数据库加密

产品文档

文档目录

产品简介

产品概述

最近更新时间: 2019-11-22 19:48:41

云数据库加密系统是针对于云平台数据库的安全产品。在云平台环境下，应用系统的数据泄漏风险和篡改风险尤为突出。云数据库加密系统采用业界先进的密码算法，实现了基于密文的检索和运算，支持列级加密。
云数据库加密系统使用云加密机来管理用户密钥和提供密码运算。能够有效保护用户的密钥安全和运算安全。
云数据库加密系统提供透明模式和API模式两种部署方式，应用系统可灵活选择。其中透明模式对应用系统的代码几乎没有入侵，原则上只需要修改数据库的IP和端口号即可。API模式一般针对于新开发的业务系统，API和常规的数据库API用法相同。

功能优势

最近更新时间: 2019-11-22 19:48:41

- 支持在密文数据上进行精确查询、模糊查询、条件查询、排序和四则运算等常见操作
- 支持MAX/MIN/COUNT/AVG/SUM等SQL函数
- 支持列级加密
- 支持数据完整性校验，防止密文数据被恶意破坏
- 支持基于属性的加密和权限撤销树进行数据共享
- 数据库加密安全代理支持横向扩展

应用场景

最近更新时间: 2019-11-22 19:46:15

云数据库加密系统提供两种应用系统接入模式:

1) 透明模式：应用系统只需修改配置文件将数据库服务器的IP和端口号修改为云数据加密系统安全代理的IP和端口号即可。

2) API接入：对于新开发的应用系统，可采用API接入方式，直接将云数据加密系统作为应用系统模块进行集成。

推荐解决方案

最近更新时间: 2019-11-22 19:46:15

对于已经上线的应用系统，可使用云数据库加密系统提供的透明模式对应用系统数据进行加密，先将数据建表语句导出进行修改后建立新的密文数据库，再将数据批量导入密文数据库中，并修改应用系统访问数据库的ip与端口。
对于新开发的应用系统，可采用API接入方式，在数据交换层通过api接入数据库加密系统。

快速入门

最近更新时间: 2019-11-04 02:19:28

透明模式下，应用系统接入云数据库加密系统主要包括创建密文数据库、存量数据迁移和应用系统数据库配置这三个步骤。同时，云数据库加密还提供明文数据导出和密文数据导出功能。

操作指南

操作指南

最近更新时间: 2019-11-12 07:43:26

准备工作：部署数据库加密安全代理、导出应用系统明文建表语句和数据。

1.创建密文数据库

最近更新时间: 2019-11-27 16:59:13

在密文库下面创建密文数据表时，需要修改建表数据：

```
-- ----------------------------
-- Table structure for sign_user_release
-- ----------------------------
DROP TABLE IF EXISTS `sign_user_release`;
CREATE TABLE `sign_user_release` (
  `sign_id` int(11) NOT NULL AUTO_INCREMENT,
  `info_id` int(11) DEFAULT NULL,
  `user_id` int(11) DEFAULT NULL,
  `user_name` varchar(64) DEFAULT NULL,
  `sign_unit_id` int(11) DEFAULT NULL,
  `sign_unit` varchar(256) DEFAULT NULL,
  `sign_time` varchar(64) DEFAULT NULL,
  `sign_ip` varchar(64) DEFAULT NULL,
  `feed_back_user_id` int(11) DEFAULT NULL,
  `feed_back_time` varchar(64) DEFAULT NULL,
  `feed_back` text,
  `file_path` text,
  `keep_field` int(11) DEFAULT NULL,
  PRIMARY KEY (`sign_id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8
sqlEnd***$$$ 0,0,0,1,0,1,1,1,0,1,0,0,0;
```

在create语句尾部加上红线标注的语句。其中“sqlEnd***$$$”为加密标志，无实际意义。后面的“0,0,0,1,0,1,1,1,0,1,0,0,0”，每一位表示一个字段，“0,1,2”表示不同的加密方式。

0代表的是不加密;

1代表的是功能加密,密文可检索,运算;

2代表的完全加密,密文不可参与运算,不能作为查询条件。

2.存量数据迁移

最近更新时间: 2019-11-22 19:46:15

创建密文数据库完成后执行，两种方式：

1）将存量数据导出为insert脚本

通过数据库加密安全代理连接数据库执行脚本。（数据库工具和自己编写的工具均可）

2）数据库加密系统提供insert脚本导入工具：UploadScript.php(明文转密文工具)

用法：php UploadScript.php SourceData.sql

说明：SourceData.sql为明文数据Insert脚本，该工具执行后，将明文数据导入到密文数据库表中。

3. 应用系统数据库配置

最近更新时间: 2019-11-04 02:26:06

应用系统数据库链接的IP和端口修改为安全代理的IP和端口

4. 明文数据导出

最近更新时间: 2019-11-04 02:26:51

在应用系统退出云数据库加密时，数据库加密系统提供将密文数据库导出为明文的工具：DumpScript.php(密文转明文工具) php DumpScript.php dumpData /home/SourceData.sql 说明：dumpData 为需要导出的密文数据库名称，该工具执行后，将数据导出为明文Insert脚本SourceData.sql；

5. 密文数据导出

最近更新时间: 2019-11-04 02:27:26

密文数据导出：DBA或其他人员不通过数据库加密安全代理，直连数据库即可操作。

约束条件

最近更新时间: 2019-11-22 19:46:15

为应用系统更好的接入云加密数据库系统，对应用系统所使用的SQL语句存在着以下约束条件：

1）不支持在一个表达式里存在多个加密运算。建议应用系统对相关sql语句进行优化和拆分。（加法和减法算同一类加密运算、乘法和除法算同一类加密运算）

例如：select a*2+3 from t_table* （a2+3 存在加和乘两种）

select * from t_table where a+3=4 （a+3=4 存在加和精确两种）

2）不支持在聚合函数中进行加密运算。建议对sql进行拆分。

例如：select MAX(ad_money+2) from adtest1；（MAX(ad_money+2)存在max函数和加法运算）

select sum(ad_money+2) from adtest1；（sum(ad_money+2)存在sum函数和加法运算）

3）不支持不同加密算法列之间的运算和比较等。建议应用系统在设计列是否加密时充分考虑此条件。

例如：a列为明文，b列为功能加密，不论a、b在或不在同一张表中，a、b两列都不能在SQL语句中直接运算

select a + b from t_table （错误）

select * from t_table where a > b （错误）

select a, b from t_table （正确，a,b间没有运算关系）

select * from t_table where a>1 and b>2 （正确）

运维指南

最近更新时间: 2019-11-22 19:46:15

运维人员的日常工作包括：检查安全代理所在服务器资源消耗情况、检查安全代理进程状态和安全代理每天产生的日志。

安全代理日志错误说明：

1：CipherSQL is NULL! 此问题出现是sql重写失败，需要检查以下项：加密机是否连接失败，sql语法是否错误，是否有不支持的加密语句等。

2：Decstr is NULL! 此问题出现是结果集解密失败，需要检查以下项：加密后的结果集是否正确等。

3：ERROR 1064 (q_dun) 此问题出现是结果集解密失败，需要检查以下项：加密后的结果集是否正确等。

4：You have an error in your SQL syntax 此问题出现是sql重写失败，需要检查以下项：sql语法是否错误，是否有不支持的加密语句，表名列名是否正确等。 5：Malformed packet 此问题出现是mysql-router拼包错误，需要检查以下项：列属性是否正确，行id是否正确等。

故障处理

最近更新时间: 2019-11-22 19:46:15

用户在使用云数据库加密系统，常见的错误及原因分析如下：

1： You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use

near 'CipherSQL is NULL!' at line 1

报错：重写sql失败

原因：加密机连接失败，sql语法错误，不支持的加密语句等。

2： ERROR 1064 (q_dun): #T##E#

报错：解密错误

原因：函数名未识别，表名或者列名未识别等。

3：ERROR 2027 (HY000): Malformed packet

报错：mysql-router拼包错误

原因：列属性错误，行id错误等。

API 接口说明

最近更新时间: 2019-11-22 19:46:15

在API模式下，应用系统调用云数据库加密系统的API接口完成相关操作。示例代码如下：

1、 RewriteDDLSQL rewriteDDLSQL = new RewriteDDLSQL(); //创建rewriteDDLSQL对象

2、 String finalSQL = rewriteDDLSQL.rewrite(sql, "test"); //获取用户的明文sql语句，以及要使用云数据库加密系统的数据库名称。如本例中明文sql语 句为参数sql，使用的数据库名称为test。finalSQL为最终的密文SQL语句。

3、 PreparedStatement statementP = con.prepareStatement(finalSQL); //将重写之后的密文SQL语句交由jdbc的statement去执行。

4、 boolean fs = statementP.execute();

5、 ResultSet rs=statementP.getResultSet(); //获得的ResultSet rs是密文的结果集，将其与jdbc的connection一同赋予QinResultSet进行解密，获取明文结果集。

6、 QinResultSet qrs= new QinResultSet(rs, con); //qrs为解密之后的明文结果集。qrs的其他操作与普通的jdbc ResultSet操作相同。

上述示例内容中，1、2为云数据库加密系统提供的SQL语句重写及加密接口，调用这两个接口可将普通明文SQL语句重写为加密之后的密文SQL语句。中间3、4、5步骤与平时使用jdbc进行数据库连接操作相同，只是将原有的SQL语句sql更换为通过云数据库加密系统处理的密文SQL语句finalSQL即可。6为数据解密接口，负责将获得的密文结果集进行解密，并返回相同格式的明文结果集。