User management

Introduction

In this lab you will explore user creation, their privileges and roles.
We start with the creation of a user that can connect only from a specific client, we grant and revoke privileges and try to assign a weak password.
In the second task we create a new user with a role.

Estimated Lab Time: 25 minutes

Objectives

In this lab, you will:

- Explore user creation and privileges
- Discover and Configure roles

Task 1: User creation and privileges

> **Note:**

- Servers:
  - app-srv as client (used by appuser)
  - mysql1 as mysql server
- Use two shells connections, one for administrative commands and the other for the user connection test

1. If you are not already connected, open connect to app-srv and install the mysql and mysqlsh clients

```
<span style="color:green">shell-app-srv$</span> <copy>ls -l
/workshop/linux/client/</copy>
```

```
<span style="color:green">shell-app-srv$</span> <copy>sudo yum -y install
/workshop/linux/client/*.rpm</copy>
```

2. To simplify our activity, set the the autosave.
   (please note the syntax that let you use MySQL Shell in command line)

```
<span style="color:green">shell-app-srv$</span> <copy>mysqlsh -- shell
options set-persist history.autoSave true</copy>
```

3. Connect to your mysql-advanced with admin user

```
<span style="color:green">shell-app-srv></span> <copy>mysqlsh
admin@mysql1:3307</copy>
```

4. Create a new user and restrict the user to your “app-srv.%”. In the real life, you probably use a specific fqdn, here we test a connection with jolly characters

```
<span style="color:blue">mysql></span> <copy>CREATE USER 'appuser'@'app-
srv.%' IDENTIFIED BY 'Welcome1!';</copy>
```

5. Grant to the new user privileges to work on world database

```
<span style="color:blue">mysql></span> <copy>GRANT ALL PRIVILEGES ON world.*
TO 'appuser'@'app-srv.%';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser'@'app-
srv.%';</copy>
```

6. Keep previous connection open and open a new shell connection to app-srv, then connect as user appuser to mysql1 to test the connection.

> Note:
> * Please remember that the user "appuser" can connect only from this server
> * Please ignore the error "Error during auto-completion cache update: Access denied..." related to lack of privileges for the user. If you want to disable the message disable **autocomplete.nameCache** option

```
<span style="color:green">shell-app-srv$</span> <copy>mysqlsh
appuser@mysql1:3307</copy>
```

```
<span style="color:blue">mysql></span> <copy>USE world;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW TABLES;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SELECT * FROM city limit 10;
</copy>
```

7. (admin connection) Switch to the administrative connection revoke privilege on city to appuser

```
<span style="color:blue">mysql></span> <copy>REVOKE SELECT ON world.* FROM
'appuser'@'app-srv.%';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser'@'app-
srv.%';</copy>
```

8. (appuser connection) Repeat the select on for the user. There is a difference?

```
<span style="color:blue">mysql></span> <copy>SELECT * FROM city limit 10;
</copy>
```

9. (appuser connection) Close and reopen the appuser connection, then repeat above commands. There is a difference?

```
<span style="color:blue">mysql></span> <copy>\q</copy>
```

```
<span style="color:green">shell-app-srv$</span> <copy>mysqlsh
appuser@mysql1:3307</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

```
<span style="color:blue">mysql></span> <copy>USE world;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SELECT * FROM city limit 10;
</copy>
```

10. (admin connection) Switch to the administrative connection revoke ‘USAGE’ privilege using and administrative connection and verify if something changed.
    As you can see, 'USAGE' privilege can’t be revoked.

```
<span style="color:blue">mysql></span> <copy>REVOKE USAGE ON *.* FROM
'appuser'@'app-srv.%';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser'@'app-srv.%';</copy>
```

11. (admin connection) Using the administrative connection revoke all privileges using and administrative connection and verify

```
<span style="color:blue">mysql></span> <copy>REVOKE ALL PRIVILEGES ON *.* FROM 'appuser'@'app-srv.%';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser'@'app-srv.%';</copy>
```

12. (appuser connection) Global privileges changes take effect immediately. Check it now that user lost all privileges over world database

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

13. (admin connection) Using the administrative connection restore user privileges to reuse it in next labs

```
<span style="color:blue">mysql></span> <copy>GRANT ALL PRIVILEGES ON world.* TO 'appuser'@'app-srv.%';</copy>
```

14. (admin connection) We play now with password enforcements settings. First load the password validation component

```
<span style="color:blue">mysql></span> <copy>INSTALL COMPONENT 'file://component_validate_password';</copy>
```

15. (admin connection) Check now the password requirements

```
<span style="color:blue">mysql></span> <copy>SHOW VARIABLES LIKE 'validate_password%';</copy>
```

16. (appuser connection) Try to set unsecure passwords for appuser

```
<span style="color:blue">mysql></span> <copy>ALTER USER 'appuser'@'app-
srv.%' IDENTIFIED BY 'appuser';</copy>
```

```
<span style="color:blue">mysql></span> <copy>ALTER USER 'appuser'@'app-
srv.%' IDENTIFIED BY 'Welcome';</copy>
```

```
<span style="color:blue">mysql></span> <copy>ALTER USER 'appuser'@'app-
srv.%'IDENTIFIED BY 'We1!';</copy>
```

17. (admin connection) Expire the password for appuser

```
<span style="color:blue">mysql></span> <copy>ALTER USER 'appuser'@'app-
srv.%' PASSWORD EXPIRE;</copy>
```

18. (appuser connection) Close and reopen connection to mysql-advanced and try to submit a command. What changed?

```
<span style="color:blue">mysql></span> <copy>\q</copy>
```

```
<span style="color:green">shell-app-srv$</span> <copy>mysqlsh
appuser@mysql1:3307</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SET PASSWORD='Welcome1!';
</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

Task 2: User Roles

1. If not already connected, connect to mysql1 through app-srv

```
<span style="color:green">shell-app-srv$</span> <copy>ssh -i
$HOME/sshkeys/id_rsa_mysql1 opc@mysql1</copy>
```

2. Reconnect to MySQL instance as admin to create a new user

```
<span style="color:green">shell></span> <copy>mysqlsh
admin@mysql1:3307</copy>
```

```
<span style="color:blue">mysql></span> <copy>CREATE USER 'appuser2'@'%'
IDENTIFIED BY 'Welcome1!';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser2'@'%';
</copy>
```

3. Now create a new role

```
<span style="color:blue">mysql></span> <copy>CREATE ROLE 'app_read';</copy>
```

4. Assign GRANT privileges to the role

```
<span style="color:blue">mysql></span> <copy>GRANT SELECT ON world.* TO
'app_read';</copy>
```

5. Grant the role to the user

```
<span style="color:blue">mysql></span> <copy>GRANT 'app_read' TO
'appuser2'@'%';</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS FOR 'appuser2'@'%';
</copy>
```

```
<span style="color:blue">mysql></span> <copy>\q</copy>
```

6. Connect now as appuser2 and submit some commands (you receive errors, why?)

```
<span style="color:green">shell></span> <copy>mysqlsh
appuser2@mysql1:3307</copy>
```

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

7. Why we don't see the world database? Let's check our grants: we have only the role...

```
<span style="color:blue">mysql></span> <copy>SHOW GRANTS;</copy>
```

8. ...but the role is active?

```
<span style="color:blue">mysql></span> <copy>SELECT current_role();</copy>
```

9. That's the problem! Set now the role for the user

```
<span style="color:blue">mysql></span> <copy>SET ROLE app_read;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SELECT current_role();</copy>
```

10. Now we are ready to work

```
<span style="color:blue">mysql></span> <copy>SHOW DATABASES;</copy>
```

```
<span style="color:blue">mysql></span> <copy>SELECT COUNT(*) FROM
world.city;</copy>
```

11. So, it's a good practice to assign a default role (please note that this command can be execute by the user itself)

```
<span style="color:blue">mysql></span> <copy>ALTER USER 'appuser2'@'%'
DEFAULT ROLE 'app_read';</copy>
```

12. Now you can exit from appuser2 connection

```
<span style="color:blue">mysql></span> <copy>\q</copy>
```

Acknowledgements

- **Author** - Marco Carlessi, Principal Sales Consultant
- **Contributors** - Perside Foster, Principal Sales Consultant, Selena Sánchez, MySQL Solutions Engineer
- **Last Updated By/Date** - Perside Foster, Partner Solutions Engineer, November 2024