TEKLRN

KUBERNETES LEVEL 30

1. Secrets
   - Overview of Secrets

2. Built-in Secrets
   - Service accounts automatically create and attach Secrets with API credentials
   - Creating your own Secrets
   - Creating a Secret Using kubectl
   - Creating a Secret manually
   - Creating a Secret from a generator
   - Generating a Secret from files
   - Generating a Secret from string literals

3. Decoding a Secret
   - Editing a Secret
   - Using Secrets
   - Using Secrets as files from a Pod

4. Projection of Secret keys to specific paths

5. Secret files permissions

6. Consuming Secret values from volumes
   - Mounted Secrets are updated automatically

7. Using Secrets as environment variables
   - Consuming Secret Values from environment variables

8. Using imagePullSecrets
   - Manually specifying an imagePullSecret
   - Arranging for imagePullSecrets to be automatically attached

9. Automatic mounting of manually created Secrets
   - Details
   - Restrictions

10. Secret and Pod lifetime interaction
    - Use cases
    - Use-Case: As container environment variables
    - Use-Case: Pod with ssh keys
    - Use-Case: Pods with prod / test credentials
    - Use-case: dotfiles in a secret volume
    - Use-case: Secret visible to one container in a Pod

11. Best practices
    - Clients that use the Secret API
    - Security properties