Kubernetes Override Sections

Advanced ⌄

Found in under `Advanced` in any section where you configure a component of the installer, under the `Kubernetes` heading. Here you can override Kubernetes configuration for each component.

Common

Common

Annotations

| Name to Create | Add to Annotations |

Annotations

In Kubernetes, annotations are key-value pairs associated with Kubernetes objects like pods, services, and nodes. Annotations are meant to be used for non-identifying metadata and are typically used to provide additional information about the objects. Unlike labels, which are used for identification and organization, annotations are more free-form and can contain arbitrary data.

Annotations are often used for various purposes, such as:

- **Documentation**.
  Providing additional information about a resource that might be useful for administrators or developers.
- **Tooling Integration**.
  Integrating with external tools or automation systems that rely on specific metadata.
- **Customisation**.
  Storing configuration information that affects the behaviour of controllers, operators, or custom tooling.

- **Audit Trailing.**
  Capturing additional information for audit or tracking purposes.

Ingress

Annotations

See explanation of <u>annotations</u> above

Services

Depending on the component you are viewing, you may see `Limits` and `Requests` broken out for each sub-component applicable to that component. When configuring Element Web you will only see the `Limits` and `Requests` config, for Integrator however, you will see `Limits` and `Requests` for each sub-component; `Appstore`; `Integrator`; `Modular Widgets`; and `Scalar Web`.

Workloads

Annotations

See explanation of **annotations** above

Resources

Depending on the component you are viewing, you may see Limits and Requests broken out for each sub-component applicable to that component. When configuring Element Web you will only see the Limits and Requests config, for Integrator however, you will see Limits and Requests for each sub-component; Appstore ; Integrator ; Modular Widgets ; and Scalar Web .

Limits

Requests

Security Context

Security Context

Force UID GID ▾

Enable pod runAsUser and fsGroup in security context. Disable if it should not be used, in the case of openshift for example. Auto attemps to detect openshift automatically.

FS Group

10019

The fsGroup GID to use if securityContextForceUidGid is enabled

Run as User

10019

The runAsUser UID to use if securityContextForceUidGid is enabled

Set Sec Comp ▾

Enable RuntimeDefault pod seccomp. disable if it should not be used, in the case of openshift for example. Auto attemps to detect openshift automatically.

Docker Secrets

Docker Secrets

Name *

Docker secret to use for ems image store

URL *

The docker registry url for this secret

Add more Docker Secrets

Host Aliases

Host Aliases

IP *

An IP resolution to add to /etc/hosts

Hostnames

An hostname of the associated ip to add t...

Add more Hostnames

Add more Host Aliases

Revision #3
Created 6 November 2024 10:22:31 by Kieran Mitchell Lane
Updated 6 November 2024 13:22:45 by Kieran Mitchell Lane