MySQL and MariaDB: Supplement

# Notes & References

Care needs to be taken when using wildcards for host names, especially when the host names overlap. Consider MySQL 5.6.17 on OpenSuSE 13.2. Create four users- two named bill and two named wendy in the following order.

mysql> CREATE USER bill@'%' IDENTIFIED BY 'password1!';

Query OK, 0 rows affected (0.00 sec)

mysql> CREATE USER bill@'%.stars.example' IDENTIFIED BY 'password1!';

Query OK, 0 rows affected (0.00 sec)

mysql> CREATE USER wendy@'%.stars.example' IDENTIFIED BY 'password1!';

Query OK, 0 rows affected (0.00 sec)

mysql> CREATE USER wendy@'%' IDENTIFIED BY 'password1!';

Query OK, 0 rows affected (0.00 sec)

Suppose the user bill authenticates from the system ankaa.stars.example. Which account is used?

[root@ankaa ~]# mysql -u bill -h 10.0.2.92 -ppassword1!

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MySQL connection id is 4

Server version: 5.6.17 openSUSE package

… Output Deleted …

MySQL [(none)]> SELECT current\_user();

+----------------+

| current\_user() |

+----------------+

| bill@% |

+----------------+

1 row in set (0.00 sec)

Now repeat the process but log in as wendy from the same host.

[root@ankaa ~]# mysql -u wendy -h 10.0.2.92 -ppassword1!

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MySQL connection id is 5

Server version: 5.6.17 openSUSE package

… Output Deleted …

MySQL [(none)]> SELECT current\_user();

+-----------------------+

| current\_user() |

+-----------------------+

| wendy@%.stars.example |

+-----------------------+

1 row in set (0.00 sec)

Before using overlapping wildcards in host names, the reader is encouraged to read the documentation <https://dev.mysql.com/doc/refman/5.7/en/account-names.html> and <https://mariadb.com/kb/en/library/create-user/> quite carefully, and then test the system to be sure that it behaves as expected.

Another subtlety in wildcards is how MySQL and MariaDB handle wildcard user names. For example, suppose that the administrator creates the user bob who can log on from any host, and that the administrator also creates a wildcard user for the host 10.0.3.57.

mysql> SELECT user, host FROM mysql.user;

+------------------+-----------+

| user | host |

+------------------+-----------+

| bob | % |

| | 10.0.3.57 |

| root | 127.0.0.1 |

| root | ::1 |

| root | aegle |

| debian-sys-maint | localhost |

| root | localhost |

+------------------+-----------+

7 rows in set (0.00 sec)

If bob tries to log on from 10.0.3.57, what account is used for authentication?

jmaxwell@siegena:~$ mysql -u bob -h aegle.asteroid.test -p

Enter password: <enter password here>

Welcome to the MySQL monitor. Commands end with ; or \g.

Your MySQL connection id is 14

Server version: 5.6.25-0ubuntu1 (Ubuntu)

… Output Deleted …

mysql> SELECT current\_user();

+----------------+

| current\_user() |

+----------------+

| @10.0.3.57 |

+----------------+

1 row in set (0.00 sec)

The collection of MySQL commands in the client can be found by running help. For example, MariaDB 10.0.24 on Ubuntu 16.04 provides the following help.

MariaDB [(none)]> help

General information about MariaDB can be found at

http://mariadb.org

List of all MySQL commands:

Note that all text commands must be first on line and end with ';'

? (\?) Synonym for `help'.

clear (\c) Clear the current input statement.

connect (\r) Reconnect to the server. Optional arguments are db and host.

delimiter (\d) Set statement delimiter.

edit (\e) Edit command with $EDITOR.

ego (\G) Send command to mysql server, display result vertically.

exit (\q) Exit mysql. Same as quit.

go (\g) Send command to mysql server.

help (\h) Display this help.

nopager (\n) Disable pager, print to stdout.

notee (\t) Don't write into outfile.

pager (\P) Set PAGER [to\_pager]. Print the query results via PAGER.

print (\p) Print current command.

prompt (\R) Change your mysql prompt.

quit (\q) Quit mysql.

rehash (\#) Rebuild completion hash.

source (\.) Execute an SQL script file. Takes a file name as an

argument.

status (\s) Get status information from the server.

system (\!) Execute a system shell command.

tee (\T) Set outfile [to\_outfile]. Append everything into given

outfile.

use (\u) Use another database. Takes database name as argument.

charset (\C) Switch to another charset. Might be needed for processing

binlog with multi-byte charsets.

warnings (\W) Show warnings after every statement.

nowarning (\w) Don't show warnings after every statement.

For server side help, type 'help contents'

Table 18-1. Default included version of MySQL, by Linux distribution

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  | Mint |  | 11 | 5.1.54 | 17.04 | 5.7.17 |
| 6.8 | 5.1.73-7 | 18.3 | 5.7.22 | 10 | 5.1.49 | 16.10 | 5.7.15 |
| 6.7 | 5.1.73-5 | 18.2 | 5.7.21 | OpenSuSE |  | 16.04 | 5.7.11 |
| 6.6 | 5.1.73-3 | 18.1 | 5.7.11 | 42.3 | 5.6.36 | 15.10 | 5.6.25 |
| 6.5 | 5.1.71-1 | 18 | 5.7.11 | 42.2 | 5.6.30 | 15.04 | 5.6.24 |
| 6.4 | 5.1.66-2 | 17.3 | 5.5.35 | 42.1 | 5.6.26 | 14.10 | 5.5.40 |
| 6.3 | 5.1.64-4 | 17.2 | 5.5.25 | 13.2 | 5.6.17 | 14.04 | 5.5.25 |
| 6.2 | 5.1.52-1 | 17.1 | 5.5.35 | 13.1 | 5.6.12 | 13.10 | 5.5.32 |
| 6.1 | 5.1.52-1 | 17 | 5.5.35 | 12.3 | 5.5.30 | 13.04 | 5.5.29 |
| 6.0 | 5.1.47-4 | 16 | 5.5.32 | 12.2 | 5.5.25a | 12.10 | 5.5.27 |
| 5.10 | 5.0.95-5 | 15 | 5.5.29 | 12.1 | 5.5.16 | 12.04 | 5.5.22 |
| 5.9 | 5.0.95-3 | 14 | 5.5.27 | 11.4 | 5.1.53 | 11.10 | 5.1.58 |
| 5.7 | 5.0.77-4 | 13 | 5.5.22 | Ubuntu |  | 11.04 | 5.1.54 |
| 5.6 | 5.0.77-4 | 12 | 5.1.58 | 17.10 | 5.7.19 |  |  |

Table 18-2. Default included version of MariaDB, by Linux distribution

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CentOS |  | 17.3 | 5.5.36 | 12.2 | 5.5.25 |
| 7.4.1709 | 5.5.26-2 | 17.2 | 5.5.36 | 12.1 | 5.2.9 |
| 7.3.1611 | 5.5.52-1 | 17.1 | 5.5.36 | 11.4 | 5.1.44 |
| 7.2.1511 | 5.5.44-2 | 17 | 5.5.53 | Ubuntu |  |
| 7.1.1503 | 5.5.41-2 | OpenSuSE |  | 17.10 | 10.1.25 |
| 7.0.1406 | 5.5.35-3 | 42.3 | 10.0.30 | 17.04 | 10.1.22 |
| Mint |  | 42.2 | 10.0.27 | 16.10 | 10.0.25 |
| 18.3 | 10.0.34 | 42.1 | 10.0.21 | 16.04 | 10.0.24 |
| 18.2 | 10.0.33 | 13.2 | 10.0.13 | 15.10 | 10.0.20 |
| 18.1 | 10.0.24-7 | 13.1 | 5.5.33 | 14.10 | 5.5.39 |
| 18 | 10.0.24-7 | 12.3 | 5.5.29 | 14.04 | 5.5.36 |

Table 18-3. Release dates of major versions of MySQL and MariaDB. For MariaDB, the first stable release is shown.

|  |  |  |  |
| --- | --- | --- | --- |
| MySQL |  | MariaDB |  |
| 5.7 | October 2015 | 10.2.6 | May 2017 |
| 5.6 | February 2013 | 10.1.8 | October 2017 |
| 5.5 | December 2010 | 10.0.10 | March 2014 |
|  |  | 5.5.23 | April 2011 |
|  |  | 5.3.5 | February 2012 |
|  |  | 5.2.4 | December 2010 |

Exercises

1. Use the MySQL command prompt on a Windows system to connect to a database. Does this change the title of the window? What happens to the title if the password is specified on the command line?
2. A user without the MySQL root password, but with the ability to start and stop the service (like root on the operating system, or a user permitted to use sudo) can reset the MySQL root password. Do so. See for example <http://dev.mysql.com/doc/refman/5.5/en/resetting-permissions.html>.
3. Use the NMap script myqsl-brute to perform a brute force attack against a MySQL server. (Configure the target so that the attack succeeds.) Follow up with the NMap scripts mysql-databases and mysql-dumphashes.
4. MySQL 5.1.53 on OpenSuSE 11.4 is vulnerable to a privilege escalation exploit; a user with FILE privileges on the database can create a database user with full privileges, including the grant option. The issue is caused by CVE 2012-5613 ([http://www.securityfocus.com/bid/56771](http://www.securityfocus.com/bid/56771/info)). Exploit code is available there, on ExploitDB (<http://www.exploit-db.com/exploits/23077/>), and on Kali as /usr/share/exploitdb/exploits/linux/local/23077.pl. Run the exploit.
5. The Metasploit module auxiliary/scanner/mysql/mysql\_hashdump is used to dump the password hashes from a MySQL / MariaDB instance, provided the attacker has credentials. Run the module.

The module auxiliary/scanner/mysql/mysql\_authbypass\_hashdump is similar, but instead of requiring credentials, the module attacks systems vulnerable to CVE 2012-2122. Run the attack.