



Do you

"GRANT ALL PRIVILEGES"

... in MySQL/MariaDB?

DevOps Engineer

Gabriel PREDA

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 MySQLMariaDB(s)

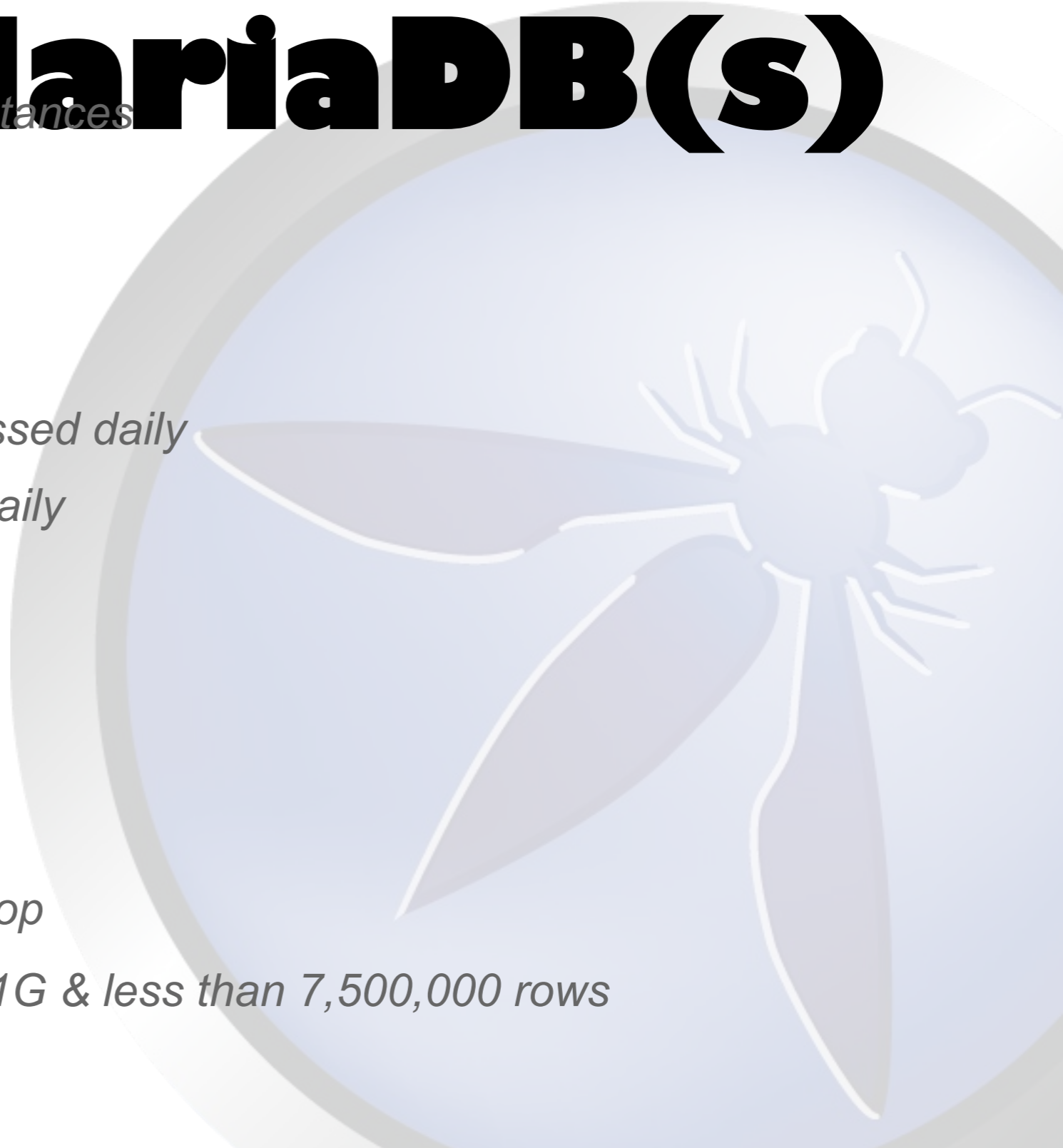
Over 15 MariaDB / TokuDB instances

- *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 Wideniuns**
- **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)

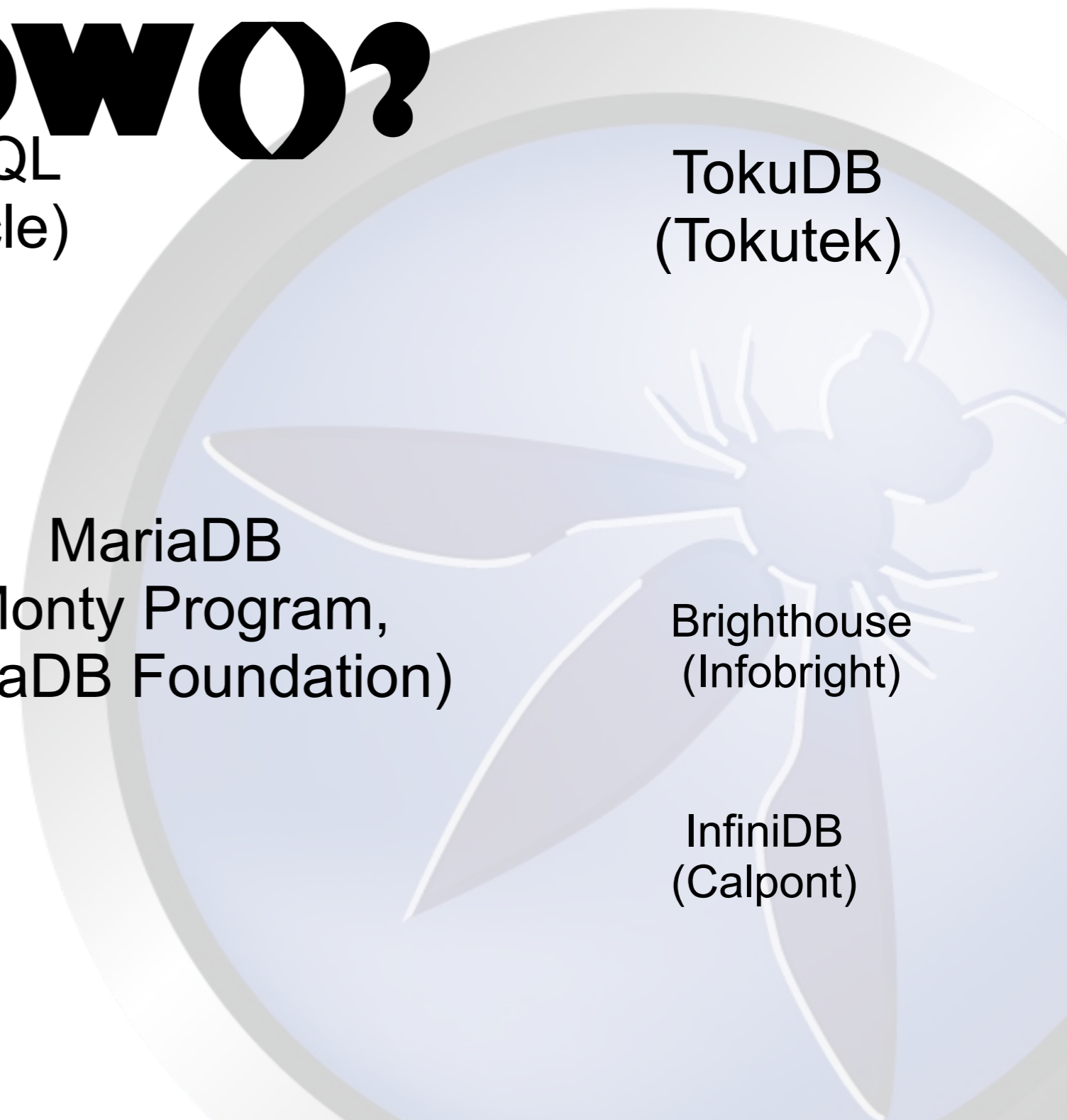
MariaDB
(Monty Program,
MariaDB Foundation)

BrightHouse
(Infobright)

Replication:

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

InfiniDB
(Calpont)

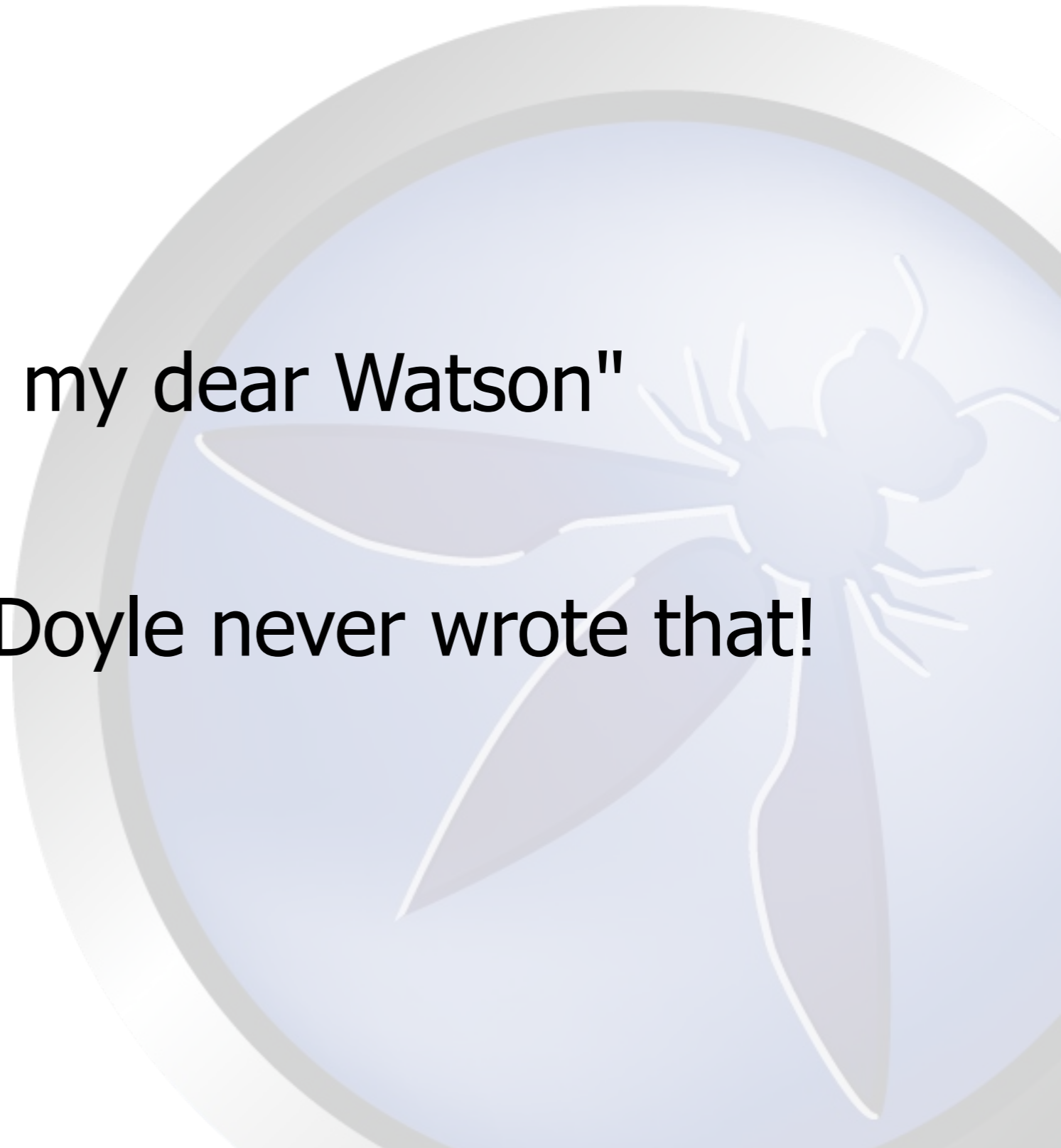




Elementary...

"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 ?

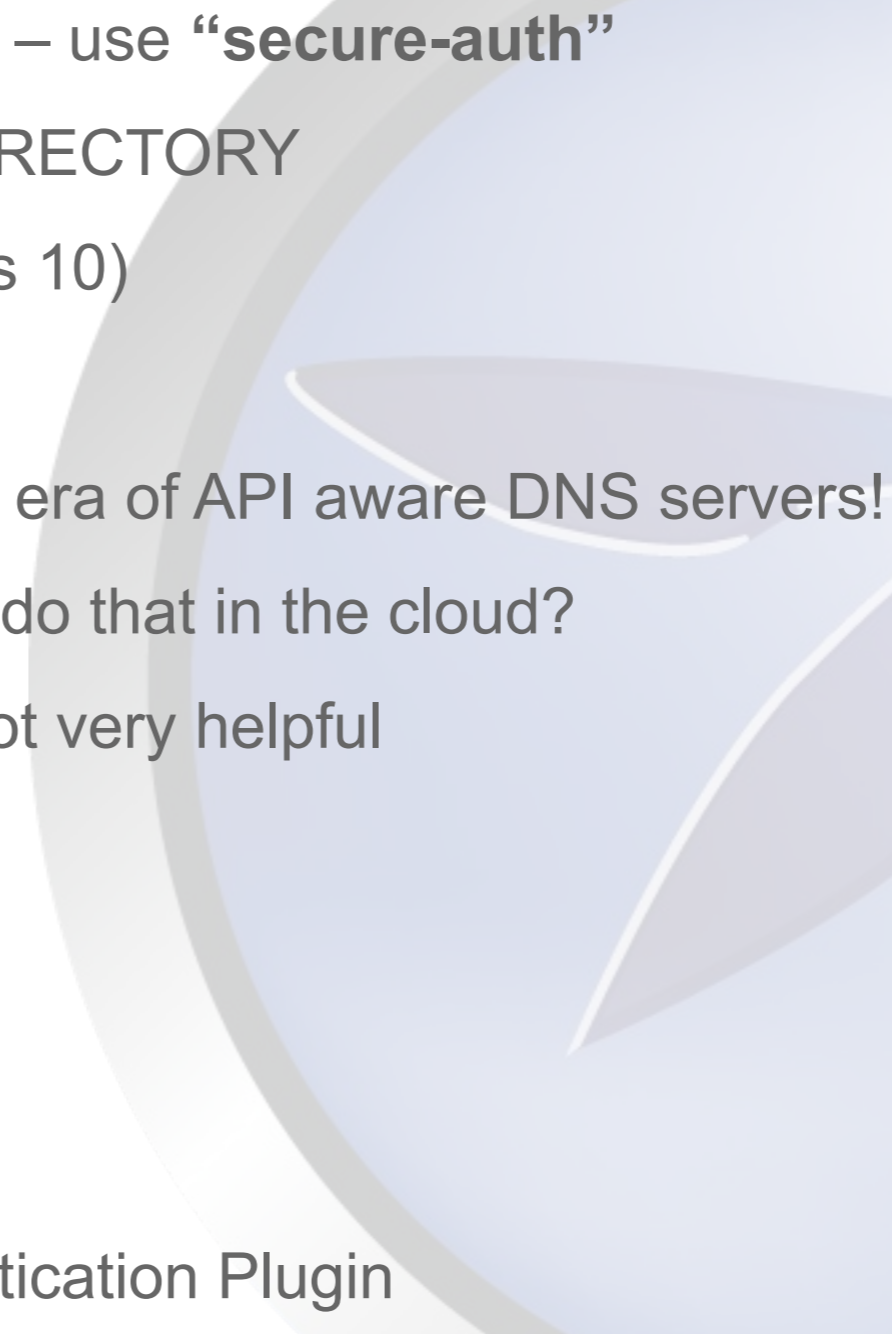
MySQL – the server

- *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?

<http://www.php.net/manual/en/mysqlinfo.api.choosing.php>



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 ALL

GRANT PRIVILEGES

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

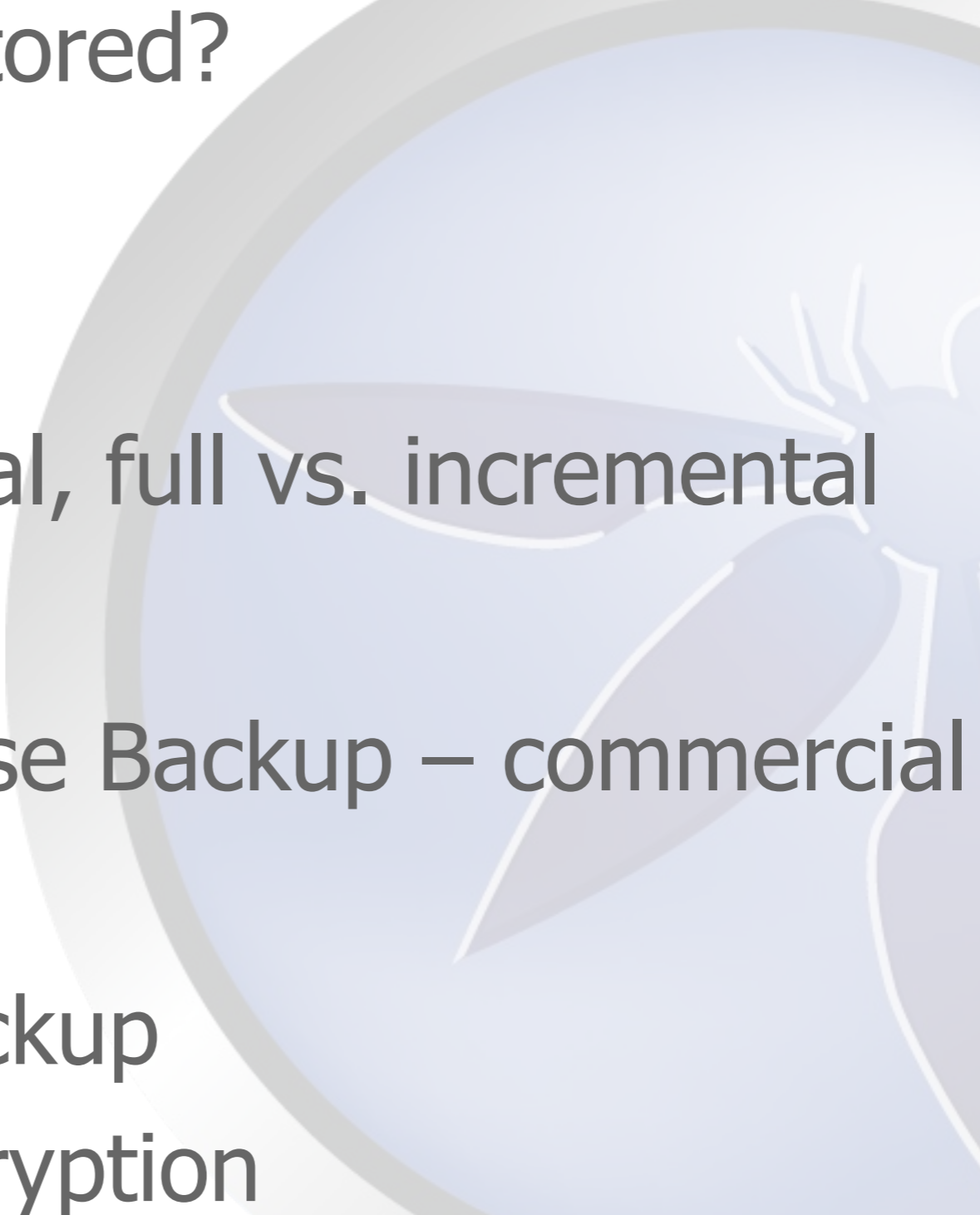


GRANT ALL PRIVILEGES

- 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
- 

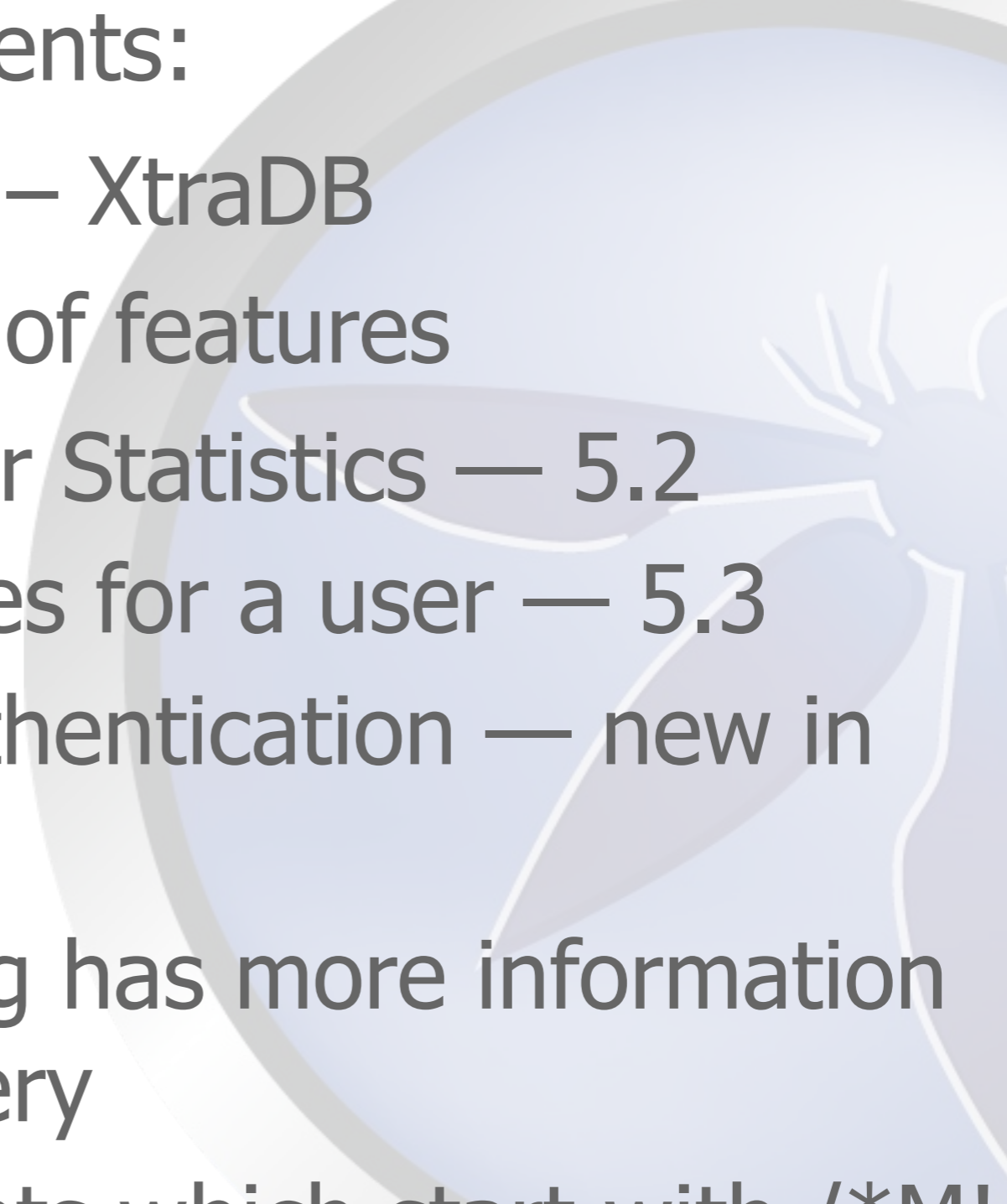


Backups

- 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:
- 



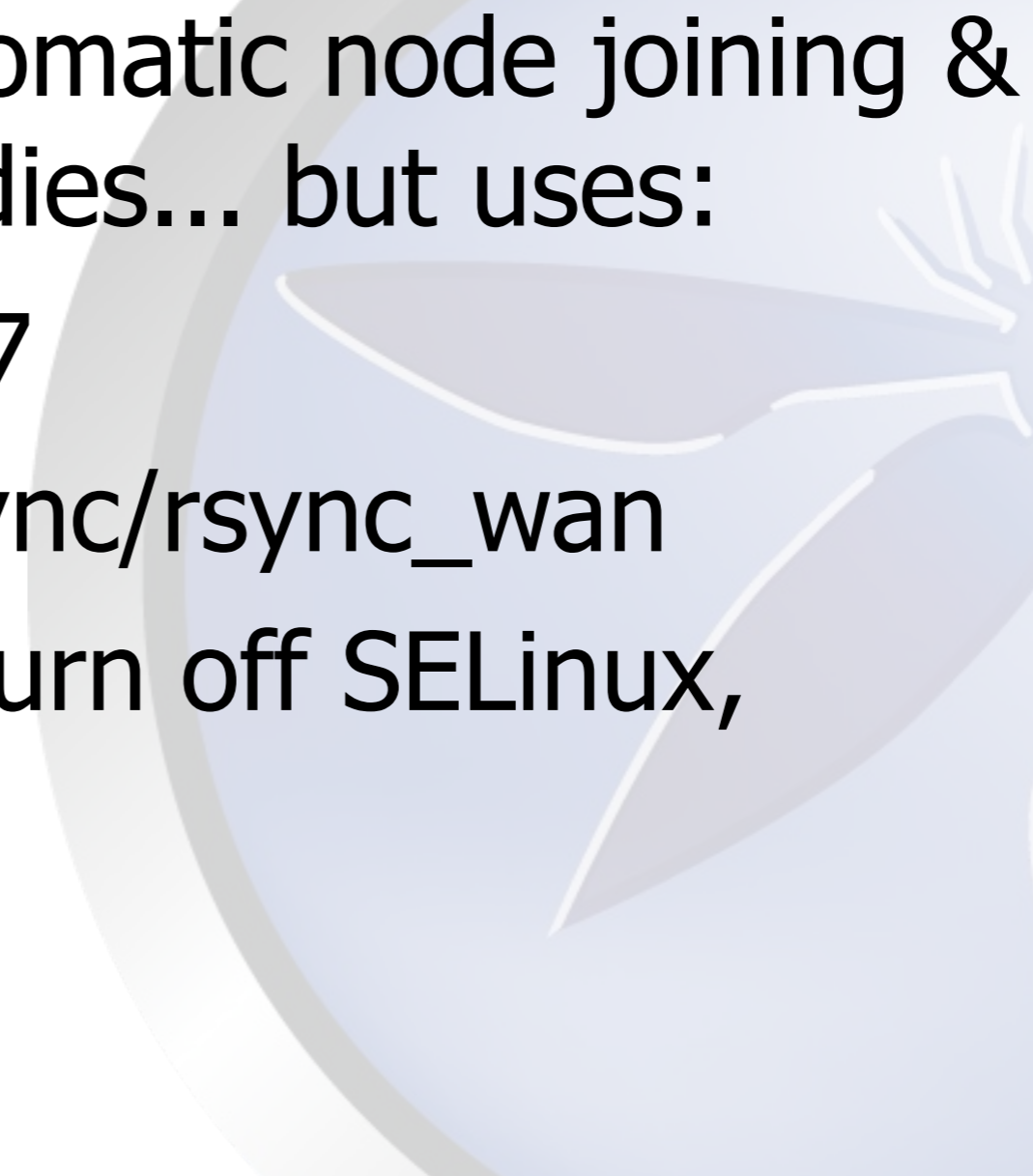
Replication

- Asynchronous
 - Semi-synchronous (MySQL 5.5)
- 



Replication

Galera synchronous (Codershhip)

- 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

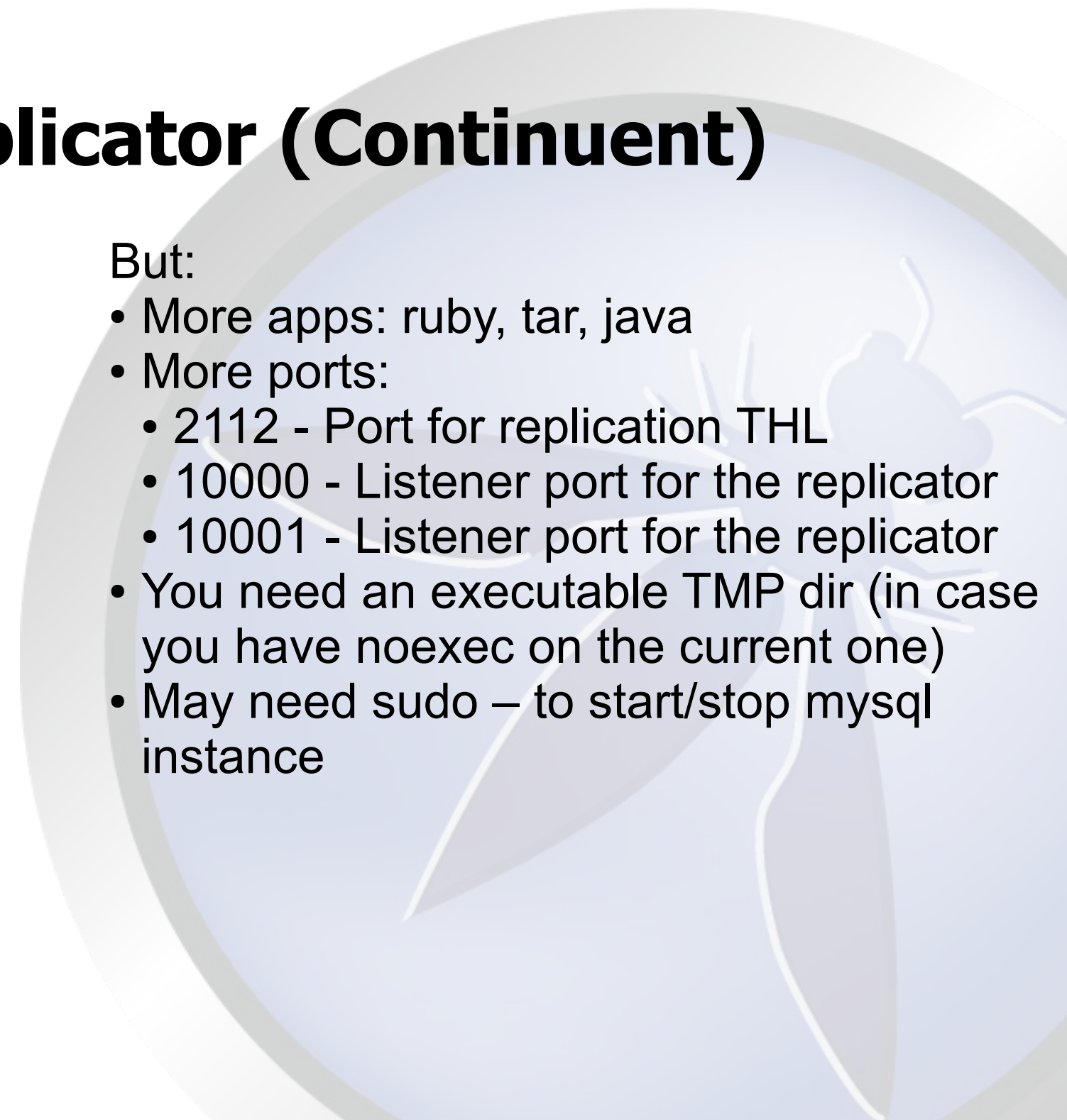
Tungsten Replicator (Continuent)

MySQL -> Oracle
MySQL -> Amazon RDS
MySQL -> PostgreSQL
MySQL -> MongoDB

PostgreSQL -> MySQL
Oracle -> MySQL

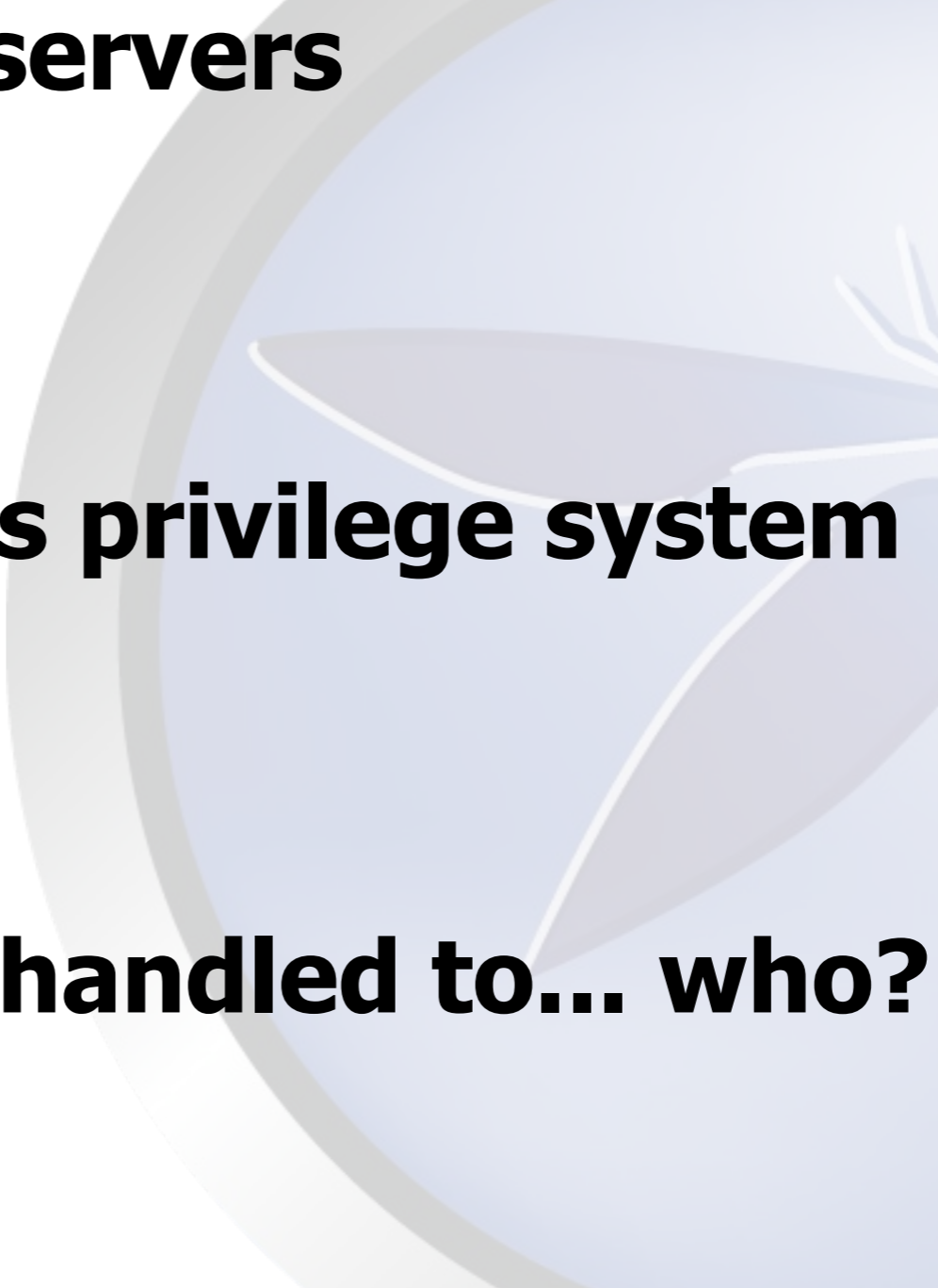
MySQL -> MySQL
PostgreSQL -> PostgreSQL
Oracle -> Oracle

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();

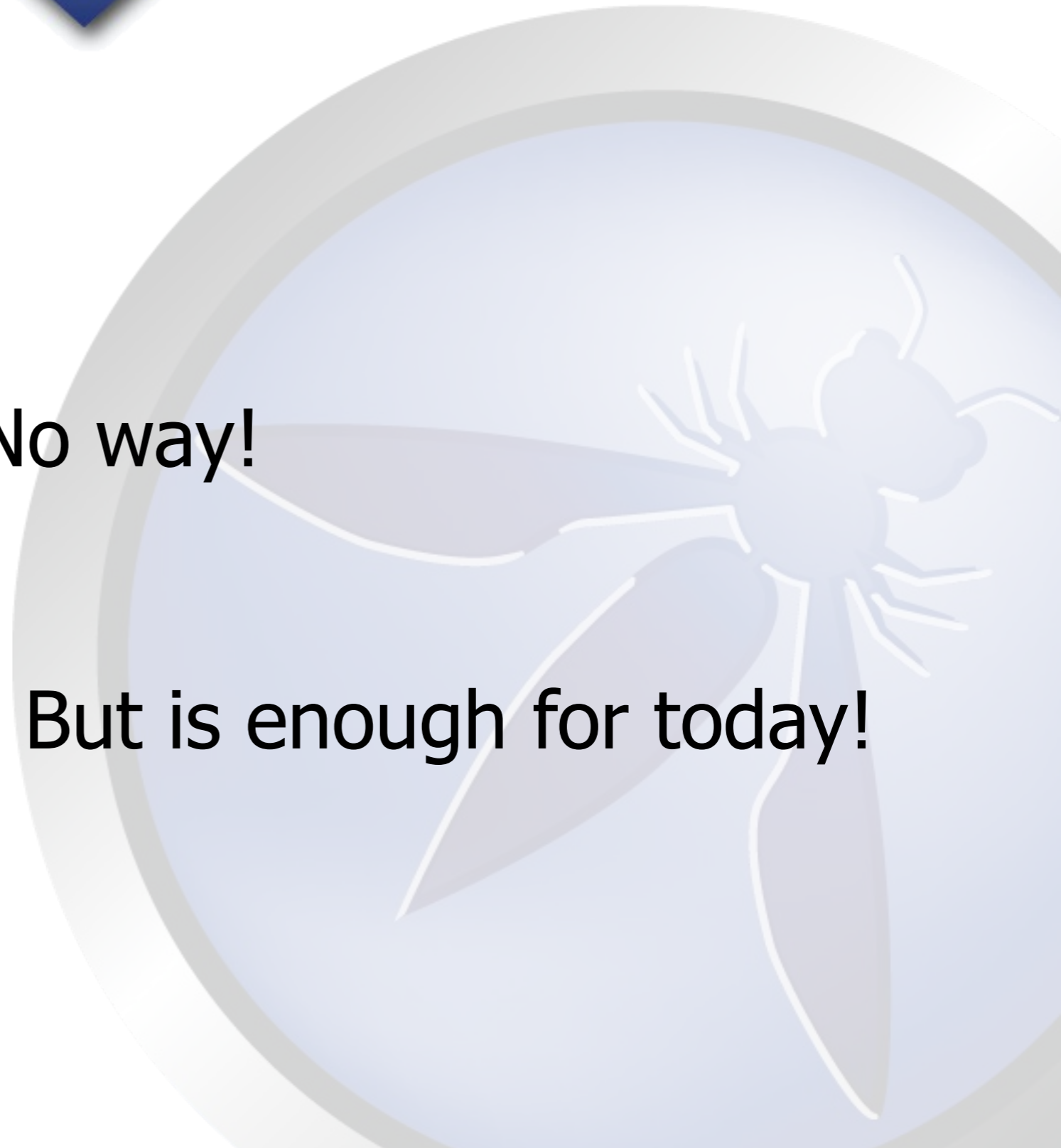
- **If you have „N” servers**
 - **HaProxy**
 - **breaks MySQL's privilege system**
 - **Puppet**
 - **All that power handled to... who?**
 - **Cloud**
- 



Is that all?

No way!

But is enough for today!





Mentions



- Company/Project website
- MySQL Manual – dev.mysql.com/doc/refman/5.[156]
- yaSSL – with a focus on SSL - Chris Conlon
- Securing MySQL for a Security Audit Presentation - Brian Mizejewski
- 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 ?

