
MySQL Shell 9.0 Release Notes

Abstract

This document contains release notes for the changes in MySQL Shell 9.0.

For additional MySQL Shell documentation, see <http://dev.mysql.com/>.

Updates to these notes occur as new product features are added, so that everybody can follow the development process. If a recent version is listed here that you cannot find on the download page (<https://dev.mysql.com/downloads/>), the version has not yet been released.

The documentation included in source and binary distributions may not be fully up to date with respect to release note entries because integration of the documentation occurs at release build time. For the most up-to-date release notes, please refer to the online documentation instead.

For legal information, see the [Legal Notices](#).

For help with using MySQL, please visit the [MySQL Forums](#), where you can discuss your issues with other MySQL users.

Document generated on: 2024-07-03 (revision: 28666)

Table of Contents

Preface and Legal Notices	1
Changes in MySQL Shell 9.0.0 (2024-07-01, Innovation Release)	3

Preface and Legal Notices

This document contains release notes for the changes in MySQL Shell 9.0.

Legal Notices

Copyright © 1997, 2024, Oracle and/or its affiliates.

License Restrictions

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications

of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Trademark Notice

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

Third-Party Content, Products, and Services Disclaimer

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Use of This Documentation

This documentation is NOT distributed under a GPL license. Use of this documentation is subject to the following terms:

You may create a printed copy of this documentation solely for your own personal use. Conversion to other formats is allowed as long as the actual content is not altered or edited in any way. You shall not publish or distribute this documentation in any form or on any media, except if you distribute the documentation in a manner similar to how Oracle disseminates it (that is, electronically for download on a Web site with the software) or on a CD-ROM or similar medium, provided however that the documentation is disseminated together with the software on the same medium. Any other use, such as any dissemination of printed copies or use of this documentation, in whole or in part, in another publication, requires the prior written consent from an authorized representative of Oracle. Oracle and/or its affiliates reserve any and all rights to this documentation not expressly granted above.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Changes in MySQL Shell 9.0.0 (2024-07-01, Innovation Release)

- [AdminAPI Added or Changed Functionality](#)
- [AdminAPI Bugs Fixed](#)
- [Utilities Added or Changed Functionality](#)
- [Utilities Bugs Fixed](#)
- [Functionality Added or Changed](#)
- [Bugs Fixed](#)

AdminAPI Added or Changed Functionality

- InnoDB ReplicaSet locking has been updated and simplified; no longer requiring multiple per-instance locks.

See [InnoDB ReplicaSet Locking](#). (Bug #35913824)

- It is now possible to dissolve a ClusterSet, partially or completely, using the following methods:
 - `clusterSet.dissolve()`: dissolves the ClusterSet completely by stopping replication between each replica and primary Cluster and removing any metadata related to the ClusterSet. Each cluster of the ClusterSet is also dissolved.
 - The `dissolve` option of `clusterSet.removeCluster()`: removes the specified Cluster from the ClusterSet, enabling it to function as a standalone Cluster.

See [Dissolving a ClusterSet](#). (Bug #108373, Bug #34564242, WL #15378)

- It is now possible to execute SQL on all reachable members of a Cluster, ClusterSet, or ReplicaSet, using `.execute()`.

See [Executing SQL on Topologies](#). (WL #15820)

AdminAPI Bugs Fixed

- MySQL Shell closed unexpectedly when calling certain AdminAPI functions on EL7 platforms. (Bug #36651010)
- `dba.reboot_cluster_from_complete_outage()` disabled `super_read_only` on the primary member of an INVALIDATED Cluster. As a result, clients continued to perform updates and introduce errant transactions.

As of this release, `dba.reboot_cluster_from_complete_outage()` enables `super_read_only` on the primary member and disables the Group Replication action `mysql_disable_super_read_only_if_primary`. (Bug #36562916)

- If an attempt to create a Replica Cluster failed due to a timeout and the revert also failed due to a timeout, the Replica Cluster could be left in an inconsistent state; ONLINE, but not associated with

the ClusterSet's metadata. This specific issue was caused by low values for `wait_timeout` and `interactive_timeout`.

The following changes were made:

- `wait_timeout` is checked and, if set to a value lower than the default of 8 hours, is set to 8 hours.
- `Cluster.rescan()` is extended with a new option, `repairMetadata` which can be enabled to resolve inconsistencies in the Cluster's metadata.
- `Cluster.dissolve()` can now be used on Clusters in this inconsistent state.

(Bug #36495756)

- The documentation for [Rescanning a Cluster](#) did not make clear that while `group_replication_transaction_size_limit` is set to the maximum value in Replica Clusters, the original value is stored in the metadata schema and is restored by `Cluster.rescan()` in the event of a switchover or failover. This overwrites any user-defined value set on the Replica Cluster.

The documentation is updated with this information. (Bug #36494958)

- Recent enhancements enabled MySQL Router to expose its configuration and defaults in the metadata schema. However, the `remove_router_metadata` function was not updated to properly clean this data.

Also, the `router_options()` function filtered the common options from the default options list. (Bug #36276246)

- `reboot_cluster_from_complete_outage()` failed for a Replica Cluster if Group Replication was stopped and the replication channel reset. This failure was caused by the absence of the recovery user.

As of this release, `reboot_cluster_from_complete_outage()` always recreates the recovery user. (Bug #35181181)

Utilities Added or Changed Functionality

- The following check was added to the Upgrade Checker utility:
 - `foreignKeyReferences`: Checks for foreign keys referencing non-unique and partial indexes.

(Bug #36553868)

- The following Upgrade Checker utility sysvar checks have been combined into a single check, `sysvars`:

- `sysVarsNewDefaults`
- `sysvarAllowedValues`
- `removedSysVars`

See [Utility Checks](#). (WL #16262)

- The following utilities now support Instance and Resource Principal authentication on Oracle Cloud Infrastructure:

- `util.dumpInstance()`
- `util.dumpSchemas()`

- `util.dumpTables()`
- `util.loadDump()`
- `util.exportTable()`
- `util.importTable()`

Each utility is extended with a new option, `ociAuth`, which enables you to specify one of the following Oracle Cloud Infrastructure authentication types:

- `api_key`
- `instance_principal`
- `resource_principal`
- `security_token`

See [MySQL Shell Utilities](#). (WL #15884)

Utilities Bugs Fixed

- The formatting of the report returned by the Upgrade Checker utility's `invalidPrivilege` check is improved in this release. Instead of returning a message for each user, the users are grouped with the message. (Bug #36613895)
- As of this release, all failed connections to the supported object storage platforms are retried three times, with a 1 second delay between retries.

If a failure occurs 10 minutes after the connection was created, the delay is changed to an exponential back-off strategy:

- First delay: 3-6 seconds
- Second delay: 18-36 seconds
- Third delay: 40-80 seconds

(Bug #36597063, Bug #36256053)

References: See also: Bug #35396788.

- `restrict_fk_on_non_standard_key`, introduced in MySQL 8.4.0, prohibits creation of foreign keys which reference only part of a composite key when enabled. This system variable is enabled by default on MySQL HeatWave Service and resulted in errors loading dumps which contained such keys when detected by the Upgrade Checker utility's `foreignKeyReferences` check.

As of this release, a new compatibility option is added the dump utilities, `force_non_standard_keys`. This disables checks for non-standard foreign keys, and cause the loader to set the session value of `restrict_fk_on_non_standard_key` to OFF. (Bug #36553849)

- Primary keys defined on an `ENUM` column were reported as missing for dumps with `ocimds:true`. This was caused by a fix in an earlier version which instructed the dump utility to ignore primary keys or unique indexes which contain one or more `ENUM` columns when selecting an index for chunking.

As of this release, information about the index selected for chunking and whether the table has a primary key is separated. (Bug #36493316)

References: See also: Bug #35180061.

- As of this release, the Schema Dump utility uses the `JSON` output format for its generated `EXPLAIN` plans. This was done for compatibility reasons. (Bug #36470302)
- It was not possible to run the Upgrade Checker utility against an MySQL HeatWave Service DB System. An error was returned relating to missing `RELOAD` privileges. `RELOAD` is not granted to MySQL HeatWave Service users.

`RELOAD` is not required by the Upgrade Checker when run against MySQL HeatWave Service DB Systems, it is only required against MySQL 5.7.x. As such, the requirement is removed in this release. (Bug #36361159)

- The Upgrade Checker utility did not validate the value of the `configPath` parameter.

As of this release, the value of `configPath` is validated before running the upgrade checks. (Bug #36332625)

- The Upgrade Checker utility behaved inconsistently in the absence of certain privileges. Sometimes returning an error and sometimes attempting to run its checks. (Bug #36332031)
- The Upgrade Checker utility's `sysvarAllowedValues` did not take into account empty strings as valid values for certain variables, such as `ssl_cipher`, resulting in false negative errors in the report. (Bug #36298612)
- It was not possible to use the Copy utilities with certain MySQL-compatible databases. SQL syntax errors were returned. (Bug #36297963)
- `util.collect_diagnostics()` failed with an `AttributeError` when run against an InnoDB Cluster on which the Group Replication plugin was uninstalled from one or more members. The utility attempted to retrieve values for Group Replication system variables which did not exist because the plugin was uninstalled.

Thanks to Ioannis Androulidakis for the contribution. (Bug #114707, Bug #36589677)

- Fixed an issue with non-ASCII character handling in the Upgrade Checker utility's `schemaInconsistency` check.

Thanks to Daniel Lenski for the contribution. (Bug #114127, Bug #36340714)

Functionality Added or Changed

- The `mysql_native_password` client plugin is now bundled with MySQL Shell. (Bug #36610756)
- MySQL Shell supports the `VECTOR` type introduced in MySQL 9.0.
(Bug #36252107, Bug #36253120)
- In previous versions, if neither port nor protocol were specified in the connection string, MySQL Shell automatically used the X Protocol. As of this release:
 - If neither port nor protocol are specified, the default is Classic Protocol.
 - If port is specified but protocol is not, the default is Classic Protocol.

In either case, if Classic Protocol fails, X Protocol is attempted instead. (WL #16317)

- The `shell` global object is extended with `register_Sql_Handler`, a function which enables you to register a custom SQL handler. This handler can execute pre-processing steps for the given SQL statements and extend the supported SQL statements with non-standard SQL. (WL #15949)

Bugs Fixed

- MySQL Shell closed unexpectedly if a native Python object was passed to a Python plugin function. (Bug #36502096)

- MySQL Shell did not prompt for a password if `-p` was specified on the command line without an argument. (Bug #36433418)
- Under certain circumstances, a password prompt was not returned although no password was provided on the command line or defined in a configuration file. (Bug #36422502, Bug #36422492)
- `--no-password` did not work if a password was defined in the server's configuration file or if it was provided earlier in the command line. (Bug #36422408)
- Auto-complete was not available in the `\sql` command. (Bug #36420389)
- If `logSql` was set to `ERROR`, MySQL Shell logged the SQL without filtering for unsafe statements. As of this release, the pattern defined in `logSql.ignorePatternUnsafe` is used to filter unsafe SQL from the log.

Also, the pattern which triggered the filter is logged. (Bug #36014067)

- Special characters, such as tab or newline, were not supported in utility calls from the command line. For example, in the following command, `\t` was not properly handled:

```
> mysqlsh root@localhost -- util import-table sample_us.tsv --schema=test --table=samples --fieldsTe
```

(Bug #34887426)

- Upgrading MySQL Shell 8.0.35, or higher, on Windows platforms, resulted in multiple installations instead of overwriting the existing installation. (Bug #113732, Bug #36259270)

