover</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>7</td>
<td>Ensure the slave (host2) has caught up</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Command</td>
<td>host1</td>
<td>host2</td>
<td>host3</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>8</td>
<td>Shun slave host3</td>
<td>datasource host3 shun</td>
<td>Master</td>
<td>Slave</td>
<td>Shunned</td>
</tr>
<tr>
<td>9</td>
<td>Perform maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Validate the host3 server configuration</td>
<td>tpm validate</td>
<td>Master</td>
<td>Slave</td>
<td>Shunned</td>
</tr>
<tr>
<td>11</td>
<td>Recover slave host3 back</td>
<td>datasource host3 recover</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>12</td>
<td>Ensure the slave { host3 } has caught up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Switch master to host2</td>
<td>switch to host2</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>14</td>
<td>Shun host1</td>
<td>datasource host1 shun</td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>15</td>
<td>Perform maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Validate the host1 server configuration</td>
<td>tpm validate</td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>17</td>
<td>Recover the slave host1 back</td>
<td>datasource host1 recover</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>18</td>
<td>Ensure the slave { host1 } has caught up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Switch master back to host1</td>
<td>switch to host1</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>20</td>
<td>Set automatic policy</td>
<td>set policy automatic</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
</tbody>
</table>

5.14.4. Making Online Schema Changes

Similar to the maintenance procedure, schema changes to an underlying dataserver may need to be performed on dataservers that are not part of an active dataservice. Although many inline schema changes, such as the addition, removal or modification of an existing table definition will be correctly replicated to slaves, other operations, such as creating new indexes, adding/removing columns or migrating table data between table definitions, is best performed individually on each dataserver while it has been temporarily taken out of the dataservice.

As with all maintenance operations it is advisable to have fully tested your DDL in a staging environment. In some cases, the impact of DDL change is minimal and therefore can safely applied to the Master node and allowing the change to be replicated down to the slaves.

In situations where the overhead of the DDL change would cause an outage to your application through table locking, use the rolling maintenance procedure below which is specific for DDL changes.

The basic process comprises of a number of steps, these are as follows:

1. If the DDL adds or removes columns, then enable the `colnames` and `dropcolumn` filters
2. If the DDL adds or removes tables, and you do not want to simply apply to the master and allow replication to handle it, then enable the `replicate` filters
3. Perform schema changes following the process summarised in the table below
4. Optionally, remove the filters enabled in the first step

Enable filters for column changes

The use of the `colnames` and `dropcolumn` filters allow you to make changes to the structure of tables, without impacting the flow of replication.

Important

During these schema changes, and whilst the filters are in place, applications MUST be forwards and backwards compatible, but MUST NOT alter data within any columns that are filtered out from replication until after the process has been completed on all hosts, and the filters disabled. Data changes to filtered columns will cause data drift and inconsistencies, resulting in potentially unexpected behaviour.

- To enable the filters, first create a file called `schemachange.json` in a directory accessible by the OS user that the software is running as.

Typically, this will the `tungsten` user and the default location for this file will be `/opt/continuent/share`

The file needs to contain a JSON block outlining ALL the columns being added and removed from all tables affected by the changes.

In the example below, we are removing the column, `operator_code` and adding `operator_desc` to the `system_operators` table and adding the column `action_date` to the `system_actions` table:
- Place your cluster into **maintenance** mode

```shell
shell> cctrl
```

```shell
cctrl> set policy maintenance
```

**Note**

If running a Composite Multimaster or Composite HA/DR topology, issue the command at the top global level to place all clusters in maintenance, or execute individually within each cluster.

- Next, enable the filters within your configuration by adding the following two parameters to the `tungsten.ini` (if running in INI method) to the `[defaults]` section on EVERY cluster node:

```
svc-extractor-filters=colnames,dropcolumn
property=replicator.filter.dropcolumn.definitionsFile=/opt/continuent/share/schemachange.json
```

Followed by `tpm update` to apply the changes.

- Or, if running as a staging install:

```shell
cd staging_dir
shell> tools/tpm update alpha \
--svc-extractor-filters=colnames,dropcolumn \
--property=replicator.filter.dropcolumn.definitionsFile=/opt/continuent/share/schemachange.json
```

- Monitor replication to ensure there are no errors before continuing

Enable filters for adding/removing tables

The use of the `replicate` filter allows you to add and remove tables without impacting the flow of replication.

**Important**

During these schema changes, and whilst the filter is in place, applications **MUST** be forwards and backwards compatible, but **MUST NOT** modify data in any new tables until after the process has been completed on all hosts, and the filters disabled. Data changes to filtered tables will cause data drift and inconsistencies, resulting in potentially unexpected behaviour.

- Place your cluster into **maintenance** mode.

```shell
shell> cctrl
```

```shell
cctrl> set policy maintenance
```

**Note**

If running a Composite Multimaster or Composite HA/DR topology, issue the command at the top global level to place all clusters in maintenance, or individually within each cluster.

- Next, enable the filters within your configuration by adding the following two parameters to the `tungsten.ini` (if running in INI method) to the `[defaults]` Section on EVERY cluster node.

In this example we plan to **ADD** the table `system_actions` and **REMOVE** the table `system_operations`, both within the `ops` schema:

```
svc-extractor-filters=replicate
property=replicator.filter.replicate.ignore=ops.system_actions,ops.system_operations
```

Followed by `tpm update` to apply the changes.

- Or, if running as a staging install:

```shell
cd staging_dir
shell> tools/tpm update alpha \
--svc-extractor-filters=replicate \
--property=replicator.filter.replicate.ignore=ops.system_actions,ops.system_operations
```
• Monitor replication to ensure there are no errors before continuing.

Apply DDL Changes

• Follow the steps outlined in the table below to make the DDL changes to all nodes, in all clusters.

• If filtering columns, once all the changes have been complete, edit the `schemachange.json` to contain an empty document:

```shell
echo "[]" > /opt/continuent/share/schemachange.json
```

Then, restart the replicators:

```shell
replicator restart
```

• If filtering tables, repeat the process of adding the replicate filter removing any tables from the ignore parameter that you have ADDED to your database.

• You can optionally fully remove the filters if you wish by removing the entries from the configuration and re-running `tpm update` however it is also perfectly fine to leave them in place. There is a potentially small CPU overhead in very busy clusters by having the filters in place, but otherwise should not have any impact.

It is advisable to monitor the system usage and make the decision based on your own business needs.

The following method assumes a schema update on the entire dataservice by modifying the schema on the slaves first. The schema shows three datasources being updated in sequence, slaves first, then the master.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
<th>host1</th>
<th>host2</th>
<th>host3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial state</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>2</td>
<td>Set the slave <code>host2</code> offline</td>
<td><code>trepctl -host host2 offline</code></td>
<td>Master</td>
<td>Offline</td>
<td>Slave</td>
</tr>
<tr>
<td>3</td>
<td>Connect to dataserver for <code>host2</code> and update schema</td>
<td><code>set sql_log_bin=0; run ddl statements</code></td>
<td>Master</td>
<td>Offline</td>
<td>Slave</td>
</tr>
<tr>
<td>4</td>
<td>Set the slave online</td>
<td><code>trepctl -host host2 online</code></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>5</td>
<td>Ensure the slave (host2) has caught up</td>
<td><code>trepctl -host host2 status</code></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>6</td>
<td>Set the slave <code>host3</code> offline</td>
<td><code>trepctl -host host3 offline</code></td>
<td>Master</td>
<td>Slave</td>
<td>Offline</td>
</tr>
<tr>
<td>7</td>
<td>Connect to dataserver for <code>host3</code> and update schema</td>
<td><code>set sql_log_bin=0; run ddl statements</code></td>
<td>Master</td>
<td>Slave</td>
<td>Offline</td>
</tr>
<tr>
<td>8</td>
<td>Set the slave (host3) online</td>
<td><code>trepctl -host host3 online</code></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>9</td>
<td>Ensure the slave (host3) has caught up</td>
<td><code>trepctl -host host3 status</code></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>10</td>
<td>Switch master to host2</td>
<td>See Section 5.5, “Switching Master Hosts”</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>11</td>
<td>Set the slave <code>host1</code> offline</td>
<td><code>trepctl -host host1 offline</code></td>
<td>Offline</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>12</td>
<td>Connect to dataserver for <code>host1</code> and update schema</td>
<td><code>set sql_log_bin=0; run ddl statements</code></td>
<td>Offline</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>13</td>
<td>Set the slave <code>host1</code> online</td>
<td><code>trepctl -host host1 online</code></td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>14</td>
<td>Ensure the slave (host1) has caught up</td>
<td><code>trepctl -host host1 status</code></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>15</td>
<td>Switch master back to host1</td>
<td>See Section 5.5, “Switching Master Hosts”</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
</tbody>
</table>

**Note**

With any schema change to a database, the database performance should be monitored to ensure that the change is not affecting the overall dataservice performance.

### 5.14.5. Upgrading or Updating your JVM

When upgrading your JVM version or installation, care should be taken as changing the JVM will momentarily remove and replace required libraries and components which may upset the operation of Continuent Tungsten while the upgrade or update takes place.
For this reason, JVM updates or changes must be treated as an OS upgrade or event, requiring a master switch and controlled stopping/shunning of services during the update process.

A sample sequence for this in a 3-node cluster is described below:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
<th>host1</th>
<th>host2</th>
<th>host3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial state</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>2</td>
<td>Shun slave host2</td>
<td>datasource host2 shun</td>
<td>Master</td>
<td>Shunned</td>
<td>Slave</td>
</tr>
<tr>
<td>3</td>
<td>Stop all services on host2</td>
<td>stopall</td>
<td>Master</td>
<td>Stopped</td>
<td>Slave</td>
</tr>
<tr>
<td>4</td>
<td>Update the JVM</td>
<td></td>
<td>Master</td>
<td>Stopped</td>
<td>Slave</td>
</tr>
<tr>
<td>5</td>
<td>Start all services on host2 slave</td>
<td>startall</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>6</td>
<td>Recover slave back</td>
<td>datasource host2 recover</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>7</td>
<td>Ensure the slave (host2) has caught up</td>
<td>ls</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>8</td>
<td>Shun slave host3</td>
<td>datasource host3 shun</td>
<td>Master</td>
<td>Slave</td>
<td>Shunned</td>
</tr>
<tr>
<td>9</td>
<td>Stop all services on host3</td>
<td>stopall</td>
<td>Master</td>
<td>Slave</td>
<td>Stopped</td>
</tr>
<tr>
<td>10</td>
<td>Update the JVM</td>
<td></td>
<td>Master</td>
<td>Slave</td>
<td>Stopped</td>
</tr>
<tr>
<td>11</td>
<td>Start all services on host3 slave</td>
<td>startall</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>12</td>
<td>Recover slave back</td>
<td>datasource host3 recover</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>13</td>
<td>Ensure the slave (host3) has caught up</td>
<td>ls</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
<tr>
<td>14</td>
<td>Switch master to host2</td>
<td>switch to host2</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>15</td>
<td>Shun host1</td>
<td>datasource host1 shun</td>
<td>Shunned</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>16</td>
<td>Stop all services on host1</td>
<td>stopall</td>
<td>Stopped</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>17</td>
<td>Update the JVM</td>
<td></td>
<td>Stopped</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>18</td>
<td>Start all services on host1 slave</td>
<td>startall</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>19</td>
<td>Recover host1 back</td>
<td>datasource host1 recover</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>20</td>
<td>Ensure the slave (host1) has caught up</td>
<td>ls</td>
<td>Slave</td>
<td>Master</td>
<td>Slave</td>
</tr>
<tr>
<td>21</td>
<td>Switch master back to host1</td>
<td>switch to host1</td>
<td>Master</td>
<td>Slave</td>
<td>Slave</td>
</tr>
</tbody>
</table>

5.15. Performing Continuent Tungsten Maintenance

Changes to the configuration should be made with tpm update. This continues the procedure of using tpm install during installation. See Section 9.5.18, "tpm update Command" for more information on using tpm update.

For information on performing upgrades to new versions of the product with the existing configuration, see Section 4.4, "Upgrading Continuent Tungsten".

For information on performing downgrades to previous versions of the product with the existing configuration, see Section 4.5, "Downgrading to an Earlier Release".

5.16. Monitoring Continuent Tungsten

It is your responsibility to properly monitor your deployments of Continuent Tungsten and Tungsten Replicator. The minimum level of monitoring must be done at three levels. Additional monitors may be run depending on your environment but these three are required in order to ensure availability and uptime.

1. Make sure the appropriate Continuent Tungsten and Tungsten Replicator services are running.
2. Make sure all datasources and replication services are ONLINE.
3. Make sure replication latency is within an acceptable range.

**Important**

Special consideration must be taken if you have multiple installations on a single server. That applies for clustering and replication or multiple replicators.
These three points must be checked for all directories where Continuent Tungsten or Tungsten Replicator are installed. In addition, all servers should be monitored for basic health of the processors, disk and network. Proper alerting and graphing will prevent many issues that will cause system failures.

5.16.1. Managing Log Files with logrotate

You can manage the logs generated by Continuent Tungsten using `logrotate`.

- `connector.log`
  ```
  /opt/continuent/tungsten-connector/log/connector.log {
    notifempty
    daily
    rotate 3
    missingok
    compress
    copytruncate
  }
  ```

- `tmsvc.log`
  ```
  /opt/continuent/tungsten-manager/log/tmsvc.log {
    notifempty
    daily
    rotate 3
    missingok
    compress
    copytruncate
  }
  ```

- `trepsvc.log`
  ```
  /opt/continuent/tungsten-replicator/log/trepsvc.log {
    notifempty
    daily
    rotate 3
    missingok
    compress
    copytruncate
  }
  ```

5.16.2. Monitoring Status Using cacti

Graphing Tungsten Replicator data is supported through Cacti extensions. These provide information gathering for the following data points:

- Applied Latency
- Sequence Number [Events applied]
- Status [Online, Offline, Error, or Other]

To configure the Cacti services:

1. Download both files from https://github.com/continuent/monitoring/tree/master/cacti
2. Place the PHP script into `/usr/share/cacti/scripts`.
3. Modify the installed PHP file with the appropriate `$ssh_user` and `$tungsten_home` location from your installation:
   - `$ssh_user` should match the user used during installation.
   - `$tungsten_home` is the installation directory and the `tungsten` subdirectory. For example, if you have installed into `/opt/continuent`, use `/opt/continuent/tungsten`.
   Add SSH arguments to specify the correct `id_rsa` file if needed.
4. Ensure that the configured `$ssh_user` has the correct SSH authorized keys to login to the server or servers being monitored. The user must also have the correct permissions and rights to write to the cache directory.
5. Test the script by running it by hand:
   ```
   shell> php -q /usr/share/cacti/scripts/get_replicator_stats.php --hostname replserver
   ```
   If you are using multiple replication services, add `--service servicename` to the command.
6. Import the XML file as a Cacti template.
7. Add the desired graphs to your servers running Continuent Tungsten. If you are using multiple replications services, you'll need to specify the desired service to graph. A graph must be added for each individual replication service.

Once configured, graphs can be used to display the activity and availability.

Figure 5.3. Cacti Monitoring: Example Graphs
5.16.3. Monitoring Status Using nagios

In addition to the scripts bundled with the software, there is a Ruby gem available with expanded checks and a mechanism to add custom checks. See https://github.com/continuent/continuent-monitors-nagios for more details.

Integration with Nagios is supported through a number of scripts that output information in a format compatible with the Nagios NRPE plugin. Using the plugin the check commands, such as `check_tungsten_latency` can be executed and the output parsed for status information.

The available commands are:

- `check_tungsten_latency`
- `check_tungsten_online`
- `check_tungsten_progress`
- `check_tungsten_services`

To configure the scripts to be executed through NRPE:

1. Install the Nagios NRPE server.
2. Start the NRPE daemon:
   ```shell
   sudo /etc/init.d/nagios-nrpe-server start
   ```
3. Add the IP of your Nagios server to the `/etc/nagios/nrpe.cfg` configuration file. For example:
   ```
alowed_hosts=127.0.0.1,192.168.2.20
   ```
4. Add the Tungsten check commands that you want to execute to the `/etc/nagios/nrpe.cfg` configuration file. For example:
   ```
   command[check_tungsten_online]=/opt/continuent/tungsten/cluster-home/bin/check_tungsten_online
   ```
5. Restart the NRPE service:
   ```shell
   sudo /etc/init.d/nagios-nrpe-server start
   ```
6. If the commands need to be executed with superuser privileges, the `/etc/sudo` or `/etc/sudoers` file must be updated to enable the commands to be executed as root through `sudo` as the `nagios` user. This can be achieved by updating the configuration file, usually performed by using the `visudo` command:
   ```
   nagios ALL=(tungsten) NOPASSWD: /opt/continuent/tungsten/cluster-home/bin/check*
   ```
   In addition, the `sudo` command should be added to the Tungsten check commands within the Nagios `nrpe.cfg`, for example:
   ```
   command[check_tungsten_online]=/usr/bin/sudo -u tungsten /opt/continuent/tungsten/cluster-home/bin/check_tungsten_online
   ```
   Restart the NRPE service for these changes to take effect.
7. Add an entry to your Nagios `services.cfg` file for each service you want to monitor:

   ```
   define service {
       host_name database
       service_description     check_tungsten_online
       check_command           check_nrpe! -H $HOSTADDRESS$ -t 30 -c check_tungsten_online
       retry_check_interval    1
       check_period            24x7
       max_check_attempts      3
       flap_detection_enabled  1
       notifications_enabled   1
       notification_period     24x7
       notification_interval   60
       notification_options    c,f,r,u,w
       normal_check_interval   5
   }
   ```

The same process can be repeated for all the hosts within your environment where there is a Tungsten service installed.

5.17. Rebuilding THL on the Master

If THL is lost on a master before the events contained within it have been applied to the slave(s), the THL will need to be rebuilt from the existing MySQL binary logs.
Important

If the MySQL binary logs no longer exist, then recovery of the lost transactions in THL will NOT be possible.

The basic sequence of operation for recovering the THL on both master and slaves is:

1. Gather the failing requested sequence numbers from all slaves:
   
   ```shell
   trepctl status
   ```
   
   pendingError           : Event extraction failed
   pendingErrorCode       : NONE
   pendingErrorEventId    : NONE
   pendingErrorSeqno      : -1
   pendingExceptionMessage: Client handshake failure: client response validation failed:
   master log does not contain requested transaction:
   master source ID=db1 client source ID=db2 requested seqno=4 master min seqno=8 master max seqno=8
   
   In the above example, when slave db2 comes back online, it requests a copy of the last seqno in local thl (4) from the master db1 to compare for data integrity purposes, which the master no longer has.

   Keep a note of the lowest sequence number and the host that it is on across all slaves for use in the next step.

2. On the slave with the lowest failing requested seqno, get the epoch, source-id and event-id [binlog position] from the THL using the command `thl list -seqno` specifying the sequence number above. This information will be needed on the extractor [master] in a later step. For example:

   ```shell
tungsten@db2:/opt/replicator> thl list -seqno 4
   SEQ# = 4 / FRAG# = 0 (last frag)
   - TIME = 2017-07-14 14:49:00.0
   - EPOCH# = 0
   - EVENTID = mysql-bin.000009:0000000000001844;56
   - SOURCEID = db1
   - METADATA = [mysql_server_id=33155307;dbms_type=mysql;is_metadata=true;service=East;shard=#UNKNOWN;heartbeat=NULL]
   - TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
   - OPTIONS = [##charset = UTF-8, autocommit = 1, sql_auto_is_null = 0, foreign_key_checks = 1, unique_checks = 1, time_zone = '+00:00', sql_mode = 'NO_ENGINE_SUBSTITUTION,STRICT_TRANS_TABLES,IGNORE_SPACE', character_set_client = 8, collation_connection = 8, collation_server = 8]
   - SCHEMA = tungsten_east
   - SQL(0) = UPDATE tungsten_east.heartbeat SET source_tstamp= '2017-07-14 14:49:00', salt= 5, name= 'NONE'  WHERE id= 1
   ```

   There are two more ways of getting the same information, use the one you are most comfortable with:

   ```json
dsctl get
   [{"extract_timestamp":"2017-07-14 14:49:00.0","eventid":"mysql-bin.000009:0000000000001844;56","fragno":4,"last_frag":true,"seqno":4,"update_timestamp":"2017-07-14 14:49:00.0", "shard_id":"#UNKNOWN"}]
   ```

   ```json
tungsten@db2:/opt/replicator>
tungsten_get_position
   {
   "applied_latency": 0,
   "epoch_number": 0,
   "eventid": "mysql-bin.000009:0000000000001844;56",
   "extract_timestamp": "2017-07-14 14:49:00.0",
   "fragno": 0,
   "last_frag": 1,
   "seqno": 4,
   "shard_id": "#UNKNOWN",
   "source_id": "db1",
   "task_id": 0,
   "update_timestamp": "2017-07-14 14:49:00.0"
   }
   ```

3. Clear all THL on the master since it is no longer needed by any slaves:

   ```shell
   thl purge
   ```

4. Use the `tungsten_set_position` command on the master with the values we got from the slave with the lowest seqno to tell the master replicator to begin generating THL starting from that event in the MySQL binary logs:

   ```shell
   tungsten_set_position --seqno=4 --epoch=0 --source-id=db1 --event-id=mysql-bin.000009:0000000000001844
   ```

   You may also use dsctl, but that requires executing the dsctl reset command first.

5. Switch the master to online state:

```
```
6. Switch the slaves to online state once the master is fully online:

   shell> trepctl online
Chapter 6. Tungsten Connector

Tungsten Connector acts as a proxy service, sitting between client applications and datasources in order to balance the load and provide high availability (HA) support. The service works by accepting raw packets from clients, and then forwarding them to the datasource. The process is reversed when packets are sent back from the datasource and then redirected back to the clients.

Figure 6.1. Tungsten Connector Basic Architecture

In addition to this basic structure, Tungsten Connector also works with the other components of Continuent Tungsten to handle some specific scenarios and situations:

- The connector works in harmony with the Tungsten Manager as part of Continuent Tungsten and enables the connector to redirect queries between known datasources within a given dataservice. For example, when the manager identifies a failed datasource, queries to that datasource are redirected to an alternative datasource without the application being aware of the change.

- The connector works with the Continuent Tungsten configuration and a number of implied or explicit directives that enable the connector to redirect requests within different datasources within the network. For example, the connector can be configured to automatically forward write requests to a database to the active master within the dataservice and reads to active slaves.

Throughout this process the connector is redirecting the network packets sent by application servers to the appropriate host. The contents and individual statements are not processed or accessed. At all times applications and clients using the connector do not need modification as to them it will appear as a MySQL server.

To start using the connector run the `tpm connector` command. This will open a connection with the MySQL CLI. See Section 6.3, “Clients and Deployment” for more detail on configuring your application to use the connector.

Important

After installation the connector will only work with the `--application-user` and `--application-password` that were provided during installation. See Section 6.6, “User Authentication” if you need more information on adding users to `user.map`.

6.1. Connector/Application Basics

Within any typical database deployment there will be two primary considerations:

- High Availability — redirecting requests to alternative servers in the event of a failure.
- Scalability — distributing reads and writes across servers in a replication architecture.

Within a typical basic database deployment clients and application servers will connect directly to databases, as shown in Figure 6.2, “Basic MySQL/Application Connectivity”.
The problem with this deployment model is that it is not able to cope with changes or problems. If one or more of your database servers fails, then the application servers must be reconfigured individually to point to an alternative server. In addition, when considering scalability, there is no provision for redirecting reads and writes to masters or slaves.

In an advanced application deployment, individual servers may have been configured to connect to masters and slaves and configured your application to talk directly to the master and/or slaves within the database infrastructure to handle the scalability offered by using replication [Figure 6.3, “Advanced MySQL/Application Connectivity”]. For this to work the application must have been modified and be read/write aware, and it must have been configured to manually connect to the different databases according to the operation being performed.
Although this handles the read/write splitting, enabling servers to write to the master and read from one or more slaves, changes to this architecture and structure are not handled. If the master fails, application servers must be manually updated to direct their queries to an alternative host.

When deploying Continuent Tungsten the connector takes over the role of primary connection from your application to the database server, and it handles the redirection of requests to the appropriate database server. Depending on your application configuration and architecture, the connector can be used in two ways:

- As a complete solution for redirecting queries between the master and slave hosts within a dataservice, including HA events.
- As an HA solution redirecting queries to the master and slaves within a dataservice, but with application driven master/slave selection.

When deploying your application with Continuent Tungsten through Tungsten Connector, the application server connectivity is through the connector. The connector takes on the role of primary connection for all requests, while routing and distributing those requests to the active datasources within the dataservice.

The Tungsten Connector is located between the clients and the database servers, providing a single connection point, while routing queries to the database servers. In the event of a failure, the Tungsten Connector can automatically route queries away from the failed server and towards servers that are still operating. During the routing process, Tungsten Connector communicates with the Tungsten Manager to determine which datasources are the most up to date, and their current role so that the packets can be routed properly.

Because the connectivity is between the application service and the Tungsten Connector, the connection to the Tungsten Connector remains constant. Changes to the datasources, including failures, role changes, and expansion or removal of datasources from the dataservice do not require any modification of the application configuration or operation.
Tungsten Connector

Figure 6.5. Tungsten Connector during a failed datasource

For example, in Figure 6.5, "Tungsten Connector during a failed datasource", the slave datasource has failed. While this would break the connection between the Tungsten Connector and the datasource, the connection between the application and Tungsten Connector remains available, and Tungsten Connector will re-route queries to an available datasource without reconfiguring the application server connectivity.

6.1.1. Connector Control Flow

The Connector makes a TCP connection to any available Manager, then all command-and-control traffic uses that channel. The Manager never initiates a connection to the Connector.

When there is a state change (i.e. shun, welcome, failover, etc.), the Manager will communicate to the Connector over the existing channel.

The Connector will re-establish a channel to an available Manager if the Manager it is connected to is stopped or lost.

6.2. Basic Connector Configuration

By default, the Tungsten Connector listens on port 9999 so as to avoid conflicting with the default MySQL listener port of 3306.

The best practice is the change the MySQL port to 13306 and the Tungsten Connector port to 3306.

For example, modify my.cnf to define the port, then restart MySQL:

```bash
port = 13306
```

For more information, see Section C.3.2, "MySQL Configuration".

Configure the the Tungsten Connector to listen on port 3306:

```bash
shell > tpm update alpha --application-port=3306
```

Important

This change is especially important if the Tungsten Connector will be installed directly on the database nodes. ALL traffic needs to flow through the Tungsten Connector, so hiding the actual MySQL port prevents mistaken connections directly to the database.

6.3. Clients and Deployment

In order to get the benefits of Continuent Tungsten your application must use the Tungsten Connector. The connector is compatible with MySQL drivers and applications. Use the tpm connector --samples command to see examples of how you can invoke a connection on your own. You may need to adapt these examples to your application and configuration method but the connection details should be the same.

```bash
shell > tpm connector --samples
```

Bash

```bash
mysql -hconnector1 -P3306 -uappuser -ppassword
```

Perl::dbi

```perl
$dbh=DBI->connecti('DBI:mysql:host=connector1;port=3306', 'appuser', 'password')
```

PHP::mysqli

```perl
$conn = new PDO("mysql:host=connector1;port=3306", 'appuser', 'password');
```

---

180
After installation the connector will only work with the --application-user [345] and --application-password [344] options that were provided during installation. See Section 6.6, "User Authentication" if you need more information on adding users to user.map.

By default the connection will always be sent to the current master. This behavior can be modified by implementing one of the routing methods to send some traffic to slave datasources.

### 6.3.1. Connection Pools

Tungsten Connector can work behind a connection pool without any issue.

Upon switch or failover, all connections in the pool will be broken but not closed. The very next time one of these pooled connections is used, it will be transparently reconnected unless autoReconnect has been disabled by the tpm installation flag:

```bash
shell > tpm update alpha --connector-autoreconnect=false
```

**Important**

When using a connection pool mechanism in applications, the dynamic connection setting maxAppliedLatency should not be used. This setting is only meaningful at connection time; since connection pools open a set of connections, the applied latency will most probably be outdated when the application will actually use the pooled connection.

### 6.4. Routing Methods

Tungsten Connector routes connections between client connections and datasources using a number of different routing methods. These routing methods affect how client applications and datasources are connected to each other, and control the level of inspection by Tungsten Connector of the connections and statements as they pass through the connector service.

The Tungsten Connector works with Tungsten Manager to automatically route clients connected to the connector to an appropriate server, balancing the load when communicating with slaves. The different methods are involved in effective read/write splitting, i.e. the ability to correctly route requests to the masters or slaves within the network according to the type of operation being performed by the client. This can be performed automatically, or manually, or through a series of specific configurable routing methods.

**Figure 6.6. Tungsten Connector routing architecture**
Routing selection is made by the connector based on the availability information using a combination of different settings and parameters. Each level overrides or augments the previous level, and each can be specified in different locations, such as the user.map, connecting string, or within individual supplied statements. The settings are processed in the order shown below; later setting override earlier settings.

For example, selecting the SQL routing method defines the default behavior. Specifying the QoS in the user.map file supersedes the SQL routing; setting QoS in a comment before the SQL statement supersedes the user and default behavior. Specifying an affinity in the comments overrides both the user and default configuration settings.

- **Selected routing method**, see Section 6.4.1, “Connector Routing Methods”
- **Quality of Service (QoS) specification**, see Section 6.4.2, “Connector Quality of Service (QoS) Selection”
- **Load balancer selection (implied by QoS)**, see Section 6.4.3, “Connector Load Balancers”
- **Slave latency, including optional maximum latency setting**, see Section 6.4.4, “Specifying Required Latency”
- **Affinity specification**, see Section 6.4.5, “Setting Read Affinity and Direct Reads”

These different routing configurations can be selected according to the global configuration, and customization at different points in the communication channel. For example, SQL-based routing configures basic load-balancing, but allows SQL comments to be used to change the default QoS mode and affinity.

<table>
<thead>
<tr>
<th>Routing Method</th>
<th>GoS</th>
<th>Latency</th>
<th>Affinity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Configuration</td>
<td>Yes</td>
<td>Implied</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection String</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>user.map</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SQL statement</td>
<td>Yes (with SQL routing enabled)</td>
<td>Yes (with SQL routing enabled)</td>
<td>No</td>
</tr>
</tbody>
</table>

At all times, the connector uses the current status of the MySQL servers to make decisions about where queries and connections should be routed. Changes to the master, and availability or accessibility of individual dataservers will always be taken into account when routing the queries. For information on what happens if failure occurs during an operation or transaction, see Section 6.7, “Connector Operational States”.

The routing methods can either involve direct reads, SmartScale, host-based routing, or SQL inspection-based routing to redirect reads and writes to the appropriate server. In addition to these implied routing methods, clients can also specifically select which host to communicate with through the use of tags and options provided through the connection string.

The selection of a datasource occurs at the point the client connects, and this datasource connection choice remains in effect until the client disconnects, unless a failover or switch occurs.

### 6.4.1. Connector Routing Methods

The supported routing methods, typical uses and use cases are listed in Table 6.1, “Routing Method Selection”.

<table>
<thead>
<tr>
<th>Routing Method</th>
<th>Host Selection</th>
<th>Auto R/W Splitting</th>
<th>Slave Latency</th>
<th>Maximum Applied Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartscale</td>
<td>By Session</td>
<td>Yes (by SQL statement)</td>
<td>Lazy</td>
<td>Yes</td>
</tr>
<tr>
<td>Direct Reads</td>
<td>By Content</td>
<td>Yes (by SQL statement)</td>
<td>Lazy</td>
<td>Yes</td>
</tr>
<tr>
<td>Host-based</td>
<td>By Hostname</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port-based</td>
<td>By Network Port</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SQL-based</td>
<td>By SQL comment</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Important**

Both SmartScale and R/W splitting cannot be enabled at the same time. This is because they are two sides of the basic functionality. R/W splitting and SmartScale both use SQL introspection to determine whether a query should be directed to a master or a slave. SmartScale combines this with an intelligent load-balancer. R/W splitting uses a simpler direct redirection.

In addition to the selection and configuration mechanisms supported, a routing method should be chosen based on your application abilities:

- **If the application is replication-aware, and can already direct queries to master or slaves based on the operation type**, use Section 6.4.9, “Host-based Routing” or Section 6.4.10, “Port-based Routing”
• If the application has full control of the SQL statements submitted (i.e. not through a third-party tool, or Object-Relational Modeling library), and can already direct queries to master or slaves based on the operation type, use Section 6.4.8, “SQL Routing”.

• If the application uses non-auto-commit statements (for example, Hibernate), Section 6.4.9, “Host-based Routing”, or Section 6.4.8, “SQL Routing”.

• If the application does not fit any of these categories, or is not replication aware use either either Section 6.4.7, “Direct Routing” or Section 6.4.6, “Smartscale Routing”.

6.4.2. Connector Quality of Service (QoS) Selection

Depending on the chosen routing and authentication method, the ‘Quality of Service’ [QoS] setting can be specified as part of the SQL statement, host, or user configuration, and affects the selection of the MySQL server:

• **RO_RELAXED [183]**

  This setting enables the connector to redirect the query as if it were read-only, and therefore prefer a slave over a master, but will choose a master if no slave is available.

• **RW_STRICT [183]**

  This setting indicates that the query is a write and should be directed to a master.

• **RW_SESSION [183]**

  Where possible, the QoS should be set for read/write splitting according to the current session state.

These hints for the connection can be set, for example by using the value in the comments during SQL routing, or by setting the corresponding QoS value in the *user.map* file.

Further, connectivity can be influenced by setting a suitable latency value, or an explicit affinity. This information can be specified either within the connection strings, within the *user.map*, or through configuration.

The rules for selection of whether a connection is made to a master or a slave is therefore controlled by comparing all of these settings and the selected routing mechanism together.

<table>
<thead>
<tr>
<th>SmartScale</th>
<th>QoS</th>
<th>Maximum Applied Latency</th>
<th>Selection Order</th>
<th>Affinity</th>
<th>Master Selected</th>
<th>Slave Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Not Specified</td>
<td>Not Specified</td>
<td>Not Specified</td>
<td>Slave:Master</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Not Enabled</td>
<td>RO_RELAXED</td>
<td>Not Specified</td>
<td>Not Specified</td>
<td>Slave:Master</td>
<td>Only if no slave available</td>
<td>Yes</td>
</tr>
<tr>
<td>Not Enabled</td>
<td>RO_RELAXED</td>
<td>Specified</td>
<td>Not Specified</td>
<td>Slave:Master</td>
<td>Only if no slave available</td>
<td>Only if slave latency &lt; --connector-max-applied-latency [350]</td>
</tr>
</tbody>
</table>

6.4.3. Connector Load Balancers

The load balancing model used, according to the selected QoS is defined by a number of different load balancing classes. These are configured automatically when different QoS is selected, be explicitly changed by altering the configuration file. The supported load balancers are detailed in the table below:

<table>
<thead>
<tr>
<th>Load Balancer</th>
<th>Default QoS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefaultLoadBalancer</td>
<td>RW_STRICT</td>
<td>Always selects the master data source</td>
</tr>
<tr>
<td>MostAdvancedSlaveLoadBalancer</td>
<td>RO_RELAXED</td>
<td>Selects the slave that has replicated the more events, by comparing data sources “high water” marks. If no slave is available, the master will be returned.</td>
</tr>
<tr>
<td>LowestLatencySlaveLoadBalancer</td>
<td>RO_RELAXED</td>
<td>Selects the slave data source that has the lowest replication lag, or applied_latency in ls -l within cctrl output. If no slave data source is eligible, the master data source will be selected.</td>
</tr>
<tr>
<td>RoundRobinSlaveLoadBalancer</td>
<td></td>
<td>Selects a slave in a round robin manner, by iterating through them using internal index. Returns the master if no slave is found online.</td>
</tr>
<tr>
<td>HighWaterSlaveLoadBalancer</td>
<td>RW_SESSION</td>
<td>Given a session high water [usually the high water mark of the update event], selects the first slave that has higher or equal high water, or the master if no slave is online or has replicated the given session event. This is the default used when SmartScale is enabled.</td>
</tr>
</tbody>
</table>
The default setting is `lowestLatencySlaveLoadBalancer`.

To change the Connector load balancer, specify the property in the configuration, i.e, to use Round Robin:

```
shell> ./tools/tpm update alpha --property=dataSourceLoadBalancer_RO_RELAXED=com.continuent.tungsten.router.resource.loadbalancer.RoundRobinSlaveLoadBalancer
```

### 6.4.4. Specifying Required Latency

Depending on the selected routing method, load balancer and QoS setting, a slave will automatically be chosen when the host connects. The maximum allowed latency can be set to limit the connection to only use a slave that is within the specified maximum applied latency limit.

This can be specified in the connection string, and enables slave selection based on the slave which has a latency within the specified limit. For example, using the connection string:

```
jdbc://connector1:3306/database?maxAppliedLatency=5
```

Will specify that a host with a replication latency of less than 5 seconds should be selected.

The option can be set globally by configuring the JDBC options used by the connector via the `--connector-max-slave-latency` [350] option to `tpm` (in seconds):

```
shell> ./tools/tpm update alpha --connector-max-slave-latency=10
```

**Warning**

The Connector computes latency by polling the Replicator every 3 seconds for the current replication-view latency. This gives the Connector an accuracy of +/- 3 seconds, which means that values of 3 or less will not function as expected.

For any queries that have a very low tolerance for replication latency, we strongly suggest you read directly from the master database server only. This ensures the latest data is being read.

**Important**

The `--connector-max-slave-latency` [350] flag does not ensure the slave has applied the latest sequence number, just that its latency at the last commit was under the specified number. This behavior can be adjusted by specifying `--use-relative-latency=true` [351] in the configuration.

NOTE: `--use-relative-latency=true` [351] is a cluster-wide setting, cctrl and trepctl will also report relative latency based on this setting.

### 6.4.4.1. Applied and Relative Latency Comparison

- **Applied Latency**

  The `appliedLatency` is the latency between the commit time of the source event and the time the last committed transaction reached the end of the corresponding pipeline within the replicator. Within a master, this indicates the latency between the transaction commit time and when it was written to the THL. In a slave, it indicates the latency between the commit time on the master database and when the transaction has been committed to the destination database. Clocks must be synchronized across hosts for this information to be accurate.

  `appliedLatency : 0.828` The latency is measured in seconds. Increasing latency may indicate that the destination database is unable to keep up with the transactions from the master. In replicators that are operating with parallel apply, `appliedLatency` indicates the latency of the trailing channel. Because the parallel apply mechanism does not update all channels simultaneously, the figure shown may trail significantly from the actual latency.

  See Section D.2.6, “Terminology: Fields `appliedLatency`” for more information.

- **Relative Latency**

  The `relativeLatency` is the latency between now and timestamp of the last event written into the local THL. This information gives an indication of how fresh the incoming THL information is. On a master, it indicates whether the master is keeping up with transactions generated on the master database. On a slave, it indicates how up to date the THL read from the master is. A large value can either indicate that the database is not busy, that a large transaction is currently being read from the source database, or from the master replicator, or that the replicator has stalled for some reason. An increasing `relativeLatency` on the slave may indicate that the replicator may have stalled and stopped applying changes to the dataserver.

  See Section D.2.70, “Terminology: Fields `relativeLatency`” for more information.

- **Comparing Relative and Applied Latencies**
Both relative and applied latency are visible via the `trepctl status`. Relative indicates the latency since the last time the `appliedLastSeqno` advanced; for example:

```shell
trepctl status
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>appliedLastEventId</td>
<td>mysql-bin.000211:0000088020004766:0</td>
</tr>
<tr>
<td>appliedLastSeqno</td>
<td>78822</td>
</tr>
<tr>
<td>appliedLatency</td>
<td>0.571</td>
</tr>
<tr>
<td>relativeLatency</td>
<td>8.944</td>
</tr>
</tbody>
</table>

In this example the last transaction had an applied latency (time to write to the slave DB) of 0.571 seconds from the time it committed on the master, and last committed something to the slave DB 8.944 seconds ago.

If relative latency increases significantly in a busy system, it may be a sign that replication is stalled. This is a good parameter to check in monitoring scripts.

- For more information, see:
  - `--connector-max-slave-latency` [350]
  - `--use-relative-latency` [351]

Section 4.1.6.3, “Relative Latency”

6.4.4.2. Advanced Troubleshooting for Latency-based Routing

To troubleshoot the latency-based routing decisions the connector makes, and uncomment the below lines in `/opt/continuent/tungsten/tungsten-connector/conf/log4j.properties`:

```properties
#log4j.logger.com.continuent.tungsten.router.resource.loadbalancer=debug, stdout
#log4j.additivity.com.continuent.tungsten.router.resource.loadbalancer=false
```

The log will then show and explain what node the connector choose and why.

```
Important
No connector restart is required to enable logging. If you re-comment the lines, a restart will be required. To disable without a connector restart, replace the word `debug` with the word `info`.
```

6.4.5. Setting Read Affinity and Direct Reads

Affinity enables you to specify at connection time that the connector should forward the connection to a particular host or service for reads, if the service is available. For example, within `user.map`:

```plaintext
user password east_west east
```

Defines a user that uses the `east_west` service, but prefers being routed to the `east` service for reading from a slave.

Affinity can also specified within the connection string:

```java
jdbc://connector1:3306/database?affinity=host3&qos=RO_RELAXED
```

Additionally, affinity JDBC options can be set globally via the `tpm` command option `connector-affinity` [348].

Affinity can also be combined with other node selection, such as QoS. For example, by combining the affinity and `RO_RELAXED` [183], then the specified slave will be used first, if the load-balancer setting matches, then another slave within the same service, and finally the master. For example, in a dataservice with three nodes, where `node1` is the master:

```shell
mysql -h127.0.0.1 -P3306 databasename@qos=RO_RELAXED\&affinity=node2
```

Would use `node2` first, then `node3`, and finally `node1` if the others are not available.

```
Note
Within a composite dataservice, you cannot specify a specific host. You can only specify a physical dataservice within the composite dataservice. For example in a composite service with east and west physical dataservices:
```

```shell
mysql -h127.0.0.1 -P3306 databasename@qos=RO_RELAXED\&affinity=east
```
Additionally, the `user.map` can be configured to direct specific users to a slave by using the `@direct` keyword. For example, the following line in `user.map` will always direct the user to a slave, ignoring latency and load balancing settings:

```plaintext
@direct readme
```

### 6.4.6. Smartscale Routing

Smartscale allows you to read your data, as much as possible, from a slave data source.

In this read-write splitting mode, the connector intelligently determines if slaves are up-to-date with respect to the master, and selects them in such a way that read operations are always strictly consistent with the last write of their current session. Sessions are per-connector-instance, in-memory objects that allow different connections to share Smartscale benefits: by providing the same session id, two connections will be able to see each other's write operations consistently.

Possible session ids are:

- **DATABASE**: applications will see write operations made to the same database as it is connected to. Reads from other databases might be outdated depending on the slave latency
- **USER**: all connections that use the same user will read data consistent with the writes made by the current user. Other users data might be outdated.
- **CONNECTION**: only writes made by the current connection are guaranteed to be read consistently. Writes from other connections might be outdated
- **PROVIDED_IN_DBNAME**: Allows you to specify a variable sessionid in the database connection string. An application, typically PHP, can pass its own session id to make smart scale even more efficient.

Typical use cases:

- Applications which can use this level of consistency typically do relatively few writes and many reads. The writes that are performed can be considered to be in a ‘silo’ of their own, that is, a given application ‘session’ only writes and reads its own data and is not concerned with the data read/written by other application ‘sessions’.
- PHP applications are good candidates for Smartscale since PHP has embedded session IDs that can be passed at connection time.
- Web based applications with user profiles match the scenario where users will update their own profile and want to see their modifications right away, but can accept latency on other users profiles.

Comparison with Direct Reads

- Smart Scale allow session consistency, while Direct Reads always read from slave, no matter whether data is up-to-date.
- However, the cost for consistency appears at the performance level, since the Connector constantly needs to check slave progress.
- If your application needs to see the data it just wrote, use SmartScale
- If your application does a lot of small reads that do not need to be up-to-date, use Direct Reads

Limitations

- Prepared Statements - Prepared statements will need to be enclosed between transaction boundaries in order to work correctly with read/write splitting. This way, they will always execute on the master. Note that all prepared statements will become invalid upon switches or failover
- Ephemeral objects - Temporary tables, session variables and other objects that are connection specific will not be accessible when reading data using Smartscale. If you need to use these ephemeral object, you should either add a ‘for update’ statement in your selects or avoid using Smartscale
- Read/write functions - Functions that create or modify data in the database should never be called with a simple SELECT statement. Always add “for update” a the end of the select call. Example:

  ```sql
  SELECT my_function_that_writes('param') FOR UPDATE
  ```

### 6.4.6.1. Specifying the Session ID

While the three first keywords (DATABASE, USER and CONNECTION) are connector-wide (a single connector instance will use these session ids for all connections), it is possible to configure the connector to allow a free string session ID. This string will have to be passed through the database name as `{dbName}?sessionId={sessionID}`. For example, when using a database named "test" and a session ID number 1234, the database name passed to the connector will be:
With mysql command line utility, the connection command will look like:
```
mysql -h connectorHost -u user -ppass -P 3306 test?sessionId=1234
```

JDBC clients will have to pass this session ID with a special tag, as follows:
```
jdbc:mysql://connector_host:3306/dbname@test?sessionId=1234?otherJdbcDriverOption=value
```

In order to use this feature, the special session id PROVIDED_IN_DBNAME needs to be specified at installation time.

Also note that a session ID specified in the database name string will override the default provided in the connector configuration file. You can thus have a default session ID set for applications that can’t specify it dynamically, and still allow other applications to connect with their own session ID variable.

### 6.4.6.2. Enabling SmartScale Routing

To enable SmartScale routing, configure the dataservice using the `--connector-smartscale` option. The session ID identification should also be specified by using the `--connector-smartscale-sessionid` option with one of the following values DATABASE, USER, CONNECTION or PROVIDED_IN_DBNAME:
```
shell> tpm configure alpha \
  ... \
  --connector-smartscale=true \
  --connector-smartscale-sessionid={DATABASE|USER|CONNECTION|PROVIDED_IN_DBNAME}
```

In this mode, any client application can open a connection to the connector, and queries will automatically be redirected according to the SQL statement content.

In addition, all users that connect to the database must be granted the REPLICATION CLIENT privilege so that the user can compare the current replicator progress for session information. This can be granted using:
```
mysql> GRANT REPLICATION CLIENT ON *.* to app_user@'%'
```

### 6.4.6.3. Disabling SmartScale Routing

To disable SmartScale routing if it has been previously configured:
```
shell> tpm configure alpha --connector-smartscale=false
```

### 6.4.6.4. SmartScale Exploit

When using DATABASE session ID, you can bypass session consistency to read from available slaves by simply connecting to one database and reading from another. For example:
```
shell> mysql -u... -p... -P3306 db1
mysql> select * from db2.user
```

As long as no update is made on db1 in the meantime, the select will be executed on a slave (if available)

### 6.4.7. Direct Routing

<table>
<thead>
<tr>
<th>Auto Read/Write Splitting</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Selection</td>
<td>Automatically, by SQL examination</td>
</tr>
<tr>
<td>Slave Selection</td>
<td>Automatically, by SQL examination</td>
</tr>
<tr>
<td>QoS Compatibility</td>
<td>None</td>
</tr>
<tr>
<td>SmartScale Compatibility</td>
<td>None</td>
</tr>
</tbody>
</table>

Direct routing is a simplified form of SmartScale that uses a highly-efficient automated read/write splitting system, where of all auto-committed read-only transactions are routed to a pool of read-only slave datasources. Unlike SmartScale, Direct routing pays no attention to the session state, or replicated data consistency.

This means that performing a write and immediately trying to read the information through a Direct routing connection may fail, because the Connector does not ensure that the written transaction exists on the selected slave.

Direct routing is therefore ideal in applications where:
- Applications perform few writes, but a high number of reads.
• High proportion of reads on ‘old’ data. For example, blogs, stores, or machine logging information.

Where applications are performing writes, followed by immediate reads of this data, for example conferencing and discussion systems, where reading stale data that has recently been written would create significant application failures, the solution should use should use SmartScale.

Read/Write splitting is supported through examination of the submitted SQL statement:

• If the statement contains `SELECT` and does not contain `FOR UPDATE`, the query is routed to an available slave.

• If the statement starts `SHOW ...` then it is routed to a slave.

• All other queries are routed to the master.

6.4.7.1. Enabling Direct Routing

To enable direct routing for a specific user, the `user.map` must be modified. Update the file with the `@direct` directive on every host running a connector. The connector will automatically read the changes after the file is saved. For example:

```
@direct sales
```

In this mode, any client application can open a connection to the connector, and queries will automatically be redirected according to the SQL statement content.

6.4.7.2. Limitations of Direct Routing

• Prepared statements must be enclosed within an explicit transaction boundary in order to be correctly routed to a master. For example:

```
BEGIN
PREPARE ...
EXECUTE ...
COMMIT
```

• Ephemeral objects, including temporary tables, session variables and other objects that are session specific will not be accessible during direct routing.

• Stored procedures that update data in the database should never be called using a basic `SELECT` statement:

```
mysql> SELECT update_function('data');
```

Instead, add the `FOR UPDATE` keywords to ensure it is routed to the master:

```
mysql> SELECT update_function('data') FOR UPDATE;
```

6.4.8. SQL Routing

<table>
<thead>
<tr>
<th>Auto Read/Write Splitting</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Selection</td>
<td>Manually, by SQL comments</td>
</tr>
<tr>
<td>Slave Selection</td>
<td>Manually, by SQL comments</td>
</tr>
<tr>
<td>QoS Compatibility</td>
<td>Supported</td>
</tr>
<tr>
<td>SmartScale Compatibility</td>
<td>Yes</td>
</tr>
<tr>
<td>Direct Compatibility</td>
<td>Yes</td>
</tr>
</tbody>
</table>

With SQL-based routing, the redirection of queries and operations through the Connector is controlled by hints on the QoS provided in the comments of individual statements. Note that this is explicit routing using SQL comments, not the automated read/write splitting supported by Direct or SmartScale routing.

Unless otherwise specified, statements will go to the current master to be executed, or whatever slave is selected by the read-write splitting configuration, if enabled. To specify that a statement can be executed on the slave, place a comment before the statement:

```
/* TUNGSTEN USE qos=RO_RELAXED */ SELECT * FROM TABLENAME
```

This style of comment indicates to the connector that the specific query that follows should go to a slave. If unavailable, the query may still be executed on the master.

```
-- TUNGSTEN USE qos=RO_RELAXED
```

This style of comment indicates to the connector that all queries that follow should go to a slave. If unavailable, any query may still be executed on the master.
**Warning**

If you force the Connector to send traffic to a slave using qos=RO_RELAXED, then any write operations that follow will also go to the slave until you tell the Connector to go back to the master by indicating qos_RW_STRICT. The application is fully responsible for where the traffic is routed to. If care is not taken, the application could send writes to a slave this way which is unacceptable from a clustering perspective. All writes must go to the master or they will be lost to a non-authoritative node, and may corrupt the data badly.

The below forces all following queries to go to the master directly, effectively "turning off" reads from the slave.

```sql
-- TUNGSTEN USE qos=RW_STRICT
```

**Important**

Please note that employing the `--` style will override any `/* */` comments.

### 6.4.8.1. Enabling SQL Routing

To enable SQL routing, use the following operations with `tpm`:

```
shell> tpm configure alpha
   --property=selective.rwsplitting=true
```

### 6.4.8.2. Limitations of SQL Routing

- Read/write splitting must be handled entirely by the client application using the comments to specify which statements are slave safe. Unless applications explicit make the decision to write and read to the hosts using the comment system, operations may go to the wrong hosts.
- Prepared statements must be executed against the master.
- When testing the operation of the read/write splitting through the `mysql` client, ensure that command-line client is called using the `-c` option to ensure that comments are preserved:

```
shell> mysql -c -h host -u tungsten -ppassword -P3306 test
```

### 6.4.9. Host-based Routing

<table>
<thead>
<tr>
<th>Auto Read/Write Splitting</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Selection</td>
<td>Manually, by hostname/IP address</td>
</tr>
<tr>
<td>Slave Selection</td>
<td>Manually, by hostname/IP address</td>
</tr>
<tr>
<td>QoS Compatibility</td>
<td>None</td>
</tr>
<tr>
<td>SmartScale Compatibility</td>
<td>None</td>
</tr>
</tbody>
</table>

Host-based routing uses specific hostnames to provide the distinction between read and write availability within the connector. Two different hostnames and associated IP addresses need to be created on each connector host. Clients connecting to one host will be routed to the current master for writing, and connections to the other host will be redirected to a current slave using the current load-balancing algorithm.

Once enabled, a client can open a connection directly to a master or slave by connecting to the appropriate IP address or hostname. For example:

```
shell> mysql -h master.localhost
```

Will connect to the currently active master, while:

```
shell> mysql -h slave.localhost
```

Would connect to any currently available slave.

### 6.4.9.1. Enabling Host-based Routing

To enable host-based routing requires both operating system and Connector based configuration changes:

1. The following steps must be made to the operating system configuration for each Connector host that will be configured within the dataservice:
   a. Add a second IP address to the host. This can be achieved either by adding or exposing a second physical ethernet device, or by exposing an alias on an existing hardware interface.
For example, to add a second IP address to the physical `eth0` interface:

```bash
shell> sudo ifconfig eth0:1 192.168.2.24
```

To ensure this is retained during a restart, update your network configuration with the additional physical interface and IP address.

b. Update the `/etc/hosts` file to reflect both addresses and appropriate hostnames. For example:

```plaintext
192.168.2.20 host1 master.host1
192.168.2.21 slave.host1
```

c. When using DNS to resolve addresses, the DNS should also be updated with hostnames to match those configured for each IP interface.

2. Update the `user.map` file on every host running a connector to reflect the desired QoS for each hostname. The connector will automatically read the changes after the file is saved.

```plaintext
@hostoption master.host1 qos=RW_STRICT
@hostoption master.host2 qos=RW_STRICT
@hostoption master.host3 qos=RW_STRICT
@hostoption slave.host1 qos=RO_RELAXED
@hostoption slave.host2 qos=RO_RELAXED
@hostoption slave.host3 qos=RO_RELAXED
```

Once configured, client applications must be configured to select the appropriate host based on the operation they are performing.

**6.4.9.2. Limitations of Host-based Routing**

- Prepared statements must be executed on the master.
- Smartscale cannot be enabled at the same time as host-based routing.
- QoS selection will not be honored.

**6.4.10. Port-based Routing**

<table>
<thead>
<tr>
<th>Auto Read/Write Splitting</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Selection</td>
<td>Manually, by network port</td>
</tr>
<tr>
<td>Slave Selection</td>
<td>Manually, by network port</td>
</tr>
<tr>
<td>QoS Compatibility</td>
<td>None</td>
</tr>
<tr>
<td>SmartScale Compatibility</td>
<td>None</td>
</tr>
</tbody>
</table>

Port-based routing configures two independent ports that enable client applications to select whether to connect to a master or slave based on the port they connect to. This method relies on the application choosing the correct port, automatic r/w splitting is not supported. Similar to host-based routing, port-based routing requires the client application to be modified to manually select the appropriate port.

Once enabled, a client can open a connection directly to a master or slave by connecting to the appropriate port. For example:

```bash
shell> mysql -P3306
```

Will connect to the currently active master, while:

```bash
shell> mysql -P3307
```

will connect to a read-resource, ideally a slave, but will revert to the master if no appropriate slave is available.

**Note**

The ports to be used for each connection type are configurable during installation.

**6.4.10.1. Enabling Port-based Routing**

Enabling port-based routing requires configuring the two ports that will accept queries. One port will be designated as the master port, one the read-only port, and queries will be automatically routed accordingly. For example:

```bash
shell> tpm configure alpha \
... \
--connector-readonly-listen-port=3307 \
```
Tungsten Connector

```bash
--connector-listen-port=3306
```

Client applications must be updated to support the two port interfaces and manually direct their queries to the appropriate master or slave.

Using port routing in this way effectively marks all connections to the read-only port as behaving in a similar fashion to setting the connection QoS to `RO_RELAXED`.

### 6.4.11. Read-only Routing

It is possible to deploy a connector that has been configured to provide read-only access to the underlying databases on the standard port. This enforces read-only connectivity through this connector, regardless of any session or connector configuration options. This can be useful for a standalone connector, or a single connector within a dataservice.

This setting places the connector into RO_RELAXED mode. The connector will choose the master if there is no available slave. See Section 6.4.2, "Connector Quality of Service (QoS) Selection" for more detail on Quality of Service modes.

To enable this functionality, configure the connector using the `--connector-readonly` option:

```bash
shell> tpm configure alpha --connector-readonly=true
```

To enable this functionality on specific hosts only, add the `--hosts` option:

```bash
shell> tpm configure alpha --connector-readonly=true --hosts=host1,host3
```

### 6.5. Using Bridge Mode

Bridge mode eliminates the need to create or define users and passwords within the user.map file. Instead, the connector acts as a router connecting the network sockets between client application and MySQL servers.

![Figure 6.7. Tungsten Connector Bridge Mode Architecture](image)

Bridge mode provides a simpler method for connecting clients to MySQL, but with reduced facilities, as outline in the table below:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Proxy Mode</th>
<th>Bridge Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master/Slave Selection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Switch/Failover</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic Read/Write Splitting</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Application-based Read/Write Splitting</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Seamless Reconnects</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Data Source Selection</td>
<td>Current data source is checked to confirm latency and affinity</td>
<td>Pass-through</td>
</tr>
</tbody>
</table>

Bridge mode connections operate as follows:

1. Client opens network connection to Connector
2. Connector allocates a network buffer for the client network connection to the database server

3. Connector opens a network connection to a database server based on the connection parameters (master/slave selection)

4. Connector allocates a network buffer for the database server to the client application

5. Connector directly attaches the network sockets sockets together

Because the network sockets between the two sides are connected directly together, the following behavior applies to bridge mode connections:

- User authentication is handled directly by the database server, rather than through the user.map file.
- In the event of a failover or switch of the database servers, all active connections to the affected servers are closed.
- Smartscale and packet inspection to provide read/write splitting are not supported, since the Connector does not access individual packet data.

One key difference is in how slave latency checking is handled:

- In Bridge mode, the latency is checked at connection time, then you will stick to the slave for the connection lifetime (which can be shortened if the slave goes offline).
- In Proxy mode, the latency is re-evaluated before each transaction, which can bring the connection to another slave if the latency becomes too high during the life of the connection.

If you have long-lasting read-only connections that should not read from stale slaves, then use Proxy mode.

If your connection lifetime is short (i.e make/break - one transaction then disconnect), or your application is not sensitive to reasonably outdated data for reads, then use Bridge mode and its optional read-only port.

### 6.5.1. Enabling Bridge Mode

To enable Bridge Mode, the `--connector-bridge-mode` option to `tpm` must be set to `true`:

```
shell> tpm configure alpha --connector-bridge-mode=true
```

The default value is `false`, i.e. use the connector in non-bridge mode with full support for read/write splitting and operation.

Bridge Mode can also be used with read-only database servers and affinity if required.

In addition to enabling and disabling Bridge Mode, the size of the buffer can also be set by using the `bridgeServerToClientBufferSize` and `bridgeClientToServerBufferSize` parameters. This configures the size of the buffer used to hold packet data before the packet is forwarded.

The default size is 1024 bytes [1KB].

- The default size is 262144 bytes [256KB].

A buffer is opened in each direction for each connection made to the connector when operating in bridge mode.

The total memory allocated can be calculated using the formula:

```
(connections * (bridgeClientToServerBufferSize + bridgeServerToClientBufferSize)
```

For example, with the default settings, 20 simultaneous connections will require 40KB of RAM to service the buffers.

For example, with the default settings, 20 simultaneous connections will require 10MB of RAM to service the buffers. With the default connector heap size the Connector should be able to handle up to 500 simultaneous connections.

### 6.6. User Authentication

When configuring Tungsten Connector it is important to ensure that you have a `user.map` in place. The role of `user.map` is to define the usernames and passwords of users that will be connecting to the dataserver.

There is no authentication within the connector. Instead, the connector sends authentication information onto the dataserver. However, the MySQL network protocol exchanges a token between the client and the dataserver in order to authenticate the connection and is designed to prevent 'man in the middle' attacks.

Unfortunately, 'man in the middle' is exactly how Tungsten Connector operates, as the man in the middle to redirect queries to different dataservers as the list of active dataservers changes during the operation of a cluster. The authentication exchange cannot be reinitiated by
the dataserver and client, so the Tungsten Connector performs this authentication exchange on behalf of the client using the user and password information from a special file called `user.map`.

Figure 6.8. Tungsten Connector Authentication

![Diagram of client, Tungsten Connector, and dataserver authentication]

To get round this limitation, the connector operates as follows:

- Client opens a connection to the connector and authenticates.
- Connector connects to the datasource using the username supplied by the client, and the corresponding password stored within `user.map`.
- Database server returns the authentication token to the connector.
- Connector sends the same authentication token back to the client.

This process gives the client application the authentication token required to enable it to communicate with the dataserver and the same token to be used by the connector.

For this system to work, a file, `user.map`, must exist on every connector installation, and it must contain the information for all users that will connect to the datasources from each client. Without this information, connectors will be unable to login on behalf of the client applications.

**Important**

All the users that require access to your MySQL servers through the Tungsten Connector must have an entry in the `user.map`. Without this information, the Tungsten Connector has no way of providing an onward connection to a MySQL server.

The `user.map` file primary role is to operate as the source for authentication information within the connector. However, through the use of additional flags and keywords, the file can also define the routing methods used by different users when connecting to datasources, and different dataservices.

### 6.6.1. `user.map` File Format

The current `user.map` file is located within the `tungsten-connector/conf` directory within an active installation. The file should be synchronized across all the servers within a dataservice. For more information on methods for keeping the file in sync, see Section 6.6.7, “Synchronizing `user.map` Data”.

The `user.map` file contains the usernames and passwords for each user that connects to the connector and the downstream MySQL server, and these entries are required for authentication. If an entry does not exist within `user.map` users will be unable to connect to MySQL through the connector.

**Important**

All the users that require access to your MySQL servers through the Tungsten Connector must have an entry in the `user.map`. Without this information, the Tungsten Connector has no way of providing an onward connection to a MySQL server.

The rules for the format of the file are as follows:

- Anything after a `#` (hash) symbol are interpreted as comments and ignored. For example:

```plaintext
# This line is a comment
```

- The following character cannot be used as the username, password or dataservice values:

```plaintext
<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>@</td>
<td>at sign</td>
</tr>
<tr>
<td>=</td>
<td>equals</td>
</tr>
<tr>
<td>?</td>
<td>question mark</td>
</tr>
</tbody>
</table>
```

- If direct reads (using the `@direct` directive, the following characters should be avoided within passwords:

```plaintext
<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;</td>
<td>ampersand</td>
</tr>
<tr>
<td>0</td>
<td>zero</td>
</tr>
<tr>
<td>=</td>
<td>equals</td>
</tr>
<tr>
<td>?</td>
<td>question mark</td>
</tr>
</tbody>
</table>
```
- Using the -(hyphen) character as a password indicates that there is an empty or no password ["""] for the specified user.

The basic format for user entries within the user.map is:

```
username password servicename [affinity]
```

Where:

- **username** — the username to be used for authentication.
- **password** — the password to be used for authentication.
- **servicename** — the name of the dataservice or composite service to which this username/password apply.
- **affinity** — if the servicename is a composite service, the affinity identifies which service should be preferred for reads.

The affinity feature routes both reads and writes when using a Multimaster topology.

For example, to configure the user sales with the password secret to use MySQL servers within the alpha dataservice:

```
sales secret alpha
```

To configure a user that has no password:

```
sales - alpha
```

To configure a user within a composite service:

```
sales secret global
```

To configure a user within a composite service, preferring the east service for read-only connections:

```
sales secret global east
```

Composite Specification in 6.0.3

The deployment used in the examples below consists of a composite dataservice global, with four member dataservices [i.e. one cluster per site]: east, west, north and south.

For example, to exclude site south from servicing read requests:

```
sales secret global east,west,north,-south
```

The above affinity string "east,west,north,-south" will try east, then west, then north. If none of the first three are available, a connection request would not succeed since south has been excluded by the negation ["-"].

In the following example, dataservices north and south would be available as random candidates if the first two (east and west) were unavailable:

```
sales secret global east,west
```

### 6.6.2. user.map Direct Routing

To enable direct reads, as defined within Section 6.4.7, "Direct Routing", the entries for the user within user.map must be prefixed using the @direct. For example:

```
@direct sales
```

Note that the standard user, password and service must be defined:

```
sales secret alpha
@direct sales
```

For limitations of direct routing, see Section 6.4.7.2, "Limitations of Direct Routing".

### 6.6.3. user.map Host Options

The user.map provides a configuration point to enable the connector to support host options that enable you to define qualities of service against specific hosts, as configured according to the guidance within Section 6.4.9, "Host-based Routing".

When configuring the host options, the hostnames must have previously been defined and be resolvable.
The QoS within user.map has the following format:

```plaintext
@hostoption hostname QoS
```

For example, to enable \texttt{RW\_STRICT} [183] on one host and \texttt{RO\_RELAXED} [183] on the other:

```plaintext
@hostoption readwrite.master qos=RW\_STRICT
@hostoption readonly.master qos=RO\_RELAXED
```

### 6.6.4. user.map Updates

When the user.map file is updated:

- The Tungsten Connector should automatically identify that the file has been changed and reload the file, updating the user map.
- To manually force the users to be updated, for example, if the user.map uses the \texttt{@script} directive, use the \texttt{tungsten flush privileges} command:

```sql
mysql> tungsten flush privileges;
```

<table>
<thead>
<tr>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>user.map reloaded successfully</td>
</tr>
</tbody>
</table>

1 row in set (0.00 sec)

If you are using the \texttt{--application-readonly-port} [345] option, this command must be run through both ports. Alternatively, you can trigger a simultaneous flush by running:

```bash
touch /opt/continuent/tungsten/continuent-connector/conf/user.map
```

- When using \texttt{@direct} entries in user.map, the connector may need to be restarted using \texttt{connector restart}:

```bash
shell> connector restart
```

This will disconnect all connected clients, but the connector itself should be unavailable only for a short time.

- When the connector installation is updated using \texttt{tpm}, for example during an upgrade, the user.map and datasync.properties are automatically copied into the new installation automatically and do not need to be manually copied or update.

To perform an update without automatically copying the user.map file using the \texttt{--connector-delete-user-map} [349] option to \texttt{tpm}.

### 6.6.5. Generating user.map Entries from a Script

The content of the user.map file can be generated automatically, for example by automatically extracting information from a separate service, such as LDAP, NIS or others. To specify the script that will generate the information, the \texttt{@script} directive can be used within the user.map:

```plaintext
@script /opt/continuent/share/usermap
```

When using the script method:

- The information must be generated in the same format as for standard entries, i.e.:

```plaintext
username password servicename
```

- If the script generates multiple entries with the same name, the later output will overwrite the previous entry.
- Multiple \texttt{@script} directives can be specified. Each will be processed in turn.
- If a generated list of usernames changes due to the scripts, the connector must be manually forced to reload the usermap using \texttt{tungsten flush privileges} on a connector connection. If you are using the \texttt{--application-readonly-port} [345] option, this command must be run through both ports. Alternatively, you can trigger a simultaneous flush by running:

```bash
touch /opt/continuent/tungsten/continuent-connector/conf/user.map
```

- If the file is placed into \texttt{/opt/continuent/share} then the script will be retained during upgrades through \texttt{tpm update}.
- If a script within the \texttt{@script} fails to be executed correctly, or generates no user entries, the connector will fail to start.

The script itself can be relatively simple, the standard output of the command must contain the user entries to be included in user.map. Standard error is ignored.

For example:

```bash
#!/bin/bash
```
echo 'app_user password dsone'

This generates a simple user entry.

### 6.6.6. Encrypting user.map Data

The user.map file allows you to use an encrypted version of the file by using the `@script` directive. Here is an example of how you can decrypt a file and return the results to user.map.

1. Change to a directory outside of the currently installed Tungsten

   Do this to ensure that the OpenSSL key and encrypted file are available after upgrades and other operations.

   ```shell
   cd /opt/continuent/share
   ```

2. Create an OpenSSL key

   In this example we will use a 1024-bit RSA private key to do the encryption and decryption. There are many options for encrypting and decrypting files but this documentation will not explore those. The same process will work with other encryption techniques. You must ensure that the decryption command runs without user input.

   ```shell
   openssl genrsa -out usermap.pem 1024
   ```

3. Create the encrypted file of user.map entries:

   ```
   tungsten secret nyc_sjc sjc
   tungsten_sjc secret sjc
   tungsten_nyc secret nyc
   ```

   Create an encrypted version of the file:

   ```shell
   openssl rsautl -encrypt -inkey usermap.pem -in user.map.entries -out user.map.entries.ssl
   ```

4. Test decryption of the encrypted file:

   ```shell
   openssl rsautl -decrypt -inkey usermap.pem -in user.map.entries.ssl
   ```

   This should return the unencrypted user.map:

   ```
   tungsten secret nyc_sjc
   tungsten_sjc secret sjc
   tungsten_nyc secret nyc
   ```

5. Update the installed and configured tungsten-connector/conf/user.map file:

   ```
   ...
   # Examples:
   # user tungstenuser has password secret and uses 'sjc_nyc' composite data service, but prefers nyc site for reading:
   #  tungstenuser secret sjc_nyc nyc
   ```

   Now add a `@script` directive to point to the encrypted file and certificate:

   ```script
   @script openssl rsautl -decrypt -inkey /opt/continuent/share/usermap.pem -in /opt/continuent/share/user.map.entries.ssl
   ```

6. Repeat the process on each host. The user.map file will be copied to the new version when you upgrade Tungsten so this process must only be completed once per host.

### 6.6.7. Synchronizing user.map Data

Continuent Tungsten does not automatically synchronize information contained within the user.map across all the nodes within the cluster. The connector does not identify, track, or update user.map content when it sees password changes.

Instead, the file must be updated by hand, through the `@script` directive, and synchronized across multiple hosts either manually or by using a script. For example:

```bash
#!/bin/bash
for HOST in host1 host2 host3 host4
do
  rsync /opt/continuent/tungsten/tungsten-connector/conf/user.map \
  $HOST:/opt/continuent/tungsten/tungsten-connector/conf/user.map
done
```
If `@script` directives, the corresponding scripts must also be included within this synchronization step.

**Important**

All servers within the cluster must have an identical `user.map` configuration. Failure to have a synchronized configuration may lead to clients being unable to connect to the connector and database servers.

### 6.6.8. `user.map` Limitations

The `user.map` configuration has the following limitations:

- Users must be defined for each dataservice; if there is a common user that can be used in any of your configured dataservices, there must be an individual line for each dataservice. For example:

  ```
  sales secret alpha
  sales secret beta
  sales secret gamma
  ```

- When using `user.map` with multiple dataservices, additional data services must exist in `dataservices.properties`. Only add the physical data services you would like to work with. Any composite data services will automatically be discovered. The connector must be restarted once the data services have been added.

- Specifying a composite dataservice that has not been defined will raise an error.

- If the `user.map` contains multiple entries for the same user, only the last entry will be used.

### 6.6.9. Host-based Authentication

In addition to the explicit user/host based authentication support, the connector also includes general host-based authentication that allows client connections only from specific hosts.

Host-based authentication is not enabled in the default installation. To enable it, create a file `authorized_hosts` within the `tungsten/tungsten-connector/conf/` directory of the active installation. The connector will then need to be restarted before host-based authentication is enabled.

**Important**

The `authorized_hosts` file is not automatically distributed during deployment and updates. The file must be manually copied to other hosts.

If the content of the `authorized_hosts` file is changed, the connector must be restarted before the changes take effect.

If the file exists, host-based authentication is enabled. If it is empty, all client connections are denied. The format of the file is that each line defines the host address and netmask in CIDR format. For example:

```
192.168.1.0/24
```

Enables connectivity from all hosts in the range 192.168.1.0-192.168.1.255.

### 6.7. Connector Operational States

During operation, the connector goes through a number of different states and state transition during specific events. The default mode is the **Online** state, where the connector operates as configured.

During operation, all configured connectors within the dataservice remain in contact with the manager, see Section 6.8, “Connector/Manager Interface” for more information.

Supported states by the Connector are:

- **Online** State
  
  The Connector operates as configured, redirecting connections to the corresponding master or slave.

- **On Hold** State
  
  In this state, the connector will continue as normal allowing existing connections to continue until the `delayBeforeOfflineIfNoManager` is reached. New connections are paused.

- **Offline** State
  
  When the connector enters the offline state, the connector terminates all connections, and blocks all new connections.
The state of a connector can be modified by using the `router` command within `cctrl`. This can be used to manually place the connector into online or offline states. For example, to put a connector online the full host and process ID must be used:

```
cctrl> router connector@host1[22476] online
```

Wildcards can be used to enable or disable all the hosts. For example, to place all connectors online:

```
cctrl> router * online
```

While in `AUTOMATIC` policy mode, connectors will automatically be placed online if they have entered the `OFFLINE` state automatically as part of a failover. If the routers have been manually placed offline, routers must be manually placed back online.

While in the `ONLINE` state, the connector behaves and alters its operation according to the following states and events:

### 6.7.1. Connections During Automatic Failure/Failover

When an automatic failure or failover is identified, for example when the dataservice is in the `AUTOMATIC` policy mode, and the master is automatically switched to a new host, the following sequence occurs:

1. All connections to the failed datasource are terminated immediately. This ensures that running transactions or operations are terminated by the database server.
2. Connections to clients will remain open and be reconnected transparently, providing they are not within a transaction. For more information, see Section 6.7.3, “Connections During Connection Failures”.

   Only if there is a problem with the connection or an I/O error will the problem be forwarded to the clients.

As with a direct database connection, the client application should handle the reconnection to the Connector, which will then be redirected to the corresponding master or slave datasource.

### 6.7.2. Connections During Manual Switch

When a manual `switch` operation has been initiated, the Connector follows this sequence:

1. New connection attempts to the old datasource are suspended; this gives the impression of a 'hung' connection that must be managed by the client application through the normal timeout procedure.
2. Existing connections to the datasource are terminated under two conditions:
   - As the connections are naturally closed.
   - Open connections are forcibly disconnected after the timeout specified by the `waitForDisconnectTimeout` parameter. By default, this is 5 seconds. To eliminate waiting, the `waitForDisconnect` parameter can be set to `false`.

   Once either condition has been met, any remaining connections are closed.
3. New connections (including re-connections) are enabled, and will be routed to the appropriate master or slave.

Client applications should be configured to reconnect to the connector with an interval larger than the disconnect timeout within the connector. This will ensure that the client reconnects when the connector is able to accept the new connection.

### 6.7.3. Connections During Connection Failures

In the event of a connection failure between a running datasource and the connector, and providing the connection is deemed idle, the connector will transparently reconnect to the failed datasource when the following conditions have been met:

- The connection is not executing any requests.
- The connection is not in the middle of a transaction.
- No temporary tables have been created during this connection.

If all three conditions are met, a new connection will be opened. Connections between the client and the connector will be unaffected.

This option is enabled by default. To disable transparent reconnections, use `--connector-autoreconnect=false` option to `tpm` during installation.

### 6.7.4. Other Errors

The Connector attempts to emulate and effectively represent any errors raised by the datasource to which the connector has routed the client connection.
The Tungsten Connector uses the Tanuki Java Service Wrapper to manage the running process. If the Connector process fails, the service wrapper will automatically restart it. If the connector fails repeatedly, attempts to restart will be stopped. The status and reason for these failures can be tracked by examining the `connector.log` log file.

Connected client applications will be terminated, but should be able to reconnect once the Connector has been restarted.

Database errors, including invalid statements, operations, or security failures, will be represented identically by the Connector to any clients.

### 6.7.5. Connector Keepalive

Connections to MySQL servers can automatically time-out according to the `wait_timeout` variable configured within the MySQL server.

To prevent these connections being automatically closed, the connector can be configured to keep the connection alive by submitting a simple `SELECT` statement (actually `SELECT 'KEEP_ALIVE'`) periodically to ensure that the MySQL timeout is not reached and the connection closed.

Two parameters configure the keepalive functionality:

- `connection.keepAlive.interval`
  
  The interval used to check for idle connections. If set to a value of 0, the keep alive check is disabled. Any value greater than zero is the interval check period in seconds.

- `connection.keepAlive.timeout`
  
  The keep-alive statement is submitted if the time since the last activity reaches this timeout value.

The default setting for both parameters is 0 (disabled).

When set to `autodetect` default, the values are automatically calculated by the connector computing suitable values based on the `wait_timeout` value configured in the MySQL server.

```plaintext
connection.keepAlive.interval = (int) Math.floor(wait_timeout * 0.10);
connection.keepAlive.timeout = (int) Math.floor(wait_timeout * 0.7);
```

These calculations cannot be modified, but the properties can be explicitly set by using the `--property` to explicitly set the property through `tpm`, for example:

```
shell> tpm update alpha --property=connection.keepAlive.interval=30
```

### 6.8. Connector/Manager Interface

The connector remains in constant communication with the Tungsten Manager during operation. This enables the connector to respond to failures and errors, whether automatically identified, or manually triggered. For example, when a manual `switch` operation occurs, the manager communicates this information to all of the connectors. Each connector then responses according to the rules outline in Section 6.7, “Connector Operational States”.

Communication between managers and the connectors is handled on ports 11999 (managed by `--router-gateway-port`) and 12000 (managed by `--mgr-rmi-remote-port`). The connection is used to exchange cluster status and individual datasource availability as identified by the manager so that decisions about active connections can be effectively made by the connector.

In the event that the connection between the connector and the manager is broken, the connector enters a failsafe mode called `on Hold`. In this state, connections to and from the connector and datasources will continue as normal until a timeout, configured by the `delayBeforeOfflineIfNoManager` property, is reached. By default, this timeout is 600 seconds (10 minutes). Once the timeout has been reached, the connector reaches the `Offline` state.

All of the information about the dataservice, including the other nodes, topology and individual node states and roles are entirely determined by the Connector by requesting this information from the Manager. No on-disk record or description is stored or stored, created, or read by the Connector. When the Connector is first started, it connects to a manager and requests the full cluster configuration.

If the Connector cannot communicate with a manager, the connector remains in the `offline` state until a manager can be reached.
6.9. Connector Command-Line Interface

The `connector` command is used for various operations that affect the Tungsten Connector, for example, starting and stopping the Tungsten Connector, getting status, updating and debugging.

When using the `connector` command-line tool, the following sub-commands are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-list [235]</td>
<td>Return a list of the current client connections through this connector.</td>
</tr>
<tr>
<td>condrestart [235]</td>
<td>Restart only if already running</td>
</tr>
<tr>
<td>console [235]</td>
<td>Launch in the current console [instead of a daemon]</td>
</tr>
<tr>
<td>dump [235]</td>
<td>Request a Java thread dump [if connector is running]</td>
</tr>
<tr>
<td>graceful-stop [seconds] [235]</td>
<td>Stops the connector gracefully, allowing outstanding open connections to finish and close before the connector process is stopped. {seconds} is an integer of zero or more, and is required. The connector will shut down immediately if there are no active connections. Specifying zero (0) will cause a shutdown without waiting for connections to terminate.</td>
</tr>
<tr>
<td>install [236]</td>
<td>Install the service to automatically start when the system boots</td>
</tr>
<tr>
<td>reconfigure [236]</td>
<td>Reconfigure the connector by forcing the connector to reread the configuration, including the configuration files and user.map.</td>
</tr>
<tr>
<td>remove [236]</td>
<td>Remove the service from starting during boot</td>
</tr>
<tr>
<td>restart [236]</td>
<td>Stop connector if already running and then start</td>
</tr>
<tr>
<td>start [236]</td>
<td>Start in the background as a daemon process</td>
</tr>
<tr>
<td>status [236]</td>
<td>Query the current status</td>
</tr>
<tr>
<td>stop [236]</td>
<td>Stop if running [whether as a daemon or in another console]</td>
</tr>
</tbody>
</table>

For more information, please see Section 8.7, "The connector Command".

6.10. Connector Inline Command Interface

When connected to a service through Tungsten Connector, the connection has access to a number of specialized commands that can be executed.

**Important**

When using Bridge Mode, these commands will not be available because you are connected directly to the database server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tungsten cluster status</td>
<td>Displays a detailed view of the information the connector has about the cluster</td>
</tr>
<tr>
<td>tungsten connection count</td>
<td>Display the current number of active connection to each datasource</td>
</tr>
<tr>
<td>tungsten connection status</td>
<td>Displays information about the connection status for the last statement executed</td>
</tr>
<tr>
<td>tungsten flush privileges</td>
<td>Reload the user.map file and update the user credentials</td>
</tr>
<tr>
<td>tungsten gc</td>
<td>Executes the connector garbage collector to free memory</td>
</tr>
<tr>
<td>tungsten help</td>
<td>Shows help description each statement</td>
</tr>
<tr>
<td>tungsten mem info</td>
<td>Display the memory usage information for the connector</td>
</tr>
<tr>
<td>tungsten show processlist</td>
<td>List all active queries on this connector instance</td>
</tr>
<tr>
<td>tungsten show variables</td>
<td>Display the connector configuration options currently in use</td>
</tr>
</tbody>
</table>
6.10.1. Connector tungsten cluster status Command

Shows the current cluster status, as far as the connector is aware. The output consists of a table showing dataservices and hosts and current status and role information:

```
mysql> tungsten cluster status;
+-----------------+-------+-------+--------+---------+----------------+-----------------------+-------------------------+
| dataServiceName | name  | host  | role   | state   | appliedLatency | activeConnectionCount | connectionsCreatedCount |
|-----------------+-------+-------+--------+---------+----------------+-----------------------+-------------------------+
| alpha           | host1 | host1 | slave  | SHUNNED | 60.0           | 0                     | 0                       |
| alpha           | host2 | host2 | master | ONLINE  | 0.0            | 1                     | 2                       |
| alpha           | host3 | host3 | slave  | SHUNNED | 61.0           | 0                     | 0                       |
+-----------------+-------+-------+--------+---------+----------------+-----------------------+-------------------------+
3 rows in set (0.01 sec)
```

The output fields are as follows:

- **dataServiceName**
  The name of the service. In connectors configured with multiple services, including composite clusters, there will be an entry for each host/servicename combination.

- **name**
  The name of the host within the service.

- **host**
  The hostname on which the service is running.

- **role**
  The current role for the host.

- **state**
  The current state for the host within the service.

- **appliedLatency**
  The applied latency of transactions; for masters the difference between the commit time and extraction, in a slave, the difference between commit time in the master and commit time in the slave.

- **activeConnectionCount**
  Count of the current number of active connections.

- **connectionsCreatedCount**
  Count of the number of connections created since the connector has been started.

6.10.2. Connector tungsten connection count Command

Displays the current list of open connections for all hosts within the cluster.

```
mysql> tungsten connection count;
+--------------+-------------+----------------------------------------------------------------------+
| Data service | Data source | Active Connections                                                   |
|--------------+-------------+----------------------------------------------------------------------+
| alpha        | ct-multi1   | [internal(OPEN) DIRECT TO ct-multi1@alpha(master:ONLINE) STATUS(OK)] |
| alpha        | ct-multi2   | []                                                                    |
| alpha        | ct-multi3   | []                                                                    |
+--------------+-------------+----------------------------------------------------------------------+
3 rows in set (0.00 sec)
```

6.10.3. Connector tungsten connection status Command

Displays the current connection status, for all connections, including indicating whether the connection is using SSL on either the incoming (client) or outgoing (MySQL) connection:

```
mysql> tungsten connection status;
+-------------------------------------------------------------------------------------+
| Message                                                                             |
| 201                                                                                 |
```

---

201
### 6.10.4. Connector tungsten flush privileges Command

Forces a reload of the `user.map` file to update the user privileges configured within the file. Only forces an update of the connector to which the client is connected.

```sql
mysql> tungsten flush privileges;
+--------------------------------+
| Message                        |
| user.map reloaded successfully |
+--------------------------------+
```

### 6.10.5. Connector tungsten gc Command

Forces a Java garbage collection for the connector, recovering memory. An example of the memory used, garbage collection, and resulting memory usage below.

```sql
mysql> tungsten gc;
+-------------------------------+
| Message                       |
| Garbage collection successful |
+-------------------------------+
```

### 6.10.6. Connector tungsten help Command

Displays the list of currently supported commands within the connector inline interface:

```sql
mysql> tungsten help;
+---------------------------------------------------------------------------+
| Message                                                                   |
+---------------------------------------------------------------------------+
| tungsten connection status: display information about the                 |
| connection used for the last request ran                                 |
| tungsten connection count: gives the count of current connections to      |
| each one of the cluster datasources                                     |
| tungsten cluster status: prints detailed information about the cluster   |
| view this connector has                                                 |
| tungsten show [full] processlist: list all running queries handled by    |
| this connector instance                                                 |
| tungsten show variables [like 'string']: list connector configuration    |
| options in use. The 'string'                                           |
+---------------------------------------------------------------------------+
```
6.10.7. Connector tungsten mem info Command

```
mysql> tungsten mem info);
```

```
+-----------------------+-------------------------------------------------------+
| JVM Memory statistics | Value in bytes                                        |
| Peak Thread Count     | 18                                                    |
| Heap Memory           | init = 67108864(65536K) used = 13469328(13153K)       |
|                       | committed = 64966176(63424K) max = 259522560(253440K) |
| Non-heap Memory       | init = 24313856(23744K) used = 14227336(13893K)       |
|                       | committed = 24313856(23744K) max = 224395264(219136K) |
| Thread Count          | 18                                                    |
+-----------------------+-------------------------------------------------------+
```

4 rows in set (0.05 sec)

6.10.8. Connector tungsten show [full] processlist Command

```
mysql> tungsten show processlist;
```

```
+------------+--------+----------+---------------+----------------+---------+------+-------+------+
| DataSource | Id     | User     | Host          | db             | Command | Time | State | Info |
|------------+--------+----------+---------------+----------------+---------+------+-------+------+
| host1      | 218886 | tungsten | client1:57739 | tungsten_alpha  | Sleep   |  316 |       | NULL |
| host1      | 218925 | tungsten | client2:58552 | tungsten_alpha  | Sleep   |  281 |       | NULL |
| host1      | 218932 | tungsten | client1:57765 | tungsten_alpha  | Sleep   |  274 |       | NULL |
+------------+--------+----------+---------------+----------------+---------+------+-------+------+
```

3 rows in set (0.05 sec)

6.10.9. Connector show slave status Command

The `show slave status` command generates a version of the standard MySQL command, with the output replaced with values generated by Tungsten. This can be useful for environments where the slave status need to be checked, but with the Tungsten Replicator state, rather than native replication.

```
mysql> show slave status;
*************************** 1. row ***************************
Slave_IO_State: Master_Host: host1
Master_User: Master_Port: 0
Connect_IO: 0
Master_log_file: mysql-bin.mysql-bin.000050
Read_Master_Log_Pos: 0
Relay_Log_File: Relay_Log_Pos: 0
Relay_Master_Log_File:
Slave_IO_Running: Slave_SQL_Running: Replicate_Do_DB:
Replicate_Ignore_DB:
Replicate_Do_Table:
Replicate_Ignore_Table:
Replicate_Wild_Do_Table:
Replicate_Wild_Ignore_Table:
Last_Errno: 0
Last_Error: Skip_Counter: 0
Exec_Master_Log_Pos: 1269
Relay_Log_Space: 0
Until_Condition:
Until_Log_File: Until_Log_Pos: 0
Master_SSL_Allowed: Master_SSL_CA_File: Master_SSL_CA_Path:
Master_SSL_Cert: Master_SSL_Cipher:
Master_SSL_Cert: Master_SSL_Verify_Server_Cert: 203
```

203
6.10.10. Connector tungsten show variables Command

The connector will intercept the command `tungsten show variables;` and display its current (loaded) configuration. The `variable_Type` column indicates the file where the configuration item is stored.

**Important**

- This command applies only to proxy mode (i.e., not bridge mode).

Just as in the MySQL `show variables` command, Tungsten Connector supports filters through the `"like string"` and its wildcard `"%"` sign.

```sql
mysql> tungsten show variables like '%timeout%';
+----------------------+----------------------------------------+----------+
<table>
<thead>
<tr>
<th>Variable_Type</th>
<th>Variable_name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>connector.properties</td>
<td>bridgeServerToClientForcedCloseTimeout</td>
<td>50</td>
</tr>
<tr>
<td>connector.properties</td>
<td>connection.close.idle.timeout</td>
<td>28800000</td>
</tr>
<tr>
<td>connector.properties</td>
<td>connection.keepAlive.timeout</td>
<td>20160</td>
</tr>
<tr>
<td>connector.properties</td>
<td>server.port.binding.timeout</td>
<td>60</td>
</tr>
<tr>
<td>router.properties</td>
<td>gatewayConnectTimeoutMs</td>
<td>5000</td>
</tr>
<tr>
<td>router.properties</td>
<td>keepAliveTimeout</td>
<td>30000</td>
</tr>
<tr>
<td>router.properties</td>
<td>readCommandRetryTimeoutMs</td>
<td>10000</td>
</tr>
<tr>
<td>router.properties</td>
<td>waitForDisconnectTimeout</td>
<td>5</td>
</tr>
<tr>
<td>router.properties</td>
<td>waitIfDisabledTimeout</td>
<td>0</td>
</tr>
<tr>
<td>router.properties</td>
<td>waitIfUnavailableTimeout</td>
<td>0</td>
</tr>
</tbody>
</table>
+-----------------------+----------------------------------------+----------+
18 rows in set (0.01 sec)
```

6.11. Advanced Configuration

6.11.1. Using MultipleDataservices

The connector is able to work with multiple dataservices. It may be a combination of master/slave or composite dataservices. The connector will communicate with managers in each dataservice and provide connectivity.

1. Configure the host as a connector for one of the dataservices. This will be the default dataservice for the connector. Any version upgrades for this cluster will also upgrade the connector. See Section 3.4, “Deploying Tungsten Connector Only” if you want the host to be fully independent.

2. Update the `dataservices.properties` file in `/opt/continuent/tungsten/cluster-home/conf`. Add a line for each new master/slave cluster the connector will connect to. Keep this file updated as you add and remove servers from each cluster.

**Important**

- Do not list composite dataservices in this file. The connector will automatically discover those from the managers in each cluster.

3. Restart the connector. Any users connected to this connector will be disconnected at this time.

```
shell> connector restart
```

4. Update the `user.map` to list new users for each new dataservice. See Section 6.6, “User Authentication” for more details. Specifically, the `user.map` may not include multiple users with the same name but different dataservices. Create unique users in each dataservice before updating `user.map`.

See Section 6.6.1, “user.map File Format” for more details.

When a site goes offline, connections to this site will be forced closed. Those connections will reconnect, as long as the site stays offline, they will be connected to remote site.

You can now enable an option so that when the site comes back online, the connector will disconnect all these connections that couldn’t get to their preferred site so that they will then reconnect to the expected site with the appropriate affinity.

Note that this only applies to bridge mode. In proxy mode, relevancy of connected data source will be re-evaluated before every transaction.
When not enabled, connections will continue to use the server originally configured until they disconnect through normal attribution. This is the default option.

To enable forced reconnection, use the `--connector-reset-when-affinity-back=true` option to `tpm`.

The connector is now ready to accept users for each of the new dataservices. Keep the `dataservices.properties` and `user.map` files updated to make sure the connector works properly.

### 6.11.2. Connector Automatic Reconnect

Automatic reconnect enables the Connector to re-establish a connection in the event of a transient failure. Under specific circumstances, the Connector will also retry the query.

1. Connector automatic reconnect is enabled by default in Proxy and Smartscale modes. Use the `tpm` command option `--connector-autoreconnect=false` to disable automatic reconnect.

2. This feature is not available while running in Bridge Mode. Use the `tpm` command option `--connector-bridge-mode=false` to disable Bridge mode.

3. Automatic reconnect enables retries of statements under the following circumstances:
   - not in bridge mode
   - not inside a transaction
   - no temp table has been created
   - no lock acquired and not released
   - the request is a read

To disable:

```bash
shell> tpm update alpha --connector-autoreconnect=false
```

The autoreconnect status can be monitored within the `autoReconnect` parameter output by the `tungsten show variables` while connected to the Connector. For example:

```bash
shell> tpm connector mysql> tungsten show variables like "autoReconnect";
```

<table>
<thead>
<tr>
<th>Variable_Type</th>
<th>Variable_name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>connector.properties</td>
<td>autoReconnect</td>
<td>false</td>
</tr>
</tbody>
</table>

1 row in set (0.00 sec)

The above output indicates that the autoreconnect feature is disabled. The `tungsten show` command is not available in Bridge mode.

### 6.11.3. Using the Connector with HA Proxy

Tungsten Connector can be used in combination with an HA Proxy installation to provide a high-availability connection to the underlying connectors that then provide an intelligent connection to the datasources within the cluster.

There are two primary ways to monitor MySQL health via HAProxy:

- **mysql-check** - an haproxy-native test
  
  The check consists of sending two MySQL packets, one Client Authentication packet, and one QUIT packet, to correctly close the MySQL session. HAProxy then parses the MySQL Handshake Initialisation packet and/or Error packet. It is a basic but useful test which does not produce errors or aborted connects on the server. This solution requires adding a user to MySQL:

  ```sql
  INSERT INTO mysql.user (Host,User) values ('{ip_of_haproxy}', '{username}');
  ```

  **Warning**

  This method does NOT check for database presence nor database consistency. To do this, we must use an external check script (via xinetd) which is explained in the next section.

- **A check script** - normally launched via xinetd, and allows for custom monitoring of the database health. This is the preferred method.
6.11.3.1. Configuring HA Proxy using the native MySQL Check

A practical example for deploying the HAProxy's native mysql-check option:

```sql
INSERT INTO mysql.user (Host,User) values ('%','haproxy');
FLUSH PRIVILEGES;
```

```plaintext
# backend
#--------------------------------------------------------------
listen connector
bind *:3306
node tcp
option tcpka   # enables keep-alive both on client and server side
balance roundrobin
option mysql-check user haproxy post-41
server conn1 db4:13306 check inter 5s rise 1 fall 1 weight 3 maxconn 5000
server conn2 db5:13306 check inter 5s rise 1 fall 1 weight 3 maxconn 5000
```

6.11.3.2. Configuring HA Proxy with a Check Script

A suitable MySQL check script configuration can be added to a basic HA Proxy installation using the following settings:

```plaintext
# backend
#--------------------------------------------------------------
listen connector
bind *:3306
node tcp
option tcpka   # enables keep-alive both on client and server side
balance roundrobin
default-server port 9200
server conn1 db4:13306 check inter 5s rise 1 fall 1 weight 3 maxconn 5000
server conn2 db5:13306 check inter 5s rise 1 fall 1 weight 3 maxconn 5000
```

The hostname and port numbers should be modified to match your cluster configuration.

This solution will work for CONNECTION-based session IDs.

For correct operation within HAProxy, a check script needs to be installed on all hosts running Tungsten Connector that will respond to A HAProxy connector check script needs to be installed on all of the hosts running connectors and a xinet listener setup.

The connector check script will listen on port 9200 for connections from HAProxy and will return the status of the connector to HAProxy in the format of HTTP return codes.

To install the check script:

1. For the check to work, a mysql user must be created within the cluster which the check script can use. The user needs the permissions to be able to run the SQL in the check script:

   ```bash
   mysql> grant usage on *.* to haproxy identified by 'secret';
   
   If you are running smartscale the user will also need replication client privilege:
   
   mysql> grant usage, replication client on *.* to haproxy identified by 'secret';
   ```

2. Add the new user on each connector host by adding the following line to `user.map`:

   ```bash
   haproxy secret cluster_name
   ```

3. Create and configure a check script on each host running Tungsten Connector. For example, create the file `/opt/continuent/share/connec-tor-check.sh`:

   ```bash
   #!/bin/sh
   # This script checks if a mysql server is healthy running on localhost. It will
   # return:
   # "HTTP/1.x 200 OK\r\n" (if mysql is running smoothly)
   # "OK"
   # "HTTP/1.x 503 Service Unavailable\r\n" (else)
   # The purpose of this script is make haproxy capable of monitoring mysql properly
   ```
Tungsten Connector

MYSQL_HOST=`hostname` #Connector Port
MYSQL_PORT="3306"            #Connector Port
MYSQL_USERNAME="haproxy"
MYSQL_PASSWORD="secret"
MYSQL_OPTS="-N -q -A test"

#If you create the following file, the proxy will return mysql down
#Routing traffic to another host
FORCE_FAIL="/dev/shm/proxyoff"
OUT=""
return_ok() {
  echo -e "HTTP/1.1 200 OK\r\n"
  echo -e "Content-Type: Content-Type: text/plain\r\n"
  echo -e "\r\n"
  echo -e "MySQL is running.\r\n"
  echo -e "\r\n"
  exit 0
}
return_fail() {
  echo -e "HTTP/1.1 503 Service Unavailable\r\n"
  echo -e "Content-Type: Content-Type: text/plain\r\n"
  echo -e "\r\n"
  echo -e "$OUT\r\n"
  exit 1
}
if [ -f "$FORCE_FAIL" ]; then
  OUT="$FORCE.FAIL found"
  return_fail;
fi
OUT=`mysql $MYSQL_OPTS --host=$MYSQL_HOST --port=$MYSQL_PORT --user=$MYSQL_USERNAME --password=$MYSQL_PASSWORD -e "select @@hostname;" 2>&1`
if [ $? -ne 0 ]; then
  return_fail;
fi
return_ok;

Set the permissions for the check script:

shell> chown tungsten.tungsten /opt/continuent/share/connectorchk.sh
shell> chmod 700 /opt/continuent/share/connectorchk.sh
shell> chmod +x /opt/continuent/share/connectorchk.sh

4. Install xinetd and add the xinetd service. On RedHat/CentOS:

shell> yum -y install  xinetd telnet

On Debian/Ubuntu:

shell> apt-get install xinetd telnet

5. Add an entry for the connector check script to /etc/services:

shell> echo "connectorchk         9200/tcp" >> /etc/services

6. Add a configuration to xinetd by creating the file /etc/xinetd.d/connectorchk with the following content:

# default: on
# description:connectorchk
service connectorchk {
  flags = REUSE
  socket_type = stream
  port = 9200
  wait = no
  user = tungsten
  server = /opt/continuent/share/connectorchk.sh
  log_on_failure = USERID
default = no
  # only_from = 0.0.0.0/0
  # recommended to put the IPs that need
to connect exclusively (security purposes)
  per_source = UNLIMITED
}

7. Now restart xinetd:

shell> service xinetd restart
8. Check the service is running:

```
shell> telnet localhost 9200
```

You should get a response similar to this:

```
HTTP/1.1 200 OK
Content-Type: text/plain
MySQL is running.
```

### 6.11.4. Using Fall-Back Bridge Mode

This feature will allow the Tungsten Connector to fall back to bridge mode if a user cannot be successfully authenticated through `user.map`.

The connector is able to employ a special fall-back bridge mode which allows for a hybrid configuration of both Proxy and Bridge modes. By default, the bridge mode fallback feature is disabled.

When `fallBackBridgeMode` is set to either RW_STRICT or RO_RELAXED, the Connector will first check the `user.map` file for an entry that matches the user name passed in the connection request. If a match is found in the `user.map`, the Connector will act in Proxy mode so the conversation with the client will be handled locally, and a new connection will be opened from the connector to the database server based on the normal Proxy mode routing rules. If the user name is not found in `user.map`, then the connector will act in Bridge mode, and the connection will be forwarded directly to the specified database server, either to the master (RW_STRICT) or to the slave (RO_RELAXED) for handling with no intercept, just a TCP-layer packet routing. There will be no query interpretation or analysis, and no auto-reconnect, just failover handling.

For more information, see Section 6.5, "Using Bridge Mode", and Section 6.6, "User Authentication".

To enable Fall-Back Bridge Mode using the DB Master:

```
shell> ./tools/tpm configure alpha --property=fallBackBridgeMode=RW_STRICT --connector-bridge-mode=false
shell> ./tools/tpm update
```

To enable Fall-Back Bridge Mode using a DB Slave (if available):

```
shell> ./tools/tpm configure alpha --property=fallBackBridgeMode=RO_RELAXED --connector-bridge-mode=false
shell> ./tools/tpm update
```

**Warning**

Updating these values require a connector restart (via tpm update) for the changes to be recognized.

**Important**

To be consistent, Bridge mode should be disabled when `fallBackBridgeMode` is enabled. The `--connector-bridge-mode` option to tpm must be set to `false`. A consistency check is performed when starting the connector.

### 6.11.4.1. Using Fall-Back SSL To Bridge Mode

SSL connections are by design unreadable until the handshake has been exchanged. Because of this, the MySQL user name in the request is not visible to the Connector immediately, and therefore the Connector is unable to check against `user.map` for `fallBackBridgeMode`.

Due to this situation, another feature was created to address SSL connections while the `fallBackBridgeMode` is enabled called `fallBackSSLToBridge`. When `fallBackSSLToBridge` is set to `true` (default), then all SSL connections will use Bridge mode, while non-SSL connections will use the `fallBackBridgeMode` setting (i.e. RW_STRICT which routes traffic to the Master or RO_RELAXED which routes to the slaves). When `fallBackSSLToBridge` is set to `false`, then SSL connections will run in non-Bridge mode - if the specified user doesn't exist in `user.map`, an error will be raised.

**Important**

The `fallBackSSLToBridge` setting is ONLY available when `fallBackBridgeMode` is enabled, and is ignored when `fallBackBridgeMode` is set to `false`.

Since `fallBackSSLToBridge` is enabled by default when `fallBackBridgeMode` is enabled, you may turn it off as follows:

```
shell> ./tools/tpm configure alpha --property=fallBackSSLToBridge=false
shell> ./tools/tpm update
```

**Warning**

Updating these values require a connector restart (via tpm update) for the changes to be recognized.
6.11.5. Using the Max Connections Feature

This feature will allow the connector behavior to be changed based on the connection count. The connector is able to mimic MySQL's `max_connections`. Depending on your needs, the connector can be configured to pile up or reject connections above this number. This is served by the following two `tpm` flags:

- `--connector-max-connections [349]` - defines the maximum number of connections the connector should allow at any time.

When the `connector-max-connections [349]` is set to a non-zero numeric value, the connector denies access to the client in one of two ways: queue (default) or reject.

- `--connector-drop-after-max-connections [349]` - defines how the connector should handle new connection requests - queue (default) or reject.

Enabling this option causes the connector to drop new connection requests when `connector-max-connections [349]` is reached by immediately sending a "Too Many Connections" error to the client, just like MySQL would.

**Important**

When a client connection request arrives at the connector, an object is created to track that client connection which uses a certain amount of memory.

The connector then checks the value of `connector-max-connections [349]` against the current connection count.

If the connection limit has been reached, the connector decides how to behave by checking the value of `connector-drop-after-max-connections [349]`.

If `connector-drop-after-max-connections [349]` is false (the default), the connector will queue the connection request, but send nothing back to the client at all. This connection check will repeat after a delay. Once the connection count falls below `connector-max-connections [349]` an attempt to connect to a server is made. In this mode, connections will continue to pile up in memory as new requests are queued, resulting in an Out of Memory error. For this reason, the `connector-drop-after-max-connections [349]` is available to prevent connection queueing when the maximum number of connections has been reached.

If `connector-drop-after-max-connections [349]` is enabled, the connector will return a "Too Many Connections" error to the client and remove the client connection object, freeing memory.

To enable `connector-max-connections [349]`:

```shell
./tools/tpm configure alpha --connector-max-connections=2500
./tools/tpm update
```

To enable `connector-drop-after-max-connections [349]` you must also set a non-zero value for `connector-max-connections [349]`:

```shell
./tools/tpm configure alpha --connector-max-connections=2500 --connector-drop-after-max-connections=true
./tools/tpm update
```

**Important**

Updating these values require a connector restart (via tpm update) for the changes to be recognized.

To select a real-world value for `connector-max-connections [349]`, set the value to a value slightly lower than the MySQL value of `max_connections` to prevent the server from ever hitting maximum. You may use the following formula for a more complex calculation: `connector-max-connections = (MySQL Master max_connections / number of connectors) * 0.95`

**Important**

When `connector-drop-after-max-connections [349]` is enabled, be sure that your load balancers are configured to identify that max connections have been reached and to switch to another connector when that happens.

6.11.6. Adjusting the Client Disconnect Delay During Manual Switch

This feature controls how the connector handles existing connections when a manual switch is invoked.

When a graceful switch is invoked via `cctrl`, by default the Connector will wait for five (5) seconds to allow in-flight activities to complete before forcibly disconnecting all active connections from the application side, no matter what type of query was in use.

If connections still exist after the timeout interval, they are forced closed, and the application will get back an error.

**Important**

This setting ONLY applies to a manual switch. During a failover, there is no wait and all connections are force-closed immediately.
This timeout is adjusted via the `tpm` option `--connector-disconnect-timeout [349]`.

For example, to change the delay to 10 seconds:

```
shell> ./tools/tpm configure alpha --connector-disconnect-timeout=10
shell> ./tools/tpm update
```

**Warning**

If you increase this value, you delay the manual switch! ONLY change this if you accept the fact that the manual switch process will last at least as long as this setting in seconds.

Do not set this value to zero (0) or there will be no attempt to disconnect at all. If you wish to disable the wait entirely, set `--property=waitForDisconnect=False` in your configuration on the connectors and run `tpm update`.

**Important**

Updating these values require a connector restart (via `tpm update`) for the changes to be recognized.

This value is reflected in the `waitForDisconnectTimeout` setting located in `cluster-home/conf/router.properties`.

### 6.11.7. Adjusting the Bridge Mode Forced Client Disconnect Timeout

This feature controls how long the Connector in Bridge mode waits before forcibly disconnecting the server side of the session after a client session ends.

Default: 500ms

When a client application opens a socket and connects to the connector, a second socket/connection to the server is created. The Connector in bridge mode then simply transfers data between these two sockets.

When a client application brutally closes a connection without following the proper disconnection protocol, the server will not know about that disconnect until the connector closes the Connector->server socket. If the connector closes the Connector->server connection too soon after a client disconnect, there is a chance that the proper disconnection messages will be missed, if sent late. If the connector does not close this connector->server connection, it would stay open indefinitely, using memory and resources that would otherwise be reclaimed. The default of 500ms is very conservative and will fit most environments where client applications disconnect properly. When the volume of connections opened and never closed exceeds a certain level, the timeout must be tuned (lowered) to close idle connections faster, or the available resources will get used up.

Many times this situation is caused by health checks, especially from monitoring scripts and load balancers checking port liveness. Many of these check do not gracefully close the connection, triggering the need for tuning the Connector.

If connections still exist after the timeout interval, they are forced closed, and a warning will be printed in the connector logs (C>S ended. S>C streaming did not finish within `bridgeServerToClientForcedCloseTimeout=500` [ms]. Will be closed anyway !).

**Important**

This setting ONLY applies to Bridge mode.

This timeout is adjusted via the `tpm` property `--property=bridgeServerToClientForcedCloseTimeout [316]` in milliseconds.

For example, to change the delay to 50 milliseconds:

```
shell> ./tools/tpm configure alpha --property=bridgeServerToClientForcedCloseTimeout=50
shell> ./tools/tpm update
```

**Warning**

If you decrease this value, you run the risk of disconnecting valid but slow sessions.

**Important**

Updating these values require a connector restart (via `tpm update`) for the changes to be recognized.

### 6.11.8. Adjusting the Connector Response to Resource Losses

This section describes how to control the Connector responses in the event of the loss of a required Datasource or all Managers.

#### 6.11.8.1. Adjusting the Connector Response to Datasource Loss

Summary: Whenever no master datasource is found, the Connector will reject connection requests.
This feature controls how long the Connector waits for the given type of DataSource to come ONLINE before forcibly disconnecting the client application.

By default, wait indefinitely for a resource to become available.

**Warning**

Prior to software versions 5.3.2/6.0.1, the ONHOLD state would reject new connection attempts instead of pausing them. Also, waitIfUnavailableTimeout was ignored, and connection attempts were never severed after timeout.

There are two (2) parameters involved in this decision-making. They are:

- **waitIfUnavailable** [default: true]
  
  If `waitIfUnavailable` is true, then the Connector will wait for up to the time period specified by `waitIfUnavailableTimeout` to make a connection for a given QOS. If the timeout expires, the Connector will disconnect the client application (reject connection attempts and close ongoing connections).

  If `waitIfUnavailable` is false, the Connector will immediately disconnect the client with an error if a connection for a given QOS cannot be made immediately.

- **waitIfUnavailableTimeout** [default: 0, wait indefinitely]
  
  If `waitIfUnavailable` is true, the Connector will wait for up to `waitIfUnavailableTimeout` number of seconds before disconnecting the client. If `waitIfUnavailable` is false, this parameter is ignored. If this parameter is set to zero (0) seconds, the Connector will wait indefinitely (client connection requests will hang forever).

For example, to immediately reject connections upon DataSource loss:

Click the link below to switch examples between Staging and INI methods...

Show Staging

Show INI

```shell
shell> tpm query staging
tungsten@db1:/opt/continuent/software/tungsten-clustering-6.0.5-41
```

```shell
tungsten@db1:/opt/continuent/software/tungsten-clustering-6.0.5-41
shell> echo The staging USER is `tpm query staging| cut -d: -f1 | cut -d@ -f1`
The staging USER is tungsten
```

```shell
shell> echo The staging HOST is `tpm query staging| cut -d: -f1 | cut -d@ -f2`
The staging HOST is db1
```

```shell
shell> echo The staging DIRECTORY is `tpm query staging| cut -d: -f2`
The staging DIRECTORY is /opt/continuent/software/tungsten-clustering-6.0.5-41
```

```shell
shell> ssh {STAGING_USER}@{STAGING_HOST}
```

```shell
shell> cd {STAGING_DIRECTORY}
```

```shell
shell> ./tools/tpm configure alpha \
   --property=waitIfUnavailable=false
```

Run the `tpm` command to update the software with the Staging-based configuration:

```shell
shell> ./tools/tpm update --replace-release
```

For information about making updates when using a Staging-method deployment, please see Section 9.3.7, “Configuration Changes from a Staging Directory”.

```shell
shell> vi /etc/tungsten/tungsten.ini
```

```ini
[alpha]
...  
property=waitIfUnavailable=false
```

Run the `tpm` command to update the software with the INI-based configuration:

```shell
shell> tpm query staging
tungsten@db1:/opt/continuent/software/tungsten-clustering-6.0.5-41
```

```shell
shell> echo The staging DIRECTORY is `tpm query staging| cut -d: -f2`
The staging DIRECTORY is /opt/continuent/software/tungsten-clustering-6.0.5-41
```

```shell
shell> cd (STAGING_DIRECTORY)
```

```shell
shell> ./tools/tpm update --replace-release
```
Warning

PLEASE NOTE: this will make switch and failover much less transparent to the application since the connections will error until the new master is elected and back online.

Important

Updating these values require a connector restart (via tpm update) for the changes to be recognized.

These entries will NOT work if placed into [defaults], each service must be handled individually.

6.11.8.2. Adjusting the Connector Response to Manager Loss

Summary: Whenever the Connector loses sight of the managers for a given data service, it will either suspend or reject new connection requests.

By default, suspend requests indefinitely until Manager communications are re-established.

This feature controls how long the Connector waits during a manager loss event to either suspend or reject the client connection.

Here is the decision chain and associated settings for what happens when the connector loses sight of the managers:

1. Delay for the value of delayBeforeOnHoldIfNoManager seconds which is 0/no delay by default.

2. Change state to ON-HOLD and begin the countdown timer starting from the delayBeforeOfflineIfNoManager value.

   In the ON-HOLD state, the connector will hang all new connections and allow existing connections to continue.

3. When the delayBeforeOfflineIfNoManager timer expires [30 seconds by default], change state to OFFLINE.

   Once OFFLINE, the Connector will break existing connections because there is no authoritative Manager node from the Connector’s perspective. Without a Manager link, any change to the cluster configuration will remain invisible to the Connector, potentially leading to writes on a slave node.

   By default, all new connection requests will hang in the OFFLINE state. If waitIfDisabled is set to false, then the Connector will instead reject all new connections.

There are multiple parameters involved in this decision-making. They are:

- delayBeforeOnHoldIfNoManager [in seconds, default: 0, i.e. no delay]

  When the connector loses sight of the managers, delay before going ON-HOLD for the value of delayBeforeOnHoldIfNoManager seconds, which is 0/no delay by default.

- delayBeforeOfflineIfNoManager [in seconds, default: 30]

  Once ON-HOLD, delay before going OFFLINE for the value of delayBeforeOfflineIfNoManager seconds, 30 by default.

- waitIfDisabled [default: true]

  If the Dataservice is OFFLINE because it is unable to communicate with any Manager, the waitIfDisabled parameter determines whether to suspend connection requests or to reject them. If waitIfDisabled is true [the default], then the Connector will wait indefinitely for manager communications to be re-established. If waitIfDisabled is set to false, the Connector will return an error immediately.

To check for data service state, use the tungsten-connector/bin/connector cluster-status command. For example:

```
$ tungsten-connector/bin/connector cluster-status
```

<table>
<thead>
<tr>
<th>Data service</th>
<th>Data service state</th>
<th>Data source</th>
<th>Is composite</th>
<th>Role</th>
<th>State</th>
<th>High water</th>
<th>Last shun reason</th>
<th>Applied latency</th>
<th>Relative latency</th>
<th>Active connections</th>
<th>Connections created</th>
</tr>
</thead>
<tbody>
<tr>
<td>europe</td>
<td>OFFLINE</td>
<td>c1</td>
<td>false</td>
<td>master</td>
<td>ONLINE</td>
<td>0(c1-bin.000002:0000000000000510;-1)</td>
<td>MANUALLY-SHUNNED</td>
<td>8.0</td>
<td>5193.0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>europe</td>
<td>OFFLINE</td>
<td>c2</td>
<td>false</td>
<td>slave</td>
<td>ONLINE</td>
<td>0(c1-bin.000002:0000000000000510;-1)</td>
<td></td>
<td>1.0</td>
<td>5190.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>europe</td>
<td>OFFLINE</td>
<td>c3</td>
<td>false</td>
<td>slave</td>
<td>ONLINE</td>
<td>0(c1-bin.000002:0000000000000510;-1)</td>
<td></td>
<td>2.0</td>
<td>5190.0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

For more information, see Connector On-Hold State [197].

For example, to decrease the ON-HOLD time to 15 seconds:

Click the link below to switch examples between Staging and INI methods...
Run the `tpm` command to update the software with the Staging-based configuration:

```
shell> ./tools/tpm configure alpha \
   --property=delayBeforeOfflineIfNoManager=15
```

Run the `tpm` command to update the software with the INI-based configuration:

```
shell> ./tools/tpm configure alpha \
   --property=waitIfDisabled=false
```

**Warning**

PLEASE NOTE: this will make switch and failover much less transparent to the application since the connections will error until communications with at least one manager has been established and the Connector is back online.

**Important**

Updating these values require a connector restart (via `tpm update`) for the changes to be recognized.

These entries will NOT work if placed into `[defaults]`, each service must be updated individually.

### 6.12. Connector General Limitations

The following general limitations exist when using the Connector; these issues do not affect the connector when using it in when using bridge mode:
• When using `mysqldump` within MySQL 5.6 or later, the `--single-transaction` option is not supported when connectivity to the database is made through the connector.

• When using `mysqldump`, the `--flush-logs` option is not supported when connectivity to the database is made through the connector.
Chapter 7. Tungsten Manager

The Tungsten Manager provides the management and monitoring of the Continuent Tungsten services to ensure that datasources, connectors and other components are running, datasources are replicating to each other, and handles failover and maintenance schedules.

7.1. Tungsten Manager Introduction

The Tungsten Manager is responsible for monitoring and managing a Continuent Tungsten dataservice. The manager has a number of control and supervisory roles for the operation of the cluster, and acts both as a control and a central information source for the status and health of the dataservice as a whole.

Primarily, the Tungsten Manager handles the following tasks:

• Monitors the replication status of each datasource within the cluster.

• Communicates and updates Tungsten Connector with information about the status of each datasource. In the event of a change of status, Tungsten Connectors are notified so that queries can be redirected accordingly.

• Manages all the individual components of the system. Using the Java JMX system the manager is able to directly control the different components to change status, control the replication process, and

• Checks to determine the availability of datasources by using either the system ping protocol (default), or using the Echo TCP/IP protocol on port 7 to determine whether a host is available. The configuration of the protocol to be used can be made by adjusting the manager properties. For more information, see Section C.2.2.3, “Host Availability Checks”.

• Includes an advanced rules engine. The rule engine is used to respond to different events within the cluster and perform the necessary operations to keep the dataservice in optimal working state. During any change in status, whether user-selected or automatically triggered due to a failure, the rules are used to make decisions about whether to restart services, swap masters, or reconfigure connectors.

In order to be able to avoid split brain, a cluster needs an odd number of members such that if there is a network partition, there’s always a chance that a majority of the members are in one of the network partitions. If there is not a majority, it’s not possible to establish a quorum and the partition with the master, and no majority, will end up with a shunned master until such time a quorum is established.

To operate with an even number of database nodes, a witness node is required, preferably an active witness, since the dynamics of establishing a quorum are more likely to succeed with an active witness than with a passive witness.

7.2. Tungsten Manager Failover Tuning

There are currently three discrete faults that can cause a failover of a master:

• Database server failure - failover will occur 20 seconds after the initial detection.

```
--property=policy.liveness.dbping.fail.threshold=1
```

The Tungsten Manager is unable to connect to the database server and gets an i/o error. If the database cannot respond to a tcp connect request after the configured number of attempts, the database server is flagged as STOPPED which initiates the failover.

This would mean, literally, that the process for the database server is gone and cannot respond to a tcp connect request. In this case, by default, the manager will try two more times, once every 10 seconds, after the initial i/o error is detected and after the then 30 second interval has elapsed, will flag the database server as being in the STOPPED state and this, in turn, initiates the failover.

• Host failure - failover will occur 30 seconds after the initial detection

```
--property=policy.liveness.hostPing.fail.threshold=2
```

The host on which the master database server is running is ‘gone’. The first indication that the master host is gone could be because the manager on that host no longer appears in the group of managers, one of which runs on each database server host. It could also be that the managers on the hosts besides the master do not see a heartbeat message from the master manager. In a variety of circumstances like this, both of the managers will, over a 60 second interval of time, once every 10 seconds, attempt to establish, definitively, that the master host is indeed either gone or completely unreachable via the network. If this is established, the remaining managers in the group will establish a quorum and the coordinator of that group will initiate failover.

• A replicator failure, if --property=policy.fence.masterReplicator [316] is set to true, will cause a failover 70 seconds after initial detection

```
--property=policy.fence.masterReplicator.threshold=6
```

215
7.3. Tungsten Manager Fault Detection, Fencing and Recovery

The information contained in this topic is meant to give a relatively comprehensive understanding of how the Tungsten Manager detects faults and the subsequent processing that leads to fencing the fault and possible recovery from faults. The main focus of this topic is the set of business rules, implemented in the Tungsten Manager, which, collectively, perform fault detection, fault fencing, and fault recovery.

7.3.1. Tungsten Manager Definitions

These definitions assume a familiarity with concepts like failover, switch, master and slave datasource etc.

- **coordinator** — every cluster designates one of the Tungsten managers in the cluster as the coordinator and it is this manager that will be responsible for taking action, if action is required, to recover the cluster's database resources to the most highly available state possible.

- **rules** — this term specifically refers to a set of 'business rules', implemented in a format required by the 'JBoss Drools' rules engine, and which are used to perform fault detection, fencing and recovery for Tungsten Clustering.

- **rule firing/triggering** — refers to the action of a rule becoming active due to the coincidence of one or more conditions specified in the rule itself. For example, a rule that detects a potential missing cluster member, called a 'heartbeat gap detection' rule, can fire if there are no other active alarms and if the rule has not 'seen' a cluster member heartbeat within the last 30-45 seconds. If a rule 'fires', further processing, specified in Java, will take effect.

- **fault/fault detection** — any condition which, if left unresolved, could lead to a lack of availability of database resources or to data inconsistency etc. Faults are detected. An example of a fault detection is to detect that a specific database server has stopped.

- **[fault] alarm** — the Tungsten Manager uses raises and processes entities that we will refer to as 'alarms' as an initial part of fault detection. A set of manager rules raise alarms under specific circumstances and that alarm stays active or triggers further processing depending on other rules. An alarm, depending on its type, may not necessarily mean that a fault has been definitively detected but that something has been detected that may or may not lead to an actual fault condition. An example of this, as you will see later, is a HeartbeatGapAlarm which occurs when the rules on a specific manager detect that a heartbeat event has not been received from one or more of the other managers in the group.

- **[fault] alarm retraction** — the action taken, by the rules, to remove an alarm from consideration for further action. For example, if the manager raises a 'Heartbeat Gap Alarm' and then, subsequently, detects that the heartbeat from the errant member has resumed, a rule will retract that alarm.

- **[fault] fence/fencing** — the action which leads to a first-level amelioration of a fault i.e. an action that keeps a fault from causing further harm - applications are isolated from the fault through the action of fencing. Fencing a fault results in the removal of the original fault condition but may also result in further recovery actions. An example of fencing the fault that is detected when a database server has stopped is to set the associated datasource to the FAILED state. This effectively makes the datasource unavailable to applications, immediately, thus isolating the application from the fault state.

- **[fault] recover/recovery** — the action which may occur after a fault is initially fenced and which leads to a condition of continued availability, data consistency etc. An example of a recovery operation is, for example, the failover that occurs after a stopped master database fault has been fenced.

- **split-brain** — a condition of a cluster such that members of the cluster group have different views of the same set of database resources and, in the most damaging incidence of split-brain, more than different cluster members designate different database resources as the master resource, resulting in applications being able, for example, to perform database updates on a database resource that should be a slave. This condition is to be avoided at all costs since the result is data loss or data corruption.

Important

The interval of time from the first detection of a fault until a failover occurs is configurable over 10 second intervals. The formula for determining the listed default failover intervals is based on the value of 'threshold' in the properties file (tungsten-manager/conf/manager.properties): interval = [threshold + 1] * 10 seconds

7.3.2. Cluster Monitoring and Notification Events
The key fact that must be understood in order that the operation of the rules can be grasped is that the rules are primarily driven by notification events which are, in turn, generated by the cluster monitoring subsystem or, in some cases, by threads internal to the manager that act as monitors for specific conditions.

As a general rule, notifications are generated in the monitoring subsystem, on each host, independently of the other hosts, and sent, by each manager, to all of the managers in the group, including itself, via group communications and the notifications are then routed to the rules engine in each manager.

These notifications are sent via a messaging protocol that guarantees that the monitoring events are received by all managers in the group in exactly the same order. This ordering is a critical part of correct rules operation for if notifications are received in a different order and used to drive the rules evaluation, the rules on each manager could arrive at a different state/conclusion based on the ordering.

The cluster monitoring subsystem driven by a set of checker threads that are configured from files found in tungsten-manager/conf and are named checker*.properties. There are currently four of these checkers, with their corresponding checker configurations stored in the following tungsten-manager/conf/checker*.properties files:

- checker.heartbeat.properties - runs a thread the generates a manager heartbeat notification for the manager. If a manager goes away from the group, either by crashing, being stopped, or having a network outage, other managers won’t ‘see’ that manager’s heartbeat and will use that as a clue that there may be something amiss on that manager’s host.
- checker.instrumentation.properties - TBD
- checker.mysqlserver.properties - polls the local mysql server for liveness/state. This checker attempts to establish a connection with the local MySQL server and to execute the query that is found in tungsten-manager/conf/mysql_checker_query.sql. The checker then evaluates the success or failure of the connect attempt and subsequent query execution and establishes the state of the MySQL server based on that evaluation. Because database server state is so critical to the operation of the cluster, particularly when it comes to availability of database resources, this particular checker uses a very fine-grained and configurable process for evaluating the state.
- checker.tungstenreplicator.properties - polls the local Tungsten replicator for liveness/state. This checker connects to the local replicator via the JMX interfaces and queries the replicator for its current state. If, in the process of connecting to the replicator, a connection cannot be established because the replicator is not running, the checker simply returns the STOPPED state.

Let’s look at the contents of one of these files - checker.mysqlserver.properties:

```
# AUTO-GENERATED: 2017-03-22T16:43:25-07:08
########################################################
# CHECKER.MYSQLSERVER.PROPERTIES #
########################################################
requiresProxy=true
name=mysql_response
class=com.continuent.tungsten.monitor.checkers.JDBCMySQLDatabaseServerChecker
# delay between each monitoring run - default 3000ms
frequency=3000
# connection will be renewed after this period
reconnectAfter=30000
servername=viveka
host=viveka
vendor=mysql
port=3306
driver=org.drizzle.jdbc.DrizzleDriver
url=jdbc:mysql:thin://viveka:3306/tungsten
username=tungsten
password=passw0rd
query=select 1
queryTimeout=5
queryFileName=mysql_checker_query.sql
```

The key thing to understand about this configuration file is that the value for the class property indicates which Java class the manager will load and that class, when alive, will then be configured with the additional properties that can be seen in this file.

Every checker will have a property frequency which indicates how often the checker thread will become active.

Then, since this checker is for MySQL server, you can see that the configuration file indicates which jdbc driver to use, which port to use to connect directly to MySQL, username, password etc. for the connection as well as the name of a file that determines what SQL the checker will run to check for the MySQL server liveness.

7.3.3. Rule Organization - Detection, Investigation, Fencing, Recovery

The main focus of manager operations are fault processing business rules, and since these rules are organized into categories based on their function. As you can infer from some of the previous definitions, there are four major categories of rules, with some ancillary ‘housekeeping’ categories. The four major categories are:
1. Fault Detection — raise alarms for specific or nascent faults.

The text shown below comes directly from the source code for the manager rules and comprise the major faults detected by the manager:

- **0600: DETECT MEMBER HEARTBEAT GAP**
  This rule fires if there are not already other alarm types pending, for a specific member, and if at least 30-45 seconds has elapsed since the last time a given manager send a ClusterMemberHeartbeat event to the group of managers. The result of this rule firing will be that a MemberHeartbeatGapAlarm is raised as well as a MembershipInvalidAlarm. Both of these alarms trigger other rules, explained later, which do further investigations of the current cluster connectivity and membership.

- **0601: DETECT STOPPED CLUSTER MANAGER**
  This rule fires after a MemberHeartbeatGapAlarm has been raised since the reason for a heartbeat gap can be that a manager has stopped. Further processing determines whether or not the manager is, indeed, stopped. This rule generates a ManagerStoppedAlarm if it determines that the manager in question is, in fact, stopped.

- **0602: DETECT DATASERVER FAULT**
  This rule fires whenever monitoring detects that a given database server is not in the ONLINE state. The result of this rule firing is a DataServerFaultAlarm which, in turn, results in further investigation via one of the investigation rules described later.

- **0604: DETECT UNREACHABLE REMOTE SERVICE**
  In the case of a composite cluster, the current coordinator on each site will connect to one manager on the remote site. After establishing this connection, the local manager will pull the remote manager for liveness and generate a RemoteServiceHeartbeatNotification that has a status of REACHABLE. If the remote manager is not reachable, the manager that is polling the remote service will generate a RemoteServiceHeartbeatNotification that has a resource state of UNREACHABLE in which case this rule triggers and a RemoteDataServiceUnreachableAlarm is raised by this rule.

- **0606: DETECT REPLICATOR FAULT**
  As the name of this rule indicates, it will detect a replicator fault. This rule triggers if it sees a replicator notification that indicates that any of the replicators in the cluster are in a STOPPED, SUSPECT or OFFLINE state. The result of triggering of this rule is at a ReplicatorFaultAlarm is raised.

2. Fault Investigation - process alarms by iteratively investigating whether or not the alarm represents a true fault that requires further action.

- **0525: INVESTIGATE MY LIVENESS**
  In this rule title the word MY refers to the manager that is currently evaluating the rule. This rule triggers when it sees a MemberHeartbeatGapAlarm and, as a result of triggering, the manager checks to see if it has both network connectivity as well as visibility of the other cluster members including, if necessary, visibility of a passive witness host. If, during this connectivity check, a manager determines that it is isolated from the rest of the cluster, it will restart itself in a failsafe mode meaning that it will shun all of its database resources and then attempt to join an existing cluster group as a part of a quorum. This rule is particularly important in cases where there are transient or even protracted network outages since it forms a part of the strategy used to avoid split-brain operations. If the manager, after restarting, is able to become part of a cluster quorum group, the process of joining that group will result in shunned resources becoming available again if appropriate.

- **0530: INVESTIGATE MEMBERSHIP VALIDITY**
  This rule is triggered when it sees a MembershipInvalidAlarm which was previously generated as the result of a member heartbeat gap. The previous rule, INVESTIGATE MY LIVENESS checks for network connectivity for the current manager. This rule checks to see if the current manager is a part of a cluster quorum group. This type of check implies a connectivity check as well but goes further to see if other managers in the group are alive and operational. This rule is another critical part of split brain avoidance since, depending on what it determines, it will take one of the following actions:
  
  - If the manager does not have network connectivity after checking, every 10 seconds, for a period of 60 seconds, it will restart itself in two different modes:
    
    a. If the manager detects that it is the last man standing, meaning that it is currently responsible for the master datasource and all of the other cluster members had previously stopped, it will restart normally, leaving the master datasource available, and will be prepared to be the leader of any new group of managers.
    
    b. If the manager is not the last man standing
Tungsten Manager

, it will restart in failsafe mode i.e. will restart with all of its resources shunned and will attempt to join an existing group.

- If the manager has network connectivity i.e. can see all of the other hosts in the cluster, it then checks to see if it is a part of a primary partition i.e. a cluster quorum group. If, the first time it checks, it determines that it is not a part of a primary partition, it immediately disconnects all existing Tungsten connector connections from itself. This has the effect, on the Tungsten connector side, of immediately suspending all new database connection requests until such time that the manager determines that it is in a primary partition. This is, again, a critical part of avoiding split-brain operation since it makes it impossible for connectors to satisfy new connection requests until a valid cluster quorum can be definitively validated.

- The manager will then keep doing this check for quorum group membership, every 10 seconds, for a period of 60 seconds. If it determines that it is not a member of a quorum group, it will use the same criteria, as mentioned previously in the network connectivity case, to determine how it shall restart i.e.:
  a. If it is the last man standing
     It will, as in the above case, restart normally, leaving the master datasource available.
  b. If the manager is not the last man standing
     , it will restart in failsafe mode i.e. will restart with all of its resources shunned and will attempt to join an existing group.

- If, after all of the previous checks, the manager establishes that it is a part of a quorum group, it will, if necessary because it disconnected Tungsten connectors during quorum validation, it will become available for Tungsten connectors to connect to it again after synchronizing its view of the cluster with the current cluster coordinator, and will then continue normal operations.

- 0550: INVESTIGATE: TIME KEEPER FOR HEARBEAT GAP ALARM

- 0550: INVESTIGATE: TIME KEEPER FOR INVALID MEMBERSHIP ALARM

- 0550: INVESTIGATE: TIME KEEPER FOR MANAGER STOPPED ALARM

- 0550: INVESTIGATE: TIME KEEPER FOR DATASERVER STOPPED ALARM

- 0551: INVESTIGATE: TIME KEEPER FOR REMOTE SERVICE STOPPED ALARM

- 0552: INVESTIGATE: TIME KEEPER FOR REPLICATOR FAULT ALARM

3. Fault Fencing - fences validated faults, rendering them less disruptive/harmful from the standpoint of the application.

- 0303: FENCE FAILED NODE

- 0304: FENCE FAULTED DATASERVER

- 0305: FENCE UNREACHABLE REMOTE SERVICE

- 0306: FENCE REPLICATOR FAULT - DIMINISHED DATASOURCE

- 0306: FENCE REPLICATOR FAULT - EXPIRED ALARM

4. Fault Recovery - attempts to render the fault completely harmless by taking some action that either corrects the fault or by providing alternative resources to manage the fault.

- 0200a: RECOVER MASTER DATASOURCE BY FAILING OVER - NON-REPLICATOR FAULT

- 0200b: RECOVER MASTER DATASOURCE BY FAILING OVER - REPLICATOR FAULT

- 0201: RECOVER COMPOSITE DATASOURCES TO ONLINE
Tungsten Manager

- 0201a: RECOVER FAILSAFE PHYSICAL SLAVE WITH ONLINE PRIMARY
- 0201: RECOVER FAILSAFE SHUNNED COMPOSITE SLAVE TO ONLINE
- 0202: RECOVER OFFLINE PHYSICAL DATASOURCES TO ONLINE
- 0203: RECOVER FAILED PHYSICAL DATASOURCES TO ONLINE
- 0204: RECOVER MASTER REPLICA TO ONLINE
- 0205: RECOVER SLAVE REPLICA TO ONLINE
- 0206: RECOVER FROM DIMINISHED STATE WHEN STOPPED REPLICA RESTARTS
- 0207: RECOVER MERGED MEMBERS
- 0208: RECOVER AND RECONCILE REMOTE DATA SERVICE STATE
- 0209: PREVENT MULTIPLE ONLINE MASTERS
- 0210: RECOVER WITNESSES TO ONLINE
- 0211: RECOVER REMOTE FAILSAFE SHUNNED COMPOSITE MASTER TO ONLINE
- 0212: RECOVER NON-READ-ONLY SLAVES TO READ-ONLY
Chapter 8. Command-line Tools

Continuent Tungsten is supplied with a number of different command-line tools and utilities that help to install manage, control and provide additional functionality on top of the core Continuent Tungsten product.

The content in this chapter provides reference information for using and working with all of these tools. Usage and operation with these tools in particular circumstances and scenarios are provided in other chapters. For example, deployments are handled in Chapter 2, Deployment, although all deployments rely on the tpm command.

Commands related to the deployment
- tpm — Tungsten package manager

Commands related to managing Continuent Tungsten
- cctrl — cluster control
- cluster_backup—cluster backup automation

Commands related to the core Tungsten Replicator
- trepctl — replicator control
- multi_trepctl — multi-replicator control
- thl — examine Tungsten History Log contents

Commands related to managing Tungsten Replicator deployments
- tungsten_provision_slave — provision or reprovision a slave from an existing master or slave database
- tungsten_read_master_events — read master events to determine the correct log position
- tungsten_set_position — set the position of the replicator

Commands related to monitoring the cluster service
- tungsten_monitor — build DDL, materialize and compare replicated data
- tungsten_health_check — checks the cluster for best practice configuration and operation
- tungsten_send_diag — assists with diag and file uploads to Continuent support
- tungsten_prep_upgrade — assists with upgrades from one topology to another

8.1. The cctrl Command

The cctrl command provides cluster management for your installed cluster, providing a command-line shell interface to obtain information and manage your cluster and structure.

8.1.1. cctrl Command-line Options


Where:
- -admin [221]

Table 8.1. cctrl Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>-admin [221]</td>
<td>Enter admin mode when connecting</td>
<td>string</td>
</tr>
</tbody>
</table>

Automatically enters admin mode when cctrl connects to the cluster:

shell> cctrl -admin
Continuent Tungsten 2.0
**Table 8.2. cctrl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>-expert [222]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter expert mode when connecting</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

Automatically enters `expert` mode when `cctrl` connects to the cluster:

```
$cctrl -expert
Continuent Tungsten 2.0
alpha: session established, encryption=false, authentication=false
[LOGICAL:EXPERT] /alpha >
```

**Table 8.3. cctrl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>-host [222]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Host name of the service manager to use</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Default</td>
<td>localhost</td>
</tr>
</tbody>
</table>

Allows you to specify the host to connect to when looking for a manager. By default, `cctrl` will connect to the local host:

```
$cctrl -host host1
Continuent Tungsten 2.0
alpha: session established, encryption=false, authentication=false
[LOGICAL] /alpha >
```

**Table 8.4. cctrl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>-logical [222]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter logical mode when connecting</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

Automatically enters `logical` mode when `cctrl` connects to the cluster. This mode is the default when connecting to a typical; using this option forces this mode:

```
$cctrl -expert
Continuent Tungsten 2.0
alpha: session established, encryption=false, authentication=false
[LOGICAL:EXPERT] /alpha >
```

**Table 8.5. cctrl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>-multi [222]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Allow support for connecting to multiple services</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

Allow support for connecting to multiple services:

```
$cctrl -multi
Continuent Tungsten 2.0
alpha: session established, encryption=false, authentication=false
[LOGICAL:EXPERT] /alpha >
```

**Table 8.6. cctrl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>-no-history [222]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Disable command history</td>
</tr>
</tbody>
</table>
Prevents `cctrl` from accessing or recording command history during interaction.

```
-physical [223]
```

### Table 8.7. `cctrl` Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-physical</td>
<td>string</td>
<td>Enter physical mode when connecting</td>
</tr>
</tbody>
</table>

Automatically enters logical mode when `cctrl` connects to the cluster. This mode is the default when connecting to a typical; using this option forces this mode:

```
shell> cctrl -physical
Continuent Tungsten 2.0
alpha: session established, encryption=false, authentication=false
[PHYSICAL] resource://>
```

```
- port [223]
```

### Table 8.8. `cctrl` Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-port</td>
<td>string</td>
<td>Specify the TCP/IP port of the service manager</td>
</tr>
<tr>
<td>Default</td>
<td>9997</td>
<td></td>
</tr>
</tbody>
</table>

Specify the TCP/IP port of the service manager

```
- proxy [223]
```

### Table 8.9. `cctrl` Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-proxy</td>
<td>string</td>
<td>Operate as a proxy service</td>
</tr>
</tbody>
</table>

Operate as a proxy service

```
- service [223]
```

### Table 8.10. `cctrl` Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-service</td>
<td>string</td>
<td>Connect to a specific service</td>
</tr>
</tbody>
</table>

Enables the selection of a specific service when first connecting to the cluster. For example:

```
shell > cctrl -service east_from_west
Continuent Tungsten 2.0
east: session established, encryption=false, authentication=false
east_from_west: session established, encryption=false, authentication=false
[LOGICAL] /east_from_west >
```

### 8.1.2. `cctrl` Modes

- Admin Mode
- Expert Mode
- Logical Mode
- Physical Mode
You can specify the mode to enter from the command-line, using the appropriate switch. For example, to start `cctrl` in `Expert` mode:

```
shell> cctrl -expert
```

The default mode is `Logical`.

You can also change the mode from within `cctrl` by issuing the appropriate command. For example, to switch to `Expert` mode:

```
[LOGICAL] /alpha >
```

WARNING: This is an expert-level command: Incorrect use may cause data corruption or make the cluster unavailable.

Do you want to continue? (y/n)> y

```
[LOGICAL:EXPERT] /alpha >
```

The current mode is always displayed as part of the command prompt within `cctrl`.

### 8.1.3. cctrl Commands

#### Table 8.11. cctrl Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Change to admin mode</td>
</tr>
<tr>
<td>cd</td>
<td>Change to a specific site within a multisite service</td>
</tr>
<tr>
<td>cluster</td>
<td>Issue a command across the entire cluster</td>
</tr>
<tr>
<td>cluster validate</td>
<td>Validate the cluster quorum configuration</td>
</tr>
<tr>
<td>create composite</td>
<td>Create a composite dataservice</td>
</tr>
<tr>
<td>datasource</td>
<td>Issue a command on a single datasource</td>
</tr>
<tr>
<td>expert</td>
<td>Change to expert mode</td>
</tr>
<tr>
<td>failover</td>
<td>Perform a failover operation from a master to a slave</td>
</tr>
<tr>
<td>help</td>
<td>Display the help information</td>
</tr>
<tr>
<td>ls</td>
<td>Show cluster status</td>
</tr>
<tr>
<td>members</td>
<td>List the managers of the dataservice</td>
</tr>
<tr>
<td>physical</td>
<td>Enter physical mode</td>
</tr>
<tr>
<td>ping</td>
<td>Test host availability</td>
</tr>
<tr>
<td>quit, exit</td>
<td>Exit cctrl</td>
</tr>
<tr>
<td>recover master using</td>
<td>Recover the master within a datasource using the specified master</td>
</tr>
<tr>
<td>replicator</td>
<td>Issue a command on a specific replicator</td>
</tr>
<tr>
<td>router</td>
<td>Issue a command on a specific router [connector]</td>
</tr>
<tr>
<td>service</td>
<td>Run a service script</td>
</tr>
<tr>
<td>set</td>
<td>Set management options</td>
</tr>
<tr>
<td>set master</td>
<td>Set the master within a datasource</td>
</tr>
<tr>
<td>show topology</td>
<td>Shows the currently configured topology</td>
</tr>
<tr>
<td>switch</td>
<td>Promote a slave to a master</td>
</tr>
</tbody>
</table>

#### 8.1.3.1. cctrl admin Command

The `admin` command enables admin mode commands and displays. Admin mode is a specialized mode used to examine and repair cluster metadata. It is not recommended for normal use.

#### 8.1.3.2. cctrl cd Command

The `cd` command changes the data service being administered. Subsequent commands will only affect the given data service name.

Using `cd ..` allows to go back to the root element. The given data service name can be either composite or physical. Note that this command can only be used when `cctrl` is run with the `-multi` flag.
8.1.3.3. cctrl cluster Command

The cluster command operates at the level of the full cluster.

8.1.3.3.1. cctrl cluster check Command

The cluster check command issues an MD5 consistency check on one or more tables in a database on the master data source. The consistency checks then replicate to each slave, whereupon the slave replicator repeats the check.

If the check fails, slaves may go offline or print a log warning depending on how the replicators are configured. The default is to go offline. You can return a replicator to the online state after a failed check by issuing a replicator online command.

The table name can also be a wildcard (*) in which case all tables will be checked. Users may optionally specify a range of rows to check using the -limit option, which takes a starting row option followed by a number of rows to check. Rows are selected in primary key order.

Usage:

The following example checks all tables in database accounting.

```plaintext
[LOGICAL] /alpha > cluster check accounting.*
```

The following command checks only the first 10 rows in a single table.

```plaintext
[LOGICAL] /alpha > cluster check accounting.invoices -limit 1,10
```

Warning

Consistency checks can be very lengthy operations for large tables and will lock them while they run. On the master this can block applications. On slaves it blocks replication.

8.1.3.3.2. cctrl cluster flush Command

The cluster flush command sends a heartbeat event through the local cluster and returns a flush sequence number that is guaranteed to be equal to or greater than the sequence number of the flush event. Slaves that reach the flush sequence number are guaranteed to have applied the flush event.

This command is commonly used for operations like switch that need to synchronize the position of one or more masters or slaves.

8.1.3.3.3. cctrl cluster heartbeat Command

The cluster heartbeat command sends a heartbeat event through the local cluster to demonstrate that all replicators are working. You should see the sequence numbers on all data sources advance by at least 1 if it is successful.

8.1.3.3.4. cctrl cluster offline Command

The cluster offline command brings all data services that are not offline into the offline state. It has no effect on services that are already offline.

8.1.3.3.5. cctrl cluster online Command

The cluster online command brings all data services that are not online into the online state. It has no effect on services that are already online.

8.1.3.3.6. cctrl cluster validate Command

The cluster validate command validates the configuration of the cluster with respect to the quorum used for decision making. The number of active managers, active witnesses and passive witnesses within the cluster is validated to ensure that there are enough active hosts to make a decision in the event of a failover or other failure event.

When executed, the validation routine checks all the available hosts, including witness hosts, and determines whether there are enough hosts, and whether their membership of the cluster is valid. In the event of deficiency, corrective action will be recommended.

By default, the command checks all hosts within the configured cluster:

```plaintext
[LOGICAL] /alpha > cluster validate
HOST host1/192.168.2.28: ALIVE
HOST host2/192.168.2.21: ALIVE
HOST host3/192.168.2.22: ALIVE
CHECKING FOR QUORUM: MUST BE AT LEAST 2 MEMBERS, OR 1 MEMBERS PLUS ALL WITNESSES
QUORUM SET MEMBERS ARE: host2, host1, host3
SIMPLE MAJORITY SIZE: 2
```
VALIDATED MEMBERS ARE: host2, host1, host3
REACHABLE MEMBERS ARE: host2, host1, host3
WITNESS HOSTS ARE:
REACHABLE WITNESSES ARE:
MEMBERSHIP IS VALID
GC VIEW OF CURRENT MEMBERS IS: host1, host2, host3
VALIDATED CURRENT MEMBERS ARE: host2, host1, host3
CONCLUSION: I AM IN A PRIMARY PARTITION OF 3 MEMBERS OUT OF THE REQUIRED MAJORITY OF 2
VALIDATION STATUS=VALID CLUSTER
ACTION=NONE

Additionally, a list of hosts to exclude from the check can be provided to verify the cluster capability when certain hosts have already failed or been shunned from the dataservice during maintenance.

To exclude hosts, add excluding and a comma-separated list of hosts to the command. For example:

```
[LOGICAL] /alpha > cluster validate excluding host3,host2
EXCLUDED host3 FROM VIEW
EXCLUDED host2 FROM VIEW
HOST host1/192.168.2.20: ALIVE
CHECKING FOR QUORUM: MUST BE AT LEAST 3 MEMBERS, OR 1 MEMBERS PLUS ALL WITNESSES
QUORUM SET MEMBERS ARE: host2, host1, host3
SIMPLE MAJORITY SIZE: 2
VALIDATED MEMBERS ARE: host1
REACHABLE MEMBERS ARE: host1
WITNESS HOSTS ARE:
REACHABLE WITNESSES ARE:
MEMBERSHIP IS VALID
GC VIEW OF CURRENT MEMBERS IS: host1
VALIDATED CURRENT MEMBERS ARE: host1
CONCLUSION: I AM IN A NON-PRIMARY PARTITION OF 1 MEMBERS OUT OF A REQUIRED MAJORITY SIZE OF 2
AND THERE ARE 0 REACHABLE WITNESSES OUT OF 0
VALIDATION STATUS=NON-PRIMARY PARTITION
ACTION=RESTART SAFE
```

Cluster validation can be used to provide validation only. To improve the support:

- Add active witnesses to the dataservice, see Section 3.5.2, “Adding Active Witnesses to an Existing Deployment”
- Add slave hosts to the dataservice, see Section 3.5.1, “Adding Datasources to an Existing Deployment”
- Add passive witnesses to the dataservice, see Section 3.5.3, “Adding Passive Witnesses to an Existing Deployment”

### 8.1.3.4. cctrl create composite Command

The `create composite` command creates a new composite data source or data service with the given name. Composite data services can only be create in the root directory ‘/’ while composite data sources need to be created from a composite data service location. Composite data source names should be the same as the physical data services Composite data service name should be named after its composite data sources

Usage:

The following example creates a composite data service named ‘sj_nyc’

```
create composite dataservice sj_nyc
```

The following example changes to the composite data service sj_nyc, then creates a composite data source named ‘sj’ in this composite data service

```
cd sj_nyc
create composite datasource sj
```

### 8.1.3.5. cctrl datasource Command

The datasource command affects a single data source.

```
datasource
backup
fail
host
offline
online
recover
restore
shun
welcome
```
### Table 8.12. `cctrldatasource` Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Backup a datasource</td>
</tr>
<tr>
<td>fail</td>
<td>Fail a datasource</td>
</tr>
<tr>
<td>host</td>
<td>Hostname of the datasource</td>
</tr>
<tr>
<td>offline</td>
<td>Put a datasource into the offline state</td>
</tr>
<tr>
<td>online</td>
<td>Put a datasource into the online state</td>
</tr>
<tr>
<td>recover</td>
<td>Recover a datasource into operation state as slave</td>
</tr>
<tr>
<td>restore</td>
<td>Restore a datasource from a previous backup</td>
</tr>
<tr>
<td>shun</td>
<td>Shun a datasource</td>
</tr>
<tr>
<td>welcome</td>
<td>Welcome a shunned datasource back to the cluster</td>
</tr>
</tbody>
</table>

#### 8.1.3.5.1. `cctrldatasource backup` Command

The `datasource backup` command invokes a backup on the data source on the named host using the default backup agent and storage agent. Backups taken in this way can be reloaded using the `datasource restore` command. The following command options are supported:

- `backupAgent` — The name of a backup agent.
- `storageAgent` — The name of a storage agent.
- `timeout` — Number of seconds to wait before the backup command times out.

On success the backup URL will be written to the console.

**Usage:**

The following example performs a backup on host saturn using the default backup agent.

```
cctrl> datasource saturn backup
```

The following example performs a backup on host mercury using the `xtrabackup` agent, which is named explicitly.

```
cctrl> datasource mercury backup xtrabackup
```

#### 8.1.3.5.2. `cctrldatasource backup` Command

#### 8.1.3.5.3. `cctrldatasource host` Command

#### 8.1.3.5.4. `cctrldatasource offline` Command

#### 8.1.3.5.5. `cctrldatasource online` Command

#### 8.1.3.5.6. `cctrldatasource recover` Command

#### 8.1.3.5.7. `cctrldatasource restore` Command

#### 8.1.3.5.8. `cctrldatasource shun` Command

#### 8.1.3.5.9. `cctrldatasource welcome` Command

When a datasource has been shunned, the datasource can be welcomed back to the dataservice by using the `welcome` command. The `welcome` command attempts to enable the datasource in the `ONLINE` state using the current roles and configuration. If the datasource was operating as a slave before it was shunned, the `welcome` command will enable the datasource as a slave.

For example, the host `host3` is a slave and currently online:

```
+----------------------------------------------------------------------------+
|host3(slave:ONLINE, progress=157454, latency=1.000)                      |
```

---

227
To switch the datasource back to the online state, the welcome is used:

```
[LOGICAL:EXPERT] /alpha > datasource host3 welcome
Data source 'host3' is now OFFLINE
```

The welcome command puts the datasource into the **OFFLINE** state. If the datasync policy mode is **AUTOMATIC**, the node will be placed into **ONLINE** mode due to automatic recovery. When in **MAINTENANCE** or **MANUAL** mode, the node must be manually set online.

The **welcome** command may not always work if there has been a failure or topology change between the moment it was shunned and welcomed back. Using the **recover** command may be a better alternative to using **welcome** when bringing a datasource back online. The **recover** commands ensures that the replicator, connector and operation of the datasource are correct within the current cluster configuration. See Section 8.1.3.14, "**cctrl recover Command**".

### 8.1.3.6. cctrl expert Command

### 8.1.3.7. cctrl failover Command

### 8.1.3.8. cctrl help Command

The help command provides help text from within the **cctrl** operation.

With no other arguments, help provides a list of the available commands:

```
[LOGICAL] /alpha > <userinput>help/1userinput
--------
Overview
--------
Description: Overview of Tungsten cctrl Commands

Commands
--------
admin                          - Enter admin mode
cd <name>                      - Change to the specified SOR cluster element
client <command>              - Issue a command on the entire cluster
class <type> <name>            - Create SOR cluster components
datasource <host> <cmd>        - Issue a command on a datasource
expert                         - Enter expert mode
failover                       - Failover from failed master to slave
help                           - Show help
ls [options]                   - Show generic cluster status
physical                      - Enter physical mode
quit or exit                   - Leave cctrl
replicator <host> <cmd>        - Issue a command on a replicator
service                       - Run a service script
set                            - Set management options
switch                         - Promote a slave to master

To get more information about particular commands type help followed by a command. Examples: 'help datasource' or 'help create composite'.
```

To get specific information about an individual command or operation, provide the command name to the help command. For example, to get information about the **ping** command, type help ping at the cctrl prompt.

### 8.1.3.9. cctrl ls Command

The **ls** command displays the current structure and status of the cluster.

```
ls [-l] [host] [[resources] | [services] | [sessions]]
```

The **ls** command operates in a number of different modes, according to the options provided on the command-line, as follows:

- **No options**
Generates a list of the current routers, datasources, and the their current status and services.

- `-l`
  Outputs extended information about the current status and configuration. The `-l` option can be used in both the standard (no option) and host specific output formats to provide more detailed information.

- `host`
- `resources`
- `services`
- `sessions`

Without any further options, the

```
[LOGICAL] /alpha &gt; ls
COORDINATOR[host1:AUTOMATIC:ONLINE]
ROUTERS:
+----------------------------------------------------------------------------+
| connector@host1[1179](ONLINE, created=0, active=0)                          |
| connector@host2[1532](ONLINE, created=0, active=0)                          |
| connector@host3[17665](ONLINE, created=0, active=0)                         |
+----------------------------------------------------------------------------+
DATASOURCES:
+----------------------------------------------------------------------------+
| host1(master:ONLINE, progress=60, THL latency=0.498)                        |
| STATUS [OK] [2013/03/22 02:25:00 PM GMT]                                    |
| | MANAGER(state=ONLINE)                                                     |
| | REPLICATOR(role=master, state=ONLINE)                                     |
| | DATASERVER(state=ONLINE)                                                  |
| | CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+
```

8.1.3.9.1. cctrl ls host

You can also specify an individual component within the cluster on which to obtain information. For example, to get the information only for a single host:

```
[LOGICAL] /alpha &gt; ls host2
COORDINATOR[host1:AUTOMATIC:ONLINE]
```

229
8.1.3.9.2. cctrl ls -l (Extended Information)

8.1.3.9.3. cctrl ls resources

The resources option generates a list of the configured resources and their current status.

8.1.3.9.4. cctrl ls services

8.1.3.9.5. cctrl ls sessions

8.1.3.10. cctrl members Command

The members command outputs a list of the currently identified managers within the dataservice.

members

For example:

[LOGICAL] /alpha > members
alpha/host1(ONLINE)/192.168.1.60:7800
alpha/host2(ONLINE)/192.168.1.61:7800
alpha/host3(ONLINE)/192.168.1.62:7800

The command outputs each identified manager service within the current dataservice.

The format of the output information is:

DATASERVICE/HOST(STATUS)/IPADDR:PORT

Where:

- DATASERVICE
  The name of the dataservice.

- HOST
  The name of the host on which the manager resides.

- STATUS
  The current status of the manager.

- IPADDR
  The IP address of the manager.

- PORT
  The primary TCP/IP port used for contacting the manager service.

The members service can be used as an indicator of the overall status of the dataservice. The information shown for each manager should within a single dataservice should be identical. If different information is shown, or an incomplete number of managers compared to the number of configured managers is provided, then it may indicate a communication or partition problem within the dataservice.

8.1.3.11. cctrl physical Command

8.1.3.12. cctrl ping Command
8.1.3.13. cctrl quit Command

Exits cctrl and returns the user to the shell. For example:

8.1.3.14. cctrl recover Command

8.1.3.15. cctrl recover master using Command

8.1.3.16. cctrl recover relay using Command

8.1.3.17. cctrl recover using Command

8.1.3.18. cctrl replicator Command

8.1.3.19. cctrl rm Command

8.1.3.20. cctrl router Command

8.1.3.21. cctrl service Command

8.1.3.22. cctrl set Command

8.1.3.23. cctrl set force Command

8.1.3.24. cctrl set master Command

8.1.3.25. cctrl switch Command

8.2. The check_tungsten_latency Command

The check_tungsten_latency command reports warning or critical status information depending on whether the latency across the nodes in the cluster is above a specific level.

Table 8.13. check_tungsten_latency Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Report a critical status if the latency is above this level</td>
</tr>
<tr>
<td>--perfdata</td>
<td>Show the latency performance information</td>
</tr>
<tr>
<td>--perslave-perfdata</td>
<td>Show the latency performance information on a per-slave basis</td>
</tr>
<tr>
<td>-w</td>
<td>Report a warning status if the latency is above this level</td>
</tr>
</tbody>
</table>

The command outputs information in the following format:

```
LEVEL: DETAIL
```

Where DETAIL includes detailed information about the status report, and LEVEL is:

- CRITICAL — latency on at least one node is above the specified threshold level for a critical report. The host reporting the high latency will be included in the DETAIL portion:

For example:

```
CRITICAL: host2=0.586s
```
Command-line Tools

- **WARNING** — latency on at least one node is above the specified threshold level for a warning report. The host reporting the high latency will be included in the DETAIL portion:

  For example:
  
  ```
  WARNING: host2=0.506s
  ```

- **OK** — status is OK; the highest reported latency will be included in the output.

  For example:
  
  ```
  OK: All slaves are running normally (max_latency=0.506)
  ```

The `-w` and `-c` options must be specified on the command line, and the critical figure must be higher than the warning figure. For example:

```shell
check_tungsten_latency -w 0.1 -c 0.5
```

Performance information can be included in the output to monitor the status. The format for the output is included in the DETAIL block and separates the maximum latency information for each node with a semicolon, and the detail block with a pipe symbol. For example:

```shell
check_tungsten_latency -w 1 -c 1 --perfdata
```

Performance information for all the slaves in the cluster can be output by using the `--perslave-perfdata` option which must be used in conjunction with the `--perfdata` option:

```shell
check_tungsten_latency -w 0.2 -c 0.5 --perfdata --perslave-perfdata
```

### 8.3. The `check_tungsten_online` Command

The `check_tungsten_online` command checks whether all the hosts in a given service are online and running.

Within a Continuent Tungsten service, the replicator, manager, and connector services are checked. All must be online for an OK response.

#### Table 8.14. `check_tungsten_online` Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h</code></td>
<td>Display the help text</td>
</tr>
<tr>
<td><code>-port</code></td>
<td>RMI port for the replicator being checked</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Check which hosts within a given service and online.</td>
</tr>
</tbody>
</table>

This command only needs to be run on one node within the service; the command returns the status for all nodes.

The command outputs information in the following format:

```
LEVEL: DETAIL
```

Where DETAIL includes detailed information about the status report, and LEVEL is:

- **CRITICAL** — status is critical and requires immediate attention. This indicates that more than one service is not running.

  For example:
  
  ```
  CRITICAL: Replicator is not running
  ```

- **WARNING** — status requires attention. This indicates that one service within the system is not online.

- **OK** — status is OK.

  For example:
  
  ```
  OK: All services are online
  ```

This output is easily parseable by various monitoring tools, including Nagios NRPE, and can be used to monitor the status of your services quickly without resorting to using the full trepctl output.

For example:

```shell
ccheck_tungsten_online
OK: All services are online
```
If you have multiple services installed, use the `-s` to specify the service:

```
shell> check_tungsten_online -s alpha
OK: All services are online
```

### 8.4. The `check_tungsten_progress` Command

The `check_tungsten_progress` command determines whether the replicator is actually making progress by executing a heartbeat operation and monitoring for this operation to complete within an optional time period (default is 1 second).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-t</code></td>
<td>Give a time period during which progress should be identified</td>
</tr>
</tbody>
</table>

The command outputs information in the following format:

```
LEVEL: DETAIL
```

Where DETAIL includes detailed information about the status report, and LEVEL is:

- **CRITICAL** — replicator is not making progress and either has not completed the heartbeat operation, or has failed. If failed, the reason will be shown in the DETAIL:

  For example:

  ```
  CRITICAL: Replicator is not ONLINE
  ```

- **OK** — replicator is making progress.

  For example:

  ```
  OK: Replicator is making progress
  ```

This output is easily parseable by various monitoring tools, including Nagios NRPE, and can be used to monitor the status of your services quickly without resorting to using the full `trepctl` output.

The time delay can be added on busy systems to ensure that the replicator is progressing, especially if you see errors like this:

```
shell> check_tungsten_progress
CRITICAL: Replicator is not ONLINE
```

For example, to wait 5 seconds to ensure the replicator is progressing:

```
shell> check_tungsten_progress -t 5
OK: Replicator is making progress
```

### 8.5. The `check_tungsten_services` Command

The `check_tungsten_services` command provides a simple check to confirm whether configured services are currently running. The command must be executed with a command-line option specifying which services should be checked and confirmed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c</code></td>
<td>Check the Connector service status.</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Display the help text.</td>
</tr>
<tr>
<td><code>-r</code></td>
<td>Check the replication services status.</td>
</tr>
</tbody>
</table>

The command outputs information in the following format:

```
LEVEL: DETAIL
```

Where DETAIL includes detailed information about the status report, and LEVEL is:

- **CRITICAL** — status is critical and requires immediate attention.

  For example:

  ```
  CRITICAL: Replicator is not running
  ```
• OK — status is OK.

For example:

```
OK: All services (Replicator) are online
```

This output is easily parseable by various monitoring tools, including Nagios NRPE, and can be used to monitor the status of your services quickly without restoring to using the full `trepctl` output.

**Note**

The `check_tungsten_services` only confirms that the services and processes are running; their state is not confirmed. To check state with a similar interface, use the `check_tungsten_online` command.

To check the services:

• To check the replicator services:

```
shell> check_tungsten_services -r
OK: All services (Replicator) are online
```

• To check the replicator and manager services are executing:

```
shell> check_tungsten_services -r
OK: All services (Replicator, Manager) are running
```

• To check the connector services:

```
shell> check_tungsten_services -c
OK: All services (Replicator) are online
```

### 8.6. The `cluster_backup` Command

The `cluster_backup` command provides a simple mechanism to execute a Tungsten Replicator backup inside of the cluster. It is designed to be called manually or as part of `cron`. The command should be added to `cron` on every server. When started, the command will check if the server is the current coordinator for the cluster. If not, the command will exit without an error. This design ensures that the command will only run on one server in the cluster.

The command supports command-line options that allow you to alter how and where the backup is executed.

```
cluster_backup
```

Where:

After the command confirms the current server is the coordinator, it will attempt to find a datasource to backup. Unless `--require-slave-backup` has been disabled, only slaves that are `ONLINE` will be eligible. If no datasource can be found, the command will exit with an error. The backup will then be started on the datasource.

The `cluster_backup` command will wait until the `cctrl` command has returned before exiting. The `cctrl` command can return prior to the backup is completed if it takes too long or if there is another error. The `tungsten_nagios_backups` check or similar should be used to make sure that you always have a recent backup available in the cluster.

See Section 5.9.2, “Automating Backups” for more information.

For example:

```
shell> crontab -l
00 00 * * * /opt/continuent/tungsten/cluster-home/bin/cluster_backup >>/opt/continuent/service_logs/cluster_backup.log 2>&1
```

All output will be sent to `/opt/continuent/service_logs/cluster_backup.log`.

### 8.7. The `connector` Command

The `connector` is the wrapper script that handles the execution of the connector service.

**Table 8.17. `connector` Commands**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>client-list</code> [235]</td>
<td>Return a list of the current client connections through this connector.</td>
</tr>
<tr>
<td><code>condrestart</code> [235]</td>
<td>Restart only if already running</td>
</tr>
</tbody>
</table>
### Command-line Tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console [235]</td>
<td>Launch in the current console (instead of a daemon)</td>
</tr>
<tr>
<td>dump [235]</td>
<td>Request a Java thread dump (if connector is running)</td>
</tr>
<tr>
<td>graceful-stop [seconds] [235]</td>
<td>Stops the connector gracefully, allowing outstanding open connections to finish and close before the connector process is stopped. (seconds) is an integer of zero or more, and is required. The connector will shut down immediately if there are no active connections. Specifying zero (0) will cause a shutdown without waiting for connections to terminate.</td>
</tr>
<tr>
<td>install [236]</td>
<td>Install the service to automatically start when the system boots</td>
</tr>
<tr>
<td>reconfigure [236]</td>
<td>Reconfigure the connector by forcing the connector to reread the configuration, including the configuration files and user.map.</td>
</tr>
<tr>
<td>remove [236]</td>
<td>Remove the service from starting during boot</td>
</tr>
<tr>
<td>restart [236]</td>
<td>Stop connector if already running and then start</td>
</tr>
<tr>
<td>start [236]</td>
<td>Start in the background as a daemon process</td>
</tr>
<tr>
<td>status [236]</td>
<td>Query the current status</td>
</tr>
<tr>
<td>stop [236]</td>
<td>Stop if running (whether as a daemon or in another console)</td>
</tr>
</tbody>
</table>

These commands and options are described below:

- **client-list [235]**

Lists all ongoing connections with origin, local and remote (mysql data source) IPs/ports

```
shell> connector client-list
Executing Tungsten Connector Service --client-list ...
+----------------------+---------------------+----------------------+------------------------+
<table>
<thead>
<tr>
<th>Client</th>
<th>Connector Inbound</th>
<th>Connector Outbound</th>
<th>Data Source</th>
</tr>
</thead>
</table>
+---------------------+---------------------+---------------------+-------------|
Done Tungsten Connector Service --client-list
```

- **condrestart [235]**

Restart the connector, only if it is already running. This can be useful to use when changing configuration or performing database management within automated scripts, as the connector will be only be restart if it was previously running.

For example, if the connector is running, **connector condrestart [235]** operates as **connector restart**:

```
shell> connector condrestart
Stopping Tungsten Connector Service... Waiting for Tungsten Connector Service to exit... Stopped Tungsten Connector Service. Starting Tungsten Connector Service... Waiting for Tungsten Connector Service...... running: PID:26646
```

However, if not already running, the operation does nothing:

```
shell> connector condrestart
Stopping Tungsten Connector Service... Tungsten Connector Service was not running.
```

- **console [235]**

Launch in the current console (instead of a daemon)

- **dump [235]**

Request a Java thread dump (if connector is running)

- **graceful-stop [seconds] [235]**

Stops the connector gracefully, allowing outstanding open connections to finish and close before the connector process is stopped. (seconds) is an integer of zero or more, and is required. The connector will shut down immediately if there are no active connections. Specifying zero (0) will cause a shutdown without waiting for connections to terminate.
### Command-line Tools

- **install**
  Installs the startup scripts for running the connector at boot. For an alternative method of deploying these start-up scripts, see `deployall`.

- **reconfigure**
  Reloads the configuration without touching existing connections. New configuration only applies to new connections. Note that this command won't work for the following settings: `connection.keepAlive.interval`, `connection.keepAlive.timeout`, `server.listen.address`, `server.port`, `server.portbinding.timeout`, `server.portbinding.retry.delay` (when reaching `server.max_connections` only)

- **remove**
  Removes the startup scripts for running the connector at boot. For an alternative method of removing these start-up scripts, see `undeployall`.

- **restart**
  Stops the connector, if it is already running, and then restarts it:
  ```
  shell> connector restart
  Stopping Tungsten Connector Service...
  Stopped Tungsten Connector Service.
  Starting Tungsten Connector Service......
  running: PID:26248
  ```

- **start**
  To start the connector service if it is not already running:
  ```
  shell> connector start
  Starting Tungsten Connector Service...
  ```

- **status**
  Checks the execution status of the connector:
  ```
  shell> connector status
  Tungsten Connector Service is running: PID:27015, Wrapper:STARTED, Java:STARTED
  ```

  If the connector is not running:
  ```
  shell> connector status
  Tungsten Connector Service is not running.
  ```

  This only provides the execution state of the connector, not the actual state of replication. To get detailed information on the status of replication use `trepctl status`.

- **stop**
  Stops the connector if it is already running:
  ```
  shell> connector stop
  Stopping Tungsten Connector Service...
  Waiting for Tungsten Connector Service to exit...
  Stopped Tungsten Connector Service.
  ```

### 8.8. The `ddlscan` Command

The `ddlscan` command scans the existing schema for a database or table and then generates a schema or file in a target database environment. For example, `ddlscan` is used in MySQL to Oracle heterogeneous deployments to translate the schema definitions within MySQL to the Oracle format. For more information on heterogeneous deployments, see Understanding Heterogeneous Deployments [in Tungsten Replicator 2.2 Manual].

For example, to generate Oracle DDL from an existing MySQL database:

```bash
```

SQL generated on Thu Sep 11 15:39:06 BST 2014 by ./ddlscan utility of Tungsten

```bash
url = jdbc:mysql:thin://host1:13306/test
user = tungsten
dbName = test
```
The format of the command is:


The available options are as follows:

**Table 8.18. ddlsan Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-conf path [237]</td>
<td>Path to a static-{svc}.properties file to read JDBC connection address and credentials</td>
</tr>
<tr>
<td>-db db [237]</td>
<td>Database to use [will substitute ${DBNAME} in the URL, if needed]</td>
</tr>
<tr>
<td>-opt opt val [238]</td>
<td>Option(s) to pass to template, try: -opt help me</td>
</tr>
<tr>
<td>-out file [238]</td>
<td>Render to file [print to stdout if not specified]</td>
</tr>
<tr>
<td>-pass secret [237]</td>
<td>JDBC password</td>
</tr>
<tr>
<td>-path path [238]</td>
<td>Add additional search path for loading Velocity templates</td>
</tr>
<tr>
<td>-rename file [238]</td>
<td>Definitions file for renaming schemas, tables and columns</td>
</tr>
<tr>
<td>-service name [237]</td>
<td>Name of a replication service instead of path to config</td>
</tr>
<tr>
<td>-tableFile file</td>
<td>New-line separated definitions file of tables to find</td>
</tr>
<tr>
<td>-tables regex [238]</td>
<td>Comma-separated list of tables to find</td>
</tr>
<tr>
<td>-template file [237]</td>
<td>Specify template file to render</td>
</tr>
<tr>
<td>-url jdbcUrl [237]</td>
<td>JDBC connection string (use single quotes to escape)</td>
</tr>
<tr>
<td>-user user [237]</td>
<td>JDBC username</td>
</tr>
</tbody>
</table>

**ddlsan** supports three different methods for execution:

- Using an explicit JDBC URL, username and password:

  ```shell```
  ddlsan -user tungsten -url 'jdbc:mysql:thin://tr-hadoop1:13306/test' -user user -pass password ...
  ```shell```

  This is useful when a deployment has not already been installed.

- By specifying an explicit configuration file:

  ```shell```
  ddlsan -conf /opt/continuent/tungsten/tungsten-replicator/conf/static-alpha.properties ...
  ```shell```

- When an existing deployment has been installed, by specifying one of the active services:

  ```shell```
  ddlsan -service alpha ...
  ```shell```

In addition, the following two options must be specified on the command-line:

- The template to be used (using the -template [237] option) for the DDL translation must be specified on the command-line. A list of the support templates and their operation are available in Table 8.19, “ddlsan Supported Templates”.

- The -db [237] parameter, which defines the database or schema that should be scanned. All tables are translated unless an explicit list, regex, or table file has been specified.

For example, to translate MySQL DDL to Oracle for all tables within the schema test using the connection to MySQL defined in the service alpha:

```shell```
  ddlsan -service alpha -template ddl-mysql-oracle.vm -db test
  ```shell```

**ddlsan** provides a series of additional command-line options, and a full list of the available templates.
8.8.1. Optional Arguments

The following arguments are optional:

- `-tables` [238]
- `-rename` [238]

A list of table renames which will be taken into account when generating target DDL. The format of the table matches the format of the `rename` filter.

- `-path` [238]

The path to additional Velocity templates to be searched when specifying the template name.

- `-opt` [238]

An additional option (and variable) which are supplied to be used within the template file. Different template files may support additional options for specifying alternative information, such as schema names, file locations and other values.

```
$ shell> ddlscan -service alpha -template ddl-mysql-oracle.vm -db test -opt schemaPrefix mysql_
```

- `-out` [238]

Sends the generated DDL output to a file, in place of sending it to standard output.

- `-help` [238]

Generates the help text of arguments.

8.8.2. Supported Templates and Usage

Table 8.19. `ddlscan` Supported Templates

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ddl-check-pkeys.vm</code></td>
<td>Reports which tables are without primary key definitions</td>
</tr>
<tr>
<td><code>ddl-mysql-hive-0.10.vm</code></td>
<td>Generates DDL from a MySQL host suitable for the base tables in a Hadoop/Hive Environment</td>
</tr>
<tr>
<td><code>ddl-mysql-hive-0.10-staging.vm</code></td>
<td>Generates DDL from a MySQL host suitable for the staging tables in a Hadoop/Hive Environment</td>
</tr>
<tr>
<td><code>ddl-mysql-hive-metadata.vm</code></td>
<td>Generates metadata as JSON to be used within a Hadoop/Hive Environment</td>
</tr>
<tr>
<td><code>ddl-mysql-oracle.vm</code></td>
<td>Generates Oracle schema from a MySQL schema</td>
</tr>
<tr>
<td><code>ddl-mysql-oracle-cdc.vm</code></td>
<td>Generates Oracle tables with CDC capture information from a MySQL schema</td>
</tr>
<tr>
<td><code>ddl-mysql-vertica.vm</code></td>
<td>Generates DDL suitable for the base tables in HP Vertica</td>
</tr>
<tr>
<td><code>ddl-mysql-vertica-staging.vm</code></td>
<td>Generates DDL suitable for the staging tables in HP Vertica</td>
</tr>
<tr>
<td><code>ddl-oracle-mysql.vm</code></td>
<td>Generates DDL for MySQL tables from an Oracle schema</td>
</tr>
<tr>
<td><code>ddl-oracle-mysql-pk-only.vm</code></td>
<td>Generates Primary Key DDL statements from an Oracle database for MySQL</td>
</tr>
</tbody>
</table>

8.8.2.1. `ddl-check-pkeys.vm`

The `ddl-check-pkeys.vm` template can be used to check whether specific tables within a schema do not have a primary key:

```
$ shell> ddlscan -service alpha -template ddl-check-pkeys.vm \
    -db sales \
    -url jdbc:mysql://localhost:13306/sales
```

/* SQL generated on Thu Sep 04 18:23:52 BST 2014 by ./ddlscan utility of Tungsten */

```
url = jdbc:mysql://localhost:13306/sales
user = tungsten
```

/* ERROR: sales.dummy1 has no primary key! */
For certain environments, particularly heterogeneous replication, the lack of primary keys can lead to inefficient replication, or even fail to replicate data at all.

### 8.8.2.2. `ddl-mysql-hive-0.10.vm`

Generates DDL suitable for a carbon-copy form of the table from the MySQL host:

```
shell> ddlscan -user tungsten -url 'jdbc:mysql://tr-hadoop1:13306/test' -pass password \
    -template ddl-mysql-hive-0.10.vm -db test
```

```
DROP TABLE IF EXISTS test.sales;
CREATE TABLE test.sales
(
    id INT,
    salesman STRING,
    planet STRING,
    value DOUBLE
);
```

Wherever possible, the closest Hive equivalent datatype is used for each source datatype, as follows:

<table>
<thead>
<tr>
<th>MySQL Datatype</th>
<th>Hive Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATETIME</td>
<td>STRING</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>TIMESTAMP</td>
</tr>
<tr>
<td>DATE</td>
<td>STRING</td>
</tr>
<tr>
<td>YEAR</td>
<td>INT</td>
</tr>
<tr>
<td>TIME</td>
<td>STRING</td>
</tr>
<tr>
<td>TINYINT</td>
<td>TINYINT</td>
</tr>
<tr>
<td>SMALLINT</td>
<td>SMALLINT</td>
</tr>
<tr>
<td>SMALLINT UNSIGNED</td>
<td>SMALLINT</td>
</tr>
<tr>
<td>MEDIUMINT</td>
<td>INT</td>
</tr>
<tr>
<td>INT</td>
<td>INT</td>
</tr>
<tr>
<td>INT UNSIGNED</td>
<td>BIGINT</td>
</tr>
<tr>
<td>BIGINT</td>
<td>BIGINT</td>
</tr>
<tr>
<td>BIGINT UNSIGNED</td>
<td>STRING</td>
</tr>
<tr>
<td>DECIMAL</td>
<td>STRING</td>
</tr>
<tr>
<td>VARCHAR</td>
<td>STRING</td>
</tr>
<tr>
<td>CHAR</td>
<td>STRING</td>
</tr>
<tr>
<td>BINARY</td>
<td>BINARY</td>
</tr>
<tr>
<td>VARBINARY</td>
<td>BINARY</td>
</tr>
</tbody>
</table>
The template supports the following optional parameters to change behavior:

- **-opt schemaPrefix**
  A prefix to be placed in front of all schemas. For example, if called with `schemaPrefix` set to `mysql_`:
  ```shell```
  shell> ddlscan ... -opt schemaPrefix mysql_
  ```
  The schema name will be prefixed, translating the schema name from `sales` into `mysql_sales`.

- **-opt tablePrefix**
  A prefix to be placed in front of all schemas. For example, if called with `tablePrefix` set to `mysql_`:
  ```shell```
  shell> ddlscan ... -opt tablePrefix mysql_
  ```
  The table name will be prefixed, translating the tablename from `sales` into `mysql_sales`.

### 8.8.2.3. `ddl-mysql-hive-0.10-staging.vm`

Staging tables within Hive define the original table columns with additional columns to track the operation type, sequence number, timestamp and unique key for each row. For example, the table `sales` in MySQL:

```sql```
mysql> describe sales;
+----------+----------+------+-----+---------+----------------+
| Field    | Type     | Null | Key | Default | Extra           |
+----------+----------+------+-----+---------+----------------+
| id       | int(11)  | NO   | PRI | NULL    | auto_increment  |
| salesman  | char(20) | YES  |     | NULL    |                |
| planet    | char(20) | YES  |     | NULL    |                |
| value     | float    | YES  |     | NULL    |                |
+----------+----------+------+-----+---------+----------------+
4 rows in set (0.00 sec)
```

Generates the following Hive-compatible DDL when using this template:

```sql```
```
DROP TABLE IF EXISTS test.stage_xxx_sales;
CREATE EXTERNAL TABLE test.stage_xxx_sales
(
  tungsten_opcode STRING ,
  tungsten_seqno INT ,
  tungsten_row_id INT ,
  tungsten_commit_timestamp TIMESTAMP ,
  id INT ,
  salesman STRING ,
  planet STRING ,
  value DOUBLE
) ROW FORMAT DELIMITED FIELDS TERMINATED BY '|' ESCAPED BY '\'|' LINES TERMINATED BY '\n'
STORED AS TEXTFILE LOCATION '/user/tungsten/staging/test/sales';
```
```
Wherever possible, the closest Hive equivalent datatype is used for each source datatype, see `ddl-mysql-hive-0.10.vm` for more information.
```
8.8.2.4. ddl-mysql-hive-metadata.vm

The Hadoop tools require information about the schema in JSON format so that the table names and primary key information can be used when materializing data from the staging tables into the base tables. This template generates that information in JSON format:

```shell
ddlscan -user tungsten -url 'jdbc:mysql://tr-hadoop1:13306/test' -pass password \
-template $template -db test
```

```json
{
  "tables": [
    {
      "schema": "test",
      "name": "sales",
      "keys": ["id"],
      "columns": [
        {"name": "id", "type": "INT"},
        {"name": "salesman", "type": "STRING"},
        {"name": "planet", "type": "STRING"},
        {"name": "value", "type": "DOUBLE"}
      ]
    }
  ]
}
```

8.8.2.5. ddl-mysql-oracle.vm

When translating MySQL tables to Oracle compatible schema, the following datatypes are migrated to their closest Oracle equivalent:

<table>
<thead>
<tr>
<th>MySQL Datatype</th>
<th>Oracle Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>INT</td>
<td>NUMBER(10, 0)</td>
</tr>
<tr>
<td>BIGINT</td>
<td>NUMBER(19, 0)</td>
</tr>
<tr>
<td>TINYINT</td>
<td>NUMBER(3, 0)</td>
</tr>
<tr>
<td>SMALLINT</td>
<td>NUMBER(5, 0)</td>
</tr>
<tr>
<td>MEDIUMINT</td>
<td>NUMBER(7, 0)</td>
</tr>
<tr>
<td>DECIMAL(x,y)</td>
<td>NUMBER(x, y)</td>
</tr>
<tr>
<td>FLOAT</td>
<td>FLOAT</td>
</tr>
<tr>
<td>CHAR(n)</td>
<td>CHAR(n)</td>
</tr>
<tr>
<td>VARCHAR(n)</td>
<td>VARCHAR2(n) (n &lt;= 2000), CLOB (n &gt; 2000)</td>
</tr>
<tr>
<td>DATE</td>
<td>DATE</td>
</tr>
<tr>
<td>DATETIME</td>
<td>DATE</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>DATE</td>
</tr>
<tr>
<td>TEXT</td>
<td>CLOB</td>
</tr>
<tr>
<td>BLOB</td>
<td>BLOB</td>
</tr>
<tr>
<td>ENUM(...)</td>
<td>VARCHAR(255)</td>
</tr>
<tr>
<td>ENUM(...)</td>
<td>VARCHAR(4000)</td>
</tr>
<tr>
<td>BIT(1)</td>
<td>NUMBER(1)</td>
</tr>
</tbody>
</table>

The following additional transformations happen automatically:

- Table names are translated to uppercase.
- Column names are translated to uppercase.
- If a column name is a reserved word in Oracle, then the column name has an underscore character appended [for example, `TABLE` becomes `TABLE_`].

In addition to the above translations, errors will be raised for the following conditions:

- If the table name starts with a number.
- If the table name exceeds 30 characters in length.
- If the table name is a reserved word in Oracle.
Command-line Tools

Warnings will be raised for the following conditions:

- If the column or column name started with a number.
- If the column name exceeds 30 characters in length, the column name will be truncated.
- If the column name is a reserved word in Oracle.

8.8.2.6. *ddl-mysql-oracle-cdc.vm*

The *ddl-mysql-oracle-cdc.vm* template generates identical tables in Oracle, from their MySQL equivalent, but with additional columns for CDC capture. For example:

```
shell> ddlscan -user tungsten -url 'jdbc:mysql://tr-hadoop1:13306/test' -pass password "template ddl-mysql-oracle-cdc.vm -db test
/
url = jdbc:mysql://tr-hadoop1:13306/test
user = tungsten
dbName = test
*/
DROP TABLE test.sales;
CREATE TABLE test.sales
(id NUMBER(10, 0) NOT NULL,
salesman CHAR,
planet CHAR,
value FLOAT,
CDC_OP_TYPE VARCHAR(1), /* CDC column */
CDC_TIMESTAMP TIMESTAMP, /* CDC column */
CDC_SEQUENCE_NUMBER NUMBER PRIMARY KEY /* CDC column */);
```

For information on the datatypes translated, see *ddl-mysql-oracle.vn*.

8.8.2.7. *ddl-mysql-vertica.vm*

The *ddl-mysql-vertica.vm* template generates DDL for generating tables within an HP Vertica database from an existing MySQL database schema. For example:

```
shell> ddlscan -user tungsten -url 'jdbc:mysql://tr-hadoop1:13306/test' -pass password "template ddl-mysql-vertica.vm -db test
/
url = jdbc:mysql://tr-hadoop1:13306/test
user = tungsten
dbName = test
*/
CREATE SCHEMA test;
DROP TABLE test.sales;
CREATE TABLE test.sales
(id INT ,
salesman CHAR(20) ,
planet CHAR(20) ,
value FLOAT ) ORDER BY id;
```

Because Vertica does not explicitly support primary keys, a default projection for the key order is created based on the primary key of the source table.

The templates translates different datatypes as follows:

<table>
<thead>
<tr>
<th>MySQL Datatype</th>
<th>Vertica Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATETIME</td>
<td>DATETIME</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>TIMESTAMP</td>
</tr>
<tr>
<td>DATE</td>
<td>DATE</td>
</tr>
<tr>
<td>TIME</td>
<td>TIME</td>
</tr>
<tr>
<td>TINYINT</td>
<td>TINYINT</td>
</tr>
</tbody>
</table>
### MySQL Datatype | Vertica Datatype
---|---
SMALLINT | SMALLINT
MEDIUMINT | INT
INT | INT
BIGINT | INT
VARCHAR | VARCHAR
CHAR | CHAR
BINARY | BINARY
VARBINARY | VARBINARY
TEXT, TINYTEXT, MEDIUMTEXT, LONGTEXT | VARCHAR(65000)
BLOB, TINYBLOB, MEDIUMBLOB, LONGBLOB | VARBINARY(65000)
FLOAT | FLOAT
DOUBLE | DOUBLE PRECISION
ENUM | VARCHAR
SET | VARCHAR(4000)
BIT(1) | BOOLEAN
BIT | CHAR(64)

In addition, the following considerations should be taken into account:

- **DECIMAL**: MySQL type is not supported.
- **TEXT**: types in MySQL are converted to a VARCHAR in Vertica of the maximum supported size.
- **BLOB**: types in MySQL are converted to a VARBINARY in Vertica of the maximum supported size.
- **SET**: types in MySQL are converted to a VARCHAR in Vertica of 4000 characters, designed to work in tandem with the `settostring` filter.
- **ENUM**: types in MySQL are converted to a VARCHAR in Vertica of the size of the longest ENUM value, designed to work in tandem with the `enuntostring` filter.

#### 8.8.2.8. *ddl-mysql-vertica-staging.vm*

The *ddl-mysql-vertica-staging.vm* template generates DDL for HP Vertica staging tables. These include the full table definition, in addition to three columns used to define the staging data, including the operation code, sequence number and unique row ID. For example:

```shell
dlscanning -user tungsten -url 'jdbc:mysql://tr-hadoop1:13306/test' -pass password \
-template dml-mysql-vertica-staging.vm -db test
```

**CREATE SCHEMA test;**

**DROP TABLE test.stage_xxx_sales;**

**CREATE TABLE test.stage_xxx_sales**

```sql
(
  tungsten_opcode CHAR(1) ,
  tungsten_seqno INT ,
  tungsten_row_id INT ,
  id INT ,
  salesman CHAR(20) ,
  planet CHAR(20) ,
  value FLOAT ) ORDER BY tungsten_seqno, tungsten_row_id;
```

#### 8.8.2.9. *ddl-oracle-mysql.vm*

The *ddl-oracle-mysql.vm* template generates the DDL required to create a schema within MySQL based on the existing Oracle schema. For example:

```shell
dlscanning -service sales -template dml-oracle-mysql.vm -db sales
```
Command-line Tools

Columns are translated as follows:

<table>
<thead>
<tr>
<th>Oracle Datatype</th>
<th>MySQL Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE</td>
<td>DATETIME</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 19</td>
<td>INT</td>
</tr>
<tr>
<td>NUMBER(n) where n &gt; 19</td>
<td>BIGINT</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 3</td>
<td>TINYINT</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 5</td>
<td>SMALLINT</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 7</td>
<td>MEDIUMINT</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 10</td>
<td>INT</td>
</tr>
<tr>
<td>NUMBER(n) where n &lt; 19</td>
<td>BIGINT</td>
</tr>
<tr>
<td>NUMBER</td>
<td>DECIMAL</td>
</tr>
<tr>
<td>FLOAT</td>
<td>FLOAT</td>
</tr>
<tr>
<td>VARCHAR</td>
<td>VARCHAR</td>
</tr>
<tr>
<td>LONG</td>
<td>LONGTEXT</td>
</tr>
<tr>
<td>BFILE</td>
<td>VARCHAR(1024)</td>
</tr>
<tr>
<td>CHAR</td>
<td>CHAR</td>
</tr>
<tr>
<td>CLOB</td>
<td>LONGTEXT</td>
</tr>
<tr>
<td>BLOB</td>
<td>LONGBLOB</td>
</tr>
<tr>
<td>LONG RAW</td>
<td>LONGBLOB</td>
</tr>
<tr>
<td>TIMESTAMP</td>
<td>TIMESTAMP</td>
</tr>
<tr>
<td>RAW</td>
<td>VARBINARY</td>
</tr>
</tbody>
</table>

The following additional transformations happen automatically:

- If a column name is a reserved word in MySQL, then the column name has an underscore character appended (for example, TABLE becomes TABLE_)

An error is raised in the following conditions:

- If the size of a FLOAT is larger than 53 points of precision.

8.8.2.10. ddl-oracle-mysql-pk-only.vm

The ddl-oracle-mysql-pk-only.vm template generates alter table statements to add the primary key, as determined from the Oracle primary key or index information. For example:
Note that it does not generate table DDL, only statements to alter existing tables with primary key information.

8.9. The deployall Command

The `deployall` tool installs the required startup scripts into the correct location so that all required services can be automatically started and stopped during the startup and shutdown of your server.

To use, the tool should be executed with superuser privileges, either directly using `sudo`, or by logging in as the superuser and running the command directly:

```
shell> sudo deployall
```

```
Adding system startup for /etc/init.d/treplicator ...

/etc/rc0.d/K80treplicator -> ../init.d/treplicator
/etc/rc1.d/K80treplicator -> ../init.d/treplicator
/etc/rc6.d/K80treplicator -> ../init.d/treplicator
/etc/rc2.d/S80treplicator -> ../init.d/treplicator
/etc/rc3.d/S80treplicator -> ../init.d/treplicator
/etc/rc4.d/S80treplicator -> ../init.d/treplicator
/etc/rc5.d/S80treplicator -> ../init.d/treplicator
```

The startup scripts are added to the correct runlevels to enable operation during standard startup and shutdown levels.

See Section 4.3, “Configuring Startup on Boot”.

To remove the scripts from the system, use `undeployall`.

8.10. env.sh Script

8.11. The manager Command

The `manager` is the wrapper script that handles the execution of the manager service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>condrestart [245]</td>
<td>Restart only if already running</td>
</tr>
<tr>
<td>console [246]</td>
<td>Launch in the current console (instead of a daemon)</td>
</tr>
<tr>
<td>dump [246]</td>
<td>Request a Java thread dump [if manager is running]</td>
</tr>
<tr>
<td>install [246]</td>
<td>Install the service to automatically start when the system boots</td>
</tr>
<tr>
<td>remove [246]</td>
<td>Remove the service from starting during boot</td>
</tr>
<tr>
<td>restart [246]</td>
<td>Stop manager if already running and then start</td>
</tr>
<tr>
<td>start [246]</td>
<td>Start in the background as a daemon process</td>
</tr>
<tr>
<td>status [246]</td>
<td>Query the current status</td>
</tr>
<tr>
<td>stop [246]</td>
<td>Stop if running [whether as a daemon or in another console]</td>
</tr>
</tbody>
</table>

These commands and options are described below:

- condrestart [245]

Restart the manager, only if it is already running. This can be useful to use when changing configuration or performing database management within automated scripts, as the manager will be only be restart if it was previously running.

For example, if the manager is running, manager condrestart operates as `manager restart`: 
Command-line Tools

```
shell> manager condrestart
Stopping Tungsten Manager Service...
Waiting for Tungsten Manager Service to exit...
Stopped Tungsten Manager Service.
Starting Tungsten Manager Service...
Waiting for Tungsten Manager Service......
running: PID:26646
```

However, if not already running, the operation does nothing:

```
shell> manager condrestart
Stopping Tungsten Manager Service...
Tungsten Manager Service was not running.
```

- **console [246]**
  
  Launch in the current console (instead of a daemon)

- **dump [246]**
  
  Request a Java thread dump (if manager is running)

- **install [246]**
  
  Installs the startup scripts for running the manager at boot. For an alternative method of deploying these start-up scripts, see deployall.

- **remove [246]**
  
  Removes the startup scripts for running the manager at boot. For an alternative method of removing these start-up scripts, see undeployall.

- **restart [246]**
  
  **Warning**

  Restarting a running manager temporarily stops and restarts replication.

  Stops the manager, if it is already running, and then restarts it:

  ```
  shell> manager restart
  Stopping Tungsten Manager Service...
  Stopped Tungsten Manager Service.
  Starting Tungsten Manager Service...
  Waiting for Tungsten Manager Service......
  running: PID:26248
  ```

  - **start [246]**
    
    To start the manager service if it is not already running:

    ```
    shell> manager start
    Starting Tungsten Manager Service...
    ```

  - **status [246]**
    
    Checks the execution status of the manager:

    ```
    shell> manager status
    Tungsten Manager Service is running: PID:27815, Wrapper:STARTED, Java:STARTED
    ```

  If the manager is not running:

  ```
  shell> manager status
  Tungsten Manager Service is not running.
  ```

  This only provides the execution state of the manager, not the actual state of replication. To get detailed information on the status of replication use trepctl status.

  - **stop [246]**
    
    Stops the manager if it is already running:

    ```
    shell> manager stop
    Stopping Tungsten Manager Service...
    Waiting for Tungsten Manager Service to exit...
    Stopped Tungsten Manager Service.
    ```
If the cluster was configured with `auto-enable=false` then you will need to put each node online individually.

### 8.12. The multi_trepctl Command

The `multi_trepctl` command provides unified status and operation support across your Continuent Tungsten installation across multiple hosts without the need to run the `trepctl` command across multiple hosts and/or services individually.

```
multi_trepctl [ --by-service ] [ --fields-appliedLastSeqNo-appliedLatency-hostRole-serviceName-state ] [ --host, --hostsself ]
list [ --output=jsonlistname-yaml ] [ --path, --paths ] [ --role, --roles ]
run [ --service, --serviceself ] [ --skip-headers ] [ --sort-by ]
```

The default operation, with no further command-line commands or arguments displays the status of all the hosts and services identified as related to the current host. In a typical single-service deployment, the command outputs the status of all services by determining the relationship between hosts connected to the default service:

```shell
> multi_trepctl
<table>
<thead>
<tr>
<th>host</th>
<th>serviceName</th>
<th>role</th>
<th>state</th>
<th>appliedLastSeqNo</th>
<th>appliedLatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tr-ms1</td>
<td>alpha</td>
<td>master</td>
<td>ONLINE</td>
<td>54</td>
<td>0.861</td>
</tr>
<tr>
<td>tr-ms2</td>
<td>alpha</td>
<td>slave</td>
<td>ONLINE</td>
<td>54</td>
<td>1.945</td>
</tr>
<tr>
<td>tr-ms3</td>
<td>alpha</td>
<td>slave</td>
<td>ONLINE</td>
<td>54</td>
<td>42.851</td>
</tr>
</tbody>
</table>
```

On a server with multiple services, information is output for each service and host:

```shell
> multi_trepctl
<table>
<thead>
<tr>
<th>host</th>
<th>serviceName</th>
<th>role</th>
<th>state</th>
<th>appliedLastSeqNo</th>
<th>appliedLatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>east1</td>
<td>east</td>
<td>master</td>
<td>ONLINE</td>
<td>64</td>
<td>0.008</td>
</tr>
<tr>
<td>west1</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>-1</td>
<td>-1.000</td>
</tr>
<tr>
<td>west2</td>
<td>west</td>
<td>master</td>
<td>ONLINE</td>
<td>294328</td>
<td>0.319</td>
</tr>
<tr>
<td>west3</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>231595</td>
<td>119.834</td>
</tr>
<tr>
<td>west3</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>231595</td>
<td>22.895</td>
</tr>
</tbody>
</table>
```

### 8.12.1. multi_trepctl Options

The `multi_trepctl` tool provides a number of options that control the information and detail output when the command is executed.

**Table 8.21. multi_trepctl Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--by-service</td>
<td>Sort the output by the service name</td>
</tr>
<tr>
<td>--fields</td>
<td>Fields to be output during during summary</td>
</tr>
<tr>
<td>--host, --hosts</td>
<td>Host or hosts on which to limit output</td>
</tr>
<tr>
<td>--output</td>
<td>Specify the output format</td>
</tr>
<tr>
<td>--paths, --path</td>
<td>Directory or directories to check when looking for tools</td>
</tr>
<tr>
<td>--role, --roles</td>
<td>Role or roles on which to limit output</td>
</tr>
<tr>
<td>--service, --services</td>
<td>Service or services on which to limit output</td>
</tr>
<tr>
<td>--skip-headers</td>
<td>Skip the headers</td>
</tr>
<tr>
<td>--sort-by</td>
<td>Sort by a specified field</td>
</tr>
</tbody>
</table>

Where:

- `--by-service [247]`

Order the output according to the service name and role within the service:

```shell
> multi_trepctl --by-service
<table>
<thead>
<tr>
<th>host</th>
<th>serviceName</th>
<th>role</th>
<th>state</th>
<th>appliedLastSeqNo</th>
<th>appliedLatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>east1</td>
<td>east</td>
<td>master</td>
<td>ONLINE</td>
<td>53</td>
<td>0.008</td>
</tr>
<tr>
<td>east2</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>64</td>
<td>68.889</td>
</tr>
<tr>
<td>west1</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>64</td>
<td>68.970</td>
</tr>
<tr>
<td>west2</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>64</td>
<td>61.097</td>
</tr>
<tr>
<td>west3</td>
<td>east</td>
<td>slave</td>
<td>ONLINE</td>
<td>294328</td>
<td>8.319</td>
</tr>
<tr>
<td>west3</td>
<td>west</td>
<td>master</td>
<td>ONLINE</td>
<td>231595</td>
<td>8.316</td>
</tr>
<tr>
<td>east3</td>
<td>west</td>
<td>slave</td>
<td>ONLINE</td>
<td>231595</td>
<td>22.855</td>
</tr>
</tbody>
</table>
```
• **--fields [248]**

Limited the output to the specified list of fields from the output of fields output by `trepctl`. For example, to limit the output to the host, role, and `appliedlatency`:

```
shell> multi_trepctl --fields=host,role,appliedlatency
```

<table>
<thead>
<tr>
<th>host</th>
<th>role</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tr-ms1</td>
<td>master</td>
<td>0.524</td>
</tr>
<tr>
<td>tr-ms2</td>
<td>slave</td>
<td>0.000</td>
</tr>
<tr>
<td>tr-ms3</td>
<td>slave</td>
<td>-1.000</td>
</tr>
</tbody>
</table>

• **--host [248], --hosts [248]**

Limit the output to the host, or a comma-separated list of hosts specified. For example:

```
shell> multi_trepctl --hosts=tr-ms1,tr-ms3
```

<table>
<thead>
<tr>
<th>host</th>
<th>servicename</th>
<th>role</th>
<th>state</th>
<th>appliedlastseqno</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tr-ms1</td>
<td>alpha</td>
<td>master</td>
<td>ONLINE</td>
<td>2322</td>
<td>0.524</td>
</tr>
<tr>
<td>tr-ms3</td>
<td>alpha</td>
<td>slave</td>
<td>OFFLINE:ERROR</td>
<td>-1</td>
<td>-1.000</td>
</tr>
</tbody>
</table>

• **--output [248]**

Specify the output format.

<table>
<thead>
<tr>
<th>Option</th>
<th>--output [248]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Specify the output format</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Default</td>
<td>info</td>
</tr>
<tr>
<td>Valid Values</td>
<td>json (JSON format), list (List format), name (Name [simplified text] format), tab (Tab-delimited format), yam (YAML format)</td>
</tr>
</tbody>
</table>

For example, to output the current status in JSON format:

```
shell> multi_trepctl --output json
```

```json
{
  ...
  "appliedlastseqno": 2322,
  "appliedlatency": 0.524,
  "host": "tr-ms1",
  "role": "master",
  "servicename": "alpha",
  "state": "ONLINE"
  ...
}
```

• **--path [248], --paths [248]**

Limit the search for `trepctl` to the specified path or comma-separated list of paths. On a deployment with multiple services, the output will be limited by the services installed within the specified directories:

```
shell> multi_trepctl --path /opt/replicator
```

<table>
<thead>
<tr>
<th>host</th>
<th>servicename</th>
<th>role</th>
<th>state</th>
<th>appliedlastseqno</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This is also useful when control of cross-site replicators is desired in MSMM topologies prior to v6.0.0.

For example, take all cross-site replicators offline:

```shell
shell> multi_trepctl --path /opt/replicator offline
```

To bring all cross-site replicators online:

```shell
shell> multi_trepctl --path /opt/replicator online
```

- `--role`, `--roles`

Limit the output to show only the specified role or comma-separated list of roles:

```shell
shell> multi_trepctl --roles=slave
```

- `--service`, `--services`

Limit the output to the specified service or comma-separated list of services:

```shell
shell> multi_trepctl --service=east
```

- `--skip-headers`

Prevents the generation of the headers when generating the list output format:

```shell
shell> multi_trepctl --skip-headers
```

- `--sort-by`

Sort by the specified fieldname. For example, to sort the output by the latency:

```shell
shell> multi_trepctl --sort-by appliedlatency
```

### 8.12.2. `multi_trepctl` Commands

The default operational mode is for `multi_trepctl list` to output the status. A specific mode can be also be specified on the command-line.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>List the information about each service</td>
</tr>
<tr>
<td>run</td>
<td>Run the specified trepctl command on all hosts/services</td>
</tr>
</tbody>
</table>

In addition to the two primary commands, `multi_trepctl` can execute commands that would normally be applied to `trepctl`, running them on each selected host, service or directory according to the options. The output format and expectation is controlled through the `list` and `run` commands.

For example:

```shell
shell> multi_trepctl status
```

Outputs the long form of the status information [as per `trepctl status`] for each identified host.
8.12.2.1. multi_trepctl list Command

The multi_trepctl list mode is the default mode for multi_trepctl and outputs the current status across all hosts and services as a table:

```
$ multi_trepctl
<table>
<thead>
<tr>
<th>host</th>
<th>servicename</th>
<th>role</th>
<th>state</th>
<th>appliedlastseqno</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1</td>
<td>firstrep</td>
<td>master</td>
<td>OFFLINE:ERROR</td>
<td>-1</td>
<td>-1.000</td>
</tr>
<tr>
<td>host2</td>
<td>firstrep</td>
<td>slave</td>
<td>GOING-ONLINE:SYNCHRONIZING</td>
<td>5271</td>
<td>4656.264</td>
</tr>
<tr>
<td>host3</td>
<td>firstrep</td>
<td>slave</td>
<td>OFFLINE:ERROR</td>
<td>-1</td>
<td>-1.000</td>
</tr>
<tr>
<td>host4</td>
<td>firstrep</td>
<td>slave</td>
<td>OFFLINE:ERROR</td>
<td>-1</td>
<td>-1.000</td>
</tr>
</tbody>
</table>
```

Or selected hosts and services if options are specified. For example, to get the status only for host1 and host2:

```
$ multi_trepctl --hosts=host1,host2
<table>
<thead>
<tr>
<th>host</th>
<th>servicename</th>
<th>role</th>
<th>state</th>
<th>appliedlastseqno</th>
<th>appliedlatency</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1</td>
<td>firstrep</td>
<td>master</td>
<td>ONLINE</td>
<td>5277</td>
<td>0.476</td>
</tr>
<tr>
<td>host2</td>
<td>firstrep</td>
<td>slave</td>
<td>ONLINE</td>
<td>5277</td>
<td>0.000</td>
</tr>
</tbody>
</table>
```

The multi_trepctl command implies that the status or information is being output from each of the commands executed on the remote hosts and services.

8.12.2.2. multi_trepctl run Command

The multi_trepctl run command can be used where the output of the corresponding trepctl command cannot be formatted into a convenient list. For example, to execute a backup on every host within a deployment:

```
$ multi_trepctl run backup
```

The same filters and host or service selection can also be made:

```
$ multi_trepctl run backup --hosts=host1,host2,host3
```

Return from the command will only take place when remote commands on each host have completed and returned.

8.13. The replicator Command

The replicator is the wrapper script that handles the execution of the replicator service.

Table 8.24. replicator Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>condrestart [250]</td>
<td>Restart only if already running</td>
</tr>
<tr>
<td>console [251]</td>
<td>Launch in the current console (instead of a daemon)</td>
</tr>
<tr>
<td>dump [251]</td>
<td>Request a Java thread dump (if replicator is running)</td>
</tr>
<tr>
<td>install [251]</td>
<td>Install the service to automatically start when the system boots</td>
</tr>
<tr>
<td>remove [251]</td>
<td>Remove the service from starting during boot</td>
</tr>
<tr>
<td>restart [251]</td>
<td>Stop replicator if already running and then start</td>
</tr>
<tr>
<td>start [251]</td>
<td>Start in the background as a daemon process</td>
</tr>
<tr>
<td>status [252]</td>
<td>Query the current status</td>
</tr>
<tr>
<td>stop [252]</td>
<td>Stop if running (whether as a daemon or in another console)</td>
</tr>
</tbody>
</table>

These commands and options are described below:

- condrestart [250]
Table 8.25. **replicator** Commands Options for *condrestart* [250]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offline</td>
<td>Start in OFFLINE state</td>
</tr>
</tbody>
</table>

Restart the replicator, only if it is already running. This can be useful to use when changing configuration or performing database management within automated scripts, as the replicator will be only be restart if it was previously running.

For example, if the replicator is running, *replicator condrestart* operates as *replicator restart*:

```shell
shell> replicator condrestart
Stopping Tungsten Replicator Service...
Waiting for Tungsten Replicator Service to exit...
Stopped Tungsten Replicator Service.
Starting Tungsten Replicator Service...
Waiting For Tungsten Replicator Service......
running: PID:26646
```

However, if not already running, the operation does nothing:

```shell
shell> replicator condrestart
Stopping Tungsten Replicator Service...
Tungsten Replicator Service was not running.
```

Table 8.26. **replicator** Commands Options for *console* [251]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offline</td>
<td>Start in OFFLINE state</td>
</tr>
</tbody>
</table>

Launch in the current console (instead of a daemon)

- **dump** [251]

Request a Java thread dump (if replicator is running)

- **install** [251]

Installs the startup scripts for running the replicator at boot. For an alternative method of deploying these start-up scripts, see *deployall*.

- **remove** [251]

Removes the startup scripts for running the replicator at boot. For an alternative method of removing these start-up scripts, see *undeployall*.

- **restart** [251]

Table 8.27. **replicator** Commands Options for *restart* [251]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offline</td>
<td>Stop and restart in OFFLINE state</td>
</tr>
</tbody>
</table>

**Warning**

Restarting a running replicator temporarily stops and restarts replication.

Stops the replicator, if it is already running, and then restarts it:

```shell
shell> replicator restart
Stopping Tungsten Replicator Service...
Stopped Tungsten Replicator Service.
Starting Tungsten Replicator Service...
Waiting for Tungsten Replicator Service......
running: PID:26248
```

- **start** [251]

Table 8.28. **replicator** Commands Options for *start* [251]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offline</td>
<td>Start in OFFLINE state</td>
</tr>
</tbody>
</table>
To start the replicator service if it is not already running:

```bash
shell> replicator start
Starting Tungsten Replicator Service...
```

− status [252]

Checks the execution status of the replicator:

```bash
shell> replicator status
Tungsten Replicator Service is running: PID:27015, Wrapper:STARTED, Java:STARTED
```

If the replicator is not running:

```bash
shell> replicator status
Tungsten Replicator Service is not running.
```

This only provides the execution state of the replicator, not the actual state of replication. To get detailed information on the status of replication use `trepctl status`.

− stop [252]

Stops the replicator if it is already running:

```bash
shell> replicator stop
Stopping Tungsten Replicator Service...
Waiting for Tungsten Replicator Service to exit...
Stopped Tungsten Replicator Service.
```

If the cluster was configured with `auto-enable=false` then you will need to put each node online individually.

### 8.14. The setupCDC.sh Command

The `setupCDC.sh` script configures an Oracle database with the necessary CDC tables to enable heterogeneous replication from Oracle to MySQL.

The script accepts one argument, the filename of the configuration file that will define the CDC configuration. The file accepts the parameters as listed in Table 8.29, "setupCDC.conf Configuration Options".

**Table 8.29. setupCDC.conf Configuration Options**

<table>
<thead>
<tr>
<th>CmdLine Option</th>
<th>INI File Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdc_type</code> [252]</td>
<td><code>cdc_type</code> [252]</td>
<td>The CDC type to be used to extract data, either synchronous [using triggers] or asynchronous [using log processing].</td>
</tr>
<tr>
<td><code>delete_publisher</code> [253]</td>
<td><code>delete_publisher</code> [253]</td>
<td>Whether the publisher user should be deleted.</td>
</tr>
<tr>
<td><code>delete_subscriber</code> [253]</td>
<td><code>delete_subscriber</code> [253]</td>
<td>Whether the subscriber user should be deleted.</td>
</tr>
<tr>
<td><code>pub_password</code> [253]</td>
<td><code>pub_password</code> [253]</td>
<td>The publisher password that will be created for the CDC service.</td>
</tr>
<tr>
<td><code>pub_user</code> [253]</td>
<td><code>pub_user</code> [253]</td>
<td>The publisher user that will be created for this CDC service.</td>
</tr>
<tr>
<td><code>service</code> [253]</td>
<td><code>service</code> [253]</td>
<td>The service name of the Tungsten Replicator service that will be created.</td>
</tr>
<tr>
<td><code>source_user</code> [254]</td>
<td><code>source_user</code> [254]</td>
<td>The source schema user with rights to access the database.</td>
</tr>
<tr>
<td><code>specific_path</code> [254]</td>
<td><code>specific_path</code> [254]</td>
<td>The path where the tungsten.tables file is located; the file must be in a shared location accessible by Tungsten Replicator.</td>
</tr>
<tr>
<td><code>specific_tables</code> [254]</td>
<td><code>specific_tables</code> [254]</td>
<td>If enabled, extract only the tables defined within a tungsten.tables file.</td>
</tr>
<tr>
<td><code>sys_pass</code> [254]</td>
<td><code>sys_pass</code> [254]</td>
<td>The system password to connect to Oracle as SYSDBA.</td>
</tr>
<tr>
<td><code>sys_user</code> [254]</td>
<td><code>sys_user</code> [254]</td>
<td>The system user to connect to Oracle as SYSDBA.</td>
</tr>
<tr>
<td><code>tungsten_user</code> [255]</td>
<td><code>tungsten_user</code> [255]</td>
<td>The subscriber [Tungsten user] that will subscribe to the changes and read the information from the CDC tables.</td>
</tr>
</tbody>
</table>

Where:

− `cdc_type` [252]
<table>
<thead>
<tr>
<th>Option</th>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
<th>Valid Values</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdc_type</td>
<td>cdc_type</td>
<td>The CDC type to be used to extract data, either synchronous (using triggers)</td>
<td>string</td>
<td></td>
<td>Do not the delete the user before creation</td>
</tr>
<tr>
<td>delete_publisher</td>
<td>delete_publisher</td>
<td>Whether the publisher user should be deleted.</td>
<td>string</td>
<td>0</td>
<td>Do not the delete the user before creation</td>
</tr>
<tr>
<td>delete_subscriber</td>
<td>delete_subscriber</td>
<td>Whether the subscriber user should be deleted.</td>
<td>string</td>
<td>1</td>
<td>Delete the user before creation</td>
</tr>
<tr>
<td>pub_password</td>
<td>pub_password</td>
<td>The publisher password that will be created for the CDC service.</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pub_user</td>
<td>pub_user</td>
<td>The publisher user that will be created for this CDC service.</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>service</td>
<td>The service name of the Tungsten Replicator service that will be created.</td>
<td>string</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command-line Tools

- **source_user** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>source_user [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>source_user [254]</td>
</tr>
<tr>
<td>Description</td>
<td>The source schema user with rights to access the database.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The source schema user with rights to access the database.

- **specific_path** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>specific_path [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>specific_path [254]</td>
</tr>
<tr>
<td>Description</td>
<td>The path where the tungsten.tables file is located; the file must be in a shared location accessible by Tungsten Replicator.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The path where the tungsten.tables file is located; the file must be in a shared location accessible by Tungsten Replicator.

- **specific_tables** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>specific_tables [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>specific_tables [254]</td>
</tr>
<tr>
<td>Description</td>
<td>If enabled, extract only the tables defined within a tungsten.tables file.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>0: Extract all tables</td>
</tr>
<tr>
<td></td>
<td>1: Use a tables file to select tables</td>
</tr>
</tbody>
</table>

If enabled, extract only the tables defined within a tungsten.tables file.

- **sys_pass** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>sys_pass [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>sys_pass [254]</td>
</tr>
<tr>
<td>Description</td>
<td>The system password to connect to Oracle as SYSDBA.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The system password to connect to Oracle as SYSDBA.

- **sys_user** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>sys_user [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>sys_user [254]</td>
</tr>
<tr>
<td>Description</td>
<td>The system user to connect to Oracle as SYSDBA.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The system user to connect to Oracle as SYSDBA.

- **tungsten_pwd** [254]

<table>
<thead>
<tr>
<th>Option</th>
<th>tungsten_pwd [254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>tungsten_pwd [254]</td>
</tr>
<tr>
<td>Description</td>
<td>The password for the subscriber user.</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The password for the subscriber user.
8.15. The startall Command

The `startall` command will start all configured services within the configured directory:

```
# startall
Starting Tungsten Replicator Service...
Waiting for Tungsten Replicator Service..........
running: PID:2578
Starting Tungsten Manager Service...
Waiting for Tungsten Manager Service..........
running: PID:2722
Starting Tungsten Connector Service...
Waiting for Tungsten Connector Service..........
running: PID:2917
```

If a service is already running, then a notification of the current state will be provided:

```
Starting Tungsten Replicator Service...
Tungsten Replicator Service is already running.
```

Note that if any service is not running, and a suitable PID is found, the file will be deleted and the services started, for example:

```
Removed stale pid file:
/opt/continuent/releases/continuent-tungsten-2.0.5-11_pid25898/tungsten-connector/bin/../var/tconnector.pid
```

8.16. The stopall Command

The `stopall` command stops all running services if they are already running:

```
# stopall
Stopping Tungsten Connector Service...
Waiting for Tungsten Connector Service to exit...
Stopped Tungsten Connector Service.
Stopping Tungsten Manager Service...
Stopped Tungsten Manager Service.
Stopping Tungsten Replicator Service...
Waiting for Tungsten Replicator Service to exit...
Stopped Tungsten Replicator Service.
```

8.17. The thl Command

The `thl` command provides an interface to the THL data, including the ability to view the list of available files, details of the enclosed event information, and the ability to purge THL files to reclaim space on disk beyond the configured log retention policy.

The command supports two command-line options that are applicable to all operations, as shown in Table 8.30, “thl Options”.

Table 8.30. thl Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-conf path</td>
<td>Path to the configuration file containing the required replicator service configuration</td>
</tr>
<tr>
<td>-service servicename</td>
<td>Name of the service to be used when looking for THL information</td>
</tr>
</tbody>
</table>

For example, to execute a command on a specific service:

```
# thl index -service firstrep
```
Individual operations are selected by use of a specific command to the `thl` command. Supported commands are:

- **index** — obtain a list of available THL files.
- **info** — obtain summary information about the available THL data.
- **list** — list one or more THL events.
- **purge** — purge THL data.
- **help** — get the command help text.

Further information on each of these operations is provided in the following sections.

### 8.17.1. thl Position Commands

The `thl` command supports a number of position and selection command-line options that can be used to select an individual THL event, or a range of events, to be displayed.

- **-seqno #**

  **Valid for:** `thl list`

  Output the THL sequence for the specific sequence number. When reviewing or searching for a specific sequence number, for example when the application of a sequence on a slave has failed, the replication data for that sequence number can be individually viewed. For example:

  ```bash
  shell> thl list -seqno 15
  SEQ# = 15 / FRAG# = 0 (last frag)
  - TIME = 2013-05-02 11:37:00.0
  - EPOCH = 7
  - EVENTID = mysql-bin.000004:0000000000003345;0
  - SOURCEID = host1
  - META_DATA = [mysql_server_id=1687011;unsafe_for_block_commit;dbms_type=mysql;
               service=firstrep;shard=cheffy]
  - TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
  - OPTIONS = [
               #charset = UTF-8, autocommit = 1, sql_auto_is_null = 0, foreign_key_checks = 0,
               unique_checks = 0, sql_mode = 'NO_AUTO_VALUE_ON_ZERO', character_set_client = 33,
               collation_connection = 33, collation_server = 8]
  - SCHEMA = cheffy
  - SQL(0) = CREATE TABLE `access_log` (...
  ...
  
  If the sequence number selected contains multiple fragments, each fragment will be output. Depending on the content of the sequence number information, the information can be output containing only the header/metadata information or only the table data (row or SQL) that was contained within the fragment. See **-headers** and **-sql** for more information.

**Note**

Unsigned integers are displayed and stored in the THL as their negative equivalents, and translated to the correct unsigned type when the data is applied to the target database.

- **-low #** and/or **-high #**

  **Valid for:** `thl list`, `thl purge`

  Specify the start (`-low [256]`) or end (`-high [256]`) of the range of sequence numbers to be output. If only `-low [256]` is specified, then all sequence numbers from that number to the end of the THL are output. If `-high [256]` is specified, all sequence numbers from the start of the available log file to the specified sequence number are output. If both numbers are specified, output all the sequence numbers within the specified range.

  For example:

  ```bash
  shell> thl list -low 320
  Will output all the sequence number fragments from number 320.
  
  shell> thl list -high 540
  Will output all the sequence number fragments up to and including 540.
  ```
Will output all the sequence number fragments from number 320 up to, and including, sequence number 540.

8.17.2. thl list Command

The `list` command to the `thl` command outputs a list of the sequence number information from the THL. By default, the entire THL as stored on disk is output. Command-line options enable you to select individual sequence numbers, sequence number ranges, or all the sequence information from a single file.

```
thl list
[-seqno #]
[-low #] | [-high #]
```

- `-file filename` [257]
  Outputs all of the sequence number fragment information from the specified THL file. If the filename has been determined from the `thl index` command, or by examining the output of other fragments, the file-based output can be used to identify statements or row data within the THL.

- `-charset charset` [257]
  Specify the character set to be used to decode the character-based row data embedded within the THL event. Without this option, data is output as a hex value.

- `-hex` [257]
  For SQL that may be in different character sets, the information can be optionally output in hex format to determine the contents and context of the statement, even though the statement itself may be unreadable on the command-line.

- `-no-checksum` [257]
  Ignores checksums within the THL. In the event of a checksum failure, use of this option will enable checksums to be ignored when the THL is being read.

- `-sql`
  Prints only the SQL for the selected sequence range. Use of this option can be useful if you want to extract the SQL and execute it directly by storing or piping the output.

- `-headers`
  Generates only the header information for the selected sequence numbers from the THL. For THL that contains a lot of SQL, obtaining the headers can be used to get basic content and context information without having to manually filter out the SQL in each fragment.

The information is output as a tab-delimited list:

```
2047 1412 0 False 2013-05-03 20:58:14.0 mysql-bin.000005:0000000579721045;0 host3
2047 1412 1 True 2013-05-03 20:58:14.0 mysql-bin.000005:0000000579721116;0 host3
2047 1412 0 False 2013-05-03 20:58:16.0 mysql-bin.000005:0000000580759206;0 host3
2047 1412 1 True 2013-05-03 20:58:16.0 mysql-bin.000005:0000000580759277;0 host3
2047 1412 0 False 2013-05-03 20:58:18.0 mysql-bin.000005:0000000581791468;0 host3
2047 1412 1 True 2013-05-03 20:58:18.0 mysql-bin.000005:0000000581791539;0 host3
```

The format of the fields output is:

- **Sequence No**
- **Epoch**
- **Fragment**
- **Last**
- **Fragment**
- **Date/Time**
- **EventID**
- **SourceID**
- **Comments**

For more information on the fields displayed, see Section D.1.1, “THL Format”.

- `-json`
  Only valid with the `-headers` option, the header information is output for the selected sequence numbers from the THL in JSON format. The field contents are identical, with each fragment of each THL sequence being contained in a JSON object, with the output consisting of an array of the these sequence objects. For example:

```
{
  "lastFrag": false,
  "epoch": 7,
  "seqno": 320,
  "time": "2013-05-02 11:41:19.0",
  "frag": 0,
}
```
For more information on the fields displayed, see THL SEQNO [492].

- **specs**

  Shows the column specifications, such as identified type, length, and additional settings, when viewing events within row-based replication. This can be helpful when examining THL data in heterogeneous replication deployments.

  For example:

  ```
  shell> thl list -low S282 -specs
  SEQ# = 5282 / FRAG# = 0 (last frag)
  - TIME = 2014-01-30 05:46:26.0
  - EPOCH# = 5278
  - EVENTID = mysql-bin.000017:0000000000001117;0
  - SOURCEID = host1
  - METADATA = [mysql_server_id=1687011;dbms_type=mysql;is_metadata=true;service=firstrep;shard=tungsten_firstrep;heartbeat=MASTER_ONLINE]
  - TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
  - SQL(0) =
    - ACTION = UPDATE
    - SCHEMA = tungsten_firstrep
    - TABLE = heartbeat
    - ROW# = 0
    - COL(index=1 name= type=4 [INTEGER] length=8 unsigned=false blob=false desc=null) = 1
    - COL(index=2 name= type=4 [INTEGER] length=8 unsigned=false blob=false desc=null) = 1416
    - COL(index=3 name= type=12 [VARCHAR] length=0 unsigned=false blob=false desc=null) = [B@65b60280
    - COL(index=4 name= type=93 [TIMESTAMP] length=0 unsigned=false blob=false desc=null) = 2014-01-30 05:46:26.0
    - COL(index=5 name= type=93 [TIMESTAMP] length=0 unsigned=false blob=false desc=null) = 2013-05-03 12:05:47.0
    - COL(index=6 name= type=4 [INTEGER] length=8 unsigned=false blob=false desc=null) = 1015
    - COL(index=7 name= type=4 [INTEGER] length=8 unsigned=false blob=false desc=null) = 0
    - COL(index=8 name= type=12 [VARCHAR] length=0 unsigned=false blob=false desc=null) = [B@105e55ab
    - KEY(index=1 name= type=4 [INTEGER] length=8 unsigned=false blob=false desc=null) = 1
  ```

  When identifying the different data types, the following effects should be noted:

  - **CHAR** and **VARCHAR** are identified as type 12, **VARCHAR**
  - **SET** is identified as an **INTEGER**
  - When the value is either **NULL** or **0** (Zero), date and time fields are shown as type 0, **NULL**
  - **ENUM** is identified as an **OTHER**
  - **BLOB** and **TEXT** are identified as type 2004, **BLOB**
  - **-timezone**

  Specify the timezone to use when display date or time values. When not specified, times are displayed using UTC.

### 8.17.3. thl index Command

The **index** command to **thl** provides a list of all the available THL files and the sequence number range stored within each file.
8.17.4. thl purge Command

The purge command to the thl command deletes sequence number information from the THL files.

```
thl purge [-low # ] [-high # ] [-y ] [-no-checksum ]
```

The purge command deletes the THL data according to the following rules:

- **Warning**

  Purging all data requires that the THL information either be recreated from the source table, or reloaded from the master replicator.

  Without any specification, a purge command will delete all of the stored THL information.

- When only -high is specified, delete all the THL data up to and including the specified sequence number.

- When only -low is specified, delete all the THL data from and including the specified sequence number.

- With a range specification, using one or both of the -low and -high options, the range of sequences will be purged. The rules are the same as for the list command, enabling purge from the start to a sequence, from a sequence to the end, or all the sequences within a given range. The ranges must be on the boundary of one or more log files. It is not possible to delete THL data from the middle of a given file.

For example, consider the following list of THL files provided by thl index:

```
shell> thl index
LogIndexEntry thl.data.0000000377(5802:5821)
LogIndexEntry thl.data.0000000378(5822:5841)
LogIndexEntry thl.data.0000000379(5842:5861)
LogIndexEntry thl.data.0000000380(5862:5881)
LogIndexEntry thl.data.0000000381(5882:5901)
LogIndexEntry thl.data.0000000382(5902:5921)
LogIndexEntry thl.data.0000000383(5922:5941)
LogIndexEntry thl.data.0000000384(5942:5961)
LogIndexEntry thl.data.0000000385(5962:5981)
LogIndexEntry thl.data.0000000386(5982:6001)
LogIndexEntry thl.data.0000000387(6002:6021)
LogIndexEntry thl.data.0000000388(6022:6041)
LogIndexEntry thl.data.0000000389(6042:6061)
LogIndexEntry thl.data.0000000390(6062:6081)
LogIndexEntry thl.data.0000000391(6082:6101)
LogIndexEntry thl.data.0000000392(6102:6121)
LogIndexEntry thl.data.0000000393(6122:6141)
LogIndexEntry thl.data.0000000394(6142:6161)
LogIndexEntry thl.data.0000000395(6162:6181)
LogIndexEntry thl.data.0000000396(6182:6201)
LogIndexEntry thl.data.0000000397(6202:6221)
LogIndexEntry thl.data.0000000398(6222:6241)
LogIndexEntry thl.data.0000000399(6242:6261)
LogIndexEntry thl.data.0000000400(6262:6266)
```

The above shows a range of THL sequences from 5802 to 6266.

To delete all of the THL from the start of the list, sequence no 5802, to 6021 [inclusive], use the -high to specify the highest number to be removed [6021]:

```
shell> thl purge -high 6021
```

```
WARNING: The purge command will break replication if you delete all events or delete events that have not reached all slaves. Are you sure you wish to delete these events [y/N]?: y
Deleting events where SEQ# <=6021
```

```
2017-02-10 16:31:36,235 [- main] INFO thl.THLManagerCtrl Transactions deleted
```

Running a thl index, sequence numbers from 6022 to 6266 are still available:

```
shell> thl index
LogIndexEntry thl.data.0000000388(6022:6041)
```

---

The optional argument -no-checksum [257] ignores the checksum information on events in the event that the checksum is corrupt.
To delete the last two THL files, specify the sequence number at the start of the file, 6242 to the \texttt{-low} to specify the sequence number:

\begin{verbatim}
shell> thl purge -low 6242 -y
\end{verbatim}

\textbf{WARNING:} The purge command will break replication if you delete all events or delete events that have not reached all slaves.

\texttt{Deleting events where SEQ# >= 6242}

\texttt{2017-02-10 16:40:42,463 [- main] INFO thl.THLManagerCtrl Transactions deleted}

A \texttt{thl index} shows the sequence as removed:

\begin{verbatim}
shell> thl index
\end{verbatim}

The confirmation message can be bypassed by using the \texttt{-y} option, which implies that the operation should proceed without further confirmation.

The optional argument \texttt{-no-checksum} ignores the checksum information on events in the event that the checksum is corrupt.

When purging, the THL files must be writeable; the replicator must either be offline or stopped when the purge operation is completed.

A purge operation may fail for the following reasons:

\begin{itemize}
  \item Fatal error: The disk log is not writable and cannot be purged.
    
The replicator is currently running and not in the \texttt{OFFLINE} state. Use \texttt{trepctl offline} to release the write lock n the THL files.
  \item Fatal error: Deletion range invalid; must include one or both log end points: low seqno=0 high seqno=1000
    
    An invalid sequence number or range was provided. The \texttt{purge} operation will refuse to purge events that do not exist in the THL files and do not match a valid file boundary, i.e. the low figure must match the start of one file and the high the end of a file. Use \texttt{thl index} to determine the valid ranges.
\end{itemize}

8.17.5. \texttt{thl info} Command

The optional argument \texttt{-no-checksum} ignores the checksum information on events in the event that the checksum is corrupt.

8.17.6. \texttt{thl help} Command

The \texttt{help} command to the \texttt{thl} command outputs the current help message text.

8.18. The \texttt{trepctl} Command

The \texttt{trepctl} command provides the main status and management interface to Tungsten Replicator. The \texttt{trepctl} command is responsible for:

\begin{itemize}
  \item Putting the replicator online or offline
  \item Performing backup and restore operations
  \item Skipping events in the THL in the event of an issue
  \item Getting status and active configuration information
\end{itemize}
The operation and control of the command is defined through a series of command-line options which specify general options, replicator wide commands, and service specific commands that provide status and control over specific services.

The `trepctl` command by default operates on the current host and configured service. For installations where there are multiple services and hosts in the deployment. Explicit selection of services and hosts is handled through the use of command-line options, for more information see Section 8.18.1, "trepctl Options".

```
trepctl
  backup [ -backup agent ] [ -limit s ] [ -storage agent ]
capabilities
  check
clear
  clients [ -json ]
flush [ -limit s ]
heartbeat [ -name ] [ -host name ]
kill [ -y ]
load
  offline [ -all-services ]
offline-deferred [ -at-event event ] [ -at-heartbeat [hostname] ] [ -at-seqno seqno ] [ -at-time YYYY-MM-DD_hh:mm:ss ] [ -immediate ]
online [ -all-services ] [ -base-seqno x ] [ -force ] [ -from-event event ] [ -no-checksum ] [ -skip-seqno seqdef ] [ -until-event event ] [ -until-heartbeat [hostname] ] [ -until-seqno seqno ] [ -until-time YYYY-MM-DD_hh:mm:ss ] [ -port number ]
properties [ -filter name ]
purge [ -limit s ] [ -y ]
reset [ -all ] [ -db ] [ -relay ] [ -thl ] [ -y ] [ -retry N ] [ -service name ]
services [ -full ] [ -json ]
setrole [ -rolemaster | -relayslave ] [ -uri ]
shard [ -delete shard ] [ -insert shard ] [ -list ] [ -update shard ]
shutdown [ -y ]
start
status [ -json ] [ -name | channel | assignment | services | shards | stages | store | tasks | watches ]
stop [ -y ]
unload [ -y ] [ -verbose ]
version
wait [ -applied seqno ] [ -limit s ] [ -state st ]
```

For individual operations, `trepctl` uses a sub-command structure on the command-line that specifies which operation is to be performed. There are two classifications of commands, global commands, which operate across all replicator services, and service-specific commands that perform operations on a specific service and/or host. For information on the global commands available, see Section 8.18.2, "trepctl Global Commands". Information on individual commands can be found in Section 8.18.3, "trepctl Service Commands".

### 8.18.1. trepctl Options

Table 8.31. `trepctl` Command-Line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host name</td>
<td>Host name of the replicator</td>
</tr>
<tr>
<td>-port number</td>
<td>Port number of the replicator</td>
</tr>
<tr>
<td>-retry N</td>
<td>Number of times to retry the connection</td>
</tr>
<tr>
<td>-service name</td>
<td>Name of the replicator service</td>
</tr>
<tr>
<td>-verbose</td>
<td>Enable verbose messages for operations</td>
</tr>
</tbody>
</table>

Global command-line options enable you to select specific hosts and services. If available, `trepctl` will read the active configuration to determining the host, service, and port information. If this is unavailable or inaccessible, the following rules are used to determine which host or service to operate upon:

- If no host is specified, then `trepctl` defaults to the host on which the command is being executed.
- If no service is specified:
  - If only one service has been configured, then `trepctl` defaults to showing information for the configured service.
  - If multiple services are configured, then `trepctl` returns an error, and requests a specific service be selected.

To use the global options:

- `-host`
Specify the host for the operation. The replicator service must be running on the remote host for this operation to work.

- **-port**
  
  Specify the base TCP/IP port used for administration. The default is port 10000; port 10001 is also used. When using different ports, `port` and `port+1` is used, i.e. if port 4996 is specified, then port 4997 will be used as well. When multiple replicators are installed on the same host, different numbers may be used.

- **-service**
  
  The servicename to be used for the requested status or control operation. When multiple services have been configured, the servicename must be specified.

  ```
  shell> trepctl status
  Processing status command...
  Operation failed: You must specify a service name with the -service flag
  ```

- **-verbose**
  
  Turns on verbose reporting of the individual operations. This includes connectivity to the replicator service and individual operation steps. This can be useful when diagnosing an issue and identifying the location of a particular problem, such as timeouts when access a remote replicator.

- **-retry**
  
  Retry the request operation the specified number of times. The default is 10.

### 8.18.2. trepctl Global Commands

The `trepctl` command supports a number of commands that are global, or which work across the replicator regardless of the configuration or selection of individual services.

#### Table 8.32. trepctl Replicator Wide Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kill</td>
<td>Shutdown the replication services immediately</td>
</tr>
<tr>
<td>services</td>
<td>List the configured replicator services</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown the replication services cleanly</td>
</tr>
<tr>
<td>version</td>
<td>Show the replicator version number and build</td>
</tr>
</tbody>
</table>

These commands can be executed on the current or a specified host. Because these commands operate for replicators irrespective of the service configuration, selecting or specifying a service is not required.

### 8.18.2.1. trepctl kill Command

The `trepctl kill` command terminates the replicator without performing any cleanup of the replicator service, THL or sequence number information stored in the database. Using this option may cause problems when the replicator service is restarted.

```
trepctl kill [ -y ]
```

When executed, `trepctl` will ask for confirmation:

```
shell> trepctl kill
Do you really want to kill the replicator process? [yes/NO]
```

The default is no. To kill the service, ignoring the interactive check, use the `-y` option:

```
shell> trepctl kill -y
Sending kill command to replicator
Replicator appears to be stopped
```

### 8.18.2.2. trepctl services Command

The `trepctl services` command outputs a list of the current replicator services configured in the system and their key parameters such as latest sequence numbers, latency, and state.

```
trepctl services [ -full ] [ -json ]
```
For example:

```shell
trepctl services
Processing services command...
NAME          VALUE
----          -----
started       true
role          master
serviceName   alpha
serviceType   local
state         ONLINE
appliedLastSeqno: 2541
appliedLatency : 0.48
Finished services command...
```

For more information on the fields displayed, see Section D.2, “Generated Field Reference”.

For a replicator with multiple services, the information is output for each configured service:

```shell
trepctl services
Processing services command...
NAME          VALUE
----          -----
started       true
role          master
serviceName   alpha
serviceType   local
state         ONLINE
appliedLastSeqno: 44
appliedLatency : 0.492
NAME          VALUE
----          -----
started       true
role          slave
serviceName   beta
serviceType   remote
state         ONLINE
appliedLastSeqno: 40
appliedLatency : 0.57
NAME          VALUE
----          -----
started       true
role          slave
serviceName   gamma
serviceType   remote
state         ONLINE
appliedLastSeqno: 41
appliedLatency : 0.06
Finished services command...
```

The information can be reported in JSON format by using the `-json` option to the command:

```shell
trepctl services -json
[
{
  "serviceType" : "local",
  "appliedLatency" : "0.48",
  "serviceName" : "alpha",
  "appliedLastSeqno" : "2541",
  "started" : "true",
  "role" : "master",
  "state" : "ONLINE"
}
]
```

The information is output as an array of objects, one object for each service identified.

If the `-full` option is added, the JSON output includes full details of the service, similar to that output by the `trepctl status` command, but for each configured service:

```shell
trepctl services -json -full
[
{
  "masterConnectURI" : ",",
  "rmiPort" : "10000",
  "clusterName" : "default",
  "currentTimeMillis" : "1370256230198",
  "state" : "ONLINE",
  "maximumStoredSeqNo" : "2541",
  "minimumStoredSeqNo" : "0",
  "pendingErrorCode" : "NONE",
  "masterListenURI" : "thl://host1:2112/",
```
Command-line Tools

Auto-refresh support added in 6.0.1. Starting with Continuent Tungsten 6.0.1, trepctl services supports the -r option to support auto-refresh.

For more information on the fields displayed, see Section D.2, “Generated Field Reference”.

8.18.2.3. trepctl shutdown Command

Deprecated in 2.0.1. This command was deprecated in 2.0.1. See Section 4.2, “Starting and Stopping Continuent Tungsten”.

The shutdown command safely shuts down the replicator service, ensuring that the current transactions being applied to the database, THL writes and Continuent Tungsten specific updates to the database are correctly completed before shutting the service down.

```
trepctl shutdown [-y]
```

When executed, trepctl will ask for confirmation:

```
shell> trepctl shutdown
Do you really want to shutdown the replicator? [yes/NO]
```

The default is no. To shutdown the service without requiring interactive responses, use the -y option:

```
shell> trepctl shutdown -y
Replicator appears to be stopped
```

8.18.2.4. trepctl version Command

The trepctl version command outputs the version number of the specified replicator service.

```
trepctl version
```

```
shelle> trepctl version
Tungsten Replicator 2.8.5 build 11
```

The system can also be used to obtain remote version:

```
shell> trepctl -h host2 version
Tungsten Replicator 2.8.5 build 11
```

Version numbers consist of two parts, the main version number which denotes the product release, and the build number. Updates and fixes to a version may use updated build numbers as part of the same product release.

8.18.3. trepctl Service Commands

The trepctl service commands operate per-service, that is, when there are multiple services in a configuration, the service name on which the command operates must be explicitly stated. For example, when a backup is executed, the backup executes on an explicit, specified service.
The individuality of different services is critical when dealing with the replicator commands. Services can be placed into online or offline states independently of each other, since each service will be replicating information between different hosts and environments.

### Table 8.33. `trepctl` Service Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Backup database</td>
</tr>
<tr>
<td>capabilities</td>
<td>List the configured replicator capabilities</td>
</tr>
<tr>
<td>check</td>
<td>Generate consistency check</td>
</tr>
<tr>
<td>clear</td>
<td>Clear one or all dynamic variables</td>
</tr>
<tr>
<td>clients</td>
<td>List clients connected to this replicator</td>
</tr>
<tr>
<td>flush</td>
<td>Synchronize transaction history log to database</td>
</tr>
<tr>
<td>heartbeat</td>
<td>Insert a heartbeat event with optional name</td>
</tr>
<tr>
<td>load</td>
<td>Load the replication service</td>
</tr>
<tr>
<td>offline</td>
<td>Set replicator to OFFLINE state</td>
</tr>
<tr>
<td>offline-deferred</td>
<td>Set replicator OFFLINE at a future point in the replication stream</td>
</tr>
<tr>
<td>online</td>
<td>Set Replicator to ONLINE with start and stop points</td>
</tr>
<tr>
<td>properties</td>
<td>Display a list of all internal properties</td>
</tr>
<tr>
<td>purge</td>
<td>Purge non-Tungsten logins on database</td>
</tr>
<tr>
<td>reset</td>
<td>Deletes the replicator service</td>
</tr>
<tr>
<td>setrole</td>
<td>Set replicator role</td>
</tr>
<tr>
<td>shard</td>
<td>List, add, update, and delete shards</td>
</tr>
<tr>
<td>start</td>
<td>Start replication service</td>
</tr>
<tr>
<td>status</td>
<td>Print replicator status information</td>
</tr>
<tr>
<td>stop</td>
<td>Stop replication service</td>
</tr>
<tr>
<td>unload</td>
<td>Unload the replication service</td>
</tr>
<tr>
<td>wait</td>
<td>Wait for the replicator to reach a specific state, time or applied sequence number</td>
</tr>
</tbody>
</table>

The following sections detail each command individually, with specific options, operations and information.

### 8.18.3.1. `trepctl backup` Command

The `trepctl backup` command performs a backup of the corresponding database for the selected service.

```
trepctl backup [-backup agent] [-limit s] [-storage agent]
```

Where:

#### Table 8.34. `trepctl backup` Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-backup agent</td>
<td>Select the backup agent</td>
</tr>
<tr>
<td>-limit s</td>
<td>The period to wait before returning after the backup request</td>
</tr>
<tr>
<td>-storage agent</td>
<td>Select the storage agent</td>
</tr>
</tbody>
</table>

Without specifying any options, the backup uses the default configured backup and storage system, and will wait indefinitely until the backup process has been completed:

```
shell> trepctl backup
Backup completed successfully; URI=storage://file-system/store-0000000002.properties
```

The return information gives the URI of the backup properties file. This information can be used when performing a restore operation as the source of the backup. See Section 8.18.3.15, "`trepctl restore` Command". Different backup solutions may require that the replicator be placed into the OFFLINE state before the backup is performed.

A log of the backup operation will be stored in the replicator log directory, if a file corresponding to the backup tool used [e.g. `mysqldump.log`].
If multiple backup agents have been configured, the backup agent can be selected on the command-line:

```shell
trepctl backup -backup mysqldump
```

If multiple storage agents have been configured, the storage agent can be selected using the `-storage` option:

```shell
trepctl backup -storage file
```

A backup will always be attempted, but the timeout to wait for the backup to be started during the command-line session can be specified using the `-limit` option. The default is to wait indefinitely. However, in a scripted environment you may want to request the backup and continue performing other operations. The `-limit` option specifies how long `trepctl` should wait before returning.

For example, to wait five seconds before returning:

```shell
trepctl -service alpha backup -limit 5
```

The backup request has been received, but not completed within the allocated time limit. The command will return. Checking the logs shows the timeout:

```shell
... management.OpenReplicatorManager Backup request timed out: seconds=5
```

Followed by the successful completion of the backup, indicated by the URI provided in the log showing where the backup file has been stored.

```
... BackupTask Storing backup result...
... FileSystemStorageAgent Allocated backup location: »
... url=file://file-system/store-0000000003.properties
... file=/opt/continuent/backups/store-0000000003-mysqldump_2013-07-15_18-14_11.sql.gz length=0
... FileSystemStorageAgent Stored backup storage file: »
... file=/opt/continuent/backups/store-0000000003.properties length=314
... BackupTask Backup completed normally: »
... url=file://file-system/store-0000000003.properties
```

The URI can be used during a restore.

### 8.18.3.2. trepctl capabilities Command

The `trepctl capabilities` command outputs a list of the supported capabilities for this replicator instance.

```shell
  trepctl capabilities
```

The information output will depend on the configuration and current role of the replicator service. Different services on the same host may have different capabilities. For example:

```shell
trepctl capabilities
```

The fields output are as follows:

- **Roles**
  Indicates whether the replicator can be a master or slave, or both.

- **Replication Model**
  The model used by the replication system. The default model for MySQL for example is push, where information is extracted from the binary log and pushed to slaves that apply the transactions. The pull model is used for heterogeneous deployments.

- **Consistency Check**
  Indicates whether the internal consistency check is supported. For more information see Section 8.18.3.3, "trepctl check Command".

- **Heartbeat**
  Indicates whether the heartbeat service is supported. For more information see Section 8.18.3.7, "trepctl heartbeat Command".

- **Flash**
Indicates whether the `trepctl flush` operation is supported.

### 8.18.3.3. trepctl check Command

The `check` command operates by running a CRC check on the schema or table specified, creating a temporary table containing the check data and values during the process. The data collected during this process is then written to a consistency table within the replication configuration schema and is used to verify the table data consistency on the master and the slave.

**Warning**

Because the check operation is creating a temporary table containing a CRC of each row within the specified schema or specific table, the size of the temporary table created can be quite large as it consists of CRC and row count information for each row of each table (within the specified row limits). The configured directory used by MySQL for temporary table creation will need a suitable amount of space to hold the temporary data.

### 8.18.3.4. trepctl clear Command

The `trepctl clear` command deletes any dynamic properties configured within the replicator service.

```
trepctl clear
```

Dynamic properties include the current active role for the service. The dynamic information is stored internally within the replicator, and also stored within a properties file on disk so that the replicator can be restarted.

For example, the replicator role may be temporarily changed to receive information from a different host or to act as a master in place of a slave. The replicator can be returned to the initial configuration for the service by clearing this dynamic property:

```
shell> trepctl clear
```

### 8.18.3.5. trepctl clients Command

Outputs a list of the clients that have been connected to the master service since it went online. If a slave service goes offline or is stopped, it will still be reported by this command.

```
trepctl clients [-json]
```

Where:

**Table 8.35. trepctl clients Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-json</td>
<td>Output the information as JSON</td>
</tr>
</tbody>
</table>

The command outputs the list of clients and the management port on which they can be reached:

```
shell> trepctl clients
Processing clients command...
host2:10000
host3:10000
Finished clients command...
```

A JSON version of the output is available when using the `-json` option:

```
shell> trepctl clients -json
[
  {
    "rmiPort": "10000",
    "rmiHost": "host2"
  },
  {
    "rmiPort": "10000",
    "rmiHost": "host3"
  }
]
```

The information is divided first by host, and then by the RMI management port.
### 8.18.3.6. trepctl flush Command

On a master, the `trepctl flush` command synchronizes the database with the transaction history log, flushing the in memory queue to the THL file on disk. The operation is not supported on a slave.

```shell
$ trepctl flush [-limit s]
```

Internally, the operation works by inserting a heartbeat event into the queue, and then confirming when the heartbeat event has been committed to disk.

To flush the replicator:

```shell
$ trepctl flush
Master log is synchronized with database at log sequence number: 3622
```

The flush operation is always initiated, and by default `trepctl` will wait until the operation completes. Using the `-limit` option, the amount of time the command-line waits before returning can be specified:

```shell
$ trepctl flush -limit 1
```

### 8.18.3.7. trepctl heartbeat Command

Inserts a heartbeat into the replication stream, which can be used to identify replication points.

```shell
$ trepctl heartbeat [-name]
```

The heartbeat system is a way of inserting an identifiable event into the THL that is independent of the data being replicated. This can be useful when performing different operations on the data where specific checkpoints must be identified.

To insert a standard heartbeat:

```shell
$ trepctl heartbeat
```

When performing specific operations, the heartbeat can be given an name:

```shell
$ trepctl heartbeat -name dataload
```

Heartbeats insert a transaction into the THL using the transaction metadata and can be used to identify whether replication is operating between replicator hosts by checking that the sequence number has been replicated to the slave. Because a new transaction is inserted, the sequence number is increased, and this can be used to identify if transactions are being replicated to the slave without requiring changes to the database. To check replication using the heartbeat:

1. Check the current transaction sequence number on the master:

```shell
$ trepctl status
Processing status command...
   NAME       VALUE        
   ......      ......        
   appliedLastEventId : mysql-bin.000009:0000000000008998;0
   appliedLastSeqno   : 3630
   ......      ......        
```

2. Insert a heartbeat event:

```shell
$ trepctl heartbeat
```

3. Check the sequence number again:

```shell
$ trepctl status
Processing status command...
   NAME       VALUE        
   ......      ......        
   appliedLastEventId : mysql-bin.000009:0000000000009310;0
   appliedLastSeqno   : 3631
   ......      ......        
```

4. Check that the sequence number on the slave matches:

```shell
$ trepctl status
Processing status command...
   NAME       VALUE        
   ......      ......        
   appliedLastEventId : mysql-bin.000009:0000000000009310;0
   appliedLastSeqno   : 3631
   ......      ......        
```

Heartbeats are given implied names, but can be created with explicit names that can be tracked during specific events and operations.
For example, when loading a specific set of data, the information may be loaded and then a backup executed on the slave before enabling standard replication. This can be achieved by configuring the slave to go offline when a specific heartbeat event is seen, loading the data on the master, inserting the heartbeat when the load has finished, and then performing the slave backup:

1. On the slave:

   ```shell
   slave shell> trepctl offline-deferred -at-heartbeat dataload
   ```

   The `trepctl offline-deferred` command configures the slave to continue in the online state until the specified event, in this case the heartbeat, is received. The deferred state can be checked by looking at the status output, and the `offlineRequests` field:

   ```
   Processing status command....
   NAME                     VALUE
   ...                     ...  
   appliedLastEventId     : mysql-bin.000009:0000000000008271;0
   appliedLastSeqno       : 3627
   appliedLatency         : 8.704
   ...
   offlineRequests        : Offline at heartbeat event: dataload
   ```

2. On the master:

   ```shell
   master shell> mysql newdb < newdb.load
   ```

3. Once the data load has completed, insert the heartbeat on the master:

   ```shell
   master shell> trepctl heartbeat -name dataload
   ```

   The heartbeat will appear in the transaction history log after the data has been loaded and will identify the end of the load.

4. When the heartbeat is received, the slave will go into the offline state. Now a backup can be created with all of the loaded data replicated from the master. Because the slave is in the offline state, no further data or changes will be recorded on the slave.

   This method of identifying specific events and points within the transaction history log can be used for a variety of different purposes where the point within the replication stream without relying on the arbitrary event or sequence number.

### Internal Implementation

Internally, the heartbeat system operates through a tag added to the metadata of the THL entry and through a dedicated `heartbeat` table within the schema created for the replicator service. The table contains the sequence number, event ID, timestamp and heartbeat name. The heartbeat information is written into a special record within the transaction history log. A sample THL entry can be seen in the output below:

```
SEQ# = 3629 / FRAG# = 0 (last frag)
- TIME = 2013-07-19 12:14:57.0
- EPOCH# = 3614
- EVENTID = mysql-bin.000009:0000000000008681;0
- SOURCEID = host1
- METADATA = [mysql_server_id=1687011;dbms_type=mysql;is_metadata=true;service=alpha;
  shard=tungsten_alpha;heartbeat=dataload]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
- OPTIONS = [##charset = UTF-8, autocommit = 1, sql_auto_is_null = 0,
  foreign_key_checks = 1, unique_checks = 1, sql_mode = 'IGNORE_SPACE',
  character_set_client = 33, collation_connection = 33, collation_server = 8]
- SCHEMA = tungsten_alpha
- SQL(0) = UPDATE tungsten_alpha.heartbeat SET source_tstamp= '2013-07-19 12:14:57',
  salt= 9, name= 'dataload'  WHERE id= 1
```

During replication, slaves identify the heartbeat and record this information into their own `heartbeat` table. Because the heartbeat is recorded into the transaction history log, the specific sequence number of the transaction, and the event itself can be easily identified.

### 8.18.3.8. trepctl load Command

Load the replicator service.

```shell
  trepctl load
```

Load the replicator service. The service name must be specified on the command-line, even when only one service is configured:

```shell
  shell> trepctl load
  Operation Failed: You must specify a service name using -service
```

The service name can be specified using the `-service` option:
8.18.3.9. `trepctl offline` Command

The `trepctl offline` command puts the replicator into the offline state, stopping replication.

```
shell> trepctl -service alpha load
Service loaded successfully: name=alpha
```

To put the replicator offline:
```
shell> trepctl offline
```

While offline:
- Transactions are not extracted from the source dataserver.
- Transactions are not applied to the destination dataserver.

Certain operations on the replicator, including updates to the operating system and dataserver should be performed while in the offline state.

By default, the replicator goes offline in deferred mode, allowing the current transactions being read from the binary log, or applied to the dataserver to complete, the sequence number table in the database is updated, and the replicator is placed offline, stopping replication.

To stop replication immediately, within the middle of an executing transaction, use the `-immediate` option:
```
shell> trepctl offline -immediate
```

8.18.3.10. `trepctl offline-deferred` Command

The `trepctl offline-deferred` sets a future sequence, event or heartbeat as the trigger to put the replicator in the offline state.

```
trepctl offline-deferred [ -at-event event ] [ -at-heartbeat [heartbeat] ] [ -at-seqno seqno ] [ -at-time YYYY-MM-DD_hh:mm:ss ]
```

Where:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-at-event event</code> [270]</td>
<td>Go offline at the specified event</td>
</tr>
<tr>
<td><code>-at-heartbeat [heartbeat]</code> [271]</td>
<td>Go offline when the specified heartbeat is identified</td>
</tr>
<tr>
<td><code>-at-seqno seqno</code> [270]</td>
<td>Go offline at the specified sequence number</td>
</tr>
<tr>
<td><code>-at-time YYYY-MM-DD_hh:mm:ss</code> [271]</td>
<td>Go offline at the specified time</td>
</tr>
</tbody>
</table>

The `trepctl offline-deferred` command can be used to put the replicator into an offline state at some future point in the replication stream by identifying a specific trigger. The replicator must be online when the `trepctl offline-deferred` command is given; if the replicator is not online, the command is ignored.

The offline process performs a clean offline event, equivalent to executing `trepctl offline`. See Section 8.18.3.9, "trepctl offline Command”.

The supported triggers are:
- `-at-seqno` [270]
  Specifies a transaction sequence number [GTID] where the replication will be stopped. For example:
  ```
  shell> trepctl offline-deferred -at-seqno 3800
  ```
  The replicator goes into offline at the end of the matching transaction. In the above example, sequence 3800 would be applied to the dataserver, then the replicator goes offline.
- `-at-event` [270]
  Specifies the event where replication should stop:
  ```
  shell> trepctl offline-deferred -at-event 'mysql-bin.000009:0000000000088140;8'
  ```
  Because there is not a one-to-one relationship between global transaction IDs and events, the replicator will go offline at a transaction that has an event ID higher than the deferred event ID. If the event specification is located within the middle of a THL transaction, the entire transaction is applied.
Command-line Tools

- **-at-heartbeat [271]**
  Specifies the name of a specific heartbeat to look for when replication should be stopped.

- **-at-time [271]**
  Specifies a time (using the format YYYY-MM-DD_hh:mm:ss) at which replication should be stopped. The time must be specified in full [date and time to the second].

  ```shell
trepctl offline-deferred -at-time 2013-09-01_00:00:00
  ``

  The transaction being executed at the time specified completes, then the replicator goes offline.

If any specified deferred point has already been reached, then the replicator will go offline anyway. For example, if the current sequence number is 3800 and the deferred sequence number specified is 3700, then the replicator will go offline immediately just as if the `trepctl offline` command has been used.

When a trigger is reached, For example if a sequence number is given, that sequence will be applied and then the replicator will go offline.

The status of the pending `trepctl offline-deferred` setting can be identified within the status output within the `offlineRequests` field:

```shell
trepctl status
offlineRequests : Offline at sequence number: 3810
```

Multiple `trepctl offline-deferred` commands can be given for each corresponding trigger type. For example, below three different triggers have been specified, sequence number, time and heartbeat event, with the status showing each deferred event separated by a semicolon:

```shell
trepctl status
... offlineRequests : Offline at heartbeat event: dataloaded;Offline at » sequence number: 3640;Offline at time: 2013-09-01 00:00:00 EDT
```

Offline deferred settings are cleared when the replicator is put into the offline state, either manually or automatically.

### 8.18.3.11. trepctl online Command

The `trepctl online` command puts the replicator into the online state. During the state change from offline to online various options can be used to control how the replicator goes back on line. For example, the replicator can be placed online, skipping one or more faulty transactions or disabling specific configurations.

```shell
trepctl online 
-all-services 
-base-seqno x 
-force 
-from-event event 
-no-checksum 
-skip-seqno seqdef 
-until-event event 
-until-heartbeat [name] 
-until-seqno seqno 
-until-time YYYY-MM-DD_hh:mm:ss
```

Where:

#### Table 8.37. trepctl online Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-all-services</td>
<td>Place online all available services</td>
</tr>
<tr>
<td>-base-seqno x</td>
<td>On a master, restart replication using the specified sequence number</td>
</tr>
<tr>
<td>-force</td>
<td>Force the online state</td>
</tr>
<tr>
<td>-from-event event</td>
<td>Start replication from the specified event</td>
</tr>
<tr>
<td>-no-checksum</td>
<td>Disable checksums for all events when going online</td>
</tr>
<tr>
<td>-skip-seqno seqdef</td>
<td>Skip one, multiple, or ranges of sequence numbers before going online</td>
</tr>
<tr>
<td>-until-event event</td>
<td>Define an event when replication will stop</td>
</tr>
<tr>
<td>-until-heartbeat [name]</td>
<td>Define a heartbeat when replication will stop</td>
</tr>
<tr>
<td>-until-seqno seqno</td>
<td>Define a sequence no when replication will stop</td>
</tr>
<tr>
<td>-until-time YYYY-MM-DD_hh:mm:ss</td>
<td>Define a time when replication will stop</td>
</tr>
</tbody>
</table>

The `trepctl online` command attempts to switch replicator into the online state. The replicator may need to be put online because it has been placed offline for maintenance, or due to a failure.

To put the replicator online use the standard form of the command:

```shell
trepctl online
```
Going online may fail if the reason for going offline was due to a fault in processing the THL, or in applying changes to the dataserver. The replicator will refuse to go online if there is a fault, but certain failures can be explicitly bypassed.

### 8.18.3.11.1. Going Online from Specific Transaction Points

If there is one, or more, event in the THL that could not be applied to the slave because of a mismatch in the data (for example, a duplicate key), the event or events can be skipped using the `-skip-seqno` option. For example, the status shows that a statement failed:

```
shell> trepctl status
...
pendingError : Event application failed: seqno=5250 fragno=0 »
  message=java.sql.SQLException: Statement failed on slave but succeeded on master
...
```

To skip the single sequence number, **5250**, shown:

```
shell> trepctl online -skip-seqno 5250
```

The sequence number specification can be specified according to the following rules:

- A single sequence number:
  ```
  shell> trepctl online -skip-seqno 5250
  ```

- A sequence range:
  ```
  shell> trepctl online -skip-seqno 5250-5260
  ```

- A comma-separated list of individual sequence numbers and/or ranges:
  ```
  shell> trepctl online -skip-seqno 5250,5251,5253-5260
  ```

### 8.18.3.11.2. Going Online from a Base Sequence Number

Alternatively, the base sequence number, the transaction ID where replication should start, can be specified explicitly:

```
shell> trepctl online -base-seqno 5260
```

**Warning**

Use of `-base-seqno` should be restricted to replicators in the **master** role only. Use on slaves may lead to duplication or corruption of data.

### 8.18.3.11.3. Going Online from a Specific Event

If the source event (for example, the MySQL binlog position) is known, this can be used as the reference point when going online and restarting replication:

```
shell> trepctl online -from-event 'mysql-bin.000011:0000000000002552;0'
```

When used, replication will start from the next event within the THL. The event ID provided must be valid. The event cannot be found in the THL, the operation will fail.

### 8.18.3.11.4. Going Online Until Specific Transaction Points

There are times when it is useful to be able to online until a specific point in time or in the replication stream. For example, when performing a bulk load parallel replication may be enabled, but only a single applier stream is required once the load has finished. The replicator can be configured to go online for a limited period, defined by transaction IDs, events, heartbeats, or a specific time.

The replicator must be in the offline state before the deferred online specifications are made. Multiple deferred online states can be specified in the same command when going online.

The setting of a future offline state can be seen by looking at the `offlineRequests` field when checking the status:

```
shell> trepctl status
...
minimumStoredSeqNo : 0
offlineRequests : Offline at sequence number: 5262;Offline at time: 2014-01-01 00:00:00 EST
pendingError : NONE
...
```

If the replicator goes offline for any reason before the deferred offline state is reached, the deferred settings are lost.
8.18.3.11.4.1. Going Online Until Specified Sequence Number

To go online until a specific transaction ID, use `-until-seqno`:

```
shell> trepctl online -until-seqno 5260
```

This will process all transactions up to, and including, sequence 5260, at which point the replicator will go offline.

8.18.3.11.4.2. Going Online Until Specified Event

To go online until a specific event ID:

```
shell> trepctl online -until-event 'mysql-bin.000011:0000000000003057:0'
```

Replication will go offline when the event ID up to the specified event has been processed.

8.18.3.11.4.3. Going Online Until Heartbeat

To go online until a heartbeat event:

```
shell> trepctl online -until-heartbeat
```

Heartbeats are inserted into the replication stream periodically, replication will stop once the heartbeat has been seen before the next transaction. A specific heartbeat can also be specified:

```
shell> trepctl online -until-heartbeat load-finished
```

8.18.3.11.4.4. Going Online Until Specified Time

To go online until a specific date and time:

```
shell> trepctl online -until-time 2014-01-01_00:00:00
```

Replication will go offline once the transaction being processed at the time specified has completed.

8.18.3.11.5. Going Online by Force

In situations where the replicator needs to go online, the online state can be forced. This changes the replicator state to online, but provides no guarantees that the online state will remain in place if another, different, error stops replication.

```
shell> trepctl online -force
```

8.18.3.11.6. Going Online without Validating Checksum

In the event of a checksum problem in the THL, checksums can be disabled using the `-no-checksum` option:

```
shell> trepctl online -no-checksum
```

This will bring the replicator online without reading or writing checksum information.

**Important**

Use of the `-no-checksum` option disables both the reading and writing of checksums on log records. If starting the replicator without checksums to get past a checksum failure, the replicator should be taken offline again once the offending event has been replicated. This will avoid generating too many local records in the THL without checksums.

8.18.3.12. trepctl properties Command

Display a list of all the internal properties. The list can be filtered.

```
trepctl properties [-filter name]
```

The list of properties can be used to determine the current configuration:

```
shell> trepctl properties
{
    "replicator.store.thl.log_file_retention": "7d",
    "replicator.filter.bidiSlave.allowBidiUnsafe": "false",
    "replicator.extractor.dbms.binlog_file_pattern": "mysql-bin",
    ...
}
```
Command-line Tools

Note

Passwords are not displayed in the output.

The information is output as a JSON object with key/value pairs for each property and corresponding value.

The list can be filtered using the -filter option:

```
shell> trepctl properties -filter shard
{
  "replicator.filter.shardfilter": »
  "com.continuent.tungsten.replicator.shard.ShardFilter",
  "replicator.filter.shardbyseqno": »
  "com.continuent.tungsten.replicator.filter.JavaScriptFilter",
  "replicator.filter.shardbyseqno.shards": "1000",
  "replicator.filter.shardfilter.enforcehome": "false",
  "replicator.filter.shardfilter.unknownShardPolicy": "error",
  "replicator.filter.shardbyseqno.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbyseqno.js",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardfilter.enabled": "true",
  "replicator.filter.shardfilter.allowWhitelisted": "false",
  "replicator.shard.default.db": "stringent",
  "replicator.filter.shardbytable": »
  "com.continuent.tungsten.replicator.filter.JavaScriptFilter",
  "replicator.filter.shardfilter.autoCreate": "false",
  "replicator.filter.shardfilter.unwantedShardPolicy": "error",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardbytable.script": »
  "../../tungsten-replicator//samples/extensions/javascript/shardbytable.js",
  "replicator.filter.shardfilter.enabled": "true",
  "replicator.filter.shardfilter.allowWhitelisted": "false",
  "replicator.shard.default.db": "stringent",
  "replicator.filter.shardbytable": »
  "com.continuent.tungsten.replicator.filter.JavaScriptFilter",
  "replicator.filter.shardfilter.autoCreate": "false",
  "replicator.filter.shardfilter.unwantedShardPolicy": "error"
}
```

The value or values from filtered properties can be retrieved by using the -values option:

```
shell> trepctl properties -filter site.name -values
default
```

If a filter that would select multiple values is specified, all the values are listed without field names:

```
shell> trepctl properties -filter shard -values
com.continuent.tungsten.replicator.shard.ShardFilter
com.continuent.tungsten.replicator.filter.JavaScriptFilter
1000
false
"../../tungsten-replicator//samples/extensions/javascript/shardbyseqno.js"
"error"
"../../tungsten-replicator//samples/extensions/javascript/shardbytable.js"
true
false
"stringent"
com.continuent.tungsten.replicator.filter.JavaScriptFilter
false
"error"
```

8.18.3.13. trepctl purge Command

Forces all logins on the attached database, other than those directly related to Continent Tungsten, to be disconnected. The command is only supported on master, and can be used to disconnect users before a switchover or taking a master offline to prevent further use of the system.

```
trepctl purge [-limit s] [-y]
```

Where:

Table 8.38. trepctl purge Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-limit s [275]</td>
<td>Specify the waiting time for the operation</td>
</tr>
<tr>
<td>-y [275]</td>
<td>Indicates that the command should continue without interactive confirmation</td>
</tr>
</tbody>
</table>

Warning

Use of the command will disconnect running users and queries and may leave the database in an unknown state. It should be used with care, and only when the dangers and potential results are understood.

To close the connections:

274
Command-line Tools

8.18.3.14. trepctl purge Command

The `trepctl purge` command removes non-Tungsten DBMS sessions. You will be prompted to confirm the operation. To skip this confirmation and purge connections, use the `-y [275]` option:

```
shell> trepctl purge
Do you really want to purge non-Tungsten DBMS sessions? [yes/NO]
```

You will be prompted to confirm the operation. To skip this confirmation and purge connections, use the `-y [275]` option:

```
shell> trepctl purge -y
Directing replicator to purge non-Tungsten sessions
Number of sessions purged: 0
```

An optional parameter, `-wait [275]`, defines the period of time that the operation will wait before returning to the command-line.

An optional parameter, `-limit [275]`, defines the period of time that the operation will wait before returning to the command-line.

8.18.3.14. trepctl reset Command

The `trepctl reset` command resets an existing replicator service, performing the following operations:

- Deleting the local THL and relay directories
- Removing the Tungsten schema from the dataserver
- Removing any dynamic properties that have previously been set

The service name must be specified, using `-service`.

```
trepctl reset [-all] [-db] [-relay] [-thl] [-y]
```

Where:

**Table 8.39. trepctl reset Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-all [275]</code></td>
<td>Deletes the thl directory, relay logs directory and tungsten database for the service. Same as specifying <code>-thl -relay -db</code></td>
</tr>
<tr>
<td><code>-db [275]</code></td>
<td>Deletes the tungsten_{service_name} database for the service</td>
</tr>
<tr>
<td><code>-relay [275]</code></td>
<td>Deletes the relay directory for the service</td>
</tr>
<tr>
<td><code>-thl [275]</code></td>
<td>Deletes the thl directory for the service</td>
</tr>
<tr>
<td><code>-y [275]</code></td>
<td>Indicates that the command should continue without interactive confirmation</td>
</tr>
</tbody>
</table>

To reset a replication service, the replication service must be offline and the service name must be specified:

```
shell> trepctl offline
```

Execute the `trepctl reset` command:

```
shell> trepctl -service alpha reset
Do you really want to delete replication service alpha completely? [yes/NO]
```

You will be prompted to confirm the deletion. To ignore the interactive prompt, use the `-y [275]` option:

```
shell> trepctl -service alpha reset -y
```

Then put the replicator back online again:

```
shell> trepctl online
```

You can also reset only part of the overall service by including one of the following options:

- Reset all components of the service.
- Reset the THL. This is equivalent to running `thl purge`.
- Reset the relay log contents.
- Reset the database, including emptying the `trep_commit_seqno` and other control tables.
- Reset the redo log contents of the service. Valid only for Oracle extraction deployments

8.18.3.15. trepctl restore Command

Restores the database on a host from a previous backup.
Command-line Tools

**trepctl** capabilities

Once the restore has been completed, the node will remain in the **OFFLINE** state. The datasource should be switched **ONLINE** using **trepctl**:

```
shell> trepctl online
```

Any outstanding events from the master will be processed and applied to the slave, which will catch up to the current master status over time.

### 8.18.3.16. **trepctl setrole** Command

The **trepctl setrole** command changes the role of the replicator service. This command can be used to change a configured host between slave and master roles, for example during switchover.

```
trepctl setrole [-role master|slave] [-uri]
```

Where:

**Table 8.40. **trepctl setrole** Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-role</td>
<td>Replicator role</td>
</tr>
<tr>
<td>-uri [276]</td>
<td>URI of the master</td>
</tr>
</tbody>
</table>

To change the role of a replicator, specify the role using the **-role** parameter. The replicator must be offline when the role change is issued:

```
shell> trepctl setrole -role master
```

When setting a slave, the URI of the master can be optionally supplied:

```
shell> trepctl setrole -role slave -uri thl://host1:2112/
```

### 8.18.3.17. **trepctl shard** Command

The **trepctl shard** command provides an interface to the replicator shard system definition system.

```
trepctl shard [-delete shard] [-insert shard] [-list] [-update shard]
```

Where:

**Table 8.41. **trepctl shard** Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-delete shard</td>
<td>Delete a shard definition</td>
</tr>
<tr>
<td>-insert shard</td>
<td>Add a new shard definition</td>
</tr>
<tr>
<td>-list</td>
<td>List configured shards</td>
</tr>
<tr>
<td>-update shard</td>
<td>Update a shard definition</td>
</tr>
</tbody>
</table>

The replicator shard system is used during multi-site replication configurations to control where information is replicated.

For more information, see Section 3.2, “Deploying Multisite/Multimaster Clusters” Section 3.3, “Deploying a Composite Cluster”.

#### 8.18.3.17.1. Listing Current Shards

To obtain a list of the currently configured shards:

```
shell> trepctl shard -list
shard_id master critical
alpha sales true
```

The shard map information can also be captured and then edited to update existing configurations:

```
shell> trepctl shard -list>shard.map
```

#### 8.18.3.17.2. Inserting a New Shard Configuration

To add a new shard map definition, either enter the information interactively:

```
shell> trepctl shard -insert
Reading from standard input
```
1 new shard inserted

Or import from a file:

```
shell> trepctl shard -insert < shard.map
Reading from standard input
1 new shard inserted
```

8.18.3.17.3. Updating an Existing Shard Configuration

To update a definition:

```
shell> trepctl shard -update < shard.map
Reading from standard input
1 shard updated
```

8.18.3.17.4. Deleting a Shard Configuration

To delete a single shard definition, specify the shard name:

```
shell> trepctl shard -delete alpha
```

8.18.3.18. trepctl start Command

Deprecated in 2.0.1. This command was deprecated in 2.0.1; use Section 8.18.3.8, “trepctl load Command”.

Start the replicator service.

```
trepctl start
```

Start the replicator service. The service name must be specified on the command-line, even when only one service is configured:

```
shell> trepctl start
Operation failed: You must specify a service name using -service
```

The service name can be specified using the -service option:

```
shell> trepctl -service alpha start
Service started successfully: name=alpha
```

8.18.3.19. trepctl status Command

The trepctl status command provides status information about the selected data service. The status information by default is a generic status report containing the key fields of status information. More detailed service information can be obtained by specifying the status name with the -name parameter.

The format of the command is:

```
trepctl status [ -json ] [ -name channels assignments services shards stages stores tasks watches ]
```

Where:

**Table 8.42. trepctl status Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-json</td>
<td>Output the information in JSON format</td>
</tr>
<tr>
<td>-name</td>
<td>Select a specific group of status information</td>
</tr>
</tbody>
</table>

For example, to get the basic status information:

```
shell> trepctl status
Processing status command...
NAME                        VALUE
appliedLastEventId          mysql-bin.000007:0000000000001353:0
appliedLastSeqno            2504
appliedLatency              0.53
channels                    1
clusterName                 default
currentTimeMillis           1369233160014
dataServerHost              host1
extensions                  3077
```

277
Command-line Tools

For more information on the field information output, see Section D.2, “Generated Field Reference”.

8.18.3.19.1. Getting Detailed Status

More detailed information about selected areas of the replicator status can be obtained by using the `-name` option.

8.18.3.19.1.1. Detailed Status: Channel Assignments

When using a single threaded replicator service, the `trepctl status -name channel-assignments` will output an empty status. In parallel replication deployments, the `trepctl status -name channel-assignments` listing will output the list of schemas and their assigned channels within the configured channel quantity configuration. For example, in the output below, only two channels are shown, although five channels were configured for parallel apply:

```
shell> trepctl status -name channel-assignments
Processing status command (channel-assignments)...
NAME      VALUE
----      ----- channel : 0
shard_id: test
NAME      VALUE
----      ----- channel : 0
shard_id: tungsten_alpha
Finished status command (channel-assignments)...
```

8.18.3.19.1.2. Detailed Status: Services

The `trepctl status -name services` status output shows a list of the currently configure internal services that are defined within the replicator.

```
shell> trepctl status -name services
Processing status command (services)...
NAME              VALUE
----              ----- accessFailures  : 0
active            : true
maxChannel        : -1
name              : channel-assignment
storeClass        : com.continuent.tungsten.replicator.channel.ChannelAssignmentService
totalAssignments : 0
Finished status command (services)...
```

8.18.3.19.1.3. Detailed Status: Shards

8.18.3.19.1.4. Detailed Status: Stages

The `trepctl status -name stages` status output lists the individual stages configured within the replicator, showing each stage, configuration, filters and other parameters applied at each replicator stage:

```
shell> trepctl status -name stages
```
8.18.3.19.1.5. Detailed Status: Stores

The `trepctl status -name stores` status output lists the individual internal stores used for replicating THL data. This includes both physical (on disk) THL storage and in-memory storage. This includes the sequence number, file size and retention information.

For example, the information shown below is taken from a master service, showing the stages, `binlog-to-q`, which reads the information from the binary log, and the in-memory `q-to-thl` that writes the information to THL.

```
shell> trepctl status -name stages
Processing status command (stages)...
NAME                      VALUE
----                      -----...
applier.class : com.continuent.tungsten.replicator.thl.THLStoreApplier
applier.name   : thl-applier
blockCommitRowCount : 1
committedMinSeqno : 15
extractor.class : com.continuent.tungsten.replicator.thl.RemoteTHLExtractor
extractor.name  : thl-remote
name           : remote-to-thl
processedMinSeqno : 1
taskCount      : 1
NAME                      VALUE
----                      -----...
applier.class : com.continuent.tungsten.replicator.thl.THLParallelQueueApplier
applier.name   : parallel-q-applier
blockCommitRowCount : 10
committedMinSeqno : 15
extractor.class : com.continuent.tungsten.replicator.thl.THLStoreExtractor
extractor.name  : thl-extractor
name           : thl-to-q
processedMinSeqno : 1
taskCount      : 1
NAME                      VALUE
----                      -----...
applier.class : com.continuent.tungsten.replicator.thl.THLParallelQueueApplier
applier.name   : parallel-q-applier
blockCommitRowCount : 1
committedMinSeqno : 15
extractor.class : com.continuent.tungsten.replicator.thl.RemoteTHLExtractor
extractor.name  : thl-remote
name           : remote-to-thl
processedMinSeqno : 1
taskCount      : 1
NAME                      VALUE
----                      -----...
applier.class : com.continuent.tungsten.replicator.thl.THLStoreApplier
applier.name   : thl-applier
blockCommitRowCount : 1
committedMinSeqno : 15
extractor.class : com.continuent.tungsten.replicator.thl.THLStoreExtractor
extractor.name  : thl-extractor
name           : thl-to-q
processedMinSeqno : 1
taskCount      : 1
Finished status command (stages)...
```

When running parallel replication, the output shows the store name, sequence number and status information for each parallel replication channel:

```
shell> trepctl status -name stores
Processing status command (stores)...
NAME                      VALUE
----                      -----...
applier.class : com.continuent.tungsten.replicator.thl.THLStoreApplier
applier.name   : thl-applier
blockCommitRowCount : 1
committedMinSeqno : 15
extractor.class : com.continuent.tungsten.replicator.thl.RemoteTHLExtractor
extractor.name  : thl-remote
name           : remote-to-thl
processedMinSeqno : 1
taskCount      : 1
Finished status command (stores)...
```
8.18.3.19.1.6. Detailed Status: Tasks

The `trepctl status -name tasks` command outputs the current list of active tasks within a given service, with one block for each stage within the replicator service.
8.18.3.19.1.7. Detailed Status: Watches

8.18.3.19.2. Getting JSON Formatted Status

Status information can also be requested in JSON format. The content of the information is identical, only the representation of the information is different, formatted in a JSON wrapper object, with one key/value pair for each field in the standard status output.

Examples of the JSON output for each status output are provided below. For more information on the fields displayed, see Section D.2, "Generated Field Reference".

trepctl status JSON Output

```json
{
  "uptimeSeconds": "2128.682",
  "masterListenUri": "thl://host1:2112/",
  "clusterName": "default",
  "pendingExceptionMessage": "NONE",
  "appliedLastEventId": "mysql-bin.000007:0000000000001353;0",
  "pendingError": "NONE",
  "resourcePrecedence": "99",
  "transitioningTo": "",
  "offlineRequests": "NONE",
  "simpleServiceName": "alpha",
  "extensions": "",
  "pendingErrorEventId": "NONE",
  "sourceId": "host1",
  "serviceName": "alpha",
  "version": "Tungsten Replicator 2.0.5 build 11",
  "role": "master",
  "currentTimeMillis": "1369233410874",
  "masterConnectUri": "",
  "rmiPort": "10000",
  "siteName": "default",
  "pendingErrorSeqno": "-1",
  "pipelineSource": "jdbc:mysql:thin://host1:3306/",
  "pendingErrorCode": "NONE",
  "maximumStoredSeqNo": "2504",
  "latestEpochNumber": "2500",
  "channels": "1",
}
```
8.18.3.19.2.1. Detailed Status: Channel Assignments JSON Output

```
shell> trepctl status -name channel-assignments -json
[
  {
    "channel" : "0",
    "shard_id" : "cheffy"
  },
  {
    "channel" : "0",
    "shard_id" : "tungsten_alpha"
  }
]
```

8.18.3.19.2.2. Detailed Status: Services JSON Output

```
shell> trepctl status -name services -json
[
  {
    "totalAssignments" : "2",
    "accessFailures" : "0",
    "storeClass" : "com.continuent.tungsten.replicator.channel.ChannelAssignmentService",
    "name" : "channel-assignment",
    "maxChannel" : "0"
  }
]
```

8.18.3.19.2.3. Detailed Status: Shards JSON Output

```
shell> trepctl status -name shards -json
[
  {
    "stage" : "q-to-dbms",
    "appliedLastEventId" : "mysql-bin.000007:0000000007224342:0",
    "appliedLatency" : "63.099",
    "appliedLastSeqno" : "2514",
    "eventCount" : "16",
    "shardId" : "cheffy"
  }
]
```

8.18.3.19.2.4. Detailed Status: Stages JSON Output

```
shell> trepctl status -name stages -json
[
  {
    "applier.name" : "thl-applier",
    "applier.class" : "com.continuent.tungsten.replicator.thl.THLStoreApplier",
    "name" : "remote-to-thl",
    "extractor.name" : "thl-remote",
    "taskCount" : "1",
    "committedMinSeqno" : "2504",
    "blockCommitRowCount" : "1",
    "processedMinSeqno" : "-1",
    "extractor.class" : "com.continuent.tungsten.replicator.thl.RemoteTHLExtractor"
  },
  {
    "applier.name" : "parallel-q-applier",
    "applier.class" : "com.continuent.tungsten.replicator.storage.InMemoryQueueAdapter",
    "name" : "thl-to-q",
    "extractor.name" : "thl-extractor",
    "taskCount" : "1",
    "committedMinSeqno" : "2504",
    "blockCommitRowCount" : "10",
    "processedMinSeqno" : "-1",
    "extractor.class" : "com.continuent.tungsten.replicator.thl.THLStoreExtractor"
  },
  {
    "applier.name" : "dbms",
    "applier.class" : "com.continuent.tungsten.replicator.applier.MySQLDrizzleApplier",
    "filter.2.name" : "bidiSlave",
    "name" : "q-to-dbms"
  }
]
8.18.3.19.2.5. Detailed Status: Stores JSON Output

curl -X POST http://localhost:8081/trepctl/status -H 'Content-Type: application/json' -d '{
  "name" : "thl",
  "fsyncOnFlush" : "false",
  "storeClass" : "com.continuent.tungsten.replicator.thl.THL",
  "maximumStoredSeqNo" : "2565",
  "minimumStoredSeqNo" : "2047",
  "logFileRetainMillis" : "604800000",
  "storeClass" : "com.continuent.tungsten.replicator.storage.InMemoryQueueStore",
  "maxSize" : "10",
  "storeSize" : "7",
  "name" : "parallel-queue",
  "eventCount" : "119"
}'

8.18.3.19.2.6. Detailed Status: Tasks JSON Output

curl -X POST http://localhost:8081/trepctl/status -H 'Content-Type: application/json' -d '{
  "taskId" : "0",
  "state" : "extract",
  "extractTime" : "604.297",
  "applyTime" : "16.708",
  "averageBlockSize" : "0.982",
  "script" : "mysql-bin.000007:0000000111424440;0",
  "appliedLastEventId" : "mysql-bin.000007:0000000111424440;0",
  "appliedLatency" : "63.787",
  "currentLastEventId" : "mysql-bin.000007:0000000111424440;0",
  "eventCount" : "219",
  "appliedLastSeqno" : "2565",
  "cancelled" : "false"
}'
8.18.3.2.7. Detailed Status: Tasks JSON Output

```
{
  "filterTime": "0.263",
  "stage": "q-to-dbms",
  "currentLastFragno": "1",
  "taskId": "0",
  "currentLastSeqno": "2614",
  "state": "apply",
  "extractTime": "533.471",
  "applyTime": "61.618",
  "averageBlockSize": "1.160",
  "otherTime": "24.052",
  "appliedLastEventId": "mysql-bin.000007:0000000110392640;0",
  "appliedLatency": "63.178",
  "currentLastEventId": "mysql-bin.000007:0000000110392711;0",
  "eventCount": "217",
  "appliedLastSeqno": "2614",
  "cancelled": "false"
}
```

8.18.3.20. `trepctl status` Command

```
8.18.3.20. trepctl stop Command

Deprecated in 2.0.1. This command was deprecated in 2.0.1; use Section 8.18.3.21, "trepctl unload Command".

Stop the replicator service.

```
trepctl stop [ -y ]
```

Stop the replicator service entirely. An interactive prompt is provided to confirm the shutdown:

```
shell> trepctl stop
Do you really want to stop replication service alpha? [yes/NO]
```

To disable the prompt, use the `-y` option:

```
shell> trepctl stop -y
Service stopped successfully: name=alpha
```

The name of the service stopped is provided for confirmation.

8.18.3.21. `trepctl unload` Command

```
8.18.3.21. trepctl unload Command

Unload the replicator service.

```
trepctl unload [ -y ]
```

Unload the replicator service entirely. An interactive prompt is provided to confirm the shutdown:

```
shell> trepctl unload
Do you really want to unload replication service alpha? [yes/NO]
```

To disable the prompt, use the `-y` option:

```
shell> trepctl unload -y
Service unloaded successfully: name=alpha
```

The name of the service unloaded is provided for confirmation.

8.18.3.22. `trepctl wait` Command

The `trepctl wait` command waits for the replicator to enter a specific state, or for a specific sequence number to be applied to the dataserver.

```
trepctl wait [ -applied seqno ] [ -limit s ] [ -state st ]
```

Where:

Table 8.43. `trepctl wait` Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-applied seqno</code>[285]</td>
<td>Specify the sequence number to be waited for</td>
</tr>
<tr>
<td><code>-limit s</code>[285]</td>
<td>Specify the number of seconds to wait for the operation to complete</td>
</tr>
</tbody>
</table>
Command-line Tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-state st</td>
<td>Specify a state to be waited for</td>
</tr>
</tbody>
</table>

The command will wait for the specified occurrence, of either a change in the replicator status (i.e. ONLINE), or for a specific sequence number to be applied. For example, to wait for the replicator to go into the ONLINE state:

```
shell> trepctl wait -state ONLINE
```

This can be useful in scripts when the state maybe changed (for example during a backup or restore operation), allowing for an operation to take place once the requested state has been reached. Once reached, trepctl returns with exit status 0.

To wait a specific sequence number to be applied:

```
shell> trepctl wait -applied 2000
```

This can be useful when performing bulk loads where the sequence number where the bulk load completed is known, or when waiting for a specific sequence number from the master to be applied on the slave. Unlike the offline-deferred operation, no change in the replicator is made. Instead, trepctl simply returns with exit status 0 when the sequence number has bee successfully applied.

If the optional -limit option is used, then trepctl waits for the specified number of seconds for the request event to occur. For example, to wait for 10 seconds for the replicator to go online:

```
shell> trepctl wait -state ONLINE -limit 10
wait timed out!
```

If the requested event does not take place before the specified time limit expires, then trepctl returns with the message 'Wait timed out!', and an exit status of 1.

8.19. The tpasswd Command

Table 8.44. tpasswd Common Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--create, c</td>
<td>Creates a new user/password</td>
</tr>
<tr>
<td>-delete, d</td>
<td>Delete a user/password combination</td>
</tr>
<tr>
<td>-e, --encrypted.password</td>
<td>Encrypt the password</td>
</tr>
<tr>
<td>-f, --file</td>
<td>Specify the location of the security.properties file</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display help text</td>
</tr>
<tr>
<td>-p, --password.file.location</td>
<td>Specify the password file location</td>
</tr>
<tr>
<td>-t, --target</td>
<td>Specify the target application</td>
</tr>
<tr>
<td>-ts, --truststore.location</td>
<td></td>
</tr>
</tbody>
</table>

8.20. The tungsten_health_check Script

The script was added in Continuent Tungsten 2.0.1. It cannot be backported to older versions.

The tungsten_health_check may be used less frequently than Section 8.21, “The tungsten_monitor Script” to check the cluster against known best practices. It implements the Tungsten Script Interface as well as these additional options.

```
tungsten_health_check [ --dataservices ] [ --diagnostic-package ] [ --directory ] [ --email ] [ --force ] [ --from ] [ --help, h ] [ --ignore ] [ --info, i ] [ --json ] [ --lock-dir ] [ --lock-timeout ] [ --mail ] [ --net-ssh-option=key=value ] [ --notice, n ] [ --show-differences ] [ --subject ] [ --test-failover ] [ --test-recover ] [ --test-switch ] [ --validate ] [ --verbose, v ]
```

Where:

Table 8.45. tungsten_health_check Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservices</td>
<td>This list of dataservices to monitoring to</td>
</tr>
<tr>
<td>--diagnostic-package</td>
<td>Create a diagnostic package if any issues are found</td>
</tr>
<tr>
<td>--directory</td>
<td>The $CONTINUENT_ROOT directory to use for running this command. It will default to the directory you use to run the script.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
--email | Email address to send to when mailing any notifications
--force | Continue operation even if script validation fails
--from | The from address for sending messages
--help, -h | Show help text
--ignore | Ignore notices that use this key
--info, -i | Display info, notice, warning, and error messages
--json | Output all messages and the return code as a JSON object
--lock-dir | Directory to store log and lock files in
--lock-timeout | The number of minutes to sleep a notice after sending it
--mail | Path to the mail program to use for sending messages
--net-ssh-option=key=value | Provide custom SSH options to use for SSH communication to other hosts.
--notice, -n | Display notice, warning, and error messages
--show-differences | Show any differences in Tungsten configuration
--subject | Email subject line
--test-failover | Test failover for each managed dataservice
--test-recover | Test recover for each managed dataservice
--test-switch | Test the switch command for each managed dataservice
--validate | Only run script validation
--verbose, -v | Verbose

Each time the `tungsten_health_check` runs, it will run a standard set of checks. Additional checks may be turned on using command line options.

- Check for errors using `tpm validate`
- Check that all servers in the dataservice are running the same version of Continuent Tungsten

The script can be run manually:

```
shell> tungsten_health_check
```

All messages will be sent to `/opt/continuent/share/tungsten_health_check/lastrun.log`.

Sending results via email

The `tungsten_health_check` is able to send you an email when problems are found. It is suggested that you run the script as root so it is able to use the mail program without warnings.

Alerts are cached to prevent them from being sent multiple times and flooding your inbox. You may pass `--reset` to clear out the cache or `--lock-timeout` to adjust the amount of time this cache is kept. The default is 3 hours.

```
shell> tungsten_health_check --from=you@yourcompany.com --to=group@yourcompany.com
```

Showing manual configuration file changes

The `tpm validate` command will fail if you have manually changed a configuration file. The file differences may be added if you include the `--show-differences` argument.

Testing Continuent Tungsten functionality

Continuent Tungsten includes a testing infrastructure that you can use at any time. By adding the `--test-switch`, `--test-failover` or `--test-recover` arguments to the command, we will test these operations on each database server.

**Caution**

This will have an impact on dataservice availability. Limit this operation to maintenance windows or times when you can experience managed outages.

**Compatibility**
The script only works with MySQL at this time.

### 8.21. The `tungsten_monitor` Script

The script was added in Continuent Tungsten 2.0.1. It cannot be backported to older versions.

The `tungsten_monitor` script provides a mechanism for monitoring the cluster state when monitoring tools like Nagios aren't available. It implements the Tungsten Script Interface as well as these additional options.

```
tungsten_monitor [ --check-log ] [ --connector-timeout ] [ --dataservices ] [ --diagnostic-package ] [ --directory ] [ --disk ] [ --elb-script ] [ --email ] [ --force ] [ --help, -h ] [ --ignore ] [ --info, -i ] [ --json ] [ --latency ] [ --lock-dir ] [ --lock-timeout ] [ --mail ] [ --max-backup-age ] [ --net-ssh-option ] [ --notice, -n ] [ --reset ] [ --subject ] [ --validate ] [ --verbose, -v ]
```

Where:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--check-log</td>
<td>Email any lines in the log file that match the egrep expression. --check-log=tungsten-manager/log/tmsvc.log:OFFLINE</td>
</tr>
<tr>
<td>--connector-timeout</td>
<td>Number of seconds to wait for a connector response</td>
</tr>
<tr>
<td>--dataservices</td>
<td>This list of dataservices to monitoring to</td>
</tr>
<tr>
<td>--diagnostic-package</td>
<td>Create a diagnostic package if any issues are found</td>
</tr>
<tr>
<td>--directory</td>
<td>The CONTINUENT_ROOT directory to use for running this command. It will default to the directory you use to run the script.</td>
</tr>
<tr>
<td>--disk</td>
<td>Display a warning if any disk usage is above this percentage</td>
</tr>
<tr>
<td>--elb-script</td>
<td>The xinetd script name that is responding to ELB liveness checks</td>
</tr>
<tr>
<td>--email</td>
<td>Email address to send to when mailing any notifications</td>
</tr>
<tr>
<td>--force</td>
<td>Continue operation even if script validation fails</td>
</tr>
<tr>
<td>--help, -h</td>
<td>Show help text</td>
</tr>
<tr>
<td>--ignore</td>
<td>Ignore notices that use this key</td>
</tr>
<tr>
<td>--info, -i</td>
<td>Display info, notice, warning, and error messages</td>
</tr>
<tr>
<td>--json</td>
<td>Output all messages and the return code as a JSON object</td>
</tr>
<tr>
<td>--latency</td>
<td>The maximum allowed latency for replicators</td>
</tr>
<tr>
<td>--lock-dir</td>
<td>Directory to store log and lock files in</td>
</tr>
<tr>
<td>--lock-timeout</td>
<td>The number of minutes to sleep a notice after sending it</td>
</tr>
<tr>
<td>--mail</td>
<td>Path to the mail program to use for sending messages</td>
</tr>
<tr>
<td>--max-backup-age</td>
<td>Maximum age in seconds of valid backups</td>
</tr>
<tr>
<td>--net-ssh-option</td>
<td>Provide custom SSH options to use for communication to other hosts.</td>
</tr>
<tr>
<td>--notice, -n</td>
<td>Display notice, warning, and error messages</td>
</tr>
<tr>
<td>--reset</td>
<td>Remove all entries from the lock directory</td>
</tr>
<tr>
<td>--subject</td>
<td>Email subject line</td>
</tr>
<tr>
<td>--validate</td>
<td>Only run script validation</td>
</tr>
<tr>
<td>--verbose, -v</td>
<td>Verbose</td>
</tr>
</tbody>
</table>

### General Operation

Each time the `tungsten_monitor` runs, it will run a standard set of checks. Additional checks may be turned on using command line options.

- Check that all Tungsten services for this host are running
- Check that all replication services and datasources are ONLINE
- Check that replication latency does not exceed a specified amount
- Check that the local connector is responsive
• Check disk usage

An example of adding it to crontab:

```shell
sh> crontab -l
10 * * * * /opt/continuent/tungsten/cluster-home/bin/tungsten_monitor >/dev/null 2>/dev/null
```

All messages will be sent to `/opt/continuent/share/tungsten_monitor/lastrun.log`.

Sending results via email

The `tungsten_monitor` is able to send you an email when problems are found. It is suggested that you run the script as root so it is able to use the mail program without warnings.

Alerts are cached to prevent them from being sent multiple times and flooding your inbox. You may pass `--reset` to clear out the cache or `--lock-timeout` to adjust the amount of time this cache is kept. The default is 3 hours.

```shell
sh> crontab -l
10 * * * * /opt/continuent/tungsten/cluster-home/bin/tungsten_monitor --from=you@yourcompany.com \\n   --to=group@yourcompany.com >/dev/null 2>/dev/null
```

Monitoring log files

The `tungsten_monitor` can optionally monitor log files for certain keywords. This example will alert you to any lines in `trepsvc.log` that include `OFFLINE`.

```shell
sh> tungsten_monitor --check-log=tungsten-replicator/log/trepsvc.log:OFFLINE
```

Monitoring backup status

Knowing you have a recent backup is an important part any Tungsten deployment. The `tungsten_monitor` will look for the latest backup across all datasources and compare it to the value `--max-backup-age`. This example will let you know if a valid backup has not been taken in 3 days.

```shell
sh> tungsten_monitor --max-backup-age=259200
```

Compatibility

The script only works with MySQL at this time.

### 8.22. The `tungsten_nagios_backups` Command

### 8.23. The `tungsten_nagios_online` Command

### 8.24. The `tungsten_provision_slave` Script

The script was added in Continuent Tungsten 2.0.1. It cannot be backported to older versions.

The `tungsten_provision_slave` script allows you to easily provision, or reprovision, a database server using information from a remote host. It implements the Tungsten Script Interface as well as these additional options.

```bash
tungsten_provision_slave [ --clear-logs ] [ --direct ] [ --directory ] [ -f, --force ] [ --help, -h ] [ --info, -i ] [ --json ] [ --mysqldump ] [ --net-ssh-option ] [ --notice, -n ] [ --offline ] [ --offline-timeout ] [ --online ] [ --service ] [ --source ] [ --validate ] [ --verbose, -v ] [ --xtrabackup ]
```

Where:

**Table 8.47. `tungsten_provision_slave` Command-line Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--clear-logs</code></td>
<td>Delete all THL and relay logs for the service</td>
</tr>
<tr>
<td><code>--direct</code></td>
<td>Use the MySQL data directory for staging and preparation</td>
</tr>
<tr>
<td><code>--directory</code></td>
<td>The $CONTINUENT_ROOT directory to use for running this command. It will default to the directory you use to run the script.</td>
</tr>
<tr>
<td><code>--force, -f</code></td>
<td>Continue operation even if script validation fails</td>
</tr>
<tr>
<td><code>--help, -h</code></td>
<td>Show help text</td>
</tr>
<tr>
<td><code>--info, -i</code></td>
<td>Display info, notice, warning, and error messages</td>
</tr>
</tbody>
</table>
## Command-line Tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--json</code></td>
<td>Output all messages and the return code as a JSON object</td>
</tr>
<tr>
<td><code>--mysqldump</code></td>
<td>Use mysqldump for generating the information</td>
</tr>
<tr>
<td><code>--net-ssh-option</code></td>
<td>Provide custom SSH options to use for SSH communication to other hosts.</td>
</tr>
<tr>
<td><code>--notice, -n</code></td>
<td>Display notice, warning, and error messages</td>
</tr>
<tr>
<td><code>--offline</code></td>
<td>Put required replication services offline before processing</td>
</tr>
<tr>
<td><code>--offline-timeout</code></td>
<td>Put required replication services offline before processing</td>
</tr>
<tr>
<td><code>--online</code></td>
<td>Put required replication services online after successful processing</td>
</tr>
<tr>
<td><code>--service</code></td>
<td>Replication service to read information from</td>
</tr>
<tr>
<td><code>--source</code></td>
<td>Server to use as a source for the backup</td>
</tr>
<tr>
<td><code>--validate</code></td>
<td>Only run script validation</td>
</tr>
<tr>
<td><code>--verbose, -v</code></td>
<td>Show verbose information during processing</td>
</tr>
<tr>
<td><code>--xtrabackup</code></td>
<td>Use xtrabackup for generating the information</td>
</tr>
</tbody>
</table>

The script will automatically put all replication services offline prior to beginning. If the services were online, the script will put them back online following a successful completion. All THL logs will be cleared prior to going online. The replicator will start replication from the position reflected on the source host.

Provisioning will fail from a slave that is stopped, or if the slave is not in either the ONLINE or OFFLINE:NORMAL (in [Tungsten Replicator 2.2 Manual]) states. This can be overridden by using the -f or --force options.

When provisioning masters, for example in fan-in (in [Tungsten Replicator 2.2 Manual]), multi-master, or when recovering a failed master in a standard master-slave topology, the service must be reset with the trepctl reset after the command is finished. The service must also be reset on all slaves.

The `--service` argument is used to determine which database server should be provisioned. If there are multiple services defined in the replicator and one of those is a master, the master service must be specified.

### Using xtrabackup

The script will use Xtrabackup by default. It will run validation prior to starting to make sure the needed scripts are available. The provision process will run Xtrabackup on the source server and stream the contents to the server you are provisioning. Passing the `--direct` Option will empty the MySQL data directory prior to doing the backup and place the streaming backup there. After taking the backup, the script will prepare the directory and restart the MySQL server.

### Using mysqldump

If you have a small dataset or don't have Xtrabackup, you may pass the `--mysqldump` option to use it. It implements the Tungsten Script Interface as well as these additional options.

### Compatibility

The script only works with MySQL at this time.

### 8.25. The `tungsten_read_master_events` Script

The script was added in Continuent Tungsten 2.0.1. It cannot be backported to older versions.

The `tungsten_read_master_events` displays the raw contents of the master datasource for the given THL records. It implements the Tungsten Script Interface as well as these additional options.


Where:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--directory</code></td>
<td>The $CONTINUENT_ROOT directory to use for running this command. It will default to the directory you use to run the script.</td>
</tr>
</tbody>
</table>
### Command-line Tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force</td>
<td>Continue operation even if script validation fails</td>
</tr>
<tr>
<td>--help, -h</td>
<td>Show help text</td>
</tr>
<tr>
<td>--high</td>
<td>Display events ending with this sequence number</td>
</tr>
<tr>
<td>--info, -i</td>
<td>Display info, notice, warning, and error messages</td>
</tr>
<tr>
<td>--json</td>
<td>Output all messages and the return code as a JSON object</td>
</tr>
<tr>
<td>--low</td>
<td>Display events starting with this sequence number</td>
</tr>
<tr>
<td>--net-ssh-option</td>
<td>Provide custom SSH options to use for SSH communication to other hosts.</td>
</tr>
<tr>
<td>--notice, -n</td>
<td>Display notice, warning, and error messages</td>
</tr>
<tr>
<td>--service</td>
<td>Replication service to read information from</td>
</tr>
<tr>
<td>--source</td>
<td>Determine metadata for the --after, --low, --high statements from this host</td>
</tr>
<tr>
<td>--validate</td>
<td>Only run script validation</td>
</tr>
<tr>
<td>--verbose, -v</td>
<td>Show verbose information during processing</td>
</tr>
</tbody>
</table>

### Display all information after a specific sequence number

This may be used when you have had a master failover or would like to see everything that happened after a certain event. It will read the start position from the sequence number passed and allow you to see all events, even if they were not extracted by the replication service.

```
shell> tungsten_read_master_events --after=1792
```

### Display information between two sequence numbers

This will show the raw master data between the two sequence numbers. It is inclusive so the information for the --low option will be included. This will only work if the sourcelid for both sequence numbers is the same.

```
shell> tungsten_read_master_events --low=4582 --high=4725
```

### Compatibility

The script only works with MySQL at this time.

The script was added in Continuent Tungsten 2.0.1 and Tungsten Replicator 2.2.0. It cannot be backported to older versions.

#### 8.26. The `tungsten_set_position` Script

The script was added in Continuent Tungsten 2.0.1. It cannot be backported to older versions.

The `tungsten_set_position` updates the `trep_commit_seqno` table to reflect the given THL sequence number or provided information. It implements the Tungsten Script Interface as well as these additional options.

```
tungsten_set_position [ --clear-logs ] [ --epoch ] [ --event-id ] [ --high ] [ --offline ] [ --offline-timeout ] [ --online ] [ --replicate-statements ] [ --seqno ] [ --service ] [ --source ] [ --source-id ] [ --sql ]
```

Where:

### Table 8.49. `tungsten_set_position` Command-line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--clear-logs</td>
<td>Delete all THL and relay logs for the service</td>
</tr>
<tr>
<td>--epoch</td>
<td>The epoch number to use for updating the <code>trep_commit_seqno</code> table</td>
</tr>
<tr>
<td>--event-id</td>
<td>The event id to use for updating the <code>trep_commit_seqno</code> table</td>
</tr>
<tr>
<td>--high</td>
<td>Display events ending with this sequence number</td>
</tr>
<tr>
<td>--low</td>
<td>Display events starting with this sequence number</td>
</tr>
<tr>
<td>--offline</td>
<td>Put required replication services offline before processing</td>
</tr>
<tr>
<td>--offline-timeout</td>
<td>Put required replication services offline before processing</td>
</tr>
</tbody>
</table>
### Command-line Tools

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--online</td>
<td>Put required replication services online after successful processing</td>
</tr>
<tr>
<td>--replicate-statements</td>
<td>Execute the events so they will be replicated if the service is a master</td>
</tr>
<tr>
<td>--seqno</td>
<td>The sequence number to use for updating the trep_commit_seqno table</td>
</tr>
<tr>
<td>--service</td>
<td>Replication service to read information from</td>
</tr>
<tr>
<td>--source</td>
<td>Determine metadata for the --after, --low, --high statements from this host</td>
</tr>
<tr>
<td>--source-id</td>
<td>The source id to use for updating the trep_commit_seqno table</td>
</tr>
<tr>
<td>--sql</td>
<td>Only output the SQL statements needed to update the schema</td>
</tr>
</tbody>
</table>

### General Operation

In order to update the trep_commit_seqno table, the replication service must be offline. You may pass the --offline option to do that for you. The --online option will put the replication services back online at successful completion.

In most cases you will want to pass the --clear-logs argument so that all THL and relay logs are delete from the server following provisioning. This ensures that any corrupted or inconsistent THL records are removed prior to replication coming back online.

The --service argument is used to determine which database server should be provisioned.

This command will fail if there is more than one record in the trep_commit_seqno table. This may happen if parallel replication does not stop cleanly. You may bypass that error with the --force option.

#### Update trep_commit_seqno with information from a THL event

This will read the THL information from the host specified as --source.

```shell
tungsten_set_position --seqno=5273 --source=db1
```

#### Update trep_commit_seqno with specific information

The script will also accept specific values to update the trep_commit_seqno table. This may be used when bringing a new master service online or when the THL event is no longer available.

```shell
tungsten_set_position --seqno=5273 --epoch=5264 --source-id=db1
tungsten_set_position --seqno=5273 --epoch=5264 --source-id=db1 --event-id=mysql-bin.000025:0000000000000421
```

### Compatibility

The script only works with MySQL at this time.

### 8.27. The undeployall Command

The undeployall command removes startup the startup and reboot scripts crteated by deployall, disabling automatic startup and shutdown of available services.

To use, the tool should be executed with superuser privileges, either directly using sudo, or by logging in as the superuser and running the command directly:

```shell
sudo deployall
```

Removing any system startup links for /etc/init.d/treplicator ...
/etc/rc0.d/K80treplicator
/etc/rc1.d/K80treplicator
/etc/rc2.d/S80treplicator
/etc/rc3.d/S80treplicator
/etc/rc4.d/S80treplicator
/etc/rc5.d/S80treplicator
/etc/rc6.d/K80treplicator

To enable the scripts on the system, use deployall.

### 8.28. The updateCDC.sh Command

The updateCDC.sh script updates and existing configuration for Oracle CDC, updating for new tables and user/password configuration.
The script accepts one argument, the filename of the configuration file that will define the CDC configuration. The file accepts the parameters as listed in Table 8.29, "setupCDC.conf Configuration Options".

To use, supply the name of the configuration file:

```
shell> ./updateCDC.sh sample.conf
```

8.29. The `zabbix_tungsten_latency` Command

8.30. The `zabbix_tungsten_online` Command

8.31. The `zabbix_tungsten_progress` Command

8.32. The `zabbix_tungsten_services` Command
Chapter 9. The tpm Deployment Command

tpm, or the Tungsten Package Manager, is a complete configuration, installation and deployment tool for Continuent Tungsten. It includes some utility commands to simplify those and other processes. In order to provide a stable system, all configuration changes must be completed using tpm. tpm makes use of ssh enabled communication and the sudo support as required by the Appendix C, Prerequisites.

tpm can operate in two different ways when performing a deployment:

- **tpm staging configuration** — a tpm configuration is created by defining the command-line arguments that define the deployment type, structure and any additional parameters. tpm then installs all the software on all the required hosts by using ssh to distribute Continuent Tungsten and the configuration, and optionally automatically starts the services on each host. tpm manages the entire deployment, configuration and upgrade procedure.

- **tpm INI configuration** — tpm uses an INI file to configure the service on the local host. The INI file must be create on each host that will run Continuent Tungsten. tpm only manages the services on the local host; in a multi-host deployment, upgrades, updates, and configuration must be handled separately on each host.

For a more detailed comparison of the two systems, see Section 9.1, “Comparing Staging and INI tpm Methods”.

During the staging-based configuration, installation and deployment, the tpm tool works as follows:

- tpm creates a local configuration file that contains the basic configuration information required by tpm. This configuration declares the basic parameters, such as the list of hosts, topology requirements, username and password information. These parameters describe top-level information, which tpm translates into more detailed configuration according to the topology and other settings.

- Within staging-based configuration, each host is accessed [using ssh], and various checks are performed, for example, checking database configuration, whether certain system parameters match required limits, and that the environment is suitable for running Continuent Tungsten.

- During an installation or upgrade, tpm copies the current distribution to each remote host.

- The core configuration file is then used to translate a number of template files within the configuration of each component of the system into the configuration properties files used by Continuent Tungsten. The configuration information is shared on every configured host within the service; this ensures that in the event of a host failure, the configuration can be recovered.

- The components of Continuent Tungsten are then started [installation] or restarted according to the configuration options.

Where possible, these steps are conducted in parallel to speed up the process and limit the interruption to services and operations.

This method of operation ensures:

- Active configurations and properties are not updated until validation is completed. This prevents a running Continuent Tungsten installation from being affected by an incompatible or potentially dangerous change to the configuration.

- Enables changes to be made to the staging configuration before the configuration is deployed.

- Services are not stopped/restarted unnecessarily.

- During an upgrade or update, the time required to reconfigure and restart is kept to a minimum.

Because of this safe approach to performing configuration, downtime is minimized, and the configuration is always based on files that are separate from, and independent of, the live configuration.

**Important**

tpm always creates the active configuration from the combination of the template files and parameters given to tpm. This means that changes to the underlying property files with the Continuent Tungsten configuration are overwritten by tpm when the service is configured or updated.

In addition to the commands that tpm supports for the installation and configuration, the command also supports a number of other utility and information modes, for example, the fetch command retrieves existing configuration information to your staging, while query returns information about an active configuration.

Using tpm is divided up between the commands that define the operation the command will perform, which are covered in Section 9.5, “tpm Commands”; configuration options, which determine the parameters that configure individual services, which are detailed in Section 9.8, “tpm Configuration Options”; and the options that alter the way tpm operates, covered in Section 9.3, “tpm Staging Configuration”.

293
9.1. Comparing Staging and INI tpm Methods

tpm supports two different deployment methodologies. Both configure one or more Continuent Tungsten services, in a safe and secure manner, but differ in the steps and process used to complete the installation. The two methods are:

- **Staging Directory**

When using the staging directory method, a single configuration that defines all services and hosts within the Continuent Tungsten deployment is created. tpm then communicates with all the hosts you are configuring to install and configure the different services required. This is best when you have a consistent configuration for all hosts and do not have any configuration management tools for your systems.

Figure 9.1. tpm Staging Based Deployment

- **INI File**

When using the INI file method, configuration for each service must be made individually using an INI configuration file on each host. This is ideal for deployments where you have a configuration management system (e.g. Puppet and Chef) to manage the INI file. It also works very well for deployments where the configuration for each system is different from the others.
The tpm Deployment Command

Figure 9.2. tpm INI Based Deployment

Table 9.1. TPM Deployment Methods

<table>
<thead>
<tr>
<th>Feature</th>
<th>Staging Directory</th>
<th>INI File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Multiple Services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy to Multiple Hosts</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Individual Host-based Configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single-Step Upgrade</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Requires SSH Configuration</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RPM/PKG Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note

Check the output of `tpm query staging` to determine which method your current installation uses. The output for an installation from a staging directory will start with `# Installed from tungsten@staging-host:/opt/continuent/software/continuent-tungsten-2.0.5-11`. An installation based on an INI file may include this line but the hostname will reference the current host and there will be an `/etc/tungsten/tungsten.ini` file present.

To install a three-node service using the staging method:

1. Extract Continuent Tungsten on your staging server.
2. On each host:
   a. Complete all the Appendix C, Prerequisites, including setting the ssh keys.
3. Execute the `tpm configure` and `tpm install` commands to configure and deploy the service from the staging server.

To install a three-node service using the INI method:

1. On each host:
   a. Extract Continuent Tungsten.
   b. Complete all the Appendix C, Prerequisites.
c. Create the INI file containing your configuration.

d. Execute the **tpm install** command to deploy the service.

When using the staging method, upgrades and updates to the configuration must be made using **tpm** from the staging directory. Configuration methods can be swapped from staging to INI only by manually recreating the INI file with the new configuration and running **tpm update**.

### 9.2. Processing Installs and Upgrades

The **tpm** command is designed to coordinate the deployment activity across all hosts in a dataservice. This is done by completing a stage on all hosts before moving on. These operations will happen on each host in parallel and **tpm** will wait for the results to come back before moving on.

- **Copy Continuent Tungsten and deployment files to each server**

  During this stage part of the Continuent Tungsten package is copied to each server. At this point only the **tpm** command is copied over so we can run validation checks locally on each machine.

  The configuration is also transferred to each server and checked for completeness. This will run some commands to make sure that we have all of the settings needed to run a full validation.

- **Validate the configuration settings**

  Each host will validate the configuration based on validation classes. This will do things like check file permissions and database credentials. If errors are found during this stage, they will be summarized and the script will exit.

  ```
  # Validation failed
  ERROR >> host3 >> Password specified for app@% does not match the running instance on » tungsten@host3:13306 (WITH PASSWORD). This may indicate that the user has a password » using the old format. (MySQLConnectorPermissionsCheck)
  # Errors for host2
  ERROR >> host2 >> Password specified for app@% does not match the running instance on » tungsten@host2:13306 (WITH PASSWORD). This may indicate that the user has a password » using the old format. (MySQLConnectorPermissionsCheck)
  # Errors for host1
  ERROR >> host1 >> Password specified for app@% does not match the running instance on » tungsten@host1:13306 (WITH PASSWORD). This may indicate that the user has a password » using the old format. (MySQLConnectorPermissionsCheck)
  ```

  At this point you should verify the configuration settings and retry the **tpm install** command. Any errors found during this stage may be skipped by running **tpm configure alpha --skip-validation-check=MySQLConnectorPermissionsCheck**. When re-running the **tpm install** command this check will be bypassed.

- **Deploy Continuent Tungsten and write configuration files**

  If validation is successful, we will move on to deploying Continuent Tungsten and writing the actual configuration files. The **tpm** command uses a JSON file that summarizes the configuration. The Continuent Tungsten processes use many different files to store the configuration and **tpm** is responsible for writing them.

  The `/opt/continuent/releases` directory will start to collect multiple directories after you have run multiple upgrades. We keep the previous versions of Continuent Tungsten in case a downgrade is needed or for review at a later date. If your upgrade has been successful, you can remove old directories. Make sure you do not remove the directory that is linked to by the `/opt/continuent/tungsten` symlink.

  **Note**

  Do not change Continuent Tungsten configuration files by hand. This will cause future updates to fail. One of the validation checks compares the file that **tpm** written with the current file. If there are differences, validation will fail.

  This is done to make sure that any configuration changes made by hand are not wiped out without giving you a chance to save them. You can run **tpm query modified-files** to see what, if any, changes have been made.

- **Start Continuent Tungsten services**
After Continuent Tungsten is fully configured, the `tpm` command will start services on all of the hosts. This process is slightly different depending on if you are doing a clean install or an upgrade.

- **Install**
  1. Check if `--start` or `--start-and-report` were provided in the configuration
  2. Start the Tungsten Replicator and Tungsten Manager on all hosts
  3. Wait for the Tungsten Manager to become responsive
  4. Start the Tungsten Connector on all hosts

- **Upgrade**
  1. Put all dataservices into `MAINTENANCE` mode
  2. Stop the Tungsten Replicator and Tungsten Manager on all nodes
  3. Start the Tungsten Replicator and Tungsten Manager on all hosts if the services were previously running
  4. Wait for the Tungsten Manager to become responsive
  5. Stop the old Tungsten Connector and Start the new Tungsten Connector on all hosts. This step is done one host at a time so that there is always one Tungsten Connector running. If `--no-connectors` was provided on the command line then this will not occur. You must go to each server running Tungsten Connector and run `tpm promote-connector`.

### 9.3. `tpm` Staging Configuration

Before installing your hosts, you must provide the desired configuration. This will be done with one or more calls to `tpm configure` as seen in the Chapter 2, Deployment. These calls place the given parameters into a staging configuration file that will be used during installation. This is done for dataservices, composite dataservices and replication services.

Instead of a subcommand, `tpm configure` accepts a service name or the word `defaults` as a subcommand. This identifies what you are configuring.

When configuring defaults, the defaults affect all configured services, with individual services able to override or set their own parameters.

```
shell> tpm configure [service_name|defaults] [tpm options] [service configuration options]
```

In addition to the Section 9.8, “`tpm` Configuration Options”, the common options in Table 9.4, “`tpm` Common Options” may be given.

The `tpm` command will store the staging configuration in the staging directory that you run it from. This behavior is changed if you have `$CONTINUENT_PROFILES` or `$REPLICATOR_PROFILES` defined in the environment. If present, `tpm` will store the staging configuration in that directory. Doing this will allow you to upgrade to a new version of the software without having to run the `tpm fetch` command.

If you are running Continuent Tungsten, the `tpm` command will only use `$CONTINUENT_PROFILES`.

If you are running Tungsten Replicator, the `tpm` command will use `$REPLICATOR_PROFILES` if it is available, before using `$CONTINUENT_PROFILES`.

#### 9.3.1. Configuring default options for all services

```
shell> ./tools/tpm configure defaults \
     --replication-user=tungsten \
     --replication-password=secret \
     --replication-port=13306
```

These options will apply to all services in the configuration file. This is useful when working with a composite dataservice or multiple independent services. These options may be overridden by calls to `tpm configure service_name` or `tpm configure service_name --hosts`.

#### 9.3.2. Configuring a single service

```
shell> ./tools/tpm configure alpha \
     --master=host1 \
     --members=host1,host2,host3 \
     --home-directory=/opt/continuent \
     --user=tungsten
```

The configuration options provided following the service name will be associated with the ‘alpha’ dataservice. These options will override any given with `tpm configure defaults`. 

297
9.3.3. Configuring a single host

```
shell> ./tools/tpm configure alpha --hosts=host3 --backup-method=xtrabackup-incremental
```

This will apply the `--repl-backup-method` option to just the host3 server. Multiple hosts may be given as a comma-separated list. The names used in the `--members`, `--slaves`, `--master`, `--connectors` options should be used when calling `--hosts`. These values will override any given in `tpm configure defaults` or `tpm configure alpha`.

9.3.4. Reviewing the current configuration

You may run the `tpm reverse` command to review the list of configuration options. This will run in the staging directory and in your installation directory. It is a good idea to run this command prior to installation and upgrades to validate the current settings.

```
shell> ./tools/tpm reverse
# Defaults for all data services and hosts
tools/tpm configure defaults
  --application-password=secret
  --application-port=3306
  --application-user=app
  --replication-password=secret
  --replication-port=13306
  --replication-user=tungsten
  --start-and-report=true
  --user=tungsten

# Options for the alpha data service
tools/tpm configure alpha
  --connectors=host1,host2,host3
  --master=host1
  --members=host1,host2,host3
```

The output includes all of the `tpm configure` commands necessary to rebuild the configuration. It includes all default, data service, and host specific configuration settings. Review this output and make changes as needed until you are satisfied.

9.3.5. Installation

After you have prepared the configuration file, it is time to install.

```
shell> ./tools/tpm install
```

This will install all services defined in configuration. The installation will be done as explained in Section 9.2, “Processing Installs and Upgrades”. This will include the full set of `--members`, `--slaves`, `--master`, and `--connectors`.

9.3.5.1. Installing a set of specific services

```
shell> ./tools/tpm install alpha,bravo
```

All hosts included in the alpha and bravo services will be installed. The installation will be done as explained in Section 9.2, “Processing Installs and Upgrades”.

9.3.5.2. Installing a set of specific hosts

```
shell> ./tools/tpm install --hosts=host1,host2
```

Only `host1` and `host2` will be installed. The installation will be done as explained in Section 9.2, “Processing Installs and Upgrades”.

9.3.6. Upgrades from a Staging Directory

This process must be run from the staging directory in order to run properly. Determine where the current software was installed from.
The **tpm Deployment Command**

```shell
tpm query staging
```

This outputs the hostname and directory where the software was installed from. Make your way to that host and the parent directory before proceeding. Unpack the new software into the `/opt/continuent/software` directory and make it your current directory.

```shell
tar zxf continuent-tungsten-2.0.5-11.tar.gz
cd continuent-tungsten-2.0.5-11
```

**Warning**

Before performing and upgrade, please ensure that you have checked the [*Appendix C, Prerequisites*](#), as software and system requirements may have changed between versions and releases.

Before any update, the current configuration must be known. If the `$CONTINUENT_PROFILES` or `$REPLICATOR_PROFILES` environment variables were used in the original deployment, these can be set to the directory location where the configuration was stored.

Alternatively, the update can be performed by fetching the existing configuration from the deployed directory by using the `tpm fetch` command:

```shell
tools/tpm fetch --reset --directory=/opt/continuent --hosts=host1,autodetect
```

This will load the configuration into the local staging directory. Review the current configuration before making any configuration changes or deploying the new software.

```shell
tools/tpm reverse
```

This will output the current configuration of all services defined in the staging directory. You can then make changes using `tpm configure` before pushing out the upgrade. Run `tpm reverse` again before `tpm update` to confirm your changes were loaded correctly.

```shell
tools/tpm configure service_name ...
tools/tpm update
```

This will update the configuration file and then push the updates to all hosts. No additional arguments are needed for the `tpm update` command since the configuration has already been loaded.

**Note**

The `tpm update` command may cause a brief outage while restarting the connectors. This will occur if you are upgrading to a new version. You can avoid that with:

```shell
tools/tpm update dataservice --no-connectors
```

The connectors must be updated separately on each server by running:

```shell
tools/tpm promote-connector
```

### 9.3.7. Configuration Changes from a Staging Directory

Where, and how, you make configuration changes depends on where you want the changes to be applied.

**Making Configuration Changes to the Current Host**

You may make changes to a specific host from the `/opt/continuent/tungsten` directory.

```shell
tools/tpm update service_name --thl-log-retention=14d
```

This will update the local configuration with the new settings and restart the replicator. You can use the `tpm help update` command to see which components will be restarted.

```shell
tools/tpm help update | grep thl-log-retention
```

If you make changes in this way then you must be sure to run `tpm fetch` from your staging directory prior to any further changes. Skipping this step may result in you pushing an old configuration from the staging directory.

**Making Configuration Changes to all hosts**

This process must be run from the staging directory in order to run properly. Determine where the current software was installed from.

```shell
tpm query staging
```
The `tpm` Deployment Command

This outputs the hostname and directory where the software was installed from. Make your way to that host and directory before proceeding.

```shell
./tools/tpm fetch --reset --directory=/opt/continuent --hosts=host1,autodetect
```

This will load the configuration into the local staging directory. Review the current configuration before making any configuration changes or deploying the new software.

```shell
./tools/tpm reverse
```

This will output the current configuration of all services defined in the staging directory. You can then make changes using `tpm configure` before pushing out the upgrade. Run `tpm reverse` again before `tpm update` to confirm your changes were loaded correctly.

```shell
./tools/tpm configure service_name ...
```

```shell
./tools/tpm update
```

This will update the configuration file and then push the updates to all hosts. No additional arguments are needed for the `tpm update` command since the configuration has already been loaded.

**Note**

The `tpm update` command may cause a brief outage while restarting the connectors. This will occur if you are upgrading to a new version. You can avoid that with:

```shell
./tools/tpm update dataservice --no-connectors
```

The connectors must be updated separately on each server by running:

```shell
tpm promote-connector
```

### 9.3.8. Converting from INI to Staging

If you currently use the INI installation method and wish to convert to using the Staging method, there is currently no easy way to do that. The procedure involves uninstalling fully on each node, then reinstalling from scratch.

If you still wish to convert from the INI installation method to using the Staging method, use the following procedure:

1. Place cluster(s) in Maintenance Mode:

   ```shell
cctrl
   cctrl> set policy maintenance
   ```

2. On the staging node, extract the software into `/opt/continuent/software/{extracted_dir}:

   ```shell
cd /opt/continuent/software
   tar zxf continuent-tungsten-2.0.5-11.tar.gz
   ```

   **Important**
   
   If this is a MSMM topology, make sure you extract both the clustering and replication packages.

3. Create the text file `config.sh` based on the output from `tpm reverse`:

   ```shell
cd continuent-tungsten-2.0.5-11
   tpm reverse > config.sh
   ```

   Review the new `config.sh` script to confirm everything is correct, making any needed edits. When ready, create the new configuration:

   ```shell
   sh config.sh
   ```

   **Important**
   
   If you are using a MSMM topology, repeat these steps using the replicator staging directory. For example:

   ```shell
cd tungsten-replicator-2.0.5-11
   /opt/replicator/tools/tpm reverse > config.sh
   sh config.sh
   ```

   Review the new configuration:

   ```shell
   tools/tpm reverse
   ```
The tpm Deployment Command

See Section 9.3, “tpm Staging Configuration” for more information.

4. On all nodes, uninstall the Tungsten software:

   Warning
   Executing this step WILL cause an interruption of service.

   \[
   \text{shell> tpm uninstall --i-am-sure}
   \]

   Important
   If you are using a MSMM topology, repeat these steps using the replicator tpm command. For example:

   \[
   \text{shell> /opt/replicator/tungsten/tools/tpm uninstall --i-am-sure}
   \]

5. On all nodes, rename the \texttt{tungsten.ini} file:

   \[
   \text{shell> mv /etc/tungsten/tungsten.ini /etc/tungsten/tungsten.ini.old}
   \]

6. On the staging node only, change to the extracted directory and execute the \texttt{tpm install} command:

   \[
   \text{shell> cd /opt/continuent/software/continuent-tungsten-2.0.5-11}
   \]
   \[
   \text{shell> ./tools/tpm install}
   \]

   Important
   If you are using a MSMM topology, repeat the install using the replicator staging directory. For example:

   \[
   \text{shell> cd /opt/continuent/software/tungsten-replicator-2.0.5-11}
   \]
   \[
   \text{shell> ./tools/tpm install}
   \]

7. Once all steps have been completed and the cluster(s) are stable, take each cluster out of maintenance mode by setting the policy back to automatic:

   \[
   \text{shell> cctrl}
   \]
   \[
   \text{cctrl> set policy automatic}
   \]

9.4. tpm INI File Configuration

\texttt{tpm} can use an INI file to manage host configuration. This is a fundamental difference from the normal model for using tpm. When using an INI configuration, the \texttt{tpm} command will only work with the local server.

In order to configure Tungsten on your server using an INI file you must still complete all of the \textit{Appendix C, Prerequisites}. Copying SSH keys between your servers is optional but setting them up makes sure that certain scripts packaged with Continuent Tungsten will still work.

9.4.1. Creating an INI file

When using an INI configuration, installation and updates will still be done using the \texttt{tpm} command. Instead of providing configuration information on the command line, the \texttt{tpm} command will look for an INI file in three files:

1. \texttt{$HOME/tungsten.ini}.
2. \texttt{/etc/tungsten/tungsten.ini}
3. \texttt{/etc/tungsten.ini}

   The INI file(s) must be readable by the tungsten system user.

   Here is an example of a \texttt{tungsten.ini} file that would setup a simple dataservice.

   \[
   \begin{verbatim}
   [defaults]
   application-password=secret
   application-port=1306
   application-user=app
   replication-password=secret
   replication-port=13306
   replication-user=tungsten
   start-and-report=true
   user=tungsten
   \end{verbatim}
   \]
The tpm Deployment Command

The property names in the INI file are the same as what is used on the command line. Simply remove the leading '-' characters and add it to the proper section. Each section in the INI file replaces a single `tpm configure` call. The section name inside of the square brackets is used as the service name. In the case of the `[defaults]` section, this will act like the `tpm configure defaults` command.

Include any host-specific options in the appropriate section. This configuration will only apply to the local server, so there is no need to put host-specific settings in a different section.

### 9.4.2. Installation with INI File

Once you have created the `tungsten.ini` file, the `tpm` command will recognize it and use it for configuration. Unpack the software into `/opt/continuent/software` and run the `tpm install` command.

```
shell> cd /opt/continuent/software
shell> ./tools/tpm install
```

The `tpm` command will read the `tungsten.ini` file and setup all dataservices on the current server.

### 9.4.3. Upgrades with an INI File

Use the `tpm update` command to upgrade to the latest version.

```
shell> cd /opt/continuent/software
shell> tar zxf continuent-tungsten-2.0.5-11.tar.gz
shell> cd continuent-tungsten-2.0.5-11
shell> ./tools/tpm update
```

After unpacking the new software into the staging directory, the `tpm update` command will read the `tungsten.ini` configuration and install the new software. All services will be stopped and the new services will be started.

**Note**

The `tpm update` command may cause a brief outage while restarting the connectors. This will occur if you are upgrading to a new version. You can avoid that with:

```
shell> ./tools/tpm update dataservice --no-connectors
```

The connectors must be updated separately on each server by running:

```
shell> tpm promote-connector
```

During the lifetime of the cluster, switches may happen and the current master may well be a different node than what is reflected in the static ini file in the `master=` line. Normally, this difference is ignored during and update or an upgrade.

However, if a customer has some kind of procedure (i.e. automation) which hand-edits the ini configuration file `master=` line at some point, and such hand-edits do not reflect the current reality at the time of the update/upgrade, an update/upgrade will fail and the cluster may be left in an indeterminate state.

**Warning**

The best practice is to NOT change the `master=` line in the INI configuration file after installation.

There is still a window of opportunity for failure. The update will continue, passing the `CurrentTopologyCheck` test and potentially leaving the cluster in an indeterminate state if the `master=` Option is set to a hostname that is not the current master or the current host.

### 9.4.4. Configuration Changes with an INI file

The `tpm update` also allows you to apply any configuration changes. Start by making any necessary changes to the `tungsten.ini` file. Then proceed to running `tpm update`.

```
shell> cd /opt/continuent/tungsten
shell> ./tools/tpm update
```

This will read the `tungsten.ini` file and apply the settings. The `tpm` command will identify what services likely need to be restarted and will just restart those. You can manually restart the desired services if you are unsure if the new configuration has been applied.
The `tpm update` command may cause a brief outage while restarting the connectors. This will occur if you are upgrading to a new version. You can avoid that with:

```shell
./tools/tpm update dataservice --no-connectors
```

The connectors must be updated separately on each server by running:

```shell
tpm promote-connector
```

### 9.4.5. Converting from Staging to INI

If you currently use the Staging installation method and wish to convert to using INI files, use the following procedure.

You can also try using the script in Section 9.4.6, "Using the `translatetoini.pl` Script".

1. Place cluster(s) in Maintenance Mode:
   ```shell
ctrl c
   c
   set policy maintenance
   ```

2. Create the text file `/etc/tungsten/tungsten.ini` on each node. They will normally all be the same.
   ```shell
   sudo mkdir /etc/tungsten
   sudo chown -R tungsten: /etc/tungsten
   chmod 700 /etc/tungsten
   touch /etc/tungsten/tungsten.ini
   chmod 600 /etc/tungsten/tungsten.ini
   ```

   Each section in the INI file replaces a single `tpm configure` call. The section name inside of [square brackets] is used as the service name. In the case of the [defaults] section, this will act like the `tpm configure defaults` command. The property names in the INI file are the same as what is used on the command line. Simply remove the leading -- characters and add it to the proper section.

   For example, to seed the `tungsten.ini` file, use the output of `tpm reverse`:
   ```shell
tpm reverse > /etc/tungsten/tungsten.ini
   ```

   Edit the new ini file and clean it up as per the rules above. For example, using vim:
   ```shell
   vim /etc/tungsten/tungsten.ini
   :%s/tools/\^tpm configure \[/g
   :%s/^--//g
   :%s/\s*\$//g
   ```

   **Important**
   In the above example, you MUST manually add the trailing square bracket ] to the end of the defaults tag and to the end of every service name section. Just search for the opening square bracket [ and make sure there is a matching closing square bracket for every one.

   See Section 9.4.1, "Creating an INI file" for more information.

3. On every node, extract the software into `/opt/continuent/software/extracted_dir`

   **Warning**
   Make sure you have the same release that is currently installed.

   ```shell
cd /opt/continuent/software
 tar zxf continuum-tungsten-2.0.5-11.tar.gz
 ```

   **Important**
   If this is a MSMM topology, make sure you extract both the clustering and replication packages.

4. On each node, change to the extracted directory and execute the `tpm` command:

   **Warning**
   Execute this step on the slaves first, then switch the master - this procedure will restart the Tungsten services so switch your master to avoid interruption of service. See Section 5.14.3, "Performing Maintenance on an Entire Dataservice" for more information.
The tpm Deployment Command

```shell
cd /opt/continuent/software/continuent-tungsten-2.0.5-11
./tools/tpm update
```

This will read the `tungsten.ini` file and apply the settings. The `tpm` command will identify what services likely need to be restarted and will just restart those. You can manually restart the desired services if you are unsure if the new configuration has been applied.

**Note**

The `tpm update` command may cause a brief outage while restarting the connectors. This will occur if you are upgrading to a new version. You can avoid that with:

```shell
./tools/tpm update_dataservice --no-connectors
```

The connectors must be updated separately on each server by running:

```shell
tpm promote-connector
```

5. If you have a MSMM topology, you must also update the cross-site replicators:

On each node, change to the extracted replicator directory and execute the `tpm` command:

```shell
cd /opt/continuent/software/tungsten-replicator-2.0.5-11
./tools/tpm update
```

6. Once all steps have been completed and the cluster(s) are stable, take each cluster out of maintenance mode by setting the policy back to automatic:

```shell
cctrl
set policy automatic
```

9.4.6. Using the `translatetoini.pl` Script

You can download a script from the documentation library, `translatetoini.pl`. You must have a copy of Perl installed to be able to execute the script.

To use the script, you can either run the script and paste in the staging output, or pipe the output from `tpm reverse` directly into the script. When supplying the staging output, you should supply the output from the within the configured staging directory. For example:

```shell
./tools/tpm reverse|../translatetoini.pl
```

The script will create the file `tungsten.ini` in the current directory containing the converted output.

To change the destination, use the `--filename` option:

```shell
./tools/tpm reverse|../translatetoini.pl --filename=t.ini
```

You can also combine multiple staging configurations into a single INI conversion by appending to an existing INI file by adding the `--append` option:

```shell
./tools/tpm reverse|../translatetoini.pl --append
```

You should always check the INI file before using it for a live installation to ensure that all of the options and parameters have been identified and configured properly.

A training video is available on how to perform the staging to INI file conversion using the `translatetoini.pl` script:

Direct link to video.

9.5. tpm Commands

All calls to `tpm` will follow a similar structure, made up of the command, which defines the type of operation, and one or more options.

```shell
tpm command [sub command] [tpm options] [command options]
```

The command options will vary for each command. The core `tpm` options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--force</code></td>
<td>Do not display confirmation prompts or stop the configure process for errors</td>
</tr>
</tbody>
</table>

304
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help [305], -h [305]</td>
<td>Displays help message</td>
</tr>
<tr>
<td>--info [305], -i [305]</td>
<td>Display info, notice, warning and error messages</td>
</tr>
<tr>
<td>--notice [305], -n [305]</td>
<td>Display notice, warning and error messages</td>
</tr>
<tr>
<td>--preview [305], -p [305]</td>
<td>Displays the help message and preview the effect of the command line options</td>
</tr>
<tr>
<td>--profile file [305]</td>
<td>Sets name of config file</td>
</tr>
<tr>
<td>--quiet [305], -q [305]</td>
<td>Only display warning and error messages</td>
</tr>
<tr>
<td>--verbose [305], -v [305]</td>
<td>Display debug, info, notice, warning and error messages</td>
</tr>
</tbody>
</table>

- --force [305]

Forces the deployment process to complete even if there are warning or error messages that would normally cause the process to fail. Forcing the installation also ignores all confirmation prompts during installation and always attempts to complete the process.

- --help [305]

Displays the help message for tpm showing the current options, commands and version information.

- --info [305]

Changes the reporting level to include information, notice, warning and error messages. Information level messages include annotations of the current process and stage in the deployment, such as configuration or generating files and configurations. This shows slightly more information than the default, but less than the full debug level offered by --verbose [305].

- --notice [305]

Sets the output level to include notice, warning, and error messages. Notice level messages include information about further steps or actions that should be taken, or things that should be noted without indicating a failure or error with the configuration options select.

- --preview [305]

- --profile file [305]

Specify the name of the configuration file to be used. This can be useful if you are performing multiple configurations or deployments from the same staging directory. The entire configuration and deployment information is stored in the file before installation is started. By specifying a different file you can have multiple deployments and configurations without requiring separate staging directories.

- --quiet [305]

Changes the error reporting level so that only warning and error messages are displayed. This mode can be useful in automated deployments as it provides output only when a warning or error exists. All other messages, including informational ones, are suppressed.

- --verbose [305]

Displays a much more detailed output of the status and progress of the deployment. In verbose mode, tpm annotates the entire process describing both what it is doing and all debug, warning and other messages in the output.

The tpm utility handles operations across all hosts in the dataservice. This is true for simple and composite dataservices as well as complex multi-master replication services. The coordination requires SSH connections between the hosts according to the Appendix C, Prerequisites. There are two exceptions for this:

1. When the --hosts [358] argument is provided to a command; that command will only be carried out on the hosts listed. Multiple hosts may be given as a comma-separated list. The names used in the --members [362], --slaves [372], --master [361], --connectors [351] arguments should be used when calling --hosts [358].

2. When you are using an INI configuration file (see Section 9.4, "tpm INI File Configuration") all calls to tpm will only affect the current host.

The installation process starts in a staging directory. This is different from the installation directory where Continuent Tungsten will ultimately be placed but may be a sub-directory. In most cases we will install to /opt/continuent but use /opt/continuent/software as a staging directory. The release package should be unpacked in the staging directory before proceeding. See the Section C.1, “Staging Host Configuration” for instructions on selecting a staging directory.

Table 9.3. tpm Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Configure a data service within the global configuration</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>connector</td>
<td>Open a connection to the configured connector using mysql</td>
</tr>
<tr>
<td>diag</td>
<td>Obtain diagnostic information</td>
</tr>
<tr>
<td>fetch</td>
<td>Fetch configuration information from a running service</td>
</tr>
<tr>
<td>firewall</td>
<td>Display firewall information for the configured services</td>
</tr>
<tr>
<td>help</td>
<td>Show command help information</td>
</tr>
<tr>
<td>install</td>
<td>Install a data service based on the existing and runtime parameters</td>
</tr>
<tr>
<td>mysql</td>
<td>Open a connection to the configured MySQL server</td>
</tr>
<tr>
<td>promote</td>
<td>Make a previously configured and prepared directory and make it the active</td>
</tr>
<tr>
<td>promote-connector</td>
<td>Restart the connectors in the active configuration</td>
</tr>
<tr>
<td>query</td>
<td>Query the active configuration for information</td>
</tr>
<tr>
<td>reset</td>
<td>Reset the cluster on each host</td>
</tr>
<tr>
<td>reset-thl</td>
<td>Reset the THL for a host</td>
</tr>
<tr>
<td>restart</td>
<td>Restart the services on specified or added hosts</td>
</tr>
<tr>
<td>start</td>
<td>Start services on specified or added hosts</td>
</tr>
<tr>
<td>stop</td>
<td>Stop services on specified or added hosts</td>
</tr>
<tr>
<td>upgrade, update</td>
<td>Update an existing configuration or software version</td>
</tr>
<tr>
<td>validate</td>
<td>Validate the current configuration</td>
</tr>
<tr>
<td>validate-update</td>
<td>Validate the current configuration and update</td>
</tr>
</tbody>
</table>

9.5.1. tpm configure Command

The configure command to tpm creates a configuration file within the current profiles directory.

9.5.2. tpm connector Command

This will open a MySQL CLI connection to the local Tungsten Connector using the current values for `--application-user` and `--application-password`.

```
shell> tpm connector
```

**Warning**

This command will fail if the mysql utility is not available or if the local server does not have a running Tungsten Connector.

**Important**

The MySQL 5.7 command-line client will now attempt to connect via SSL by default, which will fail on the Connector unless it is configured for SSL operations. You may add the `--skip-ssl` option to bypass this issue. See Section 2.7.4, “Configuring Connector SSL” for more information about using SSL with the Connector.

9.5.2.1. tpm connector `--hosts` Command

Limits the connection to the list of specified hosts. For example:

```
shell> tpm connector --hosts host1,host2
```

Would limit the connection to the connector on one of the specified hosts. The hostname must be specified in the same form as it is in the configuration.

9.5.2.2. tpm connector `--dataservice-name` Command

Limit the command to the hosts in the specified dataservice. Multiple dataservices can be specified by providing each dataservice separated by a comma.

```
shell> tpm connector --dataservice-name east
```
9.5.2.3. tpm connector --samples Command

Provides sample configuration information for various common development environments:

```
shell> tpm connector --samples

Bash                          mysql -hdemo-c11 -P3306 -uapp_user -ppassword
Perl::dbi                     $dbh=DBI->connecti('DBI:mysql:host=demo-c11;port=3306', 'app_user', 'password')
PHP::mysqli                   $dbh = new mysqli('demo-c11', 'app_user', 'password', 'schema', '3306');
PHP::pdo                      $dbh = new PDO('mysql:host=demo-c11;port=3306', 'app_user', 'password');
Python::mysql.connector       dbh = mysql.connector.connect(user='app_user', password='password', host='demo-c11', port=3306, database='schema')
Java::DriverManager           dbh=DriverManager.getConnection("jdbc:mysql://demo-c11:3306/schema", "app_user", "password")
```

9.5.3. tpm diag Command

The `tpm diag` command will create a ZIP file including log files and current dataservice status. It will connect to all servers listed in the `tpm reverse` output attempting to collect information.

```
shell> tpm diag

NOTE >> host1 >> Diagnostic information written to /home/tungsten/tungsten-diag-2013-10-09-21-04-23.zip
```

The structure of the created file will depend on the configured hosts, but will include all the logs for each accessible host configured. For example:

```
Archive:  tungsten-diag-2014-07-08-11-24-01.zip
Length  Date    Time    Name
---------  ---------- -----   ----
0  2014-07-08 11:24   tungsten-diag-2014-07-08-11-24-01/
0  2014-07-08 11:24   tungsten-diag-2014-07-08-11-24-01/ct_ssl1/
---------                     -------
534886                     31 files
```

9.5.4. tpm fetch Command

There are some cases where you would like to review the configuration or make changes prior to the upgrade. In these cases it is possible to fetch the configuration and process the upgrade as different steps.

```
shell> /tools/tpm fetch \
   --directory=/opt/continuent \
   --hosts=host1,autodetect
```
This will load the configuration into the local staging directory. You can then make changes using `tpm configure` before pushing out the upgrade.

The `tpm fetch` command supports the following arguments:

- `--hosts` [358]
  A comma-separated list of the known hosts in the cluster. If `autodetect` is included, then `tpm` will attempt to determine other hosts in the cluster by checking the configuration files for host values.

- `--user` [377]
  The username to be used when logging in to other hosts.

- `--directory`
  The installation directory of the current Continuent Tungsten installation. If `autodetect` is specified, then `tpm` will look for the installation directory by checking any running Continuent Tungsten processes.

### 9.5.5. `tpm firewall` Command

The `tpm firewall` command displays port information required to configure a firewall. When used, the information shown is for the current host:

```shell
tpm firewall
```

<table>
<thead>
<tr>
<th>From application servers</th>
<th>To host 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>9999</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>From connector servers</td>
<td>11999, 12000, 13306</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>From database servers</td>
<td>2112, 7800, 8896, 9997, 10999, 11999, 12000, 13306</td>
</tr>
</tbody>
</table>

The information shows which ports, on which hosts, should be opened to enable communication.

### 9.5.6. `tpm help` Command

The `tpm help` command outputs the help information for `tpm` showing the list of supported commands and options.

```shell
tpm help
```

Usage: tpm help [commands, config-file, template-file] [general-options] [command-options]

General options:
- `-f`, `--force` Do not display confirmation prompts or stop the configure process for errors
- `-h`, `--help` Displays help message
- `--profile file` Sets name of config file (default: tungsten.cfg)
- `-p`, `--preview` Displays the help message and preview the effect of the command line options
- `-q`, `--quiet` Only display warning and error messages
- `-n`, `--notice` Display notice, warning and error messages
- `-i`, `--info` Display info, notice, warning and error messages
- `-v`, `--verbose` Display debug, info, notice, warning and error messages

To get a list of available configuration options, use the `config-file` subcommand:

```shell
tpm help config-file
```

# Config File Options

<table>
<thead>
<tr>
<th>config_target_basename</th>
<th>[continuent-tungsten-2.0.3-11_pid10926]</th>
</tr>
</thead>
<tbody>
<tr>
<td>deployment_command</td>
<td>Current command being run</td>
</tr>
<tr>
<td>remote_package_path</td>
<td>Path on the server to use for running tpm commands</td>
</tr>
<tr>
<td>deploy_current_package</td>
<td>Deploy the current Tungsten package</td>
</tr>
<tr>
<td>deploy_package_url</td>
<td>URL for the Tungsten package to deploy</td>
</tr>
<tr>
<td>deploy_host</td>
<td>Host alias for the host to be deployed here</td>
</tr>
<tr>
<td>staging_host</td>
<td>Host being used to install</td>
</tr>
</tbody>
</table>

### 9.5.7. `tpm install` Command

The `tpm install` command performs an installation based on the current configuration (if one has been previously created), or using the configuration information provided on the command-line.

For example:
The `tpm` Deployment Command

Installs a service using the command-line configuration.

```
shell> ./tools/tpm install alpha
   --topology=master-slave
   --master=host1
   --replication-user=tungsten
   --replication-password=password
   --home-directory=/opt/continuent
   --members=host1,host2,host3
   --start
```

Installs a service using the command-line configuration.

```
shell> ./tools/tpm configure alpha
   --topology=master-slave
   --master=host1
   --replication-user=tungsten
   --replication-password=password
   --home-directory=/opt/continuent
   --members=host1,host2,host3
shell> ./tools/tpm install alpha
```

Installs a service using the command-line configuration.

```
shell> ./tools/tpm configure alpha
   --topology=master-slave
   --master=host1
   --replication-user=tungsten
   --replication-password=password
   --home-directory=/opt/continuent
   --members=host1,host2,host3
shell> ./tools/tpm install alpha
```

Installs a service using the command-line configuration.

```
shell> ./tools/tpm configure alpha
   --topology=master-slave
   --master=host1
   --replication-user=tungsten
   --replication-password=password
   --home-directory=/opt/continuent
   --members=host1,host2,host3
shell> ./tools/tpm install alpha
```

Installs a service using the command-line configuration.

```
shell> ./tools/tpm configure alpha
   --topology=master-slave
   --master=host1
   --replication-user=tungsten
   --replication-password=password
   --home-directory=/opt/continuent
   --members=host1,host2,host3
shell> ./tools/tpm install alpha
```

During installation, `tpm` checks for any host configuration problems and issues, copies the Continuent Tungsten software to each machine, creates the necessary configuration files, and if requests, starts and reports the status of the service.

If any of these steps fail, changes are backed out and installation is stopped.

9.5.8. `tpm` mysql Command

This will open a MySQL CLI connection to the local MySQL server using the current values for `--replication-user` [370], `--replication-password` [370] and `--replication-port` [370].

```
shell> ./tools/tpm mysql
```

This command will fail if the `mysql` utility is not available or if the local server does not have a running database server.

9.5.9. `tpm` promote-connector Command

The `tpm` promote-connector command should be used after performing a `tpm` update or `tpm` promote with the `--no-connectors` option.

When using this option with these commands, running connectors are not stopped and restarted with the latest configuration or application updates, which would otherwise interrupt active applications using the connector.

The `tpm` promote-connector stops and restarts the configured Connector services on all configured hosts using the currently active configuration:

```
shell> ./tools/tpm promote-connector
```

NOTE >> Command successfully completed

9.5.10. `tpm` query Command

The `query` command provides information about the current `tpm` installation. There are a number of subcommands to query specific information:

- `tpm query config` — return the full configuration values
- `tpm query dataservices` — return the list of dataservices
- `tpm query default` — return the list of configured default values
- `tpm query deployments` — return the configuration of all deployed hosts
- `tpm query manifest` — get the manifest information
- `tpm query modified-files` — return the list of files modified since installation by `tpm`
- `tpm query staging` — return the staging directory from where Continuent Tungsten was installed
- `tpm query topology` — return the current topology
- `tpm query usermap` — return the list of users organized by type from the `user.map`
The tpm Deployment Command

- **tpm query values** — return the list of configured values
- **tpm query version** — get the version of the current installation

### 9.5.10.1. tpm query config

Returns a list of all of the configuration values, both user-specified and implied within the current configuration. The information is returned in the form a JSON value:

```sh
shell> tpm query config
{
   "__system_defaults_will_be_overwritten__": {
      ...
      "staging_directory": "/home/tungsten/continuent-tungsten-2.0.5-11",
      "staging_host": "tr-ms1",
      "staging_user": "tungsten"
   }
}
```

### 9.5.10.2. tpm query dataservices

Returns the list of configured dataservices that have, or will be, installed:

```sh
shell> tpm query dataservices
alpha : PHYSICAL
```

### 9.5.10.3. tpm query deployments

Returns a list of all the individual deployment hosts and configuration information, returned in the form of a JSON object for each installation host:

```sh
shell> tpm query deployments
{
   "config_target_basename": "continuent-tungsten-2.0.5-11.pid22729",
   "dataservice_host_options": {
      'alpha': {
         'start': "true"
      }
      ...
      "staging_directory": "/home/tungsten/continuent-tungsten-2.0.5-11",
      "staging_host": "tr-ms1",
      "staging_user": "tungsten"
   }
}
```

### 9.5.10.4. tpm query manifest

Returns the manifest information for the identified release of Continuent Tungsten, including the build, source and component versions, returned in the form of a JSON value:

```sh
shell> tpm query manifest
{
   "SVN": {
      "bristlecone": {
         "URL": "https://bristlecone.googlecode.com/svn/trunk/bristlecone",
         "revision": 178
      },
      "connector": {
         "URL": "svn+ssh://svn.continuent.com/svnroot/tungsten/trunk/connector",
         "revision": 9150
      },
      "fsn": {
         "URL": "svn+ssh://svn.continuent.com/svnroot/tungsten/trunk/fsn",
         "revision": 9150
      },
      "manager": {
         "URL": "svn+ssh://svn.continuent.com/svnroot/tungsten/trunk/manager",
         "revision": 9150
      },
      "replicator": {
         "URL": "https://tungsten-replicator.googlecode.com/svn/trunk",
         "revision": 2020
      }
   },
   "date": "Fri Jan 24 22:25:07 UTC 2014",
   "host": "ip-10-250-35-16",
   "hudson": {
      "SVNRevision": null,
      "URL": "http://cc.aws.continuent.com/"
   }
}
```
9.5.10.5. tpm query modified-files

Shows the list of configuration files that have been modified since the installation was completed. Modified configuration files cannot be overwritten during an upgrade process, using this command enables you identify which files contain changes so that these modifications can be manually migrated to the new installation. To restore or replace files with their original installation, copy the .filename.orig file.

9.5.10.6. tpm query staging

Returns the host and directory from which the current installation was created:

```
shell> tpm query staging
    tungsten@host1:/home/tungsten/continuent-tungsten-2.0.5-11
```

This can be useful when the installation host and directory from which the original configuration was made need to be updated or modified.

9.5.10.7. tpm query topology

Returns the current topology and list of configured servers and roles in the form of a JSON object:

```
shell> tpm query topology
    {
      "host1": "slave",
      "host2": "slave",
      "host3": "master"
    }
```

9.5.10.8. tpm query usermap

Returns a summarized list of the currently configured users in the user.map:

```
shell> tpm query usermap
    # user.map Summary
    # Configured users
    app_user ******** alpha
    # Script entries
    # DirectRead users
    # Host-based routing entries
```

9.5.10.9. tpm query version

Returns the version for the identified version of Continuent Tungsten:

```
shell> tpm query version
    2.0.5-11
```

9.5.11. tpm reset Command

This command will clear the current state for all Tungsten services:

- Management metadata
- Replication metadata
- THL files
The tpm Deployment Command

• Relay log files
• Replication position

If you run the command from an installed directory, it will only apply to the current server. If you run it from a staging directory, it will apply to all servers unless you specify the --hosts option.

```
shell> ./tools/tpm reset
```

9.5.12. tpm reset-thl Command

This command will clear the current replication state for the Tungsten Replicator:

• THL files
• Relay log files
• Replication position

If you run the command from an installed directory, it will only apply to the current server. If you run it from a staging directory, it will apply to all servers unless you specify the --hosts option.

```
shell> ./tools/tpm reset-thl
```

9.5.13. tpm restart Command

The tpm restart command contacts the currently configured services on the current host and restarts each service. On a running system this will result in an interruption to service as the services are restarted.

The restart command can be useful in situations where services may not have started properly, or after a reboot services failed. For more information on explicitly starting components, see Section 4.2, “Starting and Stopping Continuent Tungsten”. For information on how to configure services to start during a reboot, see Section 4.3, “Configuring Startup on Boot”.

9.5.14. tpm reverse Command

The tpm reverse command will show you the commands required to rebuild the configuration for the current directory. This is useful for doing an upgrade or when copying the deployment to another server.

```
shell> ./tools/tpm reverse
# Defaults for all data services and hosts
tools/tpm configure defaults \
--application-password=secret \
--application-port=3306 \
--application-user=app \
--replication-password=secret \
--replication-port=13306 \
--replication-user=tungsten \
--start-and-report=true \
--user=tungsten
# Options for the alpha data service
tools/tpm configure alpha \
--connectors=host1,host2,host3 \
--master=host1 \
--members=host1,host2,host3
```

The tpm reverse command supports the following arguments:

• --public
  Hide passwords in the command output

• --ini-format
  Display output in ini format for use in /etc/tungsten/tungsten.ini and similar configuration files

9.5.15. tpm ssh-copy-cert Command

The tpm ssh-copy-cert command executes all the required commands to generate the required ssh certificates required for SSH operation by tpm. Executing the command should generate the required directory, certificate and add that information to the required SSH files, then ensure that the directory permissions and ownership on ~/.ssh are set correctly.
The tpm Deployment Command

For example, executing the command outputs the stages and progress:

```bash
shell> ./tools/tpm ssh-copy-cert
mkdir -p ~/.ssh
echo "-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAnMSRTwBB2Ik6FOTZYxQkXglFivniLSRxlW7U0UVEOGpTs2N
psQzH+tItyFhIPHRJwh3J6Jeo4NP2jFurhpgdY6szxeL51s5WUKSZN2mRwV
lE6Qo2J2yRmBuv9MVGofKPhgD0oGe7V3jg3L4Buwx5hFHkLtTgfj1AQFeh7QU
ewZk1C174W5EkUXNtq7F67damXsFILQ0swR25EoZczyJfjrjyoeysj3corupQF
at0h9m36e8Dr3t379Ycomwvlasyp2rFkbowHdC6H60Vd9KapQd/TY3I3E7s
wFeOnVJy4Qo1g87a/s7f0Us5j5Ss52zomG27zYUNmQ1DAGb6b1A6h+idrQImhnd+6R
8q70GM3btaqj30UAgA048gAvPzR9liVwvuShz2Rc2V3Q3xQoLiD0Q32pQdA2AQt0
XaLc4Qo756kL1R1jOfj1zJ3CPq7QFbA7i4gZmVNG10m6?+Yz8hR7j3
414tqU7QnOk7w/eKwUpFgU60Vh8aRe6u3L2b/bPY7t0Q1005EHqg8MRcXz
1g9g5jPv9Hb2tB89j5/GcT13KX7D6BByp9z7/414tqU7QnOk7w/eKwUpFgU60Vh8aRe6u3L2b/bPY7t0Q1005EHqg8MRcXz
vQ4haU7QnOk7w/eKwUpFgU60Vh8aRe6u3L2b/bPY7t0Q1005EHqg8MRcXz
-----END RSA PRIVATE KEY-----" > ~/.ssh/id_rsa
echo "ssh-rsa ... tungsten@cont-db1" > ~/.ssh/id_rsa.pub
touch ~/.ssh/authorized_keys
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 700 ~/.ssh
chmod 600 ~/.ssh/*

9.5.16. tpm start Command

The tpm start command starts configured services on the current host. This can be useful in situations where you have installed services but not configured them to be started.

```bash
shell> tpm start
...........
Getting cluster status on host1
Continuent Tungsten 2.0.5 build 11
alpha: session established

[LOGICAL] /alpha >

ROUTERS:
+----------------------------------------------------------------------------+
|connector@host1[13248](ONLINE, created=0, active=0)                         |
|connector@host2[15400](ONLINE, created=0, active=0)                         |
|connector@host3[28217](ONLINE, created=0, active=0)                         |
+----------------------------------------------------------------------------+

DATASOURCES:
+----------------------------------------------------------------------------+
|host1(master:ONLINE, progress=15, THL latency=0.105)                        |
|STATUS [OK] [2013/10/24 03:55:35 PM BST]                                    |
|  MANAGER(state=ONLINE)                                                     |
|  REPLICATOR(role=master, state=ONLINE)                                     |
|  DATASERVER(state=UNKNOWN)                                                 |
|  CONNECTIONS(created=0, active=0)                                          |
+----------------------------------------------------------------------------+

host2(slave:ONLINE, progress=15, THL latency=0.105)                        |
STATUS [OK] [2013/10/24 03:55:35 PM BST]                                    |
MANAGER(state=ONLINE)                                                     |
REPLICATOR(role=slave, host1, state=ONLINE)                                |
DATASERVER(state=UNKNOWN)                                                 |
CONNECTIONS(created=0, active=0)                                           |

host3(slave:progress=15, latency=0.800)                                    |
STATUS [OK] [2013/10/24 03:55:35 PM BST]                                    |
MANAGER(state=ONLINE)                                                     |
REPLICATOR(role=slave, host1, state=ONLINE)                                |
DATASERVER(state=UNKNOWN)                                                 |
CONNECTIONS(created=0, active=0)                                           |
+----------------------------------------------------------------------------+
```
The `tpm` Deployment Command

---

```plaintext
[LOGICAL] /alpha >
Exiting...
NOTE  >> host1 >> Command successfully completed
```

The `tpm start` can also be provided with the name of a service, which will start all the processes for that service on the current host.

See also the `tpm restart` command, Section 4.2, “Starting and Stopping Continuent Tungsten”, and Section 4.3, “Configuring Startup on Boot”.

9.5.17. tpm stop Command

The `tpm stop` command contacts all configured services on the current host and stops them if they are running.

```plaintext
shell> tpm stop
NOTE  >> host1 >> Command successfully completed
```

See also the `tpm restart` command, Section 4.2, “Starting and Stopping Continuent Tungsten”, and Section 4.3, “Configuring Startup on Boot”.

9.5.18. tpm update Command

The `tpm update` command is used when applying configuration changes or upgrading to a new version. The process is designed to be simple and maintain availability of all services. The actual process will be performed as described in Section 9.2, “Processing Installs and Upgrades”. The behavior of `tpm update` is dependent on two factors.

1. Are you upgrading to a new version or applying configuration changes to the current version?
2. The installation method used during deployment.

**Note**

Check the output of `tpm query staging` to determine which method your current installation uses. The output for an installation from a staging directory will start with a `Installed from tungsten@staging-host:/opt/continuent/software/continuent-tungsten-2.0.5-11`. An installation based on an INI file may include this line but there will be an `/etc/tungsten/tungsten.ini` file on each node.

Upgrading to a new version

If a staging directory was used; see Section 9.3.6, “Upgrades from a Staging Directory”.

If an INI file was used; see Section 9.4.3, “Upgrades with an INI File”

Applying configuration changes to the current version

If a staging directory was used; see Section 9.3.7, “Configuration Changes from a Staging Directory”.

If an INI file was used; see Section 9.4.4, “Configuration Changes with an INI file”.

Special Considerations for the Connector

As of software version 4.0.0, the `tpm` command will use `connector graceful-stop 30` followed by `connector start` when upgrading versions. If that command fails then a regular `connector stop` is run.

This behavior is also applied when using `tools/tpm update --replace-release`.

The `tpm` command will use `connector reconfigure` when changing connector settings without a version upgrade.

The use of `connector reconfigure` is disabled for the following:

- `--application-port`
- `--application-readonly-port`
- `--router-gateway-port`
- `--router-jmx-port`
- `--conn-java-mem-size`

If `connector reconfigure` can't be used, `connector graceful-stop 30` and `connector start` are used.
9.5.19. tpm validate Command

The `tpm validate` command validates the current configuration before installation. The validation checks all prerequisites that apply before an installation, and assumes that the configured hosts are currently not configured for any Tungsten services, and no Tungsten services are currently running.

```
shell> /tools/tpm validate
........
# Validation failed

```

The command can be run after performing a `tpm configure` and before a `tpm install` to ensure that any prerequisite or configuration issues are addressed before installation occurs.

9.5.20. tpm validate-update Command

The `tpm validate-update` command checks whether the configured hosts are ready to be updated. By checking the prerequisites and configuration of the dataserver and hosts, the same checks as made by `tpm` during a `tpm install` operation. Since there may have been changes to the requirements or required configuration, this check can be useful before attempting an update.

Using `tpm validate-update` is different from `tpm validate` in that it checks the environment based on the updated configuration, including the status of any existing services.

```
shell> /tools/tpm validate-update
....
WARN >> host1 >> The process limit is set to 7812, we suggest a value of at least 8096. Add 'tungsten - nproc 8096' to your /etc/security/limits.conf and restart Tungsten processes. (ProcessLimitCheck)

WARN >> host2 >> The process limit is set to 7812, we suggest a value of at least 8096. Add 'tungsten - nproc 8096' to your /etc/security/limits.conf and restart Tungsten processes. (ProcessLimitCheck)

WARN >> host3 >> The process limit is set to 7812, we suggest a value of at least 8096. Add 'tungsten - nproc 8096' to your /etc/security/limits.conf and restart Tungsten processes. (ProcessLimitCheck)

WARN >> host3 >> MyISAM tables exist within this instance - These tables are not crash safe and may lead to data loss in a failover (MySQLMyISAMCheck)

NOTE >> Command successfully completed
```

Any problems noted should be addressed before you perform the update using `tpm update`.

9.6. tpm Common Options

`tpm` accepts these options along with those in Section 9.8, “tpm Configuration Options”.

- On the command-line, using a double-dash prefix, i.e. `--skip-validation-check=MySQLConnectorPermissionsCheck`
- In an INI file, without the double-dash prefix, i.e. `skip-validation-check=MySQLConnectorPermissionsCheck`

<table>
<thead>
<tr>
<th>CmdLine Option</th>
<th>INI File Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--enable-validation-check</code></td>
<td><code>enable-validation-check</code></td>
<td>Enable a specific validation check, overriding any configured skipped checks</td>
</tr>
<tr>
<td><code>--enable-validation-warnings</code></td>
<td><code>enable-validation-warnings</code></td>
<td>Enable a specific validation warning, overriding any configured skipped warning</td>
</tr>
<tr>
<td><code>--net-ssh-option</code></td>
<td><code>net-ssh-option</code></td>
<td>Set the Net::SSH option for remote system calls</td>
</tr>
<tr>
<td><code>--property</code></td>
<td><code>property</code></td>
<td>Modify specific property values for the key in any file that the configuration script touches.</td>
</tr>
<tr>
<td><code>--remove-property</code></td>
<td><code>remove-property</code></td>
<td>Remove the setting for a previously configured property</td>
</tr>
</tbody>
</table>
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>CmdLine Option</th>
<th>INI File Option</th>
<th>Description</th>
</tr>
</thead>
</table>

#### Option

The `--enable-validation-check [316]` will specifically enable a given validation check if the check had previously been set to be ignored in a previous invocation of the configuration through `tpm`. If a check fails, installation is canceled.

Setting both `--skip-validation-check [317]` and `--enable-validation-check [316]` is equivalent to explicitly disabling the specified check.

#### Option

The `--enable-validation-warnings [316]` will specifically enable a given validation warning check if the check had previously been set to be ignored in a previous invocation of the configuration through `tpm`.

Setting both `--skip-validation-warnings [317]` and `--enable-validation-warnings [316]` is equivalent to explicitly disabling the specified check.

#### Option

Enables you to set a specific Net::SSH option. For example:

```sh
tpm update ... --net-ssh-option=compression=zlib
```

#### Option

The `--property [316]` option enables you to explicitly set property values in the target files. A number of different models are supported:

- **key=value**
  
  Set the property defined by `key` to the specified value without evaluating any template values or other rules.

- **key+=value**
  
  Add the value to the property defined by `key`. Template values and other options append their settings to the end of the specified property.

- **key~=/match/replace/ [316]**
  
  Evaluate any template values and other settings, and then perform the specified Ruby regex operation to the property defined by `key`. For example `--property=replicator.key~/=\((.*+)/somevalue,\1/` will prepend `somevalue` before the template value for `replicator.key`. 

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--net-ssh-option [316]</td>
<td>Set the Net::SSH option for remote system calls.</td>
</tr>
<tr>
<td>--property [316]</td>
<td>Modify specific property values for the key in any file that the configure script touches.</td>
</tr>
<tr>
<td>--property=key+=value [316]</td>
<td>Add the value to the property defined by <code>key</code>. Template values and other options append their settings to the end of the specified property.</td>
</tr>
<tr>
<td>--property=key=value [316]</td>
<td>Set the property defined by <code>key</code> to the specified value without evaluating any template values or other rules.</td>
</tr>
<tr>
<td>--property=key~=/match/replace/ [316]</td>
<td>Evaluate any template values and other settings, and then perform the specified Ruby regex operation to the property defined by <code>key</code>. For example <code>--property=replicator.key~/=\((.*+)/somevalue,\1/</code> will prepend <code>somevalue</code> before the template value for <code>replicator.key</code>.</td>
</tr>
</tbody>
</table>
## 9.7. tpm Validation Checks

During configuration and installation, `tpm` runs a number of configuration, operating system, datasource, and other validation checks to ensure that the correct environment, prerequisites and other settings will produce a valid, working, configuration.

All relevant checks are executed automatically unless specifically ignored (warnings) or disabled (checks) using the corresponding `--skip-validation-warnings` or `--skip-validation-check` options.
### Table 9.5. **tpm** Validation Checks

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupDirectoryWriteableCheck [321]</td>
<td>Checks that the configured backup directory is writeable</td>
</tr>
<tr>
<td>BackupDumpDirectoryWriteableCheck [321]</td>
<td>Checks the backup temp directory is writeable</td>
</tr>
<tr>
<td>BackupScriptAvailableCheck [321]</td>
<td>Checks that the configured backup script exists and can be executed</td>
</tr>
<tr>
<td>ClusterDiagnosticCheck [321]</td>
<td></td>
</tr>
<tr>
<td>ClusterStatusCheck [321]</td>
<td></td>
</tr>
<tr>
<td>CommitDirectoryCheck [321]</td>
<td></td>
</tr>
<tr>
<td>ConfigurationStorageDirectoryCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConfigureValidationCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConfiguredDirectoryCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConflictingReplicationServiceTHLPortsCheck [322]</td>
<td>Ensures that the configured connector selection is valid</td>
</tr>
<tr>
<td>ConnectorChecks [322]</td>
<td></td>
</tr>
<tr>
<td>Connector@VersionCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConnectorListenerAddressCheck [322]</td>
<td>Ensure the RW and RO addresses are different</td>
</tr>
<tr>
<td>ConnectorRWROAddressesCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConnectorSmartScaleAllowedCheck [322]</td>
<td>Confirms whether SmartScale is valid within the current configured parameters</td>
</tr>
<tr>
<td>ConnectorUserCheck [322]</td>
<td></td>
</tr>
<tr>
<td>ConsistentReplicationCredentialsCheck [323]</td>
<td></td>
</tr>
<tr>
<td>CurrentCommandCoordinatorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>CurrentConnectorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>CurrentReleaseDirectoryIsSymlink [323]</td>
<td></td>
</tr>
<tr>
<td>CurrentTopologyCheck [323]</td>
<td></td>
</tr>
<tr>
<td>CurrentVersionCheck [323]</td>
<td></td>
</tr>
<tr>
<td>DatasourceBootScriptCheck [323]</td>
<td></td>
</tr>
<tr>
<td>DifferentMasterSlaveCheck [323]</td>
<td></td>
</tr>
<tr>
<td>DirectOracleServiceSIDCheck [323]</td>
<td></td>
</tr>
<tr>
<td>ElasticsearchValidationCheck [323]</td>
<td></td>
</tr>
<tr>
<td>EncryptionCheck [323]</td>
<td></td>
</tr>
<tr>
<td>EncryptionKeystoreCheck [324]</td>
<td></td>
</tr>
<tr>
<td>FileValidationCheck [324]</td>
<td></td>
</tr>
<tr>
<td>FirewallCheck [324]</td>
<td></td>
</tr>
<tr>
<td>GlobalHostAddressesCheck [324]</td>
<td></td>
</tr>
<tr>
<td>GlobalHostOracleLibrariesFoundCheck [324]</td>
<td></td>
</tr>
<tr>
<td>GlobalMatchingPingMethodCheck [324]</td>
<td></td>
</tr>
<tr>
<td>GlobalRestartComponentsCheck [324]</td>
<td></td>
</tr>
<tr>
<td>GroupValidationCheck [324]</td>
<td></td>
</tr>
<tr>
<td>HdfsValidationCheck [324]</td>
<td></td>
</tr>
<tr>
<td>HostLicensesCheck [324]</td>
<td></td>
</tr>
<tr>
<td>HostOracleLibrariesFoundCheck [324]</td>
<td></td>
</tr>
<tr>
<td>HostReplicatorServiceRunningCheck [325]</td>
<td></td>
</tr>
<tr>
<td>HostSkippedChecks [325]</td>
<td></td>
</tr>
<tr>
<td>HostnameCheck [325]</td>
<td></td>
</tr>
<tr>
<td>HostsFileCheck [325]</td>
<td></td>
</tr>
<tr>
<td>InstallServicesCheck [325]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InstallationScriptCheck [325]</td>
<td>Checks whether a master host has been defined for the configured service.</td>
</tr>
<tr>
<td>InstallerMasterSlaveCheck [325]</td>
<td></td>
</tr>
<tr>
<td>InstallingOverExistingInstallation [325]</td>
<td></td>
</tr>
<tr>
<td>JavaUserTimezoneCheck [325]</td>
<td></td>
</tr>
<tr>
<td>JavaVersionCheck [325]</td>
<td></td>
</tr>
<tr>
<td>KeystoresCheck [325]</td>
<td></td>
</tr>
<tr>
<td>KeystoresToCommitCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerActiveWitnessConversionCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerChecks [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerHeapThresholdCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerListenerAddressCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerPingMethodCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerWitnessAvailableCheck [326]</td>
<td></td>
</tr>
<tr>
<td>ManagerWitnessNeededCheck [326]</td>
<td></td>
</tr>
<tr>
<td>MatchingHomeDirectoryCheck [326]</td>
<td></td>
</tr>
<tr>
<td>MissingReplicationServiceConfigurationCheck [326]</td>
<td>Checks if MySQL is installed</td>
</tr>
<tr>
<td>ModifiedConfigurationFilesCheck [326]</td>
<td></td>
</tr>
<tr>
<td>MySQLAllowIntensiveChecks [327]</td>
<td>Enables searching MySQL INFORMATION_SCHEMA for validation checks</td>
</tr>
<tr>
<td>MySQLApplierLogsCheck [327]</td>
<td></td>
</tr>
<tr>
<td>MySQLApplierPortCheck [327]</td>
<td></td>
</tr>
<tr>
<td>MySQLApplierServerIDCheck [327]</td>
<td></td>
</tr>
<tr>
<td>MySQLAvailableCheck [327]</td>
<td>Checks that binary logging has been enabled on MySQL</td>
</tr>
<tr>
<td>MySQLBinlogDoDbCheck [327]</td>
<td></td>
</tr>
<tr>
<td>MySQLClientCheck [327]</td>
<td>Checks whether the MySQL client command tool is available</td>
</tr>
<tr>
<td>MySQLConfigFileCheck [327]</td>
<td>Checks the existence of a MySQL configuration file</td>
</tr>
<tr>
<td>MySQLConnectorBridgeModePermissionsCheck [327]</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using</td>
</tr>
<tr>
<td>MySQLConnectorPermissionsCheck [328]</td>
<td></td>
</tr>
<tr>
<td>MySQLDefaulTableTypeCheck [328]</td>
<td>Checks the default table type for MySQL</td>
</tr>
<tr>
<td>MySQLDumpCheck [328]</td>
<td>Checks that the mysqldump command version matches the installed MySQL</td>
</tr>
<tr>
<td>MySQLGeneratedColumnCheck [328]</td>
<td>Checks whether MySQL virtual/generated columns are defined</td>
</tr>
<tr>
<td>MySQLInnoDBEnabledCheck [328]</td>
<td></td>
</tr>
<tr>
<td>MySQLJsonDataTypeCheck [328]</td>
<td></td>
</tr>
<tr>
<td>MySQLLoadDataInfilePermissionsCheck [328]</td>
<td></td>
</tr>
<tr>
<td>MySQLLoginCheck [328]</td>
<td>Checks whether super_read_only has been enabled on MySQL</td>
</tr>
<tr>
<td>MySQLMyISAMCheck [328]</td>
<td>Checks for the existence of MyISAM tables</td>
</tr>
<tr>
<td>MySQLPasswordSettingCheck [329]</td>
<td></td>
</tr>
<tr>
<td>MySQLPermissionsCheck [329]</td>
<td></td>
</tr>
<tr>
<td>MySQLReadableLogsCheck [329]</td>
<td></td>
</tr>
<tr>
<td>MySQLSettingsCheck [329]</td>
<td></td>
</tr>
<tr>
<td>MySQLSuperReadOnlyCheck [329]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MySQLTriggerCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLUnsupportedDataTypesCheck</td>
<td></td>
</tr>
<tr>
<td>MysqlConnectorCheck</td>
<td></td>
</tr>
<tr>
<td>MysqldumpAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>MysqldumpSettingsCheck</td>
<td></td>
</tr>
<tr>
<td>NewDirectoryRequiredCheck</td>
<td></td>
</tr>
<tr>
<td>NtpdRunningCheck</td>
<td></td>
</tr>
<tr>
<td>OSCheck</td>
<td></td>
</tr>
<tr>
<td>OldServicesRunningCheck</td>
<td></td>
</tr>
<tr>
<td>OpenfilesInitCheck</td>
<td></td>
</tr>
<tr>
<td>OpensslLibraryCheck</td>
<td></td>
</tr>
<tr>
<td>OracleloginCheck</td>
<td></td>
</tr>
<tr>
<td>OraclePermissionsCheck</td>
<td></td>
</tr>
<tr>
<td>OracleRedoHeaderMinerDirectoryCheck</td>
<td></td>
</tr>
<tr>
<td>OracleServiceSIDCheck</td>
<td></td>
</tr>
<tr>
<td>OracleVersionCheck</td>
<td></td>
</tr>
<tr>
<td>PGAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>ParallelReplicationCheck</td>
<td></td>
</tr>
<tr>
<td>ParallelReplicationCountCheck</td>
<td></td>
</tr>
<tr>
<td>PgControlAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>PgStandbyAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>PgdumpAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>PgdumpallAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>PingSyntaxCheck</td>
<td></td>
</tr>
<tr>
<td>PortAvailabilityCheck</td>
<td></td>
</tr>
<tr>
<td>ProfilescriptCheck</td>
<td></td>
</tr>
<tr>
<td>RMIListenerAddressCheck</td>
<td></td>
</tr>
<tr>
<td>RelayDirectoryWriteableCheck</td>
<td>Checks that the relay log directory can be written to</td>
</tr>
<tr>
<td>ReplicatorChecks</td>
<td></td>
</tr>
<tr>
<td>RestartComponentsCheck</td>
<td></td>
</tr>
<tr>
<td>RouterAffinityCheck</td>
<td></td>
</tr>
<tr>
<td>RouterBridgeModeDefaultCheck</td>
<td></td>
</tr>
<tr>
<td>RouterDelayBeforeOfflineCheck</td>
<td></td>
</tr>
<tr>
<td>RouterKeepAliveTimeoutCheck</td>
<td></td>
</tr>
<tr>
<td>RowBasedBinaryLoggingCheck</td>
<td>Checks that Row-based binary logging has been enabled for heterogeneous deployments</td>
</tr>
<tr>
<td>RsyncAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>RubyVersionCheck</td>
<td></td>
</tr>
<tr>
<td>SSHLoginCheck</td>
<td>Checks connectivity to other hosts over SSH</td>
</tr>
<tr>
<td>ServiceTransferredLogstorageCheck</td>
<td></td>
</tr>
<tr>
<td>StartingStoppedServices</td>
<td></td>
</tr>
<tr>
<td>SudoCheck</td>
<td></td>
</tr>
<tr>
<td>SwappinessCheck</td>
<td>Checks the swappiness OS configuration is within a recommended range</td>
</tr>
<tr>
<td>THLDirectoryWriteableCheck</td>
<td></td>
</tr>
</tbody>
</table>
## The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>THLListenerAddressCheck</td>
<td></td>
</tr>
<tr>
<td>THLSchemaChangeCheck</td>
<td>Ensures that the existing THL format is compatible with the new release</td>
</tr>
<tr>
<td>THLStorageCheck</td>
<td>Confirms the THL storage directory exists, is empty and writeable</td>
</tr>
<tr>
<td>THLStorageChecksum</td>
<td></td>
</tr>
<tr>
<td>TargetDirectoryDoesNotExist</td>
<td></td>
</tr>
<tr>
<td>TransferredLogStorageCheck</td>
<td></td>
</tr>
<tr>
<td>UpgradeSameProductCheck</td>
<td>Ensures that the same product is being updated</td>
</tr>
<tr>
<td>VIPEnabledHostAllowsRootCommands</td>
<td></td>
</tr>
<tr>
<td>VIPEnabledHostArpPath</td>
<td></td>
</tr>
<tr>
<td>VIPEnabledHostIfconfigPath</td>
<td></td>
</tr>
<tr>
<td>VerticaUserGroupsCheck</td>
<td>Checks that the Vertica user has the correct OS group membership</td>
</tr>
<tr>
<td>WhichAvailableCheck</td>
<td>Checks the existence of a working which command</td>
</tr>
<tr>
<td>WriteableHomeDirectoryCheck</td>
<td>Ensures the home directory can be written to</td>
</tr>
<tr>
<td>WriteableTempDirectoryCheck</td>
<td>Ensures the temporary directory can be written to</td>
</tr>
<tr>
<td>XtrabackupAvailableCheck</td>
<td></td>
</tr>
<tr>
<td>XtrabackupDirectoryWriteableCheck</td>
<td></td>
</tr>
<tr>
<td>XtrabackupSettingsCheck</td>
<td></td>
</tr>
</tbody>
</table>

- **BackupDirectoryWriteableCheck** [321]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupDirectoryWriteableCheck</td>
<td>Checks that the configured backup directory is writeable</td>
</tr>
</tbody>
</table>

Confirms that the directory defined in `--backup-dir` directory exists and can be written to.

- **BackupDumpDirectoryWriteableCheck** [321]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupDumpDirectoryWriteableCheck</td>
<td>Checks the backup temp directory is writeable</td>
</tr>
</tbody>
</table>

Confirms that the directory defined in `--backup-dump-dir` directory exists and can be written to.

- **BackupScriptAvailableCheck** [321]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BackupScriptAvailableCheck</td>
<td>Checks that the configured backup script exists and can be executed</td>
</tr>
</tbody>
</table>

Confirms that the script defined in `--backup-script` [347] exists and is executable.

- **ClusterDiagnosticCheck** [321]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterDiagnosticCheck</td>
<td></td>
</tr>
</tbody>
</table>

- **ClusterStatusCheck** [321]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClusterStatusCheck</td>
<td></td>
</tr>
</tbody>
</table>

- **CommitDirectoryCheck** [321]
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ConfigurationStorageDirectoryCheck [322]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ConfigurationStorageDirectoryCheck [322]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>ConfigureValidationCheck [322]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ConfigureValidationCheck [322]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>ConfiguredDirectoryCheck [322]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ConfiguredDirectoryCheck [322]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>ConflictingReplicationServiceTHLPortsCheck [322]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ConflictingReplicationServiceTHLPortsCheck [322]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>ConnectorChecks [322]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ConnectorChecks [322]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Ensures that the configured connector selection is valid</td>
</tr>
</tbody>
</table>

Checks that the list of connectors and the corresponding list of data services is valid.

| ConnectorDBVersionCheck [322] |  |
| **Option** | ConnectorDBVersionCheck [322] |
| **Description** |  |

| ConnectorListenerAddressCheck [322] |  |
| **Option** | ConnectorListenerAddressCheck [322] |
| **Description** |  |

| ConnectorRWROAddressesCheck [322] |  |
| **Option** | ConnectorRWROAddressesCheck [322] |
| **Description** | Ensure the RW and RO addresses are different |

For environments where the connector has been configured to use different hosts and ports for RW and RO operations, ensure that the settings are in fact different.

| ConnectorSmartScaleAllowedCheck [322] |  |
| **Option** | ConnectorSmartScaleAllowedCheck [322] |
| **Description** | Confirms whether SmartScale is valid within the current configured parameters |

Checks that both SmartScale and Read/Write splitting have been enabled.

<p>| ConnectorUserCheck [322] |  |
| <strong>Option</strong> | ConnectorUserCheck [322] |</p>
<table>
<thead>
<tr>
<th>Description</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>- ConsistentReplicationCredentialsCheck [323]</td>
<td>ConsistentReplicationCredentialsCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option ConsistentReplicationCredentialsCheck [323]</td>
<td>Description ConsistentReplicationCredentialsCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- CurrentCommandCoordinatorCheck [323]</td>
<td>CurrentCommandCoordinatorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option CurrentCommandCoordinatorCheck [323]</td>
<td>Description CurrentCommandCoordinatorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- CurrentConnectorCheck [323]</td>
<td>CurrentConnectorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option CurrentConnectorCheck [323]</td>
<td>Description CurrentConnectorCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- CurrentTopologyCheck [323]</td>
<td>CurrentTopologyCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option CurrentTopologyCheck [323]</td>
<td>Description CurrentTopologyCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- CurrentVersionCheck [323]</td>
<td>CurrentVersionCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option CurrentVersionCheck [323]</td>
<td>Description CurrentVersionCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- DatasourceBootScriptCheck [323]</td>
<td>DatasourceBootScriptCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option DatasourceBootScriptCheck [323]</td>
<td>Description DatasourceBootScriptCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- DifferentMasterSlaveCheck [323]</td>
<td>DifferentMasterSlaveCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option DifferentMasterSlaveCheck [323]</td>
<td>Description DifferentMasterSlaveCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- DirectOracleServiceSIDCheck [323]</td>
<td>DirectOracleServiceSIDCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option DirectOracleServiceSIDCheck [323]</td>
<td>Description DirectOracleServiceSIDCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- ElasticsearchValidationCheck [323]</td>
<td>ElasticsearchValidationCheck [323]</td>
<td></td>
</tr>
<tr>
<td>Option ElasticsearchValidationCheck [323]</td>
<td>Description ElasticsearchValidationCheck [323]</td>
<td></td>
</tr>
<tr>
<td>- EncryptionCheck [323]</td>
<td>EncryptionCheck [323]</td>
<td></td>
</tr>
</tbody>
</table>
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptionKeystoreCheck [324]</td>
</tr>
<tr>
<td>FileValidationCheck [324]</td>
</tr>
<tr>
<td>FirewallCheck [324]</td>
</tr>
<tr>
<td>GlobalHostAddressesCheck [324]</td>
</tr>
<tr>
<td>GlobalHostOracleLibrariesFoundCheck [324]</td>
</tr>
<tr>
<td>GlobalMatchingPingMethodCheck [324]</td>
</tr>
<tr>
<td>GlobalRestartComponentsCheck [324]</td>
</tr>
<tr>
<td>GroupValidationCheck [324]</td>
</tr>
<tr>
<td>HdfsValidationCheck [324]</td>
</tr>
<tr>
<td>HostLicensesCheck [324]</td>
</tr>
<tr>
<td>HostOracleLibrariesFoundCheck [324]</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><strong>HostReplicatorServiceRunningCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>HostSkippedChecks</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>HostnameCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>HostsFileCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>InstallServicesCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>InstallationScriptCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>InstallerMasterSlaveCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>InstallingOverExistingInstallation</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>JavaUserTimezoneCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>JavaVersionCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>KeystoresCheck</strong> [325]</td>
</tr>
<tr>
<td><strong>Option</strong></td>
</tr>
</tbody>
</table>
The `tpm` Deployment Command

<table>
<thead>
<tr>
<th>Description</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeystoresToCommitCheck [326]</td>
<td>KeystoresToCommitCheck [326]</td>
</tr>
<tr>
<td>ManagerActiveWitnessConversionCheck [326]</td>
<td>ManagerActiveWitnessConversionCheck [326]</td>
</tr>
<tr>
<td>ManagerChecks [326]</td>
<td>ManagerChecks [326]</td>
</tr>
<tr>
<td>ManagerHeapThresholdCheck [326]</td>
<td>ManagerHeapThresholdCheck [326]</td>
</tr>
<tr>
<td>ManagerListenerAddressCheck [326]</td>
<td>ManagerListenerAddressCheck [326]</td>
</tr>
<tr>
<td>ManagerPingMethodCheck [326]</td>
<td>ManagerPingMethodCheck [326]</td>
</tr>
<tr>
<td>ManagerWitnessAvailableCheck [326]</td>
<td>ManagerWitnessAvailableCheck [326]</td>
</tr>
<tr>
<td>ManagerWitnessNeededCheck [326]</td>
<td>ManagerWitnessNeededCheck [326]</td>
</tr>
<tr>
<td>MissingReplicationServiceConfigurationCheck [326]</td>
<td>MissingReplicationServiceConfigurationCheck [326]</td>
</tr>
<tr>
<td>ModifiedConfigurationFilesCheck [326]</td>
<td>ModifiedConfigurationFilesCheck [326]</td>
</tr>
</tbody>
</table>
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MySQLAllowIntensiveChecks</strong> [327]</td>
</tr>
</tbody>
</table>

Enables tpm to make use of the MySQL INFORMATION_SCHEMA to perform various validation checks. These include, but are not limited to:

- Tables not configured to use transactional tables
- Unsupported datatypes in MySQL tables

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLAllowIntensiveChecks [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enables searching MySQL INFORMATION_SCHEMA for validation checks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLApplierLogsCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Examines the log_bin variable has been defined within the running MySQL server. Binary logging must be enabled for replication to work.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLApplierPortCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks whether the MySQL client command tool is available</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLApplierServerIDCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks the existence of a MySQL configuration file</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLAvailableCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks if MySQL is installed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLBinaryLogsEnabledCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks that binary logging has been enabled on MySQL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>MySQLConnectorBridgeModePermissionsCheck [327]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

327
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQLConnectorBridgeModePermissionsCheck</td>
<td>Checks that the default table type configured for MySQL is a compatible transactional storage engine such as InnoDB</td>
</tr>
<tr>
<td>MySQLConnectorPermissionsCheck</td>
<td>Checks whether any tables contain generated or virtual columns. The test is only executed on MySQL 5.7 and only if --mysql-allow-intensive-checks has been enabled.</td>
</tr>
<tr>
<td>MySQLDefaultTableTypeCheck</td>
<td>Checks, whether any tables contain JSON columns. The test is only executed on MySQL 5.7 and only if --mysql-allow-intensive-checks has been enabled.</td>
</tr>
<tr>
<td>MySQLDumpCheck</td>
<td>Checks whether the mysqldump command within the configured PATH matches the version of MySQL being configured as a source or target. A mismatch could indicate that multiple MySQL versions are installed.</td>
</tr>
<tr>
<td>MySQLGeneratedColumnCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
<tr>
<td>MySQLInnoDBEnabledCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
<tr>
<td>MySQLJsonDataTypeCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
<tr>
<td>MySQLLoadDataInfilePermissionsCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
<tr>
<td>MySQLLoginCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
<tr>
<td>MySQLMyISAMCheck</td>
<td>Checks whether Continuent Tungsten can connect to MySQL using the configured credentials</td>
</tr>
</tbody>
</table>
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQLMyISAMCheck</td>
<td>Checks for the existence of MyISAM tables</td>
</tr>
</tbody>
</table>

Checks for the existence of MyISAM tables within the database. Use of MyISAM tables is not supported since MyISAM is not transactionally consistent. This can cause problems for both extraction and applying data.

In order to check for the existence of MyISAM tables, tpm uses two techniques:

- Looking for .MYD files within the MySQL directory, which are the files which contain MyISAM data. tpm must be able to read and see the contents of the MySQL data directory. If the configured user does not already have access, you can use the --root-command-prefix=true option to grant root access to access the filesystem.

- Using the MySQL INFORMATION_SCHEMA to look for tables defined with the MyISAM engine. For this option to work, intensive checks must have been enabled using --mysql-allow-intensive-checks.

If neither of these methods is available, the check will fail and installation will stop.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQLNoMySQLReplicationCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLNoMySQLReplicationCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLPasswordSettingCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLPasswordSettingCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLPermissionsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLPermissionsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLReadableLogsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLReadableLogsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLSettingsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLSettingsCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLSuperReadOnlyCheck</td>
<td>Checks whether super_read_only has been enabled on MySQL</td>
</tr>
<tr>
<td>MySQLSuperReadOnlyCheck</td>
<td>Checks whether super_read_only has been enabled on MySQL</td>
</tr>
</tbody>
</table>

Checks whether the super_read_only variable within MySQL has been enabled. If enabled, replication will not work. The check will test both the running server and the configuration file to determine whether the value has been enabled.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQLTriggerCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLTriggerCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLUnsupportedDataTypesCheck</td>
<td></td>
</tr>
<tr>
<td>MySQLUnsupportedDataTypesCheck</td>
<td></td>
</tr>
</tbody>
</table>

329
<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>− MysqlConnectorCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>MysqlConnectorCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− MysqlDumpAvailableCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>MysqlDumpAvailableCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− MysqlDumpSettingsCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>MysqlDumpSettingsCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− NewDirectoryRequiredCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>NewDirectoryRequiredCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− NtpdRunningCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>NtpdRunningCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OSCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OSCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OldServicesRunningCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OldServicesRunningCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OpenFilesLimitCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OpenFilesLimitCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OpenSslLibraryCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OpenSslLibraryCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OracleLoginCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OracleLoginCheck [330]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>− OraclePermissionsCheck [330]</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>OraclePermissionsCheck [330]</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>OracleRedoReaderMinerDirectoryCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>OracleServiceSIDCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>OracleVersionCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PGAvailableCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>ParallelReplicationCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>ParallelReplicationCountCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PgControlAvailableCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PgStandbyAvailableCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PgdumpAvailableCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PgdumpallAvailableCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>PingSyntaxCheck [331]</td>
<td>Description</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>PortAvailabilityCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>PortAvailabilityCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>ProfileScriptCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ProfileScriptCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RMIListenerAddressCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RMIListenerAddressCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RelayDirectoryWriteableCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RelayDirectoryWriteableCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Checks that the relay log directory can be written to</td>
</tr>
<tr>
<td></td>
<td>Confirms that the directory defined in <code>--relay-log-dir</code> directory exists and can be written to</td>
</tr>
<tr>
<td>ReplicatorChecks [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>ReplicatorChecks [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RestartComponentsCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RestartComponentsCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RouterAffinityCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RouterAffinityCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RouterBridgeModeDefaultCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RouterBridgeModeDefaultCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RouterDelayBeforeOfflineCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RouterDelayBeforeOfflineCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RouterKeepAliveTimeoutCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RouterKeepAliveTimeoutCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
<tr>
<td>RowBasedBinaryLoggingCheck [332]</td>
<td></td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td>RowBasedBinaryLoggingCheck [332]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Description

Checks that Row-based binary logging has been enabled for heterogeneous deployments.

For heterogeneous deployments, row-based binary logging must have been enabled. For all services where heterogeneous support has been enabled, for example due to `--enable-heterogeneous-service` or `--enable-batch-service` (in [Tungsten Replicator 2.2 Manual](#)), row-based logging within MySQL must have been switched on. The test looks for the value of `binlog_format=ROW`.

### Option

- **RsyncAvailableCheck**

### Description

#### RubyVersionCheck

### Description

- **SSHLoginCheck**

  Checks connectivity to other hosts over SSH.

  Checks to confirm the SSH logins to other hosts in the cluster work, without requiring a password, and without returning additional rows of information when directly, remotely, running a command.

  In the event of the check failing, the following items should be checked:

  - Confirm that it is possible to SSH to the remote site using the username provided, and without requiring a password. For example:

    ```
    host1-shell> ssh tungsten@host2
    host2-shell>
    ```

  - Remove any remote messages returned when the user logs in. This includes the output from the `Banner` argument within `/etc/ssh/sshd_config`, or text or files output by the users shell login script or profile.

  - Ensure that your remote shell has not been configured to output text or a message when a logout is attempted, for example by using:

    ```
    shell> trap 'echo logout' 0
    ```

### Option

- **ServiceTransferredLogStorageCheck**

### Description

- **StartingStoppedServices**

### Option

- **SudoCheck**

### Description

- **SwappinessCheck**

### Option

Checks whether the Linux swappiness parameter has been set to a value of 10 or less, both in the current setting and when the system reboots. A value greater than 10 may allow for running programs to be swapped out, which will affect the performance of the Continuent Tungsten when running. Change the value in `sysctl.conf`.

333
The `tpm` Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>THLDirectoryWriteableCheck</td>
<td></td>
</tr>
<tr>
<td>THLListenerAddressCheck</td>
<td></td>
</tr>
<tr>
<td>THLSchemaChangeCheck</td>
<td>Checks that the format of the current THL is compatible with the schema and format of the new software. A difference may mean that the THL needs to be reset before installation can continue.</td>
</tr>
<tr>
<td>THLStorageCheck</td>
<td>Confirms the THL storage directory exists, is empty and writeable</td>
</tr>
<tr>
<td>THLStorageChecksum</td>
<td></td>
</tr>
<tr>
<td>TargetDirectoryDoesNotExist</td>
<td></td>
</tr>
<tr>
<td>TransferredLogStorageCheck</td>
<td></td>
</tr>
<tr>
<td>UpgradeSameProductCheck</td>
<td>Ensures that the same product is being updated</td>
</tr>
<tr>
<td>VIPEnabledHostAllowsRootCommands</td>
<td></td>
</tr>
<tr>
<td>VIPEnabledHostArpPath</td>
<td></td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>VIPEnabledHostIfconfigPath</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks that the Vertica user has the correct OS group membership</td>
</tr>
</tbody>
</table>

Checks whether the user running Vertica is a member of the tungsten user's primary group. Without this setting, the CSV files generated by the replicator would not be readable by Vertica when importing them into the database during batchloading.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>VerticaUserGroupsCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks that the Vertica user has the correct OS group membership</td>
</tr>
</tbody>
</table>

Checks that the Vertica user has the correct OS group membership.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>WhichAvailableCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Checks the existence of a working <code>which</code> command</td>
</tr>
</tbody>
</table>

Checks the existence of a working `which` command.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>WriteableHomeDirectoryCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ensures the home directory can be written to</td>
</tr>
</tbody>
</table>

Checks that the home directory for the configured user can be written to.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>WriteableTempDirectoryCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ensures the temporary directory can be written to</td>
</tr>
</tbody>
</table>

Ensures the temporary directory can be written to.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>XtrabackupAvailableCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ensures the temporary directory can be written to</td>
</tr>
</tbody>
</table>

The temporary directory is used during installation to store a variety of information. This check ensures that the directory is writeable, and that files can be created and deleted correctly.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>XtrabackupDirectoryWritableCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ensures the temporary directory can be written to</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>XtrabackupSettingsCheck</strong> [335]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Ensures the temporary directory can be written to</td>
</tr>
</tbody>
</table>

### 9.8. tpm Configuration Options

**tpm** supports a large range of configuration options, which can be specified either:

- On the command-line, using a double-dash prefix, i.e. `--repl-thl-log-retention=3d` [376]
- In an INI file, without the double-dash prefix, i.e. `repl-thl-log-retention=3d` [376]
A full list of all the available options supported is provided in Table 9.6, “tpm Configuration Options”.

### Table 9.6. tpm Configuration Options

<table>
<thead>
<tr>
<th>CmdLine Option</th>
<th>INI File Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>repl-allow-bidi-unsafe [343]</td>
<td>allow-bidi-unsafe [343], repl-allow-bidi-unsafe [343]</td>
<td>Allow unsafe SQL from remote service</td>
</tr>
<tr>
<td>repl-api [344]</td>
<td>api [344], repl-api [344]</td>
<td>Enable the replication API</td>
</tr>
<tr>
<td>repl-api-host [344]</td>
<td>api-host [344], repl-api-host [344]</td>
<td>Hostname that the replication API should listen on</td>
</tr>
<tr>
<td>repl-api-password [344], repl-api-user [344]</td>
<td>api-password [344], repl-api-password [344]</td>
<td>HTTP basic auth password for the replication API</td>
</tr>
<tr>
<td>repl-api-port [344]</td>
<td>api-port [344], repl-api-port [344]</td>
<td>Port that the replication API should bind to</td>
</tr>
<tr>
<td>repl-application-password [344], repl-application-user [344]</td>
<td>application-password [344], connector-password [344], repl-application-password [344], repl-application-user [344]</td>
<td>Database password for the connector</td>
</tr>
<tr>
<td>repl-application-port [345], repl-application-listen-port [345]</td>
<td>application-port [345], connector-listen-port [345]</td>
<td>Port for the connector to listen on</td>
</tr>
<tr>
<td>repl-application-readonly-port [345], repl-application-readonly-listen-port [345]</td>
<td>application-readonly-port [345], connector-readonly-listen-port [345]</td>
<td>Port for the connector to listen for read-only connections on</td>
</tr>
<tr>
<td>repl-application-user [345], repl-application-user [345]</td>
<td>application-user [345], connector-user [345]</td>
<td>Database username for the connector</td>
</tr>
<tr>
<td>repl-auto-enable [345]</td>
<td>auto-enable [345], repl-auto-enable [345]</td>
<td>Auto-enable services after start-up</td>
</tr>
<tr>
<td>repl-auto-recovery-delay-interval [345], repl-auto-recovery-delay-interval [345]</td>
<td>auto-recovery-delay-interval [345], repl-auto-recovery-delay-interval [345]</td>
<td>Delay between going OFFLINE and attempting to go ONLINE</td>
</tr>
<tr>
<td>repl-auto-recovery-max-attempts [345], repl-auto-recovery-max-attempts [345]</td>
<td>auto-recovery-max-attempts [345], repl-auto-recovery-max-attempts [345]</td>
<td>Maximum number of attempts at automatic recovery</td>
</tr>
<tr>
<td>repl-auto-recovery-reset-interval [346], repl-auto-recovery-reset-interval [346]</td>
<td>auto-recovery-reset-interval [346], repl-auto-recovery-reset-interval [346]</td>
<td>Delay before autorecovery is deemed to have succeeded</td>
</tr>
<tr>
<td>repl-backup-directory [346], repl-backup-directory [346]</td>
<td>backup-directory [346], repl-backup-directory [346]</td>
<td>Permanent backup storage directory</td>
</tr>
<tr>
<td>repl-backup-online [346], repl-backup-online [346]</td>
<td>backup-online [346], repl-backup-online [346]</td>
<td>Does the backup script support backing up a datasource while it is ONLINE</td>
</tr>
<tr>
<td>repl-backup-retention [347], repl-backup-retention [347]</td>
<td>backup-retention [347], repl-backup-retention [347]</td>
<td>Number of backups to retain</td>
</tr>
<tr>
<td>repl-backup-script [347], repl-backup-script [347]</td>
<td>backup-script [347], repl-backup-script [347]</td>
<td>What is the path to the backup script</td>
</tr>
<tr>
<td>repl-batch-enabled [347]</td>
<td>batch-enabled [347]</td>
<td>Should the replicator service use a batch applier</td>
</tr>
<tr>
<td>repl-batch-load-template [347]</td>
<td>batch-load-template [347]</td>
<td>Value for the loadBatchTemplate property</td>
</tr>
<tr>
<td>CmdLine Option</td>
<td>INI File Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-channels [348], ... repl-channels</td>
<td>channels [348], repl-channels [348]</td>
<td>Number of replication channels to use for services</td>
</tr>
<tr>
<td>-composite-datasources [348], ...</td>
<td>composite-datasources [348],</td>
<td>Data services that should be added to this composite data service</td>
</tr>
<tr>
<td>-dataservice-composite-datasources</td>
<td>dataservice-composite-datasources [348]</td>
<td></td>
</tr>
<tr>
<td>-conn-java-enable-concurrent</td>
<td>conn-java-enable-concurrent [348]</td>
<td>Connector Java uses concurrent garbage collection</td>
</tr>
<tr>
<td>-conn-java-men-size [348]</td>
<td>conn-java-men-size [348]</td>
<td>Connector Java heap memory size used to buffer data between clients and databases</td>
</tr>
<tr>
<td>-conn-round-robin-include-master</td>
<td>conn-round-robin-include-master [348]</td>
<td>Should the Connector include the master in round-robin load balancing</td>
</tr>
<tr>
<td>-connector-affinity [348]</td>
<td>connector-affinity [348]</td>
<td>The default affinity for all connections</td>
</tr>
<tr>
<td>-connector-bridge-mode [349], ...</td>
<td>connector-bridge-mode [349], enable-connector-bridge-mode [349]</td>
<td>Enable the Tungsten Connector bridge mode</td>
</tr>
<tr>
<td>-connector-default-schema [349], ...</td>
<td>connector-default-schema [349], enable-schema [349]</td>
<td>Default schema for the connector to use</td>
</tr>
<tr>
<td>-connector-drop-after-max-connections</td>
<td>connector-drop-after-max-connections [349]</td>
<td>Instantly drop connections that arrive after --connector-max-connections has been reached</td>
</tr>
<tr>
<td>-connector-listen-interface [349]</td>
<td>connector-listen-interface [349]</td>
<td>Listen interface to use for the connector</td>
</tr>
<tr>
<td>-connector-max-connections [349]</td>
<td>connector-max-connections [349]</td>
<td>The maximum number of connections the connector should allow at any time</td>
</tr>
<tr>
<td>-connector-max-slave-latency [350],</td>
<td>connector-max-slave-latency [350]</td>
<td>The maximum applied latency for slave connections</td>
</tr>
<tr>
<td>-connector-readonly [350], ...</td>
<td>connector-readonly [350], enable-connector-readonly [350]</td>
<td>Enable the Tungsten Connector read-only mode</td>
</tr>
<tr>
<td>-connector-ro-addresses [350]</td>
<td>connector-ro-addresses [350]</td>
<td>Connector addresses that should receive a r/o connection</td>
</tr>
<tr>
<td>-connector-rw-addresses [350]</td>
<td>connector-rw-addresses [350]</td>
<td>Connector addresses that should receive a r/w connection</td>
</tr>
<tr>
<td>-connector-smartscale [350]</td>
<td>connector-smartscale [350]</td>
<td>Enable SmartScale R/W splitting in the connector</td>
</tr>
<tr>
<td>-connector-smartscale-session-id</td>
<td>connector-smartscale-session-id [350]</td>
<td>The default session ID to use with smart scale</td>
</tr>
<tr>
<td>-connectors [351], ...</td>
<td>connectors [351], dataservice-connectors [351]</td>
<td>Hostnames for the dataservice connectors</td>
</tr>
<tr>
<td>-consistency-policy [351], ...</td>
<td>consistency-policy [351], repl-consistency-policy [351]</td>
<td>Should the replicator stop or warn if a consistency check fails?</td>
</tr>
<tr>
<td>-dataservice-name [351]</td>
<td>dataservice-name [351]</td>
<td>Limit the command to the hosts in this dataservice Multiple data services may be specified by providing a comma separated list</td>
</tr>
<tr>
<td>-dataservice-relay-enabled [351]</td>
<td>dataservice-relay-enabled [351]</td>
<td>Make this dataservice the slave of another</td>
</tr>
<tr>
<td>-dataservice-schema [351]</td>
<td>dataservice-schema [351]</td>
<td>The db schema to hold dataservice details</td>
</tr>
<tr>
<td>-dataservice-thl-port [351]</td>
<td>dataservice-thl-port [351]</td>
<td>Port to use for THL operations</td>
</tr>
<tr>
<td>-dataservice-use-relative-latency</td>
<td>dataservice-use-relative-latency [351], use-relative-latency [351]</td>
<td>Enable the cluster to operate on relative latency</td>
</tr>
<tr>
<td>-dataservice-vip-enabled [352]</td>
<td>dataservice-vip-enabled [352]</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>-dataservice-vip-ipaddress [352]</td>
<td>dataservice-vip-ipaddress [352]</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>CmdLine Option</td>
<td>INI File Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>repl:datasource-boot-script [352]</td>
<td>datasource-boot-script [352]</td>
<td>Database start script</td>
</tr>
</tbody>
</table>

---

**The tpm Deployment Command**
<table>
<thead>
<tr>
<th>CmdLine Option</th>
<th>INI File Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-datasource-type [355], repl-direct-datasource-type [355]</td>
<td>direct-datasource-type [355], repl-direct-datasource-type [355]</td>
<td>Database type</td>
</tr>
<tr>
<td>--enable-active-witnesses [356], repl-active-witnesses [356]</td>
<td>active-witnesses [356], repl-active-witnesses [356]</td>
<td>Enable active witness hosts</td>
</tr>
<tr>
<td>--enable-connector-ssl [357], repl-connector-ssl [357]</td>
<td>connector-ssl [357], repl-connector-ssl [357]</td>
<td>Enable SSL encryption of connector traffic to the database</td>
</tr>
<tr>
<td>--enable-heterogenous-master [357]</td>
<td>enable-heterogenous-master [357]</td>
<td>Enable heterogenous operation for the master</td>
</tr>
<tr>
<td>--enable-heterogenous-service [357]</td>
<td>enable-heterogenous-service [357]</td>
<td>Enable heterogenous operation</td>
</tr>
<tr>
<td>--enable-heterogenous-slave [357]</td>
<td>enable-heterogenous-slave [357]</td>
<td>Enable heterogenous operation for the slave</td>
</tr>
<tr>
<td>--enable-rmi-ssl [357], repl-enable-rmi-ssl [357]</td>
<td>enable-rmi-ssl [357], repl-enable-rmi-ssl [357]</td>
<td>Enable SSL encryption of RMI communication on this host</td>
</tr>
<tr>
<td>--enable-slave-thl-listener [357], repl-enable-slave-thl-listener [357]</td>
<td>enable-slave-thl-listener [357], repl-enable-slave-thl-listener [357]</td>
<td>Should this service allow THL connections?</td>
</tr>
<tr>
<td>--enable-sudo-access [358], repl-enable-sudo-access [358], root-command-prefix [358]</td>
<td>enable-sudo-access [358], repl-enable-sudo-access [358], root-command-prefix [358]</td>
<td>Run root commands using sudo</td>
</tr>
<tr>
<td>--enable-thl-ssl [358], repl-enable-thl-ssl [358]</td>
<td>enable-thl-ssl [358], repl-enable-thl-ssl [358]</td>
<td>Enable SSL encryption of THL communication for this service</td>
</tr>
<tr>
<td>--host-name [358]</td>
<td>host-name [358]</td>
<td>DNS hostname</td>
</tr>
<tr>
<td>--hosts [358]</td>
<td>hosts [358]</td>
<td>Limit the command to the hosts listed You must use the hostname as it appears in the configuration.</td>
</tr>
<tr>
<td>--hub [358], dataservice-hub-host [358]</td>
<td>dataservice-hub-host [358], hub [358]</td>
<td>What is the hub host for this all-masters dataservice?</td>
</tr>
<tr>
<td>--hub-service [358], dataservice-hub-service [358]</td>
<td>dataservice-hub-service [358], hub-service [358]</td>
<td>The data service to use for the hub of a star topology</td>
</tr>
<tr>
<td>--install [358]</td>
<td>install [358]</td>
<td>Install service start scripts</td>
</tr>
<tr>
<td>--install-directory [359], home-directory [359]</td>
<td>home-directory [359], install-directory [359]</td>
<td>Installation directory</td>
</tr>
<tr>
<td>CmdLine Option</td>
<td>INI File Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>--java-file-encoding [359], --repl-java-file-encoding [359]</td>
<td>java-file-encoding [359], repl-java-file-encoding [359]</td>
<td>Java platform charset (esp. for heterogeneous replication)</td>
</tr>
<tr>
<td>--java-keystore-password [360]</td>
<td>java-keystore-password [360]</td>
<td>The password for unlocking the tungsten_truststore.jks file in the security directory</td>
</tr>
<tr>
<td>--java-truststore-password [360]</td>
<td>java-truststore-password [360]</td>
<td>The password for unlocking the tungsten_truststore.jks file in the security directory</td>
</tr>
<tr>
<td>--java-user-timezone [361], --repl-java-user-timezone [361]</td>
<td>java-user-timezone [361], repl-java-user-timezone [361]</td>
<td>Java VM Timezone (esp. for cross-site replication)</td>
</tr>
<tr>
<td>--log [361]</td>
<td>log [361]</td>
<td>Write all messages, visible and hidden, to this file. You may specify a filename, 'pid' or 'timestamp'.</td>
</tr>
<tr>
<td>--master [361], --dataservice-master-host [361], --mangers [361], --relay [361]</td>
<td>dataservice-master-host [361], masters [361], relay [361]</td>
<td>Hostname of the master host within this service</td>
</tr>
<tr>
<td>--master-preferred-role [361], --repl-master-preferred-role [361]</td>
<td>master-preferred-role [361], repl-master-preferred-role [361]</td>
<td>Preferred role for master THL when connecting as a slave</td>
</tr>
<tr>
<td>--master-services [361], --dataservice-master-services [361]</td>
<td>dataservice-master-services [361], master-services [361]</td>
<td>Data service names that should be used on each master</td>
</tr>
<tr>
<td>--members [362], --dataservice-members [362]</td>
<td>dataservice-hosts [362], members [362]</td>
<td>Hostnames for the dataservice members</td>
</tr>
<tr>
<td>--mgr-api [362]</td>
<td>mgr-api [362]</td>
<td>Enable the Manager API</td>
</tr>
<tr>
<td>--mgr-api-address [362]</td>
<td>mgr-api-address [362]</td>
<td>Address for the Manager API</td>
</tr>
<tr>
<td>--mgr-api-port [362]</td>
<td>mgr-api-port [362]</td>
<td>Port for the Manager API</td>
</tr>
<tr>
<td>--mgr-group-communication-port [362]</td>
<td>mgr-group-communication-port [362]</td>
<td>Port to use for manager group communication</td>
</tr>
<tr>
<td>--mgr-heap-threshold [362]</td>
<td>mgr-heap-threshold [362]</td>
<td>Java memory usage (MB) that will force a Manager restart</td>
</tr>
<tr>
<td>--mgr-listen-interface [363]</td>
<td>mgr-listen-interface [363]</td>
<td>Listen interface to use for the manager</td>
</tr>
<tr>
<td>--mgr-rmi-port [363]</td>
<td>mgr-rmi-port [363]</td>
<td>Port to use for the manager RMI server</td>
</tr>
<tr>
<td>--mgr-rmi-remote-port [363]</td>
<td>mgr-rmi-remote-port [363]</td>
<td>Port to use for calling the remote manager RMI server</td>
</tr>
<tr>
<td>--mgr-ro-slave [363]</td>
<td>mgr-ro-slave [363]</td>
<td>Make slaves read-only</td>
</tr>
<tr>
<td>--mgr-vip-arp-path [364]</td>
<td>mgr-vip-arp-path [364]</td>
<td>Path to the arp binary</td>
</tr>
<tr>
<td>--mgr-vip-ifconfig-path [364]</td>
<td>mgr-vip-ifconfig-path [364]</td>
<td>Path to the ifconfig binary</td>
</tr>
<tr>
<td>CmdLine Option</td>
<td>INI File Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-mrg-wait-for-members</td>
<td>mrg-wait-for-members</td>
<td>Wait for all datasources to be available before completing installation</td>
</tr>
<tr>
<td>-mysql-connectorj-path</td>
<td>mysql-connectorj-path</td>
<td>Path to MySQL Connector/J</td>
</tr>
<tr>
<td>-mysql-driver</td>
<td>mysql-driver</td>
<td>MySQL Driver Vendor</td>
</tr>
<tr>
<td>-mysql-enable-ansiquotes</td>
<td>repl-mysql-enable-ansiquotes</td>
<td>Enables ANSI_QUOTES mode for incoming events?</td>
</tr>
<tr>
<td>-mysql-enable-enumtostring</td>
<td>repl-mysql-enable-enumtostring</td>
<td>Enable a filter to convert ENUM values to strings</td>
</tr>
<tr>
<td>-mysql-enable-noonlykeywords</td>
<td>repl-mysql-enable-noonlykeywords</td>
<td>Enables a filter to translate DELETE FROM ONLY TO DELETE FROM and UPDATE ONLY TO UPDATE.</td>
</tr>
<tr>
<td>-mysql-enable-settostring</td>
<td>repl-mysql-enable-settostring</td>
<td>Enable a filter to convert SET types to strings</td>
</tr>
<tr>
<td>-mysql-ro-slave</td>
<td>repl-mysql-ro-slave</td>
<td>Slaves are read-only?</td>
</tr>
<tr>
<td>-mysql-server-id</td>
<td>repl-mysql-server-id</td>
<td>Explicitly set the MySQL server ID</td>
</tr>
<tr>
<td>-mysql-use-bytes-for-string</td>
<td>repl-mysql-use-bytes-for-string</td>
<td>Transfer strings as their byte representation?</td>
</tr>
<tr>
<td>-mysql-xtrabackup-dir</td>
<td>repl-mysql-xtrabackup-dir</td>
<td>Directory to use for storing xtrabackup full &amp; incremental backups</td>
</tr>
<tr>
<td>-native-slave-takeover</td>
<td>repl-native-slave-takeover</td>
<td>Takeover native replication</td>
</tr>
<tr>
<td>-no-deployment</td>
<td>no-deployment</td>
<td>Skip deployment steps that create the install directory</td>
</tr>
<tr>
<td>-no-validation</td>
<td>no-validation</td>
<td>Skip validation checks that run on each host</td>
</tr>
<tr>
<td>-pg-archive-timeout</td>
<td>repl-pg-archive-timeout</td>
<td>Timeout for sending unfilled WAL buffers (data loss window)</td>
</tr>
<tr>
<td>-pg-ctl</td>
<td>repl-pg-ctl</td>
<td>Path to the pg_ctl script</td>
</tr>
<tr>
<td>-pg-method</td>
<td>repl-pg-method</td>
<td>Postgres Replication method</td>
</tr>
<tr>
<td>-pg-standby</td>
<td>repl-pg-standby</td>
<td>Path to the pg_standby script</td>
</tr>
<tr>
<td>-postgresql-dbname</td>
<td>repl-postgresql-dbname</td>
<td>Name of the database to replicate</td>
</tr>
<tr>
<td>-postgresql-enable-mysql2pgddl</td>
<td>repl-postgresql-enable-mysql2pgddl</td>
<td>Enable MySQL to PostgreSQL DDL dialect converting filter placeholder</td>
</tr>
<tr>
<td>-postgresql-slonik</td>
<td>repl-postgresql-slonik</td>
<td>Path to the slonik executable</td>
</tr>
<tr>
<td>-postgresql-tables</td>
<td>repl-postgresql-tables</td>
<td>Tables to replicate in form: schema1.table1,schema2.table2,...</td>
</tr>
<tr>
<td>-preferred-path</td>
<td>preferred-path</td>
<td>Additional command path</td>
</tr>
<tr>
<td>-prefetch-enabled</td>
<td>prefetch-enabled</td>
<td>Should the replicator service be setup as a prefetch applier</td>
</tr>
<tr>
<td>-prefetch-max-time-ahead</td>
<td>prefetch-max-time-ahead</td>
<td>Maximum number of seconds that the prefetch applier can get in front of the standard applier</td>
</tr>
<tr>
<td>-prefetch-min-time-ahead</td>
<td>prefetch-min-time-ahead</td>
<td>Minimum number of seconds that the prefetch applier must be in front of the standard applier</td>
</tr>
<tr>
<td>-prefetch-schema</td>
<td>prefetch-schema</td>
<td>Schema to watch for timing prefetch progress</td>
</tr>
<tr>
<td>CmdLine Option</td>
<td>INI File Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-xf &lt;time&gt;</td>
<td>prefetch-sleep-time [368]</td>
<td>How long to wait when the prefetch applier gets too far ahead</td>
</tr>
<tr>
<td>-p &lt;script&gt;</td>
<td>profile-script [368]</td>
<td>Append commands to include env.sh in this profile script</td>
</tr>
<tr>
<td>-cf &lt;files&gt;</td>
<td>protect-configuration-files [369]</td>
<td>When enabled, configuration files are protected to be only readable and updatable by the configured user</td>
</tr>
<tr>
<td>-r &lt;directory&gt;</td>
<td>relay-directory [369], repl-relay-directory [369]</td>
<td>Directory for logs transferred from the master</td>
</tr>
<tr>
<td>--slave-enabled</td>
<td>relay-enabled [369]</td>
<td>Should the replicator service be setup as a relay master</td>
</tr>
<tr>
<td>-rs &lt;source&gt;</td>
<td>dataservice-rely-source [370], master-dataservice [370], relay-source [370]</td>
<td>Dataservice name to use as a relay source</td>
</tr>
<tr>
<td>-rhm &lt;host&gt;</td>
<td>datasource-host [370], repl-datasource-host [370]</td>
<td>Hostname of the datasource</td>
</tr>
<tr>
<td>-rpw &lt;password&gt;</td>
<td>datasource-password [370], repl-datasource-password [370], replication-password [370]</td>
<td>Database password</td>
</tr>
<tr>
<td>-rnp &lt;port&gt;</td>
<td>datasource-port [370], repl-datasource-port [370], replication-port [370]</td>
<td>Database network port</td>
</tr>
<tr>
<td>-ruu &lt;user&gt;</td>
<td>datasource-user [370], repl-datasource-user [370], replication-user [370]</td>
<td>User for database connection</td>
</tr>
<tr>
<td>--reset</td>
<td>reset [371]</td>
<td>Clear the current configuration before processing any arguments</td>
</tr>
<tr>
<td>-rmp &lt;port&gt;</td>
<td>repl-rmi-port [371], rmi-port [371]</td>
<td>Replication RMI listen port</td>
</tr>
<tr>
<td>-ru</td>
<td>rmi-user [371]</td>
<td>The username for RMI authentication</td>
</tr>
<tr>
<td>-rrole</td>
<td>repl-role [371], role [371]</td>
<td>What is the replication role for this service?</td>
</tr>
<tr>
<td>-rgp</td>
<td>router-gateway-port [371]</td>
<td>The router gateway port</td>
</tr>
<tr>
<td>-rjmxp</td>
<td>router-jmx-port [371]</td>
<td>The router jmx port</td>
</tr>
<tr>
<td>-sd</td>
<td>security-directory [372]</td>
<td>Storage directory for the Java security/encryption files</td>
</tr>
<tr>
<td>-saa</td>
<td>dataservice-service-alias [372], service-alias [372]</td>
<td>Replication alias of this dataservice</td>
</tr>
<tr>
<td>-stp</td>
<td>repl-service-type [372], service-type [372]</td>
<td>What is the replication service type?</td>
</tr>
<tr>
<td>--skip-statemap</td>
<td>skip-statemap [372]</td>
<td>Do not copy the cluster-home/conf/statemap.properties from the previous install</td>
</tr>
<tr>
<td>-spu</td>
<td>slave-privileged-updates [372]</td>
<td>Does login for slave update have superuser privileges</td>
</tr>
<tr>
<td>-ss</td>
<td>dataservice-slaves [372], slaves [372]</td>
<td>What are the slaves for this dataservice?</td>
</tr>
<tr>
<td>-s</td>
<td>start [372]</td>
<td>Start the services after configuration</td>
</tr>
<tr>
<td>-sar</td>
<td>start-and-report [373]</td>
<td>Start the services and report out the status after configuration</td>
</tr>
<tr>
<td>--svc-allwany-remote-service</td>
<td>repl-svc-allow-any-remote-service [373], svc-allow-any-remote-service [373]</td>
<td>Replicate from any service</td>
</tr>
<tr>
<td>--svc-applier-commit-size</td>
<td>repl-svc-applier-commit-size [373], svc-applier-commit-size [373]</td>
<td>Applier block commit size (min 1)</td>
</tr>
<tr>
<td>--svc-applier-filters</td>
<td>repl-svc-applier-filters [373], svc-applier-filters [373]</td>
<td>Replication service applier filters</td>
</tr>
</tbody>
</table>
### 9.8.1. A tpm Options

---

<table>
<thead>
<tr>
<th><strong>--allow-bidi-unsafe</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aliases</strong></td>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>--- allow-bidi-unsafe</td>
<td>--allow-bidi-unsafe [343]</td>
</tr>
<tr>
<td>--- repl-allow-bidi-unsafe</td>
<td>[343]</td>
</tr>
</tbody>
</table>

#### Description

The `--allow-bidi-unsafe` option is used to allow bidirectional unsafe operations in the tpm deployment. This is particularly useful in scenarios where direct master/master replication is required for high availability and performance. However, it should be used with caution as it can expose the system to potential data corruption risks.

**Aliases**

- **--allow-bidi-unsafe**
- **--repl-allow-bidi-unsafe**

**Option**

- **--allow-bidi-unsafe**
  - **Description**: Allow bidirectional unsafe operations in the tpm deployment.
The `tpm` Deployment Command

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>allow-bidi-unsafe [343], repl-allow-bidi-unsafe [343]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Allow unsafe SQL from remote service</td>
</tr>
<tr>
<td>Value Type</td>
<td>boolean</td>
</tr>
<tr>
<td>Valid Values</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>true</td>
</tr>
</tbody>
</table>

|--api

<table>
<thead>
<tr>
<th>Option</th>
<th>--api [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-api [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>api [344], repl-api [344]</td>
</tr>
<tr>
<td>Description</td>
<td>Enable the replication API</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

|--api-host

<table>
<thead>
<tr>
<th>Option</th>
<th>--api-host [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-api-host [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>api-host [344], repl-api-host [344]</td>
</tr>
<tr>
<td>Description</td>
<td>Hostname that the replication API should listen on</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

|--api-password

<table>
<thead>
<tr>
<th>Option</th>
<th>--api-password [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-api-password [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>api-password [344], repl-api-password [344]</td>
</tr>
<tr>
<td>Description</td>
<td>HTTP basic auth password for the replication API</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

|--api-port

<table>
<thead>
<tr>
<th>Option</th>
<th>--api-port [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-api-port [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>api-port [344], repl-api-port [344]</td>
</tr>
<tr>
<td>Description</td>
<td>Port that the replication API should bind to</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

|--api-user

<table>
<thead>
<tr>
<th>Option</th>
<th>--api-user [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-api-user [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>api-user [344], repl-api-user [344]</td>
</tr>
<tr>
<td>Description</td>
<td>HTTP basic auth username for the replication API</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

|--application-password

<table>
<thead>
<tr>
<th>Option</th>
<th>--application-password [344]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--connector-password [344]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>application-password [344], connector-password [344]</td>
</tr>
<tr>
<td>Description</td>
<td>Database password for the connector</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>
The tpm Deployment Command

### --application-port

<table>
<thead>
<tr>
<th>Option</th>
<th>--application-port 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--connector-listen-port 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>application-port 345, connector-listen-port 345</td>
</tr>
<tr>
<td>Description</td>
<td>Port for the connector to listen on</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --application-readonly-port

<table>
<thead>
<tr>
<th>Option</th>
<th>--application-readonly-port 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--connector-readonly-listen-port 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>application-readonly-port 345, connector-readonly-listen-port 345</td>
</tr>
<tr>
<td>Description</td>
<td>Port for the connector to listen for read-only connections on</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --application-user

<table>
<thead>
<tr>
<th>Option</th>
<th>--application-user 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--connector-user 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>application-user 345, connector-user 345</td>
</tr>
<tr>
<td>Description</td>
<td>Database username for the connector</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --auto-enable

<table>
<thead>
<tr>
<th>Option</th>
<th>--auto-enable 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-auto-enable 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>auto-enable 345, repl-auto-enable 345</td>
</tr>
<tr>
<td>Description</td>
<td>Auto-enable services after start-up</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --auto-recovery-delay-interval

<table>
<thead>
<tr>
<th>Option</th>
<th>--auto-recovery-delay-interval 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-auto-recovery-delay-interval 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>auto-recovery-delay-interval 345, repl-auto-recovery-delay-interval 345</td>
</tr>
<tr>
<td>Description</td>
<td>Delay between going OFFLINE and attempting to go ONLINE</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>5</td>
</tr>
</tbody>
</table>

The delay between the replicator identifying that autorecovery is needed, and autorecovery being attempted. For busy MySQL installations, larger numbers may be needed to allow time for MySQL servers to restart or recover from their failure.

### --auto-recovery-max-attempts

<table>
<thead>
<tr>
<th>Option</th>
<th>--auto-recovery-max-attempts 345</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-auto-recovery-max-attempts 345</td>
</tr>
<tr>
<td>Config File Options</td>
<td>auto-recovery-max-attempts 345, repl-auto-recovery-max-attempts 345</td>
</tr>
<tr>
<td>Description</td>
<td>Maximum number of attempts at automatic recovery</td>
</tr>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
<tr>
<td>Valid Values</td>
<td>0</td>
</tr>
</tbody>
</table>

Specifies the number of attempts the replicator will make to go back online. When the number of attempts has been reached, the replicator will remain in the OFFLINE state.
Autorecovery is not enabled until the value of this parameter is set to a non-zero value. The state of autorecovery can be determined using the \texttt{autoRecoveryEnabled} status parameter. The number of attempts made to autorecover can be tracked using the \texttt{autoRecoveryTotal} status parameter.

\textbf{--auto-recovery-reset-interval}

<table>
<thead>
<tr>
<th>Option</th>
<th>\texttt{--auto-recovery-reset-interval} [346]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>\texttt{--repl-auto-recovery-reset-interval} [346]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>\texttt{auto-recovery-reset-interval} [346], \texttt{repl-auto-recovery-reset-interval} [346]</td>
</tr>
<tr>
<td>Description</td>
<td>Delay before autorecovery is deemed to have succeeded</td>
</tr>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
<tr>
<td>Valid Values</td>
<td>5</td>
</tr>
</tbody>
</table>

The time in \texttt{ONLINE} state that indicates to the replicator that the autorecovery procedure has succeeded. For servers with very large transactions, this value should be increased to allow the transaction to be successfully applied.

\section*{9.8.2. \texttt{tpm} Options}

\textbf{--backup-directory}

<table>
<thead>
<tr>
<th>Option</th>
<th>\texttt{--backup-directory} [346]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>\texttt{--repl-backup-directory} [346]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>\texttt{backup-directory} [346], \texttt{repl-backup-directory} [346]</td>
</tr>
<tr>
<td>Description</td>
<td>Permanent backup storage directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Default</td>
<td>\texttt{(home directory)/backups}</td>
</tr>
<tr>
<td>Valid Values</td>
<td>\texttt{(home directory)/backups}</td>
</tr>
</tbody>
</table>

\textbf{--backup-dump-directory}

<table>
<thead>
<tr>
<th>Option</th>
<th>\texttt{--backup-dump-directory} [346]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>\texttt{--repl-backup-dump-directory} [346]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>\texttt{backup-dump-directory} [346], \texttt{repl-backup-dump-directory} [346]</td>
</tr>
<tr>
<td>Description</td>
<td>Backup temporary dump directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

\textbf{--backup-method}

<table>
<thead>
<tr>
<th>Option</th>
<th>\texttt{--backup-method} [346]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>\texttt{--repl-backup-method} [346]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>\texttt{backup-method} [346], \texttt{repl-backup-method} [346]</td>
</tr>
<tr>
<td>Description</td>
<td>Database backup method</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>\texttt{ebs-snapshot}</td>
</tr>
<tr>
<td></td>
<td>\texttt{file-copy-snapshot}</td>
</tr>
<tr>
<td></td>
<td>\texttt{mysqldump} Use \texttt{mysqldump}</td>
</tr>
<tr>
<td></td>
<td>\texttt{none}</td>
</tr>
<tr>
<td></td>
<td>\texttt{script} Use a custom script</td>
</tr>
<tr>
<td></td>
<td>\texttt{xtrabackup} Use Percona XtraBackup</td>
</tr>
<tr>
<td></td>
<td>\texttt{xtrabackup-full} Use Percona XtraBackup Full</td>
</tr>
<tr>
<td></td>
<td>\texttt{xtrabackup-incremental} Use Percona XtraBackup Incremental</td>
</tr>
</tbody>
</table>

\textbf{--backup-online}
<table>
<thead>
<tr>
<th>Option</th>
<th>Alias(es)</th>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--backup-online</td>
<td>--repl-backup-online</td>
<td>backup-online, repl-backup-online</td>
<td>Does the backup script support backing up a datasource while it is ONLINE</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>--backup-retention</td>
<td>--repl-backup-retention</td>
<td>backup-retention, repl-backup-retention</td>
<td>Number of backups to retain</td>
<td>numeric</td>
<td></td>
</tr>
<tr>
<td>--backup-script</td>
<td>--repl-backup-script</td>
<td>backup-script, repl-backup-script</td>
<td>What is the path to the backup script</td>
<td>filename</td>
<td></td>
</tr>
<tr>
<td>--batch-enabled</td>
<td>-</td>
<td>batch-enabled</td>
<td>Should the replicator service use a batch applier</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>--batch-load-language</td>
<td>-</td>
<td>batch-load-language</td>
<td>Which script language to use for batch loading</td>
<td>string</td>
<td>js, sql</td>
</tr>
<tr>
<td>--batch-load-template</td>
<td>-</td>
<td>batch-load-template</td>
<td>Value for the loadBatchTemplate property</td>
<td>string</td>
<td></td>
</tr>
</tbody>
</table>
### 9.8.3. C tpm Options

#### --channels

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--channels</td>
<td>Number of replication channels to use for services</td>
<td>numeric</td>
</tr>
<tr>
<td>--repl-channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>channels, repl-channels</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### --composite-datasources

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--composite-datasources</td>
<td>Data services that should be added to this composite data service</td>
<td>string</td>
</tr>
<tr>
<td>--dataservice-composite-datasources</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>composite-datasources, dataservice-composite-datasources</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### --config-file-help

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--config-file-help</td>
<td>Display help information for content of the config file</td>
<td>string</td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>config-file-help</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### --conn-java-enable-concurrent-gc

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--conn-java-enable-concurrent-gc</td>
<td>Connector Java uses concurrent garbage collection</td>
<td>string</td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>conn-java-enable-concurrent-gc</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### --conn-java-mem-size

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--conn-java-mem-size</td>
<td>Connector Java heap memory size used to buffer data between clients and databases</td>
<td>numeric</td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>conn-java-mem-size</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Valid Values:
- 256

The Connector allocates memory for each concurrent client connection, and may use up to the size of the configured MySQL `max_allowed_packet`. With multiple connections, the heap size should be configured to at least the combination of the number of concurrent connections multiplied by the maximum packet size.

#### --conn-round-robin-include-master

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--conn-round-robin-include-master</td>
<td>Should the Connector include the master in round-robin load balancing</td>
<td>string</td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>conn-round-robin-include-master</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### --connector-affinity

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--connector-affinity</td>
<td>Connector affinity</td>
<td></td>
</tr>
<tr>
<td><strong>Config File Options</strong></td>
<td>connector-affinity</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Value Type</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## The tpm Deployment Command

<table>
<thead>
<tr>
<th>Description</th>
<th>The default affinity for all connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-autoreconnect

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-autoreconnect [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-autoreconnect [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Enable auto-reconnect in the connector</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-bridge-mode

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-bridge-mode [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--enable-connector-bridge-mode [349]</code></td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>connector-bridge-mode [349], enable-connector-bridge-mode [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Enable the Tungsten Connector bridge mode</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-default-schema

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-default-schema [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--connector-forced-schema [349]</code></td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>connector-default-schema [349], connector-forced-schema [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Default schema for the connector to use</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-delete-user-map

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-delete-user-map [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-delete-user-map [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Overwrite an existing user.map file</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-disconnect-timeout

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-disconnect-timeout [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-disconnect-timeout [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Time (in seconds) to wait for active connection to disconnect before forcing them closed [default: 5]</td>
</tr>
<tr>
<td>Value Type</td>
<td>boolean</td>
</tr>
</tbody>
</table>

### --connector-drop-after-max-connections

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-drop-after-max-connections [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-drop-after-max-connections [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Instantly drop connections that arrive after --connector-max-connections has been reached</td>
</tr>
<tr>
<td>Value Type</td>
<td>boolean</td>
</tr>
</tbody>
</table>

### --connector-listen-interface

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-listen-interface [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-listen-interface [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Listen interface to use for the connector</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --connector-max-connections

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--connector-max-connections [349]</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td><code>connector-max-connections [349]</code></td>
</tr>
<tr>
<td>Description</td>
<td>Set the maximum number of connections that can be established</td>
</tr>
<tr>
<td>Value Type</td>
<td>integer</td>
</tr>
<tr>
<td>Option</td>
<td>Config File Options</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>--connector-max-connections</td>
<td>connector-max-connections</td>
</tr>
<tr>
<td>--connector-max-slave-latency</td>
<td>connector-max-applied-latency, connector-max-slave-latency</td>
</tr>
<tr>
<td>--connector-readonly</td>
<td>connector-readonly, enable-connector-readonly</td>
</tr>
<tr>
<td>--connector-ro-addresses</td>
<td>connector-ro-addresses</td>
</tr>
<tr>
<td>--connector-rw-addresses</td>
<td>connector-rw-addresses</td>
</tr>
<tr>
<td>--connector-rwsplitting</td>
<td>connector-rwsplitting</td>
</tr>
<tr>
<td>--connector-smartscale</td>
<td>connector-smartscale</td>
</tr>
<tr>
<td>--connector-smartscale-sessionid</td>
<td>connector-smartscale-sessionid</td>
</tr>
</tbody>
</table>
### 9.8.4. Dtpm Options

---

**--connectors**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--connectors

**Aliases**

--dataservice-connectors

**Config File Options**

collectors, dataservice-connectors

**Description**

Hostnames for the dataservice connectors

**Value Type**

string

---

**--consistency-policy**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--consistency-policy

**Aliases**

--repl-consistency-policy

**Config File Options**

consistency-policy, repl-consistency-policy

**Description**

Should the replicator stop or warn if a consistency check fails?

**Value Type**

string

---

**--dataservice-name**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--dataservice-name

**Config File Options**

dataservice-name

**Description**

Limit the command to the hosts in this dataservice Multiple data services may be specified by providing a comma separated list

**Value Type**

string

---

**--dataservice-relay-enabled**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--dataservice-relay-enabled

**Config File Options**

dataservice-relay-enabled

**Description**

Make this dataservice the slave of another

**Value Type**

string

---

**--dataservice-schema**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--dataservice-schema

**Config File Options**

dataservice-schema

**Description**

The db schema to hold dataservice details

**Value Type**

string

---

**--dataservice-thl-port**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--dataservice-thl-port

**Config File Options**

dataservice-thl-port

**Description**

Port to use for THL operations

**Value Type**

string

---

**--dataservice-use-relative-latency**

<table>
<thead>
<tr>
<th>Value Type</th>
<th>string</th>
</tr>
</thead>
</table>

**Option**

--dataservice-use-relative-latency

**Aliases**

--use-relative-latency

**Config File Options**

dataservice-use-relative-latency, use-relative-latency

**Description**

Enable the cluster to operate on relative latency
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>

**Option**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>

**Value Type**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>

**Aliases**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>

**Config File Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>

**Value Type**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-vip-enabled</td>
<td>Is VIP management enabled?</td>
</tr>
<tr>
<td>--dataservice-vip-ipaddress</td>
<td>VIP IP address</td>
</tr>
<tr>
<td>--dataservice-vip-netmask</td>
<td>VIP netmask</td>
</tr>
<tr>
<td>--datasource-boot-script</td>
<td>Database start script</td>
</tr>
<tr>
<td>--datasource-log-directory</td>
<td>Master log directory</td>
</tr>
<tr>
<td>--datasource-log-pattern</td>
<td>Master log filename pattern</td>
</tr>
<tr>
<td>--datasource-mysql-conf</td>
<td>MySQL config file</td>
</tr>
</tbody>
</table>
## The tpm Deployment Command

### --datasource-mysql-data-directory

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-mysql-data-directory [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-mysql-data-directory [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-mysql-data-directory [353], repl-datasource-mysql-data-directory [353]</td>
</tr>
<tr>
<td>Description</td>
<td>MySQL data directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-mysql-ibdata-directory

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-mysql-ibdata-directory [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-mysql-ibdata-directory [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-mysql-ibdata-directory [353], repl-datasource-mysql-ibdata-directory [353]</td>
</tr>
<tr>
<td>Description</td>
<td>MySQL InnoDB data directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-mysql-iblog-directory

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-mysql-iblog-directory [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-mysql-iblog-directory [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-mysql-iblog-directory [353], repl-datasource-mysql-iblog-directory [353]</td>
</tr>
<tr>
<td>Description</td>
<td>MySQL InnoDB log directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-oracle-scan

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-oracle-scan [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-oracle-scan [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-oracle-scan [353], repl-datasource-oracle-scan [353]</td>
</tr>
<tr>
<td>Description</td>
<td>Oracle SCAN</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-oracle-service

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-oracle-service [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-oracle-service [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-oracle-service [353], repl-datasource-oracle-service [353]</td>
</tr>
<tr>
<td>Description</td>
<td>Oracle Service</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-pg-archive

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-pg-archive [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-pg-archive [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-pg-archive [353], repl-datasource-pg-archive [353]</td>
</tr>
<tr>
<td>Description</td>
<td>PostgreSQL archive location</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### --datasource-pg-conf

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-pg-conf [353]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-pg-conf [353]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-pg-conf [353], repl-datasource-pg-conf [353]</td>
</tr>
<tr>
<td>Description</td>
<td>Location of postgresql.conf</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--datasource-pg-home**

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-pg-home [354]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-pg-home [354]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-pg-home [354], repl-datasource-pg-home [354]</td>
</tr>
<tr>
<td>Description</td>
<td>PostgreSQL data directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--datasource-pg-root**

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-pg-root [354]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-pg-root [354]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-pg-root [354], repl-datasource-pg-root [354]</td>
</tr>
<tr>
<td>Description</td>
<td>Root directory for postgresql installation</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--datasource-type**

<table>
<thead>
<tr>
<th>Option</th>
<th>--datasource-type [354]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-datasource-type [354]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>datasource-type [354], repl-datasource-type [354]</td>
</tr>
<tr>
<td>Description</td>
<td>Database type</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Default</td>
<td>mysql</td>
</tr>
<tr>
<td>Valid Values</td>
<td>File</td>
</tr>
<tr>
<td></td>
<td>hdfs</td>
</tr>
<tr>
<td></td>
<td>kafka</td>
</tr>
<tr>
<td></td>
<td>mongodb</td>
</tr>
<tr>
<td></td>
<td>mysql</td>
</tr>
<tr>
<td></td>
<td>oracle</td>
</tr>
<tr>
<td></td>
<td>postgres</td>
</tr>
<tr>
<td></td>
<td>vertica</td>
</tr>
<tr>
<td></td>
<td>postgres</td>
</tr>
<tr>
<td></td>
<td>vertica</td>
</tr>
</tbody>
</table>

**--delete**

<table>
<thead>
<tr>
<th>Option</th>
<th>--delete [354]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>delete [354]</td>
</tr>
<tr>
<td>Description</td>
<td>Delete the named data service from the configuration Data Service options:</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--deploy-current-package**

<table>
<thead>
<tr>
<th>Option</th>
<th>--deploy-current-package [354]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>deploy-current-package [354]</td>
</tr>
<tr>
<td>Description</td>
<td>Deploy the current Tungsten package</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--deploy-package-uri**

<table>
<thead>
<tr>
<th>Option</th>
<th>--deploy-package-uri [354]</th>
</tr>
</thead>
</table>
### Config File Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
<th>Default</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>deploy-package-uri</td>
<td>URL for the Tungsten package to deploy</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direct-datasource-log-directory</td>
<td>Master log directory</td>
<td>string</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td>direct-datasource-log-pattern</td>
<td>Master log filename pattern</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direct-datasource-oracle-scan</td>
<td>Oracle SCAN</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direct-datasource-oracle-service</td>
<td>Oracle Service</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direct-datasource-oracle-sid</td>
<td>Oracle SID</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direct-datasource-type</td>
<td>Database type</td>
<td>string</td>
<td>mysql</td>
<td>file</td>
</tr>
</tbody>
</table>

### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
<th>Default</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-datasource-log-directory</td>
<td>Master log directory</td>
<td>string</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td>--direct-datasource-log-pattern</td>
<td>Master log filename pattern</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--direct-datasource-oracle-scan</td>
<td>Oracle SCAN</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--direct-datasource-oracle-service</td>
<td>Oracle Service</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--direct-datasource-oracle-sid</td>
<td>Oracle SID</td>
<td>string</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--direct-datasource-type</td>
<td>Database type</td>
<td>string</td>
<td>mysql</td>
<td>file</td>
</tr>
</tbody>
</table>
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdfs</td>
<td>string</td>
</tr>
<tr>
<td>mongodb</td>
<td>string</td>
</tr>
<tr>
<td>mysql</td>
<td>string</td>
</tr>
<tr>
<td>oracle</td>
<td>string</td>
</tr>
<tr>
<td>vertica</td>
<td>string</td>
</tr>
</tbody>
</table>

**--direct-replication-host**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-replication-host</td>
<td>string</td>
</tr>
<tr>
<td>--direct-datasource-host</td>
<td>string</td>
</tr>
<tr>
<td>repl-direct-datasource-host</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options**
direct-datasource-host [356], direct-replication-host [356], repl-direct-datasource-host [356]

**Description**
Database server hostname

**--direct-replication-password**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-replication-password</td>
<td>string</td>
</tr>
<tr>
<td>--direct-datasource-password</td>
<td>string</td>
</tr>
<tr>
<td>repl-direct-datasource-password</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options**
direct-datasource-password [356], direct-replication-password [356], repl-direct-datasource-password [356]

**Description**
Password for datasource connection

**--direct-replication-port**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-replication-port</td>
<td>string</td>
</tr>
<tr>
<td>--direct-datasource-port</td>
<td>string</td>
</tr>
<tr>
<td>repl-direct-datasource-port</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options**
direct-datasource-port [356], direct-replication-port [356], repl-direct-datasource-port [356]

**Description**
Database server port

**--direct-replication-user**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--direct-replication-user</td>
<td>string</td>
</tr>
<tr>
<td>--direct-datasource-user</td>
<td>string</td>
</tr>
<tr>
<td>repl-direct-datasource-user</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options**
direct-datasource-user [356], direct-replication-user [356], repl-direct-datasource-user [356]

**Description**
Database login for Tungsten

**--disable-relay-logs**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--disable-relay-logs</td>
<td>string</td>
</tr>
<tr>
<td>repl-disable-relay-logs</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options**
disable-relay-logs [356], repl-disable-relay-logs [356]

**Description**
Disable the use of relay-logs?

**9.8.5. tpm Options**

**--enable-active-witnesses**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-active-witnesses</td>
<td>string</td>
</tr>
<tr>
<td>--active-witnesses</td>
<td>string</td>
</tr>
</tbody>
</table>

356
<table>
<thead>
<tr>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-witnesses</td>
<td>Enable active witness hosts</td>
<td>string</td>
</tr>
<tr>
<td>enable-active-witnesses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-connector-ssl</td>
<td>Enable SSL encryption of connector traffic to the database</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-heterogenous-master</td>
<td>Enable heterogenous operation for the master</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-heterogenous-service</td>
<td>Enable heterogenous operation</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-heterogenous-slave</td>
<td>Enable heterogenous operation for the slave</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-rmi-authentication</td>
<td>Enable RMI authentication for the services running on this host</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-rmi-ssl</td>
<td>Enable SSL encryption of RMI communication on this host</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-slave-thl-listener</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-connector-ssl</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--connector-ssl</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-rmi-authentication</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rmi-authentication</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-rmi-ssl</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rmi-ssl</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--enable-slave-thl-listener</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--repl-enable-slave-thl-listener</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

357
<table>
<thead>
<tr>
<th>Description</th>
<th>Should this service allow THL connections?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

`--enable-sudo-access`

<table>
<thead>
<tr>
<th>Option</th>
<th>--enable-sudo-access [358]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--root-command-prefix [358]</td>
</tr>
</tbody>
</table>

`Config File Options` enable-sudo-access [358], root-command-prefix [358]

<table>
<thead>
<tr>
<th>Description</th>
<th>Run root commands using sudo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

`--enable-thl-ssl`

<table>
<thead>
<tr>
<th>Option</th>
<th>--enable-thl-ssl [358]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-enable-thl-ssl [358], --thl-ssl [358]</td>
</tr>
</tbody>
</table>

`Config File Options` enable-thl-ssl [358], repl-enable-thl-ssl [358], thl-ssl [358]

<table>
<thead>
<tr>
<th>Description</th>
<th>Enable SSL encryption of THL communication for this service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### 9.8.6. TPM Options

`--host-name`

<table>
<thead>
<tr>
<th>Option</th>
<th>--host-name [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>host-name [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>DNS hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

`--hosts`

<table>
<thead>
<tr>
<th>Option</th>
<th>--hosts [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>hosts [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Limit the command to the hosts listed You must use the hostname as it appears in the configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

`--hub`

<table>
<thead>
<tr>
<th>Option</th>
<th>--hub [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Aliases</th>
<th>--dataservice-hub-host [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>dataservice-hub-host [358], hub [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>What is the hub host for this all-masters dataservice?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

`--hub-service`

<table>
<thead>
<tr>
<th>Option</th>
<th>--hub-service [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Aliases</th>
<th>--dataservice-hub-service [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>dataservice-hub-service [358], hub-service [358]</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>The data service to use for the hub of a star topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### 9.8.7. TPM Options

`--install`
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--install</strong></td>
<td>Install service start scripts</td>
<td>string</td>
</tr>
</tbody>
</table>

#### Config File Options
```
install [358]
```

**Description**
Install service start scripts

**Value Type**
string

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--install-directory</strong></td>
<td>Path to the directory where the active deployment will be installed. The configured directory will contain the software, THL and relay log information unless configured otherwise.</td>
<td>string</td>
</tr>
</tbody>
</table>

#### 9.8.8. J tpm Options

--java-connector-keystore-password

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-connector-keystore-password</strong></td>
<td>The password for unlocking the tungsten_connector_keystore.jks file in the security directory</td>
<td>string</td>
</tr>
</tbody>
</table>

#### Config File Options
```
java-connector-keystore-password [359]
```

**Description**
The password for unlocking the tungsten_connector_keystore.jks file in the security directory

**Value Type**
string

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-connector-keystore-path</strong></td>
<td>Local path to the Java Connector Keystore file.</td>
<td>filename</td>
</tr>
</tbody>
</table>

#### Config File Options
```
java-connector-keystore-path [359]
```

**Description**
Local path to the Java Connector Keystore file.

**Value Type**
filename

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-connector-truststore-password</strong></td>
<td>The password for unlocking the tungsten_connector_truststore.jks file in the security directory</td>
<td>string</td>
</tr>
</tbody>
</table>

#### Config File Options
```
java-connector-truststore-password [359]
```

**Description**
The password for unlocking the tungsten_connector_truststore.jks file in the security directory

**Value Type**
string

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-connector-truststore-path</strong></td>
<td>Local path to the Java Connector Truststore file.</td>
<td>filename</td>
</tr>
</tbody>
</table>

#### Config File Options
```
java-connector-truststore-path [359]
```

**Description**
Local path to the Java Connector Truststore file.

**Value Type**
filename

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-enable-concurrent-gc</strong></td>
<td>Replicator Java uses concurrent garbage collection</td>
<td>string</td>
</tr>
</tbody>
</table>

#### Config File Options
```
java-enable-concurrent-gc [359], repl-java-enable-concurrent-gc [359]
```

**Description**
Replicator Java uses concurrent garbage collection

**Value Type**
string

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--java-file-encoding</strong></td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

---

359
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--java-file-encoding</td>
<td>Java platform charset (esp. for heterogeneous replication)</td>
<td>string</td>
</tr>
<tr>
<td>--repl-java-file-encoding</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>java-file-encoding</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>repl-java-file-encoding</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>--java-jmxremote-access-path</td>
<td>Local path to the Java JMX Remote Access file.</td>
<td>filename</td>
</tr>
<tr>
<td>java-jmxremote-access-path</td>
<td></td>
<td>filename</td>
</tr>
<tr>
<td>--java-keystore-password</td>
<td>The password for unlocking the tungsten_keystore.jks file in the security directory</td>
<td>string</td>
</tr>
<tr>
<td>java-keystore-password</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>--java-keystore-path</td>
<td>Local path to the Java Keystore file.</td>
<td>filename</td>
</tr>
<tr>
<td>java-keystore-path</td>
<td></td>
<td>filename</td>
</tr>
<tr>
<td>--java-mem-size</td>
<td>Replicator Java heap memory size in Mb (min 128)</td>
<td>numeric</td>
</tr>
<tr>
<td>--repl-java-mem-size</td>
<td></td>
<td>numeric</td>
</tr>
<tr>
<td>java-mem-size</td>
<td></td>
<td>numeric</td>
</tr>
<tr>
<td>repl-java-mem-size</td>
<td></td>
<td>numeric</td>
</tr>
<tr>
<td>--java-passwordstore-path</td>
<td>Local path to the Java Password Store file.</td>
<td>filename</td>
</tr>
<tr>
<td>java-passwordstore-path</td>
<td></td>
<td>filename</td>
</tr>
<tr>
<td>--java-truststore-password</td>
<td>The password for unlocking the tungsten_truststore.jks file in the security directory</td>
<td>string</td>
</tr>
<tr>
<td>java-truststore-password</td>
<td></td>
<td>string</td>
</tr>
<tr>
<td>--java-truststore-path</td>
<td>Local path to the Java Truststore file.</td>
<td>filename</td>
</tr>
<tr>
<td>java-truststore-path</td>
<td></td>
<td>filename</td>
</tr>
</tbody>
</table>
### L tpm Options

--log

<table>
<thead>
<tr>
<th>Option</th>
<th>--log [361]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>log [361]</td>
</tr>
<tr>
<td>Description</td>
<td>Write all messages, visible and hidden, to this file. You may specify a filename, ‘pid’ or ‘timestamp’.</td>
</tr>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
</tbody>
</table>

--log-slave-updates

<table>
<thead>
<tr>
<th>Option</th>
<th>--log-slave-updates [361]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>log-slave-updates [361]</td>
</tr>
<tr>
<td>Description</td>
<td>Should slaves log updates to binlog</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### M tpm Options

--master

<table>
<thead>
<tr>
<th>Option</th>
<th>--master [361]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--dataservice-master-host [361], --masters [361], --relay [361]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>dataservice-master-host [361], master [361], masters [361], relay [361]</td>
</tr>
<tr>
<td>Description</td>
<td>Hostname of the master host within this service</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

The hostname of the master (extractor) within the current service. If the current host does not match this specification, then the deployment will by default be configured as a master/extractor.

--master-preferred-role

<table>
<thead>
<tr>
<th>Option</th>
<th>--master-preferred-role [361]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-master-preferred-role [361]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>master-preferred-role [361], repl-master-preferred-role [361]</td>
</tr>
<tr>
<td>Description</td>
<td>Preferred role for master THL when connecting as a slave</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>master</td>
</tr>
<tr>
<td></td>
<td>slave</td>
</tr>
</tbody>
</table>

--master-services

<table>
<thead>
<tr>
<th>Option</th>
<th>--master-services [361]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--dataservice-master-services [361]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>dataservice-master-services [361], master-services [361]</td>
</tr>
<tr>
<td>Description</td>
<td>Data service names that should be used on each master</td>
</tr>
</tbody>
</table>
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--master-thl-host</td>
<td>master-thl-host</td>
<td>Master THL Hostname</td>
<td>string</td>
</tr>
<tr>
<td>--master-thl-port</td>
<td>master-thl-port</td>
<td>Master THL Port</td>
<td>string</td>
</tr>
<tr>
<td>--members</td>
<td>dataservice-hosts, members</td>
<td>Hostnames for the dataservice members</td>
<td>string</td>
</tr>
<tr>
<td>--mgr-api</td>
<td>mgr-api</td>
<td>Enable the Manager API</td>
<td>string</td>
</tr>
<tr>
<td>--mgr-api-address</td>
<td>mgr-api-address</td>
<td>Address for the Manager API</td>
<td>string</td>
</tr>
<tr>
<td>--mgr-api-port</td>
<td>mgr-api-port</td>
<td>Port for the Manager API</td>
<td>string</td>
</tr>
<tr>
<td>--mgr-group-communication-port</td>
<td>mgr-group-communication-port</td>
<td>Port to use for manager group communication</td>
<td>string</td>
</tr>
<tr>
<td>--mgr-heap-threshold</td>
<td>mgr-heap-threshold</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Config File Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mgr-heap-threshold</code></td>
<td>Java memory usage (MB) that will force a Manager restart</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td><code>mgr-java-enable-concurrent-gc</code></td>
<td>Manager Java uses concurrent garbage collection</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td><code>mgr-java-mem-size</code></td>
<td>Manager Java heap memory size in Mb (min 128)</td>
<td>numeric</td>
<td></td>
</tr>
<tr>
<td><code>mgr-listen-interface</code></td>
<td>Listen interface to use for the manager</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td><code>mgr-policy-mode</code></td>
<td>Manager policy mode</td>
<td>string</td>
<td>automatic, maintenance, manual</td>
</tr>
<tr>
<td><code>mgr-rmi-port</code></td>
<td>Port to use for the manager RMI server</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td><code>mgr-rmi-remote-port</code></td>
<td>Port to use for calling the remote manager RMI server</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td><code>mgr-ro-slave</code></td>
<td>Make slaves read-only</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--mgr-vip-arp-path</td>
<td>Path to the arp binary</td>
</tr>
<tr>
<td>--mgr-vip-device</td>
<td>VIP network device</td>
</tr>
<tr>
<td>--mgr-vip-ifconfig-path</td>
<td>Path to the ifconfig binary</td>
</tr>
<tr>
<td>--mgr-wait-for-members</td>
<td>Wait for all datasources to be available before completing installation</td>
</tr>
<tr>
<td>--mysql-connectorj-path</td>
<td>Path to MySQL Connector/J</td>
</tr>
<tr>
<td>--mysql-driver</td>
<td>MySQL Driver Vendor</td>
</tr>
</tbody>
</table>

#### Value Types

- **string**
- **filename**

**Important**

As of Continuent Tungsten v4.0.0, the MySQL Connector/J prerequisite has been removed. The JDBC interface now uses the Drizzle driver by default.

**Note**

`tpm reverse` will display the parameter `--mysql-connectorj-path` as long as any `mysql-connector-java` file remains in `/opt/continuent/share/`

**Warning**

Do not use path `/opt/continuent/share/` inside the value for `--mysql-connectorj-path` or `tpm` will abort with an error.
### The `tpm` Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--mysql-enable-ansiquotes</code></td>
<td><code>mysql-enable-ansiquotes</code>, <code>repl-mysql-enable-ansiquotes</code></td>
<td>Enables ANSI_QUOTES mode for incoming events?</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-enable-enuestostring</code></td>
<td><code>mysql-enable-enuestostring</code>, <code>repl-mysql-enable-enuestostring</code></td>
<td>Enable a filter to convert ENUM values to strings</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-enable-noonlykeywords</code></td>
<td><code>mysql-enable-noonlykeywords</code>, <code>repl-mysql-enable-noonlykeywords</code></td>
<td>Enables a filter to translate <code>DELETE FROM ONLY</code> to <code>DELETE FROM</code> and <code>UPDATE ONLY</code> to <code>UPDATE</code>.</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-enable-settostring</code></td>
<td><code>mysql-enable-settostring</code>, <code>repl-mysql-enable-settostring</code></td>
<td>Enable a filter to convert SET types to strings</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-ro-slave</code></td>
<td><code>mysql-ro-slave</code>, <code>repl-mysql-ro-slave</code></td>
<td>Slaves are read-only?</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-server-id</code></td>
<td><code>mysql-server-id</code>, <code>repl-mysql-server-id</code></td>
<td>Explicitly set the MySQL server ID</td>
<td>string</td>
</tr>
<tr>
<td><code>--mysql-use-bytes-for-string</code></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setting this option explicitly sets the server-id information normally located in the MySQL configuration (`my.cnf`). This is useful in situations where there may be multiple MySQL installations and the server ID needs to be identified to prevent collisions when reading from the same master.
### 9.8.11. Ntpm Options

#### --native-slave-takeover

<table>
<thead>
<tr>
<th>Option</th>
<th>--native-slave-takeover [366]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-native-slave-takeover [366]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>native-slave-takeover [366], repl-native-slave-takeover [366]</td>
</tr>
<tr>
<td>Description</td>
<td>Takeover native replication</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

#### --no-deployment

<table>
<thead>
<tr>
<th>Option</th>
<th>--no-deployment [366]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>no-deployment [366]</td>
</tr>
<tr>
<td>Description</td>
<td>Skip deployment steps that create the install directory</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

#### --no-validation

<table>
<thead>
<tr>
<th>Option</th>
<th>--no-validation [366]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>no-validation [366]</td>
</tr>
<tr>
<td>Description</td>
<td>Skip validation checks that run on each host</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### 9.8.12. Ptpm Options

#### --pg-archive-timeout

<table>
<thead>
<tr>
<th>Option</th>
<th>--pg-archive-timeout [366]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-pg-archive-timeout [366]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>pg-archive-timeout [366], repl-pg-archive-timeout [366]</td>
</tr>
<tr>
<td>Description</td>
<td>Timeout for sending unfilled WAL buffers [data loss window]</td>
</tr>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
</tbody>
</table>

#### --pg-ctl

<table>
<thead>
<tr>
<th>Option</th>
<th>--pg-ctl [366]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-pg-ctl [366]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>pg-ctl [366], repl-pg-ctl [366]</td>
</tr>
<tr>
<td>Description</td>
<td>Path to the pg_ctl script</td>
</tr>
<tr>
<td>Value Type</td>
<td>filename</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
</tr>
</tbody>
</table>

**--pg-method**

<table>
<thead>
<tr>
<th>Option</th>
<th>--pg-method [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-pg-method [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>pg-method [367], repl-pg-method [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Postgres Replication method</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--pg-standby**

<table>
<thead>
<tr>
<th>Option</th>
<th>--pg-standby [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-pg-standby [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>pg-standby [367], repl-pg-standby [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Path to the pg_standby script</td>
</tr>
<tr>
<td>Value Type</td>
<td>filename</td>
</tr>
</tbody>
</table>

**--postgresql-dbname**

<table>
<thead>
<tr>
<th>Option</th>
<th>--postgresql-dbname [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-postgresql-dbname [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>postgresql-dbname [367], repl-postgresql-dbname [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Name of the database to replicate</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--postgresql-enable-mysql2pgddl**

<table>
<thead>
<tr>
<th>Option</th>
<th>--postgresql-enable-mysql2pgddl [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-postgresql-enable-mysql2pgddl [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>postgresql-enable-mysql2pgddl [367], repl-postgresql-enable-mysql2pgddl [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Enable MySQL to PostgreSQL DDL dialect converting filter placeholder</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>false</td>
</tr>
</tbody>
</table>

**--postgresql-slonik**

<table>
<thead>
<tr>
<th>Option</th>
<th>--postgresql-slonik [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-postgresql-slonik [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>postgresql-slonik [367], repl-postgresql-slonik [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Path to the slonik executable</td>
</tr>
<tr>
<td>Value Type</td>
<td>filename</td>
</tr>
</tbody>
</table>

**--postgresql-tables**

<table>
<thead>
<tr>
<th>Option</th>
<th>--postgresql-tables [367]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>--repl-postgresql-tables [367]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>postgresql-tables [367], repl-postgresql-tables [367]</td>
</tr>
<tr>
<td>Description</td>
<td>Tables to replicate in form: schema1.table1,schema2.table2,...</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

**--preferred-path**

| Option       | --preferred-path [367] |
## Config File Options: `preferred-path` [367]

<table>
<thead>
<tr>
<th>Description</th>
<th>Additional command path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>filename</td>
</tr>
</tbody>
</table>

Specifies one or more additional directories that will be added before the current `PATH` environment variable when external commands are run from within the backup environment. This affects all external tools used by Continuent Tungsten, including MySQL, Ruby, Java, and back-up/restore tools such as Percona Xtrabackup.

One or more paths can be specified by separating each directory with a colon. For example:

```sh
tpm ... --preferred-path=/usr/local/bin:/opt/bin:/opt/percona/bin
```

The `--preferred-path` information propagated to all remote servers within the `tpm` configuration. However, if the staging server is one of the servers to which you are deploying, the `PATH` must be manually updated.

### `--prefetch-enabled`

<table>
<thead>
<tr>
<th>Description</th>
<th>Should the replicator service be setup as a prefetch applier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### `--prefetch-max-time-ahead`

<table>
<thead>
<tr>
<th>Description</th>
<th>Maximum number of seconds that the prefetch applier can get in front of the standard applier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
</tbody>
</table>

### `--prefetch-min-time-ahead`

<table>
<thead>
<tr>
<th>Description</th>
<th>Minimum number of seconds that the prefetch applier must be in front of the standard applier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
</tbody>
</table>

### `--prefetch-schema`

<table>
<thead>
<tr>
<th>Description</th>
<th>Schema to watch for timing prefetch progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Default</td>
<td>tungsten</td>
</tr>
<tr>
<td>Valid Values</td>
<td>tungsten</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### `--prefetch-sleep-time`

<table>
<thead>
<tr>
<th>Description</th>
<th>How long to wait when the prefetch applier gets too far ahead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

### `--profile-script`

<table>
<thead>
<tr>
<th>Description</th>
<th>string</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Type</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Valid Values</td>
<td></td>
</tr>
</tbody>
</table>
The tpm Deployment Command

### Description
Append commands to include env.sh in this profile script

| Value Type | string |

---

### --protect-configuration-files

| Option | --protect-configuration-files [369] |
| Config File Options | protect-configuration-files [369] |

**Description**
When enabled, configuration files are protected to be only readable and updatable by the configured user

| Value Type | string |
| Valid Values | false |

When enabled (default), the configuration that contain user, password and other information are configured so that they are only readable by the configured user. For example:

```shell
ls -al /opt/continuent/tungsten/tungsten-replicator/conf/
```

When disabled, the files are readable by all users:

```shell
ll /opt/continuent/tungsten/tungsten-replicator/conf/
```

### 9.8.13. R tpm Options

---

### --relay-directory

| Option | --relay-directory [369] |
| Aliases | repl-relay-directory [369] |
| Config File Options | relay-directory [369], repl-relay-directory [369] |

**Description**
Directory for logs transferred from the master

| Value Type | string |
| Default | (home directory)/relay |
| Valid Values | (home directory)/relay |

---

### --relay-enabled

| Option | --relay-enabled [369] |
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>relay-enabled</td>
<td>Should the replicator service be setup as a relay master</td>
<td>string</td>
</tr>
</tbody>
</table>

--relay-source

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--relay-source</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

Aliases: --dataservice-relay-source [370], --master-dataservice [370]

Config File Options: dataservice-relay-source [370], master-dataservice [370], relay-source [370]

Description: Dataservice name to use as a relay source

Value Type: string

--replication-host

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--replication-host</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

Aliases: --datasource-host [370], --repl-datasource-host [370]

Config File Options: datasource-host [370], repl-datasource-host [370], replication-host [370]

Description: Hostname of the datasource

Value Type: string

Hostname of the datasource where the database is located. If the specified hostname matches the current host or member name, the database is assumed to be local. If the hostnames do not match, extraction is assumed to be via remote access. For MySQL hosts, this configures a remote replication slave (relay) connection.

--replication-password

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--replication-password</td>
<td>Database password</td>
<td>string</td>
</tr>
</tbody>
</table>

Aliases: --datasource-password [370], --repl-datasource-password [370]

Config File Options: datasource-password [370], repl-datasource-password [370], replication-password [370]

Description: Database password

Value Type: string

The password to be used when connecting to the database using the corresponding --replication-user [370].

--replication-port

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--replication-port</td>
<td></td>
<td>string</td>
</tr>
</tbody>
</table>

Aliases: --datasource-port [370], --repl-datasource-port [370]

Config File Options: datasource-port [370], repl-datasource-port [370], replication-port [370]

Description: Database network port

Value Type: string

Valid Values:
- 1521: Oracle Default
- 27017: Elasticsearch Default
- 27017: Kafka Default
- 27017: MongoDB Default
- 3306: MySQL Default
- 5432: PostgreSQL Default
- 5433: Vertica Default
- 5439: Redshift Default
- 8020: HDFS Default

The network port used to connect to the database server. The default port used depends on the database being configured.

--replication-user
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--replication-user</code></td>
<td>User for database connection</td>
</tr>
<tr>
<td><code>--datasource-user</code></td>
<td>User for database connection</td>
</tr>
<tr>
<td><code>--repl-datasource-user</code></td>
<td>User for database connection</td>
</tr>
<tr>
<td><code>--reset</code></td>
<td>Clear the current configuration before processing any arguments</td>
</tr>
<tr>
<td><code>--rmi-port</code></td>
<td>Replication RMI listen port</td>
</tr>
<tr>
<td><code>--rmi-user</code></td>
<td>The username for RMI authentication</td>
</tr>
<tr>
<td><code>--role</code></td>
<td>What is the replication role for this service?</td>
</tr>
<tr>
<td><code>--router-gateway-port</code></td>
<td>The router gateway port</td>
</tr>
<tr>
<td><code>--router-jmx-port</code></td>
<td></td>
</tr>
</tbody>
</table>

For databases that required authentication, the username to use when connecting to the database using the corresponding connection method (native, JDBC, etc.).

#### Option `--reset`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--reset</code></td>
<td>Clear the current configuration before processing any arguments</td>
</tr>
</tbody>
</table>

For staging configurations, deletes all pre-existing configuration information between updating with the new configuration values.

#### Option `--rmi-port`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--rmi-port</code></td>
<td>Replication RMI listen port</td>
</tr>
</tbody>
</table>

#### Option `--rmi-user`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--rmi-user</code></td>
<td>The username for RMI authentication</td>
</tr>
</tbody>
</table>

#### Option `--role`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--role</code></td>
<td>What is the replication role for this service?</td>
</tr>
</tbody>
</table>

#### Option `--router-gateway-port`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--router-gateway-port</code></td>
<td>The router gateway port</td>
</tr>
</tbody>
</table>

#### Option `--router-jmx-port`

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--router-jmx-port</code></td>
<td></td>
</tr>
</tbody>
</table>
9.8.14. `tpm` Options

### `--security-directory` Option

**Description:** Storage directory for the Java security/encryption files

**Value Type:** string

**Config File Options:**
- `security-directory` [372]

---

### `--service-alias` Option

**Description:** Replication alias of this dataservice

**Value Type:** string

**Valid Values:**
- local
- remote

**Config File Options:**
- `dataservice-service-alias` [372], `service-alias` [372]

---

### `--service-type` Option

**Description:** What is the replication service type?

**Value Type:** string

**Valid Values:**
- local
- remote

**Config File Options:**
- `repl-service-type` [372], `service-type` [372]

---

### `--skip-statemap` Option

**Description:** Do not copy the cluster-home/conf/statemap.properties from the previous install

**Value Type:** string

**Config File Options:**
- `skip-statemap` [372]

---

### `--slave-privileged-updates` Option

**Description:** Does login for slave update have superuser privileges

**Value Type:** string

**Config File Options:**
- `slave-privileged-updates` [372]

---

### `--slaves` Option

**Description:** What are the slaves for this dataservice?

**Value Type:** string

**Config File Options:**
- `dataservice-slaves` [372], `slaves` [372]

---

### `--start` Option

**Value Type:** string

---
The tpm Deployment Command

<table>
<thead>
<tr>
<th>Config File Options</th>
<th>start [372]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Start the services after configuration</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

--start-and-report

<table>
<thead>
<tr>
<th>Option</th>
<th>--start-and-report [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config File Options</td>
<td>start-and-report [373]</td>
</tr>
<tr>
<td>Description</td>
<td>Start the services and report out the status after configuration</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

--svc-allow-any-remote-service

<table>
<thead>
<tr>
<th>Option</th>
<th>--svc-allow-any-remote-service [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>repl-svc-allow-any-remote-service [373]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>repl-svc-allow-any-remote-service [373]</td>
</tr>
<tr>
<td>Description</td>
<td>Replicate from any service</td>
</tr>
<tr>
<td>Value Type</td>
<td>boolean</td>
</tr>
<tr>
<td>Valid Values</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>true</td>
</tr>
</tbody>
</table>

--svc-applier-block-commit-interval

<table>
<thead>
<tr>
<th>Option</th>
<th>--svc-applier-block-commit-interval [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>repl-svc-applier-block-commit-interval [373]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>repl-svc-applier-block-commit-interval [373]</td>
</tr>
<tr>
<td>Description</td>
<td>Minimum interval between commits</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
<tr>
<td>Valid Values</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>#d</td>
</tr>
<tr>
<td></td>
<td>#h</td>
</tr>
<tr>
<td></td>
<td>#m</td>
</tr>
<tr>
<td></td>
<td>#s</td>
</tr>
<tr>
<td></td>
<td>When batch service is not enabled</td>
</tr>
<tr>
<td></td>
<td>Number of days</td>
</tr>
<tr>
<td></td>
<td>Number of hours</td>
</tr>
<tr>
<td></td>
<td>Number of minutes</td>
</tr>
<tr>
<td></td>
<td>Number of seconds</td>
</tr>
</tbody>
</table>

--svc-applier-block-commit-size

<table>
<thead>
<tr>
<th>Option</th>
<th>--svc-applier-block-commit-size [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>repl-svc-applier-block-commit-size [373]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>repl-svc-applier-block-commit-size [373]</td>
</tr>
<tr>
<td>Description</td>
<td>Applier block commit size (min 1)</td>
</tr>
<tr>
<td>Value Type</td>
<td>numeric</td>
</tr>
</tbody>
</table>

--svc-applier-filters

<table>
<thead>
<tr>
<th>Option</th>
<th>--svc-applier-filters [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>repl-svc-applier-filters [373]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>repl-svc-applier-filters [373]</td>
</tr>
<tr>
<td>Description</td>
<td>Replication service applier filters</td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

--svc-extractor-filters

<table>
<thead>
<tr>
<th>Option</th>
<th>--svc-extractor-filters [373]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>repl-svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Config File Options</td>
<td>repl-svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Value Type</td>
<td>string</td>
</tr>
</tbody>
</table>

## tpm Deployment Command

### Aliases
- `--repl-svc-extractor-filters` [373]

### Config File Options
- `repl-svc-extractor-filters` [373], `svc-extractor-filters` [373]

### Description
Replication service extractor filters

### Value Type
String

### --svc-fail-on-zero-row-update

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--svc-fail-on-zero-row-update</code> [374]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--repl-svc-fail-on-zero-row-update</code> [374]</td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>repl-svc-fail-on-zero-row-update</code> [374], <code>svc-fail-on-zero-row-update</code> [374]</td>
</tr>
</tbody>
</table>

### Description
How should the replicator behave when a Row-Based Replication UPDATE does not affect any rows.

### Value Type
String

### Valid Values
- `disk`
- `memory`
- `none`

### --svc-parallelization-type

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--svc-parallelization-type</code> [374]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--repl-svc-parallelization-type</code> [374]</td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>repl-svc-parallelization-type</code> [374], <code>svc-parallelization-type</code> [374]</td>
</tr>
</tbody>
</table>

### Description
Method for implementing parallel apply

### Value Type
String

### Valid Values
- `disk`
- `memory`
- `none`

### --svc-reposition-on-source-id-change

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--svc-reposition-on-source-id-change</code> [374]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--repl-svc-reposition-on-source-id-change</code> [374]</td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>repl-svc-reposition-on-source-id-change</code> [374], <code>svc-reposition-on-source-id-change</code> [374]</td>
</tr>
</tbody>
</table>

### Description
The master will come ONLINE from the current position if the stored source_id does not match the value in the static properties

### Value Type
String

### --svc-shard-default-db

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--svc-shard-default-db</code> [374]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--repl-svc-shard-default-db</code> [374]</td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>repl-svc-shard-default-db</code> [374], <code>svc-shard-default-db</code> [374]</td>
</tr>
</tbody>
</table>

### Description
Mode for setting the shard ID from the default db

### Value Type
String

### Valid Values
- `relaxed`
- `stringent`

### --svc-table-engine

<table>
<thead>
<tr>
<th>Option</th>
<th><code>--svc-table-engine</code> [374]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td><code>--repl-svc-table-engine</code> [374]</td>
</tr>
<tr>
<td>Config File Options</td>
<td><code>repl-svc-table-engine</code> [374], <code>svc-table-engine</code> [374]</td>
</tr>
</tbody>
</table>

### Description
Replication service table engine

### Value Type
String

### Default
`innodb`

### Valid Values
- `innodb`
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--svc-thl-filters</code></td>
<td>string</td>
<td>Replication service THL filters</td>
</tr>
<tr>
<td><code>--target-dataservice</code></td>
<td>string</td>
<td>Dataservice to use to determine the value of host configuration</td>
</tr>
<tr>
<td><code>--temp-directory</code></td>
<td>string</td>
<td>Temporary Directory</td>
</tr>
<tr>
<td><code>--template-file-help</code></td>
<td>string</td>
<td>Display the keys that may be used in configuration template files</td>
</tr>
<tr>
<td><code>--thl-directory</code></td>
<td>string</td>
<td>Replicator log directory</td>
</tr>
<tr>
<td><code>--thl-do-checksum</code></td>
<td>string</td>
<td>Execute checksum operations on THL log files</td>
</tr>
</tbody>
</table>

### 9.8.15. Tpm Options

#### `--target-dataservice`

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--target-dataservice</code></td>
<td>string</td>
<td>Dataservice to use to determine the value of host configuration</td>
</tr>
</tbody>
</table>

#### `--temp-directory`

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--temp-directory</code></td>
<td>string</td>
<td>Temporary Directory</td>
</tr>
</tbody>
</table>

#### `--template-file-help`

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--template-file-help</code></td>
<td>string</td>
<td>Display the keys that may be used in configuration template files</td>
</tr>
</tbody>
</table>

#### `--thl-directory`

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--thl-directory</code></td>
<td>string</td>
<td>Replicator log directory</td>
</tr>
</tbody>
</table>

#### `--thl-do-checksum`

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--thl-do-checksum</code></td>
<td>string</td>
<td>Execute checksum operations on THL log files</td>
</tr>
</tbody>
</table>

#### `--thl-interface`
### The `tpm` Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Value Type</th>
<th>Config File Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--thl-interface</code></td>
<td>Listen interface to use for THL operations</td>
<td>string</td>
<td>repl-thl-interface, thl-interface</td>
</tr>
<tr>
<td><code>--repl-thl-interface</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--thl-log-connection-timeout</code></td>
<td>Number of seconds to wait for a connection to the THL log</td>
<td>numeric</td>
<td>repl-thl-log-connection-timeout, thl-log-connection-timeout</td>
</tr>
<tr>
<td><code>--repl-thl-log-connection-timeout</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--repl-thl-log-file-size</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--thl-log-fsync</code></td>
<td>Fsync THL records on commit. More reliable operation but adds latency to replication when using low-performance storage</td>
<td>string</td>
<td>repl-thl-log-fsync, thl-log-fsync</td>
</tr>
<tr>
<td><code>--repl-thl-log-fsync</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--thl-log-retention</code></td>
<td>How long do you want to keep THL files.</td>
<td>string</td>
<td>repl-thl-log-retention, thl-log-retention</td>
</tr>
<tr>
<td><code>--repl-thl-log-retention</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--thl-port</code></td>
<td>Port to use for THL Operations</td>
<td>string</td>
<td>repl-thl-port, thl-port</td>
</tr>
<tr>
<td><code>--repl-thl-port</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>--thl-protocol</code></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Valid Values**

- `#d`: Number of days
- `#h`: Number of hours
- `#m`: Number of minutes
- `#s`: Number of seconds
- `7d`: 7 days
### The tpm Deployment Command

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--thl-protocol</td>
<td>string</td>
</tr>
<tr>
<td>repl-thl-protocol</td>
<td>string</td>
</tr>
</tbody>
</table>

**Aliases:**
- repl-thl-protocol
- thl-protocol

**Config File Options:**
- repl-thl-protocol
- thl-protocol

**Description:** Protocol to use for THL communication with this service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--dataservice-topology</td>
<td>string</td>
</tr>
</tbody>
</table>

**Aliases:**
- dataservice-topology
- topology

**Config File Options:**
- dataservice-topology
- topology

**Description:** Replication topology for the dataservice. Valid values are star, cluster-slave, master-slave, fan-in, clustered, cluster-alias, all-masters, direct.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--user</td>
<td>string</td>
</tr>
</tbody>
</table>

**Config File Options:**
- user

**Description:** System User.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vertica-dbname</td>
<td>string</td>
</tr>
</tbody>
</table>

**Aliases:**
- repl-vertica-dbname

**Config File Options:**
- repl-vertica-dbname
- vertica-dbname

**Description:** Name of the database to replicate into.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>--witnesses</td>
<td>string</td>
</tr>
</tbody>
</table>

**Aliases:**
- dataservice-witnesses

**Config File Options:**
- dataservice-witnesses
- witnesses

**Description:** Witness hosts for the dataservice.
Chapter 10. Replication Filters

Filtering operates by applying the filter within one, or more, of the stages configured within the replicator. Stages are the individual steps that occur within a pipeline, that take information from a source (such as MySQL binary log) and write that information to an internal queue, the transaction history log, or apply it to a database. Where the filters are applied ultimately affect how the information is stores, used, or represented to the next stage or pipeline in the system.

For example, a filter that removed out all the tables from a specific database would have different effects depending on the stage it was applied. If the filter was applied on the master before writing the information into the THL, then no slave could ever access the table data, because the information would never be stored into the THL to be transferred to the slaves. However, if the filter was applied on the slave, then some slaves could replicate the table and database information, while other slaves could choose to ignore them. The filtering process also has an impact on other elements of the system. For example, filtering on the master may reduce network overhead, albeit at a reduction in the flexibility of the data transferred.

In a standard replicator configuration with MySQL, the following stages are configured in the master, as shown in Figure 10.1, "Filters: Pipeline Stages on Masters".

Figure 10.1. Filters: Pipeline Stages on Masters

```
binlog-to-q stage

Dataserver

Extract  Filter  Apply

Memory Q

Extract  Filter  Apply

THL
```

Where:
- **binlog-to-q Stage**
  The *binlog-to-q* stage reads information from the MySQL binary log and stores the information within an in-memory queue.

- **q-to-thl Stage**
  The in-memory queue is written out to the THL file on disk.

Within the slave, the stages configured by default are shown in Figure 10.2, "Filters: Pipeline Stages on Slaves".
Replication Filters

Figure 10.2. Filters: Pipeline Stages on Slaves

- **remote-to-thl stage**
  Remote THL information is read from a master datasource and written to a local file on disk.

- **thl-to-q stage**
  The THL information is read from the file on disk and stored in an in-memory queue.

- **q-to-dbms stage**
  The data from the in-memory queue is written to the target database.

Filters can be applied during any configured stage, and where the filter is applied alters the content and availability of the information. The staging and filtering mechanism can also be used to apply multiple filters to the data, altering content when it is read and when it is applied.

Where more than one filter is configured for a pipeline, each filter is executed in the order it appears in the configuration. For example, within the following fragment:

```plaintext
replicator.stage.binlog-to-q.filters=settostring,enumtostring,pkey,colnames
```

*settostring* is executed first, followed by *enumtostring*, *pkey* and *colnames*.

For certain filter combinations this order can be significant. Some filters rely on the information provided by earlier filters.

### 10.1. Enabling/Disabling Filters

A number of standard filter configurations are created and defined by default within the static properties file for the Tungsten Replicator configuration.

Filters can be enabled through `tpm` to update the filter configuration

- `--repl-svc-extractor-filters` [373]
  Apply the filter during the extraction stage, i.e. when the information is extracted from the binary log and written to the internal queue (binlog-to-q).

- `--repl-svc-thl-filters` [375]
  Apply the filter between the internal queue and when the transactions are written to the THL on the master (q-to-thl).

- `--repl-svc-remote-filters`
  Apply the filter between reading from the remote THL server and writing to the local THL files on the slave (remote-to-thl).

- `--repl-svc-applier-filters` [373]
  Apply the filter between reading from the internal queue and applying to the destination database (q-to-dbms).

Properties and options for an individual filter can be specified by setting the corresponding property value on the `tpm` command-line.

For example, to ignore a database schema on a slave, the `replicate` filter can be enabled, and the `replicator.filter.replicate.ignore` specifies the name of the schemas to be ignored. To ignore the schema `contacts`:

```plaintext
replicator.filter.replicate.ignore=contacts
```
Replication Filters

A bad filter configuration will not stop the replicator from starting, but the replicator will be placed into the OFFLINE state.

To disable a previously enabled filter, empty the filter specification and (optionally) unset the corresponding property or properties. For example:

```
shell> /tools/tpm update alpha --hosts=host1,host2,host3
   --repl-svc-applier-filters=replicate
   --remove-property=replicator.filter.replicate.ignore
```

Multiple filters can be applied on any stage, and the filters will be processes and called within the order defined within the configuration. For example, the following configuration:

```
shell> /tools/tpm update alpha --hosts=host1,host2,host3
   --repl-svc-applier-filters=enumtostring,settostring,pkey
   --remove-property=replicator.filter.replicate.ignore
```

The filters are called in order:

1. enumtostring
2. settostring
3. pkey

The order and sequence can be important if operations are being performed on the data and they are relied on later in the stage. For example, if data is being filtered by a value that exists in a SET column within the source data, the settostring filter must be defined before the data is filtered, otherwise the actual string value will not be identified.

**Warning**

In some cases, the filter order and sequence can also introduce errors. For example, when using the pkey filter and the optimizeupdates filters together, pkey may remove KEY information from the THL before optimizeupdates attempts to optimize the ROW event, causing the filter to raise a failure condition.

The currently active filters can be determined by using the `trepctl status -name stages` command:

```
shell> trepctl status -name stages
Processing status command (stages)...  
...  
   NAME             VALUE        
   .....             .....        
   applier.class    : com.continuent.tungsten.replicator.applier.MySQLDrizzleApplier
   applier.name     : dbms
   blockCommitRowCount: 10
   committedMinSeqno : 3600
   committedMaxSeqno : 3600
   extractor.class   : com.continuent.tungsten.replicator.thl.THLParallelQueueExtractor
   extractor.name    : parallel-q-extractor
   filter.0.class    : com.continuent.tungsten.replicator.filter.MySQLSessionSupportFilter
   filter.0.name     : mysqlsessions
   filter.1.class    : com.continuent.tungsten.replicator.filter.PrimaryKeyFilter
   filter.1.name     : pkey
   filter.2.name     : bidiSlave
   name              : q-to-dbms
   processedMinSeqno : 1
   taskCount          : 5
Finished status command (stages)...  
```

The above output is from a standard slave replication installation showing the default filters enabled. The filter order can be determined by the number against each filter definition.

### 10.2. Enabling Additional Filters

The Continuent Tungsten configuration includes a number of filter configurations by default. However, not all filters are given a default configuration, and for some filters, multiple configurations may be needed to achieve more complex filtering requirements. Internally, filter configuration is defined through a property file that defines the filter name and corresponding parameters.

For example, the `rename` configuration is defined as follows:

```java
replicator.filter.rename=com.continuent.tungsten.replicator.filter.RenameFilter
replicator.filter.rename.definitionsFile=${replicator.home.dir}/samples/extensions/java/rename.csv
```

The first line creates a new filter configuration using the corresponding Java class. In this case, the filter is named `rename`, as defined by the string `replicator.filter.rename`.  

380
Replication Filters

Configuration parameters for the filter are defined as values after the filter name. In this example, `definitionsFile` is the name of the property examined by the class to set the CSV file where the rename definitions are located.

To create an entirely new filter based on an existing filter class, a new property should be created with the new filter definition in the configuration file.

Additional properties from this base should then be used. For example, to create a second rename filter definition called `custom`:

```
replicator.filter.rename.custom=com.continuent.tungsten.replicator.filter.RenameFilter
replicator.filter.rename.custom.definitionsFile=/samples/extensions/java/renamecustom.csv
```

The filter can be enabled against the desired stage using the filter name `custom`:

```
shell> ./tools/tpm configure \
   --repl-svc-applier-filters=custom
```

### 10.3. Filter Status

To determine which filters are currently being applied within a replicator, use the `trepctl status -name stages` command. This outputs a list of the current stages and their configuration. For example:

```
shell> trepctl status -name stages
Processing status command (stages)...  
NAME                VALUE       
----                -----       
applier.class      : com.continuent.tungsten.replicator.thl.THLStoreApplier
applier.name       : thl-applier
blockCommitRowCount: 1
committedMinSeqno  : 15
extractor.class    : com.continuent.tungsten.replicator.thl.RemoteTHLExtractor
extractor.name     : thl-remote
name               : remote-to-thl
processedMinSeqno  : -1
taskCount          : 1
NAME                VALUE       
----                -----       
applier.class      : com.continuent.tungsten.replicator.thl.THLParallelQueueApplier
applier.name       : parallel-q-applier
blockCommitRowCount: 10
committedMinSeqno  : 15
extractor.class    : com.continuent.tungsten.replicator.thl.THLStoreExtractor
extractor.name     : thl-extractor
name               : thl-to-q
processedMinSeqno  : -1
taskCount          : 1
NAME                VALUE       
----                -----       
applier.class      : com.continuent.tungsten.replicator.applier.MySQLDrizzleApplier
applier.name       : dbms
blockCommitRowCount: 10
committedMinSeqno  : 15
extractor.class    : com.continuent.tungsten.replicator.thl.THLParallelQueueExtractor
extractor.name     : parallel-q-extractor
filter.0.class     : com.continuent.tungsten.replicator.filter.TimeDelayFilter
filter.0.name      : delay
filter.1.class     : com.continuent.tungsten.replicator.filter.MySQLSessionSupportFilter
filter.1.name      : mysqlsessions
filter.2.class     : com.continuent.tungsten.replicator.filter.PrimaryKeyFilter
filter.2.name      : pkey
name               : q-to-dbs
processedMinSeqno  : -1
taskCount          : 5
Finished status command (stages)...
```

In the output, the filters applied to the applier stage are shown in the last block of output. Filters are listed in the order in which they appear within the configuration.

For information about the filter operation and any modifications or changes made, check the `trepsvc.log` log file.

### 10.4. Filter Reference

The different filter types configured and available within the replicate are designed to provide a number of different functionality and operations. Since the information exchanged through the THL system contains a copy of the statement or the row data that is being updated, the filters allow schemas, table and column names, as well as actual data to be converted at the stage in which they are applied.

Filters are identified according to the underlying Java class that defines their operation. For different filters, further configuration and naming is applied according to the templates used when Continuent Tungsten is installed through `tpm`.
Tungsten Replicator also comes with a number of JavaScript filters that can either be used directly, or that can be modified and adapted to suit individual requirements. The majority of these filter scripts are located in `tungsten-replicator/samples/extensions/javascript`, more advanced filter scripts are located in `tungsten-replicator/samples/scripts/javascript-advanced`.

For the purposes of classification, the different filters have been categorised according to their main purpose:

- **Auditing**
  
  These filters provide methods for tracking database updates alongside the original table data. For example, in a financial database, the actual data has to be updated in the corresponding tables, but the individual changes that lead to that update must also be logged individually.

- **Content**
  
  Content filters modify or update the content of the transaction events. These may alter information, for the purposes of interoperability (such as updating enumerated or integer values to their string equivalents), or remove or filter columns, tables, and entire schemas.

- **Logging**
  
  Logging filters record information about the transactions into the standard replicator log, either for auditing or debugging purposes.

- **Optimization**
  
  The optimization filters are designed to simplify and optimize statements and row updates to improve the speed at which those updates can be applied to the destination dataserver.

- **Transformation**
  
  Transformation filters rename or reformat schemas and tables according to a set of rules. For example, multiple schemas can be merged to a single schema, or tables and column names can be updated.

- **Validation**
  
  Provide validation or consistency checking of either the data or the replication process.

- **Miscellaneous**
  
  Other filters that cannot be allocated to one of the existing filter classes.

The list of filters and their basic description are provided in the table below.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BidiRemoteSlaveFilter</td>
<td>Content</td>
<td>Suppresses events that originated on the local service (required for correct slave operation)</td>
</tr>
<tr>
<td>BuildAuditTable</td>
<td>Auditing</td>
<td>Builds an audit table of changes for specified schemas and tables</td>
</tr>
<tr>
<td>BuildIndexTable</td>
<td>Transformation</td>
<td>Merges multiple schemas into a single schema</td>
</tr>
<tr>
<td>CaseMappingFilter</td>
<td>Transformation</td>
<td>Transforms schema, table and column names to upper or lower case</td>
</tr>
<tr>
<td>CDCMetadataFilter</td>
<td>Auditing</td>
<td>Records change data capture for transactions to a separate change table (auditing)</td>
</tr>
<tr>
<td>ColumnNameFilter</td>
<td>Validation</td>
<td>Adds column name information to row-based replication events</td>
</tr>
<tr>
<td>ConsistencyCheckFilter</td>
<td>Validation</td>
<td>Adds consistency checking to events</td>
</tr>
<tr>
<td>DatabaseTransformFilter</td>
<td>Transformation</td>
<td>Transforms database or table names using regular expressions</td>
</tr>
<tr>
<td>DummyFilter</td>
<td>Miscellaneous</td>
<td>Allows for confirmation of filter configuration</td>
</tr>
<tr>
<td>EnumToStringFilter</td>
<td>Content</td>
<td>Updates enumerated values to their string-based equivalent</td>
</tr>
<tr>
<td>EventMetadataFilter</td>
<td>Content</td>
<td>Filters events based on metadata; used by default within sharding and multi-master topologies</td>
</tr>
<tr>
<td>HeartbeatFilter</td>
<td>Validation</td>
<td>Detects heartbeat events on masters or slaves</td>
</tr>
<tr>
<td>JavaScriptFilter</td>
<td>Miscellaneous</td>
<td>Enables filtering through custom JavaScripts</td>
</tr>
<tr>
<td>LoggingFilter</td>
<td>Logging</td>
<td>Logs filtered events through the standard replicator logging mechanism</td>
</tr>
<tr>
<td>MySQLSessionSupportFilter</td>
<td>Content</td>
<td>Filters transactions for session specific temporary tables and variables</td>
</tr>
<tr>
<td>OptimizeUpdatesFilter</td>
<td>Optimization</td>
<td>Optimizes update statements where the current and updated value are the same</td>
</tr>
</tbody>
</table>
Replication Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryKeyFilter</td>
<td>Optimization</td>
<td>Used during row-based replication to optimize updates using primary keys</td>
</tr>
<tr>
<td>PrintEventFilter</td>
<td>Logging</td>
<td>Outputs transaction event information to the replication logging system</td>
</tr>
<tr>
<td>RenameFilter</td>
<td>Transformation</td>
<td>Advanced schema, table and column-based renaming</td>
</tr>
<tr>
<td>ReplicateColumns-Filter</td>
<td>Content</td>
<td>Removes selected columns from row-based transaction data</td>
</tr>
<tr>
<td>ReplicateFilter</td>
<td>Content</td>
<td>Selects or ignores specification schemas and/or databases</td>
</tr>
<tr>
<td>SetToStringFilter</td>
<td>Content</td>
<td>Converts integer values in <code>set</code> datatypes to string values</td>
</tr>
<tr>
<td>ShardFilter</td>
<td></td>
<td>Used to enforce database schema sharding between specific masters</td>
</tr>
<tr>
<td>TimeDelayFilter</td>
<td>Miscellaneous</td>
<td>Delays transactions until a specific point in time has passed</td>
</tr>
</tbody>
</table>

In the following reference sections:

- Pre-configured filter name is the filter name that can be used against a stage without additional configuration.
- Property prefix is the prefix string for the filter to be used when assigning property values.
- Classname is the Java class name of the filter.
- Parameter is the name of the filter parameter can be set as a property within the configuration.
- Data compatibility indicates whether the filter is compatible with row-based events, statement-based events, or both.

### 10.4.1. ansiquotes.js Filter

The `ansiquotes` filter operates by inserting an SQL mode change to `ANSI_QUOTES` into the replication stream before a statement is executed, and returning to an empty SQL mode.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>ansiquotes</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/ansiquotes.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.ansiquotes</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>

This changes a statement such as:

`INSERT INTO notepad VALUES ('message',0);`

To:

```
SET sql_mode='ANSI_QUOTES';
INSERT INTO notepad VALUES ('message',0);
SET sql_mode='';
```

This is achieved within the JavaScript by processing the incoming events and adding a new statement before the first `DBMSData` object in each event:

```javascript
query = "SET sql_mode='ANSI_QUOTES';
newStatement = new com.continuent.tungsten.replicator.dbms.StatementData(
    query,
    null,
    null
);
data.add(0, newStatement);
```

A corresponding statement is appended to the end of the event:

```javascript
query = "SET sql_mode='';
newStatement = new com.continuent.tungsten.replicator.dbms.StatementData(
    query,
    null,
    null
);
data.add(data.size(), newStatement);
```
10.4.2. BidiRemoteSlave [BidiSlave] Filter

The BidiRemoteSlaveFilter is used by Tungsten Replicator to prevent statements that originated from this service (i.e. where data was extracted), being re-applied to the database. This is a requirement for replication to prevent data that may be transferred between hosts being re-applied, particularly in multi-master and other bi-directional replication deployments.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>bidiSlave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property prefix</td>
<td>replicator.filter.bidiSlave</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>localServiceName</td>
<td>string</td>
<td><code>${local.service.name}</code></td>
<td>Local service name of the service that reads the binary log</td>
</tr>
<tr>
<td>allowBidiUnsafe</td>
<td>boolean</td>
<td>false</td>
<td>If true, allows statements that may be unsafe for bi-directional replication</td>
</tr>
<tr>
<td>allowAnyRemoteService</td>
<td>boolean</td>
<td>false</td>
<td>If true, allows statements from any remote service, not just the current service</td>
</tr>
</tbody>
</table>

The filter works by comparing the server ID of the THL event that was created when the data was extracted against the server ID of the current server.

When deploying through the **tpm** service the filter is automatically enabled for remote slaves. For complex deployments, particularly those with bi-directional replication (including multi-master), the **allowBidiUnsafe** parameter may need to be enabled to allow certain statements to be re-executed.

10.4.3. breadcrumbs.js Filter

The breadcrumbs filter records regular ‘breadcrumb’ points into a MySQL table for systems that do not have global transaction IDs. This can be useful if recovery needs to be made to a specific point. The example also shows how metadata information for a given event can be updated based on the information from a table.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>ansiquotes</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/breadcrumbs.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.breadcrumbs</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_id</td>
<td>numeric</td>
<td>[none]</td>
<td>MySQL server ID of the current host</td>
</tr>
</tbody>
</table>

To use the filter:

1. A table is created and populated with one more rows on the master server. For example:

```sql
CREATE TABLE tungsten_svc1.breadcrumbs (
    `id` int(11) NOT NULL PRIMARY KEY,
    `counter` int(11) DEFAULT NULL,
    `last_update` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP) ENGINE=InnoDB;
INSERT INTO tungsten_svc1.breadcrumbs(id, counter) values(@@server_id, 1);
```

2. Now set an event to update the table regularly. For example, within MySQL an event can be created for this purpose:

```sql
CREATE EVENT breadcrumbs_refresh
ON SCHEDULE EVERY 5 SECOND
DO
    UPDATE tungsten_svc1.breadcrumbs SET counter=counter+1;
SET GLOBAL event_scheduler = ON;
```
The filter will extract the value of the counter each time it sees to the table, and then mark each transaction with a particular server ID with the counter value plus an offset. For convenience we assume row replication is enabled.

If you need to failover to another server that has different logs, you can figure out the restart point by looking in the THL for the breadcrumb metadata on the last transaction. Use this to search the binary logs on the new server for the correct restart point.

The filter itself work in two stages, and operates because the JavaScript instance is persistent as long as the Replicator is running. This means that data extracted during replication stays in memory and can be applied to later transactions. Hence the breadcrumb ID and offset information can be identified and used on each call to the filter function.

The first part of the filter event identifies the breadcrumb table and extracts the identified breadcrumb counter:

```java
if (table.compareToIgnoreCase("breadcrumbs") == 0)
{
    columnValues = oneRowChange.getColumnValues();
    for (row = 0; row < columnValues.size(); row++)
    {
        values = columnValues.get(row);
        server_id_value = values.get(0);
        if (server_id == null || server_id == server_id_value.getValue())
        {
            counter_value = values.get(1);
            breadcrumb_counter = counter_value.getValue();
            breadcrumb_offset = 0;
        }
    }
}
```

The second part updates the event metadata using the extracted breadcrumb information:

```java
topLevelEvent = event.getDBMSEvent();
if (topLevelEvent != null)
{
    xact_server_id = topLevelEvent.getMetadataOptionValue("mysql_server_id");
    if (server_id == xact_server_id)
    {
        topLevelEvent.setMetaDataOption("breadcrumb_counter", breadcrumb_counter);
        topLevelEvent.setMetaDataOption("breadcrumb_offset", breadcrumb_offset);
    }
}
```

To calculate the offset (i.e. the number of events since the last breadcrumb value was extracted), the filter determines if the event was the last fragment processed, and updates the offset counter:

```java
if (event.getLastFrag())
{
    breadcrumb_offset = breadcrumb_offset + 1;
}
```

### 10.4.4. BuildAuditTable Filter

The BuildAuditTable filter populates a table with all the changes to a database so that the information can be tracked for auditing purposes.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>Not defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.BuildAuditTable</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.bidiSlave</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
</tr>
<tr>
<td>targetTableName</td>
<td>string</td>
</tr>
</tbody>
</table>

### 10.4.5. BuildIndexTable Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>buildindextable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.BuildIndexTable</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.buildIndexTable</td>
</tr>
</tbody>
</table>
10.4.6. CaseMapping (CaseTransform) Filter

Pre-configured filter name: casetransform
Classname: com.continuent.tungsten.replicator.filter.CaseMappingFilter
Property prefix: replicator.filter.casetransform

Parameters:
- to_upper_case (boolean): default true, converts object names to upper case; if false, converts them to lower case

10.4.7. CDCMetadata (CustomCDC) Filter

Pre-configured filter name: customcdc
Classname: com.continuent.tungsten.replicator.filter.CDCMetadataFilter
Property prefix: replicator.filter.customcdc

Parameters:
- cdcColumnsAtFront (boolean): default false, if true, the additional CDC columns are added at the start of the table row. If false, they are added to the end of the table row.
- schemaNameSuffix (string): specifies the schema name suffix. If defined, the tables are created in a schema matching schema name of the source transaction with the schema suffix appended.
- tableNameSuffix (string): specifies the table name suffix for the CDC tables. If the schema suffix is not specified, this allows CDC tables to be created within the same schema.
- toSingleSchema (string): creates and writes CDC data within a single schema.
- sequenceBeginning (numeric): default 1, sets the sequence number of the CDC data. The sequence is used to identify individual changesets in the CDC.

10.4.8. ColumnName Filter

The ColumnNameFilter loads the table specification information for tables and adds this information to the THL data for information extracted using row-base replication.

Pre-configured filter name: colnames
Classname: com.continuent.tungsten.replicator.filter.ColumnNameFilter
Replication Filters

<table>
<thead>
<tr>
<th>Property prefix</th>
<th>replicator.filter.colnames</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>Ipnm Option compatibility</td>
<td>--svc-extractor-filters [573]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Keeps Cached Data</td>
<td>Yes</td>
</tr>
<tr>
<td>Cached Refreshed When?</td>
<td>Emptied when going OFFLINE; Updated when ALTER statement seen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>string</td>
<td>$(replicator.global.extract.db.user)</td>
<td>The username for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>$(replicator.global.extract.db.password)</td>
<td>The password for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>jdbc:mysql:thin://${replicator.global.extract.db.host}:${replicator.global.extract.db.port}/${replicator.schema}?createDB=true</td>
<td>JDBC URL of the database connection to use for looking up column definitions</td>
</tr>
</tbody>
</table>

Note

This filter is designed to be used for testing and with heterogeneous replication where the field name information can be used to construct and build target data structures.

The filter is required for the correct operation of heterogeneous replication, for example when replicating to MongoDB. The filter works by using the replicator username and password to access the underlying database and obtain the table definitions. The table definition information is cached within the replication during operation to improve performance.

When extracting data from the binary log using row-based replication, the column names for each row of changed data are added to the THL.

Enabling this filter changes the THL data from the following example, shown without the column names:

```
SEQ# = 27 / FRAG# = 0 (last frag)
- TIME = 2013-08-01 18:29:38.0
- EPOCH# = 11
- EVENTID = mysql-bin.000012:0000000000004369:0
- SOURCEID = host31
- METADATA = [mysql_server_id=1;dbms_type=mysql;service=alpha;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
- OPTIONS = [foreign_key_checks = 1, unique_checks = 1]
- SQL(0) =
  - ACTION = INSERT
  - SCHEMA = test
  - TABLE = sales
  - ROW = 0
    - COL(1: ) = 1
    - COL(2: ) = 23
    - COL(3: ) = 45
    - COL(4: ) = 45000.00
```

To a version where the column names are included as part of the THL record:

```
SEQ# = 43 / FRAG# = 0 (last frag)
- TIME = 2013-08-01 18:34:18.0
- EPOCH# = 28
- EVENTID = mysql-bin.000012:0000000000006814:0
- SOURCEID = host31
- METADATA = [mysql_server_id=1;dbms_type=mysql;service=alpha;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
- OPTIONS = [foreign_key_checks = 1, unique_checks = 1]
- SQL(0) =
  - ACTION = INSERT
  - SCHEMA = test
  - TABLE = sales
  - ROW = 0
    - COL(1: id) = 2
    - COL(2: country) = 23
    - COL(3: city) = 45
    - COL(4: value) = 45000.00
```

When the row-based data is applied to a non-MySQL database the column name information is used by the applier to specify the column, or they key when the column and value is used as a key/value pair in a document-based store.
10.4.9. ConsistencyCheck Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>Not defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.consistency.ConsistencyCheckFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>Not defined</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Not defined</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td>(none)</td>
</tr>
</tbody>
</table>

10.4.10. DatabaseTransform (dbtransform) Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dbtransform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.DatabaseTransformFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dbtransform</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>replicator.filter.dbtransform</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transformTables</td>
<td>boolean</td>
<td>false</td>
<td>If set to true, forces the rename transformations to operate on tables, not databases</td>
</tr>
<tr>
<td>from_regex1</td>
<td>string</td>
<td>foo</td>
<td>The search regular expression to use when renaming databases or tables (group 1); corresponds to to_regex1</td>
</tr>
<tr>
<td>to_regex1</td>
<td>string</td>
<td>bar</td>
<td>The replace regular expression to use when renaming databases or tables (group 1); corresponds to from_regex1</td>
</tr>
<tr>
<td>from_regex2</td>
<td>string</td>
<td></td>
<td>The search regular expression to use when renaming databases or tables (group 2); corresponds to to_regex2</td>
</tr>
<tr>
<td>to_regex2</td>
<td>string</td>
<td></td>
<td>The replace regular expression to use when renaming databases or tables (group 2); corresponds to from_regex2</td>
</tr>
<tr>
<td>from_regex3</td>
<td>string</td>
<td></td>
<td>The search regular expression to use when renaming databases or tables (group 3); corresponds to to_regex3</td>
</tr>
<tr>
<td>to_regex3</td>
<td>string</td>
<td></td>
<td>The replace regular expression to use when renaming databases or tables (group 3); corresponds to from_regex3</td>
</tr>
</tbody>
</table>

10.4.11. dbrename.js Filter

The `dbrename` JavaScript filter renames database (schemas) using two parameters from the properties file, the `dbsource` and `dbtarget`. Each event is then processed, and the statement or row based schema information is updated to `dbtarget` when the `dbsource` schema is identified.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dbrename</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dbrename.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dbrename</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>IPM Option compatibility</td>
<td>--svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>
Replication Filters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dbsource</code></td>
<td>string</td>
<td>(none)</td>
<td>Source table name (database/table to be renamed)</td>
</tr>
<tr>
<td><code>dbtarget</code></td>
<td>string</td>
<td>(none)</td>
<td>New database/table name</td>
</tr>
</tbody>
</table>

To configure the filter you would add the following to your properties:

```
replicator.filter.dbsource=com.continuent.tungsten.replicator.filter.JavaScriptFilter
dbtarget=com.continuent.tungsten.replicator.filter.JavaScriptFilter
```

The operation of the filter is straightforward, because the schema name is exposed and settable within the statement and row change objects:

```javascript
function filter(event)
{
    sourceName = filterProperties.getString("dbsource");
    targetName = filterProperties.getString("dbtarget");

    data = event.getData();
    for(i=0;i<data.size();i++)
    {
        d = data.get(i);
        if(d instanceof com.continuent.tungsten.replicator.dbms.StatementData)
        {
            if(d.getDefaultSchema() != null &&
                d.getDefaultSchema().compareTo(sourceName)==0)
            {
                d.setDefaultSchema(targetName);
            }
        } else if(d instanceof com.continuent.tungsten.replicator.dbms.RowChangeData)
        {
            rowChanges = data.get(i).getRowChanges();
            for(j=0;j<rowChanges.size();j++)
            {
                oneRowChange = rowChanges.get(j);
                if(oneRowChange.getSchemaName().compareTo(sourceName)==0)
                {
                    oneRowChange.setSchemaName(targetName);
                }
            }
        }
    }
}
```

10.4.12. **dbselector.js Filter**

Filtering only a single database schema can be useful when you want to extract a single schema for external processing, or for sharding information across multiple replication targets. The `dbselector` filter deletes all statement and row changes, except those for the selected table. To configure, the `db` parameter to the filter configuration specifies the schema to be replicated.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dbselector</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dbselector.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dbselector</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-thl, q-to-dbms</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

Within the filter, statement changes look for the schema in the `StatementData` object and remove it from the array:

```javascript
if (d instanceof com.continuent.tungsten.replicator.dbms.StatementData)
{
}
```
```java
if(d.getDefaultSchema().compareTo(db)!=0)
{
    data.remove(i);
    i--;    
}
```

Because entries are being removed from the list of statements, the iterator used to process each item must be explicitly decremented by 1 to reset the counter back to the new position.

Similarly, when looking at row changes in the `RowChangeData`:

```java
else if(d instanceof com.continuent.tungsten.replicator.dbms.RowChangeData)
{
    rowChanges = data.get(i).getRowChanges();
    for(j=0;j<rowChanges.size();j++)
    {
        oneRowChange = rowChanges.get(j);
        if(oneRowChange.getSchemaName().compareTo(db)!=0)
        {
            rowChanges.remove(j);
            j--;    
        }
    }
}
```

### 10.4.13. `dbupper.js` Filter

The `dbupper` filter changes the case of the schema name for all schemas to uppercase. The schema information is easily identified in the statement and row based information, and therefore easy to update.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dbupper</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dbupper.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dbupper</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>from</code></td>
<td>string</td>
<td>[none]</td>
<td>Database name to be converted to uppercase</td>
</tr>
</tbody>
</table>

For example, within statement data:

```java
from = d.getDefaultSchema();
if (from != null) {
    to = from.toUpperCase();
    d.setDefaultSchema(to);
}
```

### 10.4.14. `dropcolumn.js` Filter

The `dropcolumn` filter enables columns in the THL to be dropped. This can be useful when replicating Personal Identification Information, such as email addresses, phone number, personal identification numbers and others are within the THL but need to be filtered out on the slave.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dropcolumn</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dropcolumn.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dropcolumn</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>definitionsFile</code></td>
<td>Filename</td>
<td>~/dropcolumn.json</td>
<td>Location of the definitions file for dropping columns</td>
</tr>
</tbody>
</table>
Replication Filters

The filter is available by default as `dropcolumn`, and the filter is configured through a JSON file that defines the list of columns to be dropped. The filter relies on the `colnames` filter being enabled.

To enable the filter:

```
shell> tpm update --svc-extractor-filters=colnames,dropcolumn \n   --property=replicator.filter.dropcolumn.definitionsFile=/opt/continuent/share/dropcolumn.json
```

A sample configuration file is provided in `/opt/continuent/share/dropcolumn.json`. The format of the file is a JSON array of schema/table/column specifications:

```
[
  {
    "schema": "vip",
    "table": "clients",
    "columns": [
      "personal_code",
      "birth_date",
      "email"
    ]
  },
  ...
]
```

Where:

- `schema` specifies the name of the schema on which to apply the filtering. If `*` is given, all schemas are matched.
- `table` specifies the name of the table on which to apply the filtering. If `*` is given, all tables are matched.
- `columns` is an array of column names to be matched.

For example:

```
[
  {
    "schema": "vip",
    "table": "clients",
    "columns": [
      "personal_code",
      "birth_date",
      "email"
    ]
  },
  ...
]
```

Filters the columns `email`, `birth_date`, and `personal_code` within the `clients` table in the `vip` schema.

To filter the `telephone` column in any table and any schema:

```
[
  {
    "schema": "*",
    "table": "*",
    "columns": [
      "telephone"
    ]
  }
]
```

Care should be taken when dropping columns on the slave and master when the column order is different or when the names of the column differ:

- If the column order is same, even if `dropcolumn.js` is used, leave the default setting for the property `replicator.applier.dbms.getColumnMetadataFromDB=true`.
- If the column order is different on the master and slave, set `replicator.applier.dbms.getColumnMetadataFromDB=false`
- If slave's column names are different, regardless of differences in the order, use the default property setting `replicator.applier.dbms.getColumnMetadataFromDB=true`

10.4.15. `dropcomments.js` Filter

The `dropcomments` filter removes comments from statements within the event data.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th><code>dropcomments</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td><code>tungsten-replicator/samples/extensions/javascript/dropcomments.js</code></td>
</tr>
</tbody>
</table>
Replication Filters

<table>
<thead>
<tr>
<th>Property prefix</th>
<th>replicator.filter.dropcomments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>option</td>
<td>string</td>
<td>[none]</td>
<td>Name of the metadata field to be dropped</td>
</tr>
</tbody>
</table>

Row changes do not have comments, so the filter only has to change the statement information, which is achieved by using a regular expression:

```java
sqlOriginal = d.getQuery();
sqlNew = sqlOriginal.replaceAll("/*\*(?:.|
\r\n)*?\*/", "");
d.setQuery(sqlNew);
```

To handle the case where the statement could only be a comment, the statement is removed:

```java
if(sqlNew.trim().length()==0)
{
    data.remove(i);
    i--;
}
```

#### 10.4.16. dropmetadata.js Filter

All events within the replication stream contain metadata about each event. This information can be individually processed and manipulated. The `dropmetadata` filter removes specific metadata from each event, configured through the `option` parameter to the filter.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dropmetadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dropmetadata.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.ansiquotes</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>option</td>
<td>string</td>
<td>[none]</td>
<td>Name of the metadata field to be dropped</td>
</tr>
</tbody>
</table>

Metadata information can be processed at the event top-level:

```java
metaData = event.getDBMSEvent().getMetadata();
for(n = 0; n < metaData.size(); m++)
{
    option = metaData.get(n);
    if(option.getOptionName().compareTo(optionName)==0)
    {
        metaData.remove(n);
        break;
    }
}
```

#### 10.4.17. dropstatementdata.js Filter

Within certain replication deployments, enforcing that only row-based information is replicated is important to ensure that the row data is replicated properly. For example, when replicating to databases that do not accept statements, these events must be filtered out.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dropstatementdata</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/dropstatementdata.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dropstatementdata</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>option</td>
<td>string</td>
<td>[none]</td>
<td>Name of the metadata field to be dropped</td>
</tr>
</tbody>
</table>
Replication Filters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data = event.getData();</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for(i = 0; i &lt; data.size(); i++)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d = data.get(i);</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>if(d instanceof com.continuent.tungsten.replicator.dbms.StatementData)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data.remove(i);</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i--;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.4.18. Dummy Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>dummy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.DummyFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.dummy</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>tpm</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td>(none)</td>
</tr>
</tbody>
</table>

10.4.19. EnumToString Filter

The EnumToString filter translates ENUM datatypes within MySQL tables into their string equivalent within the THL.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>enumtostring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.EnumToStringFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.enumtostring</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Parameters</td>
<td>user</td>
</tr>
<tr>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>url</td>
</tr>
</tbody>
</table>

The EnumToString filter should be used with heterogeneous replication to ensure that the data is represented as the string value, not the internal numerical representation.

In the THL output below, the table has a ENUM column, country:

```
mysql> describe salesadv;
+----------+--------------------------------------+------+-----+---------+----------------+
| Field    | Type                                 | Null | Key | Default | Extra          |
+----------+--------------------------------------+------+-----+---------+----------------+
| id       | int(11)                              | NO   | PRI | NULL    | auto_increment |
| country  | enum('US','UK','France','Australia') | YES  | PRI | NULL    |                |
| city     | int(11)                              | YES  | NULL |         |                |
| salesman | set('Alan','Zachary')                | YES  | NULL |         |                |
| value    | decimal(10,2)                        | YES  | NULL |         |                |
```
When extracted in the THL, the representation uses the internal value (for example, 1 for the first enumerated value). This can be seen in the THL output below.

For the `country` column, the corresponding value in the THL is 1. With the `EnumToString` filter enabled, the value is expanded to the corresponding string value:

The information is critical when applying the data to a dataserver that is not aware of the table definition, such as when replicating to Oracle or MongoDB.

The examples here also show the Section 10.4.34, “SetToString Filter” and Section 10.4.8, “ColumnName Filter” filters.

### 10.4.20. EventMetadata Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>eventmetadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.EventMetadataFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.eventmetadata</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Ipmm Option compatibility</td>
<td>[none]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
</tbody>
</table>

### 10.4.21. `foreignkeychecks.js` Filter

The `foreignkeychecks` filter switches off foreign key checks for statements using the following statements:

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>foreignkeychecks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATE TABLE</td>
<td></td>
</tr>
<tr>
<td>DROP TABLE</td>
<td></td>
</tr>
<tr>
<td>ALTER TABLE</td>
<td></td>
</tr>
<tr>
<td>RENAME TABLE</td>
<td></td>
</tr>
</tbody>
</table>
### JavaScript Filter File

<table>
<thead>
<tr>
<th>Property prefix</th>
<th>tungsten-replicator/samples/extensions/javascript/foreignkeychecks.js</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage compatibility</td>
<td>replicator.filter.foreignkeychecks</td>
</tr>
<tr>
<td>tpmm Option compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>--svc-extractor-filters [373], --svc-applier-filters [373]</td>
</tr>
</tbody>
</table>

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

The process checks the statement data and parses the content of the SQL statement by first trimming any extraneous space, and then converting the statement to upper case:

```java
upCaseQuery = d.getQuery().trim().toUpperCase();
```

Then comparing the string for the corresponding statement types:

```java
if(upCaseQuery.startsWith("CREATE TABLE") ||
upCaseQuery.startsWith("DROP TABLE") ||
upCaseQuery.startsWith("ALTER TABLE") ||
upCaseQuery.startsWith("RENAME TABLE")
```

If they match, a new statement is inserted into the event that disables foreign key checks:

```java
query = "SET foreign_key_checks=0";
newStatement = new com.continuent.tungsten.replicator.dbms.StatementData(
    d.getDefaultSchema(),
    null,
    query
);
data.add(0, newStatement);
i++;
```

The use of `a` in the `add()` method inserts the new statement before the others within the current event.

#### 10.4.22. Heartbeat Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>[none]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.HeartbeatFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>[none]</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td>tpmm Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heartbeatInterval</td>
<td>numeric</td>
<td>3000</td>
<td>Interval in milliseconds when a heartbeat event is inserted into the THL</td>
</tr>
</tbody>
</table>

#### 10.4.23. insertsonly.js Filter

The `insertsonly` filter filters events to only include ROW-based events using `INSERT`.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>insertsonly</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/insertonly.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.insertonly</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>q-to-dbms</td>
</tr>
<tr>
<td>tpmm Option compatibility</td>
<td>--svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
Replication Filters

This is achieved by examining each row and removing row changes that do not match the `INSERT` action type:

```java
if(oneRowChange.getAction()!="INSERT")
{
  rowChanges.remove(j);
  j--;
}
```

### 10.4.24. Logging Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>logger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.LoggingFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.logger</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td>[none]</td>
</tr>
</tbody>
</table>

### 10.4.25. MySQLSessionSupport (mysqlsessions) Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>mysqlsessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.MySQLSessionSupportFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.mysqlsession</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td>[none]</td>
</tr>
</tbody>
</table>

### 10.4.26. NetworkClient Filter

The `NetworkClientFilter` processes data in selected columns

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>networkclient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.NetworkClientFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.networkclient</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Any</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-thl-filters [375], --svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
</tr>
<tr>
<td><code>definitionsFile</code></td>
<td>pathname</td>
</tr>
<tr>
<td><code>serverPort</code></td>
<td>number</td>
</tr>
<tr>
<td><code>timeout</code></td>
<td>number</td>
</tr>
</tbody>
</table>

The network filter operates by sending field data, as defined in the corresponding filter configuration file, out to a network server that processes the information and sends it back to be re-introduced in place of the original field data. This can be used to translate and reformat information during the replication scheme.
The filter operation works as follows:

- All filtered data will be sent to a single network server, at the configured port.
- A single network server can be used to provide multiple transformations.
- The JSON configuration file for the filter supports multiple types and multiple column definitions.
- The protocol used by the network filter must be followed to effectively process the information. A failure in the network server or communication will cause the replicator to raise an error and replication to go offline.
- The network server must be running before the replicator is started. If the network server cannot be found, replication will go offline.

Correct operation requires building a suitable network filter using the defined protocol, and creating the JSON configuration file. A sample filter is provided for reference.

10.4.26.1. Network Client Configuration

The format of the configuration file defines the translation operation to be requested from the network client, in addition to the schema, table and column name. The format for the file is JSON, with the top-level hash defining the operation, and an array of field selections for each field that should be processed accordingly. For example:

```json
{
    "String_to_HEX_v1": [
        {
            "table": "hextable",
            "schema": "hexdb",
            "columns": ["hexcol"]
        }
    ]
}
```

The operation in this case is `String_to_HEX_v1`; this will be sent to the network server as part of the request. The column definition follows.

To send multiple columns from different tables to the same translation:

```json
{
    "String_to_HEX_v1": [
        {
            "table": "hextable",
            "schema": "hexdb",
            "columns": ["hexcol"]
        },
        {
            "table": "hexagon",
            "schema": "sourcetext",
            "columns": ["itemtext"]
        }
    ]
}
```

Alternatively, to configure different operations for the same two tables:

```json
{
    "String_to_HEX_v1": [
        {
            "table": "hextable",
            "schema": "hexdb",
            "columns": ["hexcol"]
        }
    ],
    "HEX_to_String_v1": [
        {
            "table": "hexagon",
            "schema": "sourcetext",
            "columns": ["itemtext"]
        }
    ]
}
```
10.4.26.2. Network Filter Protocol

The network filter protocol has been designed to be both lightweight and binary data compatible, as it is designed to work with data that may be heavily encoded, binary, or compressed in nature.

The protocol operates through a combined JSON and optional binary payload structure that communicates the information. The JSON defines the communication type and metadata, while the binary payload contains the raw or translated information.

The filter communicates with the network server using the following packet types:

- **prepare**
  
  The *prepare* message is called when the filter goes online, and is designed to initialize the connection to the network server and confirm the supported filter types and operation. The format of the connection message is:

  ```json
  {'payload': -1,
   'type': 'prepare',
   'service': 'firstrep',
   'protocol': 'v0_9'}
  ```

  Where:

  - **protocol**
    
    The protocol version.
  
  - **service**
    
    The name of the replicator service that called the filter.
  
  - **type**
    
    The message type.
  
  - **payload**
    
    The size of the payload; a value of -1 indicates that there is no payload.

  The format of the response should be a JSON object and payload with the list of supported filter types in the payload section. The payload immediately follows the JSON, with the size of the list defined within the `payload` field of the returned JSON object:

  ```json
  {'payload': 22,
   'type': 'acknowledged',
   'protocol': 'v0_9',
   'service': 'firstrep',
   'return': 0
}
  ```

  Where:

  - **protocol**
    
    The protocol version.
  
  - **service**
    
    The name of the replicator service that called the filter.
  
  - **type**
    
    The message type; when acknowledging the original prepare request it should be `acknowledge`.
  
  - **return**
    
    The return value. A value of 0 [zero] indicates no faults. Any true value indicates there was an issue.
  
  - **payload**
    
    The length of the appended payload information in bytes. This is used by the filter to identify how much additional data to read after the JSON object has been read.
The payload should be a comma-separated list of the supported transformation types within the network server.

- **filter**

  The *filter* message type is sent by Tungsten Replicator for each value from the replication stream that needs to be filtered and translated in some way. The format of the request is a JSON object with a trailing block of data, the payload, that contains the information to be filtered. For example:

  ```json
  {
    "schema" : "hexdb",
    "transformation" : "String_to_HEX_v1",
    "service" : "firststep",
    "type" : "filter",
    "payload" : 22,
    "row" : 0,
    "column" : "hexcol",
    "table" : "hextable",
    "seqno" : 145196,
    "fragments" : 1,
    "protocol" : "v0_9",
    "fragment" : 1
  }
  
  Where:

  - **protocol**
    The protocol version.

  - **service**
    The service name the requested the filter.

  - **type**
    The message type, in this case, *filter*.

  - **row**
    The row of the source information from the THL that is being filtered.

  - **schema**
    The schema of the source information from the THL that is being filtered.

  - **table**
    The table of the source information from the THL that is being filtered.

  - **column**
    The column of the source information from the THL that is being filtered.

  - **seqno**
    The sequence number of the event from the THL that is being filtered.

  - **fragments**
    The number of fragments in the THL that is being filtered.

  - **fragment**
    The fragment number within the THL that is being filtered. The fragments may be sent individually and sequentially to the network server, so they may need to be retrieved, merged, and reconstituted depending on the nature of the source data and the filter being applied.

  - **transformation**
    The transformation to be performed on the supplied payload data. A single network server can support multiple transformations, so this information is provided to perform the corrupt operation. The actual transformation to be performed is taken from the JSON configuration file for the filter.

  - **payload**
    "48656c6c6f20576f726c64"
Replication Filters

The length, in bytes, of the payload data that will immediately follow the JSON filter request.

The payload that immediately follows the JSON block is the data from the column that should be processed by the network filter.

The response package should contain a copy of the supplied information from the requested filter, with the payload size updated to the size of the returned information, the message type changed to filtered, and the payload containing the translated data. For example:

```json
{
  "transformation": "String_to_HEX_v1",
  "fragments": 1,
  "type": "filtered",
  "fragment": 1,
  "return": 0,
  "seqno": 145198,
  "table": "hextable",
  "service": "firstrep",
  "protocol": "v0.9",
  "schema": "hexdb",
  "payload": 8,
  "column": "hexcol",
  "row": 0
}
```

10.4.26.3. Sample Network Client

The following sample network server script is written in Perl, and is designed to translate packed hex strings (two-hex characters per byte) from their hex representation into their character representation.

```perl
#!/usr/bin/perl
use Switch;
use IO::Socket::INET;
use JSON qw( decode_json encode_json);
use Data::Dumper;
# auto-flush on socket
$| = 1;
my $serverName = "Perl_BLOB_to_String_v1";
while(1)
{
  # creating a listening socket
  my $socket = new IO::Socket::INET (
    LocalHost => '0.0.0.0',
    LocalPort => '3112',
    Proto => 'tcp',
    Listen => 5,
    Reuse => 1);
  die "Cannot create socket $!
"
  unless $socket;
  print "********
Server waiting for client connection on port 3112
******


# Waiting for a new client connection
my $client_socket = $socket->accept();
# Get information about a newly connected client
my $client_address = $client_socket->peerhost();
my $client_port = $client_socket->peerport();
print "Connection from $client_address:$client_port
";
my $data = "";
while( $data = $client_socket->getline())
{
  # Read up to 1024 characters from the connected client
  chomp($data);
  print "\n(n)Received: <$data>\n";
  # Decode the JSON part
  my $msg = decode_json($data);
  # Extract payload
  my $payload = undef;
  if ($msg->{payload} > 0)
  {
    print STDERR "Reading $msg->{payload} bytes\n";
    $client_socket->read($payload,$msg->{payload});
    print "Payload: <$payload>\n";
  }
}
```

Replication Filters

```plaintext
switch( $msg->{'type'} )
{
  case "prepare"
  {
    print STDERR "Received prepare request\n";
    # Send acknowledged message
    my $out = '{ "protocol": "v0_9", "type": "acknowledged", ' .
                ' "return": 0, "service": "" . $msg->{'service'} . "", "payload": "", ' .
                ' length($serverName) . "", "\n": $serverName; ' .
    print $client_socket "$out";
    print "Sent: <$out>\n";
    print STDERR "Sent acknowledge request\n";
  }
  case "release"
  {
    # Send acknowledged message
    my $out = '{ "protocol": "v0_9", "type": "acknowledged", ' .
                ' "return": 0, "service": "" . $msg->{'service'} . "", "payload": 0}; ' .
    print $client_socket "$out\n";
    print "Sent: <$out>\n";
  }
  case "filter"
  {
    # Send filtered message
    print STDERR "Sending filtered payload\n";
    my $filtered = "FILTERED";
    my $out = <<END;
    {
      "protocol": "v0_9",
      "type": "filtered",
      "transformation": "$msg->{'transformation'}",
      "return": 0,
      "service": "$msg->{'service'}",
      "seqno": $msg->{'seqno'},
      "row": "$msg->{'row'}",
      "schema": "$msg->{'schema'}",
      "table": "$msg->{'table'}",
      "column": "$msg->{'column'}",
      "fragment": 1,
      "fragments": 1,
      "payload": \"{(length($filtered))}\"
    }
    END
    $out =~ s/\n//g;
    print "About to send: <$out>\n";
    $client_socket->send("$out\n" . $filtered);
    print("Response sent\n");
  }
}

print("End of loop, hoping for next packet\n");
}
# Notify client that we're done writing
shutdown($client_socket, 1);
$socket->close();
}
```

10.4.27. nocreatedbifnotexists.js Filter

The nocreatedbifnotexists filter removes statements that start with:

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>nocreatedbifnotexists</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/nocreatedbifnotexists.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.nocreatedbifnotexists</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>q-to-dbms</td>
</tr>
<tr>
<td>ipm Option compatibility</td>
<td>--svc-applier-filters [373]</td>
</tr>
</tbody>
</table>
### Replication Filters

#### Data compatibility
- Any event

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>

This can be useful in heterogeneous replication where Tungsten Replicator specific databases need to be removed from the replication stream.

The filter works in two phases. The first phase creates a global variable within the `prepare()` function that defines the string to be examined:

```java
function prepare()
{
    beginning = "CREATE DATABASE IF NOT EXISTS";
}
```

Row based changes can be ignored, but for statement based events, the SQL is examine and the statement removed if the SQL starts with the text in the `beginning` variable:

```java
sql = d.getQuery();
if(sql.startsWith(beginning))
{
    data.remove(i);
    i--;
}
```

### 10.4.28. OptimizeUpdates Filter

The `optimizeupdates` filter works with row-based events to simplify the update statement and remove columns/values that have not changed. This reduces the workload and row data exchanged between replicators.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>optimizeupdates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.OptimizeUpdatesFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.optimizeupdates</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>PPM Option compatibility</td>
<td>None</td>
</tr>
</tbody>
</table>

The filter operates by removing column values for keys in the update statement that do not change. For example, when replicating the row event from the statement:

```
mysql> update testopt set msg = 'String1', string = 'String3' where id = 1;
```

Generates the following THL event data:

```
- SQL(0) =
  - ACTION = UPDATE
  - SCHEMA = test
  - TABLE = testopt
  - ROW = 0
    - COL(1: id) = 1
    - COL(2: msg) = String1
    - COL(3: string) = String3
    - KEY(1: id) = 1
```

Column 1 [id] in this case is automatically implied by the KEY entry required for the update.

With the `optimizeupdates` filter enabled, the data in the THL is simplified to:

```
- SQL(0) =
  - ACTION = UPDATE
  - SCHEMA = test
  - TABLE = testopt
  - ROW = 0
    - COL(2: msg) = String1
    - COL(3: string) = String4
    - KEY(1: id) = 1
```
Replication Filters

In tables where there are multiple keys the stored THL information can be reduced further.

**Warning**

The filter works by comparing the value of each KEY and COL entry in the THL and determining whether the value has changed or not. If the number of keys and columns do not match then the filter will fail with the following error message:

```
Caused by: java.lang.Exception: Column and key count is different in this event! Cannot filter
```

This may be due to a filter earlier within the filter configuration that has optimized or simplified the data. For example, the `pkey` filter removes KEY entries from the THL that are not primary keys, or `dropcolumn` which drops column data.

### 10.4.29. PrimaryKey Filter

The PrimaryKey adds primary key information to row-based replication data. This is required by heterogeneous environments to ensure that the primary key is identified when updating or deleting tables. Without this information, the primary key to use, for example, as the document ID in a document store such as MongoDB, is generated dynamically. In addition, without this filter in place, when performing update or delete operations a full table scan is performed on the target dataserver to determine the record that must be updated.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>pkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.PrimaryKeyFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.pkey</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>ipm Option compatibility</td>
<td>--repl-svc-extractor-filters[373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td>Keeps Cached Data</td>
<td>Yes</td>
</tr>
<tr>
<td>Cached Refreshed When?</td>
<td>Emptied when going OFFLINE; Updated when ALTER statement seen</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>string</td>
<td>$(replicator.global.extract.db.user)</td>
<td>The username for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>$(replicator.global.extract.db.password)</td>
<td>The password for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>jdbc:mysql:thin://$(replicator.global.extract.db.host):$(replicator.global.extract.db.port)/((replicator.schema)\createDb=true)</td>
<td>JDBC URL of the database connection to use for looking up column definitions</td>
</tr>
<tr>
<td>addPkeyToInsert</td>
<td>boolean</td>
<td>false</td>
<td>If set to true, primary keys are added to INSERT operations. This setting is required for batch loading</td>
</tr>
<tr>
<td>addColumnsToDeletes</td>
<td>boolean</td>
<td>false</td>
<td>If set to true, full column metadata is added to DELETE operations. This setting is required for batch loading</td>
</tr>
</tbody>
</table>

#### Note

This filter is designed to be used for testing and with heterogeneous replication where the field name information can be used to construct and build target data structures.

For example, in the following THL fragment, the key information includes data for all columns, which the is the default behavior for UPDATE and DELETE Operations.

```
SEQ# = 142 / FRAG# = 0 (last frag)
- TIME = 2013-08-01 19:31:04.0
- EPOCH# = 122
- EVENTID = mysql-bin.000012:0000000000022187:0
- SOURCEID = host1
- METADATA = [mysql_server_id=1;dbms_type=mysql;service=alpha;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
  OPTIONS = [foreign_key_checks = 1, unique_checks = 1]
- SQL(0) =
  - ACTION = UPDATE
  - SCHEMA = test
  - TABLE = salesadv
```
### Replication Filters

When the **PrimaryKey** is enabled, the key information has been optimized to only contain the actual primary keys are added to the row-based THL record:

```
SEQ# = 142 / FRAG# = 0 (last frag)
- TIME = 2013-08-01 19:31:04.0
- EPOCH# = 122
- EVENTID = mysql-bin.000012:0000000000022187:0
- SOURCEID = host31
- METADATA = [mysql_server_id=1;dbms_type=mysql;service=alpha;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
- OPTIONS = [foreign_key_checks = 1, unique_checks = 1]
  - SQL(0) =
    - ACTION = UPDATE
    - SCHEMA = test
    - TABLE = salesadv
    - ROW# = 0
    - COL(1: id) = 2
    - COL(2: country) = 1
    - COL(3: city) = 8374
    - COL(4: salesman) = 1
    - COL(5: value) = 89000.00
    - KEY(1: id) = 2
    - KEY(2: country) = 1
    - KEY(3: city) = 8374
    - KEY(4: salesman) = 1
    - KEY(5: value) = 89000.00
```

The final line shows the addition of the primary key `id` added to THL event.

**Important**

The filter determines primary key information by examining the DDL for the table, and keeping that information in an internal cache. If the DDL for a table is not known, or an `ALTER TABLE` statement is identified, the cache information is updated before the THL is then modified with the primary key information.

In the situation where you enable the filter, but have not create primary key information on the tables, it is possible that creating or adding other index types [such as `UNIQUE`] on a table, could lead to the incorrect primary key information being updated in the THL, particularly if there are active transactions taking place during and/or immediately after the `ALTER` statement.

The safest way to perform an index update in case remains the same as for any safe DDL update:

- Put the replicator offline
- Change the DDL for the table or tables
- Put the replicator online

The two options, `addPkeyToInsert` and `addColumnsToDeletes` add the primary key information to `INSERT` and `DELETE` operations respectively. In a heterogeneous environment, these options should be enabled to prevent full-table scans during update and deletes.

### 10.4.30. PrintEvent Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>printevent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.PrintEventFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.printevent</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td>Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td>[none]</td>
</tr>
</tbody>
</table>
10.4.31. Rename Filter

The rename filter enables schemas to be renamed at the database, table and column levels, and for complex combinations of these renaming operations. Configuration is through a CSV file that defines the rename parameters. A single CSV file can contain multiple rename definitions. The rename operations occur only on ROW based events.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>rename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.RenameFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.rename</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>replicator.filter.rename</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>replicator.filter.rename</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events; Schema names of Statement events in 2.2.1 and later.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>definitionsFile</td>
<td>string</td>
<td>/{replicator.home.dir}/samples/extensions/java/rename.csv</td>
<td>Location of the CSV file that contains the rename definitions.</td>
</tr>
</tbody>
</table>

The CSV file is only read when an explicit reconfigure operation is triggered. If the file is changed, a configure operation [using tpm update] must be initiated to force reconfiguration.

To enable using the default CSV file:

```
shells> ./tools/tpm update alpha --svc-applier-filters=rename
```

The CSV consists of multiple lines, one line for each rename specification. Comments are supposed using the # character.

The format of each line of the CSV is:

```
originalSchema,originalTable,originalColumn,newSchema,newTable,newColumn
```

Where:

- `originalSchema`, `originalTable`, `originalColumn` define the original schema, table and column.
- `newSchema`, `newTable`, `newColumn` define the new schema, table and column for the corresponding original specification.

Definition can either be:

- Explicit schema, table or column name
- * character, which indicates that all entries should match.

For example, the specification:

```
*,chicago,*,newyork,-
```

Would rename the table `chicago` in every database schema to `newyork`. The schema and column names are not modified.

The specification:

```
*,chicago,destination,-,-,source
```

Would match all schemas, but update the column `destination` in the table `chicago` to the column name `source`, without changing the schema or table name.

Processing of the individual rules is executed in a specific order to allow for complex matching and application of the rename changes.

- Rules are case sensitive.
- Schema names are looked up in the following order:
  1. `schema.table` (explicit schema/table)
2. \texttt{schema.*} [explicit schema, wildcard table]

- Table names are looked up in the following order:
  1. \texttt{schema.table} [explicit schema/table]
  2. \texttt{.*.table} [wildcard schema, explicit table]

- Column names are looked up in the following order:
  1. \texttt{schema.table} [explicit schema/table]
  2. \texttt{schema.*} [explicit schema, wildcard table]
  3. \texttt{.*.table} [wildcard schema, explicit table]
  4. \texttt{.*.*} [wildcard schema, wildcard table]

- Rename operations match the first specification according to the above rules, and only one matching rule is executed.

10.4.31.1. Rename Filter Examples

When processing multiple entries that would match the same definition, the above ordering rules are applied. For example, the definition:

\begin{verbatim}
asia,*,*,america,-,-
asia,shanghai,*,europe,-,-
\end{verbatim}

Would rename \texttt{asia.shanghai} to \texttt{europe.shanghai}, while renaming all other tables in the schema \texttt{asia} to the schema \texttt{america}. This is because the explicit \texttt{schema.table} rule is matched first and then executed.

Complex renames involving multiple schemas, tables and columns can be achieved by writing multiple rules into the same CSV file. For example given a schema where all the tables currently reside in a single schema, but must be renamed to specific continents, or to a ‘miscellaneous’ schema, while also updating the column names to be more neutral would require a detailed rename definition.

Existing tables are in the schema \texttt{sales}:

\begin{verbatim}
chicago
city
\end{verbatim}

Need to be renamed to:

\begin{verbatim}
northamerica.chicago
northamerica.newyork
\end{verbatim}

Meanwhile, the table definition needs to be updated to support more complex structure:

\begin{verbatim}
Id
area
country
city
value
type
\end{verbatim}

The area is being updated to contain the region within the country, while the value should be renamed to the three-letter currency code, for example, the \texttt{london} table would rename the \texttt{value} column to \texttt{gbp}.

The definition can be divided up into simple definitions at each object level, relying on the processing order to handle the individual exceptions. Starting with the table renames for the continents:

\begin{verbatim}
sales.chicago,*,northamerica,-,-
sales.newyork,*,northamerica,-,-
sales.london,*,europe,-,-
\end{verbatim}
A single rule to handle the renaming of any table not explicitly mentioned in the list above into the `misc` schema:

```
*,*,*,misc,,-,-
```

Now a rule to change the `area` column for all tables to `region`. This requires a wildcard match against the schema and table names:

```
*,*,area,,-,-,region
```

And finally the explicit changes for the value column to the corresponding currency:

```
*,chicago,value,,-,-,usd
*,newyork,value,,-,-,usd
*,london,value,,-,-,gbp
*,paris,value,,-,-,eur
*,munch,value,,-,-,eur
*,moscow,value,,-,-,rub
*,tokyo,value,,-,-,jpy
*,shanghai,value,,-,-,cny
*,sydney,value,,-,-,aud
```

### 10.4.32. ReplicateColumns Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>replicatecolumns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td><code>com.continuent.tungsten.replicator.filter.ReplicateColumnsFilter</code></td>
</tr>
<tr>
<td>Property prefix</td>
<td><code>replicator.filter.replicatecolumns</code></td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Row events</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>Data compatibility</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ignore</code></td>
<td>string</td>
<td><code>empty</code></td>
<td>Comma separated list of tables and optional columns names to ignore during replication</td>
</tr>
<tr>
<td><code>do</code></td>
<td>string</td>
<td><code>empty</code></td>
<td>Comma separated list of tables and optional column names to replicate</td>
</tr>
</tbody>
</table>

### 10.4.33. Replicate Filter

The `replicate` filter enables explicit inclusion or exclusion of tables and schemas. Each specification supports wildcards and multiple entries.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>replicate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td><code>com.continuent.tungsten.replicator.filter.ReplicateFilter</code></td>
</tr>
<tr>
<td>Property prefix</td>
<td><code>replicator.filter.replicate</code></td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ignore</code></td>
<td>string</td>
<td><code>empty</code></td>
<td>Comma separated list of database/tables to ignore during replication</td>
</tr>
<tr>
<td><code>do</code></td>
<td>string</td>
<td><code>empty</code></td>
<td>Comma separated list of database/tables to replicate</td>
</tr>
</tbody>
</table>

Rules using the supplied parameters are evaluated as follows:

- When both `do` and `ignore` are empty, updates are allowed to any table.
- When only `do` is specified, only the schemas (or schemas and tables) mentioned in the list are replicated.
• When only `ignore` is specified, all schemas/tables are replicated except those defined.

For each parameter, a comma-separated list of schema or schema and table definitions are supported, and wildcards using `*` (any number of characters) and `?` (single character) are also honored. For example:

• `do=sales`
  Replicates only the schema `sales`.

• `ignore=sales`
  Replicates everything, ignoring the schema `sales`.

• `ignore=sales.*`
  Replicates everything, ignoring the schema `sales`.

• `ignore=sales.quarter?`
  Replicates everything, ignoring all tables within the `sales` schema starting with `sales.quarter` and a single character. This would ignore `sales.quarter1` but replicate `sales.quarterlytotals`.

• `ignore=sales.quarter*`
  Replicates everything, ignoring all tables in the schema `sales` starting with `quarter`.

• `do=*quarter`
  Replicates only the table named `quarter` within any schema.

• `do=sales.*totals,invoices`
  Replicates only tables in the `sales` schema that end with `totals`, and the entire `invoices` schema.

### 10.4.34. SetToString Filter

The `SetToString` filter converts the `SET` column type from the internal representation to a string-based representation in the THL. This is achieved by accessing the extractor database, obtaining the table definitions, and modifying the THL data before it is written into the THL file.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>SetToString</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.filter.SetToStringFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.settostring</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q</td>
</tr>
<tr>
<td>Ipm Option compatibility</td>
<td>--repl-svc-extractor-filters[373]</td>
</tr>
</tbody>
</table>

Data compatibility Row events

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>string</td>
<td>${replicator.global.extract.db.user}</td>
<td>The username for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>${replicator.global.extract.db.password}</td>
<td>The password for the connection to the database for looking up column definitions</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>jdbc:mysql:thin://${replicator.global.extract.db.host}:${replicator.global.extract.db.port}/${replicator.schema}?createDB=true</td>
<td>JDBC URL of the database connection to use for looking up column definitions</td>
</tr>
</tbody>
</table>

The `SetToString` filter should be used with heterogeneous replication to ensure that the data is represented as the string value, not the internal numerical representation.

In the THL output below, the table has a `SET` column, `salesman`:

```sql
mysql> desc salesadv;
+----------+--------------------------------------+------+-----+---------+----------------+
| Field    | Type                                 | Null | Key | Default | Extra          |
|----------+--------------------------------------+------+-----+---------+----------------+
| id       | int(11)                              | NO   | PRI | NULL    | auto_increment |
| country  | enum('US','UK','France','Australia') | YES  | PRE | NULL    | auto_increment |
```
When extracted in the THL, the representation uses the internal value (for example, 1 for the first element of the set description). This can be seen in the THL output below.

For the `salesman` column, the corresponding value in the THL is 1. With the `SetToString` filter enabled, the value is expanded to the corresponding string value:

The examples here also show the Section 10.4.19, “EnumToString Filter” and Section 10.4.8, “ColumnName Filter” filters.

### 10.4.35. Shard Filter

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>shardfilter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classname</td>
<td>com.continuent.tungsten.replicator.Filter.ShardFilter</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.shardfilter</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td></td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td></td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>boolean</td>
<td>false</td>
<td>If set to true, enables the shard filter</td>
</tr>
<tr>
<td>unknownShardPolicy</td>
<td>string</td>
<td>error</td>
<td>Select the filter policy when the shard unknown; valid values are accept, drop, warn, and error</td>
</tr>
<tr>
<td>unwantedShardPolicy</td>
<td>string</td>
<td>error</td>
<td>Select the filter policy when the shard is unwanted; valid values are accept, drop, warn, and error</td>
</tr>
<tr>
<td>enforcedHome</td>
<td>boolean</td>
<td>false</td>
<td>If true, enforce the home for the shard</td>
</tr>
<tr>
<td>allowWhitelisted</td>
<td>boolean</td>
<td>false</td>
<td>If true, allow explicitly whitelisted shards</td>
</tr>
<tr>
<td>autoCreate</td>
<td>boolean</td>
<td>false</td>
<td>If true, allow shard rules to be created automatically</td>
</tr>
</tbody>
</table>
10.4.36. **shardbyseqno.js** Filter

Shards within the replicator enable data to be parallelized when they are applied on the slave.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>shardbyseqno</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/shardbyseqno.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.shardbyseqno</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shards</td>
<td>numeric</td>
<td>[none]</td>
<td>Number of shards to be used by the applier</td>
</tr>
</tbody>
</table>

The `shardbyseqno` filter updates the shard ID, which is embedded into the event metadata, by a configurable number of shards, set by the `shards` parameter in the configuration:

```java
replicator.filter.shardbyseqno=com.continuent.tungsten.replicator.filter.JavaScriptFilter
replicator.filter.shardbyseqno.script=${replicator.home}/samples/extensions/javascript/shardbyseqno.js
replicator.filter.shardbyseqno.shards=10
```

The filter works by setting the shard ID in the event using the `setShardId()` method on the event object:

```java
event.setShardId(event.getSeqno() % shards);
```

**Note**

Care should be taken with this filter, as it assumes that the events can be applied in a completely random order by blindly updating the shard ID to a computed valued. Sharding in this way is best used when provisioning new slaves.

10.4.37. **shardbytable.js** Filter

An alternative to **sharding by sequence number** is to create a shard ID based on the individual database and table. The `shardbytable` filter achieves this at a row level by combining the schema and table information to form the shard ID. For all other events, including statement based events, the shard ID `#UNKNOWN` is used.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>shardbytable</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/shardbytable.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.shardbytable</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>q-to-dbms</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

The key part of the filter is the extraction and construction of the ID, which occurs during row processing:

```javascript
oneRowChange = rowChanges.get();
schemaName = oneRowChange.getSchemaName();
tableName = oneRowChange.getTableName();

id = schemaName + "_" + tableName;
if (proposedShardId == null) {
    proposedShardId = id;
}
```

10.4.38. **TimeDelay (delay)** Filter

The **TimeDelayFilter** delays writing events to the THL and should be used only on slaves in the **remote-to-thl** stage. This delays writing the transactions into the THL files, but allows the application of the slave data to the database to continue without further intervention.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>delay</th>
</tr>
</thead>
</table>
### Replication Filters

<table>
<thead>
<tr>
<th>Classname</th>
<th>com.continuent.tungsten.replicator.filter.TimeDelayFilter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property prefix</td>
<td>replicator.filter.delay</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>remote-to-thl</td>
</tr>
<tr>
<td>tpm Option compatibility</td>
<td>--repl-svc-thl-filters [375]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Any event</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay</td>
<td>numeric</td>
<td>300</td>
<td>Number of seconds to delay transaction processing row</td>
</tr>
</tbody>
</table>

The `TimeDelay` delays the application of transactions recorded in the THL. The delay can be used to allow point-in-time recovery of DML operations before the transaction has been applied to the slave, or where data may need to be audited or checked before transactions are committed.

**Note**

For effective operation, master and slaves should be synchronized using NTP or a similar protocol.

To enable the `TimeDelayFilter`, use `tpm` command to enable the filter operation and the required delay. For example, to enable the delay for 900 seconds:

```
shell> ./tools/tpm update alpha --hosts=host1,host2,host3 \
    --repl-svc-applier-filters=delay \
    --property=replicator.filter.delay.delay=900
```

Time delay of transaction events should be performed with care, since the delay will prevent a slave from being up to date compared to the master. In the event of a node failure, an up to date slave is required to ensure that data is safe.

### 10.4.39. `tosingledb.js` Filter

This filter updates the replicated information so that it goes to an explicit schema, as defined by the user. The filter can be used to combine multiple tables to a single schema.

- **Pre-configured filter name**: `tosingledb`
- **JavaScript Filter File**: `tungsten-replicator/samples/extensions/javascript/tosingledb.js`
- **Stage compatibility**: `q-to-dbms`
- **tpm Option compatibility**: `--svc-applier-filters` [373]
- **Data compatibility**: Any event

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db</td>
<td>string</td>
<td>[none]</td>
<td>Database name into which to replicate all tables</td>
</tr>
<tr>
<td>skip</td>
<td>string</td>
<td>[none]</td>
<td>Comma-separated list of databases to be ignored</td>
</tr>
</tbody>
</table>

A database can be optionally ignored through the `skip` parameter within the configuration:

```
--property=replicator.filter.tosingledb.db=centraldb \
--property=replicator.filter.tosingledb.skip=tungsten
```

The above configures all data to be written into `centraldb`, but skips the database `tungsten`.

Similar to other filters, the filter operates by explicitly changing the schema name to the configured schema, unless the skipped schema is in the event data. For example, at a statement level:

```java
if(oldDb!=null && oldDb.compareTo(skip)!=0)
{
    d.setDefaultSchema(db);
}
```

### 10.4.40. `truncatetext.js` Filter

The `truncatetext` filter truncates a MySQL BLOB field.
### Replication Filters

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>truncatetext</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/truncatetext.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.truncatetext</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>binlog-to-q, q-to-dbms</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>--svc-extractor-filters [373], --svc-extractor-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
</tbody>
</table>

#### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>numeric</td>
<td>(none)</td>
<td>Maximum size of truncated field [bytes]</td>
</tr>
</tbody>
</table>

The length is determined by the `length` parameter in the properties:

```
replicator.filter.truncatetext=com.continuent.tungsten.replicator.filter.JavaScriptFilter
replicator.filter.truncatetext.script=${replicator.home.dir}/samples/extensions/javascript/truncatetext.js
replicator.filter.truncatetext.length=4000
```

Statement-based events are ignored, but row-based events are processed for each volume value, checking the column type, `isBlob()` method and then truncating the contents when they are identified as larger than the configured length. To confirm the type, it is compared against the Java class `com.continuent.tungsten.replicator.extractor.mysql.SerialBlob`, the class for a serialized BLOB value. These need to be processed differently as they are not exposed as a single variable.

```java
if (value.getValue() instanceof com.continuent.tungsten.replicator.extractor.mysql.SerialBlob)
{
    blob = value.getValue();
    if (blob != null)
    {
        valueBytes = blob.getBytes(1, blob.length());
        if (blob.length() > truncateTo)
        {
            blob.truncate(truncateTo);
        }
    }
}
```

---

### 10.4.41. zerodate2null.js Filter

The `zerodate2null` filter looks complicated, but is very simple. It processes row data looking for date columns. If the corresponding value is zero within the column, the value is updated to NULL. This is required for MySQL to Oracle replication scenarios.

<table>
<thead>
<tr>
<th>Pre-configured filter name</th>
<th>zerodate2null</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript Filter File</td>
<td>tungsten-replicator/samples/extensions/javascript/zerodate2null.js</td>
</tr>
<tr>
<td>Property prefix</td>
<td>replicator.filter.zerodate2null</td>
</tr>
<tr>
<td>Stage compatibility</td>
<td>q-to-dbms</td>
</tr>
<tr>
<td><code>tpm</code> Option compatibility</td>
<td>--svc-applier-filters [373]</td>
</tr>
<tr>
<td>Data compatibility</td>
<td>Row events</td>
</tr>
</tbody>
</table>

The filter works by examining the column specification using the `getColumnSpec()` method. Each column is then checked to see if the column type is a `DATE`, `DATETIME` or `TIMESTAMP` by looking the type ID using some stored values for the date type.

Because the column index and corresponding value index match, when the value is zero, the column value is explicitly set to NULL using the `setValueNull()` method.

```java
for(j = 0; j < rowChanges.size(); j++)
{
    oneRowChange = rowChanges.get(j);
    columns = oneRowChange.getColumnSpec();
    columnValues = oneRowChange.getColumnValues();
    for (c = 0; c < columnValues.size(); c++)
    {
        columnsSpec = columns.get(c);
        type = columnsSpec.getType();
        if (type == TypesDATE || type == TypesTIMESTAMP)
        {
            for (row = 0; row < columnValues.size(); row++)
```

---

412
10.5. JavaScript Filters

In addition to the supplied Java filters, Tungsten Replicator also includes support for custom script-based filters written in JavaScript and supported through the JavaScript filter. This filter provides a JavaScript environment that exposes the transaction information as it is processed internally through an object-based JavaScript API.

The JavaScript implementation is provided through the Rhino open-source implementation. Rhino provides a direct interface between the underlying Java classes used to implement the replicator code and a full JavaScript environment. This enables scripts to be developed that have access to the replicator constructs and data structures, and allows information to be updated, reformatted, combined, extracted and reconstructed.

At the simplest level, this allows for operations such as database renames and filtering. More complex solutions allow for modification of the individual data, such as removing nulls, bad dates, and duplication of information.

**Warning**

Updating the static properties file for the replicator will break automated upgrades through `tpm`. When upgrading, `tpm` relies on existing template files to create the new configuration based on the `tpm` parameters used.

Making a backup copy of the configuration file automatically generated by `tpm`, and then using this before performing an upgrade will enable you to update your configuration automatically. Settings for the JavaScript filter will then need to be updated in the configuration file manually.

To enable a JavaScript filter that has not already been configured, the static properties file (`static-SERVICE.properties`) must be edited to include the definition of the filter using the `JavaScriptFilter` class, using the `script` property to define the location of the actual JavaScript file containing the filter definition. For example, the supplied `ansiquotes` filter is defined as follows:

```plaintext
replicator.filter.ansiquotes=com.continuent.tungsten.replicator.filter.JavaScriptFilter
replicator.filter.ansiquotes.script=${replicator.home.dir}/samples/extensions/javascript/ansiquotes.js
```

To use the filter, add the filter name, `ansiquotes` in the above example, to the required stage:

```plaintext
replicator.stage.q-to-dbms.filters=mysqlsessions,pkey,bidiSlave,ansiquotes
```

Then restart the replicator to enable the configuration:

```plaintext
shell> replicator restart
```

**Note**

This procedure will need to be enabled on each replicator that you want to use the JavaScript filter.

If there is a problem with the JavaScript filter during restart, the replicator will be placed into the `OFFLINE` state and the reason for the error will be provided within the replicator `trepsvc.log` log.

10.5.1. Writing JavaScript Filters

The JavaScript interface to the replicator enables filters to be written using standard JavaScript with a complete object-based interface to the internal Java objects and classes that make up the THL data.

For more information on the Rhino JavaScript implementation, see Rhino.

The basic structure of a Rhino JavaScript filter is as follows:

```javascript
// Prepare the filter and setup structures
prepare()
{
}
```
The following sections will examine the different data structures, functions, and information available when processing these individual events.

10.5.1. Implementable Functions

Each JavaScript filter must define one or more functions that are used to operate the filter process. The `filter()` function must be defined, as it contains the primary operation sequence for the defined filter. The function is supplied the event from the THL as the events are processed by the replicator.

In addition, two other JavaScript functions can optionally be defined that are executed before and after the filter process. Additional, user-specific functions can be defined within the filter context to support the filter operations.

- **prepare()**
  
  The `prepare()` function is called when the replicator is first started, and initializes the configured filter with any values that may be required during the filter process. These can include loading and identifying configuration values, creating lookup, exception or other reference tables and other internal JavaScript tables based on the configuration information, and reporting the generated configuration or operation for debugging.

- **filter(event)**
  
  The `filter()` function is the main function that is called each time an event is loaded from the THL. The `event` parameter to the function and is an object containing all the statement or row data for a given event.

- **release()**
  
  The `release()` function is called when the filter is deallocated and removed, typically during shutdown of the replicator, although it may also occur when a processing thread is restarted.

10.5.2. Getting Configuration Parameters

The JavaScript interface enables you to get two different sets of configuration properties, the filter specific properties, and the general replicator properties. The filter specific properties should be used configure and specify configuration information unique to that instance of the filter configuration. Since multiple filter configurations using the same filter definition can be created, using the filter-specific content is the simplest method for obtaining this information.
• Getting Filter Properties

To obtain the properties configured for the filter within the static configuration file according to the context of the filter configuration, use the filterProperties class with the getString() method. For example, the dbrename filter uses two properties, dbsource and dbtarget to identify the database to be renamed and the new name. The definition for the filter within the configuration file might be:

replicator.filter.jsdbrename=com.continuent.tungsten.replicator.filter.JavaScriptFilter
replicator.filter.jsdbrename.script=${replicator.home.dir}/samples/extensions/javascript/dbrename.js
replicator.filter.jsdbrename.dbsource=contacts
replicator.filter.jsdbrename.dbtarget=nyc_contacts

Within the JavaScript filter, they are retrieved using:

sourceName = filterProperties.getString("dbsource");
targetName = filterProperties.getString("dbtarget");

• Generic Replicator Properties

General properties can be retrieved using the properties class and the getString() method:

master = properties.getString("replicator.thl.remote_uri");

10.5.1.3. Logging Information and Exceptions

Information about the filtering process can be reported into the standard trepsvc.log file by using the logger object. This supports different methods according to the configured logging level:

• logger.info() — information level entry, used to indicate configuration, loading or progress.
• logger.debug() — information will be logged when debugging is enabled, used when showing progress during development.
• logger.error() — used to log an error that would cause a problem or replication to stop.

For example, to log an informational entry that includes data from the filter process:

logger.info("regexp: Translating string "+ valueString.valueOf());

To raise an exception that causes replication to stop, a new ReplicatorException object must be created that contains the error message:

if(col == null)
{
    throw new com.continuent.tungsten.replicator.ReplicatorException(
        'dropcolumn.js: column name in " + schema + "." + table + 
        ' is undefined - is colnames filter enabled and is it before the dropcolumn filter?'
    );
}

The error string provided will be used as the error provided through trepctl, in addition to raising an exception and backtrace within the log.

10.5.1.4. Exposed Data Structures

Within the filter() function that must be defined within the JavaScript filter, a single event object is supplied as the only argument. That event object contains all of the information about a single event as recorded within the THL as part of the replication process. Each event contains metadata information that can be used to identify or control the content, and individual statement and row data that contain the database changes.

The content of the information is a compound set of data that contains one or more further blocks of data changes, which in turn contains one or more blocks of SQL statements or row data. These blocks are defined using the Java objects that describe their internal format, and are exposed within the JavaScript wrapper as JavaScript objects, that can be parsed and manipulated.

At the top level, the Java object provided to the to the filter() function as the event argument is ReplDBMSEvent. The ReplDBMSEvent class provides the core event information with additional management metadata such as the global transaction ID (seqno), latency of the event and sharding information.

That object contains one or more DBMSData objects. Each DBMSData object contains either a StatementData object [in the case of a statement based event], or a RowChangeData object [in the case of row-based events]. For row-based events, there will be one or more OneRowChange objects for each individual row that was changed.

When processing the event information, the data that is processed is live and should be updated in place. For example, when examining statement data, the statement needs only be updated in place, not re-submitted. Statements and rows can also be explicitly removed or added by deleting or extending the arrays that make up the objects.

A basic diagram of the structure is shown in the diagram below:
Replication Filters

A single event can contain both statement and row change information within the list of individual `DBMSData` events. An event or

10.5.1.4.1. `RepDBMSEvent` Objects

The base object from which all of the data about replication can be obtained is the `RepDBMSEvent` class. The class contains all of the information about each event, including the global transaction ID and statement or row data.

The interface to the underlying information is through a series of methods that provide the embedded information or data structures, described in the table below.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getAppliedLatency()</code></td>
<td>Returns the latency of the embedded event. See Section D.2.6, “Terminology: Fields appliedLatency”</td>
</tr>
<tr>
<td><code>getData()</code></td>
<td>Returns an array of the <code>DBMSData</code> objects within the event</td>
</tr>
<tr>
<td><code>getDBMSEvent()</code></td>
<td>Returns the original <code>DBMSEvent</code> object</td>
</tr>
<tr>
<td><code>getEpochNumber()</code></td>
<td>Get the Epoch number of the stored event. See THL EPOCH# [493]</td>
</tr>
<tr>
<td><code>getEventId()</code></td>
<td>Returns the native event ID. See THL EVENTID [493]</td>
</tr>
<tr>
<td><code>getExtractedTstamp()</code></td>
<td>Returns the timestamp of the event.</td>
</tr>
<tr>
<td><code>getFragno()</code></td>
<td>Returns the fragment ID. See THL SEQNO [492]</td>
</tr>
<tr>
<td><code>getLastFrag()</code></td>
<td>Returns true if the fragment is the last fragment in the event.</td>
</tr>
<tr>
<td><code>getSequence()</code></td>
<td>Returns the native sequence number. See THL SEQNO [492]</td>
</tr>
<tr>
<td><code>getShardId()</code></td>
<td>Returns the shard ID for the event.</td>
</tr>
<tr>
<td><code>getSourceId()</code></td>
<td>Returns the source ID of the event. See THL SOURCEID [493]</td>
</tr>
<tr>
<td><code>setShardId()</code></td>
<td>Sets the shard ID for the event, which can be used by the filter to set the shard.</td>
</tr>
</tbody>
</table>

The primary method used is `getData()`, which returns an array of the individual `DBMSData` objects contain in the event:

```javascript
function filter(event) {
  data = event.getData();
  if(data != null) {
    for (i = 0; i < data.size(); i++) {
      change = data.get(i);
    ...
  }
}
```

Access to the underlying array structure uses the `get()` method to request individual objects from the array. The `size()` method returns the length of the array.

Removing or Adding Data Changes

Individual `DBMSData` objects can be removed from the replication stream by using the `remove()` method, supplying the index of the object to remove:

```javascript
data.remove(1);
```

The `add()` method can be used to add new data changes into the stream. For example, data can be duplicated across tables by creating and adding a new version of the event, for example:

```javascript
if(d.getDefaultSchema() != null && ...
```
d.getDefaultSchema().compareTo(sourceName)==0)
{
    newStatement = new
    com.continuent.tungsten.replicator.dbms.StatementData(d.getQuery(),
    null,
    targetName);
data.add(data.size(),newStatement);
}

The above code looks for statements within the sourceName schema and creates a copy of each statement into the targetName schema.

The first argument to add() is the index position to add the statement. Zero (0) indicates before any existing changes, while using size() on the array effectively adds the new statement change at the end of the array.

Updating the Shard ID

The setShardId() method can also be used to set the shard ID within an event. This can be used in filters where the shard ID is updated by examining the schema or table being updated within the embedded SQL or row data. An example of this is provided in Section 10.4.37, "shardbytable.js Filter".

10.5.1.4.2. DBMSData Objects

The DBMSData object provides encapsulation of either the SQL or row change data within the THL. The class provides no methods for interacting with the content, instead, the real object should be identified and processed accordingly. Using the JavaScript instanceof operator the underlying type can be determined:

\[
\text{if (d != null && d instanceof \text{com.continuent.tungsten.replicator.dbms.StatementData})} \\
\{
    // Process Statement data
\}
\text{else if (d != null && d instanceof \text{com.continuent.tungsten.replicator.dbms.RowChangeData})} \\
\{
    // Process Row data
\}
\]

Note the use of the full object class for the different DBMSData types.

For information on processing StatementData, see Section 10.5.1.4.3, "StatementData Objects". For row data, see Section 10.5.1.4.4, "RowChangeData Objects".

10.5.1.4.3. StatementData Objects

The StatementData class contains information about data that has been replicated as an SQL statement, as opposed to information that is replicated as row-based data.

Processing and filtering statement information relies on editing the original SQL query statement, or the metadata recorded with it in the THL, such as the schema name or character set. Care should be taken when modifying SQL statement data to ensure that you are modifying the right part of the original statement. For example, a search and replace on an SQL statement should be made with care to ensure that embedded data is not altered by the process.

The key methods used for interacting with a StatementData object are listed below:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getQuery()</td>
<td>Returns the SQL statement</td>
</tr>
<tr>
<td>setQuery()</td>
<td>Updates the SQL statement</td>
</tr>
<tr>
<td>appendToQuery()</td>
<td>Appends a string to an existing query</td>
</tr>
<tr>
<td>getDefaultSchema()</td>
<td>Returns the default schema in which the statement was executed. The schema may be null for explicit or multi-schema queries.</td>
</tr>
<tr>
<td>setDefaultSchema()</td>
<td>Set the default schema for the SQL statement</td>
</tr>
<tr>
<td>getTimestamp()</td>
<td>Gets the timestamp of the query. This is required if data must be applied with a relative value by combining the timestamp with the relative value</td>
</tr>
</tbody>
</table>

Updating the SQL

The primary method of processing statement based data is to load and identify the original SQL statement (using getQuery()), update or modify the SQL statement string, and then update the statement within the THL again using setQuery(). For example:

\[
sqlOriginal = d.getQuery();
\]
Replication Filters

```java
sqlNew = sqlOriginal.replaceAll('NOTEPAD', 'notepad');
d.setQuery(sqlNew);
```

The above replaces the uppercase 'NOTEPAD' with a lowercase version in the query before updating the stored query in the object.

Changing the Schema Name

Some schema and other information is also provided in this structure. For example, the schema name is provided within the statement data and can be explicitly updated. In the example below, the schema “products” is updated to “nyc_products”:

```java
if (change.getDefaultSchema().compareTo("products") == 0) {
    change.setDefaultSchema("nyc_products");
}
```

A similar operation should be performed for any row-based changes. A more complete example can be found in Section 10.4.11, “dbrename.js Filter”.

10.5.1.4.4. RowChangeData Objects

RowChangeData is information that has been written into the THL in row format, and therefore consists of rows of individual data divided into the individual columns that make up each row-based change. Processing of these individual changes must be performed one row at a time using the list of OneRowChange [418] objects provided.

The following methods are supported for the RowChangeData object:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appendOneRowChange(rowChange)</td>
<td>Appends a single row change to the event, using the supplied OneRowChange [418] object.</td>
</tr>
<tr>
<td>getRowChanges()</td>
<td>Returns an array list of all the changes as OneRowChange [418] objects.</td>
</tr>
<tr>
<td>setRowChanges(rowChanges)</td>
<td>Sets the row changes within the event using the supplied list of OneRowChange objects.</td>
</tr>
</tbody>
</table>

For example, a typical row-based process will operate as follows:

```java
if (d != null && d instanceof com.continuent.tungsten.replicator.dbms.RowChangeData) {
    rowChanges = d.getRowChanges();
    for(j = 0; j < rowChanges.size(); j++) {
        oneRowChange = rowChanges.get(j);
        // Do row filter
    }
}
```

The OneRowChange [418] object contains the changes for just one row within the event. The class contains the information about the tables, field names and field values. The following methods are supported:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getAction()</td>
<td>Returns the row action type, i.e. whether the row change is an INSERT, UPDATE or DELETE</td>
</tr>
<tr>
<td>getColumnSpec()</td>
<td>Returns the specification of each column within the row change</td>
</tr>
<tr>
<td>getColumnValues()</td>
<td>Returns the value of each column within the row change</td>
</tr>
<tr>
<td>getSchemaName()</td>
<td>Gets the schema name of the row change</td>
</tr>
<tr>
<td>getTableName()</td>
<td>Gets the table name of the row change</td>
</tr>
<tr>
<td>setColumnSpec()</td>
<td>Sets the column specification using an array of column specifications</td>
</tr>
<tr>
<td>setColumnValues()</td>
<td>Sets the column values</td>
</tr>
<tr>
<td>setSchemaName()</td>
<td>Sets the schema name</td>
</tr>
<tr>
<td>setTableName()</td>
<td>Sets the table name</td>
</tr>
</tbody>
</table>

Changing Schema or Table Names

The schema, table and column names are exposed at different levels within the OneRowChange [418] object. Updating the schema name can be achieved by getting and setting the name through the getSchemaName() and setSchemaName() methods. For example, to add a prefix to a schema name:

```java
rowchange.setSchemaName('prefix_' + rowchange.getSchemaName());
```

To update a table name, the getTableName() and setTableName() can be used in the same manner:

```java
oneRowChange.setTableName('prefix_' + oneRowChange.getTableName());
```
Getting Action Types

Row operations are categorised according to the action of the row change, i.e. whether the change was an insert, update or delete operation. This information can be extracted from each row change by using the `getAction()` method:

```java
action = oneRowChange.getAction();
```

The action information is returned as a string, i.e. `INSERT`, `UPDATE`, or `DELETE`. This enables information to be filtered according to the changes; for example by selectively modifying or altering events.

For example, `DELETE` events could be removed from the list of row changes:

```java
for(j=0; j<rowChanges.size(); j++)
{
    oneRowChange = rowChanges.get(j);
    if (oneRowChange.actionType == 'DELETE')
    {
        rowChanges.remove(j);
        j--;
    }
}
```

The `j--` is required because as each row change is removed, the size of the array changes and our current index within the array needs to be explicitly modified.

Extracting Column Definitions

To extract the row data, the `getColumnValues()` method returns the an array containing the value of each column in the row change. Obtaining the column specification information using `getColumnSpec()` returns a corresponding specification of each corresponding column. The column data can be used to obtain the column type information.

To change column names or values, first the column information should be identified. The column information in each row change should be retrieved and/or updated. The `getColumnSpec()` returns the column specification of the row change. The information is returned as an array of the individual columns and their specification:

```java
columns = oneRowChange.getColumnSpec();
```

For each column specification a `ColumnSpec` object is returned, which supports the following methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getIndex()</code></td>
<td>Gets the index of the column within the row change</td>
</tr>
<tr>
<td><code>getLength()</code></td>
<td>Gets the length of the column</td>
</tr>
<tr>
<td><code>getName()</code></td>
<td>Returns the column name if available</td>
</tr>
<tr>
<td><code>getType()</code></td>
<td>Gets the type number of the column</td>
</tr>
<tr>
<td><code>getTypeDescription()</code></td>
<td></td>
</tr>
<tr>
<td><code>isBlob()</code></td>
<td>Returns true if the column is a blob</td>
</tr>
<tr>
<td><code>isNullNull()</code></td>
<td>Returns true if the column is configured as NOT NULL</td>
</tr>
<tr>
<td><code>isUnsigned()</code></td>
<td>Returns true if the column is unsigned.</td>
</tr>
<tr>
<td><code>setBlob()</code></td>
<td>Set the column blob specification</td>
</tr>
<tr>
<td><code>setIndex()</code></td>
<td>Set the column index order</td>
</tr>
<tr>
<td><code>setLength()</code></td>
<td>Returns the column length</td>
</tr>
<tr>
<td><code>setName()</code></td>
<td>Set the column name</td>
</tr>
<tr>
<td><code>setNotNull()</code></td>
<td>Set whether the column is configured as NOT NULL</td>
</tr>
<tr>
<td><code>setSigned()</code></td>
<td>Set whether the column data is signed</td>
</tr>
<tr>
<td><code>setType()</code></td>
<td>Set the column type</td>
</tr>
<tr>
<td><code>setTypeDescription()</code></td>
<td></td>
</tr>
</tbody>
</table>

To identify the column type, use the `getType()` method which returns an integer matching the underlying data type. There are no predefined types, but common values include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>INT</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>CHAR or VARCHAR</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>
### Replication Filters

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEXT or BLOB</td>
<td>2004</td>
<td>Use <code>isBlob()</code> to identify if the column is a blob or not</td>
</tr>
<tr>
<td>TIME</td>
<td>92</td>
<td></td>
</tr>
<tr>
<td>DATE</td>
<td>91</td>
<td></td>
</tr>
<tr>
<td>DATETIME OF TIMESTAMP</td>
<td>92</td>
<td></td>
</tr>
<tr>
<td>DOUBLE</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Other information about the column, such as the length, and value types (unsigned, null, etc.) can be determined using the other functions against the column specification.

### Extracting Row Data

The `getColumnValues()` method returns an array that corresponds to the information returned by the `getColumnSpec()` method. That is, the method returns a complementary array of the row change values, one element for each row, where each row is itself a further array of each column:

```java
values = oneRowChange.getColumnValues();
```

This means that index 0 of the array from `getColumnSpec()` refers to the same column as index 0 of the array for a single row from `getColumnValues()`.

```java
getColumnSpec()   | msgid | message        | msgdate               
------------------|-------|----------------|----------------------|
getColumnValues() |       |                |                      |
[0]               | 1     | Hello New York!| Thursday, June 13, 2013 |
```

This enables the script to identify the column type by the index, and then the corresponding value update using the same index. In the above example, the `message` field will always be index 1 within the corresponding values.

Each value object supports the following methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getValue()</code></td>
<td>Get the current column value</td>
</tr>
<tr>
<td><code>setValue()</code></td>
<td>Set the column value to the supplied value</td>
</tr>
<tr>
<td><code>setValueNull()</code></td>
<td>Set the column value to NULL</td>
</tr>
</tbody>
</table>

For example, within the `zerodate2null` sample, dates with a zero value are set to NULL using the following code:

```java
columns = oneRowChange.getColumnSpec();
columnValues = oneRowChange.getColumnValues();
for (c = 0; c < columns.size(); c++)
{
    columnSpec = columns.get(c);
    type = columnSpec.getType();
    if (type == TypesDATE || type == TypesTIMESTAMP)
    {
        for (row = 0; row < columnValues.size(); row++)
        {
            values = columnValues.get(row);
            value = values.get(c);
            if (value.getValue() == 0)
            {
                value.setValueNull();
            }
        }
    }
}
```

In the above example, the column specification is retrieved to determine which columns are date types. Then the list of embedded row values is extracted, and iterates over each row, setting the value for a date that is zero (0) to be NULL using the `setValueNull()` method.

An alternative would be to update to an explicit value using the `setValue()` method.
Chapter 11. Performance and Tuning

To help improve the performance of Continuent Tungsten, a number of guides and tuning techniques are provided in this chapter. This may involve parameters entirely within Continuent Tungsten, or changes and modifications to the parameters within the OS.

Tuning related to the Tungsten Replicator functionality

- **Section 11.1, “Block Commit”** — Increasing performance of replication solutions making use of block commit.

Tuning related to the network performance

- **Section 11.2, “Improving Network Performance”** — Increasing performance of networking between components by tuning OS parameters.

11.1. Block Commit

Introduced in 2.0.1. The commit size and interval settings were introduced in 2.2.0.

The replicator commits changes read from the THL and commits these changes in slaves during the applier stage according to the block commit size or interval. These replace the single `replicator.global.buffer.size` parameter that controls the size of the buffers used within each stage of the replicator.

When applying transactions to the database, the decision to commit a block of transactions is controlled by two parameters:

- When the event count reaches the specified event limit (set by `--svc-applier-block-commit-size`)
- When the commit timer reaches the specified commit interval (set by `--svc-applier-block-commit-interval`)

The default operation is for block commits to take place based on the transaction count. Commits by the timer are disabled. The default block commit size is 10 transactions from the incoming stream of THL data; the block commit interval is zero (0), which indicates that the interval is disabled.

When both parameters are configured, block commit occurs when either value limit is reached. For example, if the event count is set to 10 and the commit interval to 50s, events will be committed by the applier either when the event count hits 10 or every 50 seconds, whichever is reached first. This means, for example, that even if only one transaction exists, when the 50 seconds is up, that single transaction will be applied.

The block commit size can be controlled using the `--repl-svc-applier-block-commit-size` option to `tpm`, or through the `blockCommitRowCount`. The block commit interval can be controlled using the `--repl-svc-applier-block-commit-interval` option to `tpm`, or through the `blockCommitInterval`. If only a number is supplied, it is used as the interval in milliseconds. Suffix of s, m, h, and d for seconds, minutes, hours and days are also supported.

```
shell> ./tools/tpm update alpha \
  --repl-svc-applier-block-commit-size=20 \
  --repl-svc-applier-block-commit-interval=100s
```

**Note**

The block commit parameters are supported only in applier stages; they have no effect in other stages.

Modification of the block commit interval should be made only when the commit window needs to be altered. The setting can be particularly useful in heterogeneous deployments where the nature and behaviour of the target database is different to that of the source extractor.

For example, when replicating to Oracle, reducing the number of transactions within commits reduces the locks and overheads:

```
shell> ./tools/tpm update alpha \
  --repl-svc-applier-block-commit-interval=500
```

This would apply two commits every second, regardless of the block commit size.

When replicating to a data warehouse engine, particularly when using batch loading, such as Vertica ([Tungsten Replicator 2.2 Manual]), larger block commit sizes and intervals may improve performance during the batch loading process:

```
shell> ./tools/tpm update alpha \
  --repl-svc-applier-block-commit-size=100000 \
  --repl-svc-applier-block-commit-interval=60s
```

This sets a large block commit size and interval enabling large batch loading.
11.1. Monitoring Block Commit Status

The block commit status can be monitored using the `trepctl status -name tasks` command. This outputs the `lastCommittedBlockSize` and `lastCommittedBlockTime` values which indicate the size and interval (in seconds) of the last block commit.

```
  $ trepctl status -name tasks
  Processing status command (tasks)...

  NAME                    VALUE
  ----                    -----  
  appliedLastEventId    : mysql-bin.000015:0000000000001117;0
  appliedLastSeqno      : 5271
  applyTime             : 0.066
  averageBlockSize      : 0.500
  cancelled             : false
  commits               : 10
  currentBlockSize      : 0
  currentLastEventId    : mysql-bin.000015:0000000000001117;0
  currentLastFragno     : 0
  currentLastSeqno      : 5271
  eventCount            : 5
  extractTime           : 0.394
  filterTime            : 0.017
  lastCommittedBlockSize: 1
  lastCommittedBlockTime: 0.033
  otherTime             : 0
  stage                 : q-to-dbms
  state                 : extract
  taskId                : 0
  Finished status command (tasks)...
```

11.2. Improving Network Performance

The performance of the network can be critical when replicating data. The information transferred over the network contains the full content of the THL in addition to a small protocol overhead. Improving your network performance can have a significant impact on the overall performance of the replication process.

When using the Connector and client applications, improving the network performance will aid the overall performance of your application during both the client to connector, and connector to MySQL server connectivity.

The following network parameters should be configured within your `/etc/sysctl.conf` and can safely applied to all the hosts within your cluster deployments:

```bash
# Increase size of file handles and inode cache
fs.file-max = 2097152

# tells the kernel how many TCP sockets that are not attached to any user file handle to maintain. In case this number is exceeded, orphaned connections are immediately reset and a warning is printed.
net.ipv4.tcp_max_orphans = 60000

# Do not cache metrics on closing connections
net.ipv4.tcp_no_metrics_save = 1

# Turn on window scaling which can enlarge the transfer window:
net.ipv4.tcp_window_scaling = 1

# Enable timestamps as defined in RFC1323:
net.ipv4.tcp_timestamps = 1

# Enable select acknowledgments:
net.ipv4.tcp_sack = 1

# Maximum number of remembered connection requests, which did not yet receive an acknowledgment from connecting client.
net.ipv4.tcp_max_syn_backlog = 10240

# recommended default congestion control is htcp
net.ipv4.tcp_congestion_control=htcp

# recommended for hosts with jumbo frames enabled
net.ipv4.tcp_mtu_probing=1

# Number of times SYNACKs for passive TCP connection.
net.ipv4.tcp_synack_retries = 2

# Allowed local port range
net.ipv4.ip_local_port_range = 1024 65535
```
Performance and Tuning

# Protect Against TCP Time-Wait

```
net.ipv4.tcp_rfc1337 = 1
```

# Decrease the time default value for tcp_fin_timeout connection

```
net.ipv4.tcp_fin_timeout = 15
```

# Increase number of incoming connections

```
# somaxconn defines the number of request_sock structures
# allocated per each listen call. The
# queue is persistent through the life of the listen socket.
net.core.somaxconn = 1024
```

# Increase number of incoming connections backlog queue

```
# Sets the maximum number of packets, queued on the INPUT
# side, when the interface receives packets faster than
# kernel can process then.
net.core.netdev_max_backlog = 65536
```

# Increase the maximum amount of option memory buffers

```
net.core.optmem_max = 25165824
```

# Increase the maximum total buffer-space allocatable

```
# This is measured in units of pages (4096 bytes)
net.ipv4.tcp_mem = 65536 131072 262144
net.ipv4.udp_mem = 65536 131072 262144
```

# Set the max OS send buffer size (wmem) and receive buffer
# size (rmem) to 12 MB for queues on all protocols. In other
# words set the amount of memory that is allocated for each
# TCP socket when it is opened or created while transferring files

```
# Default Socket Receive Buffer
net.core.rmem_default = 25165824
```

# Maximum Socket Receive Buffer

```
net.core.rmem_max = 25165824
```

# Increase the read-buffer space allocatable (minimum size,
# initial size, and maximum size in bytes)

```
net.ipv4.tcp_rmem = 20480 12582912 25165824
net.ipv4.udp_rmem_min = 16384
```

# Default Socket Send Buffer

```
net.core.wmemp_default = 25165824
```

# Maximum Socket Send Buffer

```
net.core.wmem_max = 25165824
```

# Increase the write-buffer space allocatable

```
net.ipv4.tcp_wmem = 20480 12582912 25165824
net.ipv4.udp_wmem_min = 16384
```

# Increase the tcp-time-wait buckets pool size to prevent simple DOS attacks

```
net.ipv4.tcp_tw_buckets = 1440000
```

11.3. Enable Heterogeneous Replication from a Cluster

The Tungsten Replicator supports replication into many different DBMS platforms. In order for this to work properly the cluster must be configured correctly. During deployment include the `--enable-heterogeneous-service=true` option in the defaults or service definition for the cluster. Use the `tpm update` command if you have already deployed the cluster.

```
shell > ./tools/tpm configure defaults \
   --enable-heterogeneous-service=true
```

During Tungsten Replicator deployment use the `--topology=cluster-slave [377]` as described in Section 3.7, “Replicating Data from a Cluster into MySQL”.

11.4. Tungsten Replicator Block Commit and Memory Usage

Replicators are implemented as Java processes, which use two types of memory: stack space, which is allocated per running thread and holds objects that are allocated within individual execution stack frames, and heap memory, which is where objects that persist across individual method calls live. Stack space is rarely a problem for Tungsten as replicators rarely run more than 200 threads and use limited recursion. The Java defaults are almost always sufficient. Heap memory on the other hand runs out if the replicator has too many transactions in memory at once. This results in the dreaded Java OutOfMemory exception, which causes the replicator to stop operating. When this happens you need to look at tuning the replicator memory size.
To understand replicator memory usage, we need to look into how replicators work internally. Replicators use a "pipeline" model of execution that streams transactions through 1 or more concurrently executing stages. As you can see from the attached diagram, a slave pipeline might have a stage to read transactions to the master and put them in the THL, a stage to read them back out of the THL into an in-memory queue, and a stage to apply those transactions to the slave. This model ensures high performance as the stages work independently. This streaming model is quite efficient and normally permits Tungsten to transfer even exceedingly large transactions, as the replicator breaks them up into smaller pieces called transaction fragments.

The pipeline model has consequences for memory management. First of all, replicators are doing many things at one, hence need enough memory to hold all current objects. Second, the replicator works fastest if the in-memory queues between stages are large enough that they do not ever become empty. This keeps delays in upstream processing from delaying things at the end of the pipeline. Also, it allows replicators to make use of block commit. Block commit is an important performance optimization in which stages try to commit many transactions at once on slaves to amortize the cost of commit. In block commit the end stage continues to commit transactions until it either runs out of work [i.e., the upstream queue becomes empty] or it hits the block commit limit. Larger upstream queues help keep the end stage from running out of work, hence increase efficiency.

Bearing this in mind, we can alter replicator behavior in a number of ways to make it use less memory or to handle larger amounts of traffic without getting a Java OutOfMemoryError. You should look at each of these when tuning memory:

- Property wrapper.java.memory in file wrapper.conf. This controls the amount of heap memory available to replicators. 1024 MB is the minimum setting for most replicators. Busy replicators, those that have multiple services, or replicators that use parallel apply should consider using 2048 MB instead. If you get a Java OutOfMemory exception, you should first try raising the current setting to a higher value. This is usually enough to get past most memory-related problems. You can set this at installation time as the --repl-java-mem-size parameter.

- Property replicator.stage.q-to-dbms.blockCommitRowCount in the replicator properties file. This parameter sets the block commit count in the final stage in a slave pipeline. If you reduce the global buffer size, it is a good idea to set this to an fixed size, such as 10, to avoid reducing the block commit effect too much. Very low block commit values in this stage can cut update rates on slaves by 50% or more in some cases. This is available at installation time as the --repl-buffer-size parameter.

- Property replicator.stage.q-to-dbms.transaction_frag_size in the replicator.properties file. This parameter controls the size of fragments for long transactions. Tungsten automatically breaks up long transactions into fragments. This parameter controls the number of bytes of binary log per transaction fragment. You can try making this value smaller to reduce overall memory usage if many transactions are simultaneously present. Normally however this value has minimal impact.

Finally, it is worth mentioning that the main cause of out-of-memory conditions in replicators is large transactions. In particular, Tungsten cannot fragment individual statements or row changes, so changes to very large column values can also result in OutOfMemory conditions. For now the best approach is to raise memory, as described above, and change your application to avoid such transactions.

The replicator commits changes read from the THL and commits these changes in slaves during the applier stage according to the block commit size or interval. These replace the single replicator.stage.q-to-dbms.transaction_frag_size parameter that controls the size of the buffers used within each stage of the replicator.

When applying transactions to the database, the decision to commit a block of transactions is controlled by two parameters:

- When the event count reaches the specified event limit (set by blockCommitRowCount)
- When the commit timer reaches the specified commit interval (set by blockCommitInterval)

The default operation is for block commits to take place based on the transaction count. Commits by the timer are disabled. The default block commit size is 10 transactions from the incoming stream of THL data; the block commit interval is zero (0), which indicates that the interval is disabled.

When both parameters are configured, block commit occurs when either value limit is reached. For example, if the event count is set to 10 and the commit interval to 50s, events will be committed by the applier either when the event count hits 10 or every 50 seconds, whichever is reached first. This means, for example, that even if only one transaction exists, when the 50 seconds is up, that single transaction will be applied.

The block commit size can be controlled using the --repl-svc-applier-block-commit-size parameter to tpm, or through the blockCommitRowCount. The block commit interval can be controlled using the --repl-svc-applier-block-commit-interval option to tpm, or through the blockCommitInterval.
Note

The block commit parameters are supported only in applier stages; they have no effect in other stages.

Modification of the block commit interval should be made only when the commit window needs to be altered. The setting can be particularly useful in heterogeneous deployments where the nature and behaviour of the target database is different to that of the source extractor.

For example, when replicating to Oracle, reducing the number of transactions within commits reduces the locks and overheads:

```
shell> ./tools/tpm update alpha \
  --repl-svc-applier-block-commit-interval=500
```

This would apply two commits every second, regardless of the block commit size.

When replicating to a data warehouse engine, particularly when using batch loading, such as Vertica [in Tungsten Replicator 2.2 Manual], larger block commit sizes and intervals may improve performance during the batch loading process:

```
shell> ./tools/tpm update alpha \
  --repl-svc-applier-block-commit-size=100000 \n  --repl-svc-applier-block-commit-interval=60s
```

This sets a large block commit size and interval enabling large batch loading.

11.5. Connector Memory Management

The memory model within the Tungsten Connector works as follows:

- Memory consumption consists of the core memory, plus the buffered memory used for each connection.
- Each connection uses the maximum size of an `INSERT`, `UPDATE`, or `SELECT`, up to the configured size of the MySQL `max_allowed_packet` parameter.

For example, with 1000 concurrent connections, and a result or insert size of 1 MB, the memory usage will be 1 GB.

The default setting for the Tungsten Connector memory size is 256 MB. The memory allocation can be increased using `tpm update` and the `--conn-java-mem-size` option:

For example, during installation:

```
shell> tpm install ... --conn-java-mem-size=1024
```

Or to update using `tpm update`:

```
shell> tpm update ... --conn-java-mem-size=1024
```
Appendix A. Troubleshooting

The following sections contain both general and specific help for identifying, troubleshooting and resolving problems. Key sections include:

- General notes on contacting and working with support and supplying information, see Section A.1, “Contacting Support”.
- Error/Cause/Solution guidance on specific issues and error messages, and how the reason can be identified and resolved, see Section A.2, “Error/Cause/Solution”.
- Additional troubleshooting for general systems and operational issues.

A.1. Contacting Support

The support portal may be accessed at https://continuent.zendesk.com.

Continuent offers paid support contracts for Continuent Tungsten and Tungsten Replicator. If you are interested in purchasing support, contact our sales team at sales@continuent.com.

A.1.1. Support Request Procedure

Please use the following procedure when requesting support so we can provide prompt service. If we are unable to understand the issue due to lack of required information, it will prevent us from providing a timely response.

1. Please provide a clear description of the problem
2. Which environment is having the issue? [Prod, QA, Dev, etc.]
3. What is the impact upon the affected environment?
4. Identify the problem host or hosts and the role [master, slave, etc]
5. Provide the steps you took to see the problem in your environment
6. Upload the resulting zip file from tpm diag, potentially run more than once on different hosts as needed. Alternatively, use the tungsten_send_diag command.
7. Provide steps already taken and commands already run to resolve the issue
9. Have you checked the Continuent documentation? https://docs.continuent.com
10. Have you checked our general knowledge base? For our Error/Cause/Solution guidance on specific issues and error messages, and how the reason can be identified and resolved, see Section A.2, “Error/Cause/Solution”.

A.1.2. Creating a Support Account

You can create a support account by logging into the support portal at https://continuent.zendesk.com. Please use your work email address so that we can recognize it and provide prompt service. If we are unable to recognize your company name it may delay our ability to provide a response.

Be sure to allow email from helpdesk@continuent.com and notifications-helpdesk@continuent.com. These addresses will be used for sending messages from Zendesk.

A.1.3.Generating Diagnostic Information

To aid in the diagnosis of issues, a copy of the logs and diagnostic information will help the support team to identify and trace the problem. There are two methods of providing this information:

- Using tpm diag

The tpm diag command will collect the logs and configuration information from the active installation and generate a Zip file with the diagnostic information for all hosts within it. The command should be executed from the staging directory. Use tpm query staging to determine this directory:

```
shell: tpm query staging
  tungsten@host1:/home/tungsten/continuent-tungsten-2.0.5-11
shell: cd /home/tungsten/continuent-tungsten-2.0.5-11
shell: ./tools/tpm diag
```
Troubleshooting

The process will create a file called `tungsten-diag-2014-03-20-10-21-29.zip`, with the corresponding date and time information replaced. This file should be included in the reported support issue as an attachment.

For a staging directory installation, `tpm diag` will collect together all of the information from each of the configured hosts in the cluster. For an INI file based installation, `tpm diag` will connect to all configured hosts if `ssh` is available. If a warning that `ssh` is not available is generated, `tpm diag` must be run individually on each host in the cluster.

- Manually Collecting Logs

  If `tpm diag` cannot be used, or fails to return all the information, the information can be collected manually:

  1. Run `tpm reverse` on all the hosts in the cluster:

      ```
      shell> tpm reverse
      ```

  2. Collect the logs from each host. Logs are available within the `service_logs` directory. This contains symbolic links to the actual log files. The original files can be included within a `tar` archive by using the `-h` option. For example:

      ```
      shell> cd /opt/continuent
      shell> tar zcfh host1-logs.tar.gz ./service_logs
      ```

      The `tpm reverse` and log archives can then be submitted as attachments with the support query.

A.1.4. Open a Support Ticket

Login to the support portal and click on ‘Submit a Request’ at the top of the screen. You can access this page directly at https://continuent.zendesk.com/requests/new.

A.1.5. Open a Support Ticket via Email

Send an email to helpdesk@continuent.com from the email address that you used to create your support account. You can include a description and attachments to help us diagnose the problem.

A.1.6. Getting Updates for all Company Support Tickets

If multiple people in your organization have created support tickets, it is possible to get updates on any support tickets they open. You should see your organization name along the top of the support portal. It will be listed after the Check Your Existing Requests tab.

To see all updates for your organization, click on the organization name and then click the Subscribe link.

If you do not see your organization name listed in the headers, open a support ticket asking us to create the organization and list the people that should be included.

A.1.7. Support Severity Level Definitions

Summary of the support severity levels with initial response targets:

- **Urgent**: initial response within an hour

  Represents a reproducible emergency condition [i.e. a condition that involves either data loss, data corruption, or lack of data availability] that makes the use or continued use of any one or more functions impossible. The condition requires an immediate solution. Continuent guarantees a maximum one (1) hour initial response time. Continuent will continue to work with Customer until Customer’s database is back in production. The full resolution and the full root cause analysis will be provided when available.

- **High**: initial response within four (4) hours

  Represents a reproducible, non-emergency condition [i.e. a condition that does not involve either data loss, data corruption or lack of database availability] that makes the use or continued use of any one or more functions difficult, and cannot be circumvented or avoided on a temporary basis by Customer. Continuent guarantees a maximum four (4) hours initial response time.

- **Normal**: initial response within one (1) business day

  Represents a reproducible, limited problem condition that may be circumvented or avoided on a temporary basis by Customer. Continuent guarantees a maximum one (1) business day initial response time.

- **Low**: no guaranteed initial response interval

  Represents minor problem conditions or documentation errors that are easily avoided or circumvented by Customer. Additional request for new feature suggestions, which are defined as new functionality in existing product, are also classified as low severity level. Continuent
Troubleshooting

does not guarantee any particular initial response time, or a commitment to fix in any particular time frame unless Customer engages Continuent for professional services work to create a fix or a new feature.

A.1.8. Generating Advanced Diagnostic Information

To aid in the diagnosis of difficult issues, below are tools and procedures to assist in the data collection.

Warning

ONLY execute the below commands and procedures when requested by Continuent support staff.

Manager Memory Usage Script

We have provided a script to easily tell us how much memory a given manager is consuming.

Place the script on all of your manager hosts (i.e. into the tungsten OS user home directory).

Note

The script assumes that `cctrl` is in the path. If not, then change the script to provide a full path for cctrl.

Manager Thread Dump Procedure

This procedure creates a Manager memory thread dump for detailed analysis.

Run this command on manager hosts when requested by Continuent support.

This will append the detailed thread dump information to the log file named `tmsvc.log` in the `/opt/continuent/tungsten/tungsten-manager/log` directory.

Manager Heap Dump Procedure

This procedure creates a Manager memory heap dump for detailed analysis.

Run this command on manager hosts when requested by Continuent support.

This will create a file named `{hostname}.hprof` in the directory where you run it.

Configuring Connector Debug Logging

This procedure allows the Connector to be configured for debug logging.

Perform this procedure on Connector hosts when requested by Continuent support.

Warning

Enabling Connector debug logging will decrease performance dramatically. Disk writes will increase as will disk space consumption. Do not use in production environments unless instructed to do so by Continuent support. In any case, run in this mode for as short a period of time as possible - just long enough to gather the needed debug information. After that is done, disable debug logging.
Troubleshooting

To enable debug logging, edit the Connector configuration file `tungsten-connector/conf/log4j.properties` and uncomment two lines. For example:

```
shell> su - tungsten
shell> vi /opt/continuent/tungsten/tungsten-connector/conf/log4j.properties
Uncomment these two lines:
#log4j.logger.org.continuent.myosotis=debug, stdout
#log4j.additivity.org.continuent.myosotis=false
so they look like this:
log4j.logger.org.continuent.myosotis=debug, stdout
log4j.additivity.org.continuent.myosotis=false
shell> connector reconfigure
```

**Warning**
When disabling debug logging, DO NOT comment the lines out! Instead replace `debug` with `info`.

To disable debug logging, edit the Connector configuration file `tungsten-connector/conf/log4j.properties` and change the keyword `debug` to `info` on for the single key `log4j.logger.org.continuent.myosotis`.

For example, this is how it should look when the edit to disable is completed:

```
shell> vi /opt/continuent/tungsten/tungsten-connector/conf/log4j.properties
... log4j.logger.org.continuent.myosotis.info, stdout ...
shell> connector reconfigure
```

### Configuring Connector Verbose Debug Logging

This procedure allows the Connector to be configured for verbose debug logging (and we mean VERBOSE).

Perform this procedure on Connector hosts when requested by Continuent support.

**Warning**
Enabling Connector verbose debug logging will decrease performance dramatically. Disk writes will increase as will disk space consumption. Do not use in production environments unless instructed to do so by Continuent support. In any case, run in this mode for as short a period of time as possible - just long enough to gather the needed debug information. After that is done, disable debug logging.

To enable verbose debug logging (and we mean VERBOSE), edit the Connector log configuration file `tungsten-connector/conf/log4j.properties` and ADD two lines. For example:

```
shell> su - tungsten
shell> vi /opt/continuent/tungsten/tungsten-connector/conf/log4j.properties
log4j.logger.org.continuent.myosotis.protocol.mysql.MySQLProtocolHandler=trace, stdout
log4j.additivity.org.continuent.myosotis.protocol.mysql.MySQLProtocolHandler=false
shell> connector reconfigure
```

**Warning**
When disabling verbose debug logging, DO NOT comment the lines out! Instead replace `trace` with `info`.

To disable verbose debug logging, edit the Connector log configuration file `tungsten-connector/conf/log4j.properties` and change the keyword `trace` to `info` for the single key `log4j.logger.org.continuent.myosotis.protocol.mysql.MySQLProtocolHandler`.

For example, this is how it should look when the edit to disable is completed:

```
shell> vi /opt/continuent/tungsten/tungsten-connector/conf/log4j.properties
... log4j.logger.org.continuent.myosotis.protocol.mysql.MySQLProtocolHandler=info, stdout ...
shell> connector reconfigure
```

### Configuring Connector Debug Logging via the Manager

This procedure allows the Manager to be configured to enable Connector-specific debug logging in the manager logs.
Perform this procedure on Manager hosts when requested by Continuent support.

**Warning**

Enabling Manager-based Connector debug logging will decrease performance. Disk writes will increase as will disk space consumption. Do not use in production environments unless instructed to do so by Continuent support. In any case, run in this mode for as short a period of time as possible - just long enough to gather the needed debug information. After that is done, disable debug logging.

To enable Manager-based Connector debug logging, edit the Manager log configuration file `tungsten-manager/conf/log4j.properties` and ADD two lines. For example:

```shell
su - tungsten
vi /opt/continuent/tungsten/tungsten-manager/conf/log4j.properties
log4j.logger.com.continuent.tungsten.manager.router.gateway.RouterGatewayProxy=DEBUG, stdout
log4j.additivity.com.continuent.tungsten.manager.router.gateway.RouterGatewayProxy=false
manager restart
```

**Warning**

When disabling Manager-based Connector debug logging, DO NOT comment the lines out! Instead replace `DEBUG` with `info`.

To disable Manager-based Connector debug logging, edit the Manager log configuration file `tungsten-manager/conf/log4j.properties` and change the keyword `DEBUG` to `info` for the single key `log4j.logger.com.continuent.tungsten.manager.router.gateway.RouterGatewayProxy`.

For example, this is how it should look when the edit to disable is completed:

```shell
vi /opt/continuent/tungsten/tungsten-manager/conf/log4j.properties
log4j.logger.com.continuent.tungsten.manager.router.gateway.RouterGatewayProxy=info, stdout
manager restart
```

**A.2. Error/Cause/Solution**

**A.2.1. Lots of entries added to replicator log**

*Last Updated: 2015-06-01*

**Condition or Error**

The logging level used by Continuent Tungsten creates a lot of entries, including `WARN`, this generates a lot of information that is difficult to find the real errors and problems. How do i change the logging level?

**Causes**

- By default, Continuent Tungsten reports a lot of information and detail, including `INFO` and other levels of detail that may generate a lot of information. For example:

Ignoring query : No schema found for this query from event 4020717251 (SET @current_db_user := NULL...)```

**Rectifications**
The logging level used to report status and other information, and that is written into the log, can be changed to reduce or lower the reporting level. To do this:

1. Edit the `~tungsten_home/tungsten/tungsten-replicator/conf/log4j.properties`
2. Find the following line:
   
   ```log4j.logger.com.continuent.tungsten.replicator.filter.ReplicateFilter=DEBUG, stdout```

   This will change the logging level so that only entries at `DEBUG` and higher will be output.

### A.2.2. Error: could not settle on encryption_client algorithm

**Last Updated: 2015-06-01**

**Condition or Error**

The following error is reported when trying to connect:

```
Error: could not settle on encryption_client algorithm
```

**Causes**

- Can be due to missing an acceptable cipher on any one of the hosts.

**Rectifications**

- This is a list of acceptable ciphers:

  ```
aes128-cbc
daes-cbc
blowfish-cbc
cast128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
idea-cbc
none
arcfour128
arcfour256
```

These can be configured in `/etc/ssh/sshd_config` under Ciphers.

Try adding a supported cipher (e.g., `aes256-cbc`) to the end of the ciphers in your ssh server config file. Note that SSH and OpenSSL ciphers are mapped, for example like the following:

```java
// Maps the SSH name of a cipher to its corresponding OpenSSL name
SSH_TO_OSSL = {
    "3des-cbc" => "des-ede3-cbc",
    "blowfish-cbc" => "bf-cbc",
    "aes128-cbc" => "aes-128-cbc",
    "aes192-cbc" => "aes-192-cbc",
    "aes256-cbc" => "aes-256-cbc",
    "idea-cbc" => "idea-cbc",
    "rc4" => "rc4",
    "none" => "none"
}
```

### A.2.3. The master replicator stopped with a JDBC error.

**Last Updated: 2015-06-01**

**Condition or Error**

The master replicator stopped with a JDBC error.

**Causes**

- The error log may show a more detailed failure with the JDBC error message:

```
INFO | jvm 1 | 2016/02/08 17:16:24 | 2016-02-08 17:16:24,627 [qktdb - pool-2-thread-1] ERROR management.tungsten.TungstenPlugin Unable to start replication service due to underlying error
INFO | jvm 1 | 2016/02/08 17:16:24 | java.lang.NumberFormatException: For input string: "0000002417562130"
INFO | jvm 1 | 2016/02/08 17:16:24 | at java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)
```
The underlying reason for the error is that MySQL has created a binlog over 2GB and the replicator could not process the event due to the limit of a Java integer.

**Rectifications**

- The solution for this error, if the log is a rotate event (use `mysqlbinlog`) is to reposition the replicator using `tungsten_set_position`.

A.2.4. ERROR backup.BackupTask Backup operation failed: null

Last Updated: 2019-01-11

**Condition or Error**

A full Xtrabackup backup has failed, and left the datasource's replicator offline.

**Causes**

- A common cause of this failure is the existence of zero-length `store-* .properties` files in the `backups/{serviceName}` directory.

**Rectifications**

- Simply remove any zero-byte `store-* .properties` files from the `backups/{serviceName}` directory and retry the backup.

A.2.5. Event application failed: seqno=20725782 fragno=0 message=java.sql.SQLDataException: Data too long for column 'eventid' at row 1

Last Updated: 2013-11-01

**Condition or Error**

Event application failed: seqno=20725782 fragno=0 message=java.sql.SQLDataException: Data too long for column 'eventid' at row 1

**Causes**

- The issue is that the eventid column in tungsten.heartbeat is shorter than tungsten.eventid. You could do an alter on the master to extend that column and let that replicate out. The column sizes match in the next version.

**Rectifications**

- The tables must be updated:

  ```sql
  mysql> ALTER TABLE `heartbeat` CHANGE `eventid` `eventid` VARCHAR( 128 ) CHARACTER SET utf8 COLLATE utf8_general_ci NULL DEFAULT NULL;
  ```

  This will update the tables from the following structure:

  ```sql
  mysql> SHOW CREATE TABLE tungsten.heartbeat;
  heartbeat | CREATE TABLE `heartbeat` ( `id` bigint(20) NOT NULL DEFAULT '0', `seqno` bigint(20) DEFAULT NULL, `eventid` varchar(32) DEFAULT NULL, `source_timestamp` timestamp NULL DEFAULT NULL, `target_timestamp` timestamp NULL DEFAULT NULL, `lag_millis` bigint(20) DEFAULT NULL, `salt` bigint(20) DEFAULT NULL, name varchar(128) DEFAULT NULL, PRIMARY KEY (`id`) ) ENGINE=InnoDB AUTO_INCREMENT=1 DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
  ```
A.2.6. Unable to update the configuration of an installed directory

Last Updated: 2013-08-07

Condition or Error

Running an update or configuration with tpm returns the error ‘Unable to update the configuration of an installed directory’

Causes

• Updates to the configuration of a running cluster must be performed from the staging directory where Continuent Tungsten was originally installed.

Rectifications

• Change to the staging directory and perform the necessary commands with tpm. To determine the staging directory, use:

  shell> tpm query staging

Then change to the staging directory and perform the updates:

  shell> ./tools/tpm configure ....

More Information

Chapter 2, Deployment

A.2.7. [S1000][unixODBC][MySQL][ODBC 5.3[w) Driver]SSL connection error: unknown error number [ISQL]ERROR: Could not SQLConnect

Last Updated: 2015-06-01

Condition or Error

We have a new server dedicated to Zabbix monitoring. Zabbix uses an ODBC connection for MySQL. When we try to connect to a Tungsten connector from the new server using ODBC we receive an error:

[S1000][unixODBC][MySQL][ODBC 5.3[w) Driver]SSL connection error: unknown error number [ISQL]ERROR: Could not SQLConnect

Causes

• The underlying cause is related to an SSL or encryption error, either the certificate is wrong, or the ciphers being used are not supported.

Examine the connector.log on the Tungsten server we are connecting to returns an error with each attempt:

INFO | jvm 1 | 2016/05/20 13:07:17 | WARN [MySQLProtocolHandler] - [172.16.0.120:43571] Error during transfer of authentication packet: no cipher suite
Troubleshooting

Connecting from to the new server using the mysql client may work:

```bash
[root@zabbix etc]# mysql -uzabbix -pZ@bbix487sql -hnas-db-ct01-a.safemls.net
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 40019
Server version: 5.6.20-68.0-log tungsten Percona Server (GPL), Release 68.0, Revision 656
```

Connecting directly MySQL database on port 13306 using the ODBC connection may also work:

```bash
[root@zabbix etc]# isql -v ct01
+---------------------------------------+
| Connected! |
|             |
| sql-statement |
| help [tablename] |
| quit |
|             |
+---------------------------------------+
```

Rectifications

- **zabbix** is trying to connect to the connector with SSL encryption, but the SSL is not operating. The easiest way to bypass this is disable SSL connections for ODBC. Add the following entry in `odbc.ini` (under the section for the host you're testing):

  ```
  useSSL = No
  ```

### A.2.8. Connector shows errors with "java.net.SocketException: Broken pipe"

**Last Updated: 2013-11-01**

**Condition or Error**

When using DirectReads, the connector reports errors with a broken pipe.

**Causes**

- The most likely culprit for this error is that the `wait_timeout` and/or `interactive_timeout` is too low. This causes a problem because pooled connections get timeouts and are closed by the MySQL server.

**Rectifications**

- Change the configuration for your MySQL server [in my.cnf] to increase these timeouts.

### A.2.9. cctrl reports MANAGER(state=STOPPED)

**Last Updated: 2013-11-01**

**Condition or Error**

`cctrl` reports the status for the manager as `MANAGER(state=STOPPED)`

**Causes**

- The manager has stopped running, possibly due to a fault or error state.

**Rectifications**

- Restart the manager process on this server is not running. You can start it by running:
  ```
  shell> manager start
  Or:
  shell> /opt/continuent/tungsten/tungsten-manager/bin/manager start
  ```

**More Information**

Section 4.2.3, “Restarting the Manager Service”

### A.2.10. Backup agent name not found: xtrabackup-full

**Last Updated: 2015-06-01**
Troubleshooting

Condition or Error
A backup was taken with \texttt{xtrabackup-full} from the master. Slave appears to not be configured for \texttt{xtrabackup-full}, which results in there being issues with the restore. How can we configure the slave to use \texttt{xtrabackup-full} for restore?

Causes
- The underlying cause and indication is that the \texttt{xtrabackup} has not been installed properly on the slave, or not installed at all, at the point when Continuent Tungsten was being installed. The following will be seen in the status output after a failed restore:

  ```
  minimumStoredSeqNo : -1
  offlineRequests : NONE
  pendingError : Unable to spawn restore request
  pendingErrorCode : NONE
  pendingErrorEventId : NONE
  pendingErrorSeqno : -1
  pendingExceptionMessage: Backup agent name not found: xtrabackup-full
  ```

  Probably the other hosts didn't require this setting specifically because xtrabackup was installed and detected when Continuent Tungsten was installed on them.

Rectifications
- The steps you need are:
  1. Install \texttt{xtrabackup} if not already installed on the slave in question
  2. If using the INI configuration method, add the line below to \texttt{/etc/tungsten/tungsten.ini}:

    ```
    backup-method=xtrabackup-full
    ```

    And then run \texttt{tpm update} on that slave host to update the configuration.

    Or if using staging method, update the configuration using:

    ```
    shell> tpm update --backup-method=xtrabackup-full
    ```

A.2.11. Replicator runs out of memory

Last Updated: 2016-05-18

Condition or Error
The replicator runs out of memory, triggers a stack trace indicator a memory condition, or the replicator fails to extract the transaction information from the MySQL binary log.

Causes
- The replicator operates by extracting (or applying) an entire transaction. This means that when extracting data from the binary log, and writing that to THL, or extracting from the THL in preparation for applying to the target, the entire transaction, or an entire statement within a multi-statement transaction, must be held in memory.

  In the event of a very large transaction having to be extracted, this can cause a problem with the memory configuration. The actual configuration of how much memory is used is determined through a combination of the number of fragments, the size of the internal buffer used to store those fragments, and the overall fragment size.

Rectifications
- Although you can increase the overall memory allocated to the replicator, changing the internal sizes used can also improve the performance and ability to extract data.

  First, try reducing the size of the buffer \texttt{replicator.global.buffer.size} used to hold the transaction fragments. The default for this value is 10, but reducing this to 5 or less will ease the required memory:

  ```
  replicator.global.buffer.size=10
  ```

  Altering the size of each fragment can also help, as it reduces the memory required to hold the data before it is written to disk and sent out over the network to slave replicators. Reducing the fragment size will reduce the memory footprint. The size is controlled by the \texttt{replicator.extractor.dbms.transaction_frag_size} parameter:

  ```
  replicator.extractor.dbms.transaction_frag_size=1000000
  ```

  Note that if you change the fragment size, you may need to reset the service on the extractor so that the binary log is parsed again. You can reset the service by using the \texttt{trepctl reset} command.
A.2.12. Replicator fails to connect after updating password

Last Updated: 2013-11-01

Condition or Error

Tungsten Replicator fails to connect after changing the tungsten user password.

Causes

- The most likely cause is that the configuration within ~/.my.cnf was forcing a connection to the cluster as tungsten user, and user change may have only been made on one host and not replicated to the other MySQL servers.

Rectifications

- First, update the credentials in ~/.my.cnf and ensure you can connect to all the slaves with the updated credentials.

Also check that tpm has been configured with the right password and that all servers have the right information. Errors such as:

```
ERROR>>host1>>Unable to connect to the MySQL server using »tungsten@host1:3306 (WITH PASSWORD) (MySQLLoginCheck)
```

Indicate that the password may not have been replicated properly. Check the following:

1. Check the user configuration information within each MySQL server and compare the values:

   ```
   mysql> select * from mysql.user where user='tungsten';
   ```

2. For any node that is not up to date, update the password manually:

   ```
   shell> mysql -u root -ppassword -P 3306 -h host1
   mysql> UPDATE `mysql`.`user` SET Password=PASSWORD('secret') WHERE User='tungsten';
   mysql> flush privileges;
   ```

3. Update the tpm and Continuent Tungsten configuration:

   ```
   shell> ./tools/tpm update alpha --datasource-password=secret
   ```

4. Restart the replicators:

   ```
   shell> replicator restart
   ```

Then put the replicators offline/online to refresh the configuration:

```
[LOGICAL] /alpha > datasource host1 offline
Datasource 'host1@alpha' is now OFFLINE
[LOGICAL] /alpha > datasource host1 online
Setting server for data source 'host1' to READ-ONLY
```

A.2.13. Attempt to write new log record with equal or lower fragno: seqno=3 previous stored fragno=32767 attempted new fragno=-32768

Last Updated: 2016-05-18

Condition or Error

The number of fragments in a single transaction has been exceeded.

Causes

- The maximum number of fragments within a single transaction within the network protocol is limited to 32768. If there is a very large transaction that exceeds this number of fragments, the replicator can stop and be unable to continue. The total transaction size is a combination of the fragment size (default is 1,000,000 bytes, or 1MB), and this maximum number (approximately 32GB).

Rectifications

- It is not possible to change the number of fragments in a single transaction, but the size of each fragment can be increased to handle much larger single transactions. To change the fragment size, configure the replicator.extractor.dbms.transaction_frag_size parameter. For example, by doubling the size, a transaction of 64GB could be handled:

  ```
  replicator.extractor.dbms.transaction_frag_size=2800000
  ```
If you change the fragment size in this way, the service on the extractor must be reset so that the transaction can be reprocessed and the binary log is parsed again. You can reset the service by using the `trepctl reset` command.

A.2.14. ORA-00257: ARCHIVER ERROR. CONNECT INTERNAL ONLY, UNTIL FREED

Last Updated: 2016-04-20

Condition or Error

It is possible for the Oracle server to get into a state where Continuent Tungsten is online, and with no other errors showing in the log. However, when logging into the Oracle server an error is returned:

ORA-00257: ARCHIVER ERROR. CONNECT INTERNAL ONLY, UNTIL FREED

Causes

- This is a lack of resources within the Oracle server, and not an issue with Continuent Tungsten.

Rectifications

- The issue can be addressed by increasing the logical size of the recovery area, by connecting to the Oracle database as the system user and running the following command:

  ```
  sqlplus sys/oracle as sysdba
  SQL>
  ALTER SYSTEM SET db_recovery_file_dest_size = 80G;
  ```

A.2.15. ERROR 1010 [HY000] at line 5094506: Error dropping database (can't rmdir './mysql-bin/', errno: 17)

Last Updated: 2013-11-01

Condition or Error

Loading a `mysqldump` into a MySQL server from a backup/restore fails.

Causes

- The problem may be that your MySQL binary logs are in a subdirectory of your MySQL `data` directory, causing MySQL to view them as a schema.

Rectifications

- Possible steps to resolution:
  1. Modify the dump file so it isn't trying to drop a schema named after the bin log directory
  2. Update the mysql configuration so the bin logs aren't in a directory in the data dir. mysql sees all directories in the data dir as a schema

A.2.16. ERROR >> host1 >> can't alloc thread

Last Updated: 2019-03-04

Condition or Error

tpm installation fails with this error

Causes

- Most common occurrence of this error is often attributed to OS permissions.

Rectifications

- Review Section C.2.3, "Directory Locations and Configuration"
  - Ensure all installation paths are owned by the correct OS user
  - Ensure OS user configured with correct sudo rights
A.2.17. ERROR 1580 [HY000] at line 5093787: You cannot ‘DROP’ a log table if logging is enabled

Last Updated: 2013-11-01

Condition or Error

Loading a mysqldump into a MySQL server from a backup/restore fails.

Causes

• This appears to be a bug in MySQL that causes mysqldump loads to fail.

Rectifications

• You should be able to import the dump by switching off the slow query log globally before running the import:

  mysql> SET GLOBAL slow_query_log=0

A.2.18. ERROR 2013 [HY000] at line 583: Lost connection to MySQL server during query

Last Updated: 2013-11-01

Condition or Error

Client was disconnected during a query with the error number.

Causes

• Usually this means that the MySQL server has closed the connection or the server has restarted. The exact cause will be more difficult to determine.

Rectifications

• We need a bit more information to provide assistance.
  1. Were you connected through the Tungsten Connector?
  2. Did anything else happen on the servers?
  3. If you were connected through the Tungsten Connector, please upload the tungsten-connector/log/connector.log file from the server you were connected to.

A.2.19. pendingExceptionMessage": "Unable to update last commit seqno: Incorrect datetime value: '2016-03-13 02:02:26' for column 'update_timestamp' at row 1

Last Updated: 2015-06-01

Condition or Error

The following error is reported when applying an event:

  pendingExceptionMessage": "Unable to update last commit seqno: Incorrect datetime value: '2016-03-13 02:02:26' for column 'update_timestamp' at row 1

Causes

• The underlying reason for this error is the format and value of the datetime value that is being represented are either incompatible with the current SQL mode within MySQL, or the datetime combination is one that occurs during a DST switch, which may be incompatible with the SQL mode.

Rectifications

• The solution is to update the SQL mode so that explicit changes are ignored when applying the data, rather than using the information defined during the session. To update the settings. Because the problem will be short lived and specific to the data being applied it can be done temporarily:
  • Edit file /opt/continuent/tungsten/tungsten-replicator/conf/static-endtest.properties
  • Find this line:
Troubleshooting

replicator.applier.dbms.ignoreSessionVars=autocommit

- Change the line to:
replicator.applier.dbms.ignoreSessionVars=autocommit|sql_mode
- Restart the replicator using:
shell> replicator restart
- Wait for the replicator to come online, and process the change that originally caused the problem. Once the data has been replicated, revert the settings in the file back to the old value and restart the replicator again.

A.2.20. Too many open processes or files

Last Updated: 2013-10-09

Condition or Error

The operating system or environment reports that the tungsten or designated Continuent Tungsten user has too many open files, processes, or both.

Causes

- User limits for processes or files have either been exhausted, or recommended limits for user configuration have not been set.

Rectifications

- Check the output of ulimit and check the configure file and process limits:

```
shell> ulimit -a
core file size (blocks, -c) 0
data seg size (kbytes, -d) unlimited
file size (blocks, -f) unlimited
max locked memory (kbytes, -l) unlimited
max memory size (kbytes, -m) unlimited
open files (-n) 256
pipe size (512 bytes, -p) 1
stack size (kbytes, -s) 8192
cpu time (seconds, -t) unlimited
max user processes (-u) 709
virtual memory (kbytes, -v) unlimited
```

If the figures reported are less than the recommended settings, see Section C.2.1, "Creating the User Environment" for guidance on how these values should be changed.

More Information

Section C.2.1, "Creating the User Environment"


Last Updated: 2017-02-15

Condition or Error

Connections to MySQL through the connector report KeepAliveTimerTask errors in the connector.log file.

Causes

- Possible causes include local scripts that kill stale connections after some fixed period of time, or the wait_timeout was changed without restarting the connector, or a bug that was fixed in v4.0.3

Rectifications

- Upgrade to the latest version if you are running a version below 4.0.3
- Check for local scripts that are killing connections
- Restart the Connector
A.2.22. Latency is high: master:ONLINE, progress=41331580333, THL latency=78849.733

Condition or Error
Latency is high: master:ONLINE, progress=41331580333, THL latency=78849.733

Causes
- There are many possible causes for this error, however, if you see the following within the log on the master it may indicate a specific issue:

```
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.replicator.thl.CommitSeqnoTable.updateLastCommitSeqno(CommitSeqnoTable.java:548)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.replicator.thl.CatalogManager.updateCommitSeqnoTable(CatalogManager.java:223)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.replicator.thl.THL.updateCommitSeqno(THL.java:593)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.replicator.thl.THLStoreApplier.apply(THLStoreApplier.java:163)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.trep.replicator.pipeline.SingleThreadStageTask.apply(SingleThreadStageTask.java:163)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.trep.replicator.pipeline.SingleThreadStageTask.runTask(SingleThreadStageTask.java:163)
INFO | jvm 1 | 2016/02/09 15:01:54 | at com.continuent.tungsten.trep.replicator.pipeline.SingleThreadStageTask.run(SingleThreadStageTask.java:176)
INFO | jvm 1 | 2016/02/09 15:01:54 | at java.lang.Thread.run(Thread.java:745)
```

The stack trace shows that the replicator is updating the trep_commit_seqno table which is normally a very fast operation.

The underlying reason may either be:
- It is possible that updates to MySQL are somehow getting delayed, which would slow down the operation of the replicator as it updates each status update.
- Check the block commit size, as low values will increase the number of updates to the table, and if the MySQL server updates are slow, this in turn slows down the operation of the replicator.

Rectifications
- Focus on making sure the IO system and MySQL commits are not being blocked.

You can try increasing `replicator.stage.q-to-thl.blockCommitRowCount` so the replicator has less commits to MySQL on the master.

You can continue to track progress through `trepctl status -name tasks` as you may see the `appliedLastSeqno` value updating less often if you increase this by a lot. Beware that increasing this value too much increases possible data loss since it creates less sync points with the slaves.

A.2.23. Triggers not firing correctly on slave

Condition or Error
Newly created triggers are not firing when executed

Causes
- If a new user (definer) was used to create the triggers, they may fail to be executed, raising the following warning in the logs:

```
INFO | jvm 1 | 2013/10/16 04:21:33 | WARNING: Could not execute query »
org.drizzle.jdbc.internal.common.query.DrizzleQuery@60dc4c81: The »
MySQL server is running with the --read-only option so it cannot »
execute this statement
```

This is an indication that the new definer does not have the required `SUPER` privilege and that a trigger is failing to run.

Rectifications
- In order to fix this issue, the new definer should be given the `SUPER` privilege on each server and then replication should be restarted. The `SUPER` privilege allows the user to run a statement on a slave server where the read_only flag has been turned on. If necessary, the scope of

440
the privilege can be restricted to an individual schema. The `GRANT` statement should be done on every database server, while the shun and recover should only be done on the slaves.

```sql
mysql> grant SUPER on *.* to user;
mysql> flush privileges;
```

Within `cctrl`

```cctrl>
datasource hostname shun;
cctrl> datasource hostname recover;
```

You should continue to review the `tungsten-replicator/log/trepsvc.log` file to see what log messages are being written there. It appears that replication is still failing and it is probably related to the same issue. If you want us to review logs to interpret the results for you, you can upload the log file here and someone will look at it.

More Information

Section A.3.1, “Triggers”

A.2.24. cctrl hangs

Last Updated: 2013-11-01

Condition or Error

cctrl hangs

Causes

- Within Continuent Tungsten 1.5.3 there is a known issue related to how the managers handle failed network connections. It's an indication that there was a network issue at some point.

Rectifications

- The temporary workaround is to put the cluster into maintenance mode, stop all managers, wait 10 seconds, then start them backup again.

More Information

Section 4.2.3, “Restarting the Manager Service”

A.2.25. Replication latency very high

Last Updated: 2013-11-01

Condition or Error

The latency of updates on the slaves is very high

Causes

- First the reason and location of the delay should be identified. It is possible for replication data to have been replicated quickly, but applying the data changes is taking a long time. Using row-based replication may increase the latency due to the increased quantity of data that must be transferred.

Rectifications

- Check the replication format:

  ```
  shell> grep binlog_format /etc/my.cnf
  binlog_format=ROW
  ```

  Slow slaves can be the cause, but it may require some configuration changes.

A.2.26. Services requires a reset

Last Updated: 2016-05-18

Condition or Error

The replicator service needs to be reset, for example if your MySQL service has been reconfigured, or when resetting a data warehouse or batch loading service after a significant change to the configuration.
Troubleshooting

Causes

- If the replicator stops replicating effectively, or the configuration and/or schema of a source or target in a datawarehouse loading solution has changed significantly. This will reset the service, starting extraction from the current point, and the target/slave from the new master position. It will also reset all the positions for reading and writing.

Rectifications

- To reset a service entirely, without having to perform a re-installation, you should follow these steps. This will reset both the THL, source database binary log reading position and the target THL and starting point.

1. Take the slave offline:
   ```
   slave-shell> trepctl offline
   ```

2. Take the master offline:
   ```
   slave-shell> trepctl offline
   ```

3. Use `trepctl` to reset the service on the master and slave. You must use the service name explicitly on the command-line:
   ```
   master-shell> trepctl -service alpha reset -y
   ```
   ```
   slave-shell> trepctl -service alpha reset -y
   ```

4. Put the slave online:
   ```
   slave-shell> trepctl offline
   ```

5. Put the master online:
   ```
   slave-shell> trepctl offline
   ```

A.2.27. `trepctl` status hangs

Last Updated: 2013-11-01

Condition or Error

`trepctl status` hangs at the end of the output after a “cannot fork” error due.

Causes

- This can be caused by THL corruption

Rectifications

- You should recreate the THL files on the slave. This can be achieved by deleting the existing THL files, which will cause the slave replicator to download all of the THL data from the master again:

  ```
  shell> replicator stop
  shell> cd /opt/continuent
  shell> mv thl thl.old;
  shell> mkdir thl
  shell> replicator start
  shell> trepctl status
  ```

A.2.28. element 'mysql_readonly' not found in path

Last Updated: 2015-06-01

Condition or Error

We are getting the following INFO message in the `tmsvc.log` every few seconds (host1 is the Master), logs attached:

```
INFO | jvm 1 | 2016/03/04 15:09:38 | |host1 |
INFO | jvm 1 | 2016/03/04 15:09:38 | +----------------------------------------------------------------------------+
INFO | jvm 1 | 2016/03/04 15:09:38 | |element 'mysql_readonly' not found in path |
INFO | jvm 1 | 2016/03/04 15:09:38 | |'/podsjqe/sjqedb1/conf/service/' while searching for entry |
INFO | jvm 1 | 2016/03/04 15:09:38 | +----------------------------------------------------------------------------+
``` 

Causes

- This is caused by the manager
Rectifications

• To prevent INFO messages being reported in the `/opt/continuent/tungsten/tungsten-manager/log/tmsvc.log` file:
  1. Put the cluster into `MAINTENANCE` mode
  2. Stop all managers
  3. Start all managers starting with the master
  4. Put the cluster into `AUTOMATIC` mode

A.2.29. Starting replication after performing a restore because of an invalid restart sequence number

Last Updated: 2013-11-01

Condition or Error

Starting replication fails because of an invalid restart sequence number. Checking the sequence number, `trep_commit_seqno` shows an empty or invalid table contents:

```
mysql> select * from tungsten.trep_commit_seqno;
+-------+--------+-----------+-----------+--------------+---------+-----------------+---------------------+
| seqno | fragno | last_frag | source_id | epoch_number | eventid | applied_latency | update_timestamp     |
|-------+--------+-----------+-----------+--------------+---------+-----------------+---------------------+
| -1    | NULL   | NULL      | NULL      | NULL         | NULL    | -1              | 2013-10-27 23:44:05 |
+-------+--------+-----------+-----------+--------------+---------+-----------------+---------------------+
1 row in set (0.00 sec)
```

Causes

• The restore may have failed to correctly restore the `tungsten` tables.

Rectifications

• Retry the restore process, making sure the replicator is stopped and there are no updates to the table taking place:
  1. Ensure no replicator processes are running:
```
shell> replicator stop
```
  2. Ensure the `/opt/continuent/thl` directory is empty:
```
shell> tpm reset-thl
```
  3. Restore the backup using whatever backup/restore tool you used.
  4. Check that `trep_commit_seqno` has a valid restart position in it
```
shell> replicator start
```

A.2.30. MySQL is incorrectly configured

Last Updated: 2013-11-01

Condition or Error

The configuration of MySQL was wrong; it included `autocommit=0` and the wrong `server-id`

Causes

• Pre-requisites were not followed correctly.

Rectifications

• Edit `my.cnf` and clean up. Restart MySQL if possible. Alternatively, set manually:
```
mysql> set GLOBAL autocommit=1;
Query OK, 0 rows affected (0.00 sec)
mysql> set GLOBAL server_id=2;
Query OK, 0 rows affected (0.01 sec)
```
A.2.31. Replicator reports an Out of Memory error

Condition or Error
Replicator reports an Out of Memory error
Causes
• The configured memory sizes within the replicator are too small for the data being replicated and applied.
Rectifications
• Raise the \texttt{wrapper.java.maxmemory} parameter, for example to 3072 (specified in megabytes) within \texttt{wrapper.conf} and restart the replicator.
More Information
Section F.4, "Memory Tuning and Performance"

A.2.32. Backup/Restore is not bringing my host back to normal

Condition or Error
A backup/restore was performed as requested, but the host is still not coming up.
Causes
• When you backup a node, the backup is stored on that physical server. The correct backup file from an active server should be used on the host being restored.
Rectifications
• You can use that backup to restore another server in two ways:
  • If the backup directory is shared between servers using NFS or a clustered file system, the commands will work like you tried.
  • You must copy the backup files between nodes. See Section 5.10.3, "Restoring from Another Slave" for instructions on that.

A.3. Known Issues

A.3.1. Triggers

Tungsten Replicator does not automatically shut off triggers on slaves. This creates problems on slaves when using row-based replication (RBR) as the trigger will run twice. Tungsten cannot do this because the setting required to do so is not available to MySQL client applications. Typical symptoms are duplicate key errors, though other problems may appear. Consider the following fixes:
• Drop triggers on slaves. This is practical in fan-in for reporting or other cases where you do not need to failover to the slave at a later time.
• Create an \texttt{is\_master()} function that triggers can use to decide whether they are on the master or slave.
• Use statement replication. Beware, however, that even in this case you may find problems with triggers and auto-increment keys.

The \texttt{is\_master()} approach is simple to implement. First, create a function like the following that returns false if we are using the Tungsten user, as would be the case on a slave.

\begin{verbatim}
create function is_master()
returns boolean
 deterministic
return if(substring_index(user(),'@',1) != 'tungsten',true,false);
\end{verbatim}

Next add this to triggers that should not run on the slave, as shown in the next example. This suppresses trigger action to insert into table bar except on the master.

\begin{verbatim}
delimiter //
create trigger foo_insert after insert on foo
  for each row begin
    if is_master() then
      insert into bar set id=NEW.id;
\end{verbatim}
As long as applications do not use the Tungsten account on the master, the preceding approach will be sufficient to suppress trigger operation.

A.4. Troubleshooting Timeouts

A.5. Troubleshooting Backups

- Operating system command failed
  Backup directory does not exist.

• Backup Retention

A.6. Running Out of Diskspace

The above indicates that the THL information could not be stored on disk. To recover from this error, make space available on the disk, or move the THL files to a different device with more space, then set the replicator service online again.

For more information on moving THL files to a different disk, see Section E.1.5.3, “Moving the THL File Location”; for information on moving the backup file location, see Section E.1.1.4, “Relocating Backup Storage”.

A.7. Troubleshooting SSH and tpm

When executing `tpm`, `ssh` is used to connect and install the software on other hosts in the cluster. If this fails, and the public key information is correct, there are a number of operations and settings that can be checked. Ensure that you have followed the Section C.2.2.2, “SSH Configuration” instructions.

- The most likely representation of this error will be when executing `tpm` during a deployment:

```
Error:
**********************************************************************
Validation failed
**********************************************************************
Errors for host:
**********************************************************************
ERROR>>host1>>Unable to SSH to host1 as root. (SSHLoginCheck)
Ensure that the host is running and that you can login as root via SSH using key authentication
```

Try running the following command:

```
shell> ssh tungsten@host1 sudo whoami
```

If the SSH and `sudo` configurations have been configured correctly, it should return `root`. Any other value indicates a failure to configure the prerequisites properly.

- Check that none of the profile scripts (`.profile`, `bash_profile`, `bashrc`, etc.) do not contain a call to `mesg n`. This may fool the non-interactive `ssh` call; the call to this command should be changed to only be executed on interactive shells.
if `tty -s`; then
  mesg n
fi

- Check that firewalls and/or antivirus software are not blocking or preventing connectivity on port 22.

If ssh has been enabled on a non-standard port, use the `-net-ssh-option-port` option to specify the alternative port.

- Make sure that the user specified in the `-user` to tpm is allowed to connect to your cluster nodes.

A.8. Troubleshooting Data Differences

It can sometimes become necessary to identify table and data differences due to unexpected behaviour or failures. There are a number of third party tools that can help identify and fix however a lot of them assume native replication is in place, the following explains the recommended methods for troubleshooting a Tungsten Environment based on MySQL as the source and target technologies.

A.8.1. Identify Structural Differences

If you suspect that there are differences to a table structure, a simple method to resolve this will be to compare schema DDL.

Extract DDL on the Master node, specifying the schema in place of `{DB}`:

```bash
shell> mysqldump -u root -p --no-data -h localhost --databases `{DB}` >master.sql
```

Repeat the same on the Slave node:

```bash
shell> mysqldump -u root -p --no-data -h localhost --databases `{DB}` >slave.sql
```

Now, using diff, you can compare the results

```bash
shell> diff master.sql slave.sql
```

Using the output of diff, you can then craft the necessary SQL statements to re-align your structure

A.8.2. Identify Data Differences

It is possible to use pt-table-checksum from the Percona Toolkit to identify data differences, providing you use the syntax described below for bypassing the native replication checks. First of all, it is advisable to familiarise yourself with the product by reading through the providers own documentation here:


Once you are ready, ensure you install the latest version to the persona toolkit on all nodes, next execute the following on the Master node:

```bash
shell> pt-table-checksum --set-vars innodb_lock_wait_timeout=500 \
  --recursion-method=none \n  --ignore-databases=mysql \n  --ignore-databases-regex=tungsten* \n  h=localhost,u=tungsten,p=secret
```

On first run, this will create a database called percona, and within that database a table called checksums. The process will gather checksum information on every table in every database excluding the mysql and tungsten related schemas. You can now execute the following SQL Statement on the slave to identify tables with data differences:

```sql
SELECT db, tbl, SUM(this_cnt) AS total_rows, COUNT(*) AS chunks
FROM percona.checksums
WHERE (master_cnt <> this_cnt
OR master_crc <> this_crc
OR ISNULL(master_crc) <> ISNULL(this_crc))
GROUP BY db, tbl;
```

This `SELECT` will return any tables that it detects are different, it won’t show you the differences, or indeed how many, this is just a basic check. To identify and fix the changes, you could use `pt-table-sync`, however this product would by default assume native replication and also try and fix the problems for you. In a tungsten environment this would not be recommended, however by using the `-print` switch you can gather the SQL needed to be executed to fix the mistakes. You should run this, and review the output to determine whether you want to manually patch the data together or consider using `tungsten_provision_slave` to retrovision a node in the case of large quantities of differences.

To use `pt-table-sync`, first identify the tables with differences on each slave, in this example, the `SELECT` statement above identified that there was a data difference on the departments table within the employees database on db2. Execute the `pt-table-sync` script on the master, passing in the database name, table name and the slave host that the difference exists on:
Troubleshooting

```
shell> pt-table-sync --databases employees --tables departments --print h=db1,u=tungsten,p=secret,P=13306 h=db2
```

The first `h=` option should be the Master, also the node you run the script from, the second `h=` option relates to the slave that the difference exists on. Executing the script will output SQL statements that can be used to patch the data, for example the above statement produces the following output:

```
UPDATE `employees`.`departments`
SET `dept_name`='Sales'
WHERE `dept_no`='d007'
LIMIT 1
/
```

The `UPDATE` statements could now be issued directly on the slave to correct the problem.

**Warning**

Generally, changing data directly on a slave is not recommended, but every environment is different. Before making any changes like this always ensure you have a FULL backup, and it would be recommended to shun the slave node (if in a clustered environment) before making any changes so as not to cause any potential interruption to connected clients.

A.9. Comparing Table Data

The Percona Toolkit includes a tool called `pt-table-checksum` that enables you to compare databases on different databases using a checksum comparison. This can be executed by running the checksum generation process on the master:

```
shell> pt-table-checksum --set-vars innodb_lock_wait_timeout=500 \
    --recursion-method=none \
    --ignore-databases=mysql \
    --ignore-databases-regex=tungsten \
    h=localhost,u=tungsten,p=secret
```

Using MySQL, the following statement must then be executed to check the checksums generated on the master:

```
mysql> <userinput>SELECT db, tbl, SUM(this_cnt) AS total_rows, COUNT(*) AS chunks \
    FROM percona.checksums WHERE ( master_cnt <> this_cnt OR master_crc \
    <> this_crc OR ISNULL(master_crc) <> ISNULL(this_crc)) GROUP BY db, tbl;</userinput>
```

Any differences will be reported and will need to manually corrected.

A.10. Troubleshooting Memory Usage
Appendix B. Release Notes

B.1. Continuent Tungsten 2.0.5 GA (24 Dec 2014)

Version End of Life. 31 October 2018

Continuent Tungsten 2.0.5 is a bugfix release that contains critical improvements to the handling of times, dates, and timestamp values between servers, including during daylight savings time switches.

Improvements, new features and functionality

- Installation and Deployment

  - An issue was discovered that altered the way different date and time values were extracted, stored in THL, and applied into target databases. The issue was related to the way the value was stored; the data was not normalized within Continuent Tungsten during replication, particularly if different timezones were used and applied across the replication deployment.

Examples of the behaviour include:

  - MySQL converts `TIMESTAMP` values in statements to UTC. Tungsten did not replicate the master time zone, which meant that replicated statements would generate different `TIMESTAMP` values when replicated to a server with a different time zone from the master.

  - MySQL `TIMESTAMP` values are stored as UTC, which means that row changes are extracted in UTC. Tungsten did not set the Java VM or MySQL session time zone to UTC when applying such changes, which could result in inconsistent values being applied to replicas.

  - Changes between standard and daylight savings time (DST) result in a short period in which master DBMS servers have a different time zone from replicas. This resulted in errors in applying time-related data generated at the time of the switch.

  - Heterogeneous replication, for example from relational DBMS like MySQL to data warehouses, would result in unexpected conversions to time-related data, again due to inconsistencies in time zones.

The replication has now been updated to normalize date and time values into UTC throughout the replication topology, including within the wrapper Java processes, databases and when storing the information in THL.

  - Replicator processes now default to UTC internally by setting the Java VM default time zone to UTC. This default can be changed by setting the replicator.time_zone property in the replicator services.properties file but is not recommended other than for problem diagnosis or specialized testing.

  - Replicas store a time zone on statements and row changes extracted from MySQL.

  - Replicators use UTC as the session time zone when applying to MySQL replicas.

  - Replicators similarly default to UTC when applying transactions to data warehouses like Hadoop, Vertica, or Amazon Redshift.

  - The thl utility prints time-related data using the default GMT time zone. This can be altered using the `-timezone` option.

Best Practices

We recommend the following steps to ensure successful replication of time-related data.

  - Standardize all DBMS server and host time zones to UTC. This minimizes time zone inconsistencies between applications and data stores. The recommendation is particularly important when replicating between different DBMS types, such as MySQL to Hadoop.

  - Use the default time zone settings for Tungsten replicator. Do not change the time zones unless specifically recommended by VMware support.

  - If you cannot standardize on UTC at least ensure that time zones are set consistently on all hosts and applications.

Arbitrary time zone settings create a number of corner cases for database management beyond replication. Standardizing on UTC helps minimize them, hence is strongly recommended.

Upgrade from Older Replicator Versions

New Tungsten replicators tag THL records with an option to show that the transaction was extracted from a time zone-aware replicator. If a replicator sees that this property is not available, it will automatically switch to the older behavior when applying such transactions to MySQL replicas. This ensures that there is as simple process to upgrade from older replicator versions, which is especially important for Continuent Tungsten clusters.
There are two ways to upgrade a replication topology that extracts from MySQL to the new, time zone-aware behavior.

- Put the master replicator offline, wait for slaves to catch up fully, then upgrade all replicators at once.
- Upgrade slave replicators first, then upgrade the master. If the replicators are running in a Continuent Tungsten cluster, you must put the cluster in maintenance mode during the upgrade to prevent master failover.

**Important**

You should not upgrade a master Tungsten Replicator before the slave replicas. This can generate transactions that may not be correctly applied by the slaves, since they are not time zone-aware.

For more information, see Section F.3, “Understanding Replication of Date/Time Values”.

### B.2. Continuent Tungsten 2.0.4 GA (9 Sep 2014)

**Version End of Life.**  31 October 2018

This is a recommended release for all customers as it contains important updates and improvements to the stability of the manager component, specifically with respect to stalls and memory usage that would cause manager failures.

We recommend Java 7 for all Continuent Tungsten 2.0 installations. Continuent are aware of issues within Java 6 that cause memory leaks which may lead to excessive memory usage within the manager. This can cause the manager to run out of memory and restart, without affecting the operation of the dataservice. These problems do not exist within Java 7.

**Improvements, new features and functionality**

- **Tungsten Manager**
  - Tungsten Manager: Improved monitoring fault-tolerance

  Under normal operating conditions, the Tungsten Manager on each DB server host will monitor the local Tungsten Replicator and the database server running on that host and relay the monitoring information thus collected to the other Tungsten Managers in the cluster. In previous releases, Continuent Tungsten was even able to continue to monitor database servers even if a manager on a given DB server node was not running.

  With this release, this functionality has been generalized to handle the monitoring of both database servers and Tungsten replication such that any time a Tungsten Manager is not running on a given DB server host, the remaining Tungsten Managers in the cluster will take over the monitoring activities for both database servers and Tungsten Replicators until the manager on that host resumes operations. This activity takes place automatically and does not require any special configuration or intervention from an administrator.

  The new functionality means that if you have configured Tungsten to fence replication failures and stops, and you stop all Tungsten services on a given node, the rest of the cluster will respond by fencing the associated data source to an **OFFLINE** or **FAILED** state.

  Full recovery of a failed node requires that a Tungsten Manager be running on the node.

- **Tungsten Connector/Tungsten Manager: Full support for ‘relative latency’**

  Support for the use and display of the `relativeLatency` has been expanded and improved. By default, absolute latency is used by the cluster to determine the configuration.

  When relative latency is used, the difference between the last commit time and the current time is displayed. This will show an increasing latency even on long running transactions, or in the event of a stalled replicator. To enable relative latency, use the `--use-relative-latency=true` option to `tpm` during configuration.

  The following changes to the operation of Continuent Tungsten have been added to this release when the use of relative latency is enabled:

  - The output of `SHOW SLAVE STATUS` has been updated to show the `Seconds_Behind_Master` value.
  - `cctrl` will output a new field, `relative`, showing the relative latency value.
  - The Tungsten Connector will use the value when the `maxAppliedLatency` option is used in the connection string to determine whether to route a connection to a master or a slave.

  For more information, see Section 5.3.1, “Latency or Relative Latency Display”.

- **Tungsten Manager: Automated Data Source Fencing Due to Replication Faults**
Continuent Tungsten can now be configured to effectively isolate data sources for which replication has stopped or exhibits an error condition. See the updated documentation on Section 5.13, “Replicator Fencing” for further information.

**Issues**: TUC-2240

For more information, see Section 5.13, “Replicator Fencing”.

**Bug Fixes**

- **Installation and Deployment**
  - The tpm command has been updated to support updated fencing mechanisms.
    
    **Issues**: TUC-2245
  
  - During an upgrade procedure, the process would mistake active witnesses for passive ones.
    
    **Issues**: TUC-2280
  
  - During an update using tpm, the replicator could end up in the **OFFLINE** state.
    
    **Issues**: TUC-2282

- When performing an update, particularly in environments such as Multi-Site, Multi-Master, the tpm command could fail to update the cluster correctly. This could leave the cluster in a diminished state, or fail to upgrade all the components. The tpm command has been updated as follows:
  - tpm will no longer attempt to upgrade a Tungsten Replicator™ with a Continuent Tungsten™ distribution, and vice versa.
  - When installing Tungsten Replicator™, and the $CONTINUENT_PROFILES variable has been set, tpm will fail, warning that the $REPLICATOR_PROFILES variable should be set instead.

  **Issues**: TUC-2288, TUC-2292

- **Tungsten Connector**
  
  - When changing connector properties, and reloading the configuration, the updated values would not be updated.

  - When using mysqldump with option **--flush-logs**, the connector would fail with an Unsupported command error.
    
    **Issues**: TUC-2209

  - When the option **showRelativeSlaveStatus=true** has been specified, the behavior of the connector for checking of latency with read/write splitting would not be used, instead the **appliedLatency** figure would be used instead.
    
    **Issues**: TUC-2243

  - The **connection.close.idle.timeout** would fail to be taken into account when the connector was running in bridge mode.
    
    **Issues**: TUC-2255

  - When the connector was running in bridge mode, and the connection was killed, the connections would not be correctly closed.
    
    **Issues**: TUC-2261

  - The Connector SmartScale would fail to round-robin through slaves when there was no discernable load on the cluster to provide load performance metrics.
    
    **Issues**: TUC-2272

  - SmartScale would wrongly load balance connections to a slave even during a switch operation.
    
    **Issues**: TUC-2273

  - The connector would update the high water setting before and after a write connection was used, creating additional overhead for connections, generating additional query overhead.
    
    **Issues**: TUC-2277

  - When using SmartScale, automatic sessions could be unnecessarily closed upon disconnection, causing slaves to miss valid queries.
    
    **Issues**: TUC-2286
Release Notes

• Tungsten Manager
  • The `checker.tungstenreplicator.properties` and `checker.mysqlserver.properties` files would fail to be created correctly on active witnesses.
    Issues: TUC-2250, TUC-2251
  • The manager would fail to show the correct status for the replicator when getting status information by proxy.
    Issues: TUC-2254
  • Under some conditions, the manager would shut down the router gateway due to an invalid membership alarm but would not restart
    the connector. This would cause all new connections to hang indefinitely.
    Issues: TUC-2278
  • When performing a reset of the replicator service, recovery of the failed service would fail.
    Issues: TUC-2290
• Other Issues
  • The `check_tungsten.sh` script could fail to locate the `tungsten.cfg` or read the correct values from the file.
    Issues: TUC-2263

B.3. Continuent Tungsten 2.0.3 GA (1 Aug 2014)

Version End of Life. 31 October 2018

This is a recommended release for all customers as it contains important updates and improvements to the stability of the manager compo-

nent, specifically with respect to stalls and memory usage that would cause manager failures.

We recommend Java 7 for all Continuent Tungsten 2.0 installations. Continuent are aware of issues within Java 6 that cause memory leaks
which may lead to excessive memory usage within the manager. This can cause the manager to run out of memory and restart, without af-
flecting the operation of the dataservice. These problems do not exist within Java 7.

Behavior Changes

The following changes have been made to Continuent Tungsten and may affect existing scripts and integration tools. Any scripts or en-
vironment which make use of these tools should check and update for the new configuration:

• Within composite clusters, TCP/IP port 7 connectivity is now required between managers on each site to confirm
  availability.

Known Issue

The following issues may affect the operation of Continuent Tungsten and should be taken into account when deploy-
ing or updating to this release.

• The default behavior of the manager is to not fence a datasource for which a replicator has stopped or gone into an
  error state. This was implemented to prevent reducing the overall availability of the deployed service. There are cases
  and deployments where clusters should not operate with replicators in stopped or error states. This could be config-
ure by changing the following properties to `true` according to the master or slave role requirements:

  `policy.fence.slaveReplicator=false`
  `policy.fence.masterReplicator=false`

  If they are set to true, the manager should fence the datasource by setting it to a 'failed' state. When this happens,
  and the datasource is a master, failover will occur. If the datasource is a slave, the datasource will just stay in the failed
  state indefinitely or until the replicator is back in the online state, in which case the datasource will be recovered to
  online.

  At present the setting of these properties are not honored.

  Issues: TUC-2241

Improvements, new features and functionality

• Tungsten Connector
  • The default buffer sizes for the Section 6.5, “Using Bridge Mode” have been updated to 262144 [256KB].
Bug Fixes

Installation and Deployment

To ensure that the correct number of the managers and witnesses are configured within the system, tpm has been updated to check and identify potential issues with the configuration. The installation and checks operate as follows:

- If there are an even number of members in the cluster (i.e. provided to `--members` option):
  - If witnesses are provided through `--witnesses`, continue normally.
  - If witnesses are not provided through `--witnesses`, an error is thrown and installation stops.
- If there are an odd number of members in the cluster (i.e. provided to `--members` option):
  - If witnesses are provided through `--witnesses`, a warning is raised and the witness declaration is ignored.
  - If witnesses are not provided through `--witnesses`, installation continues as normal.

The number of members is calculated as follows:

- Explicitly through the `--members` option.
- Implied, when `--active-witnesses=false`, then the list of hosts declared in `--master` and `--slaves`.
- Implied, when `--active-witnesses=true`, then the list of hosts declared in `--master` and `--slaves` and `--witnesses`.

Issues: TUC-2105

- If ping traffic was denied during installation, then installation could hang while the ping check was performed. A timeout has now been added to ensure that the operation completes successfully.

Issues: TUC-2107

Backup and Restore

- When using xtrabackup 2.2.x, backups would fail if the `innodb_log_file_size` option within `my.cnf` was not specified. tpm has been updated to check the value and existence of this option during installation and to provide a warning if it is not set, or set to the default.

Issues: TUC-2224

Tungsten Connector

- The connector will now re-connect to a MySQL server in the event that an opened connection is found closed between two requests (generally following a `wait_timeout` expiration).

Issues: TUC-2163

- When initially starting up, the connector would open a connection to the configured master to retrieve configuration information, but the connection would never be closed, leading to open unused connections.

Issues: TUC-2166

- The cluster status output by the tungsten cluster status within a multi-site cluster would fail to display the correct states of different data sources when an entire data service was offline.

Issues: TUC-2185

- When the connector has been configured into read-only mode, for example using `--application-readonly-port=9999`, the connector would mistakenly route statements starting `set autocommit=0` to the master, instead of being routed to a slave.

Issues: TUC-2198

- When operating in bridge mode, the connector would retain the client connection when the server had closed the connection. The connector has been updated to close all client connections when the corresponding server connection is closed.

Issues: TUC-2231

Tungsten Manager

- The manager could enter a situation where after switching relay on one physical service, remote site relay is incorrectly reconfigured to point at the new relay. This has been corrected so that reconfiguration no longer occurs in this situation.
Issues: TUC-2164
- Recovery from a composite cluster failover could create a composite split-brain situation.

Issues: TUC-2178
- A statement of record (SOR) cluster would be unable to recover a failed dataservice.

Issues: TUC-2194
- A composite datasource would not go into failsafe mode if all the managers within the cluster were stopped.

Issues: TUC-2206
- If a composite datasource becomes isolated due to a network partition, the failed datasource would not go into failsafe mode correctly.

Issues: TUC-2207
- If a witness became isolated from the rest of the cluster, the rules would not exclude the failed witness and this could lead to memory exhaustion.

Issues: TUC-2214
- Documentation
  - The descriptions and definitions of the archive and standby roles has been clarified in the documentation.
  
For more information, see Section 5.3.3, “Understanding Datasource Roles”.

- The documentation for the recovery of a multi-site multi-master installation has been updated to provide more information when covering.

Issues: TUC-2175
  For more information, see Section 3.2.5, “Resetting a single dataservice”.

B.4. Continuent Tungsten 2.0.2 GA [19 May 2014]

Version End of Life.  31 October 2018

This is a recommended release for all customers as it contains important updates and improvements to the stability of the manager component, specifically with respect to stalls and memory usage that would cause manager failures.

In addition, we recommend Java 7 for all Continuent Tungsten 2.0 installations. Continuent are aware of issues within Java 6 that cause memory leaks which may lead to excessive memory usage within the manager. This can cause the manager to run out of memory and restart, without affecting the operation of the dataservice. These problems do not exist within Java 7.

Improvements, new features and functionality

- Installation and Deployment
  - The default Java garbage collection (GC) used within the Connector, Replicator and Manager has been reconfigured to use parallel garbage collection. The default GC could produce CPU starvation issues during execution.

Issues: TUC-2101

- Tungsten Connector
  - Keep-alive functionality has been added to the Connector. When enabled, connections to the database server are kept alive, even when there is no client activity.

Issues: TUC-2103

  For more information, see Section 6.7.5, “Connector Keepalive”.

Bug Fixes

- Tungsten Manager
  - The embedded JGroups service, which manages the communication and management of the manager service has been updated to the latest version. This improves the stability of the service, and removes some of the memory leaks causing manager stalls.
Release Notes

- A number of issues the memory management on the Manager service, particularly with respect to the included JGroups support have been rectified. These issues caused the manager to use increased amounts of memory that could lead to the manager to stall.

Continent Tungsten 2.0.2 Includes the following changes made in Tungsten Replicator 2.2.1

Behavior Changes

The following changes have been made to Continent Tungsten and may affect existing scripts and integration tools. Any scripts or environment which make use of these tools should check and update for the new configuration:

- The tpm tool and configuration have been updated to support both older Oracle SIDs and the new JDBC URL format for Oracle service IDs. When configuring an Oracle service, use `--datasource-oracle-sid` for older service specifications, and `--datasource-oracle-service` for newer JDBC URL installations.

Issues: 817

Improvements, new features and functionality

- Installation and Deployment

- When using the `--enable-heterogeneous-master` (in [Tungsten Replicator 2.2 Manual]) option to tpm, the MySQL service is now checked to ensure that ROW-based replication has been enabled.

  Issues: 834

- Command-line Tools

- The thl command has been expanded to support an additional output format, `-specs`, which adds the field specifications for row-based THL output.

  Issues: 801

  For more information, see ???.

- Oracle Replication

- Templates have been added to the suite of DDL translation templates supported by ddlscan to support Oracle to MySQL replication. Two templates are included:

  - `ddl-oracle-mysql` provides standard translation of DDL when replicating from Oracle to MySQL
  - `ddl-oracle-mysql-pk-only` provides standard translation of DDL including automatic selection of a primary key from the available unique indexes if no explicit primary key is defined within Oracle DDL when replicating to MySQL

  Issues: 787

  ddlscan has been updated to support parsing of a file containing a list of tables to be parsed for DDL information. The file should be formatted as a CSV file, but only the first argument, table name, will be extracted. Lines starting with a # [hash] character are ignored.

  The file is in the same format as used by `setupCDC.sh`.

  To use the file, supply the `-tableFile` (in [Tungsten Replicator 2.2 Manual]) parameter to the command.

  Issues: 832

- Core Replicator

- The replicator has been updated to support autorecovery from transient failures that would normally cause the replicator to go OFFLINE while in either the ONLINE OR GOING-ONLINE:SYNCHRONIZING (in [Tungsten Replicator 2.2 Manual]) state. This enables the replicator to recover from errors such as MySQL restarts, or transient connection errors.

  The period, number of attempted recovery operations, and the delay before a recovery is considered successful are configurable through individual properties.

  Issues: 784

  For more information, see Deploying Automatic Replicator Recovery (in [Tungsten Replicator 2.2 Manual]).
• The way VARCHAR values were stored and represented within the replicator has been updated which improves performance significantly.

Issues: 804

• If the binary logs for MySQL were flushed and purged (using FLUSH LOGS and PURGE BINARY LOGS), and then the replicator is restarted, the replicator would fail to identify and locate the newly created logs with an MySQLExtractException.

Issues: 851

Documentation

• The deployment and recovery procedures for Multi-site/Multi-master deployments have been documented.

Issues: 797

For more information, see ???.

Bug Fixes

• Installation and Deployment

• tpm would incorrectly identify options that accepted true/false values, which could cause incorrect interpretations, or subsequent options on the command-line to be used as true/false indications.

Issues: 310

• Removing an existing parallel replication configuration using tpm would cause the replicator to fail due to a mismatch in the status table and current configuration.

Issues: 867

• Command-line Tools

• The tungsten_provision_slave tool would fail to correctly re-provision a master within a fan-in or multi-master configuration. When re-provisioning, the service should be reset with trepctl reset.

Issues: 709

• Errors when executing tungsten_provision_slave that have been generated by the underlying mysqldump or xtrabackup are now redirected to STDOUT.

Issues: 802

• The tungsten_provision_slave tool would re-provision using a slave in a OFFLINE:ERROR (in [Tungsten Replicator 2.2 Manual]) state, even though this could create a second, invalid, slave deployment. Reprovisioning from a slave in the ERROR state is now blocked, unless the -f or --force option is used.

Issues: 860

For more information, see ???.

• Oracle Replication

• Tuning for the CDC extraction from Oracle has been updated to support both a minimum sleep time parameter, minSleepTime, and the increment value used when increasing the sleep time between updates, sleepAddition.

Issues: 239

For more information, see Tuning CDC Extraction (in [Tungsten Replicator 2.2 Manual]).

• The URLs used for connecting to Oracle RAC SCAN addresses were not correct and were incompatible with non-RAC installations. The URL format has been updated to use a URL format that is compatible with both Oracle RAC and non-RAC installations.

Issues: 479

• Core Replicator

• When a timeout occurred on the connection to MySQL for the channel assignment service (part of parallel applier), the replicator would go offline, rather than retrying the connection. The service has now been updated to retry the connection if a timeout occurs. The default reconnect timeout is 120 seconds.
Issues: 783

• A slave replicator would incorrectly set the restart sequence number when reading from a master if the slave THL directory was cleared. This would cause slave replicators to fail to restart correctly.

Issues: 794

• Unsigned integers are extracted from the source database in a non-platform independent method. This would cause the Oracle applier to incorrectly attempt to apply negative values in place of their unsigned equivalents. The Oracle applier has been updated to correctly translate these values for types identified as unsigned to the correct value. When viewing these values are viewed within the THL, they will still be identified as a negative value.

Issues: 798

For more information, see ???.

• Replication would fail when processing binlog entries containing the statement `INSERT INTO ... WHERE...` when operating in mixed mode.

Issues: 807

• Filters

• The `mysqlsessionsupport` filter would cause replication to fail when the default `thread_id` was set to -1, for example when `STRICT_ALL_TABLES` SQL mode had been enabled. The replicator has been updated to interpret -1 as 0 to prevent this error.

Issues: 821

• The `rename` filter has been updated so that renaming of only the schema name for STATEMENT events. Previously, only ROW events would be renamed by the filter.

Issues: 842

B.5. Continuent Tungsten 2.0.1 GA [3 January 2014]

Version End of Life. 31 October 2018

Important

The final approved build for Continuent Tungsten 2.0.1 is build 1003. Earlier builds do not have the full set of features and functionality, and includes a number of key fixes not in earlier builds of the same release. In particular, updated support for passive witnesses was not available in earlier builds.

Continuent Tungsten 2.0.1 is the first generally available release of Continuent Tungsten 2.0, which offers major improvements to Continuent’s industry-leading database-as-a-service offering. Continuent Tungsten 2.0.1 contains all the improvements incorporated in Version 1.5.4, and the fixes and new features included within Tungsten Replicator 2.2.0, as well as the following features:

• Cluster Management
  • An improved manager that simplifies recovery of your cluster.
  • New tools to make provisioning and recovery of replication issues.
  • Improved witness host and decision engine to provide better quorum for preventing split-brain and prevent multiple live masters.
  • SSL-based encryption and authentication for cluster management through all command-line tools.

• Connector
  • SSL support enables SSL and non-SSL clients, and SSL and non-SSL connectivity between the connector and database servers.
  • Support for setting the maximum latency for slaves when redirecting queries.

• Installation and Deployment
  • Improved tpm installation tool that eases deployment and configuration of all clusters, including multi-master and multi-site/multi-master.
  • INI file based installation through tpm that enables easier installation, including through Puppet and other script-based solutions.
• Core Replication
  • Includes all Tungsten Replicator 2.2.0 features, including low-impact, low-latency replication, advanced filtering
  • Supports MySQL (5.0, 5.1, 5.5, 5.6), MariaDB (5.5) and Percona Server (5.5).
  • Supports replication to and from MySQL and Oracle, and Oracle to Oracle.
  • Data loading to Vertica and data warehouses, and real-time publishing to MongoDB.
  • SSL-based encryption for exchanging replication data.

Behavior Changes

The following changes have been made to Continuent Tungsten and may affect existing scripts and integration tools. Any scripts or environment which make use of these tools should check and update for the new configuration:

• When using the xtrabackup method for performing backups, the default is to use the xtrabackup-full operation to perform a full backup.
  
  **Issues:** TUC-1327

• The default load balancer used for load-balancing connections within the Connector has been updated to use the RO_RELAXED QoS balancer. This takes account of the HighWater mark when redirecting queries and compares the applied sequence number rather than relying only on the latency.
  
  **Issues:** TUC-1589

• Current strategy for preventing split-brain by using a witness host is not workable for many customers. The witness host configuration and checks have been changed to prevent these problems.
  
  **Issues:** TUC-1650

• Failover could be rolled back because of a failure to release a Virtual IP. The failure has been updated to trigger a warning, not a rollback of failover.
  
  **Issues:** TUC-1666

• An ‘UnknownHostException’ would cause a failover. The behavior has been updated to result in a suspect DB server.
  
  **Issues:** TUC-1667

• A new type of witness host has been added. A new active witness supports a manager-only based installation. The active witness is able to take part in decisions about failure in the event of datasource and/or network connectivity issues.

As a result, the following changes apply for all witness host selection and installation:

• Witnesses must be on the same network subnet as the existing managers.
• Dataservices must have at least three managers to provide status check during failure.
• Active witnesses can be created; these install only the manager on target hosts to act witnesses to check network connectivity to the configured dataserver and connectors configured within the service.
  
  **Issues:** TUC-1854

For more information, see **Section 2.1, “Host Types”**.

• Failover does not occur if the manager is not running, on the master host, before the time that the database server is stopped.
  
  **Issues:** TUC-1900

• Read-only MySQL slaves no longer work.
  
  **Issues:** TUC-1903

Improvements, new features and functionality

• Installation and Deployment
• tpm has been updated to support configuration of the maximum applied latency for the connector using either the `--connector-max-slave-latency` or `--connector-max-applied-latency` options.

  Issues: TUC-733

• Installer should provide a way to setup `RO_RELAXED` (read-only with no SQL checking) connectors.

  Issues: TUC-954

• Post-installation notes do not specify hosts that can run `cctrl`.

  Issues: TUC-1118

• Create a `tpm cook` command that masks the tungsten-cookbook script

  Issues: TUC-1182

• The `tpm` validation has been updated to provided warnings when the `sync_binlog` and `innodb_flush_log_at_trx_commit` MySQL options are set incorrectly.

  Issues: TUC-1656

• A new `tpm` command has been added to list different connector connection commands/syntax.

  Issues: TUC-1661

• Add default path to security files, to facilitate their retrieval.

  Issues: TUC-1676

• Support a `--dataservice-witnesses` value of "none"

  Issues: TUC-1715

• The `tpm` command should not be accessible on installed data sources.

  Issues: TUC-1717

• Allow `tpm` configuration that is compatible with puppet/chef/etc

  Issues: TUC-1735

• Auto-generated properties line should go at the top of the files.

  Issues: TUC-1739

• Add `tpm` switch for `rrIncludeMaster` router properties.

  Issues: TUC-1744

• During installation, the `security.access_file.location` property should be changed to `security.rmi.jmxremote.access_file.location`.

  Issues: TUC-1805

• Split the cross machine checks out of `MySQLPermissionsCheck`.

  Issues: TUC-1838

• The installation of Multi-Site Multi-Master deployments has been simplified.

  Issues: TUC-1923

  For more information, see Section 3.2, “Deploying Multisite/Multimaster Clusters”.

• Command-line Tools

• A completion script for command-line completion within `bash` has been added to the installation. The file is located in `tools/tpm.complete` within the installation directory.

  Issues: TUC-1591

• Write scripts to coordinate backups across an entire cluster.
Release Notes

Issues: TUC-1641
• cctrl should not report that recover is an expert command

Issues: TUC-1839
• An option, `-a, --authenticate` has been added to the tpasswd utility to validate an existing password entry.

Issues: TUC-1916
• Cookbook Utility
  • Tungsten cookbook should run manager|replicator|connector dump before collecting logs.

Issues: TUC-1660
  • Cookbook has been updated to support both active and passive witnesses.

Issues: TUC-1942
  • Cookbook has been updated to allow backups from masters to be used.

Issues: TUC-1943
• Backup and Restore
  • The datasource_backup.sh script has been updated to limit running only on the `COORDINATOR` and to find a non-MASTER datasource.

Issues: TUC-1684
• MySQL Replication
  • Add support for MySQL 5.6

Issues: TUC-1624
• Tungsten Connector
  • Support for MySQL 4.0 passwords within the connector has been included. This provides support for both old MySQL versions and older versions of the MySQL protocol used by some libraries and clients.

Issues: TUC-784
• Connector must forbid zero `keepAliveTimeout`.

Issues: TUC-1714
• In SOR deployments only, Connector logs show relay data service being added twice.

Issues: TUC-1720
• Change default `delayBeforeOfflineIfNoManager` router property to 30s and constrain it to max 60s in the code.

Issues: TUC-1752
• Router Manager connection timeout should be a property.

Issues: TUC-1754
• Add client IP and port when logging connector message.

Issues: TUC-1810
• Make tungsten cluster status more sql-like and reduce the amount of information displayed.

Issues: TUC-1814
• Connector client side SSL support for MySQL

Issues: TUC-1825
• Tungsten Manager
• cctrl should show if a given data source is secured.
  Issues: TUC-1816
• The datasource hostname recover command should not invoke the expert warning.
  Issues: TUC-1840
• Manager API
  • Smarter enabling of the Manager API
    Issues: TUC-1621
  • Support has been added to specify the addresses for the Manager API to listen on.
    Issues: TUC-1643
  • The Manager API has been updated with a method to list all the available dataservices.
    Issues: TUC-1674
  • Add DataServiceState and DataSource into the payload when applicable
    Issues: TUC-1701
  • Add classes to the Ruby libraries that handle API calls
    Issues: TUC-1707
  • Add an API call that prints the manager live properties
    Issues: TUC-1713
• Platform Specific Deployments
  • Add Java wrapper support for FreeBSD.
    Issues: TUC-1632
  • Commit FreeBSD fixes to Java sockets and port binding.
    Issues: TUC-1633
• Documentation
  • Document among the prerequisites that Tungsten installers do not support mysqld_multi.
    Issues: TUC-1679
• Other Issues
  • Write a tpm test wrapper for the cookbook testing scripts.
    Issues: TUC-1396
  • Document the process of sending emails based on specific log4j messages
    Issues: TUC-1500
  • The check_tungsten.sh script has been updated to check and restart enterprise load balancers that use the xinetd service.
    Issues: TUC-1573
  • Expand zabbix monitoring to match nagios checks.
    Issues: TUC-1638
  • Turn \texttt{SET NAMES} log message into DEBUG.
    Issues: TUC-1644
  • Remove old/extra/redundant configuration files.
Release Notes

Issues: TUC-1721
• Backport critical 1.5.4 manager changes to 2.0.1
  Issues: TUC-1855

Bug Fixes

• Installation and Deployment
  • Tungsten can’t install if the ‘mysql’ client is not in the path.
    Issues: TUC-999
  • An extra -1 flag when running sudo command would be added to the configuration.
    Issues: TUC-1025
  • Installer will not easily work when installing SOR data services one host at a time.
    Issues: TUC-1036
  • The tpm did not verify that the permissions for the tungsten DB user allow for cross-database host access.
    Issues: TUC-1146
  • Specifying a Symbolic link for the Connector/J creates a circular reference.
    Issues: TUC-1567
  • Replication of DATETIME values with a Daylight Savings Time (DST) would replicate incorrect values. Installation of a replication service where there are different timezones for the Java environment and the MySQL environment may cause incorrect replication.
    Issues: 542, TUC-1593
  • The replicator service would not be imported into the cluster directory - causes subsequent failures in switch and other operations.
    Issues: TUC-1594
  • tpm would fail to skip the GlobalHostAddressesCheck when performing a tpm configure followed by tpm validate.
    Issues: TUC-1599
  • tpm does not recognize datasources when they start with capital letter.
    Issues: TUC-1655
  • Installation of multiple replicator with tpm fails.
    Issues: TUC-1680
  • The check for Java version fails when OpenJDK does not say ‘java’.
    Issues: TUC-1681
  • The installer did not make sure that witness servers are in the same network as the cluster.
    Issues: TUC-1705
  • tpm does not install if there is a Tungsten Replicator installer already running.
    Issues: TUC-1712
  • Errors during installation of composite dataservice.
    Issues: TUC-1726
  • The tpm command returns an ssh error when attempting to install a composite data service.
    Issues: TUC-1727

• Running tpm with no arguments raises an error.
Issues: TUC-1788

• Installation fails with Ruby 1.9.

Issues: TUC-1800

• `tpm` will not throw an error if the user gives the connectorj-path as the path to a symlink instead of a real file.

Issues: TUC-1815

• `tpm` does not check dependencies of security options.

Issues: TUC-1818

• When checking process limits during installation, the check would fail the installation process instead of providing a warning.

Issues: TUC-1822

• During `tpm` validation wrongly complains about a witness not being in the same subnet.

Issues: TUC-1848

• During installation, `tpm` could install SSL support for the connector even though the MySQL server has not been configured for SSL connectivity.

Issues: TUC-1909

• Running `tpm update` would cause the master replicator to become a slave during the update when the master had changed from the configuration applied using `--dataservice-master-host`.

Issues: TUC-1921

• `tpm` could allow meaningless specifications of active witnesses.

Issues: TUC-1941

• `tpm` has been updated to provide the correct link to the documentation for further information.

Issues: TUC-1947

• Performing `tpm reset` would remove all the files within the `cluster-home/conf` directories, instead of only the files for services `tpm` was aware of.

Issues: TUC-1949

• `tpm` would require the `--active-witnesses` or `--enable-active-witnesses` option, when other witness types are available for configuration.

Issues: TUC-1951

• `tpm` would check the same witness subnet when using active witnesses, which do not need to be installed on the same subnet.

Issues: TUC-1953

• A `tpm update` operation would not recognize active witnesses properly.

Issues: TUC-1975

• A `tpm uninstall` operation would complain about missing databases in connector tests.

Issues: TUC-1978

• `tpm` would not remove the `connector.ro.properties` file if the configuration is updated to not have `--application-readonly-port`.

Issues: TUC-1981

• `tpm` would enable installation when MariaDB 10.0 was installed, even though this is not a supported configuration.

Issues: TUC-1987

• The method used to compare whether hosts were on the same subnet would fail to identify hosts correctly.

Issues: TUC-1995
• Command-line Tools
  • Running cctrl on a host which only had the connector server would not report a useful error. This has now been updated to show a warning message. 
    *Issues: TUC-1642*
  • The check_tungsten command had different command line arguments from check_tungsten.sh. 
    *Issues: TUC-1675*
  • Nagios check scripts not picking up shunned datasources 
    *Issues: TUC-1689*
  • cctrl could output the status of a host with a null value in place of the correct hostname.  
    *Issues: TUC-1893*
  • Using the recover datasource command within a composite service would fail, even though datasource recover would work. 
    *Issues: TUC-1912*
  • The check_tungsten_latency --perslave-perfdata option would not include information for relay hosts. 
    *Issues: TUC-1915*
  • A large error message could be found included within the status block of ls output within cctrl. The error message information has been redirected to the error log. 
    *Issues: TUC-1931*
  • Performing switch operations within a composite service using active witnesses could raise an error and fail. 
    *Issues: TUC-1946*
  • cctrl would be unable to create a composite datasource after dropping it. 
    *Issues: TUC-1956*
  • Backwards compatibility for the recover using has been incorporated. 
    *Issues: TUC-1971*

• Cookbook Utility
  • The tungsten-cookbook tests fails and does not print current status. 
    *Issues: TUC-1623*
  • The tungsten-cookbook uses resolveip instead of standard name resolution tools. 
    *Issues: TUC-1646*
  • The tungsten-cookbook tool sometimes misunderstands the result of composite recovery. 
    *Issues: TUC-1662*
  • Cookbook gets warnings when used with a MySQL 5.6 client. 
    *Issues: TUC-1673*
  • The cookbook does not wait for a database server to be offline properly. 
    *Issues: TUC-1685*
  • tungsten-cookbook does not check the status of the relay server after a composite recovery. 
    *Issues: TUC-1695*
  • tungsten-cookbook does not check all the components of a datasource when testing a server. 
    *Issues: TUC-1696*
• tungsten-cookbook does not collect the configuration files under cluster-home.
  Issues: TUC-1697

• Cookbook should not specify witness hosts in default configuration files etc.
  Issues: TUC-1734

• Tungsten cookbook fails the replicator test.
  Issues: TUC-1827

• Using a backup that has been copied across servers within cookbook could overwrite or replace existing backup files, which would then make the backup file appear as older than it should be, making it unavailable in restore operations.
  Issues: TUC-1936

• Backup and Restore

• The mysqldump backup option cannot restore if slow_query_log was on during the backup process.
  Issues: TUC-586

• Using xtrabackup during restore fails if MySQL is running as user ‘anything-but-mysql’ and without root access.
  Issues: TUC-1005

• When using mysqldump restore, the operation failed to disable slow and general logging before applying the restore.
  Issues: TUC-1330

• Backup fails when using the xtrabackup-full agent.
  Issues: TUC-1612

• Recovery hangs with composite data service.
  Issues: TUC-1657

• Performing a restore with xtrabackup fails.
  Issues: TUC-1672

• The datasource backup operation could fail due to a Ruby error.
  Issues: TUC-1686

• Restore with xtrabackup fails.
  Issues: TUC-1716

• Issues when recovering a failed physical dataservice.
  Issues: TUC-1793

• Backup with xtrabackup fails if datadir is not defined in my.cnf.
  Issues: TUC-1821

• When using xtrabackup restore fails.
  Issues: TUC-1846

• After a restore, datasource is welcomed and put online, but never gets to the online state.
  Issues: TUC-1861

• A restore that occurs immediately after a recover from dataserver failure always fails.
  Issues: TUC-1870

• Master datasource backup generates superficial failure message but succeeds anyway.
Issues: TUC-1896
- Restoration of a full backup would fail due to the inclusion of the `xtrabackup_incremental_basedir` directory.
  
Issues: TUC-1919
- Backup using `xtrabackup 1.6.5` would fail.
  
Issues: TUC-1920
- When using the backup files copied from another server, the replicator could mistakenly use the wrong backup files when performing a restore.
  
Issues: TUC-1948
- Core Replicator
  
  - Master failure causes partial commits on the slave with single channel parallel apply.
    
Issues: TUC-1625
  
  - Slave applier can fail to log error when DBMS fails due to exception in cleanup.
    
Issues: TUC-1626
  
  - Replication would fail on slave due to null characters created when inserting `____SERVICE____` comments.
    
Issues: TUC-1627
  
  - `LOAD (LOCAL) DATA INFILE` would fail if the request starts with white spaces.
    
Issues: TUC-1639
  
    
Issues: TUC-1658
  
  - An insecure slave can replicate from secure master.
    
Issues: TUC-1677
  
  - Replicator does not drop client connection to master and reconnect within the same time frame as in previous releases.
    
Issues: TUC-1688

- Filters
  
  - Primary key filter should be able to renew its internal connection after some timeout.
    
Issues: TUC-1803

- Tungsten Connector
  
  - TSR Session not updated when the database name changes [with sessionId set to DATABASE]
    
Issues: TUC-761
  
  - Router gateway can prevent manager startup if the connector is started before the manager
    
Issues: TUC-850
  
  - The Tungsten show processlist command would throw NPE errors.
    
Issues: TUC-1136
  
  - Selective read/write splitting [SQL-Based routing] has been updated to ensure that it is backwards compatible with previous read/write splitting configurations.
    
Issues: TUC-1489
  
  - Router must go into fail-safe mode if it loses connectivity to a manager during a critical command.
    
Issues: TUC-1549
- Use of the `SET NAMES` command were not forwarded to attached read-only connections.
  
  **Issues:** TUC-1569

- When using haproxy through a connector connection, the initial query would be rejected.
  
  **Issues:** TUC-1581

- When the `dataservices.properties` file is empty, the connector would hang. The operation has now been updated to exit with an exception if the file cannot be found.
  
  **Issues:** TUC-1586

- When in a SOR deployment, the Connector will never return connection requests with `RO_RELAXED` and affinity set to `relay node only site`.
  
  **Issues:** TUC-1620

- Affinity not honored when using direct connections.
  
  **Issues:** TUC-1628

- Connector queries for `SHOW SLAVE STATUS` return incorrect slave latency of 0 intermittently.
  
  **Issues:** TUC-1645

- The Tungsten Connector does not know it's PID following upgrade to JSW 3.5.17.
  
  **Issues:** TUC-1665

- An attempt to load a driver listener class can cause the connector to hang, at startup.
  
  **Issues:** TUC-1669

- Read connections allocated by connector get 'stale' and are closed by MySQL server due to `wait_timeout` - causes app 'transparency' issues.
  
  **Issues:** TUC-1671

- Broken connections returned to the c3p0 pool - further use of these will show errors.
  
  **Issues:** TUC-1683

- Router disconnects from a manager in the middle of a switch command - writes continue to offline master.
  
  **Issues:** TUC-1692

- Connector sessionId passed in database name not retained
  
  **Issues:** TUC-1704

- When using `USE DB` within a connector after the database had previously been dropped would be incorrectly ignored.
  
  **Issues:** TUC-1718

- The connector tungsten flush privileges command causes a temporary outage [denies new connection requests].
  
  **Issues:** TUC-1730

- Database context not changed to the correct database when `qos=DATABASE` is in use.
  
  **Issues:** TUC-1779

- Connector should require a valid manager to operate even when in maintenance mode.
  
  **Issues:** TUC-1781

- Connector allows connections to an offline/on-hold composite dataservice.
  
  **Issues:** TUC-1787

- Router notifications are being sent to routers via GCS. This is unnecessary since a manager only updates routers that are connected to it.
Issues: TUC-1790

- Pass through not handling correctly multiple results in 1.5.4.

Issues: TUC-1792

- SmartScale will fail to create a database and use immediately.

Issues: TUC-1836

- The connector could hang during installation test.

Issues: TUC-1847

- Under certain circumstances, SSL-configuration for the Connector would be unable to start properly.

Issues: TUC-1869

For more information, see Section 2.7.4, “Configuring Connector SSL”.

- Specify where to load security properties from in the connector.

Issues: TUC-1872

- A `SET NAMES` operation would not survive a switch or failover operation.

Issues: TUC-1879

- The connector command within cctrl has been disabled unless the connector and manager are installed on the same host.

To support the removed functionality, the following changes to the router command have been made:

- The `*` wildcard can be used for connectors within the router command within cctrl. For example, `router * online` will place all available connectors online.

- The built-in command-line completion provides the names of the connectors in addition to the `*` (wildcard) character for the router command.

Issues: TUC-1918

- Using cursors within stored procedures through the connector would cause a hang in the connector service.

Issues: TUC-1950

- The connector would hang when working in a cluster with active witnesses.

Issues: TUC-1954

- When specifying the affinity within a connection, the `maxAppliedLatency` configuration would be ignored.

Issues: TUC-1960

- The connector would check for changes to the `user.map` frequently, causing lag on high-load servers. The configuration has been updated to allow checking only every 10s.

Issues: TUC-1972

- Passing the `qos` option within a database name would not work when smart scale was enabled.

Issues: TUC-1982

- Tungsten Manager

  - The datasource restore command may fail when using xtrabackup if the file ownership for the backup files is wrong.

Issues: TUC-1226

- Dataservice has different "composite" status depending on how its status is called.

Issues: TUC-1614

- The switch command does not validate command line correctly.
Issues: TUC-1618

- Composite recovery would fail because a replicator that was previously a master tries to re-apply a transaction that it had previously committed.

Issues: TUC-1634

- `cctrl` would let you shun the master datasource.

Issues: TUC-1637

- During a failover, the master could be left in read-only mode.

Issues: TUC-1648

- On occasion, the manager would fail to restart after being hung.

Issues: TUC-1649

- The ping command in `cctrl` wrongly identifies witness server as unreachable.

Issues: TUC-1652

- The failure of primary data source could go unhandled due to a manager restart.

Issues: TUC-1659

- The manager reports composite recovery completion although the operation has failed.

Issues: TUC-1663

- A transient error can cause a confused state.

Issues: TUC-1678

- Composite recovery could fail, but the manager says it was complete.

Issues: TUC-1694

- The internal Call to `OpenReplicatorManager.status()` during transition from online to offline results in a NullPointerException.

Issues: TUC-1708

- Relay does not fail over when the database server is stopped.

Issues: TUC-1711

- The `cctrl` would raise an error when running a backup from a master.

Issues: TUC-1789

- Tungsten manager may report false host failures due to a temporary problem with name resolution.

Issues: TUC-1797

- `cctrl` could report a manager as ONLINE even though the datasource would in fact be OFFLINE.

Issues: TUC-1804

- The manager would not see a secured replicator.

Issues: TUC-1806

- Slave replicators never come online after a switch when using secure thl.

Issues: TUC-1807

- `cctrl` complains of missing security file when security is not enabled.

Issues: TUC-1808

- Switch in relay site fails and takes offline all nodes.
Issues: TUC-1809

• A switch in the relay site sets the relay to replicate from itself.

Issues: TUC-1811

• In a composite deployment, a switch in the primary site is not propagated to the relay.

Issues: TUC-1813

• cctrl exposes security passwords unnecessarily.

Issues: TUC-1817

• The master datasource is not available following the failover command.

Issues: TUC-1841

• The manager does not support a non-standard replicator RMI port.

Issues: TUC-1842

• In a multi-site deployment, automatic failover does not happen in maintenance mode, due to replicator issues.

Issues: TUC-1845

• During the recovery of a composite dataservice, the restore of a shunned master could fail because the previous and current roles did not match.

Issues: TUC-1857

• A stopped dataserver would not be detected if cluster was in maintenance mode when it was stopped.

Issues: TUC-1860

• Manager attempts to get status of remote replicator from the local service - causes a failure to catch up from a relay.

Issues: TUC-1864

• A switch operation could fail in single site deployment.

Issues: TUC-1867

• In a configuration with a relay of a composite site, if all active data datasources are unavailable, a switch operation would raise invalid exception messages.

Issues: TUC-1875

• recover using fails in the simplest case for 2.0.1.

Issues: TUC-1876

• Manager fails safe even if it is in the quorum set and primary partition.

Issues: TUC-1878

• Single command recover does not work - does not find datasources to recover even if they exist.

Issues: TUC-1881

• Failover causes old master node name to disappear from cctrl ls command.

Issues: TUC-1894

• ClusterManagementHandler can read/write datasources directly from the local disk - can cause cluster configuration information corruption.

Issues: TUC-1899

• Stopping managers does not cause membership validation rules to kick in. This can lead to an invalid group.

Issues: TUC-1901
• The manager rules could fail to fence a composite datasource for which all managers in the service are unreachable.
  
  **Issues:** TUC-1902

• recover using in a master service could convert one of the datasources into a relay instead of a slave.

  **Issues:** TUC-1907

• CREATE COMPOSITE DATASOURCE could result in an exception if the master datasource site was used.

  **Issues:** TUC-1911

• The manager would throw a false alarm if the `trep_commit_seqno` table was empty. This was due to the manager being started before the replicator had created the required table.

  **Issues:** TUC-1917

• Composite recovery within a cloud deployment could fail.

  **Issues:** TUC-1922

• Errors could be raised when using the set master and recover using commands within cctrl.

  **Issues:** TUC-1930

• Composite recovery could fail in a site with multiple masters.

  **Issues:** TUC-1932

• A failed master within a dataservice would cause the datasource names to disappear.

  **Issues:** TUC-1933

• Running switch command after performing recovery could fail within a multi-site deployment.

  **Issues:** TUC-1934

• Performing a switch operation when there are active witness could cause an error message indicating a fault, when in fact the operation completed successfully.

  **Issues:** TUC-1935

• After performing a switch operation, a slave could report to the previous, not active, relay.

  **Issues:** TUC-1939

• Running operations on active witness datasources would raise NullPointerException errors.

  **Issues:** TUC-1944, TUC-1945

• Errors would be reported in the log when deserializing configuration information between the manager and connector.

  **Issues:** TUC-1963

• Automatic failover would fail to run if an active witness was the coordinator for the dataservice.

  **Issues:** TUC-1964

• Connectors would disappear after restarting the coordinator.

  **Issues:** TUC-1966

• The coordinator would attempt to check database server liveness if a manager on a witness host goes away.

  **Issues:** TUC-1970

• Composite recovery using a streaming backup results in a site with multiple masters.

  **Issues:** TUC-1992

• Installing a composite dataservice would create two master services.
• Manager API
  • API call for a single server does not report replicator status.
  
    Issues: TUC-1615
  • API “promote” command does not operate in a composite dataservice.
  
    Issues: TUC-1617
  • Some indispensable commands missing from manager API.
  
    Issues: TUC-1654
  • Manager API does not answer to /manager/status/svc_name without Accept header
  
    Issues: TUC-1690
  • The Manager API lets you shun a master.
  
    Issues: TUC-1706
  • The call to ‘policy’ API fails in composite dataservice.
  
    Issues: TUC-1725

• Platform Specific Deployments
  • Windows service registration scripts won't work.
  
    Issues: TUC-1636
  • FreeBSD: Replicator hangs when going offline. Can cause switch to hang/abort.
  
    Issues: TUC-1668

• Documentation
  • Document the process for changing the replication username and password.
  
    Issues: TUC-638
  • Documentation has been added for deploying Continuent Tungsten with INI files
  
    Issues: TUC-1888

  For more information, see Section 9.4, “tpm INI File Configuration”.

  • Documentation on the different tpm commands has been added to the documentation.
  
    Issues: TUC-1890

  For more information, see Section 9.5, “tpm Commands”.

  • Documentation for the new tools designed to ease usability with Continuent Tungsten have been added.
  
    Issues: TUC-1891, TUC-1892


• Other Issues
  • The shared libraries used by Continuent Tungsten have now been centralized in the cluster-home directory.
  
    Issues: TUC-1310
  • Some build warnings in Java 1.6 become errors in Java 1.7.
  
    Issues: TUC-1731
• The test_connection_routing_and_isolation.rb test never selects the correct master.

  Issues: TUC-1780

• During testing, a test that stops and restarts the replicator fails because a replicator that is actually running shows up, subsequently, as stopped.

  Issues: TUC-1895

• The wrapper for the service was not honoring the configured wait period during a restart, which could cause a hang or failure when the service was restarted.

  Issues: TUC-1910, TUC-1913

Continuent Tungsten 2.0.1 Includes the following changes made in Tungsten Replicator 2.2.0

Continuent Tungsten 2.2.0 is a bug fix and feature release that contains a number of key improvements to the installation and management of the replicator:

• tpm is now the default installation and deployment tool; use of tungsten-installer, configure, configure-service, and update are deprecated.

• tpm incorporates support for both INI file and staging directory deployments. See ???.

• Deployments are possible using standard Linux RPM and PKG deployments. See ???.

• tpm has been improved to handle heterogeneous deployments more easily.

• New command-line tools have been added to make recovery easier during a failure. See ???, ???, ???.

• Improvements to the core replicator, including identification and recovery from failure.

• New multi_trepctl tool for monitoring multiple hosts/services.

Behavior Changes

The following changes have been made to Continuent Tungsten and may affect existing scripts and integration tools. Any scripts or environment which make use of these tools should check and update for the new configuration:

• The thl info command has been updated so that the output also displays the lowest and highest THL file, sizes and dates.

  Issues: 471

  For more information, see ???.

• The following commands to trepctl have been deprecated and will be removed in a future release:

  • trepctl start has been replaced with trepctl load

  • trepctl stop has been replaced with trepctl unload

  • trepctl shutdown has been deprecated; use ??? to stop the replicator.

  Issues: 672

  For more information, see ???, ???, ???.

• The tpm command has been updated to be the default method for installing deployments using the cookbook. To use the old tungsten-installer command, set the use_old_installer environment variable.

  Issues: 691

Known Issues

The following issues may affect the operation of Continuent Tungsten and should be taken into account when deploying or updating to this release.

• Installation and Deployment
Installations for Amazon RDS must use tungsten-installer; support is not currently available for tpm.

Improvements, new features and functionality

Installation and Deployment

• For heterogeneous deployments, three new options have been added to tpm:
  • `--enable-heterogeneous-master` [in Tungsten Replicator 2.2 Manual]
    This option applies a range of settings, including `--mysql-use-bytes-for=string=false`, `--java-file-encoding=UTF8`, `--mysql-enable-enumtostring=true`, and `--mysql-enable-settostring=true`. This option also enables the `columnname` and `pkey` filters.
  • `--enable-heterogeneous-slave` [in Tungsten Replicator 2.2 Manual]
    This option disables parallel replication for hosts that do not support it, and sets the `--java-file-encoding=UTF8` option.
  • `--enable-heterogeneous-service` [in Tungsten Replicator 2.2 Manual]

Issues: 692
For more information, see Install MongoDB Applier [in Tungsten Replicator 2.2 Manual], Install Vertica Applier [in Tungsten Replicator 2.2 Manual].

• A new command-line tool, `tungsten_set_position`, has been created. This enables the position of either a master or slave to be set with respect to reading local or remote events. This provides easier control over during the recovery of a slave or master in the event of a failure.
  
  Issues: 684
  For more information, see ???, ???.

• A new command-line tool, `tungsten_provision_slave`, has been created. This allows for an automated backup of an existing host and restore of that data to a new host. The script can be used to provision new slaves based on existing slave configurations, or to recover a slave that has failed.
  
  Issues: 689
  For more information, see ???, ???.

• A new command-line tool, `tungsten_read_master_events`, has been created. This enables events from the MySQL binary log to be viewed based on the THL event ID.
  
  Issues: 694
  For more information, see ???, ???.

• The trepctl properties command has been updated to support a `--values` option that outputs only the values for filtered properties.
  
  Issues: 719
  For more information, see ???.

• The multi_trepctl command has been added. The tool enables status and other output from multiple hosts and/or services, providing a simpler way of monitoring a typical Continuent Tungsten installation.
  
  Issues: 756
  For more information, see ???.

Oracle Replication

• The ddlscan tool and the `ddl-mysql-oracle.vm` template have been modified to support custom included templates on a per table basis.
Release Notes

The tool has also been updated to support additional paths for searching for velocity templates using the -path option.

Issues: 723

Core Replicator

- The block commit process has been updated to support different configurations. Two new parameters have been added, which affect the block commit size, and enable transactions to be committed to a slave in blocks either based on the number of events, or the time interval since the last commit occurred.
  - repl-svc-applier-block-commit-size sets the number of events that will trigger a block commit. The default is 10.
  - repl-svc-applier-block-commit-interval sets the time interval between block commits. The default is 0 (disabled).

Issues: 677, 699
For more information, see ???.

Filters

- The dropcolumn JavaScript filter has been added. The filter enables individual columns to be removed from the THL so that personal identification information (PII) can be removed on a slave.

Issues: 716
For more information, see ???.

Bug Fixes

Installation and Deployment

- When performing a Vertica deployment, tpm would fail to create the correct configuration parameters. In addition, error messages and warnings would be generated that did not apply to Vertica installations. tpm has been updated to simplify the Vertica installation process.

Issues: 688, 781
For more information, see Install Vertica Applier [in [Tungsten Replicator 2.2 Manual]].

- tpm would allow parallel replication to be configured in heterogeneous environments where parallel replication was not supported. During deployment, tpm now reports an error if parallel configuration parameters are supplied for datasource types other than MySQL or Oracle.

Issues: 733

- When configuring a single host to support a parallel, multi-channel deployment, tpm would report that this operation was not supported. tpm has now been updated to support single host parallel apply configurations.

Issues: 737

- Configuring an installation with a preferred path for MySQL deployments using the --preferred-path option would not set the PATH variable correctly, this would lead to the tools from an incorrect directory being used when performing backup or restore operations. tpm has been updated to correctly set the environment during execution.

Issues: 752

Command-line Tools

- When using the -sql option to the thl, additional metadata and options would be displayed. The tool has now been updated to only output the corresponding SQL.

Issues: 264

- DATETIME values could be displayed incorrectly in the THL when using the thl tool to show log contents.

Issues: 676

- An incorrect RMI port could be used within a deployment if a non-standard RMI port was specified during installation, affecting the operation of trepctl. The precedence for selecting the RMI port to use has been updated to use the -port, the system property, and then service properties for the selected service and/or trepctl executable.
Release Notes

Issues: 695

• Backup and Restore

• During installation, tpm would fail to check the version for Percona XtraBackup when working with built-in InnoDB support in MySQL. The check has now been updated and validation will fail if XtraBackup 2.1 or later is used with a MySQL 5.1 and built-in InnoDB support.

Issues: 671

• When using xtrabackup during a restore operation, the restore would fail. The problem was due to a difference in the interface for XtraBackup 2.1.6.

Issues: 778

• Oracle Replication

• When performing an Oracle deployment, tpm would apply incorrect parameters and filters and check MySQL specific environment information. The following changes have been made:
  
  • The colnames filter is no longer added to Oracle master (extractor) deployments.
  
  • Incorrect schema value would be defined for the replicator schema.

  The check for mysqldump is still performed on an Oracle master host; use --preferred-path to set a valid location, or disable the MySQLDumpCheck validation check.

Issues: 685

• Core Replicator

• DECIMAL values could be extracted from the MySQL binary log incorrectly when using statement based logging.

Issues: 650

• A null pointer exception could be raised by the master, which would lead to the slave failing to connect to the master correctly. The slave will now retry the connection.

Issues: 698

• A slave replicator could fail when synchronizing the THL if the master goes offline. This was due to network interrupts during a failure not being recognised properly.

Issues: 714

• In certain circumstances, a replicator could apply transactions that had been generated by itself. This could happen during a failover, leading to events written to the THL, but without the trep_commit_seqno table having been updated. To fix this problem, consistency checks on the THL contents are now performed during startup. In addition, all repli- cators now write their currently assigned role to a file within the configuration directory of the running replication service, called static servicename role.

  When the replicator goes online, a static servicename role file is examined. If the current role identified in that file was a master, and the current role of the replicator is a slave, then the THL consistency checks are enabled. These check the following situations:

  • If the trep_commit_seqno is out of sync with the contents of the THL provided that the last THL record exists and matches the source-id of the transaction.

  • If the current log position is different to the THL position, and assuming that THL position exists, then an error will be raised and the replicator will go offline. This behavior can be overridden by using the trepctl online -force command.

  Once the checks have been completed, the new role for the replicator is updated in the static servicename role file.

  Important

  The static servicename role file must be deleted, or the THL files must be deleted, when restoring a backup. This is to ensure that the correct current log position is identified.

Issues: 735
• An UnsupportedEncodingException error could occur when extracting statement based replication events if the MySQL character set did not match a valid Java character set used by the replicator.

  Issues: 743

• When using Row-based replication, replicating into a table on the slave that did not exist, a Null-Pointer Exception would be raised. The replicator now correctly raises an SQL error indicating that the table does not exist.

  Issues: 747

• During a master failure under load, the number of transactions making it to the slave before the master replicator fails.

  Issues: 753

• Upgrading a replicator and changing the hostname could cause the replicator to skip events in the THL. This was due to the way in which the source-id of events in the slave replicator checks the information compared to the remote THL read from the master. This particularly affect standalone replicators. The fix adds a new property, `replicator.repositionOnSourceIdChange`. This is a boolean value, and specifies whether the replicator should try to reposition to the correct location in the THL when the source ID has been modified.

  Issues: 754

• Running trepctl reset on a service deployed in an multi-master [all master] configuration would not correctly remove the schema from the database.

  Issues: 758

• Replication of temporary tables with the same name, but within different sessions would cause a conflict in the slave.

  Issues: 772

• Filters

  • The pkey would not renew connections to the master to determine the primary key information. When replication had been running for a long time, the active connection would be dropped, but never renewed. The filter has been updated to re-connect on failure.

  Issues: 670

For more information, see ???.
Appendix C. Prerequisites

Before you install Continuent Tungsten, there are a number of setup and prerequisite installation and configuration steps that must have taken place before any installation can continue. Section C.1, “Staging Host Configuration” and Section C.2, “Host Configuration” must be performed on every host within your chosen cluster or replication configuration. Additional steps are required to configure explicit databases, such as Section C.3, “MySQL Database Setup”, and will need to be performed on each appropriate host.

C.1. Staging Host Configuration

The staging host will form the base of your operation for creating your cluster. The primary role of the staging host is to hold the Continuent Tungsten™ software, and to install, transfer, and initiate the Continuent Tungsten™ service on each of the nodes within the cluster. The staging host can be a separate machine, or a machine that will be part of the cluster.

The recommended way to use Continuent Tungsten™ is to configure SSH on each machine within the cluster and allow the tpm tool to connect and perform the necessary installation and setup operations to create your cluster environment, as shown in Figure C.1, “Tungsten Deployment”.

Figure C.1. Tungsten Deployment

1. Create a new Tungsten user that will be used to manage and install Continuent Tungsten™. The recommended choice for MySQL installations is to create a new user, tungsten. You will need to create this user on each host in the cluster. You can create the new user using adduser:

```
shell> sudo adduser tungsten
```

You can add the user to the mysql group adding the command-line option:

```
shell> sudo usermod -G mysql -a tungsten
```
2. Login as the `tungsten` user:

```
shell> su - tungsten
```

3. Create an SSH key file, but do not configure a password:

```
tungsten:shell> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/tungsten/.ssh/id_rsa):
Created directory '/home/tungsten/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tungsten/.ssh/id_rsa.
Your public key has been saved in /home/tungsten/.ssh/id_rsa.pub.
The key fingerprint is:
The key's randomart image is:
```
+--[ RSA 2048]----+
|                 |
|                 |
|             .   |
|            . .  |
|        S .. +   |
|       . o .X .  |
|        .oEO + . |
|       .o.=o. o  |
|      o=+..    . |
+-----------------+
```

This creates both a public and private keyfile; the public keyfile will be shared with the hosts in the cluster to allow hosts to connect to each other.

4. Within the staging server, profiles for the different cluster configurations are stored within a single directory. You can simplify the management of these different services by configuring a specific directory where these configurations will be stored. To set the directory, specify the directory within the `CONTINUENT_PROFILES` environment variable, adding this variable to your shell startup script (`.bashrc`, for example) within your staging server.

```
shell> mkdir -p /opt/continuent/software/conf
shell> export CONTINUENT_PROFILES=/opt/continuent/software/conf
shell> export REPLICATOR_PROFILES=/opt/continuent/software/replicator.conf
```

We now have a staging server setup, an SSH keypair for our login information, and are ready to start setting up each host within the cluster.

### C.2. Host Configuration

Each host in your cluster must be configured with the `tungsten` user, have the SSH key added, and then be configured to ensure the system and directories are ready for the Tungsten services to be installed and configured.

There are a number of key steps to the configuration process:

- Creating a user environment for the Tungsten service
- Creating the SSH authorization for the user on each host
- Configuring the directories and install locations
- Installing necessary software and tools
- Configuring `sudo` access to enable the configured user to perform administration commands

**Important**

The operations in the following sections must be performed on each host within your cluster. Failure to perform each step may prevent the installation and deployment of Tungsten cluster.

#### C.2.1. Creating the User Environment

The `tungsten` user should be created with a home directory that will be used to hold the Tungsten distribution files (not the installation files), and will be used to execute and create the different Tungsten services.

For Tungsten to work correctly, the `tungsten` user must be able to open a larger number of files/sockets for communication between the different components and processes as . You can check this by using `ulimit`:

```
shell> ulimit -a
core file size (blocks, -c)  8
```
The system should be configured to allow a minimum of 65535 open files. You should configure both the `tungsten` user and the database user with this limit by editing the `/etc/security/limits.conf` file:

```
tungsten    -    nofile    65535
mysql       -    nofile    65535
```

In addition, the number of running processes supported should be increased to ensure that there are no restrictions on the running processes or threads:

```
tungsten    -    nproc    8096
mysql       -    nproc    8096
```

You must logout and log back in again for the `ulimit` changes to take effect.

You may also need to set the limit settings on the specific service if your operating system uses the `systemctl` service management framework. To configure your file limits for the specific service:

1. Copy the MySQL service configuration file template to the configuration directory if it does not already exist:
   ```shell>
   sudo cp /lib/systemd/system/mysql.service /etc/systemd/system/
   ```
2. Edit the file, and add the following to the end of the configuration information:
   ```ini
   LimitNOFILE=Infinity
   
   This configures an unlimited number of open files, you can also specify a number, for example:
   ```ini
   LimitNOFILE=65535
   ```
3. Reload the systemctl daemon configuration:
   ```shell>
   sudo systemctl daemon-reload
   ```
4. Now restart the MySQL service:
   ```shell>
   service mysql restart
   ```

**Warning**

On Debian/Ubuntu hosts, limits are not inherited when using `su`/`sudo`. This may lead to problems when remotely starting or restarting services. To resolve this issue, uncomment the following line within `/etc/pam.d/su`:

```
session required pam_limits.so
```

Integration with AppArmor

Make sure that Apparmor, if configured, has been enabled to support access to the `/tmp` directory for the MySQL processes. For example, add the following to the MySQL configuration file (usually `/etc/apparmor.d/local/usr.sbin.mysqld`):

```
/tmp/** rwk
```

**C.2.2. Configuring Network and SSH Environment**

The hostname, DNS, IP address and accessibility of this information must be consistent. For the cluster to operate successfully, each host must be identifiable and accessible to each other host, either by name or IP address.

Individual hosts within your cluster must be reachable and most conform to the following:

- Do not use the `localhost` or `127.0.0.1` addresses.
- Do not use Zeroconf (`.local`) addresses. These may not resolve properly or fully on some systems.
- The server hostname [as returned by the `hostname`] must match the names you use when configuring your service.
Prerequisites

- The IP address that resolves on the hostname for that host must resolve to the IP address (not 127.0.0.1). The default configuration for many Linux installations is for the hostname to resolve to the same as `localhost`:

  127.0.0.1 localhost
  127.0.0.1 host1

- Each host in the cluster must be able to resolve the address for all the other hosts in the cluster. To prevent errors within the DNS system causing timeouts or bad resolution, all hosts in the cluster, in addition to the witness host, should be added to `/etc/hosts`:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>localhost</td>
</tr>
<tr>
<td>192.168.1.60</td>
<td>host1</td>
</tr>
<tr>
<td>192.168.1.61</td>
<td>host2</td>
</tr>
<tr>
<td>192.168.1.62</td>
<td>host3</td>
</tr>
<tr>
<td>192.168.1.63</td>
<td>host4</td>
</tr>
</tbody>
</table>

  In addition to explicitly adding hostnames to `/etc/hosts`, the name server switch file, `/etc/nsswitch.conf` should be updated to ensure that hosts are searched first before using DNS services. For example:

  ```
  hosts:      files dns
  ```

  **Important**

  Failure to add explicit hosts and change this resolution order can lead to transient DNS resolving errors triggering timeouts and failsafe switching of hosts within the cluster.

- The IP address of each host within the cluster must resolve to the same IP address on each node. For example, if `host1` resolves to 192.168.0.69 on `host1`, the same IP address must be returned when looking up `host1` on the host `host2`.

  To double check this, you should perform the following tests:

  1. Confirm the hostname:

     ```
     shell> uname -n
     ```

     **Warning**

     The hostname cannot contain underscores.

  2. Confirm the IP address:

     ```
     shell> hostname --ip-address
     ```

  3. Confirm that the hostnames of the other hosts in the cluster resolve correctly to a valid IP address. You should confirm on each host that you can identify and connect to each other host in the planned cluster:

     ```
     shell> nslookup host1
     shell> ping host1
     ```

     If the host does not resolve, either ensure that the hosts are added to the DNS service, or explicitly add the information to the `/etc/hosts` file.

     **Warning**

     If using `/etc/hosts` then you must ensure that the information is correct and consistent on each host, and double check using the above method that the IP address resolves correctly for every host in the cluster.

### Witness Hosts

Continuent Tungsten includes support for verifying the network status using a witness host.

Active Witness Hosts operate as standalone managers, and therefore require the same rights and requirements as a standard Continuent Tungsten host.

Passive Witness Hosts can be any stable network device. The passive witness host will be contacted using `ping` in the event of a network failure to confirm that network services are operational and that the problem is with an individual node.

#### C.2.2.1. Network Ports

The following network ports should be open between specific hosts to allow communication between the different components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Service</td>
<td>Database Host</td>
<td>Database Host</td>
<td>7</td>
<td>Checking availability</td>
</tr>
</tbody>
</table>
Prerequisites

<table>
<thead>
<tr>
<th>Component</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>#</td>
<td>#</td>
<td>2112</td>
<td>THL replication</td>
</tr>
<tr>
<td>#</td>
<td>#</td>
<td>#</td>
<td>7800-7805</td>
<td>Manager Remote Method Invocation (RMI)</td>
</tr>
<tr>
<td>#</td>
<td>#</td>
<td>#</td>
<td>9997</td>
<td>Manager Remote Method Invocation (RMI)</td>
</tr>
<tr>
<td>#</td>
<td>#</td>
<td>#</td>
<td>10000-10001</td>
<td>Replication connection listener port</td>
</tr>
<tr>
<td>#</td>
<td>#</td>
<td>#</td>
<td>11999-12000</td>
<td>Tungsten manager</td>
</tr>
<tr>
<td>Connector Service</td>
<td>Connector Host</td>
<td>Manager Hosts</td>
<td>11999</td>
<td>Tungsten manager</td>
</tr>
<tr>
<td>Connector Service</td>
<td>#</td>
<td>#</td>
<td>13306</td>
<td>Database connectivity</td>
</tr>
<tr>
<td>Client Application</td>
<td>Client</td>
<td>Connector</td>
<td>3306</td>
<td>Database connectivity for client</td>
</tr>
</tbody>
</table>

For composite clusters, communication between each cluster within the composite configuration can be limited to the following ports:

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database service</td>
<td>9997</td>
<td>Manager Remote Method Invocation (RMI)</td>
</tr>
<tr>
<td>#</td>
<td>2112</td>
<td>THL replication</td>
</tr>
<tr>
<td>#</td>
<td>11999-12000</td>
<td>Tungsten Manager</td>
</tr>
<tr>
<td>Client Application</td>
<td>13306</td>
<td>MySQL port for Connectivity</td>
</tr>
<tr>
<td>Manager Hosts</td>
<td>7</td>
<td>Communication between managers within composite clusters</td>
</tr>
</tbody>
</table>

For Multisite, Multimaster (MSMM) clusters that communicate through replication, the communication between sites can be limited to the following ports:

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>2114</td>
<td>THL replication</td>
</tr>
<tr>
<td>#</td>
<td>10002-10003</td>
<td>Replication connection listener ports</td>
</tr>
<tr>
<td>Client Application</td>
<td>13306</td>
<td>MySQL port for Connectivity</td>
</tr>
<tr>
<td>Manager Hosts</td>
<td>7</td>
<td>Communication between managers within multi-site, multi-master clusters</td>
</tr>
</tbody>
</table>

If a system has a firewall enabled, in addition to enabling communication between hosts as in the table above, the localhost must allow port-to-port traffic on the loopback connection without restrictions. For example, using `iptables` this can be enabled using the following command rule:

```shell
iptables -A INPUT -i lo --state NEW -j ACCEPT
```

### C.2.2.2. SSH Configuration

For password-less SSH to work between the different hosts in the cluster, you need to copy both the public and private keys between the hosts in the cluster. This will allow the staging server, and each host, to communicate directly with each other using the designated login.

To achieve this, on each host in the cluster:

1. Copy the public [.ssh/id_rsa.pub] and private key [.ssh/id_rsa] from the staging server to the .tungsten/.ssh directory.

2. Add the public key to the .ssh/authorized_keys file.

```shell
cat .ssh/id_rsa.pub >> .ssh/authorized_keys
```

3. Ensure that the file permissions on the .ssh directory are correct:

```shell
chmod 700 ~/.ssh
chmod 600 ~/.ssh/*
```

With each host configured, you should try to connecting to each host from the staging server to confirm that the SSH information has been correctly configured. You can do this by connecting to the host using `ssh`:

```shell
ssh tungsten@host
```

You should have logged into the host at the tungsten home directory, and that directory should be writable by the tungsten user.
Prerequisites

C.2.2.3. Host Availability Checks

The manager checks the availability of other hosts, for example to determine whether the host is still up, rather than just an individual service on that host. These checks must be able to be performed by one of the two available methods. Without these checks, it is possible for the availability of hosts to be falsely determined. These checks are performed using one of two protocols:

- **ping** — the preferred method using the system ping (ICMP) command.

- **default** — no longer the default method even though it is labeled that way. Uses the TCP/IP echo protocol on port 7. The port must be available on the source and destination host, not blocked by a system or network firewall.

The configuration of which service to use depends on the setting of the **--mgr-ping-method** option during configuration. If not option is given, **tpm** will test **ping** first and then try **default** after. An error will be thrown if neither option works for all members of the dataservice.

C.2.3. Directory Locations and Configuration

On each host within the cluster you must pick, and configure, a number of directories to be used by Continuent Tungsten™, as follows:

- **/tmp Directory**

The /tmp directory must be accessible and executable, as it is the location where some software will be extracted and executed during installation and setup. The directory must be writable by the tungsten user.

On some systems, the /tmp filesystem is mounted as a separate filesystem and explicitly configured to be non-executable [using the noexec filesystem option]. Check the output from the mount command.

- **Installation Directory**

Continuent Tungsten™ needs to be installed in a specific directory. The recommended solution is to use /opt/continuent. This information will be required when you configure the cluster service.

The directory should be created, and the owner and permissions set for the configured user:

```plaintext
shell> sudo mkdir /opt/continuent
shell> sudo chown -R tungsten: /opt/continuent
shell> sudo chmod 700 /opt/continuent
```

- **Home Directory**

The home directory of the tungsten user must be writable by that user.

C.2.4. Configure Software

Continuent Tungsten™ relies on the following software. Each host must use the same version of each tool.

<table>
<thead>
<tr>
<th>Software</th>
<th>Versions Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ruby</td>
<td>1.8.7, 1.9.3, or 2.0.0 to 2.4.0 or higher(^a)</td>
<td>JRuby is not supported</td>
</tr>
<tr>
<td>Ruby OpenSSL Module</td>
<td>-</td>
<td>Checking using ruby -ropenssl -e 'p &quot;works&quot;'</td>
</tr>
<tr>
<td>Ruby Gems</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Ruby io-console module</td>
<td>-</td>
<td>Install using gem install io-console(^b)</td>
</tr>
<tr>
<td>Ruby net-ssh module</td>
<td>-</td>
<td>Install using gem install net-ssh(^c)</td>
</tr>
<tr>
<td>Ruby net-scp module</td>
<td>-</td>
<td>Install using gem install net-scp(^d)</td>
</tr>
<tr>
<td>GNU tar</td>
<td>-</td>
<td>gtar is required for Solaris due to limitations in the native tar command</td>
</tr>
</tbody>
</table>

Java Runtime Environment | Java SE 7 [or compatible] |

\(^a\) Ruby 1.9.1 and 1.9.2 are not supported; these releases remove the execute bit during installation.

\(^b\) io-console is only needed for SSH activities, and only needed for Ruby v2.0 and greater.

\(^c\) For Ruby 1.8.7 the minimum version of net-ssh is 2.5.2, install using gem install net-ssh -v 2.5.2

\(^d\) For Ruby 1.8.7 the minimum version of net-scp is 1.0.4, install using gem install net-scp -v 10.4

These tools must be installed, running, and available to all users on each host.

To check the current version for any installed tool, login as the configured user (e.g. **tungsten**), and execute the command to get the latest version. For example:

- **Java**
Prerequisites

Run `java -version`:

```
shell> java -version
openjdk version "1.8.0_102"
OpenJDK Runtime Environment (build 1.8.0_102-b14)
OpenJDK 64-Bit Server VM (build 25.102-b14, mixed mode)
```

Continuent Tungsten is known to work with Java using the following JVMs:

- Oracle JVM/JDK 8
- OpenJDK 7

On certain environments, a separate tool such as `alternatives` (RedHat/CentOS) or `update-alternatives` (Debian/Ubuntu) may need to be used to switch Java versions globally or for individual users. For example, within CentOS:

```
shell> alternatives --display
```

**Important**

It is recommended to switch off all automated software and operating system update procedures. These can automatically install and restart different services which may be identified as failures by Tungsten Replicator. Software and Operating System updates should be handled by following the appropriate Section 5.14, “Performing Database or OS Maintenance” procedures.

It also recommended to install `ntp` or a similar time synchronization tool so that each host in the cluster has the same physical time.

C.2.5. sudo Configuration

Tungsten requires that the user you have configured to run the server has `sudo` credentials so that it can run and install services as `root`.

Within Ubuntu you can do this by editing the `/etc/sudoers` file using `visudo` and adding the following lines:

```
Defaults:tungsten   !authenticate
...              
# Allow tungsten to run any command
tungsten ALL=(ALL) ALL
```

For a secure environment where `sudo` access is not permitted for all operations, a minimum configuration can be used:

```
tungsten ALL=(ALL)
```

`sudo` can also be configured to handle only specific directories or files. For example, when using `xtrabackup`, or additional tools in the Tungsten toolkit, such as `tungsten_provision_slave`, additional commands must be added to the permitted list:

```
tungsten ALL=(ALL) NOPASSWD: /sbin/service, /usr/bin/innobackupex, /bin/rm, *
/bin/mv, /bin/chown, /bin/chmod, /usr/bin/scp, /bin/tar, /usr/bin/which, *
/etc/init.d/mysql, /usr/bin/test, *
/apps/tungsten/continuent/tungsten/tungsten-replicator/scripts/xtrabackup.sh, *
/apps/tungsten/continuent/tungsten/tools/tpm, /usr/bin/innobackupex-1.5.1, *
/bin/cat, /bin/find
```

Within Red Hat Linux add the following line:

```
tungsten ALL=(root) NOPASSWD: /usr/bin/which, /etc/init.d/mysql
```

For a secure environment where `sudo` access is not permitted for all operations, a minimum configuration can be used:

```
tungsten ALL=(root) NOPASSWD: ALL
```

When using `xtrabackup`, or additional tools in the Tungsten toolkit, such as `tungsten_provision_slave`, additional commands must be added to the permitted list:

```
tungsten ALL=(root) NOPASSWD: /sbin/service, /usr/bin/innobackupex, /bin/rm, *
/bin/mv, /bin/chown, /bin/chmod, /usr/bin/scp, /bin/tar, /usr/bin/which, *
/etc/init.d/mysql, /usr/bin/test, *
/apps/tungsten/continuent/tungsten/tungsten-replicator/scripts/xtrabackup.sh, *
/apps/tungsten/continuent/tungsten/tools/tpm, /usr/bin/innobackupex-1.5.1, *
/bin/cat, /bin/find
```

**Note**

On some versions of `sudo`, use of `sudo` is deliberately disabled for `ssh` sessions. To enable support via `ssh`, comment out the requirement for `requiretty`:

```
#Defaults requiretty
```
C.2.6. SELinux Configuration

Important
Tungsten best practice is to DISABLE SELinux.

If you are having problems, disable SELinux entirely and test fully. Once the system is fully operational and stable, then re-enable SELinux and see if the problem comes back. If so, then detailed configuration will be required. Such configuration is outside the scope of the Continuent Support Agreement.

To determine the current state of SELinux enforcement, use the `getenforce` command. For example:

```
shell> getenforce
Disabled
```

To disable SELinux, use the `setenforce` command. For example:

```
shell> setenforce 0
```

Warning
Disclaimer: Continuent support staff will do our best to help but can’t guarantee results. SELinux context errors are extremely difficult to debug, and difficult to determine the appropriate command to give the correct context. A simple “cp” command could carry an incorrect context to the destination. Since every system is different, the possible variations in configuration are endless.

Any suggestions below are just that - suggestions, and your mileage may vary. You have been warned.

When SELinux is enabled, systemctl may refuse to start mysqld if the listener port or location on disk have been changed. The solution is to inform SELinux about any changed or additional resources.

Tungsten best practice is to change the default MySQL port from 3306 to 13306 so that requesting clients do not accidentally connect directly to the database without being routed by the Connector.

If using a non-standard port for MySQL and SELinux is enabled, you must also change the port context, for example:

```
shell > semanage port -a -t mysqld_port_t -p tcp 13306
```

Ensure the file contexts are set correctly for SELinux. For example, to allow MySQL data to be stored in a non-standard location (i.e. `/data`):

```
shell > semanage fcontext -a -t etc_runtime_t /data
shell > restorecon -Rv /data/
shell > semanage fcontext -a -t mysql_db_t "/data(/.*)?"
shell > restorecon -Rv /data/*
```

C.3. MySQL Database Setup

For replication between MySQL hosts, you must configure each MySQL database server to support the required user names and core MySQL configuration.

Important
For MySQL extraction, Continuent Tungsten must have write access to the database so that status and progress information can be recorded correctly.

Note
Native MySQL replication should not be running when you install Continuent Tungsten™. The replication service will be completely handled by Continuent Tungsten™, and the normal replication, management and monitoring techniques will not provide you with the information you need.

C.3.1. MySQL Version Support

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>Support Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>5.0, 5.1, 5.5, 5.6, 5.7</td>
<td>Primary platform</td>
<td>Statement and row based replication is supported. MyISAM and InnoDB table types are fully supported; MyISAM tables may introduce replication errors during failover scenarios. JSON datatype support only available in Tungsten Replicator v5.3 onwards</td>
</tr>
<tr>
<td>Percona</td>
<td>5.5, 5.6, 5.7</td>
<td>Primary platform</td>
<td>Statement and row based replication is supported. MyISAM and InnoDB table types are fully supported; MyISAM tables may introduce replication errors during failover scenarios. JSON datatype support only available in Tungsten Replicator v5.3 onwards</td>
</tr>
</tbody>
</table>
### Prerequisites

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>Support Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MariaDB</td>
<td>5.5, 10.0, 10.1</td>
<td>Primary platform</td>
<td>failover scenarios. JSON datatype support only available in Tungsten Replicator v5.3 onwards</td>
</tr>
</tbody>
</table>

### C.3.2. MySQL Configuration

Each MySQL Server should be configured identically within the system. Although binary logging must be enabled on each host, replication should not be configured, since Tungsten Replicator will be handling that process.

The configured `tungsten` user must be able to read the MySQL configuration file (for installation) and the binary logs. Either the `tungsten` user should be a member of the appropriate group (i.e. `mysql`), or the permissions altered accordingly.

**Important**

Parsing of `mysqld_multi` configuration files is not currently supported. To use a `mysqld_multi` installation, copy the relevant portion of the configuration file to a separate file to be used during installation.

To setup your MySQL servers, you need to do the following:

- Configure your `my.cnf` settings. The following changes should be made to the `[mysqld]` section of your `my.cnf` file:

  - By default, MySQL is configured only to listen on the localhost address (127.0.0.1). The `bind-address` parameter should be checked to ensure that it is either set to a valid value, or commented to allow listening on all available network interfaces:
    ```
    #bind-address = 127.0.0.1
    ```
  
  - Specify the server id
    
    Each server must have a unique server id:
    ```
    server-id = 1
    ```

  - [Optional] Reconfigure the default MySQL TCP/IP port
    
    Change the listening port to 13306. The Tungsten Connector will listen on the normal port 3306 for MySQL connections and send them to the database using port 13306.
    ```
    port = 13306
    ```

    If you are not using Tungsten Connector, the setting can remain at the default of 3306.

  - Ensure that the maximum number of open files matches the configuration of the database user. This was configured earlier at 65535 files.
    ```
    open_files_limit = 65535
    ```

  - Enable binary logs
    
    Tungsten Replicator operates by reading the binary logs on each machine, so logging must be enabled:
    ```
    log-bin = mysql-bin
    ```

  - Set the `sync_binlog` parameter to 1 (one).

    **Note**

    In MySQL 5.7, the default value is 1.

    The MySQL `sync_binlog` parameter sets the frequency at which the binary log is flushed to disk. A value of zero indicates that the binary log should not be synchronized to disk, which implies that only standard operating system flushing of writes will occur. A value greater than one configures the binary log to be flushed only after `sync_binlog` events have been written. This can introduce a delay into writing information to the binary log, and therefore replication, but also opens the system to potential data loss if the binary log has not been flushed when a fatal system error occurs.

    Setting a value of value 1 (one) will synchronize the binary log on disk after each event has been written.
    ```
    sync_binlog = 1
    ```

  - Increase MySQL protocol packet sizes
The replicator can apply statements up to the maximum size of a single transaction, so the maximum allowed protocol packet size must be increased to support this:

```
max_allowed_packet = 52m
```

- **Configure InnoDB as the default storage engine**

  Continental Tungsten needs to use a transaction safe storage engine to ensure the validity of the database. The InnoDB storage engine also provides automatic recovery in the event of a failure. Using MyISAM can lead to table corruption, and in the event of a switchover or failure, and inconsistent state of the database, making it difficult to recover or restart replication effectively.

  InnoDB should therefore be the default storage engine for all tables, and any existing tables should be converted to InnoDB before deploying Continental Tungsten.

```
default-storage-engine = InnoDB
```

- **Configure InnoDB Settings**

  Tungsten Replicator creates tables and must use InnoDB tables to store the status information for replication configuration and application.

  The MySQL option `innodb_flush_log_at_trx_commit` configures how InnoDB writes and confirms writes to disk during a transaction. The available values are:

  - A value of 0 (zero) provides the best performance, but it does so at the potential risk of losing information in the event of a system or hardware failure. For use with Continental Tungsten™ the value should never be set to 0, otherwise the cluster health may be affected during a failure or failover scenario.
  
  - A value of 1 (one) provides the best transaction stability by ensuring that all writes to disk are flushed and committed before the transaction is returned as complete. Using this setting implies an increased disk load and so may impact the overall performance.

  When using Continental Tungsten™ in a multi-master, multi-site, fan-in or data critical cluster, the value of `innodb_flush_log_at_trx_commit` should be set to 1. This not only ensures that the transactional data being stored in the cluster are safely written to disk, this setting also ensures that the metadata written by Continental Tungsten™ describing the cluster and replication status is also written to disk and therefore available in the event of a failover or recovery situation.

  - A value of 2 (two) ensures that transactions are committed to disk, but data loss may occur if the disk data is not flushed from any OS or hardware-based buffering before a hardware failure, but the disk overhead is much lower and provides higher performance.

  This setting must be used as a minimum for all Continental Tungsten™ installations, and should be the setting for all configurations that do not require `innodb_flush_log_at_trx_commit` set to 1.

  At a minimum `innodb_flush_log_at_trx_commit` should be set to 2; a warning will be generated if this value is set to zero:

  ```
  innodb_flush_log_at_trx_commit = 2
  ```

  MySQL configuration settings can be modified on a running cluster, providing you switch your host to maintenance mode before reconfiguring and restarting MySQL Server. See Section 5.14, “Performing Database or OS Maintenance”.

  Optional configuration changes that can be made to your MySQL configuration:

  - **InnoDB Flush Method**

    ```
    innodb_flush_method=O_DIRECT
    ```

    The InnoDB flush method can effect the performance of writes within MySQL and the system as a whole.

    **O_DIRECT** is generally recommended as it eliminates double-buffering of InnoDB writes through the OS page cache. Otherwise, MySQL will be contending with Tungsten and other processes for pages there — MySQL is quite active and has a lot of hot pages for indexes and the like this can result lower i/o throughput for other processes.

    Tungsten particularly depends on the page cache being stable when using parallel apply. There is one thread that scans forward over the THL pages to coordinate the channels and keep them from getting too far ahead. We then depend on those pages staying in cache for a while so that all the channels can read them — as you are aware parallel apply works like a bunch of parallel table scans that are traveling like a school of sardines over the same part of the THL. If pages get kicked out again before all the channels see them, parallel replication will start to serialize as it has to wait for the OS to read them back in again. If they stay in memory on the other hand, the reads on the THL are in-memory, and fast. For more information on parallel replication, see Section 4.1, “Deploying Parallel Replication”.

  - **Increase InnoDB log file size**
Prerequisites

The default InnoDB log file size is 5MB. This should be increased to a larger file size, due to a known issue with xtrabackup during backup and restore operations.

To change the file size, read the corresponding information in the MySQL manual for configuring the file size information. See MySQL 5.1, MySQL 5.5, MySQL 5.6, MySQL 5.7.

**Binary Logging Format**

Tungsten Replicator works with both statement and row-based logging, and therefore also mixed-based logging. The chosen format is entirely up to the systems and preferences, and there are no differences or changes required for Tungsten Replicator to operate. For native MySQL to MySQL master/slave replication, either format will work fine.

Depending on the exact use case and deployment, different binary log formats imply different requirements and settings. Certain deployment types and environments require different settings:

- For multi-master deployment, use row-based logging. This will help to avoid data drift where statements make fractional changes to the data in place of explicit updates.
- Use row-based logging for heterogeneous deployments. All deployments to Oracle, MongoDB, Vertica and others rely on row-based logging.
- Use mixed replication if warnings are raised within the MySQL log indicating that statement only is transferring possibly dangerous statements.
- Use statement or mixed replication for transactions that update many rows; this reduces the size of the binary log and improves the performance when the transaction are applied on the slave.
- Use row replication for transactions that have temporary tables. Temporary tables are replicated if statement or mixed based logging is in effect, and use of temporary tables can stop replication as the table is unavailable between transactions. Using row-based logging also prevents these tables entering the binary log, which means they do not clog and delay replication.

The configuration of the MySQL server can be permanently changed to use an explicit replication by modifying the configuration in the configuration file:

```
binlog-format = row
```

**Note**

In MySQL 5.7, the default format is **ROW**.

For temporary changes during execution of explicit statements, the binlog format can be changed by executing the following statement:

```
mysql> SET binlog-format = ROW;
```

You must restart MySQL after any changes have been made.

- Ensure the **tungsten** user can access the MySQL binary logs by either opening up the directory permissions, or adding the **tungsten** user to the group owner for the directory.

### C.3.3. MySQL Configuration for Multimaster Deployments

If you are inserting to the same table at the same time at two or more different sites, and using bi-directional or multimaster replication, then special care must be taken to avoid primary key conflicts. Either the auto-increment keys on each need to be offset so they do not conflict, or the application needs to be able to generate unique keys taking multiple sites into account.

**Important**

The following configuration is required if your application is relying upon the MySQL-native auto-increment primary key feature:

Use the `auto-increment-increment` and `auto-increment-offset` variables to affect the way that MySQL generates the next value in an auto-increment field.

For example, edit `my.cnf` on all servers:

```
# for all servers at site 1
auto-increment-increment = 10
auto-increment-offset = 1
```
C.3.4. MySQL Configuration for Heterogeneous Deployments

The following are required for replication to heterogeneous targets to ensure that MySQL has been configured and generating row change information correctly:

- MySQL must be using Row-based replication for information to be replicated to heterogenous targets. For the best results, you should change the global binary log format, ideally in the configuration file \texttt{my.cnf}:

  \begin{verbatim}
  binlog-format = row
  \end{verbatim}

  Alternatively, the global binlog format can be changed by executing the following statement:

  \begin{verbatim}
  mysql> SET GLOBAL binlog-format = ROW;
  \end{verbatim}

  For MySQL 5.6.2 and later, you must enable full row log images:

  \begin{verbatim}
  binlog-row-image = full
  \end{verbatim}

  This information will be forgotten when the MySQL server is restarted; placing the configuration in the \texttt{my.cnf} file will ensure this option is permanently enabled.

- Table format should be updated to UTF8 by updating the MySQL configuration \texttt{my.cnf}:

  \begin{verbatim}
  character-set-server=utf8
  collation-server=utf8_general_ci
  \end{verbatim}

  Tables must also be configured as UTF8 tables, and existing tables should be updated to UTF8 support before they are replicated to prevent character set corruption issues.

- To prevent timezone configuration storing zone adjusted values and exporting this information to the binary log and PostgreSQL, fix the timezone configuration to use UTC within the configuration file \texttt{my.cnf}:

  \begin{verbatim}
  default-time-zone='+00:00'
  \end{verbatim}

C.3.5. MySQL User Configuration

- Tungsten User Login

  The \texttt{tungsten} user connects to the MySQL database and applies the data from the replication stream from other data sources in the data service. The user must therefore be able execute any SQL statement on the server, including grants for other users. The user must have the following privileges in addition to privileges for creating, updating and deleting DDL and data within the database:

  - \texttt{SUPER} privilege is required so that the user can perform all administrative operations including setting global variables.
  - \texttt{GRANT OPTION} privilege is required so that users and grants can be updated.

  To create a user with suitable privileges:

  \begin{verbatim}
  mysql> CREATE USER tungsten@'%' IDENTIFIED BY 'password';
  mysql> GRANT ALL ON *.* TO tungsten@'%' WITH GRANT OPTION;
  \end{verbatim}

  The connection will be made from the host to the local MySQL server. You may also need to create an explicit entry for this connection. For example, on the host \texttt{host1}, create the user with an explicit host reference:

  \begin{verbatim}
  mysql> CREATE USER tungsten@'host1' IDENTIFIED BY 'password';
  mysql> GRANT ALL ON *.* TO tungsten@'host1' WITH GRANT OPTION;
  \end{verbatim}

  The above commands enable logins from any host using the user name/password combination. If you want to limit the configuration to only include the hosts within your cluster you must create and grant individual user/host combinations:
Prerequisites

MySQL Application Login

Tungsten Connector requires a user that can be used as the application user to connect to the MySQL server. The login will allow connections to the MySQL databases servers to be used in a consistent fashion across different hosts within the cluster. You must configure this user with access to your database, and then use it as the ‘application’ user in your cluster configuration.

```
mysql> CREATE USER app_user@'%' IDENTIFIED BY 'password!';
```

Additional application user logins can be configured by using the `user.map` file within your Continuent Tungsten™ configuration.

As noted above, the creation of explicit host-specific user entries may be required.

C.4. Oracle Database Setup

Important

For Oracle extraction, Continuent Tungsten must have write access to the database so that status and progress information can be recorded correctly.

C.4.1. Oracle Version Support

<table>
<thead>
<tr>
<th>Database</th>
<th>Version</th>
<th>Support Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>10g Release 2</td>
<td>Primary Platform</td>
<td>Synchronous CDC is supported on Standard Edition only; Synchronous and Asynchronous are supported on Enterpris Editions</td>
</tr>
</tbody>
</table>

C.4.2. Oracle Environment Variables

Ensure the `tungsten` user being used for the master Tungsten Replicator service has the same environment setup as an Oracle database user. The user must have the following environment variables set:

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Sample Directory</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORACLE_HOME</td>
<td><code>/home/oracle/app/oracle/product/11.2.0/dbhome_2</code></td>
<td>The home directory of the Oracle installation.</td>
</tr>
<tr>
<td>LD_LIBRARY_PATH</td>
<td><code>$ORACLE_HOME/lib</code></td>
<td>The library directory of the Oracle installation.</td>
</tr>
<tr>
<td>ORACLE_SID</td>
<td><code>orcl</code></td>
<td>Oracle System ID for this installation.</td>
</tr>
<tr>
<td>JAVA_HOME</td>
<td></td>
<td>The home of the Java installation.</td>
</tr>
<tr>
<td>PATH</td>
<td><code>$ORACLE_HOME/bin:$JAVA_HOME/bin</code></td>
<td>Must include the Oracle and Java binary directories.</td>
</tr>
<tr>
<td>CLASSPATH</td>
<td><code>$ORACLE_HOME/ucp/lib/ucp-jar:$ORACLE_HOME/jdbc/lib/ojdbc6.jar:$CLASSPATH</code></td>
<td>Must include the key Oracle libraries the Oracle JDBC driver.</td>
</tr>
</tbody>
</table>

These should be set within the `.bashrc` or `.profile` to ensure these values are set correctly for all logins.

C.5. Prerequisite Checklist

To simplify the process of preparing your hosts, the checklist below is designed to provide a quick summary of the main prerequisites required.

A PDF version of this checklist can also be downloaded [here](#).

Host Specific

<table>
<thead>
<tr>
<th>Pre-Req</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create OS User – Typically called <code>tungsten</code></td>
<td></td>
</tr>
</tbody>
</table>
### Prerequisites

<table>
<thead>
<tr>
<th>Pre-Req</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set <strong>ulimit</strong> for OS User</td>
<td></td>
</tr>
<tr>
<td>Configure sudoers</td>
<td></td>
</tr>
<tr>
<td>Disable SELinux</td>
<td></td>
</tr>
<tr>
<td>Compile <code>/etc/hosts</code></td>
<td></td>
</tr>
<tr>
<td>Setup SSH between hosts</td>
<td></td>
</tr>
<tr>
<td>Create directory for installation [Typically, <code>/opt/continuent</code>]</td>
<td></td>
</tr>
<tr>
<td>Create directory for software package if using tar bundle [Typically, <code>/opt/continuent/software</code>]</td>
<td></td>
</tr>
<tr>
<td>Create directory for configuration file if INI Install (<code>/etc/tungsten</code>)</td>
<td></td>
</tr>
<tr>
<td>Check ownership of new directories set to new OS user</td>
<td></td>
</tr>
<tr>
<td>Install Ruby</td>
<td></td>
</tr>
<tr>
<td>Install Ruby gems: <code>net-ssh</code></td>
<td></td>
</tr>
<tr>
<td>Install Ruby gems: <code>net-scp</code></td>
<td></td>
</tr>
<tr>
<td>Install Java 8</td>
<td></td>
</tr>
</tbody>
</table>

### Network Specific

<table>
<thead>
<tr>
<th>Pre-Req</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure Network ports open</td>
<td></td>
</tr>
</tbody>
</table>

### Database Specific (All Topologies)

<table>
<thead>
<tr>
<th>Pre-Req</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure <code>server-id</code> unique amongst all nodes</td>
<td></td>
</tr>
<tr>
<td>Increase Open Files limits</td>
<td></td>
</tr>
<tr>
<td>Ensure <code>bin-log</code>ing enabled for cluster nodes, or source replicator nodes</td>
<td></td>
</tr>
<tr>
<td>Review <code>sync_binlog</code> parameter</td>
<td></td>
</tr>
<tr>
<td>Increase, if required, <code>max_allowed_packet</code></td>
<td></td>
</tr>
<tr>
<td>Review InnoDB settings</td>
<td></td>
</tr>
<tr>
<td>Set <code>binlog_format</code> to <code>ROW</code> [Essential for Multimaster or heterogeneous deployments]</td>
<td></td>
</tr>
<tr>
<td>Ensure <code>auto_increment</code> offsets adjusted for Multimaster deployments</td>
<td></td>
</tr>
<tr>
<td>Create DB user with FULL privileges and <code>GRANT OPTION</code> – typically called <code>tungsten</code> (Used by managers and replicators)</td>
<td></td>
</tr>
</tbody>
</table>

### Database Specific for Clustering Deployments

<table>
<thead>
<tr>
<th>Pre-Req</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change DB port from default (eg 13306)</td>
<td></td>
</tr>
<tr>
<td>Create user with FULL privileges except <code>SUPER</code>, for use by connectors – typically called <code>app_user</code></td>
<td></td>
</tr>
<tr>
<td>Ensure additional application DB user accounts have <code>REPLICATION_CLIENT</code> privilege (Only if connectors configured to use <code>SMARTSCALE</code>)</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D. Terminology Reference

Continuent Tungsten involves a number of different terminology that helps define different parts of the product, and specific areas of the output information from different commands. Some of this information is shared across different tools and systems.

This appendix includes a reference to the most common terms and terminology used across Continuent Tungsten.

D.1. Transaction History Log (THL)

The Transaction History Log (THL) stores transactional data from different data servers in a universal format that is then used to exchange and transfer the information between replicator instances. Because the THL is stored and independently managed from the data servers that it reads and writes, the data can be moved, exchanged, and transmuted during processing.

The THL is created by any replicator service acting as a master, where the information is read from the database using the native format, such as the MySQL binary log, or Oracle Change Data Capture (CDC), writing the information to the THL. Once in the THL, the THL data can be exchanged with other processes, including transmission over the network, and then applied to a destination database. Within Tungsten Replicator, this process is handled through the pipeline stages that read and write information between the THL and internal queues.

Information stored in THL is recorded in a series of event records in sequential format. The THL therefore acts as a queue of the transactions. On a replicator reading data from a database, the THL represents the queue of transactions applied on the source database. On a replicator applying that information to a database, the THL represents the list of the transactions to be written. The THL has the following properties:

- THL is a sequential list of events
- THL events are written to a THL file through a single thread (to enforce the sequential nature)
- THL events can be read from individually or sequentially, and multiple threads can read the same THL at the same time
- THL events are immutable; once stored, the contents of the THL are never modified or individually deleted (although entire files may be deleted)
- THL is written to disk without any buffering to prevent software failure causing a problem; the operating system buffers are used.

THL data is stored on disk within the \texttt{thl} directory of your Tungsten Replicator installation. The exact location can configured using \texttt{logDir} parameter of the THL component. A sample directory is shown below:

```
total 710504
-rw-r--r-- 1 tungsten tungsten         0 May  2 10:48 disklog.lck
-rw-r--r-- 1 tungsten tungsten 100042900 Jun  4 10:10 thl.data.00000000013
-rw-r--r-- 1 tungsten tungsten 100185311 Jun  4 11:41 thl.data.00000000014
-rw-rw-r-- 1 tungsten tungsten 100441159 Jun  4 11:41 thl.data.00000000015
-rw-rw-r-- 1 tungsten tungsten 10089492 Jun  4 11:44 thl.data.00000000016
-rw-rw-r-- 1 tungsten tungsten 10035613 Jun  4 11:44 thl.data.00000000017
-rw-rw-r-- 1 tungsten tungsten 100035516 Jun  4 11:44 thl.data.00000000018
-rw-rw-r-- 1 tungsten tungsten 101698669 Jun  4 11:45 thl.data.00000000019
-rw-rw-r-- 1 tungsten tungsten 23886641 Jun  5 21:55 thl.data.00000000020
```

The THL files have the format \texttt{thl.data.#########}, and the sequence number increases for each new log file. The size of each log file is controlled by the \texttt{--thl-log-file-size} configuration parameter. The log files are automatically managed by Tungsten Replicator, with old files automatically removed according to the retention policy set by the \texttt{--thl-log-retention} configuration parameter. The files can be manually purged or moved. See Section E.1.5.1, “Purging THL Log Information on a Slave”.

The THL can be viewed and managed by using the \texttt{thl} command. For more information, see Section 8.17, “The \texttt{thl} Command”.

D.1.1. THL Format

The THL is stored on disk in a specific format that combines the information about the SQL and row data, metadata about the environment in which the row changes and SQL changes were made (metadata), and the log specific information, including the source, database, and timestamp of the information.

A sample of the output is shown below, the information is taken from the output of the \texttt{thl} command:

```
SEQ# = 0 / FRAG# = 0 (last frag)
TIME = 2013-03-21 18:47:39.0
EPOCH# = 0
EVENTID = mysql-bin.000010:0000000000000439:0
SOURCEID = host1
METADATA = [mysql_server_id=10;dbms_type=mysql;is_metadata=true;service=dsone;]
```

In versions up to 5.3.2:

```
SEQ# = 0 / FRAG# = 0 (last frag)
TIME = 2013-03-21 18:47:39.0
EPOCH# = 0
EVENTID = mysql-bin.000010:0000000000000439:0
SOURCEID = host1
METADATA = [mysql_server_id=10;dbms_type=mysql;is_metadata=true;service=dsone;]
```
The sample above shows the information for the SQL executed on a MySQL server. The `EVENT_ID` [493] shows the MySQL binary log from which the statement has been read. The MySQL server has stored the information in the binary log using `STATEMENT` or `MIXED` mode; log events written in `ROW` mode store the individual row differences. A summary of the THL stored format information, including both hidden values and the information included in the `thl` command output is provided in Table D.1, "THL Event Format".

### Table D.1. THL Event Format

<table>
<thead>
<tr>
<th>Displayed Field</th>
<th>Internal Name</th>
<th>Data type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>record_length</td>
<td>Integer</td>
<td>4 bytes</td>
<td>Length of the full record information, including this field</td>
</tr>
<tr>
<td>-</td>
<td>record_type</td>
<td>Byte</td>
<td>1 byte</td>
<td>Event record type identifier</td>
</tr>
<tr>
<td>-</td>
<td>header_length</td>
<td>Unsigned int</td>
<td>4 bytes</td>
<td>Length of the header information</td>
</tr>
<tr>
<td><strong>SEQ#</strong>[492]</td>
<td>seqno</td>
<td>Unsigned long</td>
<td>8 bytes</td>
<td>Log sequence number, a sequential value given to each log entry</td>
</tr>
<tr>
<td><strong>FRAG#</strong>[492]</td>
<td>fragno</td>
<td>Unsigned short</td>
<td>2 bytes</td>
<td>Event fragment number. An event can consist of multiple fragments of SQL or row log data</td>
</tr>
<tr>
<td>-</td>
<td>last_frag</td>
<td>Byte</td>
<td>1 byte</td>
<td>Indicates whether the fragment is the last fragment in the sequence</td>
</tr>
<tr>
<td><strong>EPOCH#</strong>[493]</td>
<td>epoch_number</td>
<td>Unsigned long</td>
<td>8 bytes</td>
<td>Event epoch number. Used to identify log sections within the master THL</td>
</tr>
<tr>
<td><strong>SOURCEID</strong>[493]</td>
<td>source_id</td>
<td>UTF-8 String</td>
<td>Variable (null terminated)</td>
<td>Event source ID, the hostname or identity of the dataserver that generated the event</td>
</tr>
<tr>
<td><strong>EVENTID</strong>[493]</td>
<td>event_id</td>
<td>UTF-8 String</td>
<td>Variable (null terminated)</td>
<td>Event ID; in MySQL, for example, the binlog file-name and position that contained the original event</td>
</tr>
<tr>
<td><strong>SHARDID</strong>[494]</td>
<td>shard_id</td>
<td>UTF-8 String</td>
<td>Variable (null terminated)</td>
<td>Shard ID to which the event belongs</td>
</tr>
<tr>
<td><strong>TIME</strong>[493]</td>
<td>tstamp</td>
<td>Unsigned long</td>
<td>8 bytes</td>
<td>Time of the commit that triggered the event</td>
</tr>
<tr>
<td>-</td>
<td>data_length</td>
<td>Unsigned int</td>
<td>4 bytes</td>
<td>Length of the included event data</td>
</tr>
<tr>
<td>-</td>
<td>event</td>
<td>Binary</td>
<td>Variable</td>
<td>Serialized Java object containing the SQL or ROW data</td>
</tr>
<tr>
<td><strong>METADATA</strong>[493]</td>
<td>Part of event</td>
<td>-</td>
<td>-</td>
<td>Metadata about the event</td>
</tr>
<tr>
<td><strong>TYPE</strong>[493]</td>
<td>Part of event</td>
<td>-</td>
<td>-</td>
<td>Internal storage type of the event</td>
</tr>
<tr>
<td><strong>OPTIONS</strong>[493]</td>
<td>Part of event</td>
<td>-</td>
<td>-</td>
<td>Options about the event operation</td>
</tr>
<tr>
<td><strong>SCHEMA</strong>[494]</td>
<td>Part of event</td>
<td>-</td>
<td>-</td>
<td>Schema used in the event</td>
</tr>
<tr>
<td><strong>SQL</strong>[494]</td>
<td>Part of event</td>
<td>-</td>
<td>-</td>
<td>SQL statement or row data</td>
</tr>
<tr>
<td>-</td>
<td>crc_method</td>
<td>Byte</td>
<td>1 byte</td>
<td>Method used to compute the CRC for the event.</td>
</tr>
<tr>
<td>-</td>
<td>crc</td>
<td>Unsigned int</td>
<td>4 bytes</td>
<td>CRC of the event record (not including the CRC value)</td>
</tr>
</tbody>
</table>

**SEQ#**[492] and **FRAG#**[492]

Individual events within the log are identified by a sequential **SEQUENCE**[492] number. Events are further divided into individual fragments. Fragments are numbered from 0 within a given sequence number. Events are applied to the database wholesale, fragments are used to divide up the size of the statement or row information within the log file. The fragments are stored internally in memory before being applied to the database and therefore memory usage is directly affected by the size and number of fragments held in memory.

The sequence number as generated during this process is unique and therefore acts as a global transaction ID across a cluster. It can be used to determine whether the slaves and master are in sync, and can be used to identify individual transactions within the replication stream.
• **EPOCH** [493]

   The *EPOCH* value is used as a check to ensure that the logs on the slave and the master match. The *EPOCH* is stored in the THL, and a new *EPOCH* is generated each time a master goes online. The *EPOCH* value is then written and stored in the THL alongside each individual event. The *EPOCH* acts as an additional check, beyond the sequence number, to validate the information between the slave and the master. The *EPOCH* value is used to prevent the following situations:

   - In the event of a failover where there are events stored in the master log, but which did not make it to a slave, the *EPOCH* acts as a check so that when the master rejoins as the slave, the *EPOCH* numbers will not match the slave and the new master. The trapped transactions be identified by examining the THL output.
   
   - When a slave joins a master, the existence of the *EPOCH* prevents the slave from accepting events that happen to match only the sequence number, but not the corresponding *EPOCH*.

Each time a Tungsten Replicator master goes online, the *EPOCH* number is incremented. When the slave connects, it requests the *SEQUENCE* and *EPOCH*, and the master confirms that the requested *SEQUENCE* has the requested *EPOCH*. If not, the request is rejected and the slave gets a validation error:

```
pendingExceptionMessage: Client handshake failure: Client response validation failed: «
  Log epoch numbers do not match: client source ID=west-db2 seqno=408129 »
  server epoch number=408128 client epoch number=189069
```

When this error occurs, the THL should be examined and compared between the master and slave to determine if there really is a mismatch between the two databases. For more information, see Section 5.8, “Managing Transaction Failures”.

• **SOURCEID** [493]

   The *SOURCEID* is a string identifying the source of the event stored in the THL. Typically it is the hostname or host identifier.

• **EVENTID** [493]

   The *EVENTID* is a string identifying the source of the event information in the log. Within a MySQL installed, the *EVENTID* contains the binary log name and position which provided the original statement or row data.

   **Note**

   The event ID shown is the end of the corresponding event stored in the THL, not the beginning. When examining the mysqlbinlog for an sequence ID in the THL, you should check the EVENTID of the previous THL sequence number to determine where to start looking within the binary log.

• **TIME** [493]

   When the source information is committed to the database, that information is stored into the corresponding binary log (MySQL) or CDC (Oracle). That information is stored in the THL. The time recorded in the THL is the time the data was committed, not the time the data was recorded into the log file.

   The *TIME* value as stored in the THL is used to compute latency information when reading and applying data on a slave.

• **METADATA** [493]

   Part of the binary *EVENT* payload stored within the event fragment, the metadata is collected and stored in the fragment based on information generated by the replicator. The information is stored as a series of key/value pairs. Examples of the information stored include:

   - MySQL server ID
   - Source database type
   - Name of the Replicator service that generated the THL
   - Any 'heartbeat' operations sent through the replicator service, including those automatically generated by the service, such as when the master goes online
   - The name of the shard to which the event belongs
   - Whether the contained data is safe to be applied through a block commit operation

• **TYPE** [493]

   The stored event type. Replicator has the potential to use a number of different stored formats for the THL data. The default type is based on the `com.continuent.tungsten.replicator.event.ReplDBMSEvent`.

• **OPTIONS** [493]
Part of the EVENT binary payload, the OPTIONS [493] include information about the individual event that have been extracted from the database. These include settings such as the autocommit status, character set and other information, which is used when the information is applied to the database.

There will be one OPTIONS [493] block for each SQL [494] statement stored in the event.

- **SCHEMA [494]**
  
  Part of the EVENT structure, the SCHEMA [494] provides the database or schema name in which the statement or row data was applied.

- **SHARDID [494]**
  
  When using parallel apply, provides the generated shard ID for the event when it is applied by the parallel applier thread.

- **SQL [494]**
  
  For statement based events, the SQL of the statement that was recorded. Multiple individual SQL statements as part of a transaction can be contained within a single event fragment.

For example, the MySQL statement:

```sql
mysql> INSERT INTO user VALUES (null, 'Charles', now());
Query OK, 1 row affected (0.01 sec)
```

Stores the following into the THL:

```
SEQ# = 3583 / FRAG# = 0 (last frag)
- TIME = 2013-05-27 11:49:45.0
- EPOCH = 2500
- EVENTID = mysql-bin.000007:0000000625753960;0
- SOURCEID = host1
- METADATA = [mysql_server_id=1687011;dbms_type=mysql;service=firstrep;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
  SQL(0) = SET INSERT_ID = 3
  OPTIONS = [##charset = ISO8859_1, autocommit = 1, sql_auto_is_null = 0, foreign_key_checks = 1, unique_checks = 1, sql_mode = '', character_set_client = 8, collation_connection = 8, collation_server = 8]
  SCHEMA = test
  SQL(1) = INSERT INTO user VALUES (null, 'Charles', now()) /* ___SERVICE___ = [firstrep] */
```

For row based events, the information is further defined by the individual row data, including the action type (UPDATE, INSERT or DELETE), SCHEMA [494], TABLE [494] and individual ROW data. For each ROW, there may be one or more COL [494] (column) and identifying KEY [494] event to identify the row on which the action is to be performed.

The same statement when recorded in ROW [494] format:

```
SEQ# = 3582 / FRAG# = 0 (last frag)
- TIME = 2013-05-27 11:45:19.0
- EPOCH = 2500
- EVENTID = mysql-bin.000007:0000000625753710;0
- SOURCEID = host1
- METADATA = [mysql_server_id=1687011;dbms_type=mysql;service=firstrep;shard=test]
- TYPE = com.continuent.tungsten.replicator.event.ReplDBMSEvent
  SQL(0) =
  - ACTION = INSERT
  - SCHEMA = test
  - TABLE = user
  - ROW# = 0
    - COL(1): = 2
    - COL(2): = Charles
    - COL(3): = 2013-05-27 11:45:19.0
```

### D.2. Generated Field Reference

When using any of the tools within Continuent Tungsten status information is output using a common set of fields that describe different status information. These field names and terms are constant throughout all of the different tools. A description of each of these different fields is provided below.

#### D.2.1. Terminology: Fields **accessFailures**

#### D.2.2. Terminology: Fields **active**
D.2.3. Terminology: Fields activeSeqno

D.2.4. Terminology: Fields appliedLastEventId

The event ID from the source database of the last corresponding event from the stage that has been applied to the database.

MySQL

When extracting from MySQL, the output from `trepctl` shows the MySQL binary log file and the byte position within the log where the transaction was extracted:

```
shell> trepctl status
Processing status command...
NAME VALUE
... appliedLastEventId : mysql-bin.000064:0000000002757461;0
...```

Oracle CDC

When extracting from Oracle using the CDC method, the event ID is composed of the Oracle SCN number:

```
NAME VALUE
... appliedLastEventId : ora:16626156
```  

Oracle Redo Reader

When extracting from Oracle using the Redo Reader method, the event ID is composed of a combination of Oracle SCN, transaction, and PLOG file numbers, separated by a hash symbol:

```
NAME VALUE
... appliedLastEventId : 8931871791244#0018.002.000196e1#LAST#8931871791237#180644
```  

The format is:

```
COMMITSCN#XID#LCR#MINSCN#PLOGSEQ
```

- COMMITSCN
  Last committed Oracle System Change Number (SCN).
- XID
  Transaction ID.
- LCR
  Last committed record number.
- MINSCN
  Minimum stored Oracle SCN.
- PLOGSEQ
  PLOG file sequence number.

D.2.5. Terminology: Fields appliedLastSeqno

The last sequence number for the transaction from the Tungsten stage that has been applied to the database. This indicates the last actual transaction information written into the slave database.

```
appliedLastSeqno : 212
```  

When using parallel replication, this parameter returns the minimum applied sequence number among all the channels applying data.

D.2.6. Terminology: Fields appliedLatency

The `appliedLatency` is the latency between the commit time of the source event and the time the last committed transaction reached the end of the corresponding pipeline within the replicator.
Within a master, this indicates the latency between the transaction commit time and when it was written to the THL. In a slave, it indicates the latency between the commit time on the master database and when the transaction has been committed to the destination database. Clocks must be synchronized across hosts for this information to be accurate.

| appliedLatency : 0.828 |

The latency is measured in seconds. Increasing latency may indicate that the destination database is unable to keep up with the transactions from the master.

In replicators that are operating with parallel apply, `appliedLatency` indicates the latency of the trailing channel. Because the parallel apply mechanism does not update all channels simultaneously, the figure shown may trail significantly from the actual latency.

D.2.7. Terminology: Fields `applier.class`

Classname of the current applier engine

D.2.8. Terminology: Fields `applier.name`

Name of the current applier engine

D.2.9. Terminology: Fields `applyTime`

D.2.10. Terminology: Fields `autoRecoveryEnabled`

Indicates whether autorecovery has been enabled by setting the `--auto-recovery-max-attempts`. The field indicates the value as either `true` or `false` accordingly.

D.2.11. Terminology: Fields `autoRecoveryTotal`

A count of the number of times the replicator has used autorecovery to go back online since the replicator was started. This can be used to determine if autorecovery has been used. More details on autorecovery can be found in the `trepsvc.log` file.

The counter is reset when the replicator determines that the replicator has successfully gone online after an autorecovery.

D.2.12. Terminology: Fields `averageBlockSize`

D.2.13. Terminology: Fields `blockCommitRowCount`


D.2.15. Terminology: Fields `channel`

D.2.16. Terminology: Fields `channels`

The number of channels being used to apply transactions to the target dataserver. In a standard replication setup there is typically only one channel. When parallel replication is in effect, there will be more than one channel used to apply transactions.

| channels : 1 |

D.2.17. Terminology: Fields `clusterName`

The name of the cluster. This information is different to the service name and is used to identify the cluster, rather than the individual service information being output.

D.2.18. Terminology: Fields `commits`

D.2.19. Terminology: Fields `committedMinSeqno`
D.2.20. Terminology: Fields criticalPartition

D.2.21. Terminology: Fields currentBlockSize

D.2.22. Terminology: Fields currentEventId

   Event ID of the transaction currently being processed

D.2.23. Terminology: Fields currentLastEventId

D.2.24. Terminology: Fields currentLastFragno

D.2.25. Terminology: Fields currentLastSeqno


   The current time on the host, in milliseconds since the epoch. This information can used to confirm that the time on different hosts is within a suitable limit. Internally, the information is used to record the time when transactions are applied, and may therefore the appliedLatency figure.

D.2.27. Terminology: Fields dataServerHost

D.2.28. Terminology: Fields discardCount

D.2.29. Terminology: Fields doChecksum

D.2.30. Terminology: Fields estimatedOfflineInterval

D.2.31. Terminology: Fields eventCount

D.2.32. Terminology: Fields extensions

D.2.33. Terminology: Fields extractTime

D.2.34. Terminology: Fields extractor.class

D.2.35. Terminology: Fields extractor.name

D.2.36. Terminology: Fields filter.#.class

D.2.37. Terminology: Fields filter.#.name

D.2.38. Terminology: Fields filterTime
D.2.39. Terminology: Fields *flushIntervalMillis*

D.2.40. Terminology: Fields *fsyncOnFlush*

D.2.41. Terminology: Fields *headSeqno*

D.2.42. Terminology: Fields *intervalGuard*

D.2.43. Terminology: Fields *lastCommittedBlockSize*

The *lastCommittedBlockSize* contains the size of the last block that was committed as part of the block commit procedure. The value is only displayed on appliers and defines the number of events in the last block. By comparing this value to the configured block commit size, the commit type can be determined.

For more information, see Section 11.1, "Block Commit".

D.2.44. Terminology: Fields *lastCommittedBlockTime*

The *lastCommittedBlockTime* contains the duration since the last committed block. The value is only displayed on appliers and defines the number of seconds since the last block was committed. By comparing this value to the configured block interval, the commit type can be determined.

For more information, see Section 11.1, "Block Commit".

D.2.45. Terminology: Fields *latestEpochNumber*

D.2.46. Terminology: Fields *logConnectionTimeout*

D.2.47. Terminology: Fields *logDir*

D.2.48. Terminology: Fields *logFileRetainMillis*

D.2.49. Terminology: Fields *logFileSize*

D.2.50. Terminology: Fields *masterConnectUri*

The URI being used to extract THL information. On a master, the information may be empty, or may contain the reference to the underlying extractor source where information is being read.

On a slave, the URI indicates the host from which THL data is being read:

```
masterConnectUri : thl://host1:2112/
```

In a secure installation where SSL is being used to exchange data, the URI protocol will be *thls*:

```
masterConnectUri : thls://host1:2112/
```

D.2.51. Terminology: Fields *masterListenUri*

The URI on which the replicator is listening for incoming slave requests. On a master, this is the URI used to distribute THL information.

```
masterListenUri : thls://host1:2112/
```

D.2.52. Terminology: Fields *maxChannel*
D.2.53. Terminology: Fields  maxDelayInterval

D.2.54. Terminology: Fields  maxOfflineInterval

D.2.55. Terminology: Fields  maxSize

D.2.56. Terminology: Fields  maximumStoredSeqNo

The maximum transaction ID that has been stored locally on the machine in the THL. Because Tungsten Replicator operates in stages, it is sometimes important to compare the sequence and latency between information being ready from the source into the THL, and then from the THL into the database. You can compare this value to the appliedLastSeqno, which indicates the last sequence committed to the database. The information is provided at a resolution of milliseconds.

maximumStoredSeqNo : 25

D.2.57. Terminology: Fields  minimumStoredSeqNo

The minimum transaction ID stored locally in the THL on the host:

minimumStoredSeqNo : 0

The figure should match the lowest transaction ID as output by the thl index command. On a busy host, or one where the THL information has been purged, the figure will show the corresponding transaction ID as stored in the THL.

D.2.58. Terminology: Fields  name

D.2.59. Terminology: Fields  offlineRequests

Contains the specifications of one or more future offline events that have been configured for the replicator. Multiple events are separated by a semicolon:

shell> trepctl status
...
    minimumStoredSeqNo : 0
    offlineRequests : Offline at sequence number: 5262; Offline at time: 2014-01-01 00:00:00 EST
    pendingError : NONE

D.2.60. Terminology: Fields  otherTime

D.2.61. Terminology: Fields  pendingError


D.2.63. Terminology: Fields  pendingErrorEventId

D.2.64. Terminology: Fields  pendingErrorSeqno

The sequence number where the current error was identified

D.2.65. Terminology: Fields  pendingExceptionMessage

The current error message that caused the current replicator offline

D.2.66. Terminology: Fields  pipelineSource

The source for data for the current pipeline. On a master, the pipeline source is the database that the master is connected to and extracting data from. Within a slave, the pipeline source is the master replicator that is providing THL data.
D.2.67. Terminology: Fields processedMinSeqno

D.2.68. Terminology: Fields queues

D.2.69. Terminology: Fields readOnly

D.2.70. Terminology: Fields relativeLatency

The relativeLatency is the latency between now and timestamp of the last event written into the local THL. This information gives an indication of how fresh the incoming THL information is. On a master, it indicates whether the master is keeping up with transactions generated on the master database. On a slave, it indicates how up to date the THL read from the master is.

A large value can either indicate that the database is not busy, that a large transaction is currently being read from the source database, or from the master replicator, or that the replicator has stalled for some reason.

An increasing relativeLatency on the slave may indicate that the replicator may have stalled and stopped applying changes to the dataserver.

D.2.71. Terminology: Fields resourcePrecedence

D.2.72. Terminology: Fields rmiPort

D.2.73. Terminology: Fields role

The current role of the host in the corresponding service specification. Primary roles are master and slave.

D.2.74. Terminology: Fields seqnoType

The internal class used to store the transaction ID. In MySQL replication, the sequence number is typically stored internally as a Java Long [java.lang.Long]. In heterogeneous replication environments, the type used may be different to match the required information from the source database.

D.2.75. Terminology: Fields serializationCount

D.2.76. Terminology: Fields serialized

D.2.77. Terminology: Fields serviceName

The name of the configured service, as defined when the deployment was first created through tpm.

```
serviceName : alpha
```

A replicator may support multiple services. The information is output to confirm the service information being displayed.

D.2.78. Terminology: Fields serviceType

The configured service type. Where the replicator is on the same host as the database, the service is considered to be local. When reading or write to a remote dataserver, the service is remote.

D.2.79. Terminology: Fields shard_id

D.2.80. Terminology: Fields simpleServiceName

A simplified version of the serviceName.
D.2.81. Terminology: Fields siteName

D.2.82. Terminology: Fields sourceId

D.2.83. Terminology: Fields stage

D.2.84. Terminology: Fields started

D.2.85. Terminology: Fields state

D.2.86. Terminology: Fields stopRequested

D.2.87. Terminology: Fields store.

D.2.88. Terminology: Fields storeClass

D.2.89. Terminology: Fields syncInterval

D.2.90. Terminology: Fields taskCount

D.2.91. Terminology: Fields taskId

D.2.92. Terminology: Fields timeInStateSeconds

D.2.93. Terminology: Fields timeoutMillis

D.2.94. Terminology: Fields totalAssignments

D.2.95. Terminology: Fields transitioningTo

D.2.96. Terminology: Fields uptimeSeconds

D.2.97. Terminology: Fields version
Appendix E. Files, Directories, and Environment

E.1. The Continuent Tungsten Install Directory

Any Continuent Tungsten™ installation creates an installation directory that contains the software and the additional directories where active information, such as the transaction history log and backup data is stored. A sample of the directory is shown below, and a description of the individual directories is provided in Table E.1, “Continuent Tungsten Directory Structure”.

```
shell> ls -al /opt/continuent
```

```
total 40
drwxr-xr-x  9 tungsten root  4096 Mar 21 18:47 .
drwxr-xr-x  3 root root  4096 Mar 21 18:00 ..
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:44 backups
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:47 conf
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:44 relay
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:47 releases
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:47 service_logs
drwxrwxr-x  2 tungsten tungsten 4096 Mar 21 18:47 share
drwxrwxr-x  3 tungsten tungsten 4096 Mar 21 18:44 thl
lnwxrwxrwx  1 tungsten tungsten   62 Mar 21 18:47 tungsten -> /opt/continuent/releases/continuent-tungsten-2.8.3-11_pid31409
```

The directories shown in the table are relative to the installation directory, the recommended location is /opt/continuent. For example, the THL files would be located in /opt/continuent/thl.

**Table E.1. Continuent Tungsten Directory Structure**

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backups</td>
<td>Default directory for backup file storage</td>
</tr>
<tr>
<td>conf</td>
<td>Configuration directory with a copy of the current and past configurations</td>
</tr>
<tr>
<td>relay</td>
<td>Location for relay logs if relay logs have been enabled.</td>
</tr>
<tr>
<td>releases</td>
<td>Contains one or more active installations of the Continuent Tungsten software, referenced according to the version number and active process ID.</td>
</tr>
<tr>
<td>service-logs</td>
<td>Logging information for the active installation</td>
</tr>
<tr>
<td>share</td>
<td>Active installation information, including the active JAR for the MySQL connection</td>
</tr>
<tr>
<td>thl</td>
<td>The Transaction History Log files, stored in a directory named after each active service.</td>
</tr>
<tr>
<td>tungsten</td>
<td>Symbolic link to the currently active release in releases.</td>
</tr>
</tbody>
</table>

Some advice for the contents of specific directories within the main installation directory are described in the following sections.

E.1.1. The backups Directory

The **backups** directory is the default location for the data and metadata from any backup performed manually or automatically by Continuent Tungsten™. The backup data and metadata for each backup will be stored in this directory.

An example of the directory content is shown below:

```
shell> ls -al /opt/continuent/backups/
```

```
total 130788
drwxrwxr-x  2 tungsten tungsten      4096 Apr  4 16:09 .
drwxrwxr-x  3 tungsten tungsten      4096 Apr  4 11:51 ..
-rw-r--r--  1 tungsten tungsten        71 Apr  4 16:09 storage.index
-rw-r--r--  1 tungsten tungsten 133907646 Apr  4 16:09 store-0000000001-mysqldump_2013-04-04_16-08_42.sql.gz
-rw-r--r--  1 tungsten tungsten       317 Apr  4 16:09 store-0000000001.properties
```

The **storage.index** contains the backup file index information. The actual backup data is stored in the GZipped file. The properties of the backup file, including the tool used to create the backup, and the checksum information, are location in the corresponding .properties file. Note that each backup and property file is uniquely numbered so that you can identify and restore a specific backup.

Different backups scripts and methods may place their backup information in a separate subdirectory. For example, **xtrabackup** stores backup data into /opt/continuent/backups/xtrabackup.

E.1.1.1. Automatically Deleting Backup Files

The Tungsten Replicator will automatically remove old backup files. This is controlled by the **--repl-backup-retention** setting and defaults to 3. Use the **tpm update** command to modify this setting. Following the successful creation of a new backup, the number of backups will be
compared to the retention value. Any excess backups will be removed from the /opt/continuent/backups directory or whatever directory is configured for --repl-backup-directory [346].

The backup retention will only remove files starting with store. If you are using a backup method that creates additional information then those files may not be fully removed until the next backup process begins. This includes xtrabackup-full, xtrabackup-incremental and any snapshot based backup methods. You may manually clean these excess files if space is needed before the next backup method. If you delete information associated with an existing backup, any attempts to restore it will fail.

### E.1.1.2. Manually Deleting Backup Files

If you no longer need one or more backup files, you can delete the files from the filesystem. You must delete both the SQL data, and the corresponding properties file. For example, from the following directory:

```
shell> ls -al /opt/continuent/backups
```

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Apr 16</td>
<td>13:57</td>
<td>.</td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Apr 16</td>
<td>13:54</td>
<td>..</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>71</td>
<td>Apr 16</td>
<td>13:56</td>
<td>storage.index</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>517170</td>
<td>Apr 15</td>
<td>18:02</td>
<td>store-0000000004-mysqldump-13324673891435527.sql</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>310</td>
<td>Apr 15</td>
<td>18:02</td>
<td>store-0000000004.properties</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>781991444</td>
<td>Apr 16</td>
<td>13:57</td>
<td>store-0000000006-mysqldump-3081853249977885370.sql</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>314</td>
<td>Apr 16</td>
<td>13:57</td>
<td>store-0000000006.properties</td>
</tr>
</tbody>
</table>

To delete the backup files for index 4:

```
shell> rm /opt/continuent/backups/alpha/store-0000000004*
```

See the information in Section E.1.1.3, “Copying Backup Files” about additional files related to a single backup. There may be additional files associated with the backup that you will need to manually remove.

**Warning**

Removing a backup should only be performed if you know that the backup is safe to be removed and will not be required. If the backup data is required, copy the backup files from the backup directory before deleting the files in the backup directory to make space.

### E.1.1.3. Copying Backup Files

The files created during any backup can copied to another directory or system using any suitable means. Once the backup has been completed, the files will not be modified or updated and are therefore safe to be moved or actively copied to another location without fear of corruption of the backup information.

There are multiple files associated with each backup. The number of files will depend on the backup method that was used. All backups will use at least two files in the /opt/continuent/backups directory.

```
$ ls -al /opt/continuent/backups
```

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Apr 16</td>
<td>13:57</td>
<td>.</td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Apr 16</td>
<td>13:54</td>
<td>..</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>71</td>
<td>Apr 16</td>
<td>13:56</td>
<td>storage.index</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>517170</td>
<td>Apr 15</td>
<td>18:02</td>
<td>store-0000000004-mysqldump-13324673891435527.sql</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>310</td>
<td>Apr 15</td>
<td>18:02</td>
<td>store-0000000004.properties</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>781991444</td>
<td>Apr 16</td>
<td>13:57</td>
<td>store-0000000006-mysqldump-3081853249977885370.sql</td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>tungsten</td>
<td>tungsten</td>
<td>314</td>
<td>Apr 16</td>
<td>13:57</td>
<td>store-0000000006.properties</td>
</tr>
</tbody>
</table>

```
$ scp store-[0-9]* host3:$PWD/
```

```
store-0000000001-full_xtrabackup_2014-08-16_15-44_86                   100%   70     0.1KB/s   00:00
store-0000000001.properties                                            100%  314     0.3KB/s   00:00
```

**Note**

Check the ownership of files if you have trouble transferring files or restoring the backup. They should be owned by the Tungsten system user to ensure proper operation.

If xtrabackup-full method was used, you must transfer the corresponding directory from /opt/continuent/backups/xtrabackup. In this example that would be /opt/continuent/backups/xtrabackup_full_xtrabackup_2014-08-16_15-44_86.

```
$ cd /opt/continuent/backups
$ scp store-[0-9]* host3:$PWD/                                          
store-0000000001-full_xtrabackup_2014-08-16_15-44_86                   100%   70     0.1KB/s   00:00
store-0000000001.properties                                            100%  314     0.3KB/s   00:00
```

If the xtrabackup-incremental method was used, you must transfer multiple directories. In addition to the corresponding directory from /opt/continuent/backups/xtrabackup you must transfer all xtrabackup-incremental directories since the most recent xtrabackup-full backup and then transfer that xtrabackup-full directory. See the example below for further explanation:

```
$ ls -ltr /opt/continuent/backups/xtrabackup/
```

<table>
<thead>
<tr>
<th>Mode</th>
<th>User</th>
<th>Group</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Oct 16</td>
<td>20:55</td>
<td>incr_xtrabackup_2014-10-16_20-55_73</td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Oct 17</td>
<td>20:55</td>
<td>full_xtrabackup_2014-10-17_20-55_1</td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Oct 19</td>
<td>20:57</td>
<td>incr_xtrabackup_2014-10-19_20-57_76</td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>tungsten</td>
<td>tungsten</td>
<td>4096</td>
<td>Oct 20</td>
<td>20:58</td>
<td>full_xtrabackup_2014-10-20_20-57_43</td>
</tr>
</tbody>
</table>

```
$ rsync -azE ssh full_xtrabackup_2014-08-16_15-44_86 host3:$PWD/          
```

```
503```
In this example there are two instances of `xtrabackup-full` backups and four `xtrabackup-incremental` backups.

- To restore either of the `xtrabackup-full` backups then they would be copied to the target host on their own.
- To restore `incr_xtrabackup_2014-10-21_20-58_97`, it must be copied along with `full_xtrabackup_2014-10-20_20-57_41`.
- To restore `incr_xtrabackup_2014-10-19_20-57_76`, it must be copied along with `incr_xtrabackup_2014-10-18_20-55_38` and `full_xtrabackup_2014-10-17_20-55_1`.

### E.1.1.4. Relocating Backup Storage

If the filesystem on which the main installation directory is running out of space and you need to increase the space available for backup files without interrupting the service, you can use symbolic links to relocate the backup information.

**Note**

When using an NFS mount point when backing up with `xtrabackup`, the command must have the necessary access rights and permissions to change the ownership of files within the mounted directory. Failure to update the permissions and ownership will cause the `xtrabackup` command to fail. The following settings should be made on the directory:

- Ensure the `no_root_squash` option on the NFS export is not set.
- Change the group and owner of the mount point to the `tungsten` user and `mysql` group:
  ```shell```
  chown tungsten /mnt/backups
  chgrp mysql /mnt/backups
  ```
  Owner and group IDs on NFS directories must match across all the hosts using the NFS mount point. Inconsistencies in the owner and group IDs may lead to backup failures.

- Change the permissions to permit at least owner and group modifications:
  ```shell```
  chmod 770 /mnt/backups
  ```
- Mount the directory:
  ```shell```
  mount host1:/exports/backups /mnt/backups
  ```

The backup directory can be changed using two different methods:

- **Section E.1.1.4.1, “Relocating Backup Storage using Symbolic Links”**
- **Section E.1.1.4.2, “Relocating Backup Storage using Configuration Changes”**

#### E.1.1.4.1. Relocating Backup Storage using Symbolic Links

To relocate the backup directory using symbolic links:

1. Ensure that no active backup is taking place of the current host. Your service does not need to be offline to complete this operation.

2. Create a new directory, or attach a new filesystem and location on which the backups will be located. You can use a directory on another filesystem or connect to a SAN, NFS or other filesystem where the new directory will be located. For example:
  ```shell```
  mkdir /mnt/backupdata/continuent
  ```

3. **Optional**

Copy the existing backup directory to the new directory location. For example:
  ```shell```
  rsync -r /opt/continuent/backups/* /mnt/backupdata/continuent/
  ```

4. Move the existing directory to a temporary location:
  ```shell```
  mv /opt/continuent/backups /opt/continuent/old-backups
  ```

5. Create a symbolic link from the new directory to the original directory location:
  ```shell```
  ln -s /mnt/backupdata/continuent /opt/continuent/backups
  ```
The backup directory has now been moved. If you want to verify that the new backup directory is working, you can optionally run a backup and ensure that the backup process completes correctly.

### E.1.4.2. Relocating Backup Storage using Configuration Changes

To relocate the backup directory by reconfiguration:

1. Ensure that no active backup is taking place of the current host. Your service does not need to be offline to complete this operation.

2. Create a new directory, or attach a new filesystem and location on which the backups will be located. You can use a directory on another filesystem or connect to a SAN, NFS or other filesystem where the new directory will be located. For example:

```shell
mkdir /mnt/backupdata/continuent
```

3. Optional

   Copy the existing backup directory to the new directory location. For example:

   ```shell
rsync -r /opt/continuent/backups/* /mnt/backupdata/continuent/
```

4. Following the directions for `tpm update` to apply the `--backup-directory=/mnt/backupdata/continuent` setting.

The backup directory has now been moved. If you want to verify that the new backup directory is working, you can optionally run a backup and ensure that the backup process completes correctly.

### E.1.2. The `releases` Directory

The `releases` directory contains a copy of each installed release. As new versions are installed and updated (through `tpm update`), a new directory is created with the corresponding version of the software.

For example, a number of releases are listed below:

```shell
ll /opt/continuent/releases/
```

```
total 20
drwxr-xr-x 5 tungsten mysql 4896 May 23 16:19 ./
drwxr-xr-x 9 tungsten mysql 4896 May 23 16:19 ../
drwxr-xr-x 10 tungsten mysql 4896 May 23 16:19 continuent-tungsten-2.0.5-11_pid16184/
drwxr-xr-x 10 tungsten mysql 4896 May 23 16:19 continuent-tungsten-2.0.5-11_pid14577/
drwxr-xr-x 10 tungsten mysql 4896 May 23 16:19 continuent-tungsten-2.0.5-11_pid23747/
drwxr-xr-x 10 tungsten mysql 4896 May 23 16:19 continuent-tungsten-2.0.5-11_pid24978/
```

The latest release currently in use can be determined by checking the symbolic link, `tungsten` within the installation directory. For example:

```shell
ll /opt/continuent
```

```
total 40
drwxr-xr-x 9 tungsten mysql 4896 May 23 16:19 ./
drwxr-xr-x 3 root root 4096 Apr 29 16:09 ../
drwxr-xr-x 2 tungsten mysql 4896 May 30 13:27 backups/
drwxr-xr-x 2 tungsten mysql 4896 May 23 16:19 conf/
drwxr-xr-x 3 tungsten mysql 4896 May 10 19:09 relay/
drwxr-xr-x 5 tungsten mysql 4896 May 23 16:19 releases/
drwxr-xr-x 2 tungsten mysql 4896 May 10 19:09 service_logs/
drwxr-xr-x 2 tungsten mysql 4896 May 23 16:18 share/
drwxr-xr-x 3 tungsten mysql 4896 May 10 19:09 thl/
lrwxrwxrwx 1 tungsten mysql 63 May 23 16:19 tungsten -> /opt/continuent/releases/continuent-tungsten-2.0.5-11_pid24978/
```

If multiple services are running on the host, search for `.pid` files within the installation directory to determine which release directories are currently in use by an active service:

```shell
find /opt/continuent -name "*.pid"
```

```
/p/t/continuent/releases/continuent-tungsten-2.0.5-11_pid24978/tungsten-replicator/var/treplicator.pid
/p/t/continuent/releases/continuent-tungsten-2.0.5-11_pid24978/tungsten-connector/var/tconnector.pid
/p/t/continuent/releases/continuent-tungsten-2.0.5-11_pid24978/tungsten-manager/var/tmanager.pid
```

Directories within the `releases` directory that are no longer being used can be safely removed.

### E.1.3. The `service_logs` Directory

The `service_logs` directory contains links to the log files for the currently active release. The directory contains the following links:

- `connector.log` — a link to the Tungsten Connector log.
- `tmsvc.log` — a link to the Continuent Tungsten manager log.
- `trepsvc.log` — a link to the Tungsten Replicator log.
E.1.4. The share Directory

The share directory contains information that is shared among all installed releases and instances of Continuent Tungsten. Unlike other directories, the share directory is not overwritten or replaced during installation or update using `tpm`. This means that the directory can be used to hold information, such as filter configurations, without the contents being removed when the installation is updated.

E.1.5. The thl Directory

The transaction history log (THL) retains a copy of the SQL statements from each master host, and it is the information within the THL that is transferred between hosts and applied to the database. The THL information is written to disk and stored in the thl directory:

```
$ ls -al /opt/continuent/thl/alpha/
```

THL files are created on both the master and slaves within the cluster. THL data can be examined using the `thl` command. The THL is written into individual files, which are by default, no more than 1 GB in size each. From the listing above, you can see that each file has a unique file index number. A new file is created when the file size limit is reached, and given the next THL log file number. To determine the sequence number that is stored within log, use the `thl` command:

```
$ thl index
```

The THL files are retained for seven days by default, although this parameter is configurable. Due to the nature and potential size required to store the information for the THL, you should monitor the disk space and usage.

The purge is continuous and is based on the date the log file was written. Each time the replicator finishes the current THL log file, it checks for files that have exceeded the defined retention configuration and spawns a job within the replicator to delete files older than the retention policy. Old files are only removed when the current THL log file rotates.
E.1.5.1. Purging THL Log Information on a Slave

Warning

Purging the THL on a slave node can potentially remove information that has not yet been applied to the database. Please check and ensure that the THL data that you are purging has been applied to the database before continuing.

The THL files can be explicitly purged to recover disk space, but you should ensure that the currently applied sequence no to the database is not purged, and that additional hosts are not reading the THL information.

To purge the logs on a SLAVE node:

1. Determine the highest sequence number from the THL that you want to delete. To purge the logs up until the latest sequence number, you can use `trepctl` to determine the highest applied sequence number:

```
shell> trepctl services
Processing services command...
NAME    VALUE
------    -----....
appliedLastSeqno : 3672
appliedLatency   : 331.0
role            : slave
serviceName     : alpha
serviceType     : local
started         : true
state           : ONLINE
Finished services command...
```

2. Shun the slave datasource and put the replicator into the offline state using `cctrl`:

```
shell> cctrl
[LOGICAL] /alpha > datasource host1 shun
[LOGICAL] /alpha > replicator host1 offline
```

Important

NEVER Shun the Master datasource!

3. Use the `thl` command to purge the logs up to the specified transaction sequence number. You will be prompted to confirm the operation:

```
shell> thl purge -high 3672
WARNING: The purge command will break replication if you delete all events or delete events that have not reached all slaves.
Are you sure you wish to delete these events [y/N]?
y
Deleting events where SEQ# <=3670
2013-04-16 14:09:42,384 [ - main] INFO  thl.THLManagerCtrl Transactions deleted
```

4. Recover the host back into the cluster:

```
shell> cctrl
[LOGICAL] /alpha > datasource host1 recover
```

You can now check the current THL file information:

```
shell> thl index
LogIndexEntry thl.data.0000000024(3240:3672)
```

For more information on purging events using `thl`, see Section 8.17.4, "thl purge Command".

E.1.5.2. Purging THL Log Information on a Master

Warning

Purging the THL on a Master node can potentially remove information that has not yet been applied to the slave databases. Please check and ensure that the THL data that you are purging has been applied to the database on all slaves before continuing.

Important

If the situation allows, it may be better to switch the Master role to a current, up-to-date slave, then perform the steps to purge THL from a slave on the old master host using Section E.1.5.1, "Purging THL Log Information on a Slave".
Warning

Follow the below steps with great caution! Failure to follow best practices will result in slaves unable to apply transactions, forcing a full re-provisioning. For those steps, please see Section 5.6.1.1, "Provision or Reprovision a Slave".

The THL files can be explicitly purged to recover disk space, but you should ensure that the currently applied sequence no to the database is not purged, and that additional hosts are not reading the THL information.

To purge the logs on a MASTER node:

1. Determine the highest sequence number from the THL that you want to delete. To purge the logs up until the latest sequence number, you can use `trepctl` to determine the highest applied sequence number:

   ```
   shell> trepctl services
   Processing services command...
   NAME     VALUE
   appliedLastSeqno: 3675
   appliedLatency : 0.835
   role        : master
   serviceName : alpha
   serviceType : local
   started     : true
   state       : ONLINE
   Finished services command...
   ```

2. Set the cluster to Maintenance mode and put the replicator into the offline state using `cctrl`:

   ```
   shell> cctrl
   [LOGICAL] /alpha > set policy maintenance
   [LOGICAL] /alpha > replicator host1 offline
   ```

3. Use the `thl` command to purge the logs up to the specified transaction sequence number. You will be prompted to confirm the operation:

   ```
   shell> thl purge -high 3670
   WARNING: The purge command will break replication if you delete all events or delete events that have not reached all slaves.
   Are you sure you wish to delete these events [y/N]?
   y
   Deleting events where SEQ# <=3670
   2013-04-16 14:09:42,384 [ - main] INFO thl.THLManagerCtrl Transactions deleted
   ```

4. Set the cluster to Automatic mode and put the replicator online using `cctrl`:

   ```
   shell> cctrl
   [LOGICAL] /alpha > replicator host1 online
   [LOGICAL] /alpha > set policy automatic
   ```

You can now check the current THL file information:

```
shell> thl index
LogIndexEntry thl.data.0000000024(3240:3672)
```  

For more information on purging events using `thl`, see Section 8.17.4, "thl purge Command".

E.1.5.3. Moving the THL File Location

The location of the THL directory where THL files are stored can be changed, either by using a symbolic link or by changing the configuration to point to the new directory:

- Changing the directory location using symbolic links can be used in an emergency if the space on a filesystem has been exhausted. See Section E.1.5.3.1, "Relocating THL Storage using Symbolic Links"

- Changing the directory location through reconfiguration can be used when a permanent change to the THL location is required. See Section E.1.5.3.2, "Relocating THL Storage using Configuration Changes".

E.1.5.3.1. Relocating THL Storage using Symbolic Links

In an emergency, the directory currently holding the THL information, can be moved using symbolic links to relocate the files to a location with more space.

Moving the THL location requires updating the location for a slave by temporarily setting the slave offline, updating the THL location, and re-enabling back into the cluster:

1. Shun the datasource and switch your node into the offline state using `cctrl`
2. Create a new directory, or attach a new filesystem and location on which the THL content will be located. You can use a directory on another filesystem or connect to a SAN, NFS or other filesystem where the new directory will be located. For example:

```
shell> mkdir /mnt/data/thl
```

3. Copy the existing THL directory to the new directory location. For example:

```
shell> rsync -r /opt/continuent/thl/* /mnt/data/thl/
```

4. Move the existing directory to a temporary location:

```
shell> mv /opt/continuent/thl /opt/continuent/old-thl
```

5. Create a symbolic link from the new directory to the original directory location:

```
shell> ln -s /mnt/data/thl /opt/continuent/thl
```

6. Recover the host back into the cluster:

```
shell> cctrl -expert
[LOGICAL:EXPERT] /alpha > datasource host1 recover
```

To change the THL location on a master:

1. Manually promote an existing slave to be the new master:

```
[LOGICAL] /alpha > switch to host2
SELECTED SLAVE: host2@alpha
PURGE REMAINING ACTIVE SESSIONS ON CURRENT MASTER 'host1@alpha'
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON MASTER 'host1@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host1@alpha'
PUT THE NEW MASTER 'host2@alpha' ONLINE
PUT THE PRIOR MASTER 'host1@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host1@alpha' TO POINT TO NEW MASTER 'host2@alpha'
SWITCH TO 'host2@alpha' WAS SUCCESSFUL
```

2. Update the THL location as provided in the previous sequence.

3. Switch the updated slave back to be the master:

```
[LOGICAL] /alpha > switch to host1
SELECTED SLAVE: host1@alpha
PURGE REMAINING ACTIVE SESSIONS ON CURRENT MASTER 'host2@alpha'
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON MASTER 'host2@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host2@alpha'
PUT THE NEW MASTER 'host1@alpha' ONLINE
PUT THE PRIOR MASTER 'host2@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host2@alpha' TO POINT TO NEW MASTER 'host1@alpha'
SWITCH TO 'host1@alpha' WAS SUCCESSFUL
```

## E.1.5.3.2. Relocating THL Storage using Configuration Changes

To permanently change the directory currently holding the THL information can be reconfigured to a new directory location.

To update the location for a slave by temporarily setting the slave offline, updating the THL location, and re-enabling back into the cluster:

1. Shun the datasource and switch your node into the offline state using `cctrl`:

```
shell> cctrl -expert
[LOGICAL:EXPERT] /alpha > datasource host1 shun
[LOGICAL:EXPERT] /alpha > replicator host1 offline
```

2. Create a new directory, or attach a new filesystem and location on which the THL content will be located. You can use a directory on another filesystem or connect to a SAN, NFS or other filesystem where the new directory will be located. For example:

```
shell> mkdir /mnt/data/thl
```

3. Copy the existing THL directory to the new directory location. For example:

```
shell> rsync -r /opt/continuent/thl/* /mnt/data/thl/
```

4. Change the directory location using `tpm` to update the configuration for a specific host:
5. Recover the host back into the cluster:

```shell
shell> cctrl -expert
[LOGICAL:EXPERT] /alpha > datasource host1 recover
```

To change the TBL location on a master:

1. Manually promote an existing slave to be the new master:

```shell
[LOGICAL] /alpha > switch to host2
SELECTED SLAVE: host2@alpha
PURGE REMAINING ACTIVE SESSIONS ON CURRENT MASTER 'host1@alpha'
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON MASTER 'host1@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host1@alpha'
PUT THE NEW MASTER 'host2@alpha' ONLINE
PUT THE PRIOR MASTER 'host1@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host3@alpha' TO POINT TO NEW MASTER 'host2@alpha'
SWITCH TO 'host2@alpha' WAS SUCCESSFUL
```

2. Update the TBL location as provided in the previous sequence.

3. Switch the updated slave back to be the master:

```shell
[LOGICAL] /alpha > switch to host1
SELECTED SLAVE: host1@alpha
PURGE REMAINING ACTIVE SESSIONS ON CURRENT MASTER 'host2@alpha'
PURGED A TOTAL OF 0 ACTIVE SESSIONS ON MASTER 'host2@alpha'
FLUSH TRANSACTIONS ON CURRENT MASTER 'host2@alpha'
PUT THE NEW MASTER 'host1@alpha' ONLINE
PUT THE PRIOR MASTER 'host2@alpha' ONLINE AS A SLAVE
RECONFIGURING SLAVE 'host3@alpha' TO POINT TO NEW MASTER 'host1@alpha'
SWITCH TO 'host1@alpha' WAS SUCCESSFUL
```

E.1.5.4. Changing the TBL Retention Times

TBL files are by default retained for seven days, but the retention period can be adjusted according to the requirements of the service. Longer times retain the logs for longer, increasing disk space usage while allowing access to the TBL information for longer. Shorter logs reduce disk space usage while reducing the amount of log data available.

**Note**

The files are automatically managed by Continuent Tungsten. Old TBL files are deleted only when new data is written to the current files. If there has been no TBL activity, the log files remain until new TBL information is written.

Use the `tpm update` command to apply the `--repl-thl-log-retention` setting. The replication service will be restarted on each host with updated retention configuration.

E.1.6. The **tungsten** Directory

```
shell> ls -l /opt/continuent/tungsten/
```

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bristlecone</td>
<td>Contains the bristlecone load-testing tools.</td>
</tr>
<tr>
<td>cluster-home</td>
<td>Home directory for the main tools, configuration and libraries of the Continuent Tungsten installation.</td>
</tr>
<tr>
<td>cookbook</td>
<td>Cookbook installation and testing tools.</td>
</tr>
<tr>
<td>INSTALL</td>
<td>Text file describing the basic installation process for Continuent Tungsten</td>
</tr>
<tr>
<td>README.LICENSES</td>
<td>Software license information.</td>
</tr>
</tbody>
</table>
Files, Directories, and Environment

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tools</td>
<td>Directory containing the tools for installing and configuring Continuent Tungsten.</td>
</tr>
<tr>
<td>tungsten-connector</td>
<td>Installed directory of the Tungsten Connector installation.</td>
</tr>
<tr>
<td>tungsten-manager</td>
<td>Installed directory of the Tungsten Manager installation.</td>
</tr>
<tr>
<td>tungsten-replicator</td>
<td>Installed directory of the Tungsten Replicator installation.</td>
</tr>
</tbody>
</table>

E.1.6.1. The **tungsten-connector** Directory

This directory holds all of the files, libraries, configuration and other information used to support the installation of Tungsten Connector.

E.1.6.1.1. The **tungsten-connector** Directory

This directory holds library files specific to Tungsten Connector. When perform patches or extending functionality specifically for Tungsten Connector, JAR files can be placed into this directory.

E.1.6.2. The **tungsten-manager** Directory

This directory holds all of the files, libraries, configuration and other information used to support the installation of Tungsten Manager.

E.1.6.2.1. The **tungsten-manager/lib** Directory

This directory holds library files specific to Tungsten Manager. When perform patches or extending functionality specifically for Tungsten Manager, JAR files can be placed into this directory.

E.1.6.3. The **tungsten-replicator** Directory

This directory holds all of the files, libraries, configuration and other information used to support the installation of Tungsten Manager.

E.1.6.3.1. The **tungsten-replicator/lib** Directory

This directory holds library files specific to Tungsten Replicator. When perform patches or extending functionality specifically for Tungsten Replicator, for example when adding JDBC libraries for other databases, the JAR files can be placed into this directory.

E.1.6.3.2. The **tungsten-replicator/scripts** Directory

This directory contains scripts used to support Tungsten Replicator operation.

E.2. Log Files

E.3. Environment Variables

- **$CONTINUENT_PROFILES**

  This environment variable is used by `tpm` as the location for storing the `deploy.cfg` file that is created by `tpm` during a `tpm configure` or `tpm install` operation. For more information, see Section 9.3, “`tpm` Staging Configuration”.

- **$REPLICATOR_PROFILES**

  When using `tpm` with Tungsten Replicator, `$REPLICATOR_PROFILES` is used for storing the `deploy.cfg` file during configuration and installation. If `$REPLICATOR_PROFILES` does not exist, then `$CONTINUENT_PROFILES` if it exists. For more information, see Section 9.3, “`tpm` Staging Configuration”.

- **$CONTINUENT_ROOT**

  The `$CONTINUENT_ROOT` variable is created by the `env.sh` file that is created when installing Continuent Tungsten. When defined, the variable will contain the installation directory of the corresponding Continuent Tungsten installation.

On hosts where multiple installations have been created, the variable can be used to point to different installations.
Appendix F. Internals

Continuent Tungsten includes a number of different systems and elements to provide the core services and functionality. Some of these are designed only to be customer-configured. Others should be changed only on the advice of Continuent or Continuent support. This chapter covers a range of different systems that are designated as internal features and functionality.

This chapter contains information on the following sections of Continuent Tungsten:

- **Section F.1, “Extending Backup and Restore Behavior”** — details on how the backup scripts operate and how to write custom backup scripts.
- **Section F.2, “Character Sets in Database and Continuent Tungsten”** — covers how character sets affect replication and command-line tool output.
- **Section F.4, “Memory Tuning and Performance”** — information on how the memory is used and allocated within Continuent Tungsten.

F.1. Extending Backup and Restore Behavior

The backup and restore system within Continuent Tungsten is handled entirely by the replicator. When a backup is initiated, the replicator on the specified datasource is asked to start the backup process.

The backup and restore system both use a modular mechanism that is used to perform the actual backup or restore operation. This can be configured to use specific backup tools or a custom script.

F.1.1. Backup Behavior

When a backup is requested, the Tungsten Replicator performs a number of separate, discrete, operations designed to perform the backup operation.

The backup operation performs the following steps:

1. Tungsten Replicator identifies the filename where properties about the backup will be stored. The file is used as the primary interface between the underlying backup script and Tungsten Replicator.

2. Tungsten Replicator executes the configured backup/restore script, supplying any configured arguments, and the location of a properties file, which the script updates with the location of the backup file created during the process.

3. If the backup completes successfully, the file generated by the backup process is copied into the configured Continuent Tungsten directory (for example, `/opt/continuent/backups`).

4. Tungsten Replicator updates the property information with a CRC value for the backup file and the standard metadata for backups, including the tool used to create the backup.

A log is created of the backup process into a file according to the configured backup configuration. For example, when backing up using `mysqldump` the log is written to the log directory as `mysqldump.log`. When using a custom script, the log is written to `script.log`.

As standard, Tungsten Replicator supports two primary backup types, `mysqldump` and `xtrabackup`. A third option is based on the incremental version of the `xtrabackup` tool. The use of external backup script enables additional backup tools and methods to be supported.

To create a custom backup script, see **Section F.1.3, “Writing a Custom Backup/Restore Script”** for a list of requirements and samples.

F.1.2. Restore Behavior

The restore operation operates in a similar manner to the backup operation. The same script is called (but supplied with the `--restore` command-line option).

The restore operation performs the following steps:

1. Tungsten Replicator creates a temporary properties file, which contains the location of the backup file to be restored.

2. Tungsten Replicator executes the configured backup/restore script in restore mode, supplying any configured arguments, and the location of the properties file.

3. The script used during the restore process should read the supplied properties file to determine the location of the backup file.

4. The script performs all the necessary steps to achieve the restore process, including stopping the dataserver, restoring the data, and restarting the dataserver.
5. The replicator will remain in the OFFLINE state once the restore process has finished.

F.1.3. Writing a Custom Backup/Restore Script

The synopsis of the custom script is as follows:

```
SCRIPT { -backup-restore } -properties FILE -options OPTIONS
```

Where:

- `-backup` — indicates that the script should work in the backup mode and create a backup.
- `-restore` — indicates that the script should work in the restore mode and restore a previous backup.
- `-properties` — defines the name of the properties file. When called in `backup` mode, the properties file should be updated by the script with the location of the generated backup file. When called in `restore` mode, the file should be examined by the script to determine the backup file that will be used to perform the restore operation.
- `-options` — specifies any unique options to the script.

The custom script must support the following:

- The script must be capable of performing both the backup and the restore operation. Tungsten Replicator selects the operation by providing the `-backup` or `-restore` option to the script on the command-line.
- The script must parse command-line arguments to extract the operation type, properties file and other settings.
- Accept the name of the properties file to be used during the backup process. This is supplied on the command-line using the format:

  ```
  -properties FILENAME
  ```

  The properties file is used by Tungsten Replicator to exchange information about the backup or restore.

- Must parse any additional options supplied on the command-line using the format:

  ```
  -options ARG1=VAL1&ARG2=VAL2
  ```

- Must be responsible for executing whatever steps are required to create a consistent snapshot of the dataserver

- Must place the contents of the database backup into a single file. If the backup process generates multiple files, then the contents should be packaged using `tar` or `zip`.

The script has to determine the files that were generated during the backup process and collect them into a single file as appropriate.

- Must update the supplied properties with the name of the backup file generated, as follows:

  ```
  file=BACKUPFILE
  ```

  If the file has not been updated with the information, or the file cannot be found, then the backup is considered to have failed.

Once the backup process has completed, the backup file specified in the properties file will be moved to the configured backup location (for example `/opt/continuent/backups`).

- Tungsten Replicator will forward all `STDOUT` and `STDERR` from the script to the log file `script.log` within the log directory. This file is recreated each time a backup is executed.

- Script should have an exit (return) value of 0 for success, and 1 for failure. The script is responsible for handling any errors in the underlying backup tool or script used to perform the backup, but it must then pass the corresponding success or failure condition using the exit code.

A sample Ruby script that creates a simple text file as the backup content, but demonstrates the core operations for the script is shown below:

```ruby
#!/usr/bin/env ruby
require '/opt/continuent/tungsten/cluster-home/lib/ruby/tungsten'
require '/opt/continuent/tungsten/tungsten-replicator/lib/ruby/backup'
class MyCustomBackupScript < TungstenBackupScript
def backup
  TU.info("Take a backup with arg1 = #{@options[:arg1]} and myarg = #{@options[:myarg]}")
  storage_file = '/opt/continuent/backups/backup_' + Time.now.strftime("%Y-%m-%d_%H-%M") + rand(100).to_s
  TU.cmd_result("echo 'my backup' > #{storage_file}"")
end
```

513
F.1.4. Enabling a Custom Backup Script

To enable a custom backup script, the installation must be updated through `tpm` to use the script backup method. To update the configuration:

1. Create or copy the backup script into a suitable location, for example `/opt/continuent/share`.
2. Copy the script to each of the datasources within your dataservice.
3. Update the configuration using `tpm`. The `--repl-backup-method` should be set to `script`, and the directory location set using the `--repl-backup-script` option:

   ```bash
   shell> ./tools/tpm update --repl-backup-method=script
   --repl-backup-script=/opt/continuent/share/mcbackup.pl
   --repl-backup-online=true
   ```

   The `--repl-backup-online` option indicates whether the backup script operates in online or offline mode. If set to false, replicator must be in the offline state because the backup process is started.

   To pass additional arguments or options to the script, use the `replicator.backup.agent.script.options` property to supply a list of ampersand separate key/value pairs, for example:
These are the custom parameters which are supplied to the script as the value of the -options parameter when the script is called.

Once the backup script has been enabled within the configuration it can be used when performing a backup through the standard backup or restore interface:

For example, within cctrl:

```
[LOGICAL:EXPERT] /alpha > datasource host2 backup script
```

Note

Note that the name of the backup method is script, not the actual name of the script being used.

F.2. Character Sets in Database and Continuent Tungsten

Character sets within the databases and within the configuration for Java and the wrappers for Continuent Tungsten must match to enable the information to be extracted and viewed.

For example, if you are extracting with the UTF-8 character set, the data must be applied to the target database using the same character set. In addition, the Tungsten Replicator should be configured with a corresponding matching character set. For installations where replication is between identical database flavours (for example, MySQL or MySQL) no explicit setting should be made. For heterogeneous deployments, the character set should be set explicitly.

When installing and using Continuent Tungsten, be aware of the following aspects when using character sets:

- When installing Continuent Tungsten, use the --java-file-encoding to tpm to configure the character set.
- When using the thl command, the character set may need to be explicitly stated to view the content correctly:

```
shell> thl list -charset utf8
```

For more information on setting character sets within your database, see your documentation for the database:

- MySQL
- Oracle

For more information on the character set names and support within Java, see:

- Java 6 SE
- Java 7 SE

F.3. Understanding Replication of Date/Time Values

- Replicator processes default to UTC internally by setting the Java VM default time zone to UTC. This default can be changed by setting the replicator.time._zone property in the replicator services.properties file but is not recommended other than for problem diagnosis or specialized testing.
- Replicas store a time zone on statements and row changes extracted from MySQL.
- Replicators use UTC as the session time zone when applying to MySQL replicas.
- Replicators similarly default to UTC when applying transactions to data warehouses like Hadoop, Vertica, or Amazon Redshift.
- The thl utility prints time-related data using the default GMT time zone. This can be altered using the -timezone option.

Best Practices

We recommend the following steps to ensure successful replication of time-related data:

- Standardize all DBMS server and host time zones to UTC. This minimizes time zone inconsistencies between applications and data stores. The recommendation is particularly important when replicating between different DBMS types, such as MySQL to Hadoop.
- Use the default time zone settings for Tungsten replicator. Do not change the time zones unless specifically recommended by Continuent support.
F.4. Memory Tuning and Performance

Different areas of Continuent Tungsten use memory in different ways, according to the operation and requirements of the component. Specific information on how memory is used by different components and how it is used is available below:

- **Tungsten Replicator** — Memory performance and tuning options.
- **Tungsten Connector** — Memory usage requirements and tuning options.

F.4.1. Understanding Tungsten Replicator Memory Tuning

Replicators are implemented as Java processes, which use two types of memory: stack space, which is allocated per running thread and holds objects that are allocated within individual execution stack frames, and heap memory, which is where objects that persist across individual method calls live. Stack space is rarely a problem for Tungsten as replicators rarely run more than 200 threads and use limited recursion. The Java defaults are almost always sufficient. Heap memory on the other hand runs out if the replicator has too many transactions in memory at once. This results in the dreaded Java OutOfMemory exception, which causes the replicator to stop operating. When this happens you need to look at tuning the replicator memory size.

To understand replicator memory usage, we need to look into how replicators work internally. Replicators use a "pipeline" model of execution that streams transactions through 1 or more concurrently executing stages. As you can see from the attached diagram, a slave pipeline might have a stage to read transactions to the master and put them in the THL, a stage to read them back out of the THL into an in-memory queue, and a stage to apply those transactions to the slave. This model ensures high performance as the stages work independently. This streaming model is quite efficient and normally permits Tungsten to transfer even exceedingly large transactions, as the replicator breaks them up into smaller pieces called transaction fragments.

The pipeline model has consequences for memory management. First of all, replicators are doing many things at once, hence need enough memory to hold all current objects. Second, the replicator works fastest if the in-memory queues between stages are large enough that they do not ever become empty. This keeps delays in upstream processing from delaying things at the end of the pipeline. Also, it allows replicators to make use of block commit. Block commit is an important performance optimization in which stages try to commit many transactions at once on slaves to amortize the cost of commit. In block commit the end stage continues to commit transactions until it either runs out of work (i.e., the upstream queue becomes empty) or it hits the block commit limit. Larger upstream queues help keep the end stage from running out of work, hence increase efficiency.

Bearing this in mind, we can alter replicator behavior in a number of ways to make it use less memory or to handle larger amounts of traffic without getting a Java OutOfMemory error. You should look at each of these when tuning memory:

- **Property replicator.global.buffer.size** in the `replicator.properties` file. This controls two things, the size of in-memory queues in the replicator as well as the block commit size. If you still have problems after increasing the heap size, try reducing this value. It reduces the number of objects simultaneously stored on the Java heap. A value of 2 is a good setting to try to get around temporary problems. This can be set at installation time as the `--repl-buffer-size` parameter.

- **Property replicator.stage.q-to-dbms.blockCommitRowCount** in the replicator properties file. This parameter sets the block commit count in the final stage in a slave pipeline. If you reduce the global buffer size, it is a good idea to set this to a fixed size, such as 10, to avoid reducing the block commit effect too much. Very low block commit values in this stage can cut update rates on slaves by 50% or more in some cases. This is available at installation time as the `--repl-svc-applier-buffer-size` parameter.

- **Property replicator.extractor.dbms.transaction_frag_size** in the `replicator.properties` file. This parameter controls the size of fragments for long transactions. Tungsten automatically breaks up long transactions into fragments. This parameter controls the number of bytes of binary per transaction fragment. You can try making this value smaller to reduce overall memory usage if many transactions are simultaneously present. Normally however this value has minimal impact.

Finally, it is worth mentioning that the main cause of out-of-memory conditions in replicators is large transactions. In particular, Tungsten cannot fragment individual statements or row changes, so changes to very large column values can also result in OutOfMemory conditions. For now the best approach is to raise memory, as described above, and change your application to avoid such transactions.
F.4.2. Connector Memory Management

The memory model within the Tungsten Connector works as follows:

- Memory consumption consists of the core memory, plus the buffered memory used for each connection.
- Each connection uses the maximum size of an INSERT, UPDATE or SELECT, up to the configured size of the MySQL max_allowed_packet parameter.

For example, with 1000 concurrent connections, and a result or insert size of 1 MB, the memory usage will be 1 GB.

The default setting for the Tungsten Connector memory size is 256 MB. The memory allocation can be increased using `tpm` and the `--conn-java-mem-size` option:

For example, during installation:

```bash
shell> tpm install ... --conn-java-mem-size=1024
```

Or to update using `tpm update`:

```bash
shell> tpm update ... --conn-java-mem-size=1024
```

F.5. Tungsten Replicator Pipelines and Stages

A pipeline (or service) acts upon data.

Pipelines consist of a variable number of stages.

Every stage's workflow consists of three (3) actions, which are:

- **Extract**: the source for extraction could be the mysql server binary logs on a master, and the local THL on disk for a slave
- **Filter**: any configured filters are applied here
- **Apply**: the apply target can be THL on disk on a master, and the database server on a slave

Stages can be customized with filters, and filters are invoked on a per-stage basis.

By default, there are two pipeline services defined:

- **Master replication service**, which contains two (2) stages:
  - **binlog-to-q**: reads information from the MySQL binary log and stores the information within an in-memory queue.
  - **q-to-thl**: in-memory queue is written out to the THL file on disk.

- **Slave replication service**, which contains three (3) stages:
  - **remote-to-thl**: remote THL information is read from a master datasource and written to a local file on disk.
  - **thl-to-q**: THL information is read from the file on disk and stored in an in-memory queue.
  - **q-to-dbms**: data from the in-memory queue is written to the target database.

F.6. Continuent Tungsten Schemas
Appendix G. Frequently Asked Questions (FAQ)

The following sections provide the questions and answers to questions often asked by customers and in forums.

G.1. General Questions

G.1.1. How do I update the IP address of one or more hosts in the cluster?

To update the IP address used by one or more hosts in your cluster, you must perform the following steps:

1. If possible, switch the node into SHUNNED mode.
2. Reconfigure the IP address on the machine.
3. Update the hostname lookup, for example, by editing the IP configuration in /etc/hosts.
4. Restart the networking to reconfigure the service.
5. On the node that has changed IP address, run:

   shell> tpm update

   The above updates the configuration, but does not restart the individual services, which may still have the old, incorrect, IP address information for the host cached.
6. Restart the node services:

   shell> tpm restart

7. On each other node within the cluster:
   a. Update the hostname lookup for the new node, for example, by updating the IP configuration in /etc/hosts.
   b. Update the configuration, using tpm:

      shell> tpm update

   c. Restart the services:

      shell> tpm restart

G.1.2. How do I fix the mysql-connectorj to drizzle MySQL driver bug which prevents my application from connecting through the Connector?

When upgrading from version 2 to v4+, or simply just moving away from the mysql-connectorj driver to the Drizzle driver, the update process doesn't correctly remove all the connectorJ properties, causing a mismatch when connectors that did get the update try to make a connection to the cluster.

This is a known issue logged as CT-7

As yet, a fix has not been found, but the following workaround will correct the issue by hand:

To properly identify this issue, check the extended output of cctrl for the active driver. There will be one line of output for each node in the local cluster. Repeat once per cluster, on which node does not matter.

shell> echo ls -l | cctrl -expert| grep driver: | awk '{print $3}'

For example, for a three-node cluster, you may see something like this:

com.mysql.jdbc.Driver
com.mysql.jdbc.Driver
com.mysql.jdbc.Driver

If any line on any node in any cluster shows the com.mysql.jdbc.Driver, please use the workaround below:

**Warning**

If you have multiple clusters, either MSMM, CMM or Composite HA/DR, always ensure you check ALL clusters. Especially in Composite clusters, the Master cluster, and especially the Master node, must be checked and corrected if necessary.

Ensure the tpm update was done with the --replace-release option.
Review the `tpm reverse` output and analyze based on the following:

- `--mysql-driver=drizzle [364]` should exist in the defaults section
- You may (or may not) see the old `--mysql-connectorj-path [364]` entry within each service definition or in the defaults
- If none of the above appear in the output, then the default drizzle driver will be active by default as of v4.0.0.

Repeat the following steps for all clusters, one by one:

1. Place the cluster into Maintenance Mode using the `cctrl` command:

```
cctrl> set policy maintenance
```

2. Stop all managers on all nodes within the single cluster:

```
shell> manager stop
Stopping Tungsten Manager Service...
Waiting for Tungsten Manager Service to exit...
Stopped Tungsten Manager Service.
```

3. On all nodes within the single cluster, remove all files from the `/opt/continuent/tungsten/cluster-home/conf/cluster/{local_service-name}/datasource/` directory.

Only delete the files from the local cluster service name directory, do not touch the composite service directory if there is one.

4. Start all managers on all nodes within the single cluster, starting with the master:

```
shell> manager start
Starting Tungsten Manager Service...
Waiting for Tungsten Manager Service ...
running: PID:24819
```

5. Place the cluster back into Automatic Mode

```
shell> echo set policy automatic | cctrl -expert
Tungsten Clustering 6.0.3 build 608
alpha: session established, encryption=false, authentication=false
[LOGICAL:EXPERT] /alpha > set policy automatic
policy mode is now AUTOMATIC
[LOGICAL:EXPERT] /alpha >
Exiting...
```

Once the above has been completed, confirm that the procedure has worked as follows:

```
shell> echo ls -l | cctrl -expert| grep driver: | awk '{print $3}'
org.drizzle.jdbc.DrizzleDriver
org.drizzle.jdbc.DrizzleDriver
org.drizzle.jdbc.DrizzleDriver
```

G.1.3. How do I update the password for the replication user in the cluster?

If you need to change the password used by Continuent Tungsten to connect to a datasource and apply changes, the password can be updated first by changing the information within the your datasource, and then by updating the configuration using `tpm update`. The new password is not checked until the Tungsten Replicator process is starting. Changing the password and then updating the configuration will keep replication from failing.

1. Within `cctrl` set the maintenance policy mode:

```
cctrl> set policy maintenance
```

2. Within MySQL, update the password for the user, allowing the change to be replicated to the other datasources:

```
mysql> SET PASSWORD FOR tungsten@'%' = PASSWORD('new_pass');
```

3. Follow the directions for `tpm update` to apply the `--datasource-password=new_pass [370]` setting.

4. Set the policy mode in `cctrl` back to `AUTOMATIC`:

```
cctrl> set policy automatic
```

G.1.4. One of my hosts is regularly a number of seconds behind my other slaves?

The most likely culprit for this issue is that the time is different on the machine in question. If you have `ntp` or a similar network time tool installed on your machine, use it to update the current time across all the hosts within your deployment:
Frequently Asked Questions (FAQ)

G.1.5. Does the replicate filter (i.e. replicate.do and replicate.ignore) address both DML and DDL?

Both filters replicate.do and replicate.ignore will either do or ignore both DML and DDL.

DDL is currently ONLY replicated for MySQL to MySQL or Oracle to Oracle topologies, or within MySQL Clusters, although it would be advisable not to use ignore/do filters in a clustered environment where data/structural integrity is key.

With replicate.do, all DML and DDL will be replicated ONLY for any database or table listed as part of the do filter.

With replicate.ignore, all DML and DDL will be replicated except for any database or table listed as part of the ignore filter.

G.1.6. How do you change the replicator heap size after installation?

You can change the configuration by running the following command from the staging directory:

```bash
shell> ./tools/tpm --host=host1 --java-mem-size=2048
```

G.1.7. On a Tungsten Replicator slave, how do I set both the local slave THL listener port and the upstream master’s THL listener port?

You need to specify two options: `thl-port` to set the slave THL listener port and `master-thl-port` to define the upstream master THL listener port. Otherwise `thl-port` alone sets BOTH.

G.2. Cloud Deployment and Management

G.2.1. Do we support a 3-node cluster spread across three AWS Availability Zones?

This is a normal deployment pattern for working in AWS reduce risk. A single cluster works quite well in this topology.

G.2.2. What are the best settings for the Tungsten connector intelligent proxy?

Standard settings work out of the box. Fine tuning can be done by working with the specific customer application during a Proof-Of-Concept or Production roll-out.

G.2.3. How do we use Tungsten to scale DB nodes up/down?

Currently a manual process. New puppet modules to aid this process are being developed, and will be included in the documentation when completed. Here is a link to the relevant procedure Section 3.5.1, “Adding Datasources to an Existing Deployment”.

G.2.4. Do you handle bandwidth/traffic management to the DB servers?

This is not something currently supported.
Appendix H. Ecosystem Support

In addition to the core utilities provided by Continuent Tungsten, additional tools and scripts are available that augment the core code with additional functionality, such as integrating with third-party monitoring systems, or providing additional functionality that is designed to be used and adapted for specific needs and requirements.

Different documentation and information exists for the following tools:

- Github — a selection of tools and utilities are provided in Github to further support and expand the functionality of Continuent Tungsten during deployment, monitoring, and management.
- logrotate — provides configuration information for users making use of the logrotate to manage Continuent Tungsten logs.
- Cacti — templates and scripts to enable monitoring through the Cacti environment.
- Nagios — templates and scripts to enable monitoring through the Nagios environment.
Appendix I. Configuration Property Reference