



MySQL Enterprise Edition & MySQLによるコンプライアンス対応

Shinya Sugiyama / 杉山真也

MySQL Principal Sales Consult, MySQL Global Business Unit

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

MySQL Enterprise Edition : Agenda

Enterprise Edition General Information

- 1 MySQL Enterpriseのご紹介
- 2 レポーティング, 管理ツール, 拡張機能
- 3 技術サポート& オラクル製品との動作保証

Security Introduction

- 4 MySQLによるコンプライアンス対応

A high-speed photograph of a dolphin leaping from the surface of the ocean. The dolphin is captured mid-air, its body arched as it moves from the bottom right towards the top left. Water droplets and spray are frozen around the dolphin's head and body, emphasizing the motion. The background is a clear, deep blue sky. The dolphin's reflection is visible in the calm water below.

MySQL Enterpriseのご紹介

http://www-jp.mysql.com/downloads/ MySQL :: MySQL ... x

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

Please Log In serverNolanaSequenci... MySQL Sales Consultin... zimbra 受信箱 (2) My Oracle Support Media Pack Search

Enterprise Community Yum Repository APT Repository Windows Archives

MySQL Downloads

購入に関するお問い合わせ

MySQL Enterprise Edition(commercial)
MySQL Enterprise Edition includes the most comprehensive set of advanced features and management tools for MySQL.

- MySQL Database
- MySQL Storage Engines (InnoDB, MyISAM, etc.)
- MySQL Connectors (JDBC, ODBC, .Net, etc.)
- MySQL Replication
- MySQL Fabric
- MySQL Partitioning
- MySQL Utilities
- MySQL Workbench
- MySQL Enterprise Backup
- MySQL Enterprise Monitor
- MySQL Enterprise HA
- MySQL Enterprise Scalability
- MySQL Enterprise Security
- MySQL Enterprise Audit

[Learn More »](#)
[Download from Oracle eDelivery »](#)

MySQL Cluster CGE(commercial)
MySQL Cluster is a real-time open source transactional database designed for fast, always-on access to data under high throughput conditions.

- MySQL Cluster
- MySQL Cluster Manager
- Plus, everything in MySQL Enterprise Edition

[Learn More »](#)
[Download from Oracle eDelivery »](#)

MySQL Community Edition(GPL)
[Community \(GPL\) Downloads »](#)

MySQL お問い合わせ窓口
0120-065556

【受付時間】
平日 9:00-12:00/13:00-18:00
(祝日及び年末年始休業日を除きます)

MySQL-
Sales_jp_grp@oracle.com

USA:
+1-866-221-0634

Canada:
+1-866-221-0634

Germany:
+49 89 143 01280

France:
+33 1 57 60 83 57

Italy:
+39 02 249 59 120

UK:
+44 207 553 8447

Japan: 0120-065556

China:
10800-811-0823

India:

MySQLのコミュニティ版と商用版

コミュニティ版 (GPL)	商用版 (Commercial)
• MySQL Community Server • MySQL Cluster (Community Edition) • MySQL GUI管理ツール • MySQLコネクタ (JDBC, ODBC, etc) • ドキュメント • フォーラム	• Standard Edition • Enterprise Edition • MySQL Cluster Carrier Grade Edition • 商用ライセンス (組み込み用) • トレーニング • プロフェッショナルサービス

- コミュニティ版ソフトウェアはGPLでソースコードも公開し提供
- 商用版は、付加価値として技術サポートや管理機能、拡張機能を有償で提供

[参照: MySQL Downloads](#)

MySQL Enterprise Edition のサービスカテゴリー



拡張機能

- 拡張性
- 高可用性
- セキュリティ
- 監査
- 暗号化



管理ツール

- 監視
- バックアップ
- 開発
- 管理
- マイグレーション



サポート

- 技術サポート
- コンサルティングサポート
- オラクル製品との動作保証



	MySQL Editions		
	Standard SE	Enterprise EE	Cluster CGE
機能概要			
MySQL Database	✓	✓	✓
MySQL Connectors	✓	✓	✓
MySQL Replication	✓	✓	✓
MySQL Fabric		✓	✓
MySQL Partitioning		✓	✓
MySQL Utilities		✓	✓
Storage Engine: MyISAM, InnoDB	✓	✓	✓
Storage Engine: NDB (ndbcluster)			✓
MySQL Workbench SE/EE*	✓	✓	✓
MySQL Enterprise Monitor*		✓	✓
MySQL Enterprise Backup*		✓	✓
MySQL Enterprise Security (外部認証サポート) *		✓	✓
MySQL Enterprise Audit (ポリシーベース監査機能) *		✓	✓
MySQL Enterprise Encryption (非対称暗号化)*		✓	✓
MySQL Enterprise Scalability (スレッドプール) *		✓	✓
MySQL Enterprise High Availability (HAサポート) *		✓	✓
Oracle Enterprise Manager for MySQL *		✓	✓
MySQL Cluster Manager (MySQL Cluster管理) *			✓
MySQL Cluster Geo-Replication			✓

*商用版のみで利用可能な追加機能

	MySQL Editions		
	Standard SE	Enterprise EE	Cluster CGE
Oracle Premium Support			
24時間365日サポート	✓	✓	✓
インシデント数無制限	✓	✓	✓
ナレッジベース	✓	✓	✓
バグ修正&パッチ提供	✓	✓	✓
コンサルティングサポート	✓	✓	✓
オラクル製品との動作保証			
Oracle Linux	✓	✓	✓
Oracle VM	✓	✓	✓
Oracle Solaris	✓	✓	✓
Oracle Enterprise Manager		✓	✓
Oracle GoldenGate		✓	✓
Oracle Data Integrator		✓	✓
Oracle Fusion Middleware		✓	✓
Oracle Secure Backup		✓	✓
Oracle Audit Vault and Database Firewall		✓	✓

※最新の対比表は、[MySQL Editionsのサイト](#)を参照下さい。

MySQL Enterprise Edition 管理ツールと拡張機能概要

MySQL Enterprise Edition

MySQL Enterprise Monitor

複数サーバの一括管理、クエリ性能分析

MySQL Enterprise Backup

高速なオンラインバックアップ、ポイントインタイムリカバリ

MySQL Enterprise Scalability

Thread Poolプラグインによる性能拡張性の向上

MySQL Enterprise Security

LDAPやWindows Active Directoryとの外部認証と統合管理

MySQL Enterprise Audit

ユーザ処理の監査、Oracle DBと同じツールで管理可能

MySQL Enterprise Encryption

非対称暗号化([公開鍵暗号](#))の業界標準機能を提供

Oracle Enterprise Manager for MySQL

Oracle Enterprise ManagerからMySQLを統合管理可能

Oracle Premier Support

24x7, インシデント無制限、コンサルティングサポート

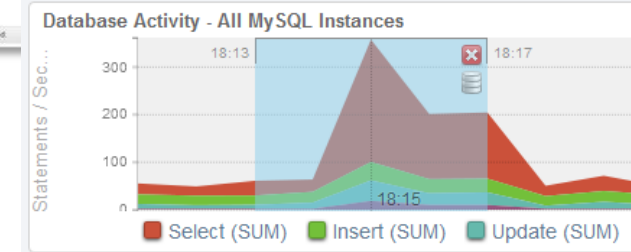
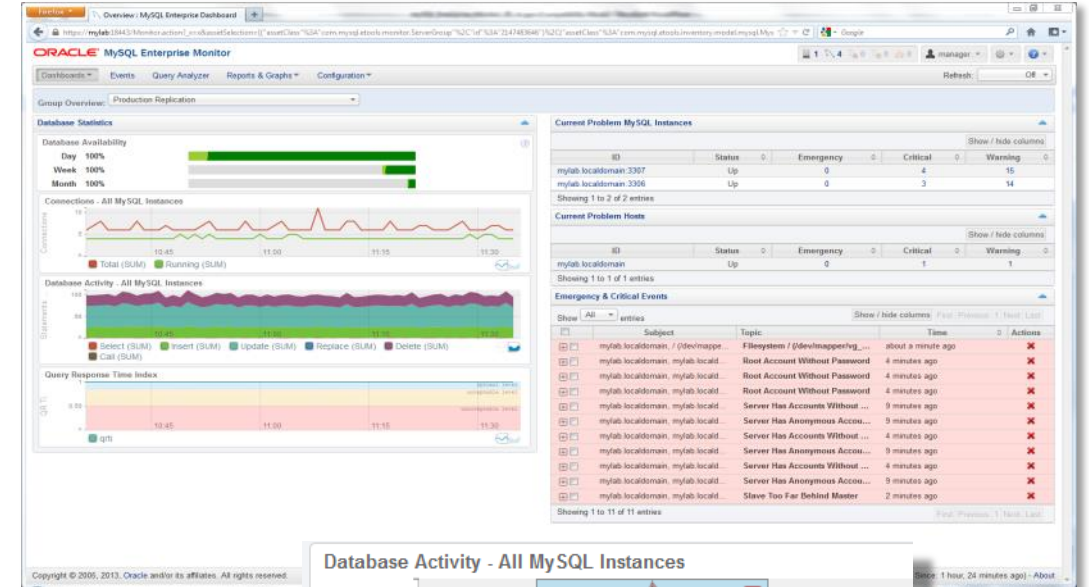
MySQL Enterprise Edition 管理ツール



1. MySQL Enterprise Monitor

- パフォーマンスと可用性の監視
- 問題のあるSQL文の検知
- ディスク監視と容量プランニング
- クラウド対応アーキテクチャ
 - ポリシーベースの設定
 - エージェント導入不要
- MySQL監視を10分以内で開始可能

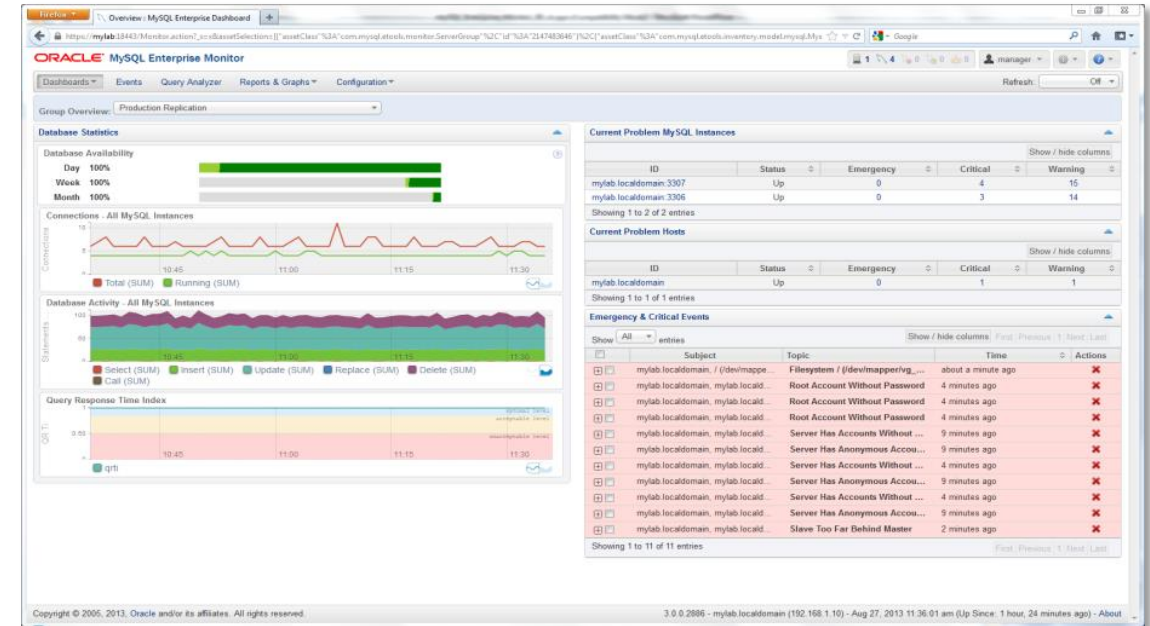
参照: [MySQL Enterprise Monitor](#)



	Current	Worst	Subject	Topic
+	!	!	mylab.localdomain, mylab.localdomain:3306	Root Account Without Password
+	!	!	mylab.localdomain, mylab.localdomain:3306	Server Has Accounts Without A Password
+	✓	!	mylab.localdomain, mylab.localdomain:3306	Average Statement Execution Time Excess...
+	✓	!	mylab.localdomain, mylab.localdomain:3306	SQL Statement Generates Errors or Warnings
+	!	!	mylab.localdomain, mylab.localdomain:3306	Server Has Anonymous Accounts
+	✓	!	mylab.localdomain, mylab.localdomain:3306	MySQL Instance Is Experiencing A Query P...
+	!	!	mylab.localdomain, mylab.localdomain:3306	InnoDB Log Buffer Flushed To Disk After Ea...
+	!	!	mylab.localdomain, mylab.localdomain:3306	User Has Rights To Database That Does Not...

Enterprise Monitor Dashboard

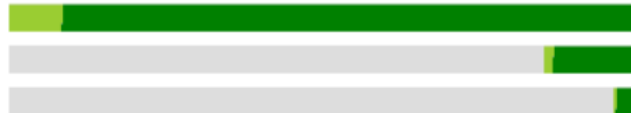
- サービスレベルのモニタリング
- リアルタイムパフォーマンス監視
- 警告と通知による迅速な対応
- ベストプラクティスアドバイザー
- 全MySQL サーバを視覚的に管理



Database Statistics

Database Availability

Day 100%
Week 100%
Month 100%



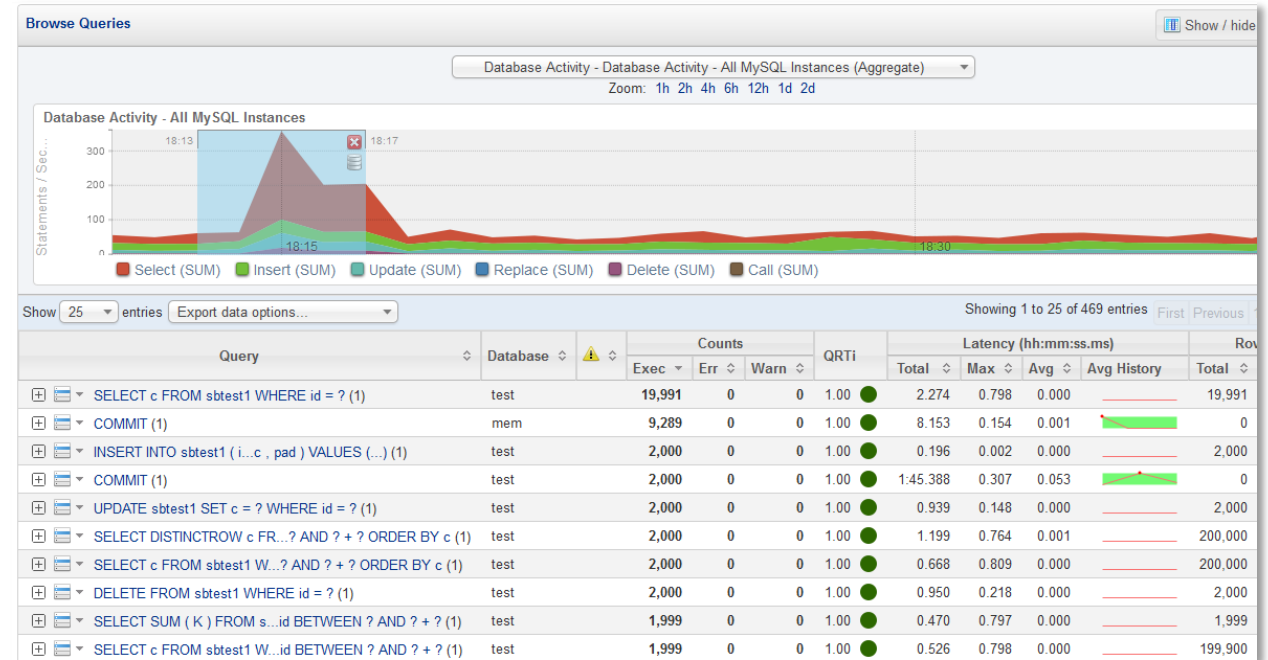
"The MySQL Enterprise Monitor is an absolute must for any DBA who takes his work seriously."

- Adrian Baumann, System Specialist
Federal Office of Information Technology & Telecommunications



Enterprise Query Analyzer

- 全クエリーのリアルタイム統合監視
- パフォーマンスの可視化
- コストの大きいクエリーの設定
- クエリー統計詳細の確認
- Query Response Time index (QRTi)
 - クエリーサービスレベル指針
 - サーバー、インスタンスのサービスレベル
 - クエリーパフォーマンス指標



"With the MySQL Query Analyzer, we were able to identify and analyze problematic SQL code, and triple our database performance. More importantly, we were able to accomplish this in three days, rather than taking weeks."

Keith Souhrada
Software Development Engineer
Big Fish Games

Enterprise Replication Monitor

- レプリケーショントポロジーの自動検知
- マスター/スレーブのパフォーマンス監視
- レプリケーションアドバイザーによるサポート
- レプリケーションのベストプラクティスを提示

"I use the MySQL Enterprise Monitor every day to monitor and keep tabs on our MySQL databases. Quick one stop shopping for keeping tabs on them."

-Wes Homer,
Sr System and Network Administrator



Replication Monitoring										
^ Servers	Type	Threads		Time Behind	Binary Logs		Master Position		Log Space	
		IO	SQL		Current File	Position	Binary Log	Position	Binary Logs	Relay Logs
  ▾ Replication 1 (4)	MIXED									
 mylab.localdomain:3306	master/slave			00:00:00	mylab-bin.000001	791	mylab-bin.000001	791	791 B	1.1 KB
 mylab.localdomain:3307	master/slave			00:00:00	mylab-bin.000001	791	mylab-bin.000001	791	791 B	1.1 KB
 mylab.localdomain:3308	master/slave			00:00:00	mylab-bin.000001	986	mylab-bin.000001	791	0.96 KB	1.1 KB
 MLORD-PC:3306	slave			00:00:00			mylab-bin.000001	986		1.29 KB

Best Practice Advisors

- MySQLベストプラクティスを適用可能
- 14アドバイザのカテゴリー
- 250以上のサブアドバイザカテゴリー
- 閾値ベースの警告管理
 - 指数移動平均
 - 変更率の検知
- 問題解決のアドバイスを提供
 - カスタムスクリプトの作成、展開、バージョンング、管理にかかる時間を短縮。
 - データベース管理者だけでは発見不可能な問題やチューニング方法をアドバイス。

Advisors	
 Edit Selected Advisors	 Disable Selected Advisors
 Create Advisor	 Import/Export
Administration	Configured: 26 of 26
Agent	Configured: 3 of 3
Availability	Configured: 6 of 6
Backup	Configured: 5 of 5
Cluster	Configured: 10 of 10
Graphing	Configured: 87 of 87
Memory Usage	Configured: 6 of 6
Monitoring and Support Services	Configured: 5 of 5
Operating System	Configured: 5 of 5
Performance	Configured: 23 of 23
Query Analysis	Configured: 4 of 4
Replication	Configured: 13 of 13
Schema	Configured: 17 of 17
Security	Configured: 26 of 26

"I definitely recommend the MySQL Enterprise Monitor to DBAs who don't have a ton of MySQL experience. It makes monitoring MySQL security, performance and availability very easy to understand and to act on."

Sandi Barr
Sr. Software Engineer
Schneider Electric



MySQL Enterprise Monitor + Backup

- バックアップ結果のモニタリング
- バックアップパフォーマンスのモニタリング
- 最新バックアップ取得を確実にする事が可能

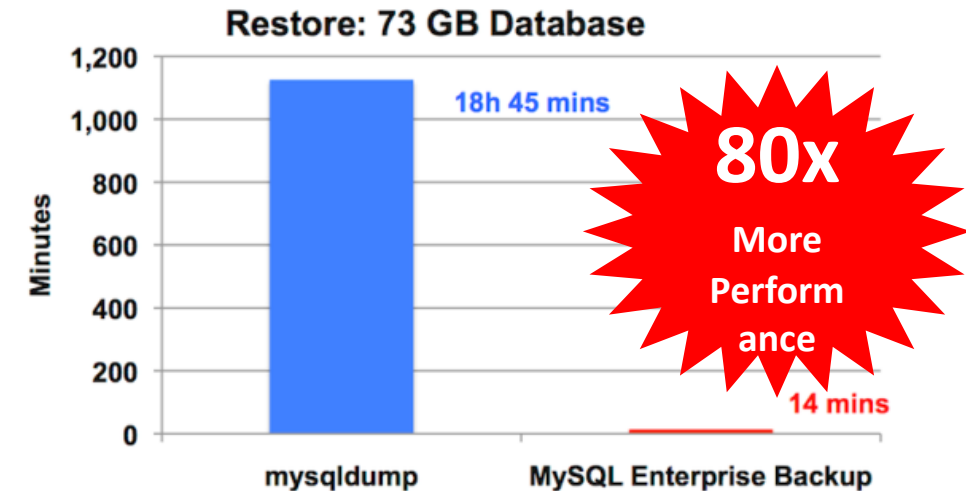
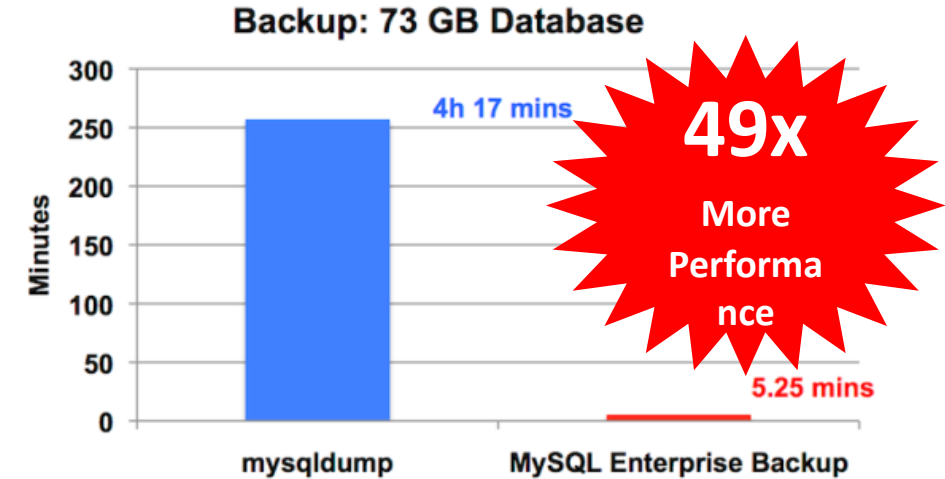
ORACLE MySQL Enterprise Monitor

Dashboards ▾ Events Query Analyzer Reports & Graphs ▾ Configuration ▾						
Advisors						
Edit Selected Advisors Disable Selected Advisors Create Advisor Import/Export						
Administration		Configured: 26 of 26				
Agent		Configured: 3 of 3				
Availability		Configured: 6 of 6				
Backup		Configured: 5 of 5				
☐ Item	Info	Coverage	Schedule	Event Handling		
MySQL Enterprise Backup Failed		100% (1/1)	5m	0	0	0 "FAILURE"
MySQL Enterprise Backup Succeeded		100% (1/1)	5m	1	0	0 "SUCCESS"
Last Full MySQL Enterprise Backup Too Old		100% (1/1)	6h	1	0	0 7
Incremental MySQL Enterprise Backups Not Enabled		100% (1/1)	6h	1	0	0 0
MySQL Enterprise Backup Lock Time Excessive		100% (1/1)	5m	0	0	0 10 60

MySQL Enterprise Backup

高速、オンラインバックアップ & リカバリ

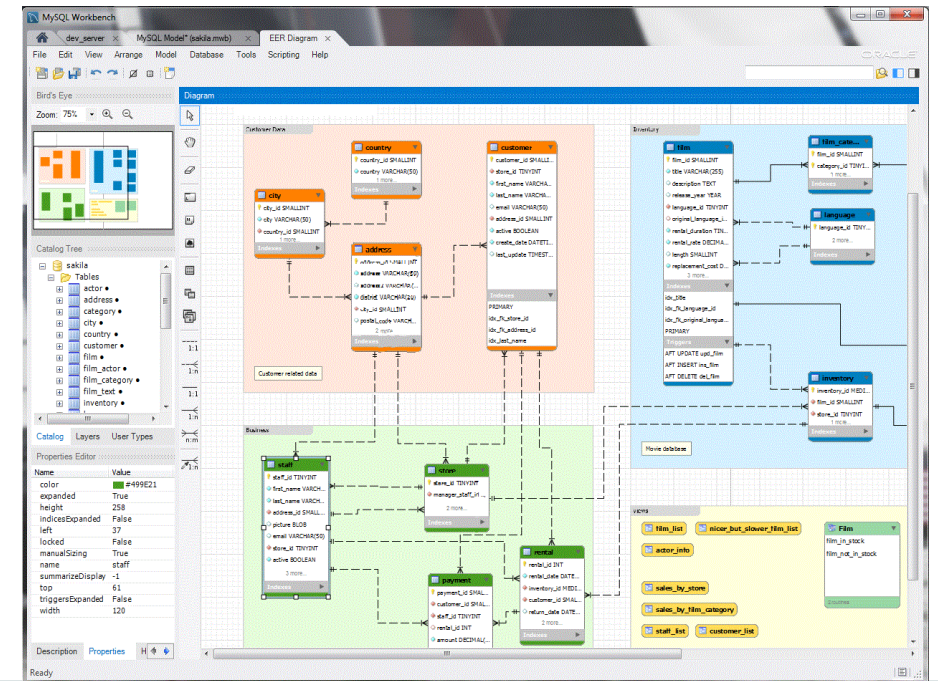
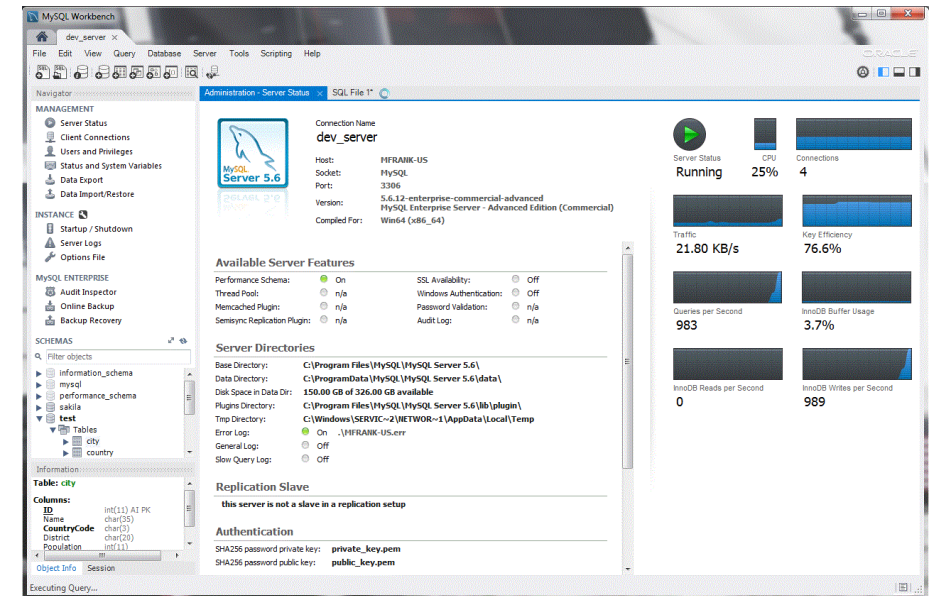
- InnoDBのオンラインバックアップツール
- フル、増分、部分バックアップ(圧縮可能)
- ポイントインタイム、フル、部分リカバリ
- マルチスレッドによる並列バックアップ&リカバリ処理
- クラウドストレージとの直接の連携(S3, etc.)
- 暗号化 – AES 256
- バイナリログおよびリレーログのバックアップ
- Oracle Secure Backupとの連携
- マルチプラットフォーム対応 (Windows, Linux, Unix)



MySQL Workbench 6.2

MySQL Workbench は、データベースアーキテクト、開発者、DBAのための統合ビジュアルツールです。

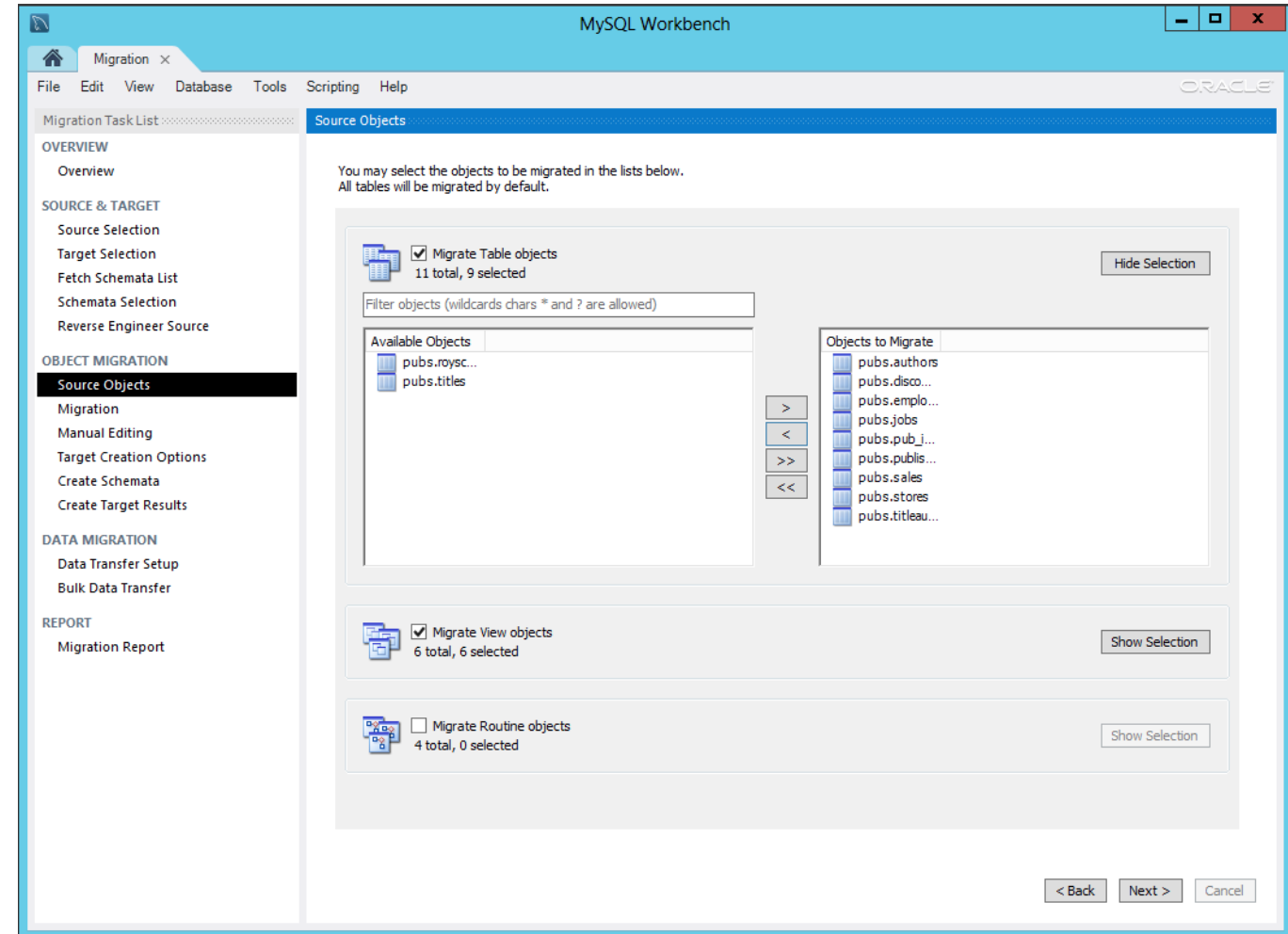
- Fabric対応
 - Fabricノードの追加、構成確認、接続
 - Performance Dashboard
 - パフォーマンススキーマのレポートとグラフ
 - Visual Explain
 - GIS Viewer
 - マイグレーション
 - **New** Microsoft Access
 - Microsoft SQL Server, Sybase, PostgreSQL
- 商用: DBドキュメント出力, データモデルの検証,
MySQL Enterprise Backup GUI, MySQL Enterprise Audit GUI



MySQL Workbench EE

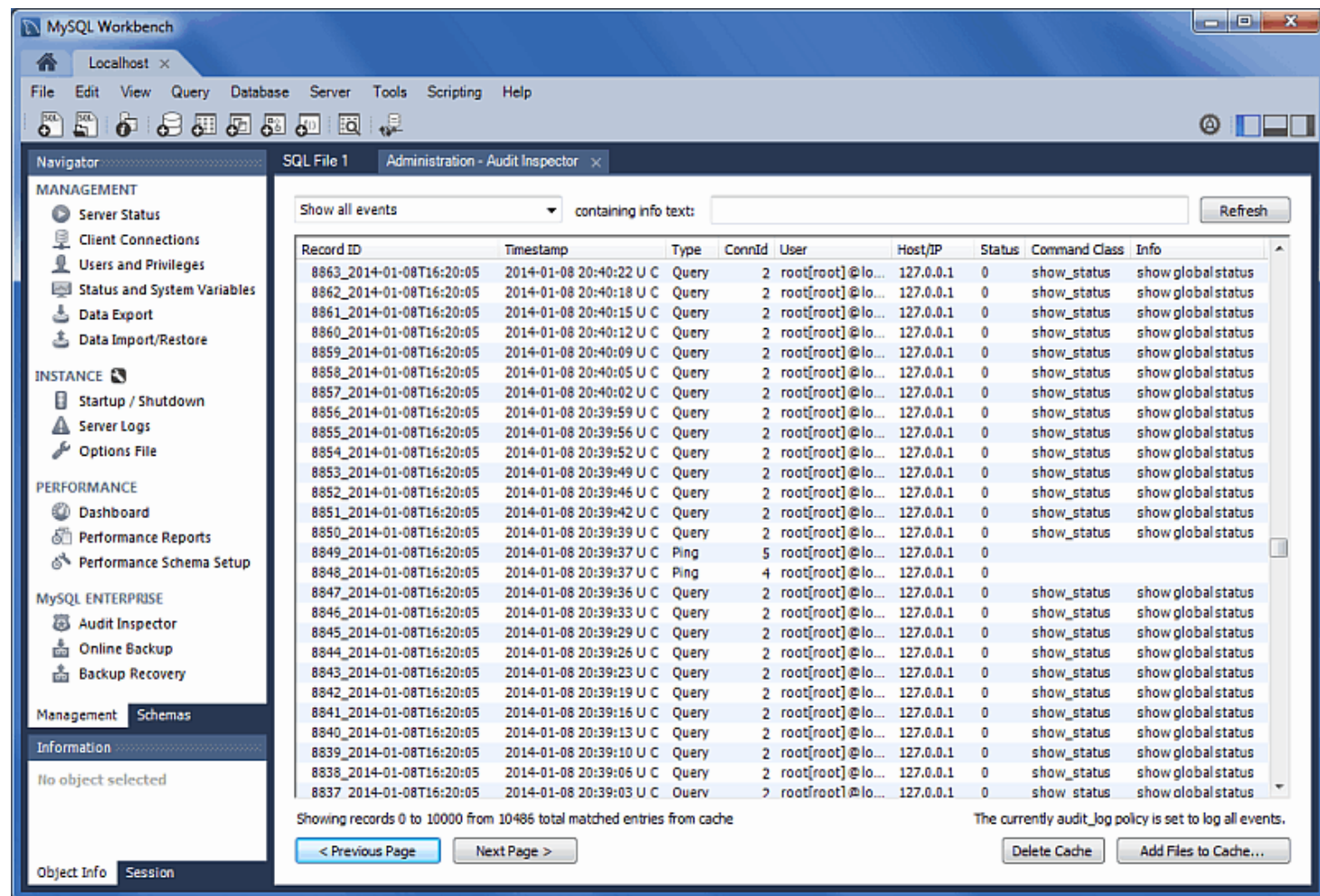
- データベースマイグレーション
 - From Microsoft SQL Server, PostgreSQL, Sybase ASE, Sybase SQL Anywhere, SQLite, Microsoft Access, and more
- 移行プロジェクトの管理
- 移行元DB と移行先DBの選定
- オブジェクトの移行
- データマイグレーション
- MySQLバージョンアップグレード

New! Database Migration Wizard
for SQL Server, Sybase, SQLite, SQL Anywhere & PostgreSQL



MySQL Workbench EE + Audit

- 監査イベントへ迅速且つ容易にアクセス可能
- インデックスを利用した監査ログの検索が可能
 - イベントタイプ
 - ユーザーアカウント
 - 日付範囲
 - テキストマッチ



MySQL Workbench EE + Backup

- バックアップジョブの作成と管理
 - 新規バックアップジョブの作成
 - バックアップジョブのスケジュール化と自動実行
 - 有効なバックアップジョブ確認
 - 最新バックアップアクティビティの確認
- バックアップデータのリストア
 - フル、差分、部分的

The screenshot displays the MySQL Enterprise Backup configuration window within the MySQL Workbench EE interface. The left sidebar shows the 'MySQL ENTERPRISE' section with 'Audit Inspector', 'Online Backup', and 'Backup Recovery' options. The main window is titled 'MySQL Enterprise Backup' and contains the following sections:

- Backup Jobs configured for this MySQL Instance:** A table listing backup jobs and their status.
- Backup Job Details:** Configuration details for a selected job.
- Recent Activity:** A table showing the history of backup operations.

Annotations on the screenshot include:

- A red box around the 'Backup Jobs' table.
- A red box around the 'Backup Job Details' section.
- A red box around the 'Recent Activity' table.
- A red arrow pointing to the 'View Log...' button with the text: 'Only displayed when a backup job is currently being executed'.
- A red arrow pointing to the 'Execute Now' button with the text: 'Immediately execute a backup job'.

Backup Job	Latest Backup	Next Full Backup	Next Incr. Backup	Configuration Status
Full (full data)	in the last hour	2014-01-09 17:24:00	not scheduled	✓
backupsinc (full data)	in the last hour	not scheduled	2014-01-09 18:00:00	✓
TestingWorld (partial...)	in the last hour	not scheduled	not scheduled	✓

Target Host:	PHILIP-US3306
MEB Version:	3.8.2
MySQL Data Directory:	C:\ProgramData\MySQL\MySQL Server 5.6\data\
Storage Directory:	C:\MySQL BackupHome\Full
212.00 GB of 326.00 GB available	
Latest Full Backup:	2014-01-09 17:11:38
Latest Incr. Backup:	Never
Next Full Backup:	2014-01-09 17:24:00
Next Incr. Backup:	Not scheduled

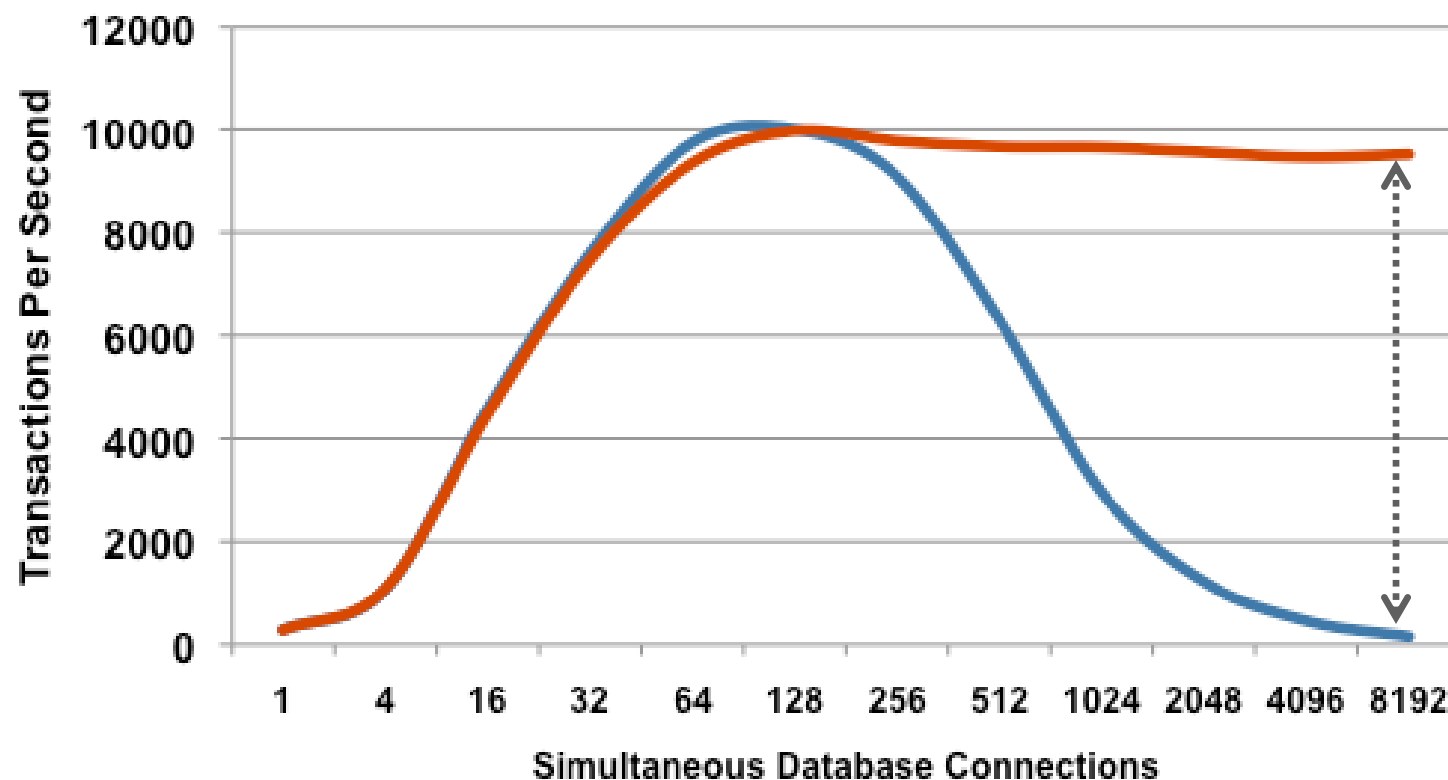
Job	Type	Format	Status	Start Time	End Time	Total Time
Full	FULL	DIRECTORY	✓ SUCCESS	2014-01-09 17:10:52	2014-01-09 17:11:38	1min 26s
Full	FULL	DIRECTORY	✓ SUCCESS	2014-01-09 17:09:49	2014-01-09 17:10:38	1min 29s
TestingWorld	INCREMENTAL	DIRECTORY	✓ SUCCESS	2014-01-09 17:08:56	2014-01-09 17:09:12	56s
TestingWorld	PARTIAL	DIRECTORY	✓ SUCCESS	2014-01-09 17:08:06	2014-01-09 17:08:28	22s
Full	FULL	DIRECTORY	✓ SUCCESS	2014-01-09 17:07:25	2014-01-09 17:07:46	21s
backupsinc	INCREMENTAL	DIRECTORY	✓ SUCCESS	2014-01-09 17:00:01	2014-01-09 17:00:21	20s
backupsinc	FULL	DIRECTORY	✓ SUCCESS	2014-01-09 16:25:12	2014-01-09 16:25:47	35s

MySQL Enterprise Scalability : Thread Pool

Provides 60x better scalability

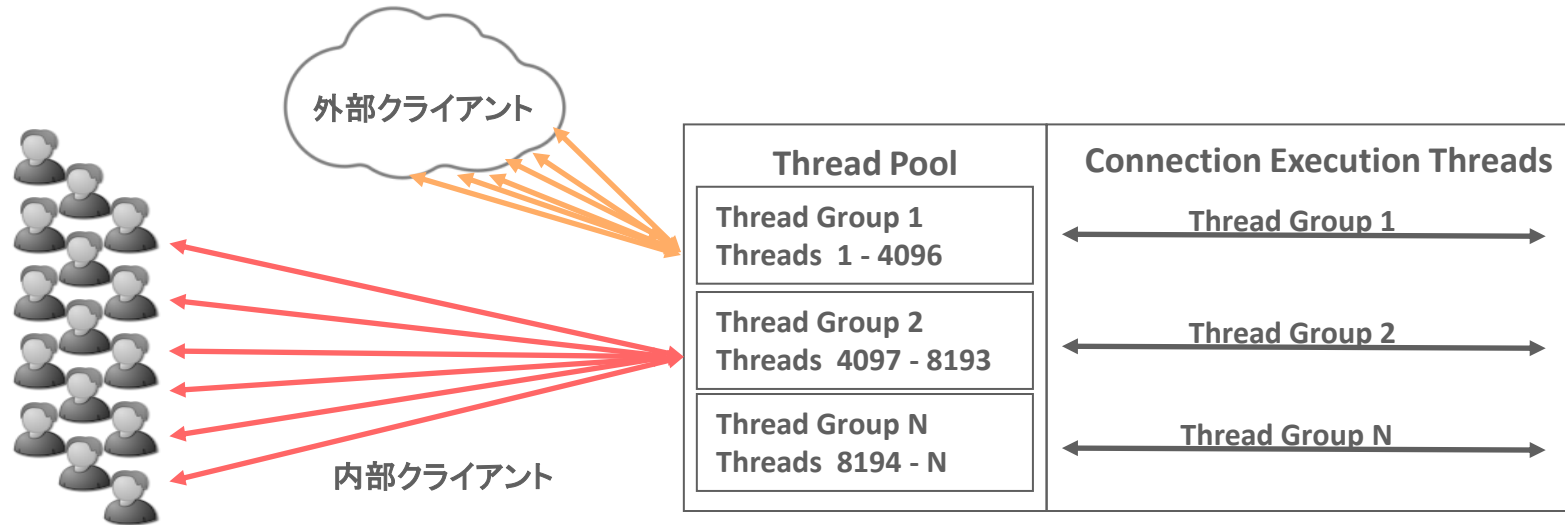
- ユーザ接続数の増加に対応し、パフォーマンスとスケーラビリティを維持

MySQL 5.6 Sysbench OLTP Read/Write



参照: [MySQL Enterprise Scalability](#)

MySQL Enterprise Scalability : Thread Pool



- スレッド・グループ数を設定可能(デフォルト = 16)
 - 各スレッドグループは最大4096再利用可能なスレッドをサポート
- ラウンド・ロビンによって各接続をスレッド・グループに割り当て
- スレッドは優先付けされステートメントキューに挿入される
 - サーバの負荷や接続増加に対応したスケーラビリティを確保



技術サポート& オラクル製品との動作保証

MySQL Enterprise Support

- 最大のMySQLのエンジニアリングおよびサポート組織
- MySQL開発チームによるサポート
- 29言語で世界クラスのサポートを提供
- メンテナンス・リリース、バグ修正、パッチ、アップデートの提供
- 24時間x365日サポート
- 無制限サポート・インシデント
- MySQL コンサルティング・サポート

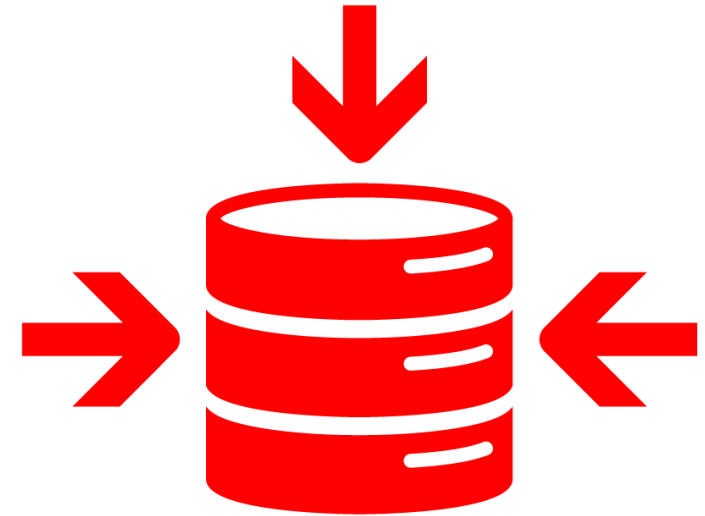


Get immediate help for any MySQL
issue, plus expert advice

MySQL Consultative Support

Make the Most of your Deployments

- リモート・トラブル・シューティング
- レプリケーション・レビュー
- パーティショニング・レビュー
- スキーマ・レビュー
- クエリー・レビュー
- パフォーマンス・チューニング
- ...and more



参照: [MySQL コンサルティング・サポート](#)

MySQL & オラクル製品との動作保証

- Oracle Linux
- Oracle VM
- Oracle Solaris
- Oracle Clusterware
- Oracle Secure Backup
- Oracle Enterprise Manager
- Oracle Fusion Middleware
- Oracle GoldenGate
- Oracle Audit Vault & Database Firewall
- MyOracle Online Support

MySQL Integrates into your Oracle Environment



Oracle Enterprise Manager for MySQL

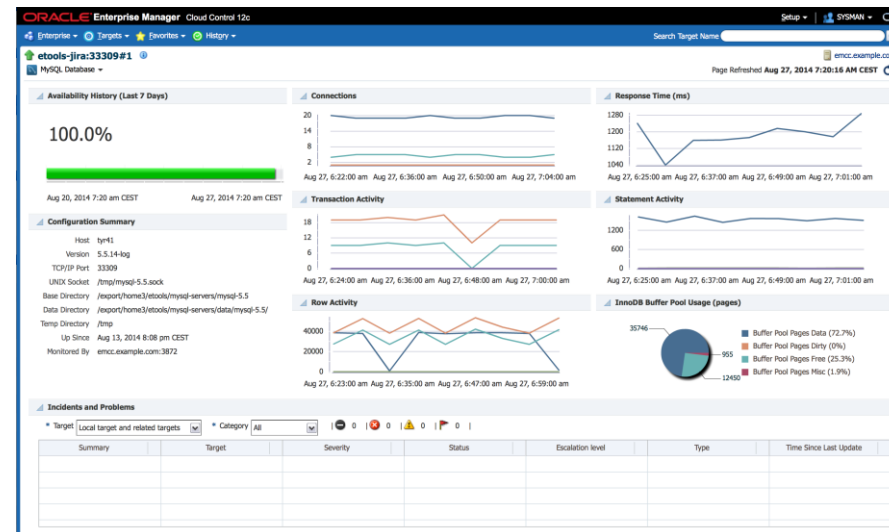
NEW

Webおよびクラウド向けオラクル製品を単一のダッシュボードで管理

- 推計70%のオラクルデータベースのお客様がMySQLを併用
 - Webやカスタムアプリケーション、部門システム、組み込みアプリケーション
 - もっともご要望の多かった製品連携



ORACLE®
ENTERPRISE MANAGER

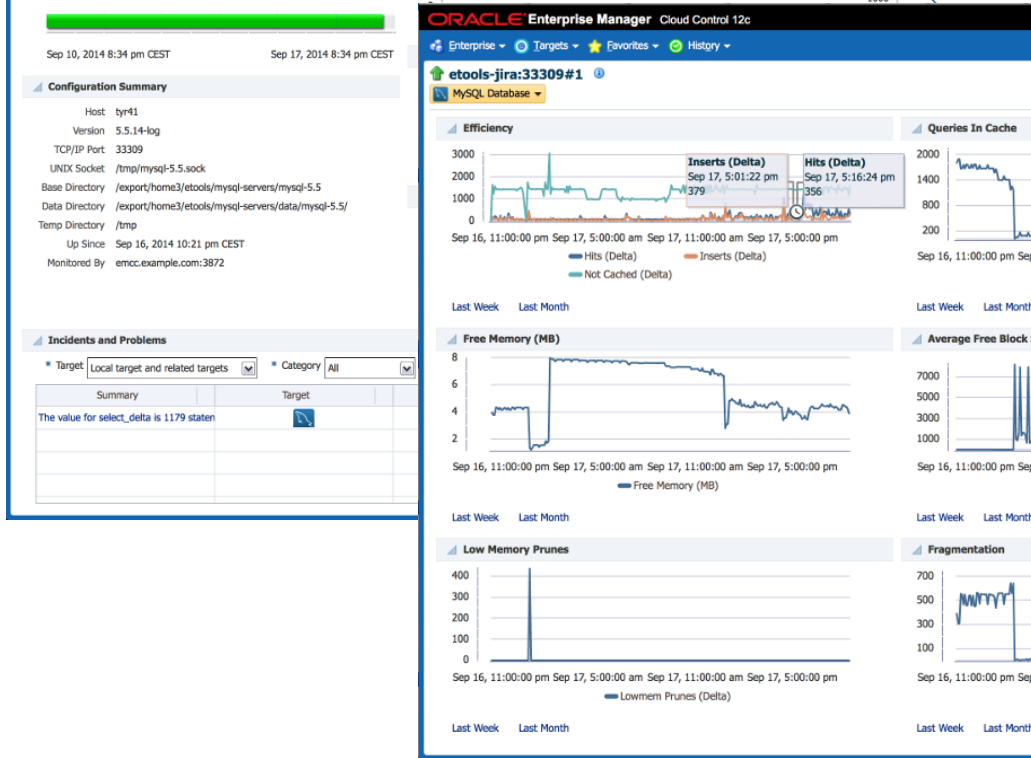
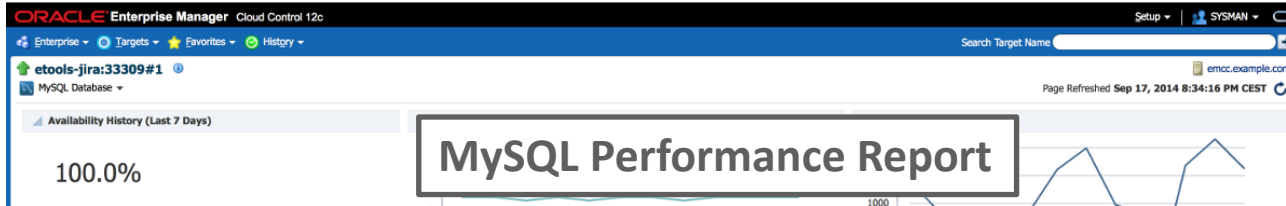


Oracle Enterprise Manager for MySQL概要

機能	概要
可用性のモニタリング	可用性監視と測定によるSLA管理
パフォーマンスモニタリング	パフォーマンス指標とKPI管理
設定のモニタリング	構成収集とオプションの変更履歴管理
アラートと通知	SMTP、SNMP、OS コマンド、スクリプト
全ての使用可能なメトリックを収集	500以上の指標を収集
レポート	時系列グラフを含むパフォーマンスレポート
MySQLの自動検知	プラグインはリモート監視をサポートするため、各サーバーへのOracle Management Agent のインストールは不要

参照: [Oracle Enterprise Manager for MySQL](#)

MySQL Performance Monitoring



Metrics & Collection Settings

Metric and Collection Settings

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
etools-jira:33309#1						
Connection Activity						
Aborted Clients (Delta)	>	10	50	None	Every 5 Minutes	Edit
Aborted Connects (Delta)	>	1	5	None	Every 5 Minutes	Edit
DML Statement Activity						
Select (Delta)	>	300	500	None	Every 5 Minutes	Edit
Query Cache Activity						
Lowmem Prunes (Delta)	>	1200		None	Every 5 Minutes	Edit
Replication Slave Activity						
Seconds Behind Master	>	60	600	None	Every 5 Minutes	Edit
Response						
Status (up/down)	<			Down	Every 1 Minute	Edit

TIP Empty Thresholds will disable alerts for that metric.

Related Links

- Advanced Threshold Management
- Past Apply Operations
- Pending Apply Operations

動画によるデモは、MySQL Enterprise Managerのサイトにて視聴する事が可能です。

[Oracle Enterprise Manager for MySQL](#)

MySQLによるコンプライアンス対応

企業コンプライアンス

企業コンプライアンス（きぎょうコンプライアンス、corporation compliance）とは、コーポレートガバナンスの基本原理の一つで、企業が法律や内規などのごく基本的なルールに従って活動すること。**ビジネスコンプライアンス**という場合もある。「コンプライアンス」は「企業が法律に従うこと」に限られない「遵守」「応諾」「従順」などを意味する。

PCIデータセキュリティスタンダード

PCIデータセキュリティスタンダード（PCI DSS：Payment Card Industry Data Security Standard）は、クレジットカード情報および取引情報を保護するために2004年12月、JCB・American Express・Discover・マスターカード・VISAの国際ペイメントブランド5社が共同で策定した、クレジットカード業界におけるグローバルセキュリティ基準である。2010年10月28日に改訂版であるV2.0が発表された。このバージョンは2011年11月1日発効となる。これに伴いV1.2は2011年10月31日に失効した。

コーポレート・ガバナンス（英：corporate governance）とは、企業の不正行為の防止と競争力・収益力の向上を総合的にとらえ、長期的な企業価値の増大に向けた企業経営の仕組み^[1]。

企業統治（きぎょうとうち）とも訳される。

首脳部で決定された方策をいかに実行するかはマネジメント（運営）、その運営状況をいかに管理・監督するかは内部統制（内部管理・監督、Internal control）、さらに企業のシステムが健全に機能しているかを審査するのは監査（内部監査と外部監査に別れる）という。

参照： Wikipedia

データベースアカウント管理

PCI DSS Requirements v3.0	Milestone	Status <i>Please enter "yes" if fully compliant with the requirement</i>	If status is "N/A", please explain why requirement is Not Applicable
Requirement 8: Assign a unique ID to each person with computer access			
8.1 Define and implement policies and procedures to ensure proper user identification management for nonconsumer users and administrators on all system components as follows:			
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	4		
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	4		
8.1.3 Immediately revoke access for any terminated users.	4		
8.1.4 Remove/disable inactive user accounts at least every 90 days.	4		
8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	4		
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	4		

参照: Prioritized_Approach_v3

MySQLにおけるUNIQUE IDの付与

PCIDSS 8

ユーザー名とパスワードのみを使用してユーザーを認証する他のほとんどのデータベースとは異なり、MySQLでは、ユーザーを認証する際に、追加のlocationパラメータを使用します。このlocationパラメータは、通常、ホスト名、IPアドレスまたはワイルドカード(%)です。MySQLでは、この追加のパラメータを使用して、データベースへのユーザー・アクセスをドメイン内の特定のホストに制限する場合があります。また、これによって、接続元のホストに応じて、ユーザーに異なるパスワードと一連の権限を適用できます。

```
root@localhost [mysql]>select user,host,password from mysql.user;
```

user	host	password
root	localhost	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35
root	centos01	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35
GTID_SSL_USER	192.168.56.%	*84AE91CE95DAA59A02F658041290FEECF1BEE392
admin	%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35
root	192.168.56.%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35
audited_user	192.168.56.0/255.255.255.0	*CED32AC7E202DBC0858C9E8935348E7ED3E083D4
GTID_USER	192.168.56.%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35
sec_password	192.168.56.%	*6FDB5274DE9FC54EDC81BD5909DEBE93CF739D48

8 rows in set (0.00 sec)

User Account

アクセス元 Host / IP

不要なアカウントの削除

～MySQL 5.6x

[Drop the Extra Roots] root@localhost [mysql]>DROP USER root@'127.0.0.1', root@':::1';

```
root@localhost [mysql]>SELECT user,host,plugin,password,password_expired FROM mysql.user;
```

user	host	plugin	password	password_expired
root	localhost		*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	centos01		*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	127.0.0.1			N
root	:::1			N
admin	%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	192.168.56.%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
audited_user	192.168.56.0/255.255.255.0	mysql_native_password	*CED32AC7E202DBC0858C9E8935348E7ED3E083D4	N
GTID_USER	192.168.56.%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N

8 rows in set (0.00 sec)

```
root@localhost [mysql]>DROP USER root@'127.0.0.1', root@':::1';  
Query OK, 0 rows affected (0.01 sec)
```

```
root@localhost [mysql]>SELECT user,host,plugin,password,password_expired FROM mysql.user;
```

user	host	plugin	password	password_expired
root	localhost		*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	centos01		*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
admin	%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	192.168.56.%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
audited_user	192.168.56.0/255.255.255.0	mysql_native_password	*CED32AC7E202DBC0858C9E8935348E7ED3E083D4	N
GTID_USER	192.168.56.%	mysql_native_password	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N

6 rows in set (0.00 sec)

不要なアカウントの削除

mysql_secure_installationを利用した不要アカウント削除

- 1) ルートアカウントのパスワードを設定することができます。
- 2) ローカルホスト以外からアクセス可能なルート・アカウントを削除する事が出来ます。
- 3) 匿名のユーザーアカウントを削除することができます。
- 4) testデータベースを削除する事が出来ます。(Defaultで全てのユーザーがアクセス可能)

```
[root@Centos03 mysql]# ./bin/mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MySQL to secure it, we'll need the current  
password for the root user. If you've just installed MySQL, and  
you haven't set the root password yet, the password will be blank,  
so you should just press enter here.
```

```
Enter current password for root (enter for none):  
OK, successfully used password, moving on...
```

```
Setting the root password ensures that nobody can log into the MySQL  
root user without the proper authorisation.
```

```
Set root password? [Y/n] Y  
New password:  
Re-enter new password:  
Password updated successfully!  
Reloading privilege tables..  
... Success!
```

```
By default, a MySQL installation has an anonymous user, allowing anyone  
to log into MySQL without having to have a user account created for  
them. This is intended only for testing, and to make the installation  
go a bit smoother. You should remove them before moving into a  
production environment.
```

```
Remove anonymous users? [Y/n] Y  
... Success!
```

```
Set root password? [Y/n] Y
```

```
Remove anonymous users? [Y/n] Y
```

```
Disallow root login remotely? [Y/n] Y
```

```
Remove test database and access to it? [Y/n] Y
```

```
Reload privilege tables now? [Y/n] Y
```

```
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| mysql |  
| performance_schema |  
+-----+  
3 rows in set (0.00 sec)
```

```
mysql> select user,host,password from mysql.user;  
+-----+-----+-----+  
| user | host | password |  
+-----+-----+-----+  
| root | localhost | *A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35 |  
| root | 127.0.0.1 | *A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35 |  
| root | ::1 | *A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35 |  
+-----+-----+-----+  
3 rows in set (0.00 sec)
```

参照: [4.4.5 mysql_secure_installation](#)

Automatic Password Expiration

Since: MySQL 5.6.6~

PCIDSS 8.2.6

```
root@localhost [mysql]>ALTER USER 'sec_password'@'192.168.56.%' PASSWORD EXPIRE;
```

```
root@localhost [mysql]>select user,host,password,password_expired from user;
```

user	host	password	password_expired
root	localhost	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	centos01	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
admin	%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
root	192.168.56.%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
audited_user	192.168.56.0/255.255.255.0	*CED32AC7E202DBC0858C9E8935348E7ED3E083D4	N
GTID_USER	192.168.56.%	*A41ECFBE1191DDE4713F2B6F5A6CD5D0D0D5DC35	N
sec_password	192.168.56.%	*BEA2508E06B227E173EAA0F221C2C838C7545E41	Y

7 rows in set (0.00 sec)

```
[admin@CentOS02 ~]$ mysql -h 192.168.56.101 -u sec_password -p
```

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 8

Server version: 5.6.21-enterprise-commercial-advanced-log

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their

owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
sec_password@192.168.56.101 [(none)]> use mysql
```

```
ERROR 1820 (HY000): You must SET PASSWORD before executing this statement
```

```
sec_password@192.168.56.101 [(none)]>
```

MySQL 5.6 introduces password-expiration capability, to enable database administrators to expire account passwords and **require users to reset their password.**

```
SET PASSWORD FOR sec_password@"192.168.56.%"=PASSWORD('Password_2014-');
```

Automatic Password Expiration

Since: MySQL5.7~

PCIDSS 8.1.4, 8.2.4

ssl_cipher	blob	NO		NULL	
x509_issuer	blob	NO		NULL	
x509_subject	blob	NO		NULL	
max_questions	int(11) unsigned	NO		0	
max_updates	int(11) unsigned	NO		0	
max_connections	int(11) unsigned	NO		0	
max_user_connections	int(11) unsigned	NO		0	
plugin	char(64)	NO		mysql_native_password	
authentication_string	text	YES		NULL	
password_expired	enum('N','Y')	NO		N	
password_last_changed	timestamp	YES		NULL	
password_lifetime	smallint(5) unsigned	YES		NULL	

45 rows in set (0.00 sec)

root@localhost [mysql]>

Alter_routine_priv	enum('N','Y')	NO		N	
Create_user_priv	enum('N','Y')	NO		N	
Event_priv	enum('N','Y')				
Trigger_priv	enum('N','Y')				
Create_tablespace_priv	enum('N','Y')				
ssl_type	enum('', 'ANY', 'X509', 'SPR				
ssl_cipher	blob				
x509_issuer	blob				
x509_subject	blob				
max_questions	int(11) unsigned				
max_updates	int(11) unsigned				
max_connections	int(11) unsigned				
max_user_connections	int(11) unsigned				
plugin	char(64)				
authentication_string	text				
password_expired	enum('N','Y')				

43 rows in set (0.00 sec)

Two columns are added

password_last_changed

password_lifetime

[Global Configuration]

SET GLOBAL default_password_lifetime = 180;

[Individual user accounts]

ALTER USER joro@localhost PASSWORD EXPIRE INTERVAL 90 DAY;

ALTER USER joro@localhost PASSWORD EXPIRE DEFAULT;

ALTER USER joro@localhost PASSWORD EXPIRE NEVER;

参考 : 6.3.6 Password Expiration Policy

Account Management (The Password Validation)

Since: MySQL 5.6.6～

PCIDSS 8.2.3

```
root@localhost [mysql]>SHOW VARIABLES LIKE 'validate_password%';
```

Variable_name	Value
validate_password_dictionary_file	/usr/local/mysql/data/band_dictionary.txt
validate_password_length	8
validate_password_mixed_case_count	1
validate_password_number_count	1
validate_password_policy	STRONG
validate_password_special_char_count	1

パスワードは、7文字以上、英数を含む必要がある。

```
6 rows in set (0.00 sec)
```

8文字以下、小文字のみ、数字未入力、辞書に登録済みの文字はパスワードとしては不適切な為、ERROR 1819で拒否される。

```
root@localhost [mysql]>
```

```
plugin-load=validate_password.so
```

```
validate-password=FORCE_PLUS_PERMANENT
```

```
validate_password_policy=2
```

```
validate_password_dictionary_file=/usr/local/mysql/data/band_dictionary.txt
```

```
[admin@CentOS01 ~]$ perror 1819;
```

```
MySQL error code 1819 (ER_NOT_VALID_PASSWORD): Your password does not satisfy the current policy requirements
```

```
[admin@CentOS01 ~]$
```

ホストアクセスブロック

PCIDSS 8.1.6, 8.1.7

```
root@localhost [performance_schema]>desc host_cache;
```

Field	Type	Null	Key	Default
IP	varchar(64)	NO		NULL
HOST	varchar(255)	YES		NULL
HOST_VALIDATED	enum('YES','NO')	NO		NULL
SUM_CONNECT_ERRORS	bigint(20)	NO		NULL
COUNT_HOST_BLOCKED_ERRORS	bigint(20)	NO		NULL
COUNT_NAMEINFO_TRANSIENT_ERRORS	bigint(20)	NO		NULL
COUNT_NAMEINFO_PERMANENT_ERRORS	bigint(20)	NO		NULL
COUNT_FORMAT_ERRORS	bigint(20)	NO		NULL
COUNT_ADDRINFO_TRANSIENT_ERRORS	bigint(20)	NO		NULL
COUNT_ADDRINFO_PERMANENT_ERRORS	bigint(20)	NO		NULL
COUNT_FCRDNS_ERRORS	bigint(20)	NO		NULL
COUNT_HOST_ACL_ERRORS	bigint(20)	NO		NULL
COUNT_NO_AUTH_PLUGIN_ERRORS	bigint(20)	NO		NULL
COUNT_AUTH_PLUGIN_ERRORS	bigint(20)	NO		NULL
COUNT_HANDSHAKE_ERRORS	bigint(20)	NO		NULL
COUNT_PROXY_USER_ERRORS	bigint(20)	NO		NULL
COUNT_PROXY_USER_ACL_ERRORS	bigint(20)	NO		NULL
COUNT_AUTHENTICATION_ERRORS	bigint(20)	NO		NULL
COUNT_SSL_ERRORS	bigint(20)	NO		NULL
COUNT_MAX_USER_CONNECTIONS_ERRORS	bigint(20)	NO		NULL
COUNT_MAX_USER_CONNECTIONS_PER_HOUR_ERRORS	bigint(20)	NO		NULL
COUNT_DEFAULT_DATABASE_ERRORS	bigint(20)	NO		NULL
COUNT_INIT_CONNECT_ERRORS	bigint(20)	NO		NULL
COUNT_LOCAL_ERRORS	bigint(20)	NO		NULL
COUNT_UNKNOWN_ERRORS	bigint(20)	NO		NULL
FIRST_SEEN	timestamp	NO		NULL
LAST_SEEN	timestamp	NO		NULL
FIRST_ERROR_SEEN	timestamp	NO		NULL
LAST_ERROR_SEEN	timestamp	NO		NULL

29 rows in set (0.00 sec)

```
root@localhost [performance_schema]>select @@global.max_connect_errors;
```

```
-----+-----+
| @@global.max_connect_errors |
+-----+-----+
```

100

1 row in set (0.00 sec)

The default is 100 as of MySQL 5.6.6, 10 before that.

- ※ skip_name_resolveが設定されている場合は有効にならない。
- ※ Unlock: は、[FLUSH HOSTS](#) か [mysqladmin flush-hosts](#) コマンドにて実行
- ※ [FLUSH HOSTS](#) and [TRUNCATE TABLE host_cache](#) は同じ結果になります。
- ※ 基本的にはローカルネットワークアクセスコントロール用途

Public Networkにデータを送受信する場合の暗号化

PCI DSS Requirements v3.0	Milestone	Status <i>Please enter "yes" if fully compliant with the requirement</i>	If status is "N/A", please explain why requirement is Not Applicable
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS). • Satellite communications	2		
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control is prohibited.	2		

参照: Prioritized_Approach_v3

SSL による通信の暗号化

PCIDSS 4.1

```
[admin@CentOS02 ~]$ mysql -h 192.168.56.101 -u admin -p --ssl-ca=/usr/local/mysql/ssl/sql-ssl-cert.pem
```

Enter password:

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 20

Server version: 5.6.21-enterprise-commercial-advanced-log MySQL Enterprise

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
admin@192.168.56.101 [(none)]> show status like 'SSL_version';
```

Variable_name	Value
Ssl_version	TLSv1

```
root@localhost [(none)]> SHOW VARIABLES LIKE '%ssl%';
```

Variable_name	Value
have_openssl	YES
have_ssl	YES
ssl_ca	/usr/local/mysql/ssl/sql-ssl-cert.pem
ssl_capath	
ssl_cert	/usr/local/mysql/ssl/sql-gtid-cert.pem
ssl_cipher	
ssl_cr1	
ssl_cr1path	
ssl_key	/usr/local/mysql/ssl/sql-ssl-repl-key.pem

MySQL 5.0.10 is bundled with yaSSL for enabling SSL.
MySQL 5.6.6, SSL support is included by default

```
GTID_SSL_USER@192.168.56.101 [(none)]> show status like 'ssl_cipher';
```

Variable_name	Value
Ssl_cipher	DHE-RSA-AES256-SHA

1 row in set (0.00 sec)

オンプレミスとパブリッククラウド間でデータベース操作やレプリケーションなどをSSLを使い安全に行う事が可能。



MySQL Enterprise Security

- SSLに対応した通信
- アクセスコントロール
 - 外部認証方式へのアクセス
 - 標準認証インタフェース対応 (Unix、LDAP、Kerberosなど)
 - プロキシ／非プロキシユーザー
- 監査と監視
 - MySQLのセキュリティアドバイザ
 - Oracle Audit Vaultとの互換性 (ログフォーマット)
- Oracle Database FirewallによるFirewallサポートも可能

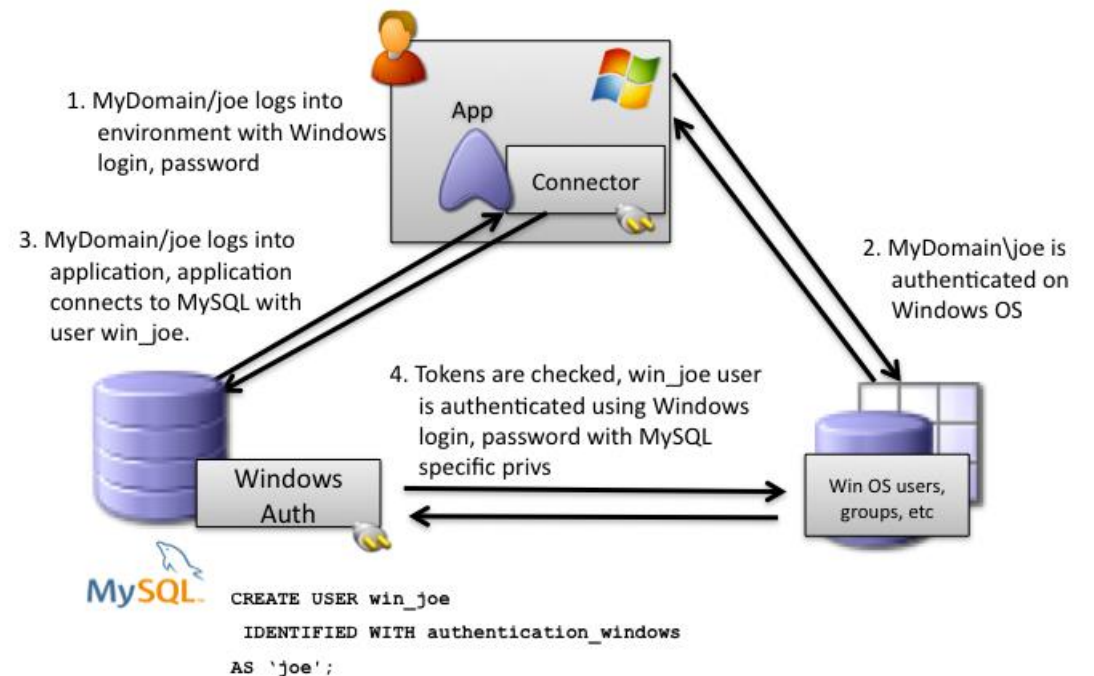


MySQL Enterprise Authentication

EE

外部認証のサポート

- PAM (Pluggable Authentication Modules)
 - 外部認証方式へのアクセス
 - 標準のインタフェース (Unix, LDAP, Kerberosなど)
 - プロキシ/非プロキシユーザー
- Windows
 - ネイティブWindowsサービス (WAD) へのアクセス
 - Windowsにログイン済みユーザを認証
- プラガブル認証API



MySQLアプリケーションを既存のセキュリティ・インフラストラクチャ/SOPと統合

データに対するアクセスを追跡と監視

PCI DSS Requirements v3.0	Milestone	Status <i>Please enter "yes" if fully compliant with the requirement</i>	If status is "N/A", please explain why requirement is Not Applicable
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	5		
Requirement 10: Track and monitor all access to network resources and cardholder data			
10.1 Implement audit trails to link all access to system components to each individual user.	4		
10.2 Implement automated audit trails for all system components to reconstruct the following events.			
10.2.1 All individual user accesses to cardholder data.	4		
10.2.2 All actions taken by any individual with root or administrative privileges.	4		
10.2.3 Access to all audit trails.	4		
10.2.4 Invalid logical access attempts.	4		

参照: Prioritized_Approach_v3

MySQL Enterprise Audit

ポリシーベースの監査機能を提供

- ログオン、クエリーの情報監査可能
- ユーザがポリシーを設定可能: フィルタリング、ログローテーション
- 動的に設定を変更可能: Audit設定時にサーバの再起動が不要
- Oracleの仕様に合わせXMLベースの監査ログを出力
- サイズに基づいた監査ログファイルの自動ローテーション
- XML ベースの監査ログストリーム
- MySQL 5.5のAudit APIを使って実装 / MySQL 5.5.28 以上で使用可能

コンプライアンス対応等で監査が必要なアプリケーションでもMySQLを利用可能

MySQL Enterprise Audit

PCIDSS 10

EE

管理者



```
mysql> INSTALL PLUGIN audit_log SONAME 'audit_log.so';
```

```
mysql> SHOW VARIABLES LIKE 'audit_log%';
```

Variable_name	Value
audit_log_buffer_size	1048576
audit_log_file	audit.log
audit_log_flush	OFF
audit_log_policy	ALL
audit_log_rotate_on_size	1044480
audit_log_strategy	SYNCHRONOUS

1. DBA enables Audit plugin

Joe (ユーザー)



```
shell> mysql -h joeshost -u joe -p  
Enter password: *****
```

```
mysql> SELECT * FROM joes_table;
```

FIRST_NAME	LAST_NAME
Joe	User

2. User Joe connects and runs a query



3. Joe's connection & query logged

```
<?xml version="1.0" encoding="UTF-8"?>  
<AUDIT>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:52:12"  
    NAME="Audit"  
    SERVER_ID="1"  
    VERSION="1"  
    STARTUP_OPTIONS="--port=3306"  
    OS_VERSION="i686-Linux"  
    MYSQL_VERSION="5.5.28-debug-log"/>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:52:41"  
    NAME="Connect"  
    CONNECTION_ID="1"  
    STATUS="0"  
    USER="joe"  
    PRIV_USER="root"  
    OS_LOGIN=""  
    PROXY_USER=""  
    HOST="SERVER1"  
    IP="127.0.0.1"  
    DB="joes_db"/>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:53:45"  
    NAME="Query"  
    CONNECTION_ID="1"  
    STATUS="0"  
    SQLTEXT="SELECT * FROM joes_table;"/>  
</AUDIT>
```

WHO

WHERE

WHEN

WHAT

Audit Log Filtering

What's new in Security Tools ?

- Event filtering by account name
 - **SET GLOBAL audit_log_include_accounts='root@localhost';**
 - **SET GLOBAL audit_log_exclude_accounts='secure@localhost';**
- Event filtering by status
 - **SET GLOBAL audit_log_statement_policy=ALL;**
 - **SET GLOBAL audit_log_connection_policy=ERRORS;**
- Better instrumentation and statistics
 - **SHOW STATUS LIKE 'Audit_log_events_filtered';**

会員データを安全に保護

PCI DSS Requirements v3.0	Milestone	Status <i>Please enter "yes" if fully compliant with the requirement</i>	If status is "N/A", please explain why requirement is Not Applicable
Requirement 3: Protect stored cardholder data			
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention.	1		
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data irretrievable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	1		

参照: Prioritized_Approach_v3

MySQLの機能を利用した暗号化(共通鍵暗号)

Since: MySQL 4.0.2~

PCIDSS 3

```
root@localhost > select (HEX(AES_ENCRYPT("AES暗号化-個人情報01", 'password')))) into @AES_ENC;
Query OK, 1 row affected (0.00 sec)

root@localhost > select @AES_ENC;
+-----+
| @AES_ENC |
+-----+
| D8F991170C3468696E4D963AE4A8E2A1D6404D7066F30A5D0419C0EC80D0602B |
+-----+
1 row in set (0.00 sec)

root@localhost > select AES_DECRYPT(UNHEX(@AES_ENC), 'password');
+-----+
| AES_DECRYPT(UNHEX(@AES_ENC), "password") |
+-----+
| AES暗号化-個人情報01 |
+-----+
1 row in set (0.00 sec)

root@localhost >
```

AES_ENCRYPT(str,key_str),
AES_DECRYPT(crypt_str,key_str)が
MySQL標準で使用方法が可能なものの中で、
暗号的に最も安全な暗号化関数でした。

標準128ビットのキーの長さを使用したエンコード
暗号化・復号化文字列は共に同じものを利用

AES暗号化は128ビットのキーの長さを使用したエンコードを行いますが、
256ビットまで延長する事が出来ます。

MySQLの機能を利用した暗号化(共通鍵暗号) Since: MySQL 5.6.17~

PCIDSS 3

```
root@localhost > SELECT @@session.block_encryption_mode;
+-----+
| @@session.block_encryption_mode |
+-----+
| aes-128-ecb                      |
+-----+
1 row in set (0.00 sec)

root@localhost > SET block_encryption_mode = 'aes-256-cbc';
Query OK, 0 rows affected (0.00 sec)

root@localhost > SELECT @@session.block_encryption_mode;
+-----+
| @@session.block_encryption_mode |
+-----+
| aes-256-cbc                    |
+-----+
1 row in set (0.00 sec)

root@localhost > SET @key_str = SHA2('password',512);
Query OK, 0 rows affected (0.00 sec)

root@localhost > SELECT @key_str;
+-----+
| @key_str                        |
+-----+
| b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6 |
+-----+
1 row in set (0.00 sec)

root@localhost > SET @init_vector = RANDOM_BYTES(16);
Query OK, 0 rows affected (0.00 sec)

root@localhost > SET @crypt_str = HEX(AES_ENCRYPT("AES暗号化-個人情報01",@key_str,@init_vector));
Query OK, 0 rows affected (0.00 sec)

root@localhost > SELECT @crypt_str;
+-----+
| @crypt_str                      |
+-----+
| 6BFA4275B9167BC976C13CDE295FDF7EADB41DB27C6BD75CFA6F44255422AB28 |
+-----+
1 row in set (0.00 sec)

root@localhost > SELECT AES_DECRYPT(UNHEX(@crypt_str),@key_str,@init_vector);
+-----+
| AES_DECRYPT(UNHEX(@crypt_str),@key_str,@init_vector) |
+-----+
| AES暗号化-個人情報01                                |
+-----+
1 row in set (0.00 sec)

root@localhost >
```

AES_ENCRYPT(str,key_str[,init_vector])
AES_DECRYPT(crypt_str,key_str[,init_vector])

128, 192 or 256 bitの暗号化方法が設定可能
暗号化の必要性和暗号化によるオーバーヘッドにより選択

標準256ビットのキーの長さを使用したエンコード
暗号化・復号化文字列は共に同じものを利用

MySQL Enterprise Encryption

- MySQLの暗号化ライブラリ
 - AES256による対称鍵暗号
 - 公開鍵 / 非対称鍵暗号
- キーの管理
 - 公開鍵および秘密鍵の生成
 - 鍵交換方式: RSA, DSA, DH
- 署名とデータの検証
 - 電子署名、検証、妥当性確認のための暗号学的ハッシュ関数
- Oracle Key Vaultとの統合



Enterprise Encryption Functions

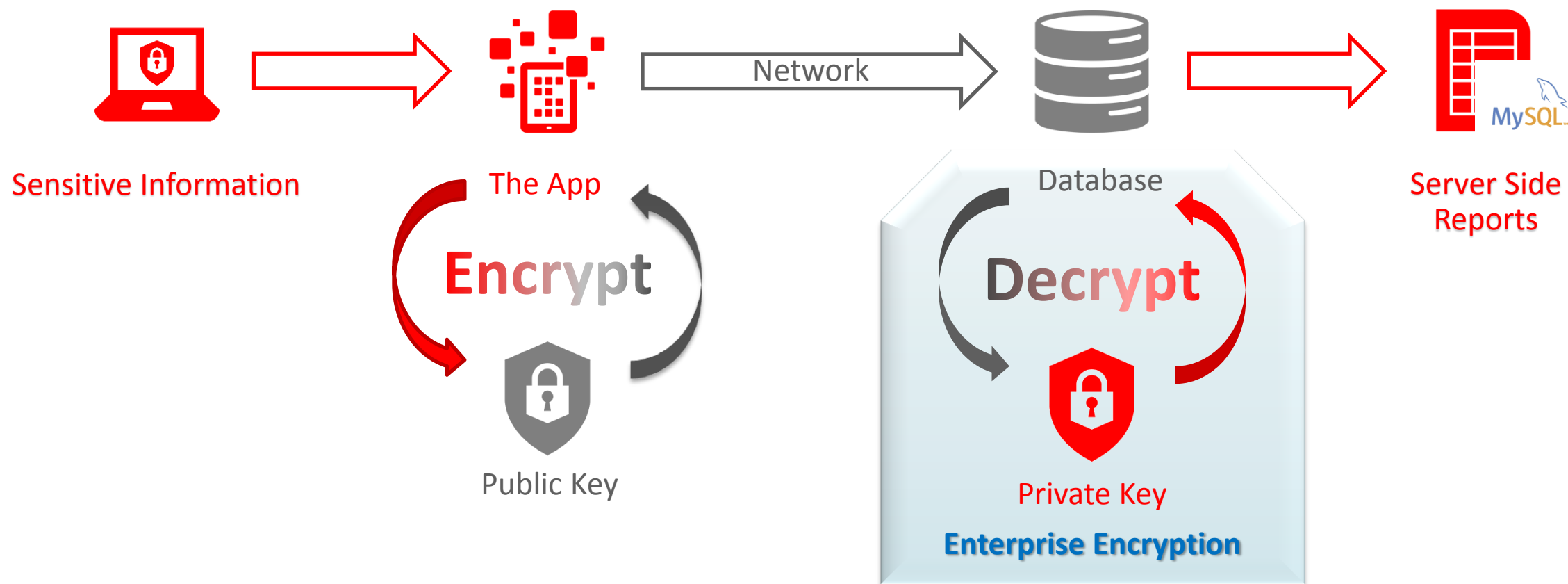
What's new in Security Tools ?

- Interface to the OpenSSL library
- Allow generation and handling of RSA, DSA and DH key pairs
 - SET @priv = CREATE_ASYMMETRIC_PRIV_KEY('RSA', 1024);
 - SET @pub = CREATE_ASYMMETRIC_PUB_KEY('RSA', @priv);
 - SET @digest = CREATE_DIGEST('SHA512', 'cleartext');
 - SET @sig = ASYMMETRIC_ENCRYPT('RSA', @digest, @priv);
- Key generators use standard PEM format (compatible with external tools)

例：機密情報の取り扱い

Handling Sensitive Information

EE



MySQL Enterprise Encryption

PCIDSS 3

非対称暗号: RSA, DSA, and DH 等の暗号化をサポート



```
個人情報管理者>SELECT "=== [RSA] Private and Public鍵の作成===" as STEP1;
+-----+
| STEP1 |
+-----+
| === [RSA] Private and Public鍵の作成=== |
+-----+
1 row in set (0.00 sec)

個人情報管理者>CREATE TABLE priv_key SELECT CREATE_ASYMMETRIC_PRIV_KEY('RSA', 1024); /** 管理者用鍵 **/
Query OK, 1 row affected (0.04 sec)
Records: 1 Duplicates: 0 Warnings: 0

個人情報管理者>SELECT * FROM priv_key into @priv_key;
Query OK, 1 row affected (0.01 sec)

個人情報管理者>CREATE TABLE pub_key SELECT CREATE_ASYMMETRIC_PUB_KEY('RSA', @priv_key); /** アプリケーション開発者共有鍵 **/
Query OK, 1 row affected (0.02 sec)
Records: 1 Duplicates: 0 Warnings: 0

個人情報管理者>SELECT * FROM pub_key into @pub_key;
Query OK, 1 row affected (0.00 sec)

個人情報管理者>
```

create_asymmetric_priv_key
ファンクションでPrivate鍵の発行

create_asymmetric_pub_key
ファンクションでPublic鍵の発行

こちらの例では、RSA 1024で暗号化しています

The maximum key length (OpenSSLによる制約)	
RSA	16,384
DSA	10,000
DH	10,000

参照: [12.17.4 Enterprise Encryption Function Descriptions](#)

```
個人情報管理者>SELECT @priv_key\G
*****1..row*****
@priv_key: -----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDX7aUxdyXb0mw2HtBhFyUskdcG/eLbEku6Uz0xux61wMHKRJ+t
OHRyBGSV1tRAYQt0TxXGwbgl1kFpGU6oYT1484EphRURXov4SRAPsa9aC/pq00UC
XsoYPJBBkMYE96hJ5KpTd8Mo5RcVrQK/rJEHNIS8Swpl7drCpLmXHJEdwIDAQAB
AoGAXq9E2vYGuaxCwdCtS4XctTiwc+hsy+b2rSbHFMGa69RESZyt9sVkr0mIqfP0
Su7DGRN81xUnc8gZkr6YmVnA2yxjLrDdoy7rVwQTMLE0e3DVxHU5Xwefbczo9R65
b0t+YUJrLL5Ywys3/Y1yh767gmEoLD1VYoHZDhF51PBudHECQD314h62kkwNx+P
0i4foKkw+oAcM3rARpyzZKvVsyRy3ZZY1K1judHzEwBakkGntY6CqfahWmTseAKk
VlQ51AXjAkeA30LXT50ad/ire0cJ2cHBoGRC4+uh8U0TxYrfWpfz6YbwaOF34qPv
Pcz5ve84aYE3QxwWUjE6Fm0bYCD4T8UrXQJAS1SA0bkUvdferTo/qxkVkjgyIkVG
NdE9HBI8JFRfxehGSbbxsxfHMv1iVwBRm6LC/PE/rKMxp1hEGsgcEwkvWJARg3f
KagOkh7pDyLpWg/nWlyZYNQHGIIQ9A1DUFx1vx0MspyU1ZTC+Q1CH07U0KvVb0m9
JUULCNxrfppZ0A36MQJBAKnhG++Swwx20TsBAz8TpYE8sES0QyPevHD/XY7Wisce
cGE7x28G0QMoNXf1mtqUT//kGGpLdkTpzjhe/tq3as=
-----END RSA PRIVATE KEY-----

1 row in set (0.00 sec)

個人情報管理者>SELECT @pub_key\G
*****1..row*****
@pub_key: -----BEGIN RSA PUBLIC KEY-----
MIGJAoGBANftptF3jds6bDYe0GEXJ5yR1wb94tsQpTpTPTG7HrXAweREn604dFhs
ZJXw1EBhc3RPFcbBuDwwQwkZTqhhOXjzgSkdFstc6/hJEA+xr1oL+mo7RQJeyhg8
kEGQxgT3qEmwq1N3wyj1E9y9FAr+skQc0hLxLCkvt2sKkuZccK3AgMBAAE=
-----END RSA PUBLIC KEY-----
```



MySQL Enterprise Encryption

EE

MySQL Enterprise Encryption は非対称暗号化(公開鍵暗号)の業界標準機能を提供
機密データの保護や HIPAA, SOX 法, PCI DSSなどの規制要件の遵守に役立てる事が可能。

```
開発チーム>CREATE TABLE enc_pub SELECT HEX(ASYMMETRIC_ENCRYPT('RSA','MASAカード オラ次郎 1234-5678-9012-3456 99/99',@pub_key)) as 'Card_Info';
Query OK, 1 row affected (0.07 sec)
Records: 1 Duplicates: 0 Warnings: 0
```

Public鍵による暗号化

```
開発チーム>select * from enc_pub\G
***** 1. row *****
Card_Info: 0ECFEF85397A941293630ECF40FA2345C66783E4C8131357EE06DBFC4939FB0B85B35E67A33E62F1764CA6158210EFC26B16C094BE92E5B7F11E22FE365E77D96239C0
AD1AA7AD0AF5792D10A435C73AC65CE36BA200C5A0568757F0A424AEDC9D032FEA3EC6DCED13A5FF85F57E21818606F01437D94240EC4503BB3932B89
1 row in set (0.00 sec)
```

暗号化されたデータ

```
個人情報管理者>select Card_Info from enc_pub into @enc_pub;
Query OK, 1 row affected (0.00 sec)

個人情報管理者>SELECT ASYMMETRIC_DECRYPT('RSA', UNHEX(@enc_pub),@priv_key);
+-----+
| ASYMMETRIC_DECRYPT('RSA', UNHEX(@enc_pub), @priv_key) |
+-----+
| MASACARD オラ次郎 1234-5678-9012-3456 99/99          |
+-----+
1 row in set (0.01 sec)

個人情報管理者>
```

Public鍵で暗号化したデータを
Private鍵で復号化

Private, Public鍵を分けて管理出来る環境においては、よりセキュアにデータを保護をする事が可能。

[Demo](#)

MySQL Enterprise Encryption

EE

MySQL のバイナリログと REDO ログの暗号化

```
#141017 15:52:24 server id 1 end_log_pos 8089 CRC32 0x9d08bd6b Query thread_id=2 exec_time=0 error_code=0
SET TIMESTAMP=1413528744/*!*/;
insert into test3 select '暗号化の設定が無い場合'
/*!*/;
# at 8089
#141017 15:52:24 server id 1 end_log_pos 8120 CRC32 0xa0d8c34d xid = 129
COMMIT/*!*/;
# at 8120
#141017 15:52:56 server id 1 end_log_pos 8198 CRC32 0xfab9f08c Query thread_id=2 exec_time=0 error_code=0
SET TIMESTAMP=1413528776/*!*/;
BEGIN
/*!*/;
# at 8198
#141017 15:52:56 server id 1 end_log_pos 8253 CRC32 0x7171e109 Table_map: `audit_test`.`test3` mapped to number 79
# at 8253
#141017 15:52:56 server id 1 end_log_pos 8419 CRC32 0xfe7cf4dd Write_rows: table id 79 flags: STMT_END_F

BINLOG '
yLxAVBMBAAAAANwAAAD0gAAAAAE8AAAAAAAEACmF1ZG10X3Rlc3QABXRlc3QzAAH8AQIACeFxcQ==
yLxAVB4BAAAApgAAAOmGAAAAAE8AAAAAAAEAAgAB//6AAH8FLXi1LrE4aKLi38JKD97n+Vs18kb1
ehwIaDZo0LZyj4scdsDj9xU3VteGN5lbZMxfKkCIekc7kVEgAf8f51rVdY/b9m74+x+Z0b4y03JG
/pv5OX5RwI5LhSAT93xV8K3DcpuenD8VntAvDAK4ymARbYlQanWnj+12dVZ9Mt iC3fR8/g==
'/*!*/;
```

暗号鍵を利用してDML処理したデータはバイナリログ上で暗号化されています。

```
個人情報管理者>>insert into test3 select '暗号化の設定が無い場合';
Query OK, 1 row affected (0.02 sec)
Records: 1 Duplicates: 0 Warnings: 0
```

```
個人情報管理者>>insert into test3 SELECT ASYMMETRIC_ENCRYPT('RSA','プライベート鍵にて暗号化しています', @priv_key);
Query OK, 1 row affected (0.02 sec)
Records: 1 Duplicates: 0 Warnings: 0
```

```
個人情報管理者>>
```

Get Started Today!

MySQL Enterprise Edition Trial



30日間トライアル

Oracle Software Delivery Cloud

<http://edelivery.oracle.com/>

製品パックを選択: “MySQL Database”

製品マニュアル: <http://dev.mysql.com/doc/index-enterprise.html>

事例紹介: <http://www.mysql.com/why-mysql/case-studies/#ja-5-0>

Contact a MySQL Sales Rep



[MySQL お問い合わせ窓口]

電話: 0120-065556

【受付時間】平日 9:00-12:00/13:00-18:00

(祝日及び年末年始休業日を除きます)

メール: MySQL-Sales_jp_grp@oracle.com

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

ORACLE®