



如何打造固若金汤的MySQL

马楚成 (Ivan Ma)

2017-10-24

安全港声明

以下内容旨在阐明产品的整体方向。

该内容仅供参考，不可纳入任何合同。该信息不承诺提供任何资料、代码或功能，并且不应该作为制定购买决策的依据。

本文档所述的 Oracle 产品的任何特性或功能的开发、发行和时间规划均由 Oracle 自行决定。

「数据即资产」成为最核心的产业趋势和思维方式

- 数据就是资产

- 要管理好，要完整，一致，方便使用，但一定要**安全**。

- 数据丢失，数据损坏，资料被盗，数据泄露

- 导致一损失

- 收入下降，

- 数据恢复成本

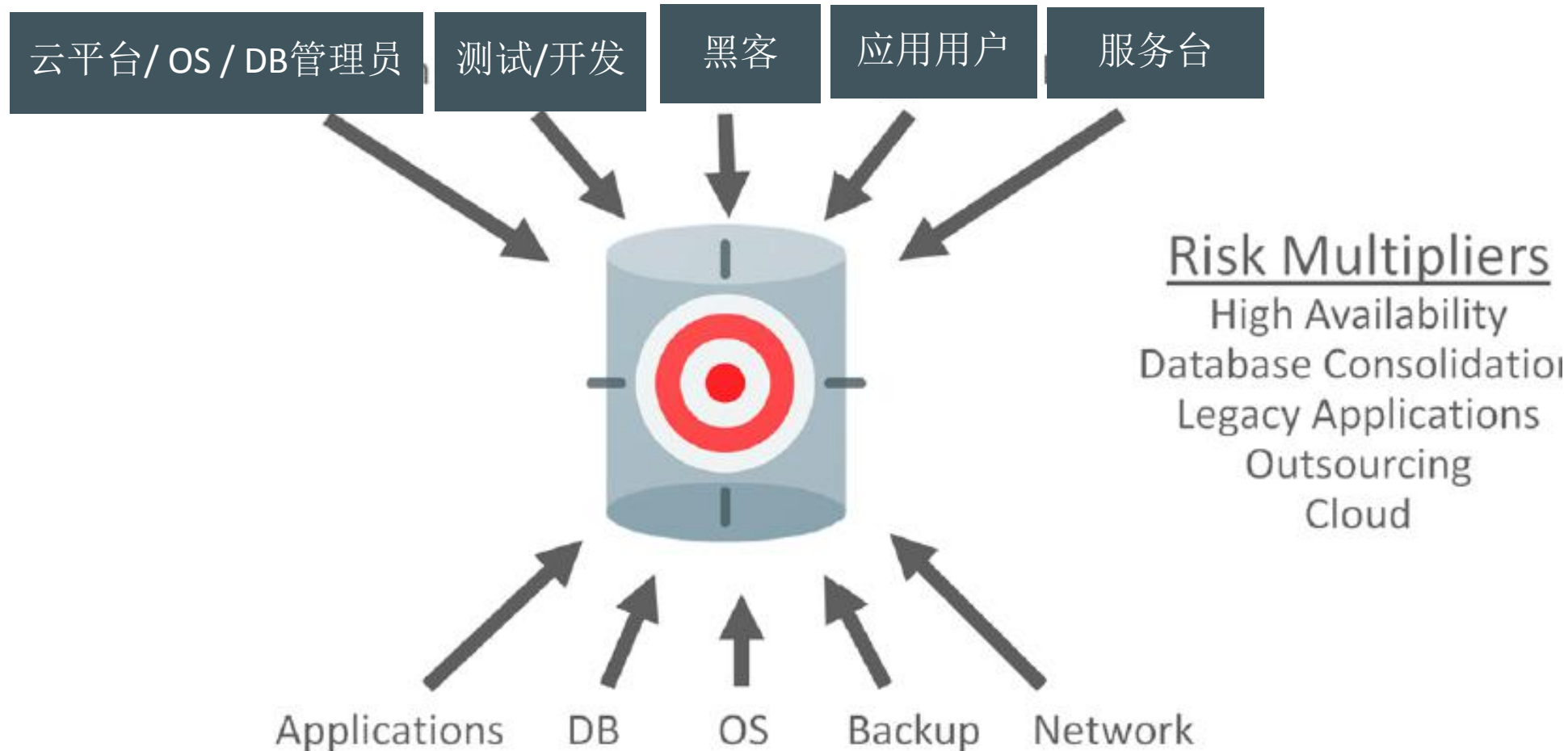
- 损害他人和补偿，

- 客户不信任，

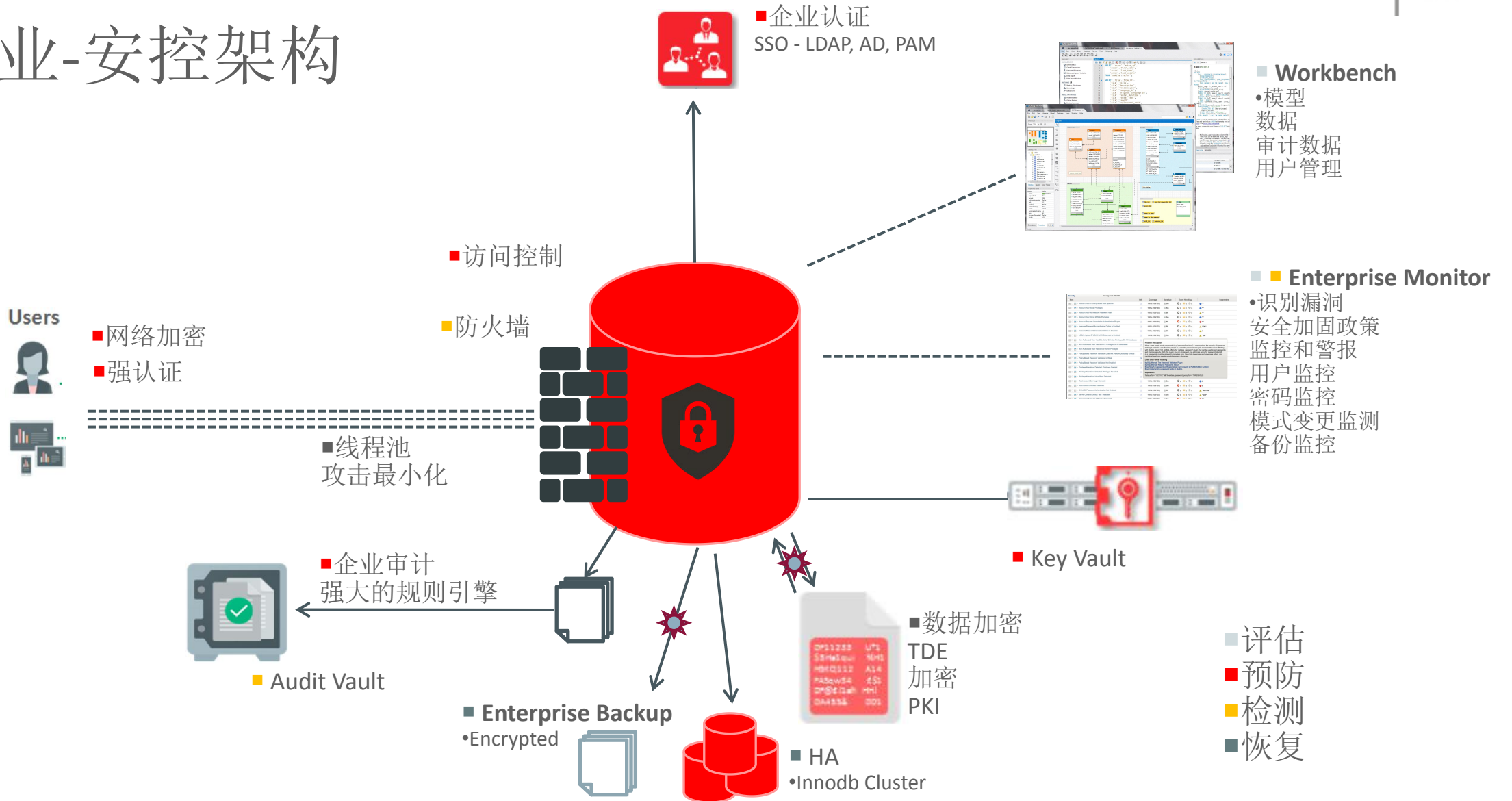
- 监管审核，公司操作 **STOP!**



复杂 / 风险 越来越高



企业-安控架构



数据安全

- 评估 – MySQL Enterprise Monitor, WorkBench
 - 保护数据的预防措施 Prevent
 - 网络传输加密 – SSL 连接
 - 数据存储加密 - TDE (透明数据加密)
 - 利用防火墙避免攻击 – MySQL Enterprise Firewall
 - 多份数据, 做好备份 / 恢复准备 – 数据复制, 备份/恢复
 - 数据库的安全功能 (权限, 认证, 密码, SSL, . . .)
 - 检测和恢复 Detect & Recover
 - 数据审计
 - 检查和警报 / 通知 – MySQL Enterprise Monitor
 - 锁住帐户 – Account Locking
- ORACLE 数据恢复 – Data Recovery

安全配置小提示

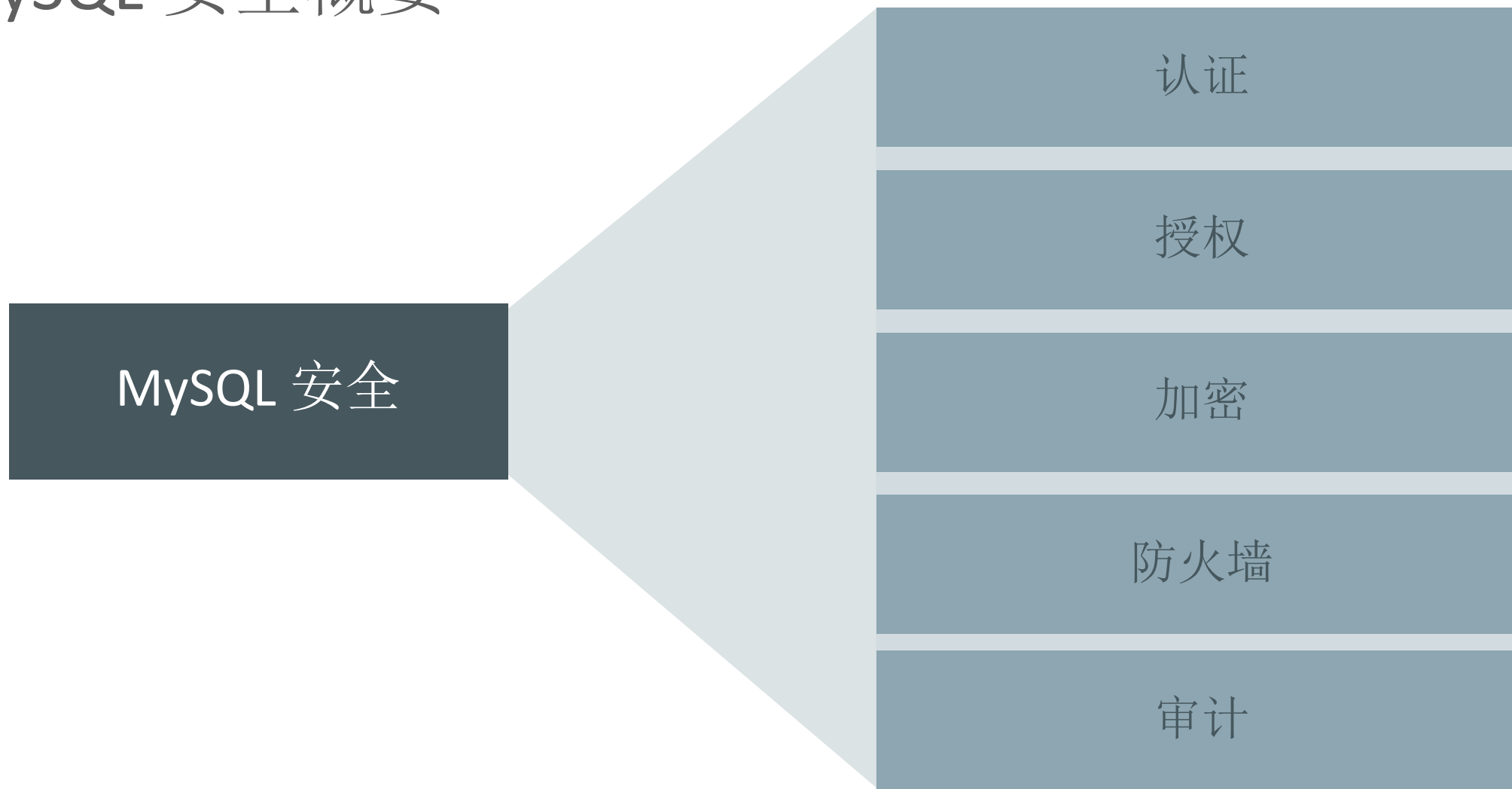
- root password –
 - MySQL 5.6（以前）→ 默认没有密码
 - MySQL 5.7 - 默认是有密码
- 可以改‘root’@‘localhost’的用户名

```
mysql> rename user root@'localhost' to 'myroot'@'localhost';  
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> select user,host from mysql.user;  
+-----+-----+  
| user      | host      |  
+-----+-----+  
| myuser    | %         |  
| myroot    | localhost |  
| mysql.session | localhost |  
| mysql.sys  | localhost |  
+-----+-----+  
4 rows in set (0.01 sec)
```

- 禁用或限制远程访问
 - skip-networking
 - bind-address=127.0.0.1
 - mysql> GRANT SELECT, INSERT ON mydb.* TO 'someuser'@'somehost';

MySQL 安全概要



MySQL 认证

- 内置认证
 - `mysql.user` 表记录用户和加密的密码
- MySQL Native, SHA 256 密码插件
 - `native` 使用 SHA1 或 SHA-256 插件通过散列为每个用户生成密码
- MySQL Enterprise Authentication
 - Microsoft Active Directory
 - Linux PAMs (Pluggable Authentication Modules)
 - 支持 LDAP 等等
- X.509
 - 服务器认证客户端证书

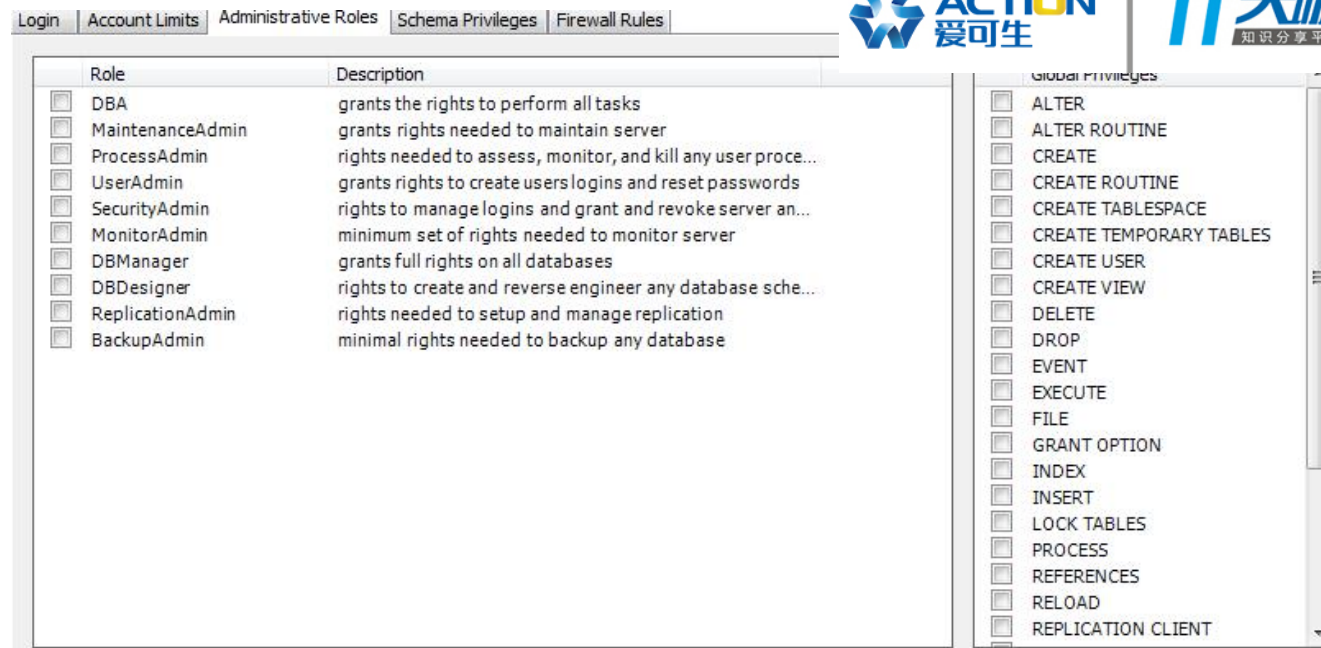
```

+-----+-----+-----+
| user      | plugin                | authentication_string |
+-----+-----+-----+
| root      | mysql_native_password | *1E97552497867D450D5C30F3441CD95BADF54751 |
| myproxy1  | mysql_no_login        | |
| root      | mysql_native_password | *1E97552497867D450D5C30F3441CD95BADF54751 |
| sha256user | sha256_password      | $5$R3yx~yCNF0d[N=gd$5P13/oobZ.iyx0QehsyRK.UIXo1hQX6mlJR8mBG/m89 |
+-----+-----+-----+
4 rows in set (0.00 sec)

```

MySQL权限

- 管理权限
- 数据库权限



MySQL 授权

- 管理权限
- 数据库权限
- 会话限制

DETAILS FOR ACCOUNT NEWSUSER@70

Login Account Limits Administrative Roles Schema Privileges Firewall Rules

Max. Queries:	<input type="text" value="0"/>	Number of queries the account can execute within one hour.
Max. Updates:	<input type="text" value="0"/>	Number of updates the account can execute within one hour.
Max. Connections:	<input type="text" value="0"/>	The number of times the account can connect to the server per hour.
Concurrent Connections:	<input type="text" value="0"/>	The number of simultaneous connections to the server the account can have.

```
mysql> CREATE USER 'francis'@'localhost' IDENTIFIED BY 'frank'  
-> WITH MAX_QUERIES_PER_HOUR 20  
-> MAX_UPDATES_PER_HOUR 10  
-> MAX_CONNECTIONS_PER_HOUR 5  
-> MAX_USER_CONNECTIONS 2;
```

MySQL 授权

- 管理权限
- 数据库权限
- 会话限制
- 权限控制的精细化管理

Column privileges

User	Host	Scope	Select	Insert	Update	References
myuser2	localhost	tpcc.orders.o_id	Y	N	N	N

User	Host	Scope	Select	Insert	Update	Delete	Create	Drop	Grant	Refer...	Index	Alter	Creat...	Show...	Trigger
root	localhost	<global>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
mysqlbackup	localhost	<global>	Y	N	N	N	Y	N	N	N	N	Y	N	N	N
root	%	<global>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
tpcc	%	tpcc	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
tpcc	%	tpcc.orders	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	Y
myuser1	localhost	tpcc.orders	N	Y	N	N	N	N	N	N	N	N	N	N	N
myuser2	localhost	tpcc.orders	N	N	N	N	N	N	N	N	N	N	N	N	N

MySQL 授权

- 管理权限
- 数据库权限
- 会话限制
- 权限控制的精细化管理

Role	Description
<input type="checkbox"/> DBA	grants the rights to perform all tasks
<input type="checkbox"/> MaintenanceAdmin	grants rights needed to maintain server
<input type="checkbox"/> ProcessAdmin	rights needed to assess, monitor, and kill any user process
<input type="checkbox"/> UserAdmin	grants rights to create users logins and reset passwords
<input type="checkbox"/> SecurityAdmin	rights to manage logins and grant and revoke server administrative privileges
<input type="checkbox"/> MonitorAdmin	minimum set of rights needed to monitor server
<input type="checkbox"/> DBManager	grants full rights on all databases
<input type="checkbox"/> DBDesigner	rights to create and reverse engineer any database schema
<input type="checkbox"/> ReplicationAdmin	rights needed to setup and manage replication
<input type="checkbox"/> BackupAdmin	minimal rights needed to backup any database

Max. Queries: Number of queries the account can execute within one hour.

Max. Updates: Number of updates the account can execute within one hour.

Max. Connections: The number of times the account can connect to the server per hour.

Concurrent Connections: The number of simultaneous connections to the server the account can have.

Column privileges

User	Host	Scope	Select	Insert	Update	References
myuser2	localhost	tpcc.orders.o_id	Y	N	N	N

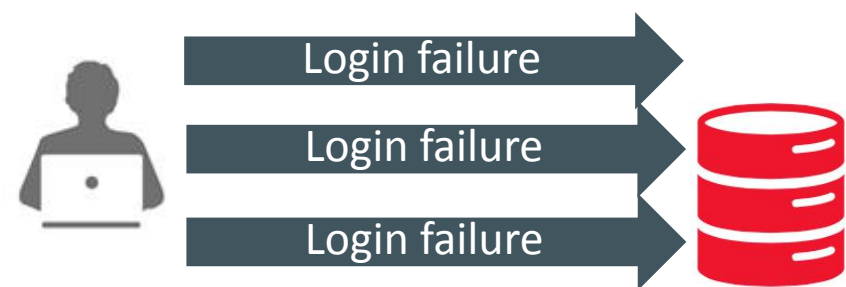
Table privileges

User	Host	Scope	Select	Insert	Update	Delete	Create	Drop	Grant	Refer...	Index	Alter	Creat...	Show...	Trigger
root	localhost	<global>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
mysqlbackup	localhost	<global>	Y	N	N	N	Y	N	N	N	N	Y	N	N	N
root	%	<global>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
tpcc	%	tpcc	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
tpcc	%	tpcc.orders	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	Y
myuser1	localhost	tpcc.orders	N	Y	N	N	N	N	N	N	N	N	N	N	N
myuser2	localhost	tpcc.orders	N	N	N	N	N	N	N	N	N	N	N	N	N



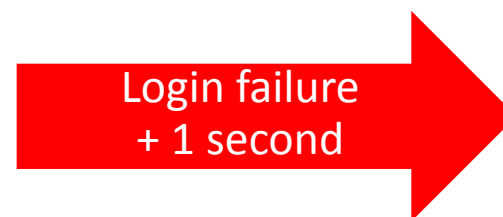
连接插件(plugin-load-add=connection_control.so)

- 防止重复登入失败来猜秘密
 - 每一次登入失败，延长登入时间



PLUGIN_NAME	PLUGIN_STATUS
CONNECTION_CONTROL	ACTIVE
CONNECTION_CONTROL_FAILED_LOGIN_ATTEMPTS	ACTIVE

Variable_name	Value
connection_control_failed_connections_threshold	3
connection_control_max_connection_delay	2147483647
connection_control_min_connection_delay	1000



MySQL 密码策略

- 无密码账户
 - 给每个账户设置密码防止越权使用
- 密码验证插件
 - 强制设置“强”密码
- 密码期限/轮换
 - 要求用户重设密码
- 锁定账户(v. 5.7)

MySQL Database 强化保安配置

- 审计行为
 - 使用 *Enterprise Audit*
 - 变更时暂时启动查询日志
 - 监控和定期检查
- 限制或禁用远程访问
 - 使用 “skip-networking” 或 bind-address=127.0.0.1
 - 远程访问限制主机IP
- 考虑更改默认端口
- 更改root用户名
- 禁用未授权读取本地文件
 - 禁用 LOAD DATA LOCAL INFILE
- 在非默认端口上运行 MySQL
 - 找到数据库更加困难
- 限制 MySQL OS 用户
- 连接加密
 - SSL /TLS 传送数据
 - 客户端和服务器的复制

MySQL 企业版



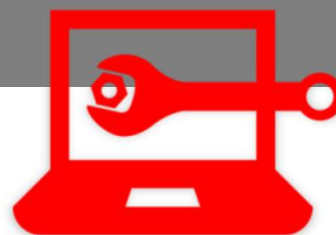
高级功能

- 可扩展性
- 高可用性
- 验证
- 审计
- 加密 + TDE
- 防火墙



管理工具

- 监控
- 备份
- 开发
- 管理
- 数据迁移



技术支持

- 技术支持
- 顾问支持
- Oracle 认证

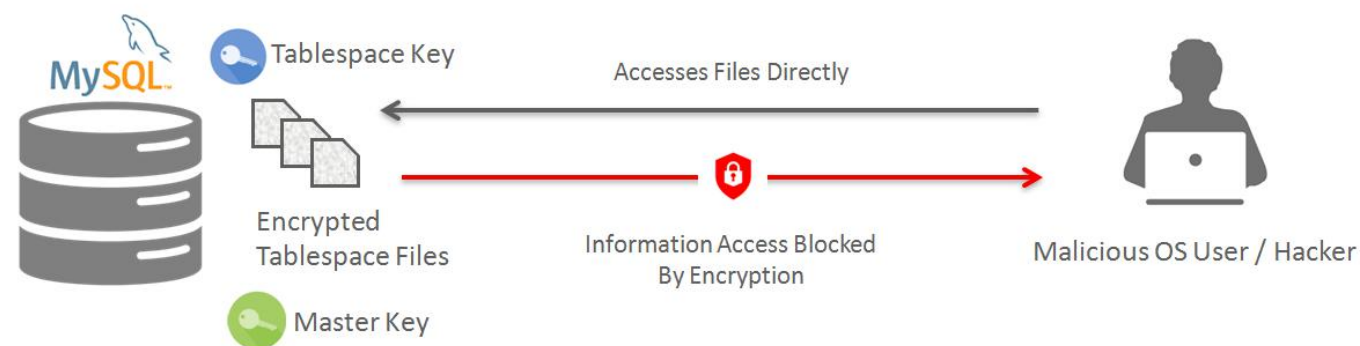


MySQL 企业版

- MySQL Enterprise **Authentication**
 - 外部认证模块
 - Microsoft AD, Linux PAMs
- MySQL Enterprise **Encryption**
 - 公钥/私钥加密
 - 非对称加密
 - 数字签名, 数据验证
- MySQL Enterprise **Firewall**
 - 阻止 SQL 注入攻击
 - 检测入侵
- MySQL Enterprise **Audit**
 - 审计用户行为, 合规审计
- MySQL Enterprise **Monitor**
 - 变更数据库设置, 用户权限, 数据库定义, 密码
- MySQL Enterprise **Backup**
 - 安全备份, AES 256 加密
- MySQL Enterprise **Transparent Data Encryption**
 - 据存储加密 – 对应用访问是透明
 - AES 256加密
 - 密钥管理

MySQL Enterprise Transparent Data Encryption

- 跟强的安全性
 - 强化OS对数据安全控制
 - 易于使用和管理
 - 对数据库用户/应用-透明访问
- 满足安全性和监管需求
 - 适合需要加密的场景
 - 医疗，财务服务，政府等等。
- 保护和管理密钥
 - 支持标准KMIP 1.2协议
 - 支持Oracle密钥库和其他密钥存储库



MySQL Enterprise Monitor

- 执行MySQL安全最佳实践
 - 识别漏洞
 - 评估当前的设置与安全性加强策略
- 监控 & 警告
 - 监控用户
 - 监控密码
 - 监控模式变更
 - 监控备份
 - 配置管理
 - 配置优化建议
- 集中用户管理

Item	Info	Coverage	Schedule	Event Handling	Parameters
Account Has An Overly Broad Host Specifier	?	100% (103/103)	5m	0 2 0	""
Account Has Global Privileges	?	100% (103/103)	5m	0 2 0	""
Account Has Old Insecure Password Hash	?	100% (103/103)	6h	0 2 0	""
Account Has Strong MySQL Privileges	?	100% (103/103)	5m	0 2 0	""
Account Requires Unavailable Authentication Plugins	?	100% (103/103)	6h	1 3 0	""
Insecure Password Authentication Option Is Enabled	?	100% (103/103)	6h	0 2 0	"ON"
Insecure Password Generation Option Is Enabled	?	100% (103/103)	6h	0 2 0	1
LOCAL Option Of LOAD DATA Statement Is Enabled	?	100% (103/103)	5m	0 2 0	"ON"
Non-Authorized User Has DB, Table, Or Index Privileges On All Databases	?				
Non-Authorized User Has GRANT Privileges On All Databases	?				
Non-Authorized User Has Server Admin Privileges	?				
Policy-Based Password Validation Does Not Perform Dictionary Checks	?				
Policy-Based Password Validation Is Weak	?				
Policy-Based Password Validation Not Enabled	?				
Privilege Alterations Detected: Privileges Granted	?				
Privilege Alterations Detected: Privileges Revoked	?				
Privilege Alterations Have Been Detected	?				
Root Account Can Login Remotely	?	100% (103/103)	5m	0 2 0	0
Root Account Without Password	?	100% (103/103)	5m	1 3 0	0
SHA-256 Password Authentication Not Enabled	?	100% (103/103)	6h	0 2 0	"ACTIVE"
Server Contains Default "test" Database	?	100% (103/103)	5m	0 3 0	"test"

Problem Description
 When users create weak passwords (e.g. 'password' or 'abcd') it compromises the security of the server, making it easier for unauthorized people to guess the password and gain access to the server. Starting with MySQL Server 5.6, MySQL offers the 'validate_password' plugin that can be used to test passwords and improve security. With this plugin you can implement and enforce a policy for password strength (e.g. passwords must be at least 8 characters long, have both lowercase and uppercase letters, and contain at least one special nonalphanumeric character).

Links and Further Reading
[MySQL Manual: The Password Validation Plugin](#)
[MySQL Manual: Keeping Passwords Secure](#)
[Blog: New 5.6 password verification plugin \(and impacts to PASSWORD\(\) function\)](#)
[Blog: Implementing a password policy in MySQL](#)

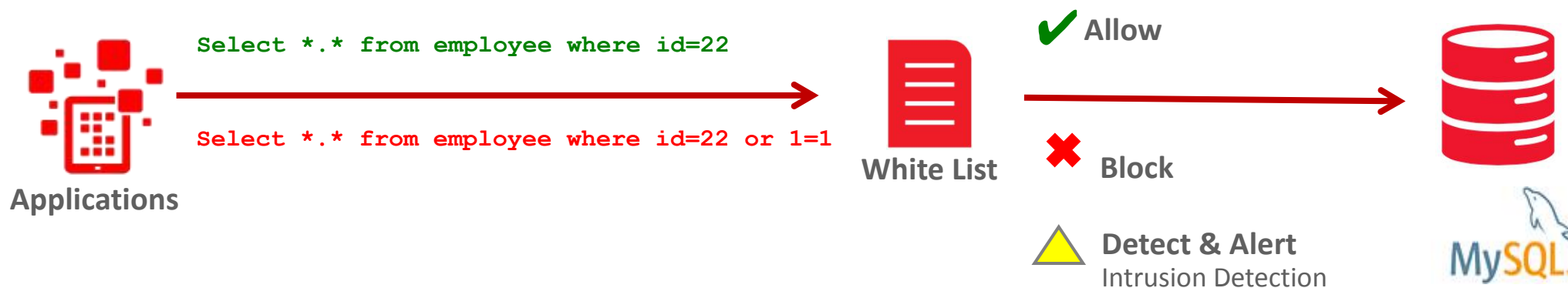
Expression
 %status% == "ACTIVE" && %validate_password_policy% == THRESHOLD

"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 Firewall

- 阻止 SQL 注入攻击
 - 允许: 匹配白名单的SQL语句
 - 阻止: 白名单中不存在的SQL语句
- 入侵检测系统
 - 检测: 白名单中不存在的SQL语句
 - 执行SQL语句并且发出警告



MySQL Enterprise Firewall 详细

- 防火墙操作作用于用户级别
- 每个用户的可设置状态如下

—RECORDING `call mysql.set_firewall_mode ('fwuser@localhost', 'RECORDING');`

—PROTECTING `call mysql.set_firewall_mode ('fwuser@localhost', 'PROTECTING');`

—DETECTING `call mysql.set_firewall_mode ('fwuser@localhost', 'DETECTING');`

—OFF `call mysql.set_firewall_mode ('fwuser@localhost', 'OFF');`

MySQL Enterprise Firewall: 每个用户的白名单

The screenshot shows the MySQL Enterprise Firewall Administration interface. The main window is titled "Administration - Users and Privileges" and displays "Details for account jsmith@%". The "Firewall Rules" tab is active, showing a list of active rules and rules being recorded.

User Accounts

User	From Host	FW
(!) <anonymous>	%	OF
janedoe	%	OF
jsmith	%	RE
mfrank	%	OF
mysqlbackup	localhost	OF
newuser	%	OF
robsmith	%	OF
root	%	OF
root	localhost	OF
root	::1	OF
root	127.0.0.1	OF
webuser	localhost	OF

Details for account jsmith@%

Mode: RECORDING

Active rules (64):

```
SHOW FIELDS FROM `sakila`.`category`
SHOW FULL TABLES FROM `sakila`
SELECT `st`, * FROM `performance_schema`.`events_stages_history_long` `st` WHERE `st`.`nesting_event_id` = ?
EXPLAIN `mysql`.`db`
SHOW FULL TABLES FROM `actor`
SHOW FIELDS FROM `sakila`.`actor_info`
SHOW SESSION VARIABLES LIKE ?
SHOW FIELDS FROM `sakila`.`city`
SHOW FIELDS FROM `sakila`.`film`
SHOW FIELDS FROM `sakila`.`language`
SHOW INDEXES FROM `sakila`.`address`
SHOW GLOBAL VARIABLES
SELECT NAME, TYPE FROM `mysql`.`proc` WHERE `Db` = ?
```

Rules being recorded (64):

```
SHOW FIELDS FROM `sakila`.`category`
SHOW FULL TABLES FROM `sakila`
SELECT `st`, * FROM `performance_schema`.`events_stages_history_long` `st` WHERE `st`.`nesting_event_id` = ?
EXPLAIN `mysql`.`db`
SHOW FULL TABLES FROM `actor`
SHOW FIELDS FROM `sakila`.`actor_info`
SHOW SESSION VARIABLES LIKE ?
SHOW FIELDS FROM `sakila`.`city`
SHOW FIELDS FROM `sakila`.`film`
SHOW FIELDS FROM `sakila`.`language`
SHOW INDEXES FROM `sakila`.`address`
SHOW GLOBAL VARIABLES
SELECT NAME, TYPE FROM `mysql`.`proc` WHERE `Db` = ?
SELECT * FROM `sakila`.`actor_info` LIMIT ?, ...
SHOW FIELDS FROM `sakila`.`customer_list`
SHOW FIELDS FROM `sakila`.`sales_by_film_category`
SHOW FIELDS FROM `sakila`.`actor`
SELECT `st`, * FROM `performance_schema`.`events_statements_current` `st` JOIN `performance_schema`.`threads` `thr` ON `thr`.`thread_id` = `st`.`thread_id` WHERE `thr`.`SELECT CURRENT_USER ()
SHOW FIELDS FROM `sakila`.`sales_by_store`
```

Buttons: Add Account, Delete, Refresh, Revert, Apply

MySQL Enterprise Firewall: 保护模式下，阻止SQL会发生什么？

- 客户端应用会发生错误

```
mysql> SELECT first_name, last_name FROM customer WHERE customer_id = 1 OR TRUE;
```

```
ERROR 1045 (28000): Statement was blocked by Firewall
```

```
mysql> SHOW DATABASES;
```

```
ERROR 1045 (28000): Statement was blocked by Firewall
```

```
mysql> TRUNCATE TABLE mysql.user;
```

```
ERROR 1045 (28000): Statement was blocked by Firewall
```

- 记录到错误日志
- 增量计数器

MySQL Enterprise Authentication

- 与集中认证架构集成
 - 集中账号管理
 - 密码策略管理
 - 群组 & 角色
- PAM (Pluggable Authentication Modules)
 - 标准接口 (Unix, LDAP, Kerberos, others)
 - Windows
 - 使用原生 Windows 服务 - Windows Active Directory 或本地主机



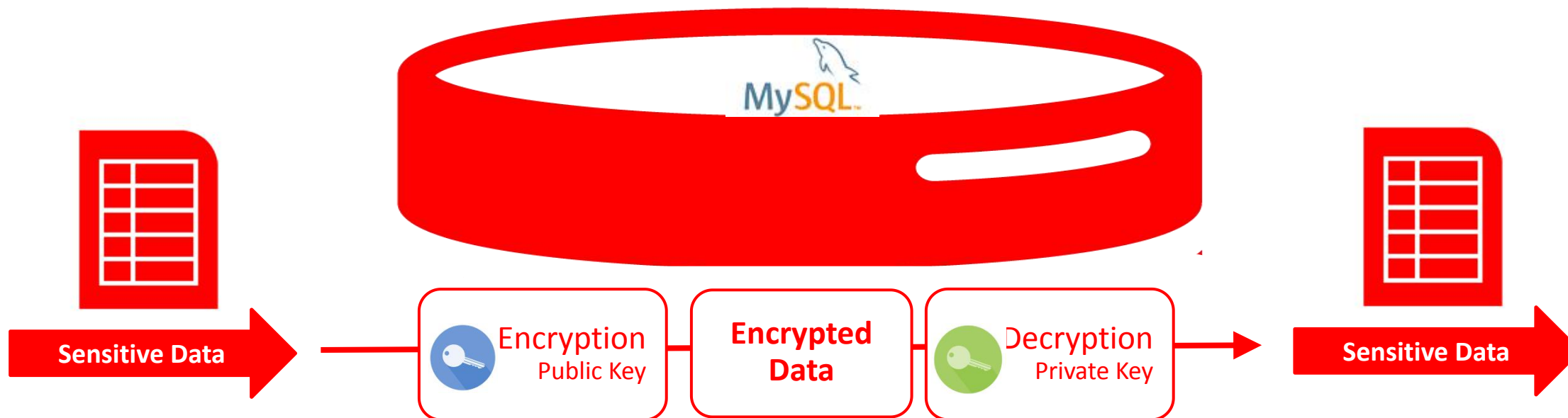
MySQL Enterprise Encryption

- MySQL 加密函数
 - 对称加密AES256 (所有版本)
 - 公钥 / 非对称加密– RSA
- 密钥管理函数
 - 生成公钥和私钥
- 签名和数据验证函数
 - 密码散列数字签名，验证&确认 – RSA, DSA



MySQL Enterprise Encryption

MySQL内加密解密



私钥公钥对

- 使用MySQL Enterprise Encryption 函数生成
- 使用外部生成(e.g. OpenSSL)

MySQL Enterprise Audit

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

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



audit_log_buffer_size	1048576
audit_log_connection_policy	ALL
audit_log_current_session	OFF
audit_log_exclude_accounts	
audit_log_file	audit.log
audit_log_flush	OFF
audit_log_format	NEW
audit_log_include_accounts	
audit_log_policy	ALL
audit_log_rotate_on_size	0
audit_log_statement_policy	ALL
audit_log_strategy	ASYNCHRONOUS

1. DBA enables Audit plugin

```
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>
```


新发布的功能 – 审计过滤

- 新加“Event” 模式
 - 更细化方法定义
- 简单，强大功能
 - 以 JSON 定义

Event class	Event subclass
GENERAL	STATUS
CONNECTION	CONNECT
	CHANGE_USER
	DISCONNECT
TABLE_ACCESS	READ
	INSERT
	UPDATE
	DELETE



MySQL 审计 提供“abort”新功能

MySQL 5.7.20

- 该功能可以通过编写符合SQL语句的审计过滤规则
 - 对于符合筛选规则的SQL, 可以阻止执行。
 - 参考 [Audit Log Filtering](#).

```
"event": {  
  "name": qualifying event subclass names  
  "abort": condition  
}
```

```
{  
  "filter": {  
    "class": {  
      "name": "table_access",  
      "event": {  
        "name": [ "insert", "update", "delete" ],  
        "abort": true  
      }  
    }  
  }  
}
```

对 finance.bank_account 的DELETE/INSERT/UPDATE操作

```
mysql@virtual-41:/opt/demo/10-security/secure-audit-filter
[mysql@virtual-41 secure-audit-filter]$ mysql -uroot -h127.0.0.1 -pmysql
```

场景1：

对app_user01 停用审计，其他用户打开审计

```
Mysql>create user app_user01 identified by 'Mysql@1234';  
Mysql>grant all on *.* to 'app_user01';
```

```
Mysql>SELECT audit_log_filter_set_filter('all_enabled', '{"filter": {"log": true } }') AS 'Result';
```

```
Mysql>SELECT audit_log_filter_set_filter('all_disabled', '{"filter": {"log": false } }') AS 'Result';
```

```
Mysql>SELECT audit_log_filter_set_user('%', 'all_enabled') AS 'Result';
```

```
Mysql> SELECT audit_log_filter_set_user('app_user01@%', 'all_disabled') AS 'Result';
```

场景2： 对appdb停用审计

```
select audit_log_filter_set_filter ('log_appdb', ' "filter": {  
  "class": [ {  
    "name": "table_access",  
    "event": { "name": ["insert", "update", "delete", "read"],  
      "log": { "field": {  
        "name": "table_database.str", "value": "appdb"  
      } } } },  
    { "name": "general", "log": false }  
  ] } } ');
```

```
SELECT audit_log_filter_set_user('%', 'log_appdb') AS 'Result';
```

MySQL Enterprise Backup

- InnoDB在线备份 (可编辑脚本接口)
- 全备, 增量, 部分备份(包含压缩)
- 加密 (AES 256)
- 时间点, 完整, 部分恢复
- 状态元数据, 进度, 历史记录
- 扩展 – 高性能/无限制的数据库容量
- Windows, Linux, Unix
- Oracle认证的Oracle Secure Backup , NetBackup, Tivoli, 等等

MySQL Workbench

MySQL57-3357 x

File Edit View Query Database Server Tools Scripting Help

Navigator

- MANAGEMENT
 - Server Status
 - Client Connections
 - Users and Privileges
 - Status and System Variables
 - Data Export
 - Data Import/Restore
- INSTANCE
 - Startup / Shutdown
 - Server Logs
 - Options File
- PERFORMANCE
 - Dashboard
 - Performance Reports
 - Performance Schema Setup
- MYSQL ENTERPRISE
 - Audit Inspector
 - Firewall
 - Online Backup**
 - Restore

Query 1 Administration - Online Backup x

MySQL Enterprise

MySQL Enterprise Backup

Backup Profile Name: Full Data / Not Scheduled

Comments:

Schedule Contents Options **Advanced**

Manually specify additional options to be passed directly to the MySQL Enterprise Backup command.
NOTE: configured values are not validated in any way.

```
encrypt  
key=23D987F3A047B475C900127148F9E0394857983645192874A2B3049570C12A34
```

Management Schemas

Information

MySQL Workbench

MySQL57-3357 x

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

MYSQL ENTERPRISE

- Audit Inspector
- Firewall
- Online Backup**
- Restore

Query 1 Administration - Online Backup x

MySQL Enterprise Backup

Backup Jobs configured for this MySQL Instance Backup Job Details

Use right-click context menu for more options

Backup Job	Latest Backup	Next Full Backup
backup (full data)	in the last hour	2017-05-11 11:22:58
backup2 (full data)	n/a	2017-05-11 11:22:58

Target Host: CHOMA 4.1.0

Directory: C:\Program Files\MySQL\MySQL Enterprise Backup\bin

Storage: C:\MySQL\MySQL Enterprise Backup

Backup Size: 22.95 GB

Backup Frequency: Never

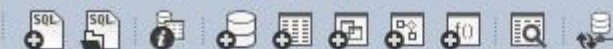
Backup Retention: Never

Backup Schedule: not scheduled

Backup Retention: not scheduled

New Job Configure Job

Execute Backup to Image File...



Navigator

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

MYSQL ENTERPRISE

- Audit Inspector
- Firewall
- Online Backup
- Restore

Management Schemas

Information

Query 1

MySQL

Backup Profile Name

Comments:

Schedule Conte

Manually spec
NOTE: configencrypt
key=23D987

Backup log for C:\MySQLBackupHome\backup\2017-04-16\my3357.img.log

MySQL Enterprise Backup version 4.1.0 Windows-6.2-AMD64 [Wed 03/01/2017]
Copyright (c) 2003, 2017, Oracle and/or its affiliates. All Rights Reserved.

```
170406 16:03:11 MAIN  INFO: A thread created with Id '436'
170406 16:03:11 MAIN  INFO: Starting with following command line ...
C:\Program Files\MySQL\MySQL Enterprise Backup 4.1\mysqlbackup.exe
--defaults-file=C:\MySQLBackupHome\2b779930-1a9f-11e7-95d9-b86b2334ab78.cnf
--backup-dir=C:\MySQLBackupHome\backup\2017-04-16\my3357.img
--backup-image=C:\MySQLBackupHome\backup\2017-04-16\my3357.img.mbi
--show-progress=stdout backup-to-image
```

```
170406 16:03:11 MAIN  INFO:
170406 16:03:11 MAIN  INFO: MySQL server version is '5.7.17-enterprise-commercial-advanced-log'
170406 16:03:11 MAIN  INFO: MySQL server compile os version is 'Win64'
170406 16:03:11 MAIN  INFO: Got some server configuration information from running server.
```

```
170406 16:03:11 MAIN  INFO: Server system variable 'old_alter_table' was set to '0'. Setting it to '1'.
IMPORTANT: Please check that mysqlbackup run completes successfully.
At the end of a successful 'backup-to-image' run mysqlbackup
prints "mysqlbackup completed OK!".
```

```
170406 16:03:11 MAIN  INFO: MEB logfile created at C:\MySQLBackupHome\backup\2017-04-16\my3357.img\meta\MEB_2017-04-06.16-03-11_image_backup.log
```

Server Repository Options:

```
datadir           = C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\
innodb_data_home_dir  =
innodb_data_file_path = ibdata1:12M:autoextend
innodb_log_group_home_dir = C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\
innodb_log_files_in_group = 2
innodb_log_file_size  = 50331648
innodb_undo_directory = C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\
innodb_undo_tablespaces = 0
innodb_undo_logs      = 128
innodb_buffer_pool_filename = ib_buffer_pool
innodb_page_size      = 16384
```

Close

Backup : MySQL Enterprise... x

https://localhost:18443/Backup.action?_x=x&assetSelection={["assetClass"%3A"com.mysql.eto...

ORACLE MySQL Enterprise Monitor

1 3 0 0 13 admin

Dashboards Events Query Analyzer Reports & Graphs Refresh: Off

Instance Backup Overview

All

Current Status History Apr 6, 2017 2:27:56 pm x

Instance: CHOMA-HK2:3357, Backup ID: 14914600516869295

Backup Status

Backup Type: FULL	Exit State: SUCCESS
Start Time: Apr 6, 2017 2:27:31 pm (an hour ago)	End Time: Apr 6, 2017 2:27:56 pm (an hour ago)
Start LSN: 3637416960	End LSN: 3637417429
Binlog File: CHOMA-HK2-bin.000009	Binlog Position: -1
Backup Destination: C:\MySQLBackupHome\backup\2017-04-16	

Backup Configuration

Backup Format: IMAGE	MySQL Data Dir: C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\
Compression Level: 1	Engines: CSV:InnoDB:MEMORY:MyISAM:PERFORMANCE

InnoDB Configuration

Data File Path: ibdata1:12M:autoextend	File Format: Barracuda
Log Files in Group: 2	Log File Size: 48 MiB
Data Home Directory:	Log Group Home Directory: C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\

Backup Command

```
mysqlbackup --defaults-file=c:\MySQLBackupHome\e7d5404f-0947-11e7-86bf-b86b2334ab78.cnf --skip-unused-pages --backup-image=c:\MySQLBackupHome\backup\2017-04-16\2017-04-16.img --backup-dir=C:\MySQLBackupHome\backup\2017-04-16 --compress --skip-unused-pages --no-locking backup-to-image
```

Progress Log

Copyright © 2005, 2017, Oracle and/or its affiliates. All rights reserved. 3.3.3.1199 - CHOMA-HK2 () - Apr 6, 2017 3:53:29 pm HKT (Up Since: 1 hour, 36 minutes ago) - About

```
[mysqld]
datadir = C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\

[mysqlbackup]
datadir = C:\ProgramData\MySQL\MySQL Server 5.7\Data57a\
innodb_data_home_dir =
backup_dir = C:\MySQLBackupHome\backup
incremental_backup_dir = C:\MySQLBackupHome\backup\inc
incremental_base = history:last_backup
comments =

encrypt
key=23D987F3A047B475C900127148F9E0394857983645192874A2B3049570C12A34
```

更安全的数据库

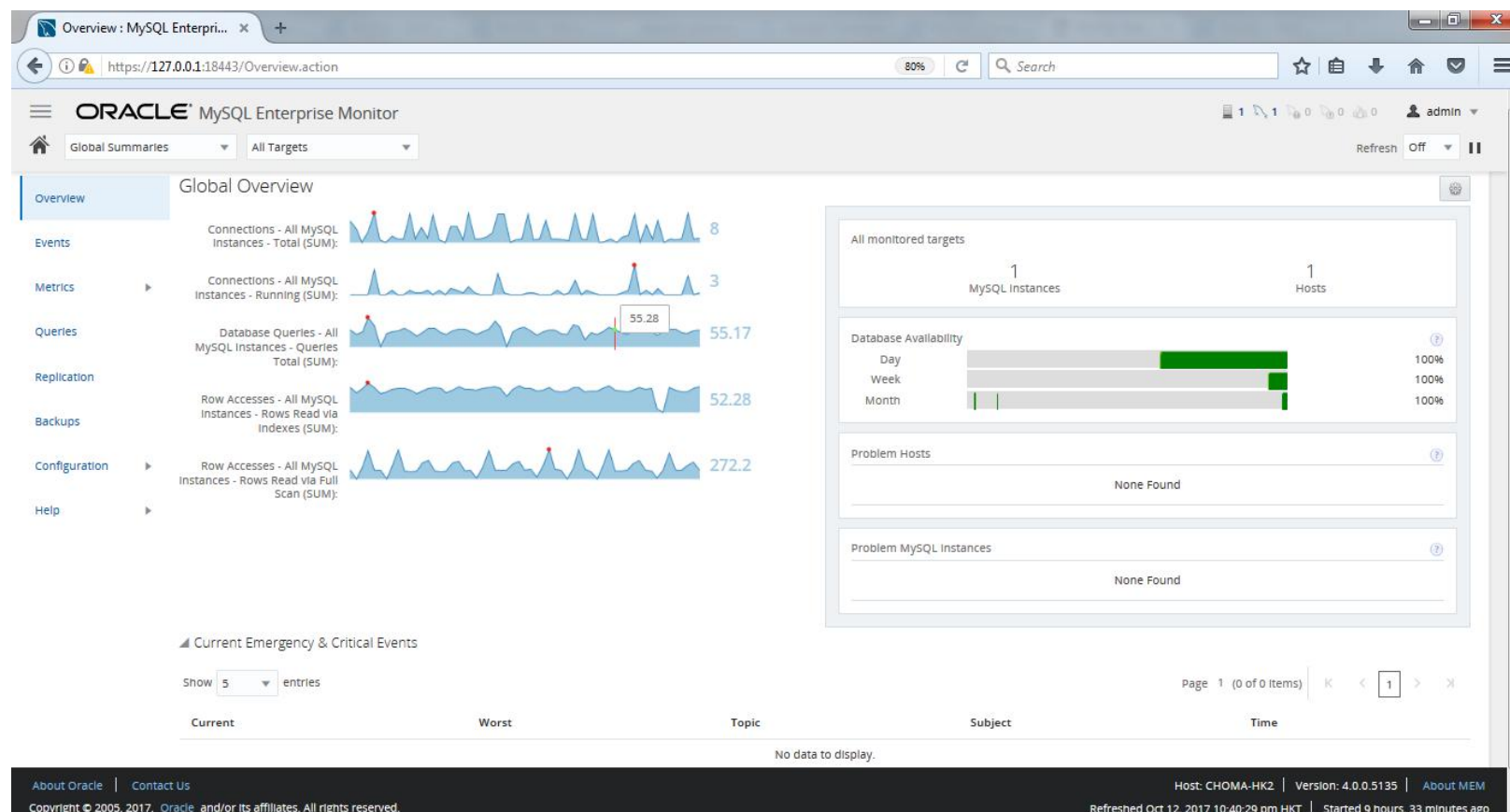
采用MySQL 企业版

- MySQL Enterprise **Authentication**
 - 验证模块插件
Microsoft AD, Linux PAM, LDAP
- MySQL Enterprise **Encryption**
 - 公共/私人密钥加密
 - 非对称加密
 - 数码签名, 数据验证
- MySQL Enterprise **Firewall**
 - 阻止SQL注入攻击
 - 入侵检测
- MySQL Enterprise **Audit**
 - 用户活动审计, 合规性
- MySQL Enterprise **Monitor**
 - 数据库配置, 用户权限, 数据库架构, 空密码通知
- MySQL Enterprise **Backup**
 - 以AES 256加密- 保护备份数据
- MySQL Enterprise **TDE**
 - AES 256 加密
 - 密钥管理



MySQL Enterprise Monitor 4.0 新发布

- 对 Group Replication / InnoDB clusters - 全局监控
 - 拓卜图
 - 详细指标 / 图表
 - Best Practice advice
- 新版面
- MySQL NDB Cluster 7.5.7+ monitoring



MySQL Enterprise Monitor 4.0 新发布

- MySQL NDB Cluster 7.5.7+ monitoring

NDB Cluster Memory

Selected Metric: Total Allocation | Refreshed: Sep 15, 2017 3:19:02 pm | Reload

Schemas: ndbmemcache, world_ndb, mysql, sys

Tables: cache_policies, memcache_server_r..., containers, city, key_prefixes, last_memcached..., ndb_clusters, countrylanguage, country, SYSTAB_0, NDBEVENTS_0, meta, demo_..., extern_...

NDB Cluster Memory

Table View | Treemap View | Refreshed: Sep 15, 2017 3:19:00 pm | Reload

Schema Name	Table Name	Object Name	Type	Fragment Number	Node Id	Block Instance	Fixed Size Allocation	Fixed Size Eleme
world_ndb	city		User table	0	3	1	96 KIB	368 b
world_ndb	city		User table	3	6	1	96 KIB	7.64 KIB
world_ndb	city		User table	0	4	1	96 KIB	368 b
world_ndb	city		User table	1	5	1	96 KIB	3.95 KIB
world_ndb	city		User table	1	6	1	96 KIB	3.95 KIB
world_ndb	city		User table	2	3	1	96 KIB	3.23 KIB
world_ndb	city		User table	2	4	1	96 KIB	3.23 KIB
world_ndb	city		User table	3	5	1	96 KIB	7.64 KIB
ndbmemcache	containers		User table	2	4	1	32 KIB	31.8 KIB
ndbmemcache	cache_policies		User table	0	4	1	32 KIB	31.8 KIB

Host: CHOMA-HK2 | Version: 4.0.0.5135 | About MEM

Refreshed Oct 12, 2017 10:59:56 pm HKT | Started 9 hours, 52 minutes ago

评估- MySQL Enterprise Monitor

- 强制执行MySQL安全最佳做法
 - 识别漏洞
 - 根据安全强化策略评估当前设置
- 监控和警报
 - 用户监控
 - 密码监控
 - 模式变更监测
 - 备份监控
 - 配置管理
 - 配置调优建议
- 集中用户管理

Item	Info	Coverage	Schedule	Event Handling	Parameters
Account Has An Overly Broad Host Specifier	?	100% (103/103)	5m	0 2 0	""
Account Has Global Privileges	?	100% (103/103)	5m	0 2 0	""
Account Has Old Insecure Password Hash	?	100% (103/103)	6h	0 2 0	""
Account Has Strong MySQL Privileges	?	100% (103/103)	5m	0 2 0	""
Account Requires Unavailable Authentication Plugins	?	100% (103/103)	6h	1 3 0	""
Insecure Password Authentication Option Is Enabled	?	100% (103/103)	6h	0 2 0	"ON"
Insecure Password Generation Option Is Enabled	?	100% (103/103)	6h	0 2 0	1
LOCAL Option Of LOAD DATA Statement Is Enabled	?	100% (103/103)	5m	0 2 0	"ON"
Non-Authorized User Has DB, Table, Or Index Privileges On All Databases	?				
Non-Authorized User Has GRANT Privileges On All Databases	?				
Non-Authorized User Has Server Admin Privileges	?				
Policy-Based Password Validation Does Not Perform Dictionary Checks	?				
Policy-Based Password Validation Is Weak	?				
Policy-Based Password Validation Not Enabled	?				
Privilege Alterations Detected: Privileges Granted	?				
Privilege Alterations Detected: Privileges Revoked	?				
Privilege Alterations Have Been Detected	?				
Root Account Can Login Remotely	?	100% (103/103)	5m	1 3 0	0
Root Account Without Password	?	100% (103/103)	5m	1 3 0	0
SHA-256 Password Authentication Not Enabled	?	100% (103/103)	6h	0 2 0	"ACTIVE"
Server Contains Default "test" Database	?	100% (103/103)	5m	0 3 0	"test"

Problem Description
 When users create weak passwords (e.g. 'password' or 'abcd') it compromises the security of the server, making it easier for unauthorized people to guess the password and gain access to the server. Starting with MySQL Server 5.6, MySQL offers the 'validate_password' plugin that can be used to test passwords and improve security. With this plugin you can implement and enforce a policy for password strength (e.g. passwords must be at least 8 characters long, have both lowercase and uppercase letters, and contain at least one special nonalphanumeric character).

Links and Further Reading
[MySQL Manual: The Password Validation Plugin](#)
[MySQL Manual: Keeping Passwords Secure](#)
[Blog: New 5.6 password verification plugin \(and impacts to PASSWORD\(\) function\)](#)
[Blog: Implementing a password policy in MySQL](#)

Expression
 %status% == "ACTIVE" && %validate_password_policy% == THRESHOLD

"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 企业版



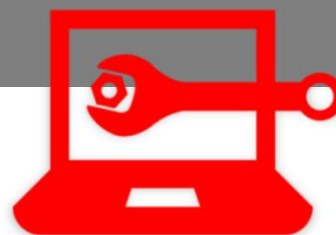
高级功能

- 可扩展性
- 高可用性
- 安全性
- 审计
- 加密
- Firewall + TDE



管理工具

- 监控
- 备份
- 开发
- 管理
- 迁移



支持

- 技术支持
- 咨询支持
- Oracle 认证



参考

- [MySQL Enterprise Security](#)
- [MySQL Enterprise Authentication](#)
- [MySQL Enterprise Firewall](#)
- [MySQL Enterprise Transparent Data Encryption](#)
- [MySQL Enterprise Audit](#)
- [MySQL Enterprise Backup](#)
- [MySQL Enterprise Monitor](#)
- [Encryption Functions](#)
- [Enterprise Encryption Functions](#)

谢谢!