Tool Detection

The tool used to build an application is detected as follows:

If a specific tool is explicitly configured, then that tool is selected to create your application's manifests.

The tool can be explicitly specified in the Application custom resource like this:

```
apiVersion: argoproj.io/v1alpha1
kind: Application
metadata:
  ...
spec:
  ...
  source:
    ...

    # Tool -> plain directory
    directory:
      recurse: true
...
```

You also can select the tool in the Application creation wizard in the web user interface. The default is 'Directory'. Press the dropdown button beneath the tool name if you want to choose a different one.

If not, then the tool is detected implicitly as follows:

- **Helm** if there's a file matching `Chart.yaml`.
- **Kustomize** if there's a `kustomization.yaml`, `kustomization.yml`, or `Kustomization`

Otherwise it is assumed to be a plain **directory** application.

Disable built-in tools

Built-in config management tools can be optionally disabled by setting one of the following keys, in the `argocd-cm` ConfigMap, to `false`: `kustomize.e` `jsonnet.enable`. Once the tool is disabled, Argo CD will assume the application target directory contains plain Kubernetes YAML manifests.

stable

Disabling unused config management tools can be a helpful security enhancement. Vulnerabilities are sometimes limited to certain config management tools. Even if there is no vulnerability, an attacker may use a certain tool to take advantage of a misconfiguration in an Argo CD instance. Disabling unused config management tools limits the tools available to malicious actors.

Multirepo, multi-provider CI/CD. Link GitHub, GitLab, Bitbucket, Perforce in one project.
Try TeamCity

Ads by EthicalAds

stable