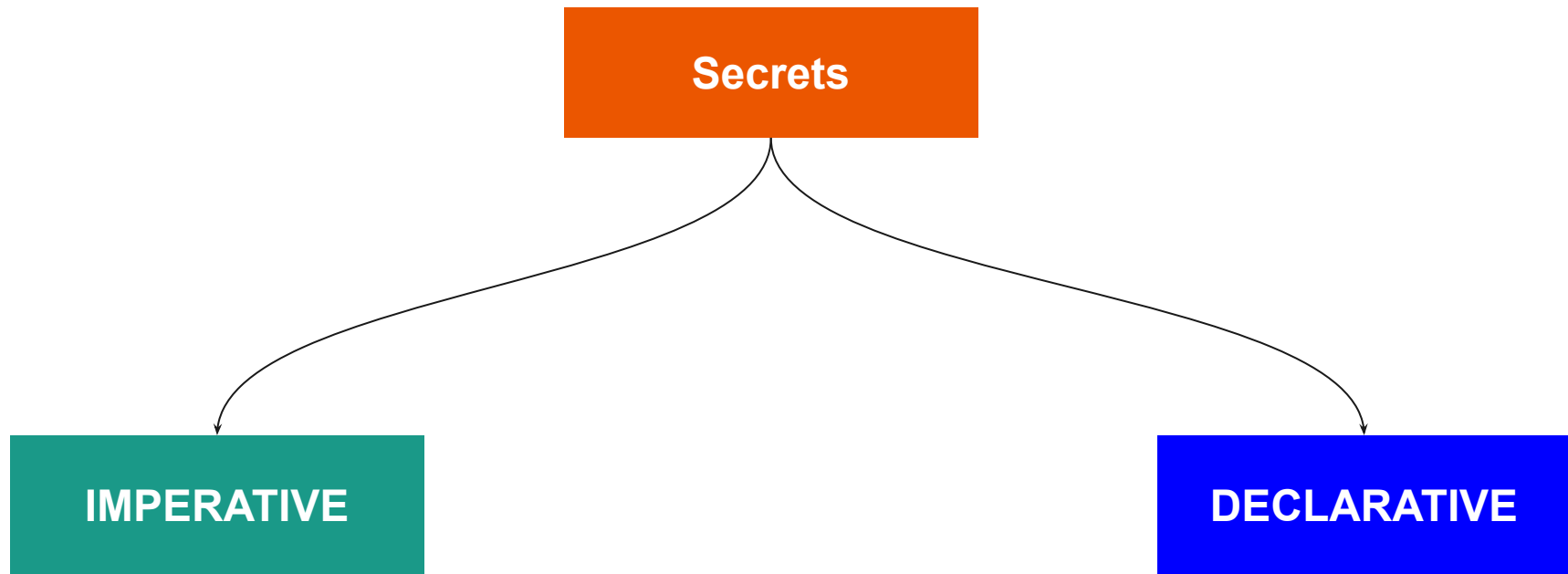


# CKA/CKAD : Complete Certification Guide

Secrets in Kubernetes YAML  
Overview



# CKA/CKAD Certification



## Secrets insertion in PODs

```
Secret Name : db-access-details  
UserName : sqladmin  
Password : hr@43$EFrL
```

```
echo -n 'sqladmin' > ./username.txt  
echo -n 'hr@43$EFrL' > ./password.txt
```

```
SYNTAX : kubectl create secret [TYPE] [NAME] [DATA]
```

```
Kubectl create secret generic db-access-details --from-file=./username.txt  
--from-file=./password.txt
```

# CKA/CKAD Certification

- **Types of Secrets**
- **Opaque Secrets** – The default Secret type.
- **Service account token Secrets** – Used to store a token that identifies a service account.
- **Docker config Secrets** – Stores the credentials for accessing a Docker registry for images.
- **Basic authentication Secret** – Used for storing credentials needed for basic authentication. Like - username and password

# CKA/CKAD Certification

- **Types of Secrets**
- **SSH authentication secrets** – Used for storing data used in SSH authentication. Like private key value pair.
- **TLS secrets** – For storing a certificate and its associated key that are typically used for TLS . This data is primarily used with TLS termination of the Ingress resource, but may be used with other resources or directly by a workload.
- **Bootstrap token Secrets** – Used for tokens used during the node bootstrap process. It stores tokens used to sign well known ConfigMaps.

## Secrets insertion in PODs

Secret Name : db-access-details  
UserName : sqladmin  
Password : hr@43\$EFrL

```
# echo -n 'sqladmin' | base64  
c3FsYWRTaW4=  
# echo -n 'hr@43$EFrL' | base64  
aHJANDMkRUZyTA==
```

```
apiVersion: v1  
kind: Secret  
metadata:  
  name: db-access-details  
type: Opaque  
stringData:  
  username: c3FsYWRTaW4=  
  password: aHJANDMkRUZyTA==
```

# Thank You...

Don't be the Same! Be Better!!!

---