Security in UCP

UCP offers a variety of features to help secure our Docker cluster. One of these is a role-based access control system designed to help manage permissions in our cluster. In this lesson, we will explore role-based access control in UCP.

Relevant Documentation

- UCP Access Control Model
- Create Teams with LDAP

Lesson Reference

On the left, select **Access Control**.

Select **Users** to create and manage users.

Create a new user with the username `bob`.

Manage Organizations and Teams from the *Orgs & Teams* panel.

Manage Docker Swarm resource sets by going to **Shared Resources** > **Collections**.

Select **View Children** next to the *Swarm* collection. Create a new collection by clicking **Create Collection**. Give it the name `mycollection`.

Select **Swarm** > **Services**, then click on our `nginx` service.

Click the gear icon to configure the service. Select **Collection**, pick **View Children** for the *Swarm* collection, then use the **Select Collection** button that appears when hovering over *mycollection*. Click **Save**. This will add the service to our collection.

Click **Access Control** > **Roles** to explore the roles that are available. Use the **Kubernetes** and **Swarm** to view roles for Kubernetes and Docker Swarm, respectively.

Go to **Access Control** > **Grants**, then select **Swarm** at the top. Click **Create Grant**.

Select the **bob** user for the *Subject*. For the *Resource Set*, select **View Children** next to *Swarm*, then choose **Select Collection** by hovering over *mycollection*. For the *Role*, select **View Only**, then click **Create**.

Congratulations! You just granted the Bob user the ability to view information about your `nginx` service.

Feel free to further explore the UCP access control features.

Also, check out the LDAP integration settings.

On the left, select **admin** > **Admin Settings** > **Authentication & Authorization**, then click the **LDAP** toggle.