安华金和云数据库加密系统

用户手册

■**文档编号**	PM-2017-MysqlTDE-EnCloud-01	■**密级**	完全公开
■**版本编号**	V7.0.4	■**日期**	2017.04.4

■**适用性声明**

本模板用于撰写安华金和公司介绍、项目方案、商业计划书等

目录

一. 产品简介

安华金和针对客户对 MySQL 数据库的高安全性需求，提供云数据库加密系统（简称 DBCoffer-EnCloud）产品。安华金和云数据库加密系统使用透明加密技术，在不影响 MySQL 原有功能的基础上，实现对高敏感及重要文件的加密保护。能够主动保护内部的数据安全，对数据库系统进行有效的安全加固。

DBCoffer-EnCloud 基于用户的实际需求，使用 TDE(Transparent Data Encryption)透明加密技术，是一款高效的数据库防泄漏产品。能够实现对 MySQL 数据库中的敏感数据加密存储、访问控制增强功能。能够防止外部黑客攻击、防止内部运维人员窃取数据，从根源上防止敏感数据的泄露。

二. 特别说明

本产品共包含 MysqlTDE-TDE、MysqlTDE-Web 控制台 两部分，

MysqlTDE-TDE:

此镜像为 TDE 载体，以 **Mysql 5.6.35 的 RPM 版本为基础，通过对 InnoDB 引擎的改进，在不影响 Mysql 原有功能基础上，实现透明、高效的密文存储、增强的权限控制功能。**

MysqlTDE-Web 控制台

此镜像部署有安全服务和 Web 控制台，安全服务为后台运行，主要负责密钥的分配以及权限的控制，然后需要通过 Web 控制台来对安全服务初始化、启动、停止，license 管理，以及密钥管理、算法选择、权限分配等功能。

★ 其中 MysqlTDE-TDE 镜像完全依赖

MysqlTDE-Web 控制台镜像，二者缺一不可。

三. 产品部署

- 首先登录阿里云市场，然后搜索“云数据库加密系统（MysqlTDE）” 镜像，然后对搜索出的两个镜像分别进行购买部署，如下图所示：

用户初次访问产品，需首先通过安全管理员（secadmin）登录 Web 控制台配置相关系统信息，包括：安全服务、TDE 加密配置、权限设置等等。

如部署的两台 ECS 中间存在防火墙或其他访问控制，请打开以下端口

源服务器	目的服务器	端口	备注
MysqlTDE	Web 控制台	9200	TDE 与安全服务通讯端口

3.1 Web 管理端配置

- 购买镜像以后，在合适的客户端上打开浏览器，在地址栏内输入 Web 控制台的访问 IP 地址如： https://192.168.123.234 进入产品登录页面
- 安全管理员：secadmin 默认密码 secadmin1234

如下图所示：

初次登录需要对安全服务进行初始配置，如无特别要求，保持默认即可，过程如下

A）

B）


最大连接数
2048
句柄等待时间
14400
最大语句句柄
1024
继续
跳过

C）

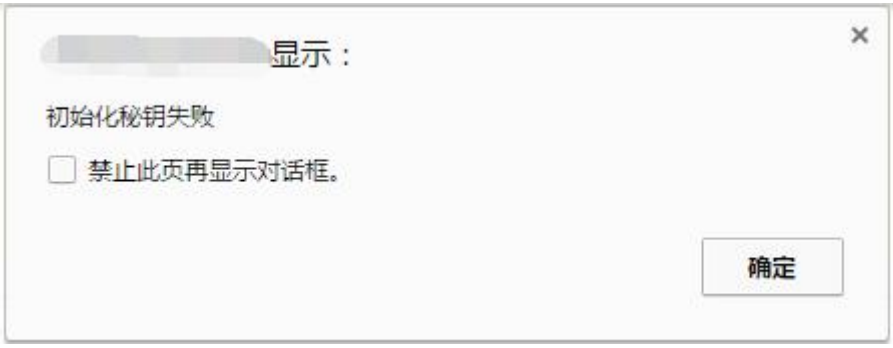

系统日志路径
/home/dbfw/dbcoffer/secu
系统日志大小
100
MB
异常日志路径
/home/dbfw/dbcoffer/secu
异常日志大小
1
MB
完成
跳过

3.2 安全服务初始化

通过 secadmin 用户登录 Web 控制台后，进入管理员页面，进入 “安全服务” 页面 在安全服务列表 中选择相应服务点击“...”-->“初始化密钥库”按钮，如下图所示：

在弹出的界面设置密码，密码规则为“数字+字母，十位及以上”，然后点击“确定”按钮，经过短暂等待至“初始化成功”，此步将以此密码为基础生成 主密钥，然后根据主密钥生成 65535 个加密密钥，在之后的 mysql 初始化时将从中随机选取一个作为加密密钥进行初始化，且每次 Mysql 初始化时获取的密钥不同，以保证数据的安全性，密钥丢失将造成数据不可恢复等严重后果，所以请妥善保存密钥（参看 3.6 节），如下图所示

如果密码复杂性不符要求，会弹出如下类似提示：



3.3 获取主机 ID

安全服务初始化以后，点击“查看主机 ID”按钮，输入初始化安全服务时设置的密码，点击“确定”按钮，将获取的主机 ID 发给厂商，厂商将提供 License 文件，如下图所示：

如果密码输入错误，或者未先进行初始化会出现如下类似错误提示，如已确定流程及密码无误，仍然出现错误，请联系厂商

3.4 导入 license

从厂商获取 License 文件以后，使用 secadmin 用户登录 Web 控制台，点击“导入 license”按钮，然后在弹出的窗口中输入初始化安全服务时设置的密码，点击“浏览”按钮并选择正确的 License 文件，点击“上传”按钮，提示成功并显示 license 信息，如下图所示：

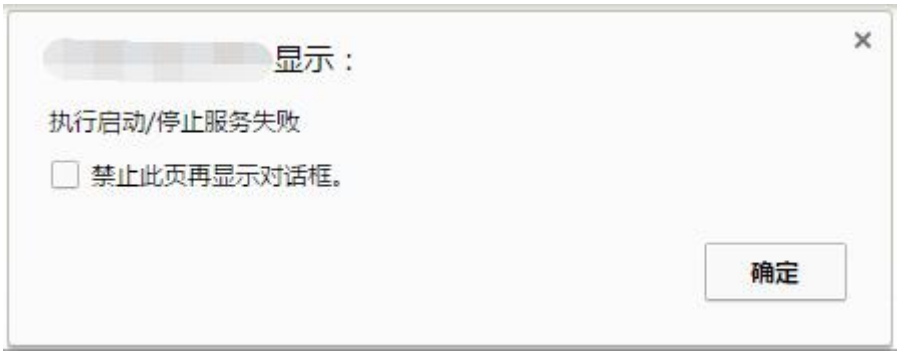
导入成功提示

如导入时报如下类似错误，请联系厂商更换 license 文件

3.5 启动安全服务

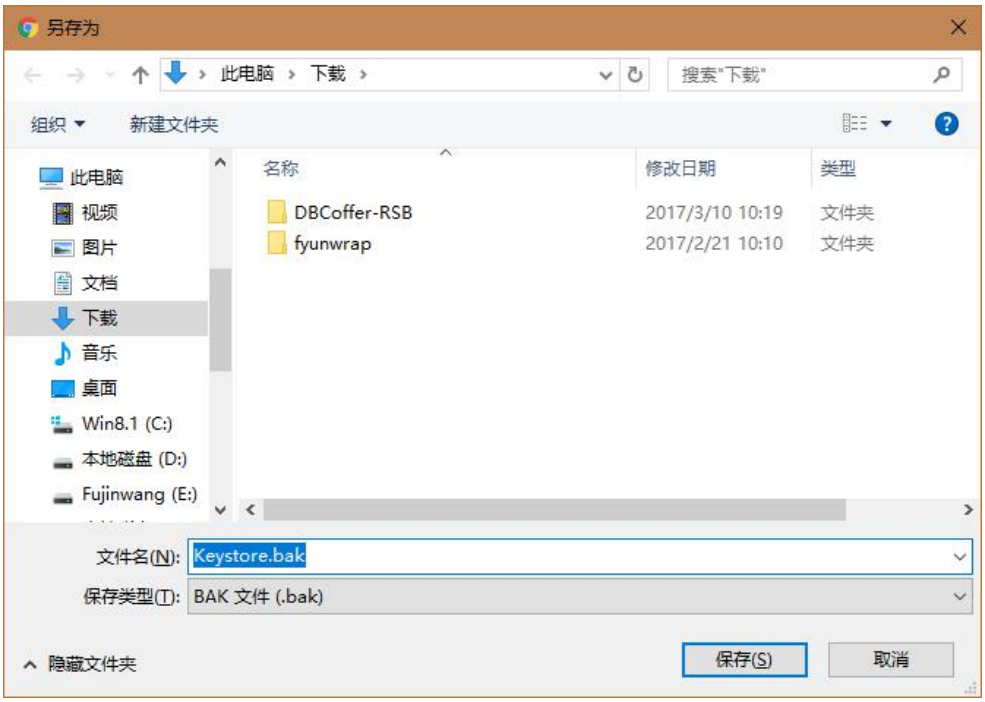
导入 license 以后，点击“停止/运行”按钮，然后在弹出的界面输入初始化安全密钥库时设置的密码，点击“确定”启动安全服务（初次启动时时间稍长，请耐心等待）至提示成功，如下图所示：

如果 license 文件过期会导致以下类似错误提示，请及时联系厂商更新 license



3.6 备份密钥库

安全服务在初始化后的第一次启动时需要备份密钥库，在安全服务界面 点击“备份密钥库”按钮，在弹出的界面输入初始化密钥库时的密码，点击“生成密钥库”按钮，稍等片刻，备份成功，点击“点击下载文件”可以选择本地路径进行保存，本密钥库极为重要，丢失可致数据无法恢复，请妥善保存，如下图所示



如果密码输入错误，会有“备份失败”错误，如确定密码输入无误请联系厂商处理

3.7 初始化 Mysql

购买镜像后，在合适客户端上使用 SSH 工具登录云数据库加密系统（MysqlTDE）服务器的 root 用户，镜像内为 rpm 默认安装，运行初始化脚本时添加安全服务地址即可

然后执行以下命令

[mysql@iZ2ze82zo6fcwepjv9h4ybZ ~]$ **mysql_install_db --datadir=/var/lib/mysql/ --defaults-file=/usr/my.cnf --user=mysql --innodb_master_secservice=172.16.0.31（Web 控制台的私有 IP 地址，见 3.2 节图片标记 IP）**

注：此命令只在初始化时执行，标蓝的部分根据实际情况进行调整，其中 innodb_master_secservice 参数值将写入云数据库加密系统（MysqlTDE）服务器的 /etc/secureServiceAPI.conf 配置文件下的 MasterServerIp 配置项下，如安全服务地址有变更可根据实际情况修改该项 IP 部分，端口部分请保持不变，否则会导致无法与安全服务通讯的错误，修改后 Mysql 需要重启。

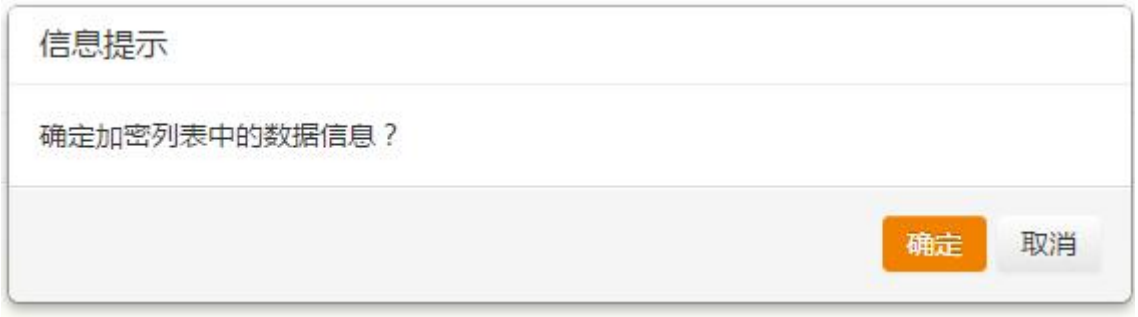
执行后会看到如下类似输出

```
[root@iz2ze1jtxhlmhdz5kimw40Z mysql]# mysql_install_db --datadir=/var/lib/mysql/ --user=mysql
WARNING: The host 'iz2ze1jtxhlmhdz5kimw40Z' could not be looked up with /usr/bin/resolveip.
This probably means that your libc libraries are not 100 % compatible
with this binary MySQL version. The MySQL daemon, mysqld, should work
normally with the exception that host name resolving will not work.
This means that you should use IP addresses instead of hostnames
when specifying MySQL privileges !

Installing MySQL system tables...2017-04-06 10:54:57 0 [Warning] TIMESTAMP with implicit DEFAUL
 (see documentation for more details).
2017-04-06 10:54:57 0 [Note] Ignoring --secure-file-priv value as server is running with --boot
2017-04-06 10:54:57 0 [Note] /usr/sbin/mysqld (mysqld 5.6.35) starting as process 3658 ...
[1] mysql load InnoDB_sec storage engined .
[2] InnoDB_sec storage engined load algorithm library ok .
/etc/secureServiceAPI.conf exists !
[3] InnoDB_sec storage engined start request algorithm id and crypt key .
```

此时登录 web 控制台界面》实例查询界面，会看到一条 MysqlTDE 内网 IP 的未初始化记录，如下图所示：

然后 为此数据库对应的记录选择加密设备及算法（当前只支持自带 SystemDevice 设备以及 MySQL 内置算法即 AES128 算法），点击保存，等待 mysql 初始化完成



当数据库初始化成功后出现类似如下显示，至此 Mysql 已初始化完毕，保持 MysqlTDE 和 Web 控制台正常运行，且二者之间通信正常，用户可按 Mysql 正常版本进行使用。

```
 --opt_bootstrap: 1
[4] InnoDB_sec storage engined with opt_bootstrap init data .
2017-03-18 11:24:28 1909 [Note] Binlog end
2017-03-18 11:24:28 1909 [Note] InnoDB: FTS optimize thread exiting.
2017-03-18 11:24:28 1909 [Note] InnoDB: Starting shutdown...
2017-03-18 11:24:30 1909 [Note] InnoDB: Shutdown completed; log sequence number 1625987
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

  /usr/local/mysql/bin/mysqladmin -u root password 'new-password'
  /usr/local/mysql/bin/mysqladmin -u root -h iZ2zec3pro7umjqa4yue3nZ password 'new-password'

Alternatively you can run:

  /usr/local/mysql/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:

  cd . ; /usr/local/mysql/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl

  cd mysql-test ; perl mysql-test-run.pl

Please report any problems at http://bugs.mysql.com/

The latest information about MySQL is available on the web at

  http://www.mysql.com

Support MySQL by buying support/licenses at http://shop.mysql.com

WARNING: Found existing config file /usr/local/mysql/my.cnf on the system.
Because this file might be in use, it was not replaced,
but was used in bootstrap (unless you used --defaults-file)
and when you later start the server.
The new default config file was created as /usr/local/mysql/my-new.cnf,
please compare it with your file and take the changes you need.

WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server
```

3.8 启动 Mysql

- TDE 对使用者来说完全透明，Mysql 初始化完成后用户即可根据自身实际情况使用数据库了，

  本节命令仅供参考

- 在适合客户端上使用 SSH 工具登录 ECS 服务器 root 用户，然后执行以下标红命令

```
[root@iZ2ze82zo6fcwepjv9h4ybZ ~]# service mysql start
```

设置用户密码及远程登录权限

```
[root@iZ2ze82zo6fcwepjv9h4ybZ ~]#  mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.6.35 Source distribution
Copyright (c) 2000, 2016, 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.
mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> update user set host='%' where host='localhost';
Query OK, 2 rows affected (0.00 sec)
Rows matched: 2  Changed: 2  Warnings: 0
mysql> update user set password=password('dbsec') where user='root';
Query OK, 4 rows affected (0.00 sec)（密码根据实际情况而定）
Rows matched: 4  Changed: 4  Warnings: 0
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
mysql> exit
```

3.9 数据加密

安华金和云数据库加密系统针对新建数据库和已有数据库采用两种加密方式。

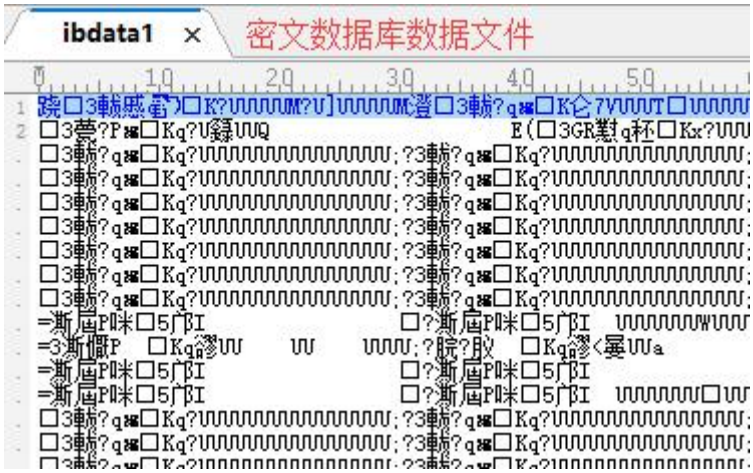
3.9.1 新建数据库加密

针对新建数据库，用户可以直接使用 Workbench ，Navicat for mysql……等数据库客户端连接 3.7 和 3.8 节设置的数据库，使用界面或脚本创建数据库，数据表等对象，创建以后插入的数据库即为密文数据。

如在加密数据库上创建如下数据表，并插入数据

```
CREATE TABLE t_coffer (ci INT,cv VARCHAR(100));
INSERT INTO t_coffer values(123,'teststr');
```

查看数据文件如下：



3.9.2 已有数据库加密

针对已有数据库，用户需使用 Workbench ，Navicat for mysql……等数据库客户端连接已有的明文数据库，将数据进行全部导出，然后再连接 3.7 和 3.8 节设置的数据库，将数据进行导入，数据导入以后即为密文数据。

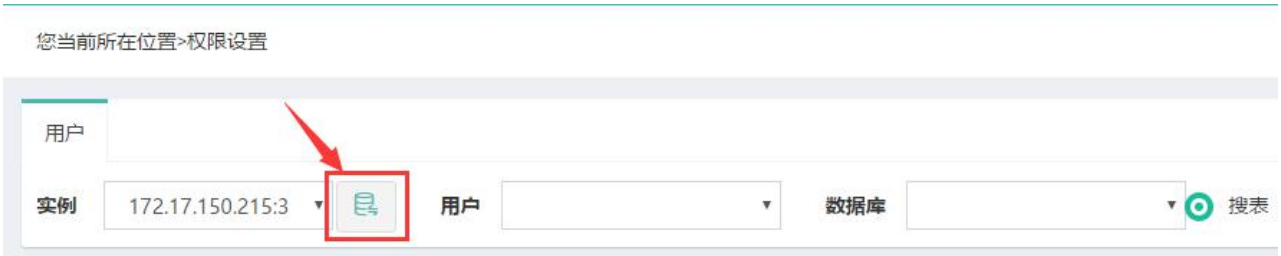
注：如用户将数据解密，则需反序进行，即：客户端工具连接密文数据库，将数据导出，然后导入明文数据库。

3.10 权限设定

权限设定可从“表权限设置”维度进行设置：

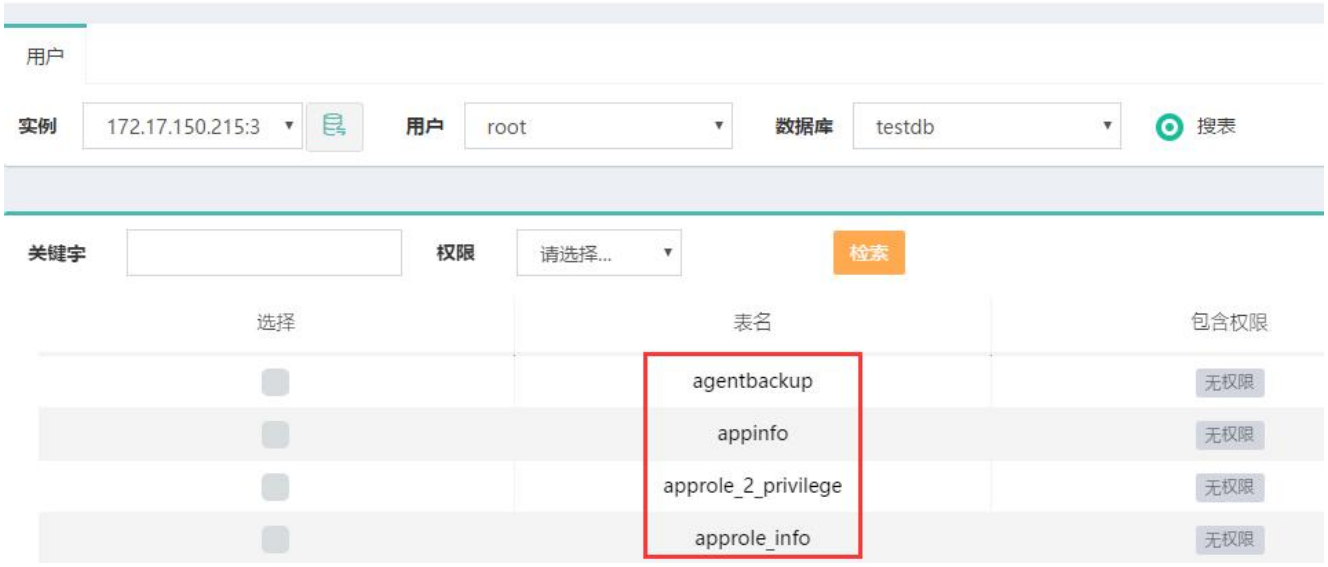
3.10.1 用户权限设置

使用 secadmin 登录 Web 控制平台，选择“权限设置”--->“同步” 标识(**注：数据表或用户有变化时请及时同步信息**)，



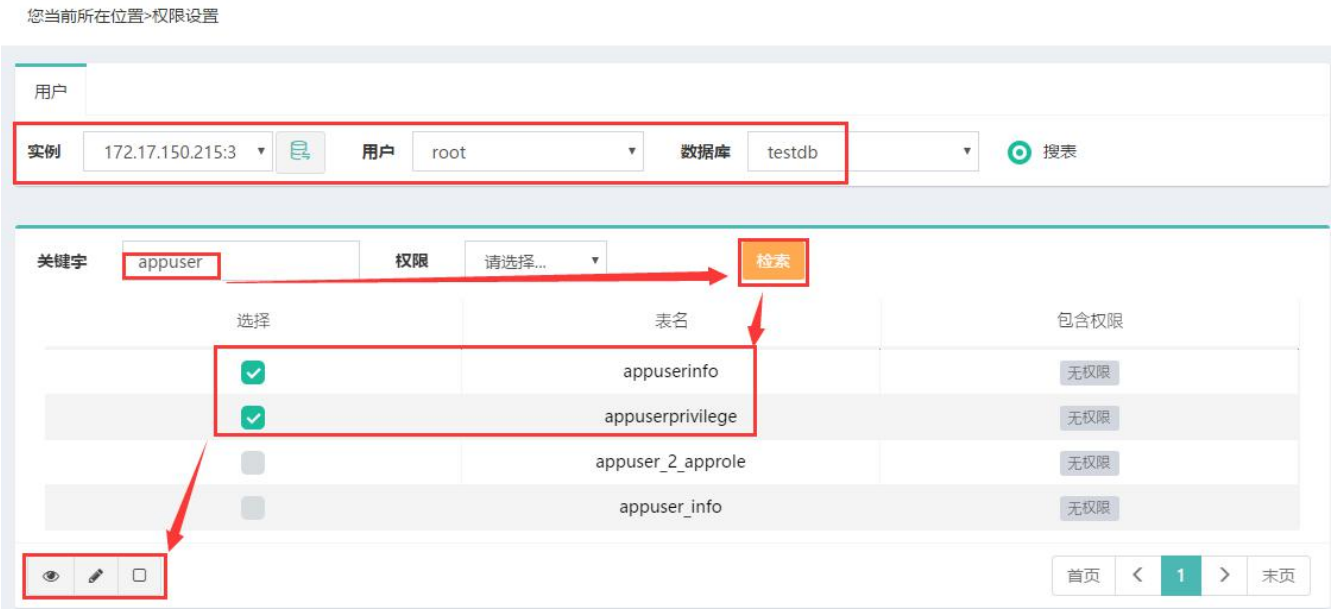
在弹出的界面输入密文数据库的用户名及密码，点击“确定” 按钮，然后将显示所有用户及数据库，然后点击“确定”按钮，同步到 Web 控制台，如下图所示：

您当前所在位置>权限设置



3.10.1.1 全部权限设定

同步数据库信息后，用权限设置界面，选定要设定权限的用户，然后可在“关键字”栏输入要设定的表名，选择表，及用户，可直接点击下方权限按钮进行全部权限设定



授权以后显示如下

如按上图设置权限，然后执行语句，将不能成功，报错如下：

3.11 删除实例

删除实例操作后，数据将不可恢复，请在删除前确保

A）导出所有数据

B）mysql 服务以停止

然后点击“删除”按钮并确定，状态如下所示

删除后点击“检索”按钮，确认已被删除