ChatGPT

CKA 2025 – Q12: cert-manager CRDs & kubectl explain

Task summary

1. **Verify cert-manager** – Ensure the cert-manager application is running in your cluster.
2. **List cert-manager CRDs** – Use kubectl's default output format to list all Custom Resource Definitions from cert-manager and save them to `~/resources.yaml`. Do **not** specify an output format.
3. **Document the `subject` field** – Use kubectl to extract the documentation for the `subject` field of the Certificate custom resource and save it to `~/subject.yaml` (any output format is allowed).

Step-by-step instructions

1. Verify cert-manager deployment

Check that cert-manager's namespace and pods exist:

```
kubectl get ns
kubectl get pods -n cert-manager
```

Confirm that cert-manager's CRDs are installed:

```
kubectl get crd | grep cert-manager.io
```

You should see CRDs such as `certificates.cert-manager.io`, `clusterissuers.cert-manager.io`, etc.

2. Generate a list of cert-manager CRDs

Use kubectl's default output (table) and redirect it to a file. Do **not** set an output format:

```
kubectl get crd | grep cert-manager.io > ~/resources.yaml
```

The `resources.yaml` file will contain a table of CRDs with their names and creation timestamps. Although the file is named `.yaml`, its contents remain the default tabular output.

3. Document the `subject` field of Certificate

The `subject` field lives under `spec` of the `Certificate` CRD. Use `kubectl explain` to retrieve its description and nested fields:

```
kubectl explain certificates.cert-manager.io.spec.subject --recursive > ~/
subject.yaml
```

This command writes the documentation for `spec.subject` to `~/subject.yaml`. The `--recursive` flag includes nested subfields such as `commonName`, `organizationalUnits`, etc. You can verify the file with `less ~/subject.yaml`.

Notes

- **Do not set an explicit output format** when generating `resources.yaml`; the question requires the default kubectl format.
- **Any format is acceptable** for `subject.yaml`, but using `--recursive` gives you a complete overview of the field.
- These steps assume cert-manager is already installed in the cluster. If it isn't, install it first before proceeding.
