链滴

mysql 被人勒索比特比并删库

作者：limao
原文链接：https://ld246.com/article/1576721171359
来源网站：链滴

事情的经过是这样的,2019 年 8 月 22 日早上打开网站发现全部后台接口连接不上,看了下 console 报提示后台 500, 我又登录了下 xshell 看了下 日志 ,乖乖 半夜 2 点多以后数据库就连接不上了,打开 sqlyg 进去我都蒙蔽了, 我的库呢.....我的业务库一个都没有了,dev,prod 都没了,只留下一个库 " PLEASE_READ_ME_VVV " 点进去就留下一段话

To recover your lost Database and avoid leaking it: Send us 0.045 Bitcoin (BTC) to our Bitcon address 1McksxpysJGSG9a9zHvan5f8Y1nfpDbVYF and contact us by Email with your Server IP or Domain name and a Proof of Payment. Your Database is downloaded and backed up on our servers. Backups that we have right now: *. Any email without your server IP Address or Domain Name and a Proof of Payment together will be ignored. If we dont receive your ayment in the next 10 Days, we will make your database public or use them otherwise.

大概意思就是:

要恢复丢失的数据库并避免泄漏：请将 0.045 比特币（BTC）发送到我们的比特币地址 1Mcksxpysjgg9a9zhvan5f8y1nfpdbvyf，并通过电子邮件与您的服务器 IP 或域名和付款证明联系。您的数据库下载并备份到我们的 服务器 上。我们现在拥有的备份：*。任何没有您的服务器 IP 地址或域名和付证明一起的电子邮件都将被忽略。如果我们在未来 10 天内没有收到您的付款，我们将公开您的数据或使用它们。

上来我就百度加谷歌,一看大伙被黑的不止我一个我就放心了哈哈.

第一步：检测是否开启 MySQL 的 binlog

SHOW VARIABLES LIKE bin_log;

查询结果：

```
mysql> SHOW VARIABLES LIKE 'log_bin%';
+---------------------------------+-----------------------------------+
| Variable_name                   | Value                             |
+---------------------------------+-----------------------------------+
| log_bin                         | ON                                |
| log_bin_basename                | /www/server/data/mysql-bin        |
| log_bin_index                   | /www/server/data/mysql-bin.index  |
| log_bin_trust_function_creators | OFF                               |
| log_bin_use_v1_row_events       | OFF                               |
+---------------------------------+-----------------------------------+
5 rows in set (0.00 sec)
```

这一步至关总要，如果没有开启 binlog 的基本就不用看后面的步骤了。log_bin 是 ON 说明 MySQL 是开启了 binlog 的，总算是谢天谢地。从配置来看，log_bin_basename 的值是 /usr/local/var/mysql/master-bin 就是 Binlog 的基础文件名了。

```
mysql -uroot -p (wd: /www/server/mysql)
mysql> show master logs;
+------------------+-----------+
| Log_name         | File_size |
+------------------+-----------+
| mysql-bin.000010 | 318489974 |
| mysql-bin.000011 |       154 |
+------------------+-----------+
2 rows in set (0.00 sec)
```

原文链接：mysql 被人勒索比特比并删库

目录里面有个叫 binlog.000001 的文件，这个就是我服务器数据库的二级制日志了，这个二进制日是一个记录我们数据库所有操作的日志，所以原则上来说是可以直接恢复表的。

第二步：利用 binlog 手动恢复数据

如果整个数据库被删除，那么binlog就必须从数据库创建到被删除保持完整，比如说，我是上个月号开始创建名为mine的数据库和名为blog的表，那么binlog就需要从上周创建开始一直到现在都必存在，假设你是这个月一号才开启的binlog就比较麻烦了，好在我的数据库是一直开启的。

利用 mysqlbinlog 命令恢复数据库

进入到 master-bin.000001 的目录然后执行：

```
mysqlbinlog --start-datetime='2019-01-01 00:00:00' --stop-datetime='2019-06-24 10:30:00' b
nlog.000001 | mysql -uroot -p
```

然后基本就恢复七七八八了,我大概恢复了百分之90左右,剩下额自己手动不齐了下字段,基本数据都回了.

通过这个事情总结如下

1. mysql 端口不要使用默认端口(其实开源的中间件最好都不要用默认端口)
2. 如数据库这样的重要开源软件,不要暴漏在公网上,如果非要通过外网访问,记得加ip白名单
3. 数据库用户加权限 root 用户强烈只能host访问(感觉目前用root 当用户的人 挺多的)