



# kubernetes

---

*Kubernetes: User Management*

## *KUBERNETES : Administration*

---

- In Kubernetes we can set-up the **Authorization Mechanism**.
- There are two types of users, administrator can create:
- A **Normal user**, that allowed to use the Cluster Externally via Kubectl.
- Normal user doesn't support any log-in/log-out mechanism.
- **Service User**, which is managed by an Object in Kubernetes.
- Service User needs authentication with the cluster either via **Pod or kubelet**.
- Service user credentials managed like **secrets**.

## *KUBERNETES : Administration*

---

- There are multiple **Authentication mechanism** for normal user:
- Client Certificate
- Bearer Tokens
- Authentication Proxy
- HTTP Basic Authentication
- OpenID
- Webhooks

## *KUBERNETES : Administration*

---

- Service Users are using the **Service Account Tokens**.
- They are stored as credentials using **secrets**.
- Those Secrets **Mounted in pods** to allow communication between the Services.
- Service users are specific to **Namespace**
- Service Users are being created using the API or manually using Objects.

## *KUBERNETES : Administration*

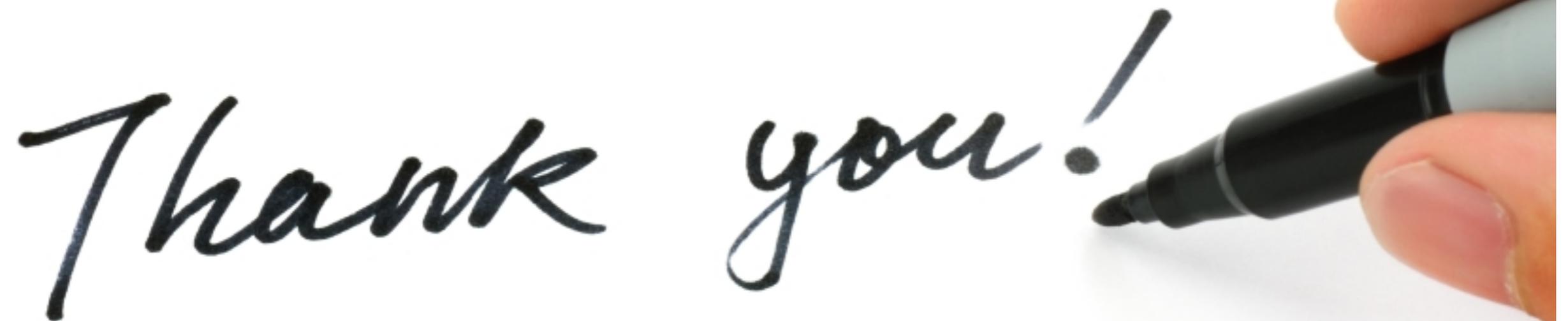
---

- After Normal user Authenticate, it have access to everything in Kube Cluster.
- To limit the access, admin needs to configure authorization.
- They can be configured by:
  - **ABAC** (Attribute Base Account Control)
  - **RBAC** (Role Base Account Control)
  - **WebHook** (Authorization by remote Service)

*Will see you in Next Lecture...*

---

*Thank you!*

A close-up photograph of a hand holding a black marker, writing the words 'Thank you!' in a cursive script on a white surface. The hand is positioned on the right side of the frame, with the fingers gripping the marker. The text is written in a dark, fluid cursive style. The background is plain white.

*See you in next lecture ...*