Role-Based Access Control concept

A major benefit of the TWCloud system is being able to control how and which user can access the resources in the system. Superior management is essential for large and complex systems in order for a substantial number of users to access the system, and use its resources at the same time. The TWCloud uses role-based access control (RBAC) to regulate permissions and access to its system resources based on the roles of individual users. RBAC is a way to provide quick access, and, at the same time, control the actions a user can perform based on their roles. With RBAC, you can assign general permissions quickly through the use of roles, but you cannot modify the permissions in a pre-existing role. You can also create custom roles for users with particular needs.

Your password and username are associated with your role in the TWCloud system, meaning that your user account comes with role-specific authorizations. Authorizations are permissions that enable a role or a user to accomplish specific actions. Permissions vary according to the role. For example, some permissions enable a user or a role to:

- Create a user account, assign roles and permissions, and assign resources to each role.
- Modify user information and password.
- Configure the TWCloud's settings.
- Assign resources to specific users in a particular role.
- Allow and deny user login to TWCloud Admin.

What's next?
Case study