Installation sur Debian

Installation

L'installation se fait via apt

```
sudo apt-get update
sudo apt-get install mysql-server
```

Apres l'installation, deux utilisateurs sont crée dans le fichier debian.cnf

```
sudo cat /etc/mysql/debian.cnf
# Automatically generated for Debian scripts. DO NOT TOUCH!
[client]
host     = localhost
user     = debian-sys-maint
password = JOmSbYCrYAn2NmLY
socket   = /var/run/mysqld/mysqld.sock
[mysql_upgrade]
host     = localhost
user     = debian-sys-maint
password = JOmSbYCrYAn2NmLY
socket   = /var/run/mysqld/mysqld.sock
```

Ce qui donne après connexion:

```
pilou@pilou-pc:~$ mysql -u debian-sys-maint -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.20-0ubuntu0.19.10.1 (Ubuntu)
```

La configuration du serveur est dans /etc/mysql avec deux repertoire 1 pour la configuratoin serveur et 1 pour le client:

```
#
# The MySQL database server configuration file.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html

# Here is entries for some specific programs
# The following values assume you have at least 32M ram

[mysqld]
#
# * Basic Settings
#
user            = mysql
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
# port          = 3306
# datadir       = /var/lib/mysql


# If MySQL is running as a replication slave, this should be
# changed.  Ref https://dev.mysql.com/doc/refman/8.0/en/server-system-
variables.html#sysvar_tmpdir
# tmpdir                = /tmp
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 127.0.0.1
#
# * Fine Tuning
#
key_buffer_size         = 16M
# max_allowed_packet    = 64M
# thread_stack          = 256K
```

```
# thread_cache_size       = -1

# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
myisam-recover-options  = BACKUP

# max_connections        = 151

# table_open_cache       = 4000

#
# * Logging and Replication
#
# Both location gets rotated by the cronjob.
#
# Log all queries
# Be aware that this log type is a performance killer.
# general_log_file        = /var/log/mysql/query.log
# general_log             = 1
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
#
# Here you can see queries with especially long duration
# slow_query_log                = 1
# slow_query_log_file   = /var/log/mysql/mysql-slow.log
# long_query_time = 2
# log-queries-not-using-indexes
#
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see README.Debian about
#       other settings you may need to change.
# server-id             = 1
# log_bin                       = /var/log/mysql/mysql-bin.log
# binlog_expire_logs_seconds    = 2592000
max_binlog_size   = 100M
# binlog_do_db          = include_database_name
# binlog_ignore_db      = include_database_name
```

Securisation

L'idée est d'avoir une base de sécurisation pour MySQL

```
pilou@pilou-pc:~$ sudo mysql_secure_installation utility

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: Y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Please set the password for root here.

New password:

Re-enter new password:

Estimated strength of the password: 50
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) :
Y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
```

```
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
Success.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y
Success.

All done!
```

Securisation Systeme

Installation de Lynis

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys
C80E383C3DE9F082E01391A0366C67DE91CA5D5F
sudo apt install apt-transport-https
sudo apt update
sudo apt install lynis
```

L'execution de Lynis permet de valider l'installation d'une machine

```
./lynis audit system

[ Lynis 3.0.0 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2020, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  19.10
  Kernel version:            5.3.0
  Hardware platform:         x86_64
  Hostname:                  pilou-pc
  ---------------------------------------------------
  Profiles:                  /home/pilou/lynis/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
```

```
  Plugin directory:           ./plugins
  ---------------------------------------------------
  Auditor:                    [Not Specified]
  Language:                   en
  Test category:              all
  Test group:                 all
  ---------------------------------------------------
  - Program update status...                                    [ NO UPDATE ]

[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: pam
    [..]
  - Plugin: systemd
    [................]

[+] Boot and services
------------------------------------
  - Service Manager                                             [ systemd ]
  - Checking UEFI boot                                          [ DISABLED ]
  - Checking presence GRUB2                                     [ FOUND ]
    - Checking for password protection                          [ NONE ]
  - Check running services (systemctl)                          [ DONE ]
        Result: found 32 running services
  - Check enabled services at boot (systemctl)                  [ DONE ]
        Result: found 59 enabled services
  - Check startup files (permissions)                           [ OK ]
  - Running 'systemd-analyze security'
        - ModemManager.service:                                 [ MEDIUM ]
        - NetworkManager.service:                               [ EXPOSED ]
        - accounts-daemon.service:                              [ UNSAFE ]
        - acpid.service:                                        [ UNSAFE ]
        - alsa-state.service:                                   [ UNSAFE ]
```

- anacron.service: [UNSAFE]
- apport.service: [UNSAFE]
- avahi-daemon.service: [UNSAFE]
- bluetooth.service: [MEDIUM]
- cron.service: [UNSAFE]
- cups-browsed.service: [UNSAFE]
- cups.service: [UNSAFE]
- dbus.service: [UNSAFE]
- dm-event.service: [UNSAFE]
- dmesg.service: [UNSAFE]
- emergency.service: [UNSAFE]
- getty@tty1.service: [UNSAFE]
- grub-common.service: [UNSAFE]
- haveged.service: [MEDIUM]
- irqbalance.service: [MEDIUM]
- kerneloops.service: [UNSAFE]
- lvm2-lvmpolld.service: [UNSAFE]
- mysql.service: [UNSAFE]
- networkd-dispatcher.service: [UNSAFE]
- ofono.service: [UNSAFE]
- ondemand.service: [UNSAFE]
- packagekit.service: [UNSAFE]
- plymouth-start.service: [UNSAFE]
- polkit.service: [UNSAFE]
- rc-local.service: [UNSAFE]
- rescue.service: [UNSAFE]
- rsync.service: [UNSAFE]
- rsyslog.service: [UNSAFE]
- rtkit-daemon.service: [MEDIUM]
- sddm.service: [UNSAFE]
- snapd.service: [UNSAFE]
- systemd-ask-password-console.service: [UNSAFE]
- systemd-ask-password-plymouth.service: [UNSAFE]
- systemd-ask-password-wall.service: [UNSAFE]
- systemd-fsckd.service: [UNSAFE]
- systemd-initctl.service: [UNSAFE]
- systemd-journald.service: [OK]
- systemd-logind.service: [OK]
- systemd-networkd.service: [OK]
- systemd-resolved.service: [OK]

```
        - systemd-rfkill.service:                                [ UNSAFE ]
        - systemd-timesyncd.service:                             [ OK ]
        - systemd-udevd.service:                                 [ EXPOSED ]
        - thermald.service:                                      [ UNSAFE ]
        - udisks2.service:                                       [ UNSAFE ]
        - unattended-upgrades.service:                           [ UNSAFE ]
        - upower.service:                                        [ OK ]
        - user@1000.service:                                     [ UNSAFE ]
        - uuidd.service:                                         [ OK ]
        - vboxadd-service.service:                               [ UNSAFE ]
        - whoopsie.service:                                      [ UNSAFE ]
        - wpa_supplicant.service:                                [ UNSAFE ]
```

Optimisation

l'outil mysqltuner permet de valider un fichier my.cnf

```
pilou@pilou-pc:~/mysqltuner$ perl mysqltuner.pl
 >>  MySQLTuner 1.7.19 - Major Hayden <major@mhtx.net>
 >>  Bug reports, feature requests, and downloads at http://mysqltuner.com/
 >>  Run with '--help' for additional options and output filtering

[--] Skipped version check for MySQLTuner script
Please enter your MySQL administrative login: debian-sys-maint
Please enter your MySQL administrative password: [OK] Currently running supported MySQL
version 8.0.20-0ubuntu0.19.10.1
[OK] Operating on 64-bit architecture

-------- Log file Recommendations
------------------------------------------------------------------
[OK] Log file /var/log/mysql/error.log exists
[--] Log file: /var/log/mysql/error.log(3K)
[OK] Log file /var/log/mysql/error.log is readable.
[OK] Log file /var/log/mysql/error.log is not empty
[OK] Log file /var/log/mysql/error.log is smaller than 32 Mb
[!!] /var/log/mysql/error.log contains 6 warning(s).
[!!] /var/log/mysql/error.log contains 3 error(s).
[--] 4 start(s) detected in /var/log/mysql/error.log
[--] 1) 2020-06-09T07:43:48.981428Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: ready
```

```
for connections. Version: '8.0.20-0ubuntu0.19.10.1' socket: '/var/run/mysqld/mysqld.sock'
port: 3306 (Ubuntu).
[--] 2) 2020-06-09T07:43:48.910374Z 0 [System] [MY-011323] [Server] X Plugin ready for
connections. Socket: '/var/run/mysqld/mysqlx.sock' bind-address: '::' port: 33060
[--] 3) 2020-06-09T07:43:46.480121Z 0 [System] [MY-011323] [Server] X Plugin ready for
connections. Bind-address: '::' port: 33060
[--] 4) 2020-06-09T07:43:43.480774Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: ready
for connections. Version: '8.0.20-0ubuntu0.19.10.1' socket:
'/tmp/tmp.pYBOETvCu0/mysqld.sock' port: 0 (Ubuntu).
[--] 2 shutdown(s) detected in /var/log/mysql/error.log
[--] 1) 2020-06-09T07:43:47.628975Z 0 [System] [MY-010910] [Server] /usr/sbin/mysqld: Shutdown
complete (mysqld 8.0.20-0ubuntu0.19.10.1) (Ubuntu).
[--] 2) 2020-06-09T07:43:45.029894Z 0 [System] [MY-010910] [Server] /usr/sbin/mysqld: Shutdown
complete (mysqld 8.0.20-0ubuntu0.19.10.1) (Ubuntu).

-------- Storage Engine Statistics
-------------------------------------------------------------------
[--] Status: +ARCHIVE +BLACKHOLE +CSV -FEDERATED +InnoDB +MEMORY +MRG_MYISAM +MyISAM
+PERFORMANCE_SCHEMA
[--] Data in InnoDB tables: 16.0K (Tables: 1)
[OK] Total fragmented tables: 0

-------- Analysis Performance Metrics
-------------------------------------------------------------------
[--] innodb_stats_on_metadata: OFF
[OK] No stat updates during querying INFORMATION_SCHEMA.

-------- Security Recommendations
-------------------------------------------------------------------
[--] Skipped due to unsupported feature for MySQL 8

-------- CVE Security Recommendations
-------------------------------------------------------------------
[OK] NO SECURITY CVE FOUND FOR YOUR VERSION

-------- Performance Metrics
-------------------------------------------------------------------------
[--] Up for: 32m 53s (118 q [0.060 qps], 57 conn, TX: 255K, RX: 14K)
[--] Reads / Writes: 98% / 2%
[--] Binary logging is enabled (GTID MODE: OFF)
[--] Physical Memory     : 2.9G
```

```
[--] Max MySQL memory    : 9.8G
[--] Other process memory: 0B
[--] Total buffers: 176.0M global + 65.1M per thread (151 max threads)
[--] P_S Max memory usage: 72B
[--] Galera GCache Max memory usage: 0B
[OK] Maximum reached memory usage: 241.1M (8.06% of installed RAM)
[!!] Maximum possible memory usage: 9.8G (334.59% of installed RAM)
[!!] Overall possible memory usage with other process exceeded memory
[OK] Slow queries: 0% (0/118)
[OK] Highest usage of available connections: 0% (1/151)
[!!] Aborted connections: 19.30%  (11/57)
[!!] name resolution is active : a reverse name resolution is made for each new connection and
can reduce performance
[--] Query cache have been removed in MySQL 8
[OK] Sorts requiring temporary tables: 0% (0 temp sorts / 7 sorts)
[OK] No joins without indexes
[OK] Temporary tables created on disk: 0% (0 on disk / 11 total)
[OK] Thread cache hit rate: 96% (2 created / 57 connections)
[OK] Table cache hit rate: 81% (337 open / 416 opened)
[OK] table_definition_cache(2000) is upper than number of tables(311)
[OK] Open file limit used: 0% (6/10K)
[OK] Table locks acquired immediately: 100% (8 immediate / 8 locks)
[OK] Binlog cache memory access: 100.00% (3 Memory / 3 Total)

-------- Performance schema
------------------------------------------------------------------------
[--] Memory used by P_S: 72B
[--] Sys schema is installed.

-------- ThreadPool Metrics
------------------------------------------------------------------------
[--] ThreadPool stat is disabled.

-------- MyISAM Metrics
------------------------------------------------------------------------
[--] MyISAM Metrics are disabled on last MySQL versions.

-------- InnoDB Metrics
------------------------------------------------------------------------
[--] InnoDB is enabled.
[--] InnoDB Thread Concurrency: 0
```

```
[OK] InnoDB File per table is activated
[OK] InnoDB buffer pool / data size: 128.0M/16.0K
[!!] Ratio InnoDB log file size / InnoDB Buffer pool size (75 %): 48.0M * 2/128.0M should be
equal to 25%
[OK] InnoDB buffer pool instances: 1
[--] Number of InnoDB Buffer Pool Chunk : 1 for 1 Buffer Pool Instance(s)
[OK] Innodb_buffer_pool_size aligned with Innodb_buffer_pool_chunk_size &
Innodb_buffer_pool_instances
[OK] InnoDB Read buffer efficiency: 96.90% (27237 hits/ 28107 total)
[OK] InnoDB Write log efficiency: 90.05% (724 hits/ 804 total)
[OK] InnoDB log waits: 0.00% (0 waits / 80 writes)

-------- AriaDB Metrics
-----------------------------------------------------------------------------
[--] AriaDB is disabled.

-------- TokuDB Metrics
-----------------------------------------------------------------------------
[--] TokuDB is disabled.

-------- XtraDB Metrics
-----------------------------------------------------------------------------
[--] XtraDB is disabled.

-------- Galera Metrics
-----------------------------------------------------------------------------
[--] Galera is disabled.

-------- Replication Metrics
-------------------------------------------------------------------------
[--] Galera Synchronous replication: NO
[--] No replication slave(s) for this server.
[--] Binlog format: ROW
[--] XA support enabled: ON
[--] Semi synchronous replication Master: Not Activated
[--] Semi synchronous replication Slave: Not Activated
[--] This is a standalone server

-------- Recommendations
---------------------------------------------------------------------------
General recommendations:
```

```
    Control warning line(s) into /var/log/mysql/error.log file
    Control error line(s) into /var/log/mysql/error.log file
    MySQL was started within the last 24 hours - recommendations may be inaccurate
    Reduce your overall MySQL memory footprint for system stability
    Dedicate this server to your database for highest performance.
    Reduce or eliminate unclosed connections and network issues
    Configure your accounts with ip or subnets only, then update your configuration with skip-
name-resolve=1
    Before changing innodb_log_file_size and/or innodb_log_files_in_group read this:
https://bit.ly/2TcGgtU
Variables to adjust:
  *** MySQL's maximum memory usage is dangerously high ***
  *** Add RAM before increasing MySQL buffer variables ***
    innodb_log_file_size should be (=16M) if possible, so InnoDB total log files size equals
to 25% of buffer pool size.
```

Revision #3
Created 9 June 2020 05:39:22 by ggpilou2
Updated 9 June 2020 06:20:54 by ggpilou2