MySQL的最新版本8.1及MySQL的安全最佳实践

徐轶韬

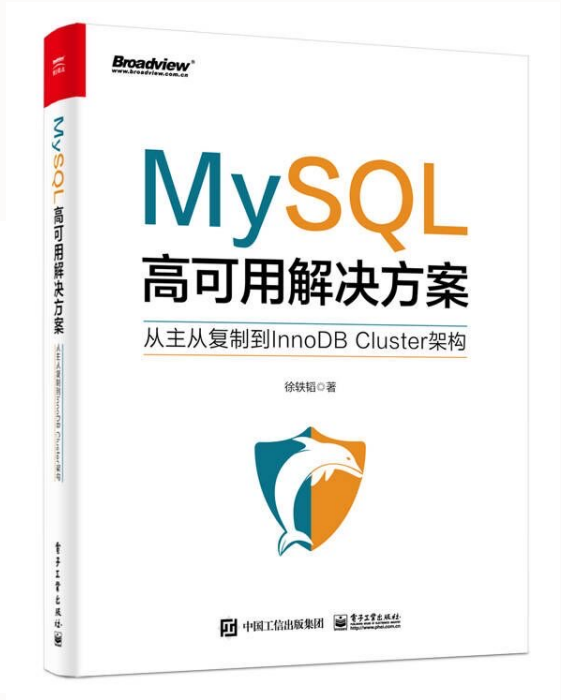
甲骨文公司MySQL解决方案首席工程师

ORACLE

徐轶韬

甲骨文公司MySQL解决方案首席工程师

公众号“MySQL解决方案工程师”的内容作者和运营者。



《MySQL高可用解决方案——从主从复制到InnoDB Cluster架构》作者

MySQL版本——长期稳定版与创新版（ LTS & Innovation Releases ）

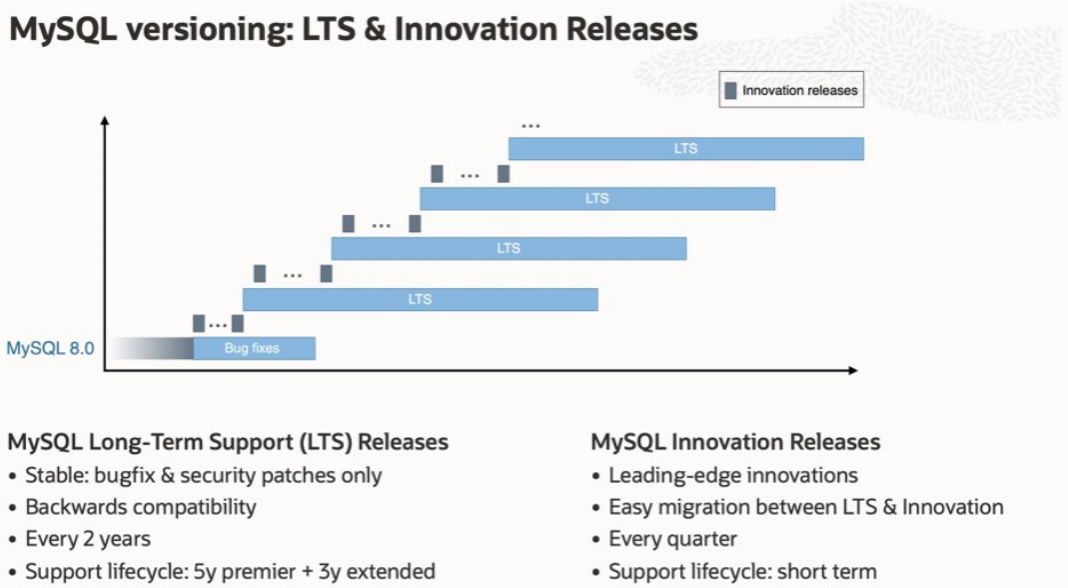
https://blogs.oracle.com/mysql/post/introducing-mysql-innovation-and-longterm-support-lts-versions

长期稳定版将与8.0.xx一起发布

- 8.0.xx+ 仅包含错误修复、不会引入非必要功能

创新版

- 包含错误修复和新特性，与现有的8.0类似



MySQL 8.1.0 是第一个创新版本，
MySQL 8.0.34+ 将仅包含错误修复直至 8.0 (EOL)2026年4月

Oracle Lifetime Support for MySQL

从GA开始最长8年提供错误修复、补丁、升级

特性	标准支持服务 (1 至 5 年)	延伸支持服务 (6 至 8 年)	持续支持服务 (9 年以上)
24x7 支持服务	•	•	•
无限制的支持事件	•	•	•
知识库	•	•	•
维护版本、错误修复、补丁、更新	•	•	仅限已有

MySQL Version	GA(YYYY-MM)	Premier (~5年)	Extended (6~8年)	Sustain (9年以后)
5.0	2005-10	x	x	○
5.1	2008-12	x	x	○
5.5	2010-12	x	x	○
5.6	2013-02	x	x	○
5.7	2015-10	**2020-10**	2023-10	(预定)
8.0	2018-04	2025-04	2026-04	(预定)

▶ https://www.oracle.com/us/assets/lifetime-support-technology-069183.pdf

8.0.34/8.1.0 参数

MySQL Parameters

mysqld | mysql | variable | status | charset | collation | privilege | function | information_schema | performance_schema | keyword | error

Version: 8.0.33 8.0.34 8.1.0 Difference only Include plugins

Parameter	8.0.33	8.0.34	8.1.0
build_id	acbc49ebed904cdd4e3e61226adcda0a8c0ad719	f183cd3ecfc35a4aa5da997063d5e8c97ffca986	9ad00ba9c420608e3d596a40a133fd20d019a80e
connection_memory_chunk_size	8912	8192	8192
innodb_version	8.0.33	8.0.34	8.1.0
performance_schema_error_size	5288	5293	5335
performance_schema_max_statement_classes	219	219	220
tls_certificates_enforced_validation			OFF
version	8.0.33	8.0.34	8.1.0

MySQL Shell 8.1

8.1.0 [2023-07-18] ➔ 8.1.1 [2023-07-26]

- 8.1.1
  - MySQL Shell dump/load支持OCI专用端点的PAR与对象存储
  - 8.1.0 ➔ MySQL HeatWave Service包含一个名为mysql_audit的模式。这将导致在运行dump/load到另一个DB系统时出现重复对象错误
- 如果AWS HEAD请求因授权错误而失败，则不会重试。在此版本中，如果这样的请求失败并出现400 HTTP错误，则会重试。
- 如果刷新AWS凭证的过程定义了过期时间，刷新过程将在所需时间之前5分钟触发。(Bug #35468541)
  - 存储过程产生的错误不会在经典MySQL协议连接上返回。(Bug #35549008)

MySQL Shell 8.1

8.1.0 :

- InnoDB Cluster的只读副本
  - <cluster>.addReplicaInstance( )
- 支持转储至OCI的PAR（Pre-Authenticated Request） 或对象存储
  - util.dumpInstance(outputUrl[, options])
  - util.dumpSchemas(schemas, outputUrl[, options])
  - util.dumpTables(schema, tables, outputUrl[, options])
- 复制实例、模式，表 [https://dev.mysql.com/doc/mysql-shell/8.1/en/mysql-shell-utils-copy.html] 例：

```
JS> util.copyInstance('mysql://User001@DBSystemIPAddress,{threads: 6, deferTableIndexes: "all", compatibility: ["strip_restricted_grants", "strip_definers", "create_invisible_pks"]})
JS> util.copySchemas(['sakila'], 'user@localhost:4101',{schema: "mySakilaSchema"})
JS> util.copyTables('sakila', ['actor'], 'root@localhost:4101',{schema: "mySakilaSchema"})
```

MySQL Server 8.1

账户管理

validate_password.changed_characters_percentage

审计

- audit_log_database (-D)选择存储过滤条件表的数据库
  - 例： $> mysql -u root -D *database_name* -p < audit_log_filter_linux_install.sql
- Audit log direct writes
  - 显示直接写入审计日志的次数(依赖审计日志策略)

binlog

- libmysqlclient中添加了函数，使开发人员能够访问MySQL服务器二进制日志mysql_binlog_open()，mysql_binlog_fetch()，及 mysql_binlog_close()。

MySQL EE中增加遥测组件

OpenTelemetry (OTel)项目是一个开源的可观察性框架，提供了一个通用可观察性标准。它使用户能够检测他们的应用程序，以便导出可观察数据:跟踪、度量和日志，从而增加调试和测试的粒度。

遥测组件

```
Mysql> install component 'file://component_telemetry';
```

```
mysql> show variables like 'tel%';
+-----------------------------------------------------+---------------------------------+
| Variable_name                                       | Value                           |
+-----------------------------------------------------+---------------------------------+
| telemetry.otel_bsp_max_export_batch_size            | 512                             |
| telemetry.otel_bsp_max_queue_size                   | 2048                            |
| telemetry.otel_bsp_schedule_delay                   | 5000                            |
| telemetry.otel_exporter_otlp_traces_certificates    |                                 |
| telemetry.otel_exporter_otlp_traces_client_certificates |                             |
| telemetry.otel_exporter_otlp_traces_client_key      |                                 |
| telemetry.otel_exporter_otlp_traces_compression     | none                            |
| telemetry.otel_exporter_otlp_traces_endpoint        | http://localhost:4318/v1/traces |
| telemetry.otel_exporter_otlp_traces_headers         |                                 |
| telemetry.otel_exporter_otlp_traces_protocol        | http/protobuf                   |
| telemetry.otel_exporter_otlp_traces_timeout         | 10000                           |
| telemetry.otel_log_level                            | info                            |
| telemetry.otel_resource_attributes                  |                                 |
| telemetry.query_text_enabled                        | ON                              |
| telemetry.trace_enabled                             | ON                              |
+-----------------------------------------------------+---------------------------------+
15 rows in set (0.00 sec)
```

MySQL 客户端

https://dev.mysql.com/doc/refman/8.1/en/telemetry-trace-install.html

```
[opc@mysql8034-update (158.101.111.196) ~]$ export LD_LIBRARY_PATH=/usr/lib64/mysql/private
[opc@mysql8034-update (158.101.111.196) ~]$ mysql --telemetry_client -uroot -h127.0.0.1 -P3310
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 109828
Server version: 8.1.0-commercial MySQL Enterprise Server - Commercial

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

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

telemetry_client: Using OTLP HTTP exporter to endpoint <http://localhost:4318/v1/traces>
Telemetry plugin <telemetry_client> is loaded.

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

mysql>
```

JSON 格式的EXPLAIN输出至变量

EXPLAIN FORMAT=JSON INTO *var_name stmt*

```
mysql> explain format=json into @x select 1;
Query OK, 0 rows affected (0.00 sec)

mysql> select @x
    -> ;
+-------------------------------------------------------------------------------+
| @x                                                                            |
+-------------------------------------------------------------------------------+
| {
  "query_block": {
    "select_id": 1,
    "message": "No tables used"
  }
} |
+-------------------------------------------------------------------------------+
1 row in set (0.00 sec)
```


CURRENT_USER() - 作为 VARCHAR / TEXT 字段的默认值

```
mysql> SELECT CURRENT_USER();
+--------------------+
| CURRENT_USER()     |
+--------------------+
|  sakila@localhost  |
+--------------------+
1 row in set (0.00 sec)

mysql> CREATE TABLE t (
    >   c1 VARCHAR(288) DEFAULT (USER()),
    >   c2 VARCHAR(288) DEFAULT (CURRENT_USER()),
    >   c3 VARCHAR(288) DEFAULT (SESSION_USER()),
    >   c4 VARCHAR(288) DEFAULT (SYSTEM_USER())
    > );
```


组复制

在选择新的主节点之前，group_replication_set_as_primary()等待所有事务完成，包括当前正在处理的所有DML操作。在8.1中，该函数的处理包含正在运行的的DDL语句(例如，ALTER TABLE)完成。

MySQL Router 8.1

- 支持 InnoDB Cluster Read Replicas
- 从客户端到路由器和路由器到服务器的TLS会话可以缓存并在需要时恢复。缩短了连接握手，节省时间和资源。
- 重试连接(connect_retry_timeout) 当服务器遭遇暂时性错误、拒绝连接时，重新尝试连接。
- 支持语句跟踪——调试、测试，应用程序连接比较等

MySQL InnoDB Cluster只读副本

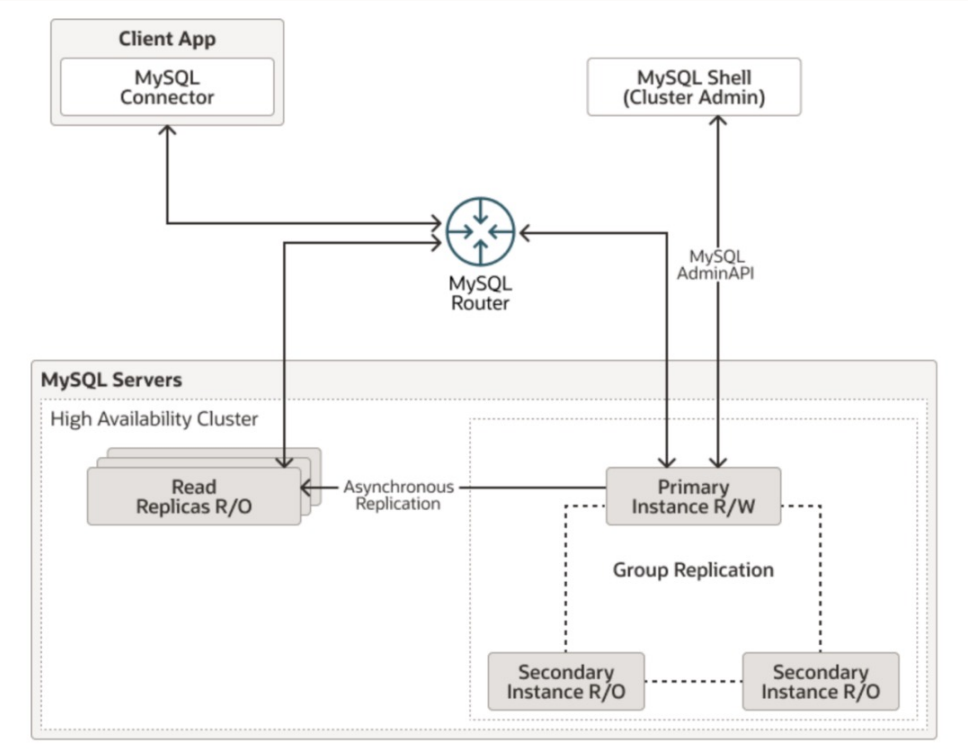
<cluster>.addReplicaInstance(‘<host>:<port’ , {label:’ rr1’ , replicationSources: [‘primary’]})

<cluster>.setRoutingOption([router], option, value)

```
MySQL  mysql8034-update:3310 ssl  mysql_innodb_cluster_metadata  JS > x.routingOptions()
{
    "clusterName": "mycluster",
    "global": {
        "read_only_targets": "secondaries",
        "stats_updates_frequency": null,
        "tags": {}
    },
    "routers": {
        "mysql8034-update.sub06260250450.mysqlvcn.oraclevcn.com::": {}
    }
}
```

“目标只读副本：

- all:目标集群的所有目标副本与其他次要集群的成员一起用于R/O流量
- read_replicas:只有目标集群的只读副本用于R/O流量
- secondaries:只有目标集群的次要成员才能用于R/O流量（默认）



MySQL 8.0.33 (InnoDB Cluster)

MySQL Shell/InnoDB Cluster

- 使用SSL 认证
- MySQL Shell 通过SSH连接转储
- MySQL Shell (OCI Cloud Shell) - 修复使用 OpenSSL加载/转储的内部错误

MySQL Router

- 修复了多个性能和连接(安全/ssl)问题
- 修复MySQL路由器从列出的第一个服务器查询元数据，而不考虑该服务器的角色。

MySQL Operator 8.0.33 / 8.0.34 / 8.1

8.0.33-2.0.9 (2023-04-18) & 8.0.33-2.0.10 (2023-05-19)

- 使用8.0.33镜像
- 默认的容器注册从DockerHub更改为OCR
- mysql/mysql-operator ➔ container-registry.oracle.com/mysql/community-operator
- 添加了自定义集群域检测，允许名称不是“cluster”。“local”用于集群内的服务。

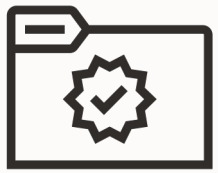
8.0.34 ：除了标准的MySQL Shell升级以匹配Kubernetes版本的MySQL Operator外，不包含功能更改。

8.1.0 :

•备份计划创建的cron作业引用一个Operator镜像，并对Operator的镜像的版本进行更新。 (WL #15583)

•增加了对每个MySQL服务器提供度量的支持。 (WL #15584)

为什么要升级？



增加处理故障的工时

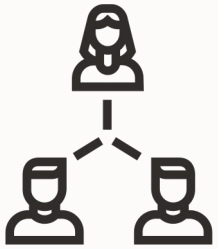
- 厂商支持到期
- 无法提供新的错误修复
- 故障需要由应用程序或者系统对应解决

安全风险增大

- 无法充分应对安全脆弱性
- 遭遇非法攻击停止服务
- 機会損失、信用低下

无法获得性能提升

- 无法享受新功能新特性带来的好处
- 更换硬件时需要考虑所支持的OS



无法降低运维成本

- 存在多个版本、运维管理方法复杂
- 技术方法限定在个人，系统更改难度高

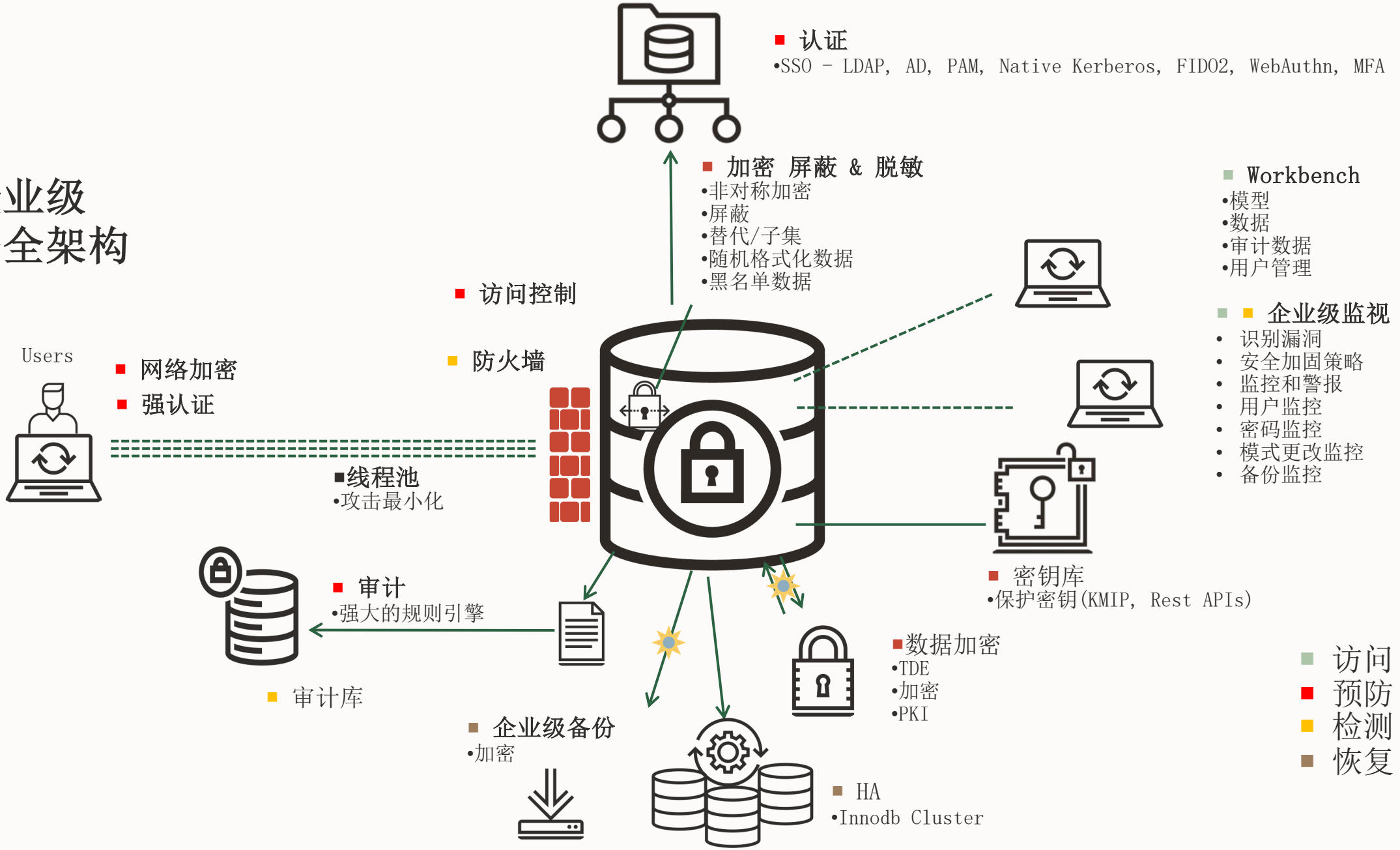
安全风险——数据库遭受的攻击方式

1. SQL注入
   - 防范方法： 数据库防火墙，白名单，输入验证
2. 缓冲区溢出
   - 防范方法 ：经常更新数据库软件，数据库防火墙，白名单，输入验证
3. 内幕滥用
   - 防范方法 ：严格的访问控制，用户特定的身份验证，审计，监控，加密
4. 蛮力破解
   - 防范方法 ：在指定次数的错误尝试后锁定帐户
5. 网络窃听
   - 防范方法 ：所有连接和传输都需要SSL/TLS
6. 恶意软件
   - 防范方法 ：严格访问控制，有限的网络IP访问，更改默认设置，加密

安全风险——访问数据库的恶意行为

1. 信息披露：获取信用卡及其他个人信息
   - 防御：数据和网络加密，执行更严格的访问控制
2. 拒绝服务：运行资源密集型查询
   - 防御：资源使用限制——设置各种限制包括最大连接、会话、超时，…
3. 提升权限：检索和使用管理员权限
   - 防御：更强的身份验证、访问控制、审计
4. 欺骗：检索并使用其他凭证
   - 防御：更强的帐户和密码策略
5. 篡改：更改数据库中的数据，删除事务记录
   - 防御：更严格的访问控制、审计、监控、备份

企业级
安全架构


■ 认证
•SSO – LDAP, AD, PAM, Native Kerberos, FIDO2, WebAuthn, MFA
■ 加密 屏蔽 & 脱敏
•非对称加密
•屏蔽
•替代/子集
•随机格式化数据
•黑名单数据
■ Workbench
•模型
•数据
•审计数据
•用户管理
■ 企业级监视
• 识别漏洞
• 安全加固策略
• 监控和警报
• 用户监控
• 密码监控
• 模式更改监控
• 备份监控
■ 访问控制
■ 防火墙
Users
■ 网络加密
■ 强认证
■线程池
•攻击最小化
■ 审计
•强大的规则引擎
■ 审计库
■ 密钥库
•保护密钥(KMIP, Rest APIs)
■数据加密
•TDE
•加密
•PKI
■ 企业级备份
•加密
■ HA
•Innodb Cluster
■ 访问
■ 预防
■ 检测
■ 恢复

Oracle 安全流程

- Oracle安全实践
  - 关键补丁更新、安全警报、公告
  - 在支持期间处理敏感的“私人/个人”信息
  - 源代码保护
  - 安全编码标准
  - 安全分析与测试
  - 员工筛选及教育
  - 架构安全性审查
  - 受信任的安装包存储库
- MySQL 安全性指南
- MySQL 提供安全性方面的知识库

MySQL的安全脆弱性

https://www.oracle.com/security-alerts/

Oracle公司提供的产品(MySQL)原则上是安全的，但有时会发现极其罕见的重大安全漏洞。甲骨文公司将迅速采取行动修复该漏洞，并最终发布安全信息，包括对漏洞的简要说明、由此带来的风险、避免方法和提供补丁的时间。

Critical Patch Updates

Critical Patch Updates are collections of security fixes for Oracle products. They are available to customers with valid support contracts. Starting in April 2022, Critical Patch Updates will be released on the third Tuesday of January, April, July, and October (They were previously published on the Tuesday closest to the 17th day of January, April, July, and October). The next four dates are:

- 18 July 2023
- 17 October 2023
- 16 January 2024
- 16 April 2024

阻碍升级的原因有哪些？

调查兼容性，应用对应处理麻烦…

能够正常运行的系统不要碰…

构建环境的人离职了，环境相关的工作搁置…

不打算使用InnoDB，继续使用MyISAM…

升级实施过程
降低予想外的风险

- 版本间的差异确认（关键字、参数、函数等）
- MySQL升级测试
- 应用程序测试
- 制定生产环境上线计划

MySQL 社区

- MySQL 社区背景
- MySQL社区提交代码
  - Oracle Contribution Agreement (OCA)
- MySQL 免费认证

MySQL社区背景

- 处理MySQL社区贡献流程
- 支持MySQL用户组https://dev.mysql.com/community/mug/
- 支持并参与第三方主办的活动https://dev.mysql.com/community/
- 制作培训视频
  - MySQL 短片
  - MySQL 入门系列
    - https://www.youtube.com/@mysql

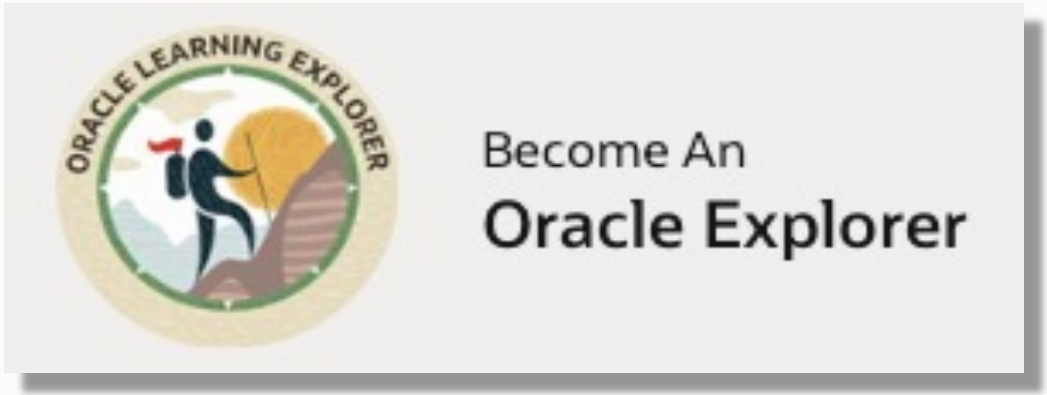
- MySQL RockStar Program
  - 奖励那些投入精力推广MySQL的最活跃的MySQL社区成员
  - 1st Edition: https://blogs.oracle.com/mysql/post/mysql-rockstars-2022
- MySQL ACE Program
  - 处理MySQL项目的ACE Program
  - https://ace.oracle.com/pls/apex/ace_program/r/oracle-aces/home

如何贡献MySQL的代码

- 成为MySQL开源项目贡献者社区的一员，
  ://forums.oracle.com/ords/apexds/post/contributing-code-to-mysql-8037
- 贡献者需要：
  - 希望改变/修复MySQL中的某些东西或有一个新功能
  - 下载 MySQL 代码http://dev.mysql.com/downloads/
  - 一个账户用于bugs.mysql.com http://bugs.mysql.com 或
  - GitHub t https://github.com
- 签署 Oracle Contribution Agreement (OCA) https://oca.opensource.oracle.com/
  - OCA是一个简短的法律协议，它保护贡献者和Oracle免受法律攻击。通过签署OCA，贡献者同意Oracle在法律上被允许在Oracle软件中使用贡献的代码，并且据贡献者所知，这些代码存在专利问题的阻碍

MySQL免费认证

- MySQL社区团队与Oracle大学合作，可以通过mylearn.oracle.com向与会者提供免费的培训凭证/积分，用户可以在指定时间段(2个月)内使用。
- 如果您感兴趣，请提供以下详细信息，MySQL社区将与您联系：
  - First name
  - Last name
  - Email Add
  - ress
  - Country
- https://education.oracle.com/



Contact Us

- **Find MySQL Community at:**
- MySQL Community Pages, https://dev.mysql.com/community/
- MySQL Slack, https://mysqlcommunity.slack.com
- The Oracle MySQL Blog, https://blogs.oracle.com/mysql/
- Planet MySQL, https://planet.mysql.com/
- LinkedIn, https://www.linkedin.com/groups/60715/
- Blog, https://lefred.be/
- MySQL Forums, http://lists.mysql.com/
- Discussion forums, http://forums.mysql.com


ORACLE