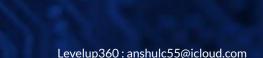


**Ensuring Containers are Immutable** 



#### **K8s: Certification**

## **Container Immutability**

- Immutable Containers don't change during their lifetime.
- Instead of being changed, Immutable containers are replaced with new Containers.
- This means that Container file system remain static and container doesn't depend on non-immutable hosts that require privilege access.

### **K8s: Certification**

## **Immutability and Security**

- Immutability has security benefits.
  - Attacker can't download malicious code to container or alter the container runtime code.
- Avoid elevated privilege.

#### **K8s: Certification**

```
apiVersion: v1
kind: Pod
metadata:
 name: security-context-demo
spec:
 volumes:
  - name: sec-ctx-vol
    emptyDir: {}
  containers:
  - name: sec-ctx-demo
    image: busybox:1.28
    command: [ "sh", "-c", "sleep 1h"
   volumeMounts:
    - name: sec-ctx-vol
    mountPath: /data/demo
   securityContext:
      ReadOnlyRootFilesystem: true
```

Immutable Container do not change their code, it means they should not be able to write to container file system.

Use ReadOnlyRootFilesystem: true to enforce this. A container without this setting might not be considered Immutable.

If Application not allowed to write data at root. Use Volume Mount to support data writing at specific locations.

# Thank You...

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