



MySQL Enterprise Edition

Product Guide

A MySQL® White Paper



Table of Contents

Introduction	3
MySQL Enterprise Edition	3
Data Protection and Regulatory Compliance.....	4
MySQL Enterprise Authentication	6
MySQL Enterprise Transparent Data Encryption (TDE)	7
MySQL Enterprise Encryption	8
MySQL Enterprise Masking and De-identification	8
MySQL Enterprise Firewall.....	10
MySQL Enterprise Audit.....	11
MySQL Security Technical Implementation Guide (STIG).....	12
CIS Benchmark for MySQL Enterprise Edition.....	13
MySQL Enterprise Scalability	14
MySQL Enterprise High Availability.....	17
MySQL Enterprise Backup.....	18
MySQL Operator for Kubernetes.....	19
MySQL Enterprise Stored Programs	20
MySQL Enterprise Telemetry	21
Oracle Enterprise Manager for MySQL.....	23
Oracle Product Certifications/Integrations.....	24
Oracle Premier Support	25
HeatWave.....	25
Conclusion	26
Additional Resources	27

Introduction

Whether you are building high volume websites, enterprise and departmental applications, or e-commerce applications, your organization needs the tools to build and manage these business-critical database applications. This paper explores how you can confidently deploy MySQL as part of a cost-effective solution for delivering high-performing, highly available, reliable and scalable applications. It examines some of the challenges associated with delivering secure applications that protect sensitive data and meet regulatory requirements and how MySQL Enterprise Edition can address these challenges.

MySQL Enterprise Edition, combines the most secure, scalable, “always on” version of the MySQL database with online backup, monitoring, management and SQL development tools, all backed by Oracle Premier Support, 24x7 global enterprise-class support services. Further, MySQL Enterprise Edition supports your use of MySQL in conjunction with many of the Oracle products and tools you may already be familiar with or are currently using. MySQL Enterprise Edition is specifically designed to help you bring MySQL applications to market faster, mitigate risk, and ensure you meet customer and end-user Service Level Agreements (SLAs).

MySQL Enterprise Edition

MySQL is the world's most popular open source database. Whether you are a fast growing web property, software vendor, a large organization or an SMB, MySQL can cost-effectively help you deliver high performance, scalable database applications. If you are currently using MySQL, you probably started with MySQL Community Edition. In fact, in many instances MySQL enters an organization via an application development project and makes its way into the data center when the application is deployed for production use. Challenges arise when these applications become vital to business revenues or key business functions. The most common challenges around running MySQL and other open source technologies are revealed by a simple line of questioning:

How will you know:

- If you are using the most reliable, secure, scalable, up-to-date version?
- If a server or application is down?
- If MySQL is configured to scale-out as your customer base grows?
- If there is a replication master/slave synchronization or latency issue?
- If something else is affecting the performance of a server?

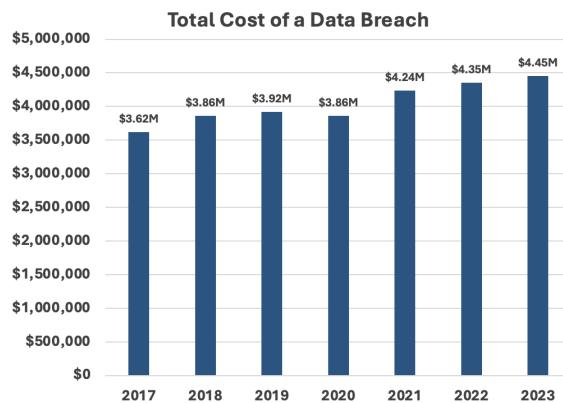
How will you implement MySQL recommended best practices to:

- Configure MySQL variables to ensure your applications run at their peak performance?
- Monitor your MySQL environment to ensure you can meet your SLA commitments?
- Integrate MySQL with your existing security standards and infrastructure?
- Protect your data from malicious individuals and organizations?
- Comply with industry and government security regulations?
- Setup your high availability and disaster recovery environment?

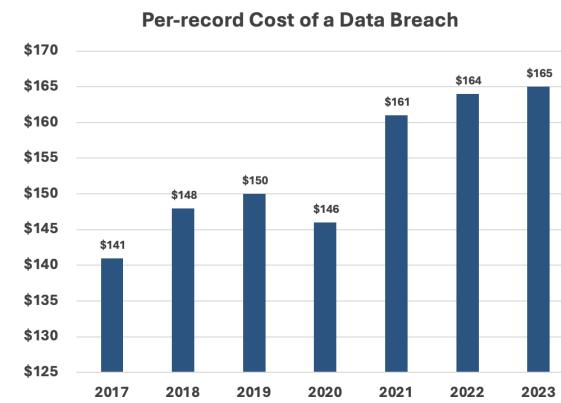
To help you answer these questions with confidence, Oracle provides MySQL Enterprise Edition. MySQL Enterprise Edition is a commercial offering comprised of the MySQL database with security, encryption, auditing, high availability and scalability, online backup, monitoring, and management. MySQL Enterprise Edition is backed by Oracle Premier 24x7 support for organizations delivering highly available, business critical applications and services.

Data Protection and Regulatory Compliance

Data protection and regulatory compliance are key requirements to prevent lost revenue, damaged reputation, and regulatory fines. According to the [2023 IBM, Cost of a Data Breach Report](#), the cost of a data breach and the per-record cost of a data breach reached new highs. These rising costs consist of business disruption, detection and escalation efforts, post-breach response costs, and notification costs.



The cost of a data breach climbed to a new high



Per-record cost of a data breach reached a new high

These data breach figures highlight just how vulnerable personal data is and how important it is to be handled and used responsibly. In response, governments and

industries around the globe have put numerous regulations in place to protect the privacy and security of Personally Identifiable Information (PII). Well known examples of regulatory laws are HIPAA, GDPR, and PCI-DSS. However, many additional regulations have been enacted such as CCPA, DMA, and more, making it difficult for organizations to meet hundreds of individual compliance requirements.

Data Protection Laws & Regulations

Hundreds of Industry and Government Regulations Around the World



Even though there are so many individual regulations, most of them share similar requirements. For example:

- **Assessing potential security risks** such as weak configurations and overprivileged accounts.
- **Monitoring and blocking** unauthorized database activity.
- **Encrypting data in motion and at rest** so that data is unreadable.
- **De-identify personal information** before it can be shared.
- **Recovering stolen data** from a breach.
- **Identifying and notifying** regulators in case of a breach.

The following sections provide detailed information about the MySQL Enterprise Edition tools and technologies that enable organizations to meet these regulatory requirements and protect sensitive data.



MySQL Enterprise Authentication

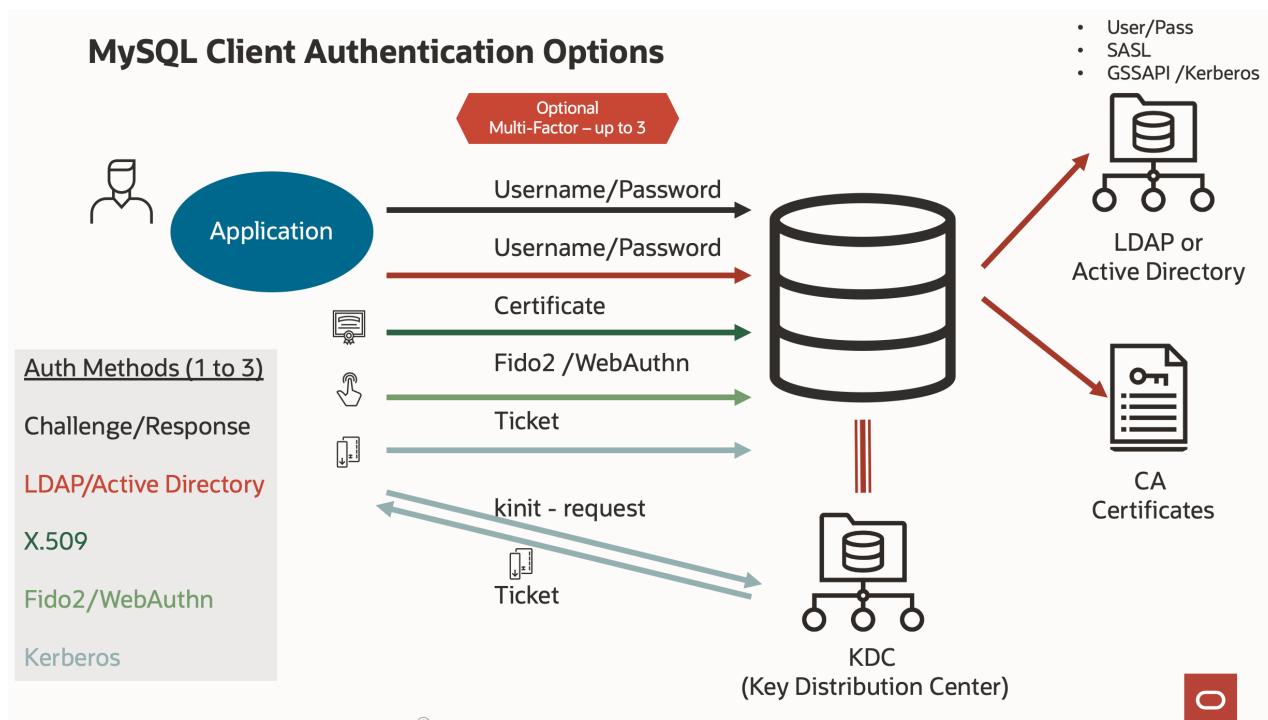
MySQL Enterprise Edition provides ready to use external authentication modules to easily integrate existing security infrastructures, including Linux Pluggable Authentication Modules (PAM) and Windows Active Directory. By authenticating MySQL users from centralized directories, organizations can implement Single Sign On. The same usernames, passwords and permissions can be used. This makes MySQL DBAs more productive by eliminating the need to manage credentials in individual systems. It also makes IT infrastructures more secure by leveraging existing security rules and processes (e.g. identifying weak passwords and managing password expiration).

MySQL External Authentication

MySQL Enterprise Edition provides ready to use, external authentication modules for users who authenticate users via centralized authentication infrastructure products. Each is described below:

- **MySQL LDAP Authentication** - Enables you to configure MySQL to query LDAP and Active Directory users and groups for Authentication of client connections. Supports various LDAP authentication protocols including User/Password, GSSAPI Kerberos, and SASL. Bind MySQL users to DNs to manage groups of users and their MySQL permissions.
- **MySQL Native Kerberos Authentication** - Enables customers to leverage existing Kerberos authentication infrastructure such as single sign on. MySQL Enterprise both MIT (GSSAPI) and Microsoft (SSPI) Kerberos implementations.
- **MySQL External Authentication for PAM** - Enables you to configure MySQL to use Linux PAMs (Pluggable Authentication Modules) to authenticate users via PAMs for various authentication methods, such as Linux passwords or an LDAP directory.
- **MySQL External Authentication for Windows** - Enables you to configure MySQL to use native Windows services to authenticate client connections. Users who have logged in to Windows can connect from MySQL client programs to the server based on the token information in their environment without specifying an additional password.
- **MySQL Multifactor Authentication (MFA)** - Enables you to require a user to provide two or more verification factors to access the MySQL Database. Username and passwords are vulnerable to various attacks. By requiring multiple factors adds

additional security hardening to keep your organization safer from cybercrime. MySQL MFA allows you to combine up to 3 authentication methods.

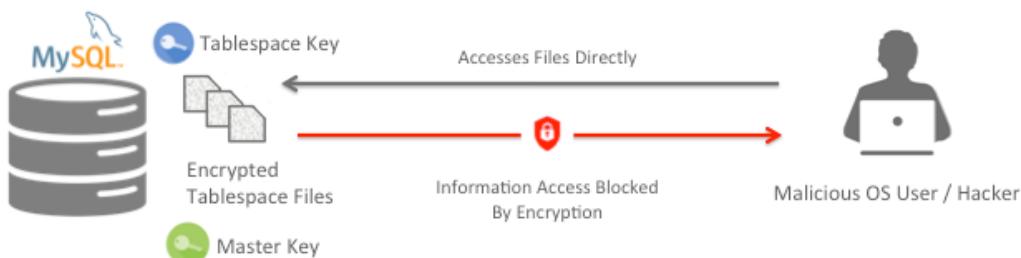


MySQL Enterprise Authentication provides multiple methods to authenticate users.

To learn more about MySQL Enterprise Authentication visit:
<http://www.mysql.com/products/enterprise/security.html>

MySQL Enterprise Transparent Data Encryption (TDE)

MySQL Enterprise Transparent Data Encryption (TDE) protects your critical data by enabling data-at-rest encryption in the database. It protects the privacy of your information, prevents data breaches and helps meet regulatory requirements including the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and numerous others.





MySQL Enterprise TDE enables data-at-rest encryption by encrypting the physical files of the database. Data is encrypted automatically, in real time, prior to writing to storage and decrypted when read from storage. As a result, hackers and malicious users are unable to read sensitive data from tablespace files, database backups or disks.

MySQL Enterprise TDE uses a two-tier encryption key architecture, consisting of a master encryption key and tablespace keys which provides easy key management and rotation. Tablespace keys are managed automatically behind the scenes while the master encryption key is stored in a centralized key management solution such as Oracle Key Vault, which enforces clear separation of keys from encrypted data.

MySQL Enterprise Encryption

To protect sensitive data throughout its lifecycle, MySQL Enterprise Encryption provides industry standard functionality for asymmetric encryption (Public Key Cryptography). MySQL Enterprise Encryption provides encryption, key generation, digital signatures and other cryptographic features to help organizations protect confidential data and comply with regulatory requirements including HIPAA, Sarbanes-Oxley, and the PCI Data Security Standard.

MySQL Enterprise Encryption gives DBAs and Developers the tools they need for:

- Asymmetric Public Key Encryption (RSA)
- Asymmetric Private Key Decryption (RSA)
- Generate Public/Private Key (RSA, DSA, DH)
- Derive Symmetric Keys from Public and Private Key pairs (DH)
- Digitally Sign Data (RSA, DSA)
- Verify Data Signature (RSA, DSA)
- Validation Data Authenticity (RSA, DSA)

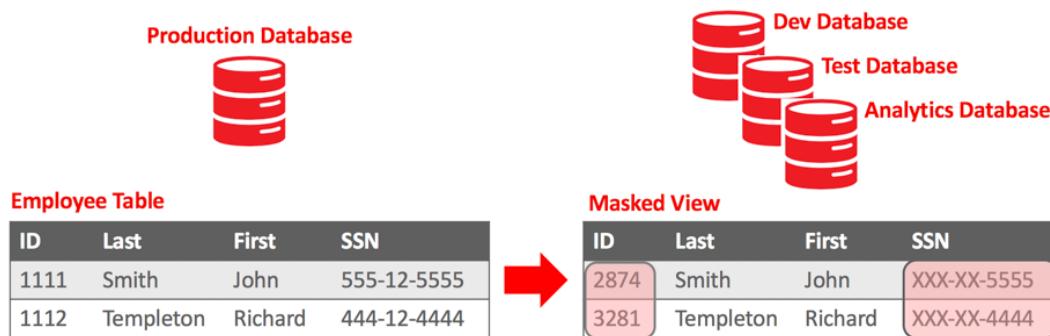
This enables software developers to encrypt data by using RDS, DHS and DH encryption algorithms without changing existing applications.

MySQL Enterprise Masking and De-identification

MySQL Enterprise Masking and De-identification provides an easy to use, built-in database solution to help organizations protect sensitive data from unauthorized uses by hiding and replacing real values with substitutes.

MySQL Enterprise Masking and De-identification enables organization to:

- **Meet regulatory requirements and data privacy laws** such GDPR, PCI DSS and HIPPA that require data de-identification.
- **Significantly reduce the risk of a data breach** by preventing unauthorized access to confidential data.
- **Protect confidential information** while improving development, test and analytics environments.



MySQL Enterprise Masking and De-identification protects sensitive data from unauthorized users.

Meet Industry Regulation Requirements and Data Privacy Mandates

All major industry regulations require data masking of PII (personally identifiable information), PANs (Primary Account Number) and other confidential data so that only authorized personnel can access the data. MySQL Enterprise Masking and De-identification provides specific functions to mask and de-identify confidential data so your IT organization can comply with privacy regulations, including:

- **GDPR:** General Data Protection Directive
- **PCI DSS:** Payment Card Industry Data Security Standard
- **HIPAA:** Health Insurance Portability and Accountability Act
- **HITECH:** Health Information Technology for Economic and Clinical Health Act
- **Data Protection Act:** United Kingdom
- **SOX:** Sarbanes Oxley
- **FERPA:** Family Educational Rights and Privacy Act
- And many more

Improve the Security of Dev, Test and Analytics Environments

Organizations can reduce the risk of a data breach by masking sensitive or confidential application data so it can be used in non-production systems. Real values are replaced with realistic but fictitious values, allowing production data to be safely used for development, testing, analytics or sharing with 3rd party partners for non-production purposes.

Built-in & Easy to Use

MySQL Enterprise Data Masking is implemented in the MySQL Server itself, so the masking logic is centralized. It's simple to implement masking functions on sensitive fields, which can be done on an existing database without affecting database operations, requiring changes in application code or changes to the production data itself. MySQL Enterprise Data Masking operates in memory with minimal performance impact.

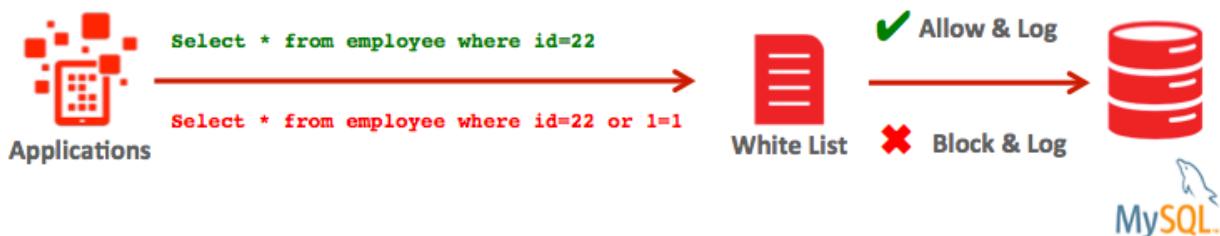
Robust Data Masking Functions

MySQL Enterprise Masking and De-identification can hide or obfuscate sensitive data, by controlling how the data appears. It features robust masking algorithms including selective masking, blurring, random data substitution and other special techniques for credit card numbers, account numbers and other personally identifiable information, enabling IT departments to maintain structural rules to de-identify values. MySQL Enterprise Masking and De-identification functions include:

- **Selective Masking** - Obscures a particular portion of numbers or strings such as phone numbers, and payment card numbers.
- **Strict or Relaxed Masking** – Implement strict or relaxed masking to obfuscate data
- **Random Data Substitution** – Replace real values with random values while maintaining format consistency.
- **Blurring** – Add a random variance to existing values such as randomized numeric ranges for salaries.
- **Dictionary substitution** – Randomly replace values from task specific dictionaries.
- **Blacklisting and substitution** – Replace specifically blacklisted data, but leave non-blacklisted in place.

MySQL Enterprise Firewall

MySQL Enterprise Firewall guards against cyber security threats by providing real-time protection against database specific attacks, such as an SQL Injection. MySQL Enterprise Firewall monitors for database threats, automatically creates a whitelist of approved SQL statements and blocks unauthorized database activity.



- **Real-time Threat Monitoring** - All incoming queries pass through a SQL analysis engine and are matched against an approved allowlist of expected SQL statements.
- **Block Suspicious Traffic** - Statements that do not match the approved allowlist are blocked, logged and can be analyzed to help block a potential SQL injection attack.
- **Learn and Build Allowlists** - Automatically create user specific allowlists of pre-approved SQL statements using a self-learning system.
- **Transparent Protection** - MySQL Enterprise Firewall requires no changes to your application regardless of development language, framework or 3rd party application.
- **High Performance** - MySQL Enterprise Firewall runs within each MySQL instance and provides scale-out performance.
- **Logging** - MySQL Enterprise Firewall tracks and provides metrics on both allowed and blocked SQL statements. Blocked statements are logged for inspection and alerting.

MySQL Enterprise Audit

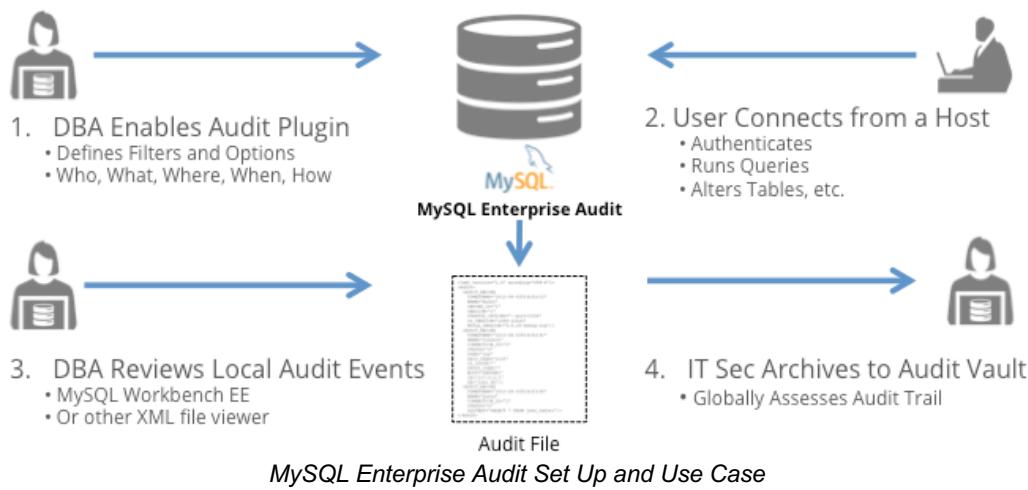
Today's web-based applications have evolved from nice-to-have enablers to the mission-critical revenue generating mechanisms that characterize the modern e-business model. In this virtual marketplace, PCI compliance guidelines ensure credit card data is secure within e-commerce apps. From a corporate standpoint, Sarbanes-Oxley, HIPAA and other government imposed mandates guard the medical, financial, public sector and other personal data centric industries with required logging, archiving and "upon request" access to audit trails that reveal the eyes and hands that have viewed and acted upon the most sensitive of data. In all use cases, requirements for capturing application level user activity are most commonly implemented on the back-end database.

With this in mind, MySQL provides an open pluggable audit interface that enables all MySQL users to write their own auditing solutions based on application specific requirements. To help users quickly and seamlessly add auditing compliance to their existing applications, MySQL Enterprise Edition includes MySQL Enterprise Audit, an easy to use policy-based auditing solution that enables users to:

- **Protect Sensitive Data using Powerful Filtering** - Define what you audit using templates or design highly custom filters using simple JSON filter definition. Filter on connections, users, table access, access type, statement status (success/failure), query content, and more.
- **Meet Regulatory Compliance Standards** - Provide the data your organization and auditors need to be in compliance with requirements including PCI, HIPAA, FERPA, SOX and more.

- **Achieve Security Goals through Comprehensive Auditing** - Trust but verify DBA activity, prove your data's validity and perform forensic analysis to investigate or discover data breaches.
- **Easy Integration with Audit Vaults and Stores** - Externally archive and analyze XML-based audit logs with ease using Oracle Audit Vault and other third party solutions including Splunk.
- **Dynamic and Easy to Manage** - Dynamically enable/disable audit stream, change filtering, and more with no downtime. Automatically rotate audit log files based on size.
- **Low Overhead** - Collects critical audit data with minimal performance impact. Use fine grain filtering to minimize audit log size and IO impact.

A common set up and use case scenario is depicted here:



To learn more about MySQL Enterprise Audit visit:

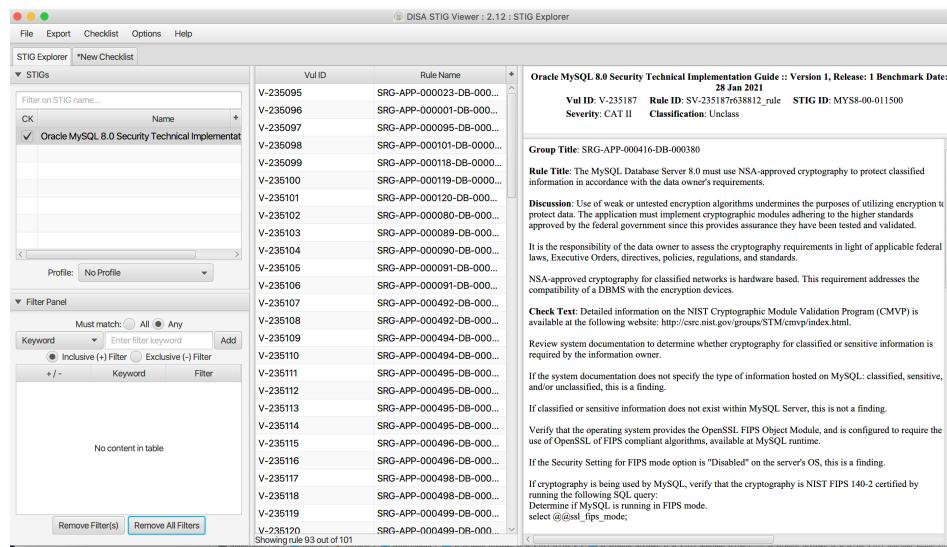
<http://www.mysql.com/products/enterprise/audit.html>

MySQL Security Technical Implementation Guide (STIG)

The United States Department of Defense (DoD) approves and publishes the Security Technical Implementation Guide (STIG) for MySQL Enterprise Edition 8.0. The Defense Information Systems Agency (DISA) evaluated MySQL Enterprise Edition against stringent DoD's security requirements. The resulting guide for MySQL Enterprise Edition provides comprehensive steps towards meeting security requirements for government systems.

DISA STIGs include a description of requirements explaining:

- What are the related security risks and vulnerabilities?
- Is a vulnerability applicable to a product?
- Whether the product has inherent protection or if you need to check the product settings.
- Which settings to inspect and how - pass (protected) or fail via a series of checks.
- Changes needed when a check fails.
- Other mitigating actions to put in place to minimize security risk.
- Use of additional products to provide added protection.



The screenshot shows the MySQL Security Technical Implementation Guide (STIG) interface. The left pane displays a list of requirements under the heading 'Oracle MySQL 8.0 Security Technical Implementation Guide :: Version 1, Release: 1 Benchmark Date: 28 Jan 2021'. The right pane provides detailed information for each requirement, including the Rule ID, Rule Name, and a description of the rule's purpose and implementation details. The interface includes a search bar, filter panel, and a table of contents.

MySQL Security Technical Implementation Guide (STIG)

Download the DISA STIG for MySQL Enterprise Edition:

<https://public.cyber.mil/announcement/stig-update-disa-has-released-the-oracle-mysql-8-0-stig/>

CIS Benchmark for MySQL Enterprise Edition

The Center for Internet Security (CIS) is a global community of cybersecurity experts. CIS develops CIS Benchmarks, secure configuration and implementation guidelines used to safeguard against cyber threats. The CIS MySQL Benchmark provides prescriptive guidance for establishing a secure configuration posture for MySQL Enterprise Edition.

CIS benchmarks go through continuous consensus reviews by security professionals and in this case MySQL experts. Reviewers come from consulting, software development, audit and compliance, security research, operations, government, and

legal, providing a diversity of perspectives on cybersecurity. Although the CIS Benchmarks focuses on Linux based platforms, many of the concepts and practices transfer to other platforms supported by MySQL. Bring your systems into compliance using a secure baseline by implementing and auditing against CIS Benchmarks.

The CIS Benchmark recommendations are recognized as a secure configuration standard for many government and industry regulations, including:

- DoD Cloud Computing Security Recommendation Guide (SRG)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST)

Download the CIS Benchmark for MySQL Enterprise Edition:

https://www.cisecurity.org/benchmark/oracle_mysql

MySQL Enterprise Scalability

By default, the MySQL Database provides a complex thread-handling model that provides excellent throughput and performance for online and web-based applications. User connections are mapped to execution threads on a one-to-one basis with each connection/thread assignment remaining intact until the connection is terminated by the client. Under this model the MySQL Database provides scalable concurrency of both user connections and query executions.

While this model serves and scales most web deployment use cases very well it does have the potential to limit scalability as connection and query loads increase at an increasing rate. This use case is becoming more common as application clients now extend far beyond the keyboard to mobile and other web-enabled devices. For the most highly trafficked applications when concurrent connections grow from hundreds to thousands and associated query executions grow proportionally scalability challenges and limitations with the default model are potentially exposed:

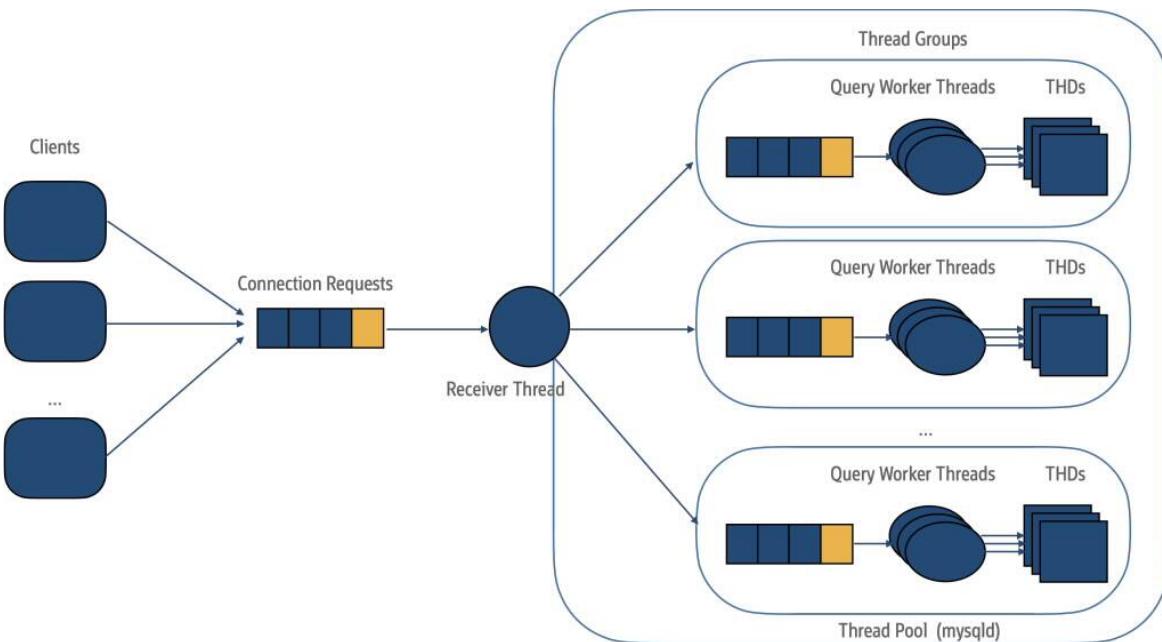
- Current model does not prioritize connection queries for execution, regardless of the number that have been submitted or that are in a “wait” status. No prioritization of queries means that all attempt to execute in parallel with no regard for server resource limitations.

- More concurrency of query executions requires significantly more server memory. In an extreme case if the amount of memory needed by all active connections exceeds server memory, the MySQL server may revert to memory/disk swapping, which will greatly impact user response times.
- More query executions also leads to more cache flushing, which leads to more cache misses and disk I/O requests. More disk I/O leads to longer query execution and user response times.
- Write intensive applications are impacted significantly as concurrent DML statement execution times can degrade exponentially as disk I/O increases.

MySQL Thread Pool

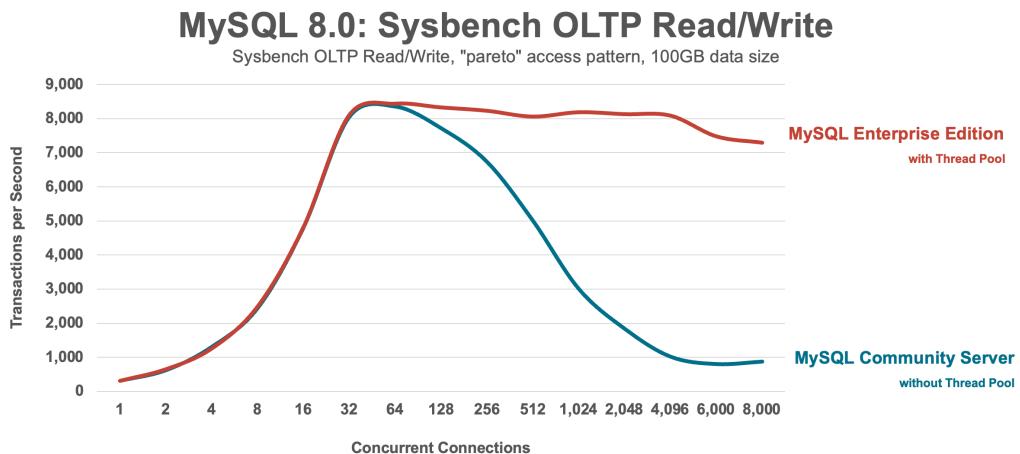
To meet these challenges around the most demanding “mobilized” application user and workloads MySQL Enterprise Edition provides the MySQL Thread Pool. The Thread Pool is a user configurable option that provides an efficient, alternate thread-handling model designed to sustain performance and scalability as concurrent user loads continue to grow. In these use cases the Thread Pool addresses the limitations to scalability by:

- Managing/controlling query execution until the MySQL server has the resources to execute it.
- Splitting threads into managed Thread Groups. Inbound connections are assigned to a group via a round-robin algorithm and the number of concurrent connections/threads per group is limited based on queue prioritization and nature of queries awaiting execution. Transactional queries are given a higher priority in queue than non-transactional, but queue prioritization can be overridden at the user level as needed.
- Avoiding deadlocks when queries are stalled or executing for long period of time.



MySQL Thread Pool Architecture

The result is sustained performance and scalability as concurrent user connections and work loads grow as shown here in a benchmark.

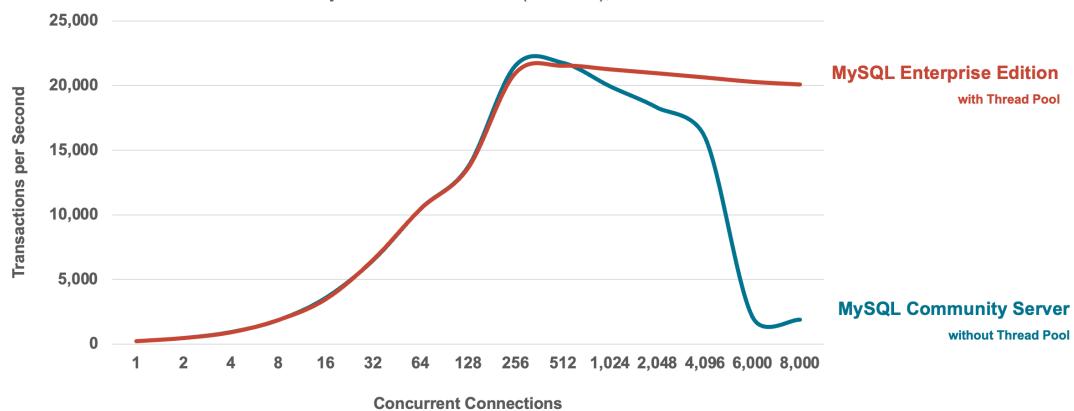


9x Better Scalability

MySQL Enterprise Edition provides 9x better scalability for OLTP Read/Write activity with Thread Pool

MySQL 8.0: Sysbench TPCC

Sysbench TPCC 1000W (1K DWH), 100GB data size



10x Better Scalability

MySQL Enterprise Edition provides 10x better scalability for OLTP Read/Write activity with Thread Pool

SysBench OLTP benchmarks show that the MySQL Thread Pool provides a significant improvement in sustained performance and scalability for applications that service a growing number of concurrent user connections and query executions.

To learn more about MySQL Enterprise Scalability visit:
<http://www.mysql.com/products/enterprise/scalability.html>.

MySQL Enterprise High Availability

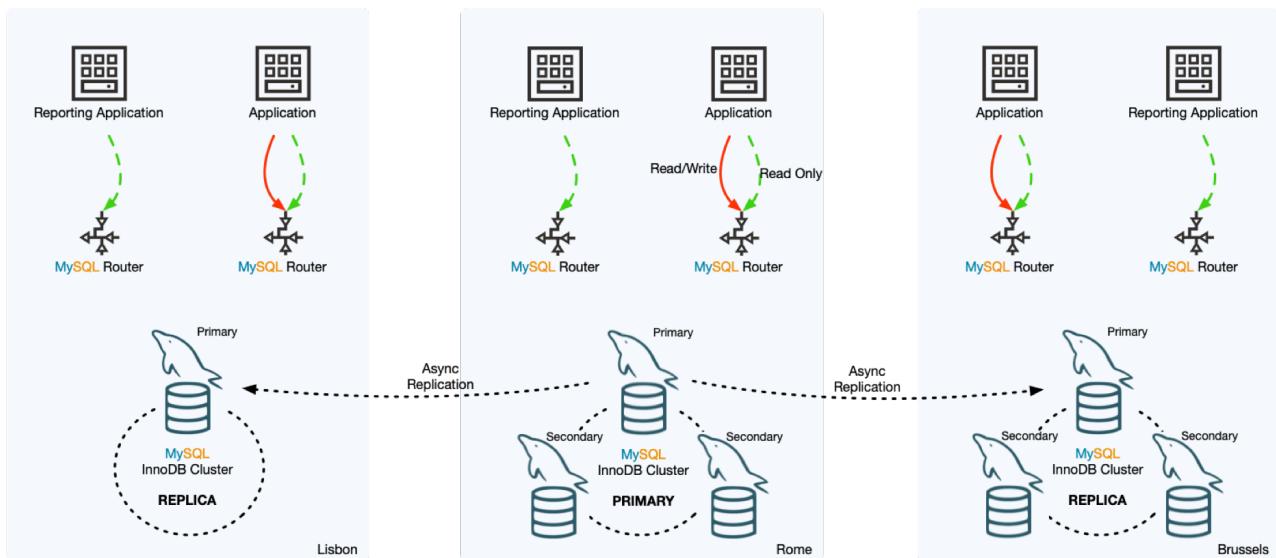
High Availability with MySQL InnoDB Cluster

MySQL InnoDB Cluster delivers a complete high availability solution for MySQL. Each server in an InnoDB Cluster replicates data to all members of the cluster while providing fault tolerance, automated failover, and elasticity. MySQL InnoDB Cluster provides built-in group membership management, data consistency guarantees, node failure detection and database failover, without the need for manual intervention.

Disaster Recovery with MySQL InnoDB ClusterSet

MySQL InnoDB ClusterSet provides disaster tolerance for InnoDB Cluster deployments by linking a primary InnoDB Cluster with one or more replicas of itself in different datacenters. InnoDB ClusterSet automatically manages replication from the primary cluster to the replica clusters using a dedicated ClusterSet replication channel. If the primary cluster becomes unavailable due to the loss of the data center or the loss of

network connectivity, you can make a replica cluster active instead to restore the availability of the service.



MySQL InnoDB ClusterSet provides disaster recovery for MySQL.

MySQL Enterprise Backup

Backup

MySQL Enterprise Backup performs online "Hot", non-blocking backups of MySQL databases. Full backups can be performed on all InnoDB data while MySQL is online, without interrupting queries or updates. In addition, incremental backups are supported so that only data that has changed from a previous backup are backed up. Also partial backups are supported when only certain tables or tablespaces need to be backed up.

Restore

MySQL Enterprise Backup restores data from a full backup with full backward compatibility. Consistent Point-in-Time Recovery (PITR) enables restoration to a specific point in time. Using MySQL backups and binlog, you can also perform fine-grained roll forward recovery to a specific transaction. A partial restore allows recovery of targeted tables or tablespaces. In addition, you can restore backups to a separate location, or create clones for fast replication setup or administration.



Compression

MySQL Enterprise Backup supports creating compressed backup files, typically reducing backup size from 70% to over 90% when compared to the size of actual database files, reducing storage and other costs.

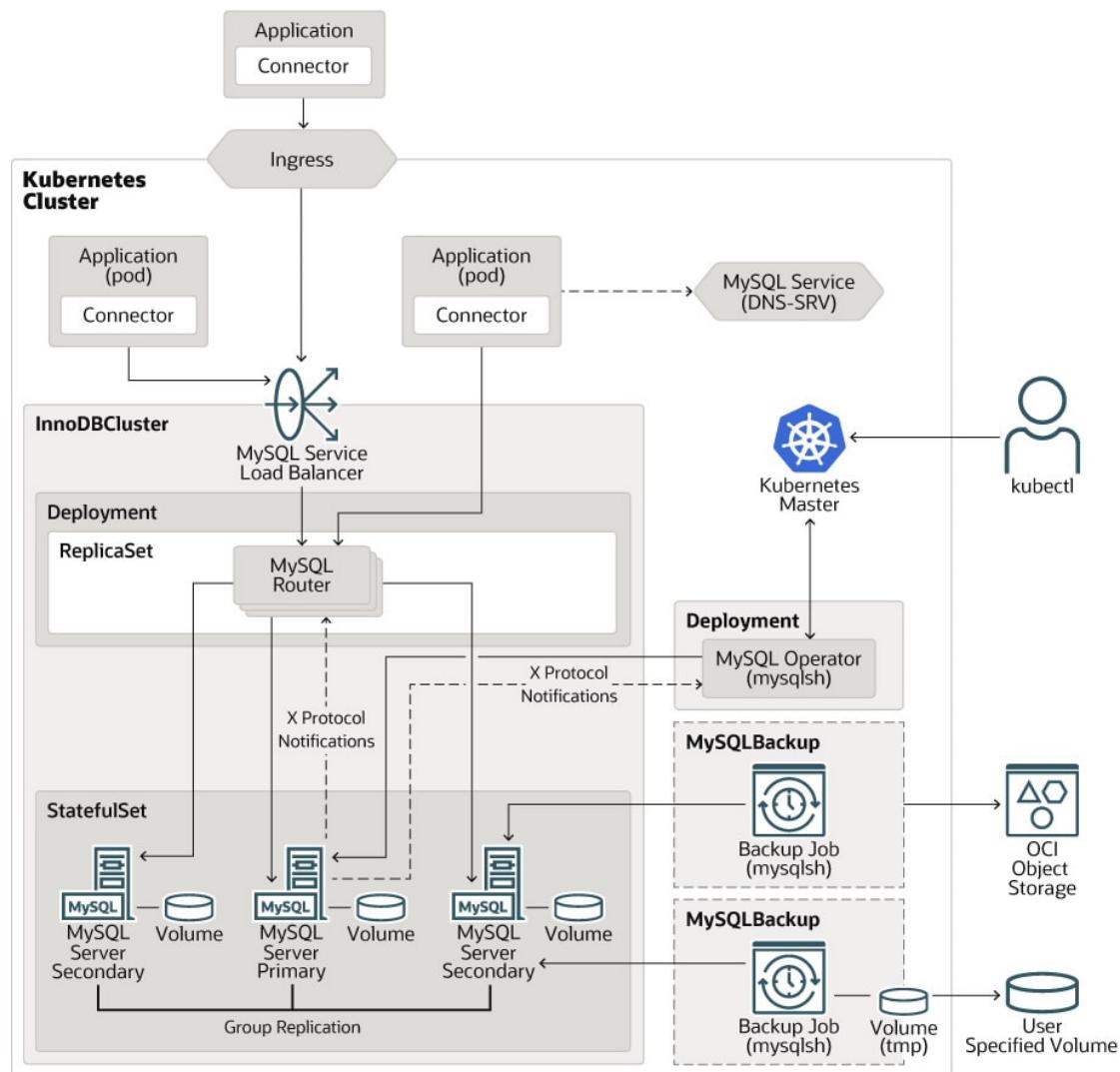
Direct to Cloud Storage

Support for Oracle Storage Cloud, AWS S3 (Simple Storage Service) API to backup and restore direct to inexpensive Cloud Storage (S3, Swift, and more)

MySQL Operator for Kubernetes

Containers, microservices and Kubernetes are helping organizations accelerate their digital transformation initiatives. One of the primary benefits of containerized applications, built using a microservices architecture and managed using Kubernetes, is the portability they provide between Private, Public and Hybrid Cloud.

The MySQL Operator for Kubernetes manages the lifecycle of a high availability MySQL InnoDB Cluster inside Kubernetes. It automates the full MySQL InnoDB Cluster lifecycle including set up, updates, backups and maintenance. For supporting best security practices, the Operator also ensures defaulting to TLS communication, encouraging usage of TLS certificates with integration into Kubernetes certificate management, and restricting the container's capabilities.



MySQL Enterprise Stored Programs

MySQL is natural choice for JavaScript developers who need persistent storage. JavaScript stored programs enable DBAs and developers to build richer, modern, more powerful apps within the MySQL Server. Developers can express complex programming logic directly inside the MySQL Server, minimizing data movement between the database server and applications.

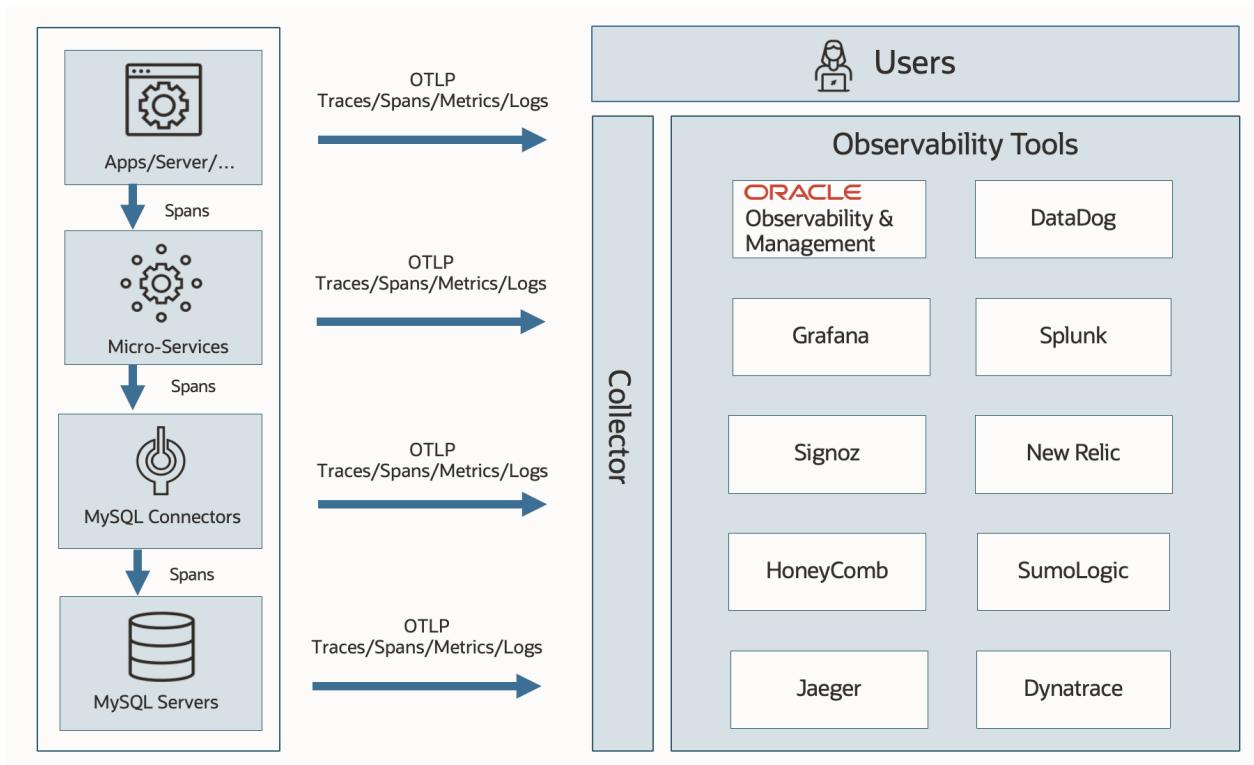
There are many benefits to writing stored programs in JavaScript, instead of SQL:

	SQL Stored Programs	JavaScript Stored Programs
Expressiveness	✗ Difficult to use, lacks basic constructs	✓ Highly expressive and robust
Efficiency	✗ Challenging to optimize due to interpreted code	✓ JavaScript apps are fast and optimized by GraalVM
Ecosystem	✗ Lacks support from IDEs, debuggers, testing frameworks, etc.	✓ Massive ecosystem of tools for developers of JavaScript applications
Developers	✗ Lacks experienced programmers within ecosystem	✓ JavaScript is the most popular developer language
Reusable 3 rd Party Libraries	✗ Few, mostly code examples	✓ Millions

MySQL Enterprise Telemetry

MySQL Enterprise Telemetry allows users to define, create, and collect telemetry data from MySQL to monitor MySQL performance and behavior from a variety of observability and management tools.

MySQL provides telemetry data, such as traces and metrics, using the CNCF (Cloud Native Compute Foundation) OpenTelemetry observability framework— a vendor neutral standard that includes common libraries, protocols and tools.



Monitor MySQL from Industry Leading Observability Tools

Traces

Telemetry tracing provides a holistic view of how your entire system operates all the way to the MySQL Database level. OpenTelemetry traces offer several valuable benefits for users of MySQL Enterprise Telemetry:

- Improved Debugging - Reveals the entire journey of a request, pinpointing bottlenecks and errors, helping identify issues faster and with more context.
- Simplified Troubleshooting and Incident resolution - Tracing lets you track the request across apps, microservices to the database, pinpointing the root cause within the specific service that's malfunctioning.
- Performance optimization - By visualizing request flows, you can spot the slowest requests.
- Database Performance Analysis - Reveals how long requests spend interacting within the MySQL database, helping you identify slow database queries to optimize for improved performance.

Metrics

MySQL Enterprise Telemetry metrics are highly configurable allowing users to specify what to send from over 300 MySQL gauges and counters. Metrics can easily be enabled and disabled and timing intervals for exporting metrics from MySQL can be customized.

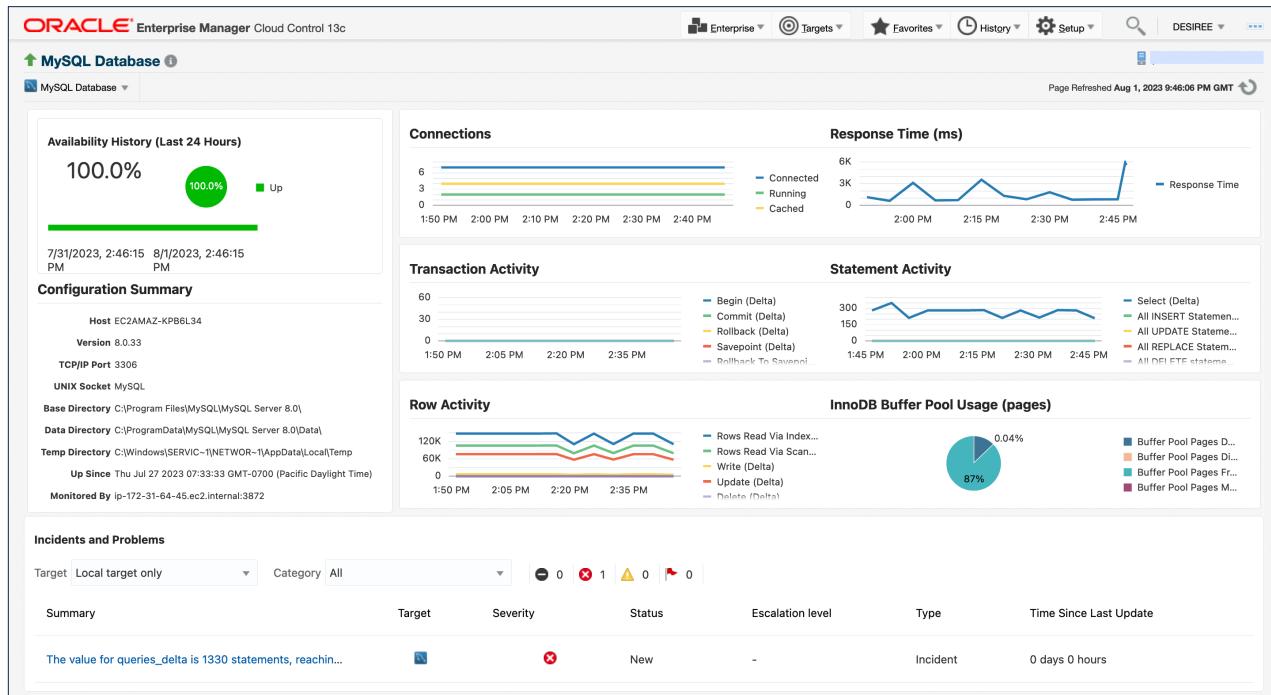
OpenTelemetry metrics offer several valuable benefits for users of MySQL Enterprise Telemetry:

- Quantifiable Performance Measurement - Metrics precisely measure various aspects of database performance. Allowing for evaluation and identification of bottlenecks or opportunities for optimization.
- Detailed Insights - Metrics can capture a wide range of data points, including database connection counts, query execution times, cache hit rates, and more. This detailed information provides a deeper understanding of how the database is functioning.
- Proactive Monitoring - By continuously collecting and analyzing metrics, you can proactively identify potential issues before they impact user experience. This enables preventative maintenance and ensures optimal database performance.
- Trend Analysis - Over time, metrics data can be used to identify trends and patterns. This allows you to forecast future resource needs and make data-driven decisions for database scaling or optimization.
- Correlation with Tracing Data - When used in conjunction with tracing data, metrics provide a holistic view of database behavior. You can correlate specific metrics with trace data to pinpoint the root cause of performance issues or identify queries that consume excessive resources.

MySQL OpenTelemetry metrics equips you with the quantitative data necessary to make informed decisions about your MySQL Enterprise database, ensuring its efficiency, scalability, and optimal user experience.

Oracle Enterprise Manager for MySQL

Oracle Enterprise Manager for MySQL provides Oracle developers and DBAs with real-time monitoring and delivers comprehensive performance, availability and configuration information for your MySQL databases. Enterprise Manager collects more than 500 metrics covering various MySQL components. Custom critical and warning thresholds can then be set for each of the collected metrics. Plus, DBAs can track configuration details over time to easily keep track of configuration changes.



Oracle Enterprise Manager for MySQL allows DBAs to manage MySQL databases.

More information about Oracle Enterprise Manager for MySQL is available at:
<http://www.mysql.com/products/enterprise/em.html>

Oracle Product Certifications/Integrations

An estimated 70% of Oracle's customers also use MySQL. MySQL Enterprise Edition makes managing MySQL easier in these environments by certifying and supporting the use of the MySQL Database in conjunction with many Oracle products. These include:

- Oracle Linux
- Oracle VM
- Oracle Secure Backup
- Oracle Golden Gate
- Oracle Audit Vault and Database Firewall
- Oracle Enterprise Manager

Oracle Premier Support

Oracle offers 24x7, global support for MySQL. The MySQL Support team is composed of seasoned MySQL developers, who are database experts and understand the issues and challenges you face. With Oracle Premier Support, you can lower the total cost and risk of owning your MySQL databases, improve the return from your IT investment, and optimize the business value of your IT solutions. MySQL support is included in the subscription for end users, and available separately from commercial licenses for ISVs and OEMs. Oracle Premier Support for MySQL includes the following features:

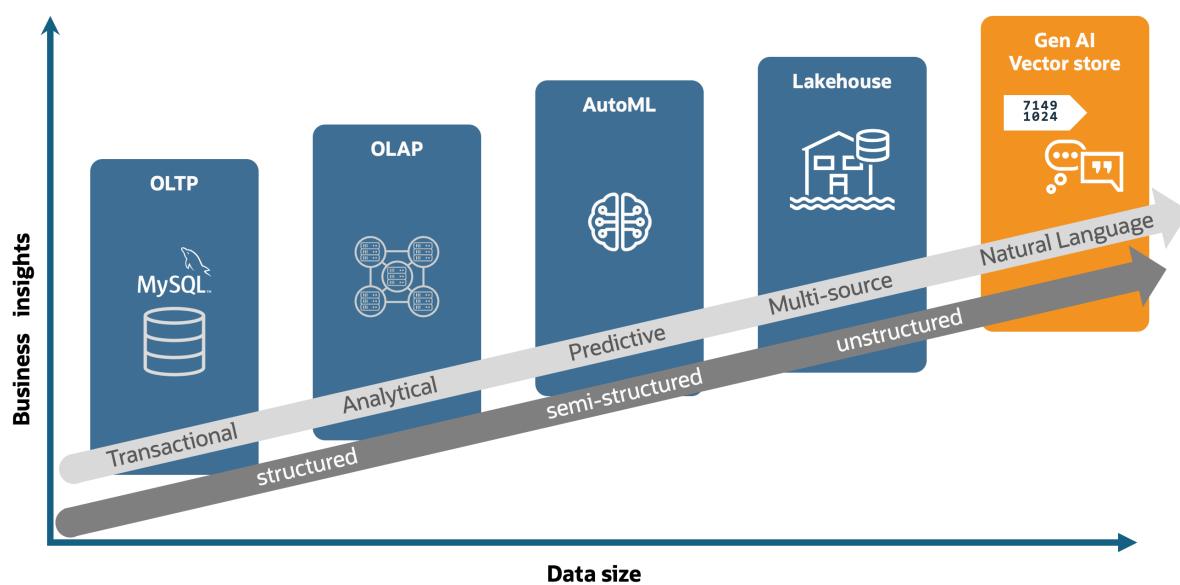
- 24 X 7 production support
- Unlimited support incidents
- Knowledge Base
- Maintenance releases, bug fixes, patches and updates
- Staffed by the most experienced MySQL Engineers in the industry
- The ability to get MySQL support in 29 languages

Learn more about Oracle Premier Support:

<http://mysql.com/support/>

HeatWave

HeatWave is the cloud database service built and operated by the MySQL Engineering Team.



HeatWave GenAI - Take advantage of generative AI without AI expertise or data movement. HeatWave GenAI provides integrated and automated generative AI with in-database large language models (LLMs); an automated, in-database vector store; and the ability to have contextual conversations in natural language.

HeatWave MySQL - Accelerate MySQL query performance by orders of magnitude and get real-time analytics on your transactional data—without the complexity, latency, risks, and cost of ETL duplication. Rely on the only cloud service built on MySQL Enterprise Edition.

HeatWave Lakehouse - Query data in various formats in object storage and optionally combine it with transactional data in MySQL databases. HeatWave Lakehouse delivers unmatched performance and price-performance.

HeatWave AutoML - Automate the pipeline to build, train, and explain ML models using data in object storage and MySQL Database—with moving the data to a separate ML cloud service and at no additional cost.

Conclusion

In this paper we explored the components that are included in MySQL Enterprise Edition. These components are designed to help you mitigate security risk and meet Service Level Agreements (SLAs) as you implement applications built on the lower that comes with standardizing on MySQL and other open source technologies. MySQL Enterprise Edition extends the MySQL Database to include advanced security features for Authentication, Encryption, Firewall, Masking, and Auditing. MySQL Enterprise HA provides native high availability and cross-region disaster recovery. Enterprise Backup augments your HA environment by performing online "Hot", non-blocking backups of your MySQL databases. Oracle Enterprise Monitor for MySQL provides real-time monitoring and delivers comprehensive performance, availability and configuration information for your MySQL databases. Finally, the Oracle Premier Support provides you with 24x7 support with quick answers and resolutions when you need help, so your systems provide uninterrupted availability to your customers.

For customers that want a cloud service built and managed by the MySQL Engineering Team, HeatWave provides automated and integrated generative AI and machine learning (ML) in one cloud service for transactions and lakehouse scale analytics. Get



faster insights from all your data with unmatched performance and deploy apps in your choice of cloud providers.

Additional Resources

Try MySQL Enterprise Edition:

<https://www.oracle.com/mysql/technologies/mysql-enterprise-edition-downloads.html>

MySQL Enterprise Edition: White Papers

<https://www.mysql.com/why-mysql/white-papers/>

MySQL Enterprise Edition: On Demand Webinars

<https://www.mysql.com/news-and-events/on-demand-webinars/>

To contact a MySQL Representative:

<http://www.mysql.com/about/contact/>