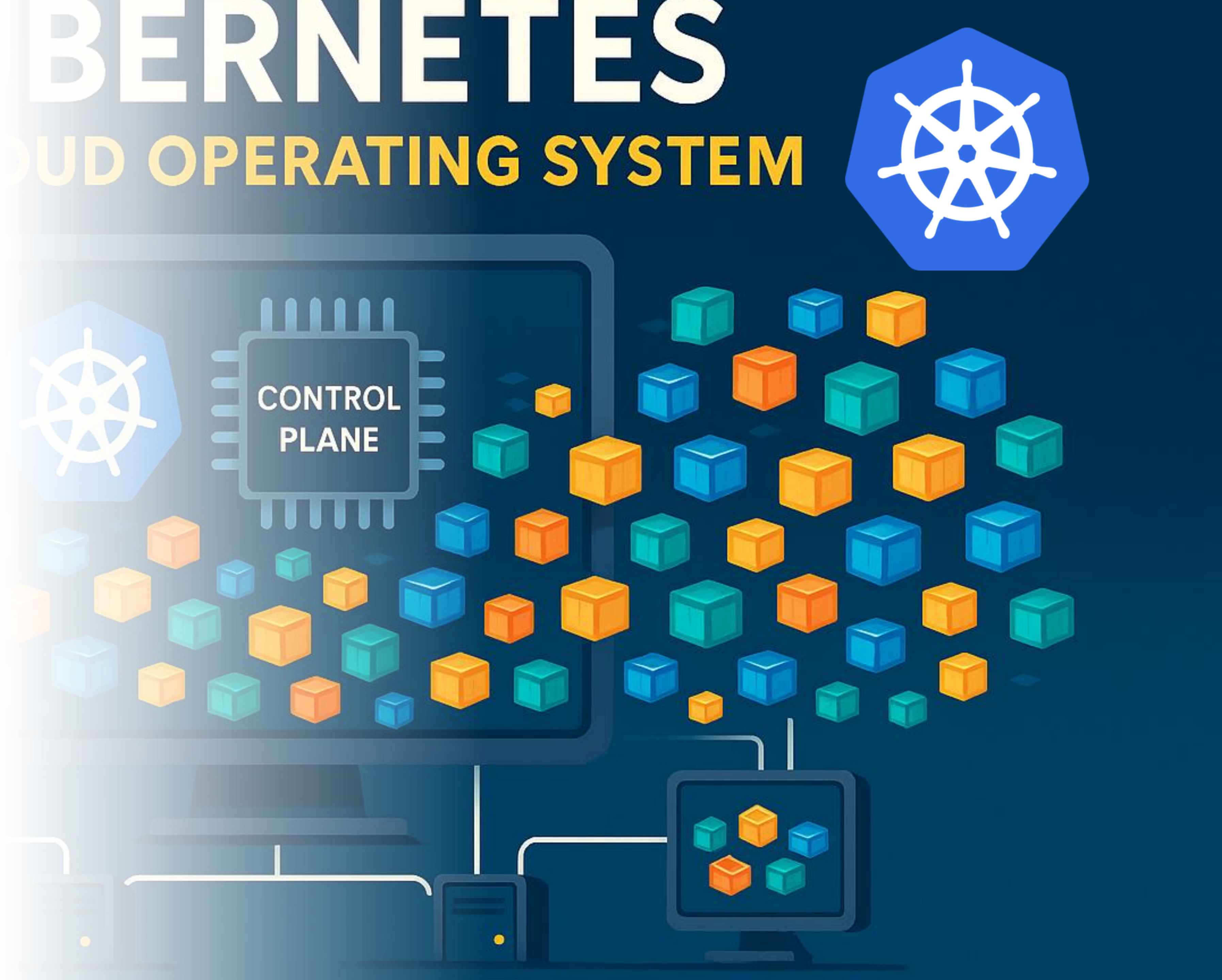
CS-UY 3913
Container
Operating Systems



K8 Secrets

Instructor: Magdy Salem

Agenda

- What is a Secret?
- Use Cases
- Types of Secrets
- Creating Secrets
- Consuming Secrets in Pods
- Security Considerations

What is a Secret?

- A Kubernetes object used to store sensitive information
- Data is base64 encoded
- Used to avoid embedding credentials in container images or YAML files
- Typical use: passwords, API keys, certificates

Use Cases

- • Storing database credentials
- • TLS certificates for HTTPS communication
- • API tokens or OAuth credentials
- • SSH keys and Git credentials

Types of Secrets

- Opaque (default): generic key-value pairs
- kubernetes.io/dockerconfigjson: for registry credentials
- kubernetes.io/tls: for TLS cert/key
- bootstrap.kubernetes.io/token: bootstrap tokens for cluster join

Creating Secrets

- From literals:

```
kubectl create secret generic db-secret --from-literal=username=admin --from-literal=password=secret123
```

- From files:

```
kubectl create secret generic app-secret --from-file=config.json
```

- Declarative (YAML): base64 encode values manually

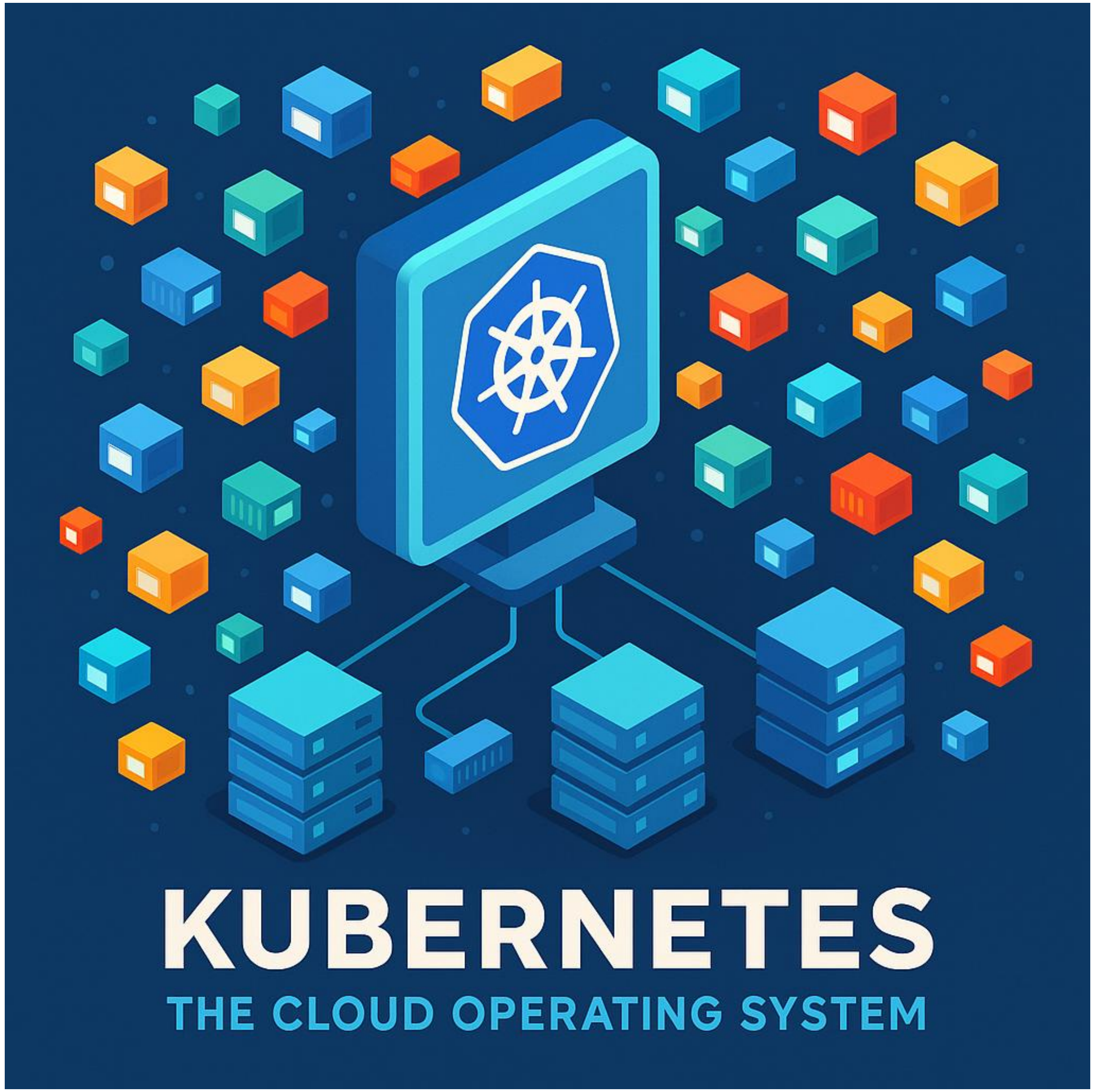
Consuming Secrets in Pods

- As environment variables:
- As mounted files (volumes):
- Containers can read secrets securely at runtime

Security Considerations

- Secrets are base64 encoded, not encrypted by default
- Enable encryption at rest using Kubernetes configuration
- Apply strict RBAC policies to restrict access
- Use read-only mounts and limit container privilege

Demo



Lab