



Do you

**“GRANT ALL PRIVILEGES”**

*... in MySQL/MariaDB?*

*DevOps Engineer*

**Gabriel PREDA**

[gabriel@e-radical.ro](mailto:gabriel@e-radical.ro)  
@eRadical



# DevOps = new BORG

*DevOps Engineer ???*

- *Development*
  - *Web Applications* (“Certified MySQL Associate”, “Zend Certified Engineer”)
  - *Real Time Analytics*
- *Operations*
  - ***MySQL DBA (15+ instances)***
  - *Sysadmin (<25 virtual & physical servers)*



# My MySQL MariaDB(s)

*Over 15 MariaDB / TokuDB instances*

- *Statistics in MariaDB*
  - *< 1TB from Oct 2012*
  - *< 12G raw data daily*
  - *< 12,000,000 events processed daily*
  - *< 90,000,000 rows added daily*

*BigData?*

*NO!!!*

- *I can copy all of that to my laptop*
- *“Working data set” - less than 1G & less than 7,500,000 rows*



# MySQL History

- 1983 – first version of **MySQL** created by **Monty Widenius**
- **1994 – MySQL is released OpenSource**
- 2004 Oct – **MySQL 4.1 GA**
- 2005 Oct – InnoDB (Innobase) is bought by Oracle – Black Friday
- 2008 Jan – MySQL AB is bought by Sun (1bn \$)
- 2008 Nov – **MySQL 5.1 GA**
- 2009 Apr – Sun is bought by Oracle (7,4 bn \$)
- 2010 Dec – **MySQL 5.5 GA**
- 2012 Apr – **MariaDB 5.5 GA**
- 2013 Feb – **MySQL 5.6** – first version made by Oracle
- **2013 Feb – MySQL will be replaced by MariaDB in Fedora & OpenSuSE**

\* Max Mether – SkySQL “MySQL and MariaDB: Past, Present and Future”



# where are we now?

Drizzle

MySQL  
(Oracle)

TokuDB  
(Tokutek)

Percona Server  
(Percona)

MariaDB  
(Monty Program,  
MariaDB Foundation)

Brighthouse  
(Infobright)

Replication:

- Asynchronous
- Semi-synchronous
- Galera Synchronous (Codership)
- Tungsten Replication (Continuent)

InfiniDB  
(Calpont)



# **Elementary...**

**"Elementary, my dear Watson"**

**Sir Arthur Conan Doyle never wrote that!**



# Elementary ?

OS Level:

- *is .bash\_history your friend?*

MySQL – *the client*

- *Is .mysql\_history your friend?*
- *LOAD DATA LOCAL* – set “local-infile=0”

DoS

- `test` database – *create table & write – disk space: 0% :)*
- *select \* from CHARACTER\_SETS a, CHARACTER\_SETS b, CHARACTER\_SETS c, ... 39^6 = 3,518,743,761 rows*
- *SELECT REPEAT('a', 1024\*1024) INTO @a01; ..... @a99;*



# Elementary ?

## MySQL – the server

- *Data files*
  - *Issue: behavior by “storage engine” (MyISAM, InnoDB, CSV, ...)*
- *Slow query log*
- *General log* – *Use general log for a detailed record of users activity*
- *Error log* – *monitor error log for failed logins (log\_warnings = 2)*
- *Binary log*
  - *hash passwords for grants outside*
  - *cycle faster – expire\_logs\_days=0 – “It's not our defaults”*
  - *Statement || Row Based Replication – it really does not matter!*
- *Relay logs – no control – ouch!*
- *Are you using SSL?*
- *Have a documented policy & follow it*
- *Over 20 security privileges*



# Elementary ?

## MySQL – the server

- “old-passwords” – 4.1 hashing – use “**secure-auth**”
- skip-symbolic-links - DATA\_DIRECTORY
- max\_connect\_errors (default is 10)
- skip-grant-tables – really?
- skip-name-resolve – not in the era of API aware DNS servers!
- skip-networking – how do you do that in the cloud?
- bind-address=127.0.0.1 – is not very helpful
- secure\_file\_priv=/path/
- Authentication interface
  - Oracle commercial plugins
    - PAM Plugin
    - Windows Native Authentication Plugin
  - Percona PAM Plugin – since 2011



# Application Security

- SQL Injections – ~~mysql\_real\_escape\_string()~~
- Prepared Statements
- An App can have more than 1 user. Really! I'm not kidding!
- ... and more than one SCHEMA! SoC? Anybody?

## PHP

Use a newer decent API:

- MySQL – ~~mysql\_connect()~~
- PDO – new PDO();
- MySQLi – new mysqli();
- ORM! Ever heard?



For the Love of God  
Damien Hirst  
2007

# GRANT ALL PRIVILEGES

Do you?

GRANT ALL PRIVILEGES

ON \*.\*

TO 'some\_user'@'%'

IDENTIFIED BY 'thisIsTheActualPassword'

WITH GRANT OPTION;

FLUSH PRIVILEGES;

Please don't!



GRANT

priv\_type  
[(column\_list)]

[, priv\_type  
[(column\_list)]] ...

ON [object\_type]  
priv\_level

TO user\_specification  
[, user\_specification] ...

[REQUIRE {NONE |  
ssl\_option [AND]

user\_specification:

user

[

  | IDENTIFIED BY [PASSWORD] 'password'  
  | IDENTIFIED WITH auth\_plugin [AS 'auth\_string']  
]

ssl\_option:

SSL

X509

CIPHER 'cipher'

ISSUER 'issuer'

SUBJECT 'subject'

with\_option:

GRANT OPTION

MAX\_QUERIES\_PER\_HOUR count

MAX\_UPDATES\_PER\_HOUR count

MAX\_CONNECTIONS\_PER\_HOUR count

MAX\_USER\_CONNECTIONS count

# GRANT ALL PRIVILEGES

- Don't use % in host part or use it wisely:
  - 11.22.33.% - still too many can connect
  - 11.22.33.4\_ - now only 10
- SUPER must die
- Username limited to 16 chars
- Use limits for a user:
  - MAX\_QUERIES\_PER\_HOUR
  - MAX\_UPDATES\_PER\_HOUR
  - MAX\_CONNECTIONS\_PER\_HOUR
  - MAX\_USER\_CONNECTIONS

# GRANT ALL PRIVILEGES

- mysql\_secure\_installation script
- SecuRich – RBAC for MySQL
- Percona Toolkit - pt-config-diff, pt-deadlock-logger, pt-heartbeat, pt-kill, pt-show-grants
- Start using SSL
  - No revocation
  - No pure SSL port
  - 5 to 16% performance penalty



# Backups

- Where are they stored?
  - In the cloud?
- Encrypted?
- Logical vs. Physical, full vs. incremental
- Products:
  - MySQL Enterprise Backup – commercial
  - mysqldump
  - Percona XtraBackup
    - Now with encryption

# Forks or !Forks

- Drop in replacements:
  - Percona Server – XtraDB
  - MariaDB – lot's of features
    - Extended User Statistics — 5.2
    - KILL all queries for a user — 5.3
    - Pluggable Authentication — new in 5.2
    - slow query log has more information about the query
    - Long comments which start with /\*MI

# Replication

- Is «a slave» «a backup» ?
- GRANTs
  - REPLICATION CLIENT - Enable the user to ask where master or slave servers are
  - REPLICATION SLAVE - Enable replication slaves to read binary log events from the master
- Must open port between Master & replica
- Monitor the replication threads:



# Replication

- Asynchronous
- Semi-synchronous (MySQL 5.5)



# Replication

## Galera synchronous (Codership)

- Multi-master, automatic node joining & lots of other goodies... but uses:
  - extra port: 4567
  - mysqldump, rsync/rsync\_wan
  - Might need to turn off SELinux, AppArmor
- SSL from 0.8.2
- Available as/in:



# Replication

## Tungsten Replicator (Continuent)



Universal translator – TOS: “Metamorphosis”



# Replication

## Tungsten Replicator (Continuent)

MySQL -> Oracle

MySQL -> Amazon RDS

MySQL -> PostgreSQL

MySQL -> MongoDB

PostgreSQL -> MySQL

Oracle -> MySQL

MySQL -> MySQL

PostgreSQL -> PostgreSQL

Oracle -> Oracle

But:

- More apps: ruby, tar, java
- More ports:
  - 2112 - Port for replication THL
  - 10000 - Listener port for the replicator
  - 10001 - Listener port for the replicator
- You need an executable TMP dir (in case you have noexec on the current one)
- May need sudo – to start/stop mysql instance

# new Stuff();

- If you have „N” servers
- HaProxy
  - breaks MySQL's privilege system
- Puppet
  - All that power handled to... who?
- Cloud



???

Is that all?

No way!

But is enough for today!

# Mentions

- Company/Project website
- MySQL Manual – [dev.mysql.com/doc/refman/5.\[156\]](http://dev.mysql.com/doc/refman/5.1/5.6)
- yaSSL – with a focus on SSL - Chris Conlon
- Securing MySQL for a Security Audit Presentation - Brian Miezejewski
- MySQL Security - Domas Mituzas
- MySQL Security, Privileges & User Management – Kenny Gryp – Percona Live 2012
- Why Are Databases So Hard To Secure? - Sheeri Kritzer Cabral
- Google-Hacking MySQL and More MySQL Security - Sheeri Kritzer Cabral
- **OurSQL: The MySQL Database Community Podcast -**  
**<http://www.oursql.com> - Sheeri Kritzer Cabral & Gerry Narvaja**



# Questions ?

