Taming the Pets

Managing a heterogenous and sovereign multi-cloud container platform

Lukas Reusser <lukas.reusser@sbb.ch>
Michael Grüner <michael.gruener@sbb.ch>
Boston, 22.05.2023

Swiss Federal Railways

Swiss Federal Railways – Facts & Figures

- Employees: 34’227
- Working in IT: 1’500
- Developers: 700

Swiss Federal Railways – Facts & Figures

- Employees: 34’227
- Working in IT: 1’500
- Developers: 700
- Trains on the network per day: 11’338

Swiss Federal Railways – Facts & Figures

- Employees: 34’227
- Working in IT: 1’500
- Developers: 700
- Trains on the network per day: 11’338
- Passengers per day: 1.16 millions

Swiss Federal Railways – Facts & Figures

- Employees: 34’227
- Working in IT: 1’500
- Developers: 700
- Trains on the network per day: 11’338
- Passengers per day: 1.16 millions
- Mobile app has 3.5 million active users daily (40% of Swiss population)

Swiss Federal Railways – Facts & Figures

- Employees: 34’227
- Working in IT: 1’500
- Developers: 700
- Trains on the network per day: 11’338
- Passengers per day: 1.16 millions
- Mobile app has 3.5 million active users daily (40% of Swiss population)
- 300’000 tickets sold per day

Swiss Federal Railways – Fun Facts

- Longest Tunnel: 57.1 km (35.5 mi) (Gotthard Base Tunnel) world record
- 8 Hydroelectric power plants

Swiss Federal Railways – Chocolate Quiz

What is the customer punctuality of our trains?
(with less than 3 minutes of delay):

- 72.1%
- 79.4%
- 88.3%
- 92.5%

Swiss Federal Railways – Chocolate Quiz

What is the customer punctuality of our trains?
(with less than 3 minutes of delay):

- 72.1%
- 79.4%
- 88.3%
- 92.5%

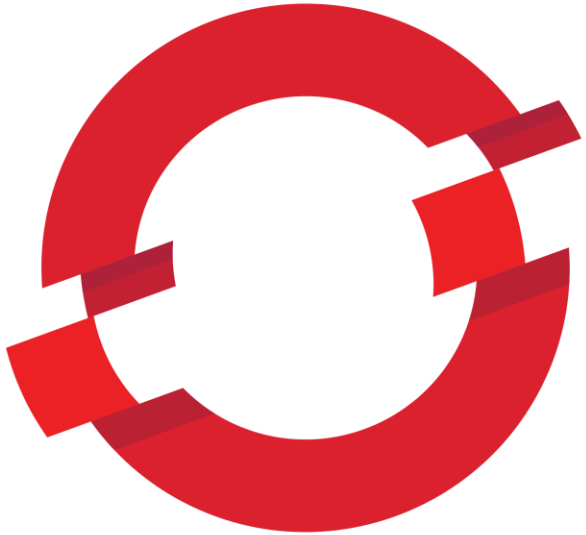
No one wants Swiss chocolate?

Swiss Federal Railways – Chocolate Quiz

What is the customer punctuality of our trains?
(with less than 3 minutes of delay):

- 72.1%
- 79.4%
- 88.3%
- 92.5% ←

No one wants Swiss chocolate?



Introducing:
The Swiss Railways Container Platform

Container Platform History

- Started with OpenShift 3.0 in 2015
- One cluster on AWS
- One huge cluster (for that time) on premise
- Operation was not as good as today:
  - Monitoring missed expiration of internal CA
  - Long nights because of Ansible “gather facts...”
  - Different kind of performance issues: SDN, iptables, number of pods on nodes, etc.
- Number of clusters grow, especially with OpenShift 4

Container Platform Today

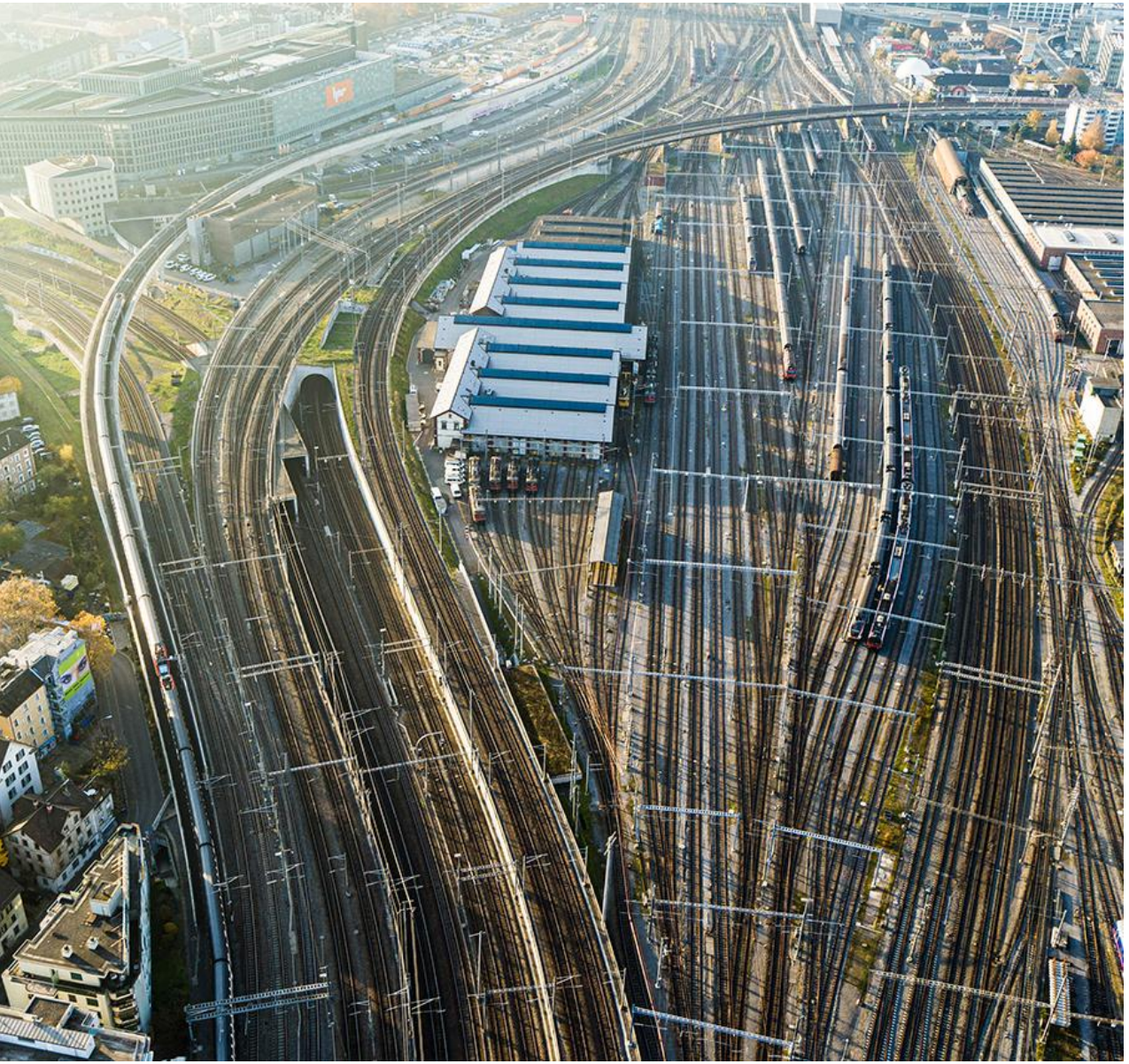
- 42 clusters, 800 nodes, 11’000 vCPUs, tons of memory
- 6 Development clusters
- 19 Test clusters
- 17 Production clusters
- Multi cloud strategy
  - AWS
  - Azure
  - Open Telekom Cloud
- Applications: mostly Java Spring Boot, Kafka, PostgreSQL

SBB CFF FFS

Container Platform Team

Container Platform Team

- 7 Engineers (including product owner) + scrum master
- 24/7 on-call service + engineer on duty
- Having fun at and beside work

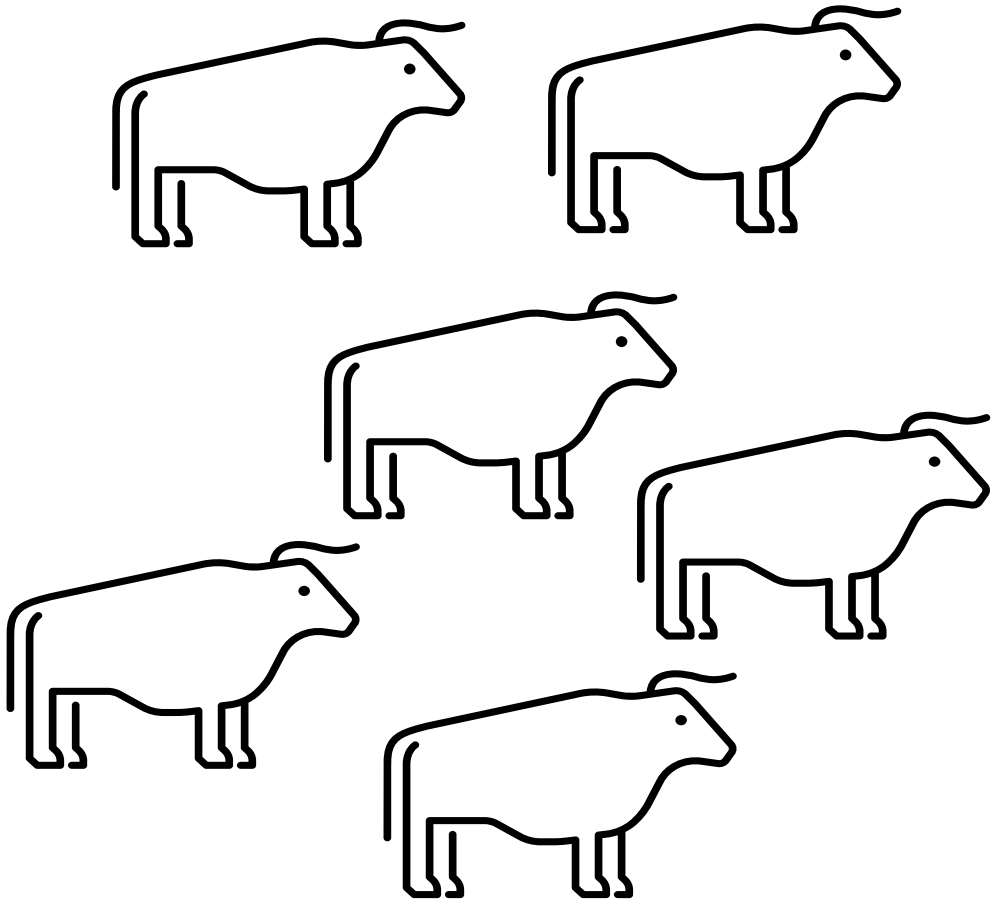


The Challenge

Pet

vs.

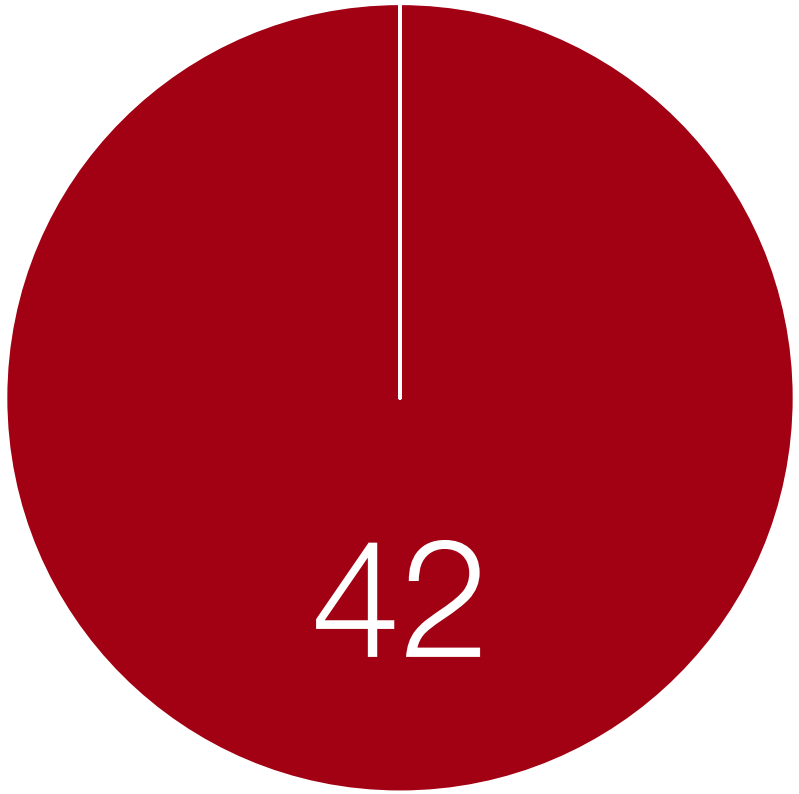
Cattle



Ideal world

All clusters are equal ...

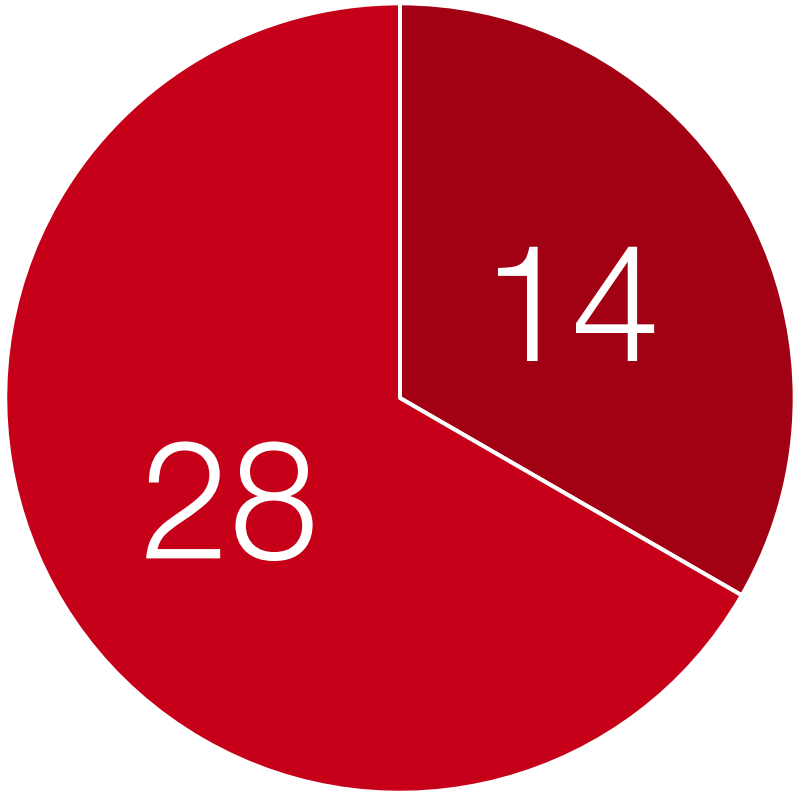
OpenShift
Cluster



Reality

… but some clusters are less equal than others …

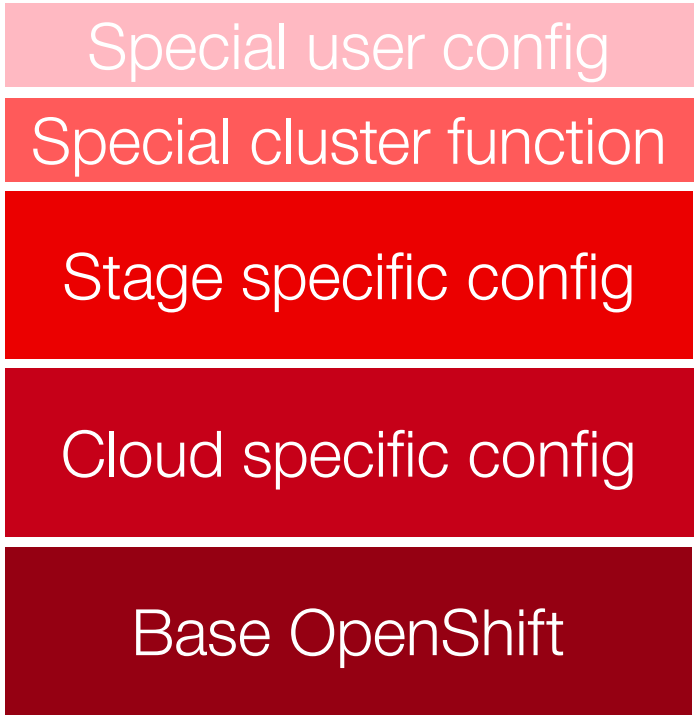
Dedicated clusters



Shared clusters

Harsh Truth

… and probably not even 2 clusters are the same.



Acceptance

We are not a cattle farm …

Acceptance

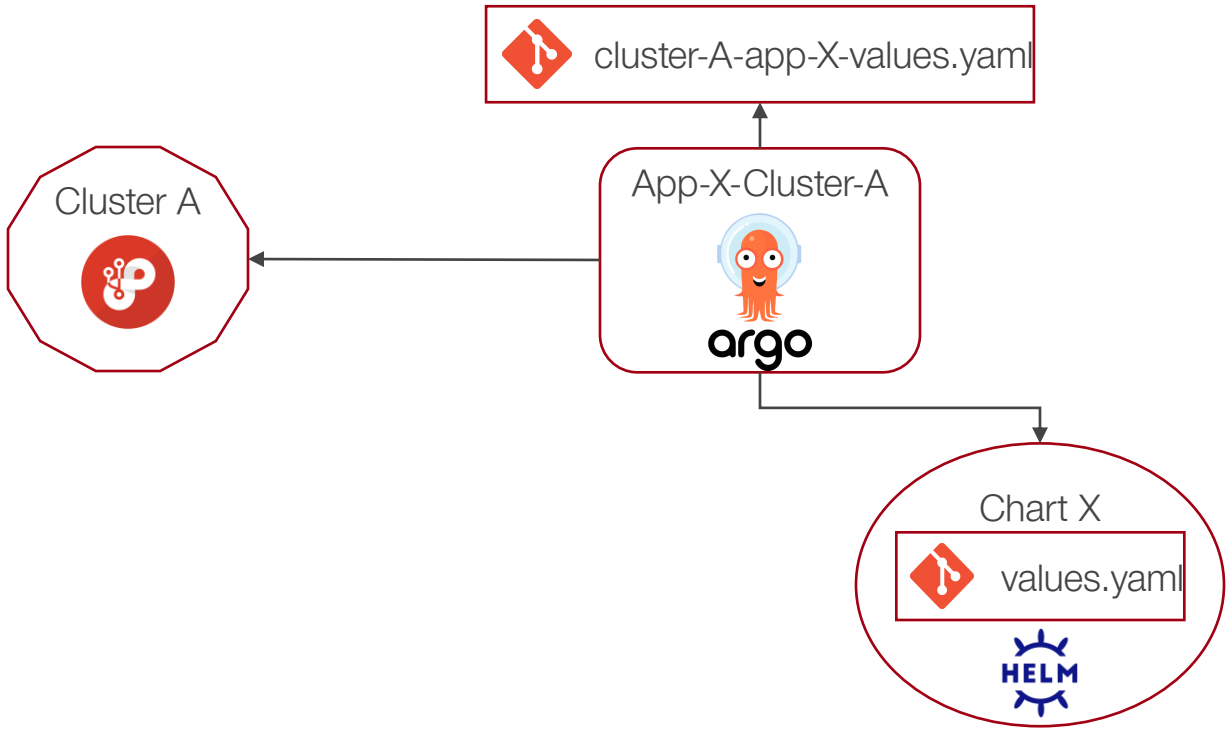
We are not a cattle farm …

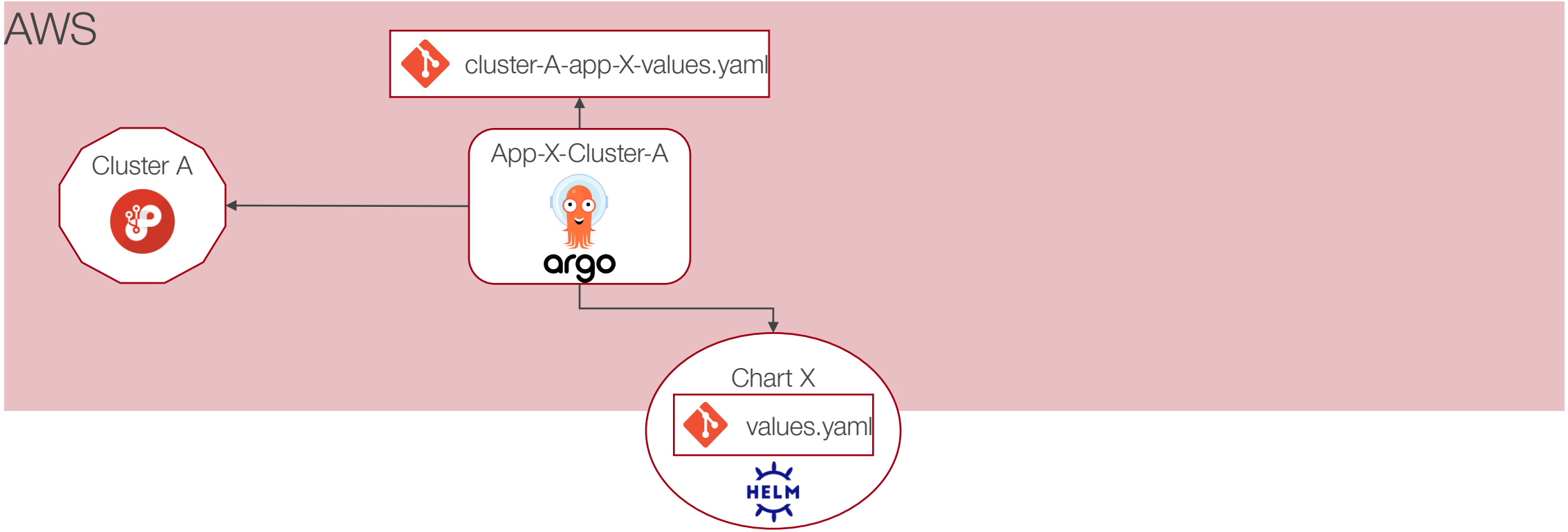
… we are a pet hotel.

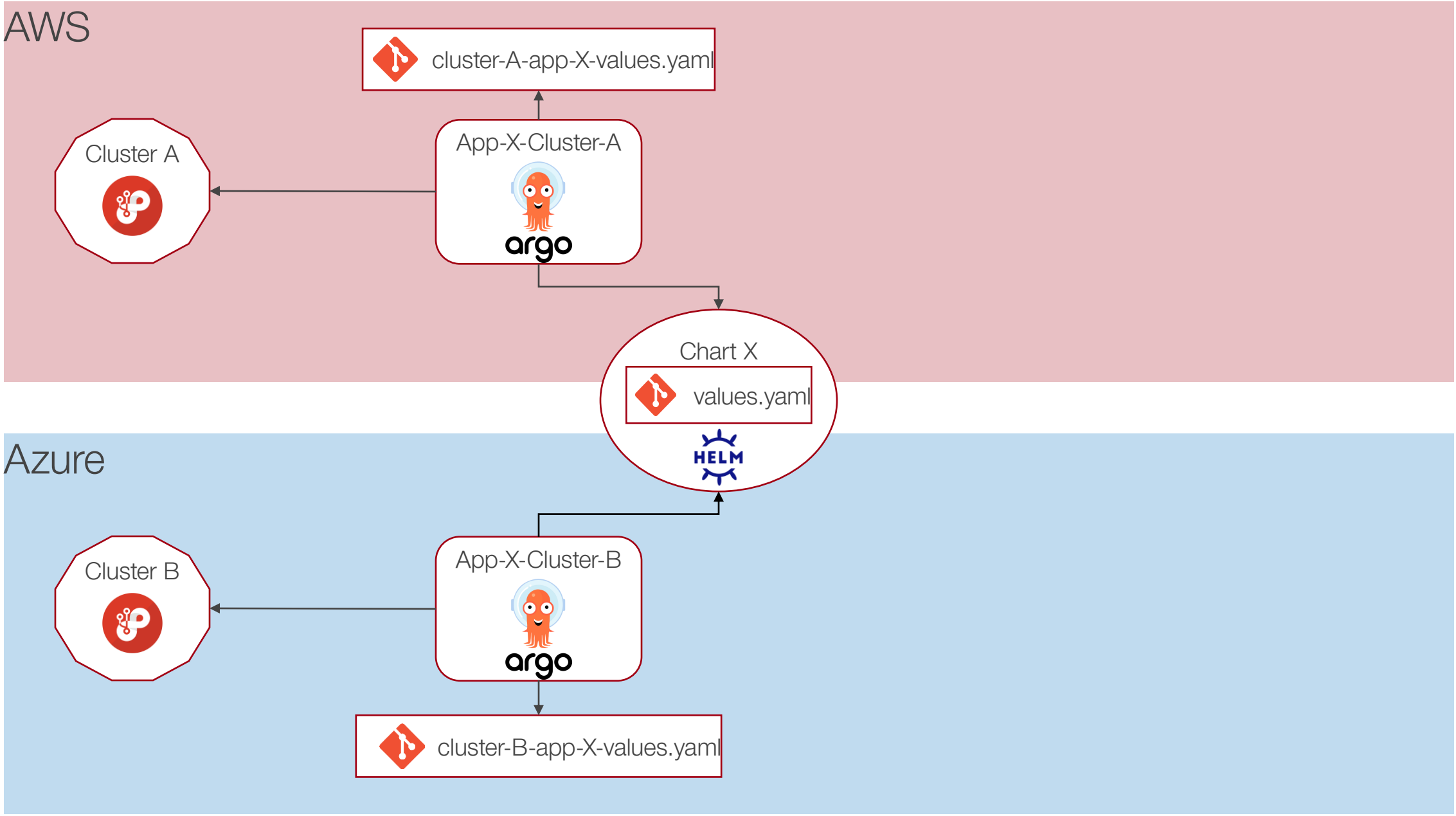
The Tools

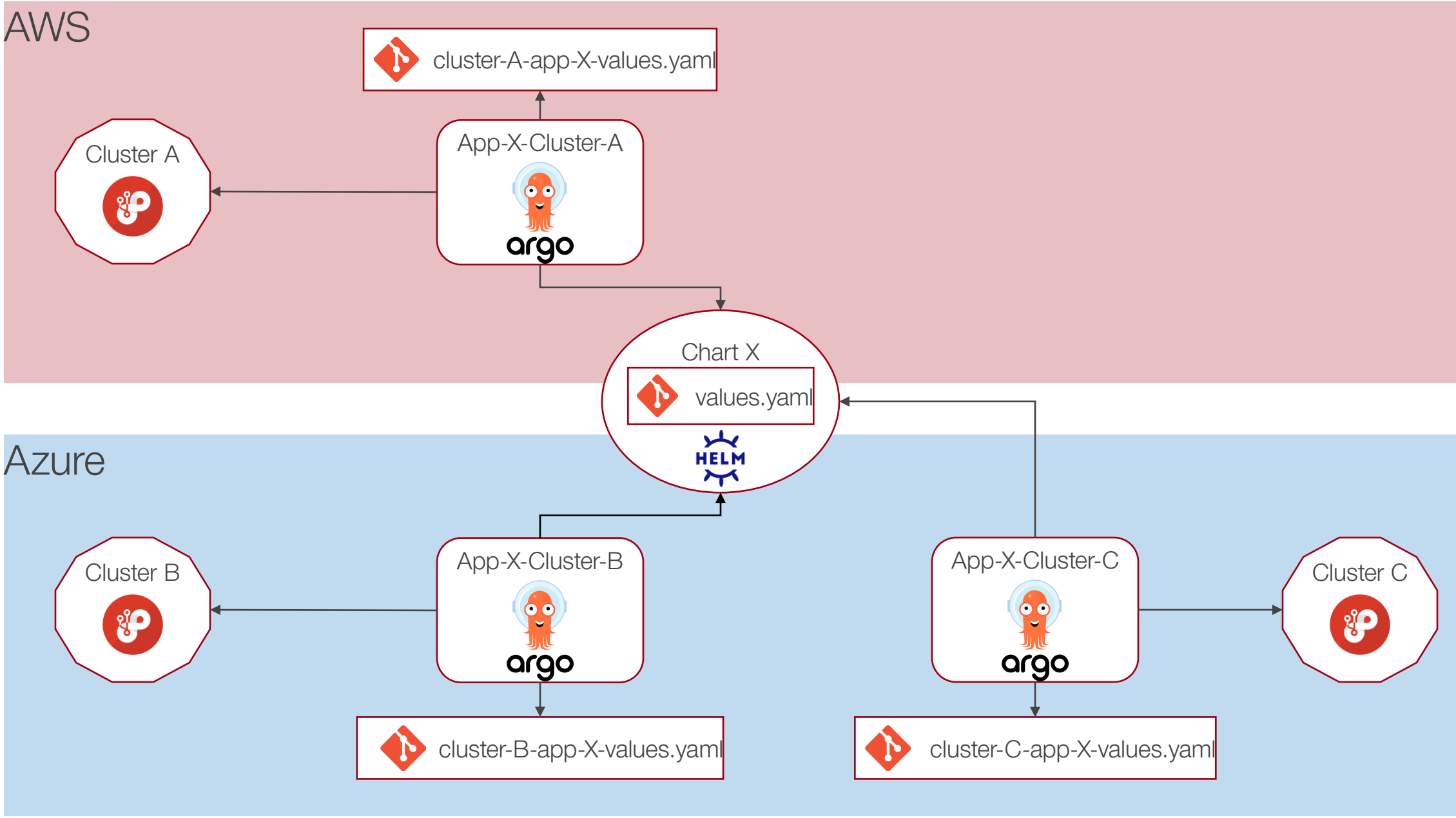
(and their issues)

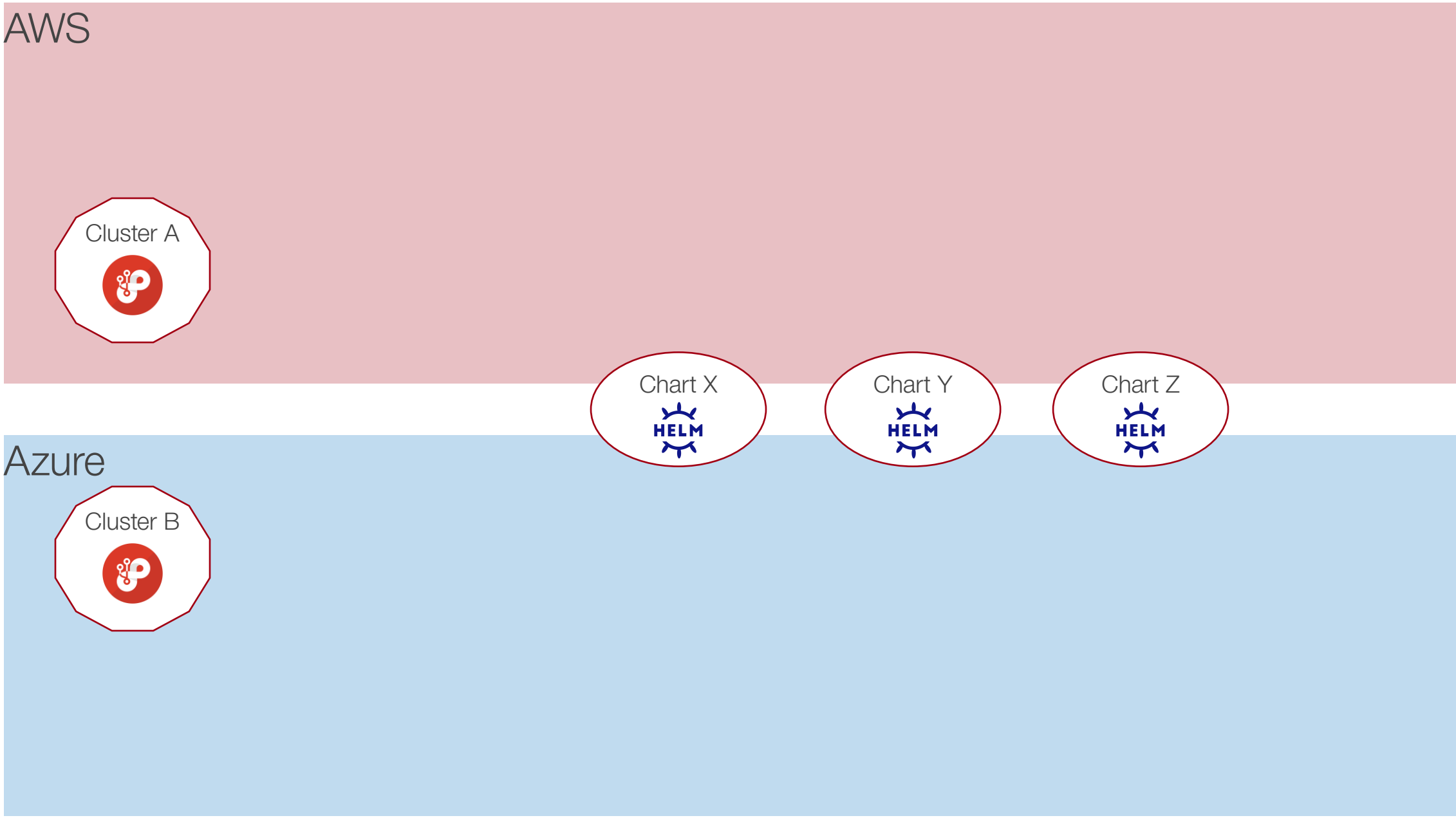
The Tools

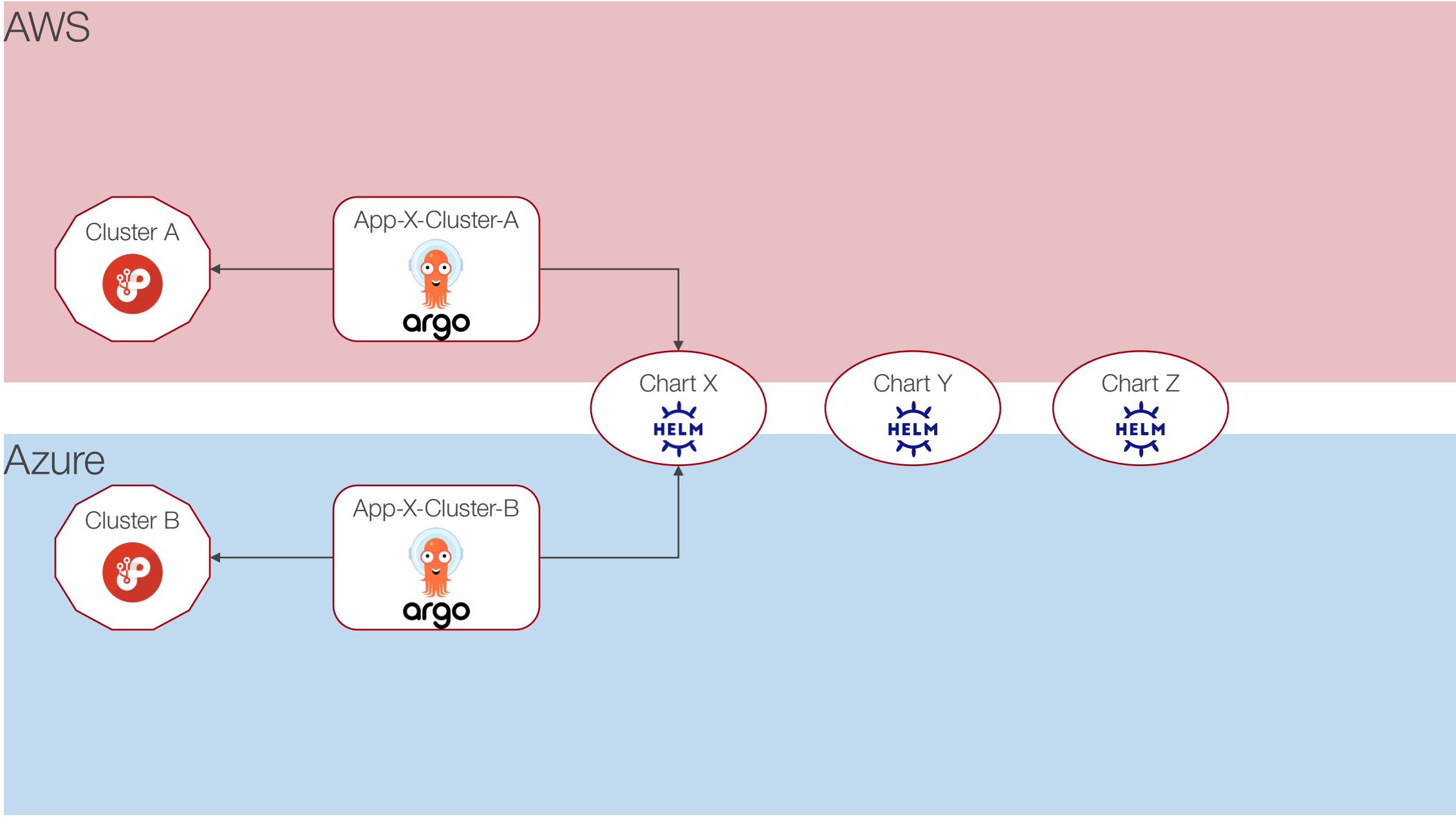

cluster-A-app-X-values.yaml
Cluster A
App-X-Cluster-A
argo
Chart X
values.yaml
HELM

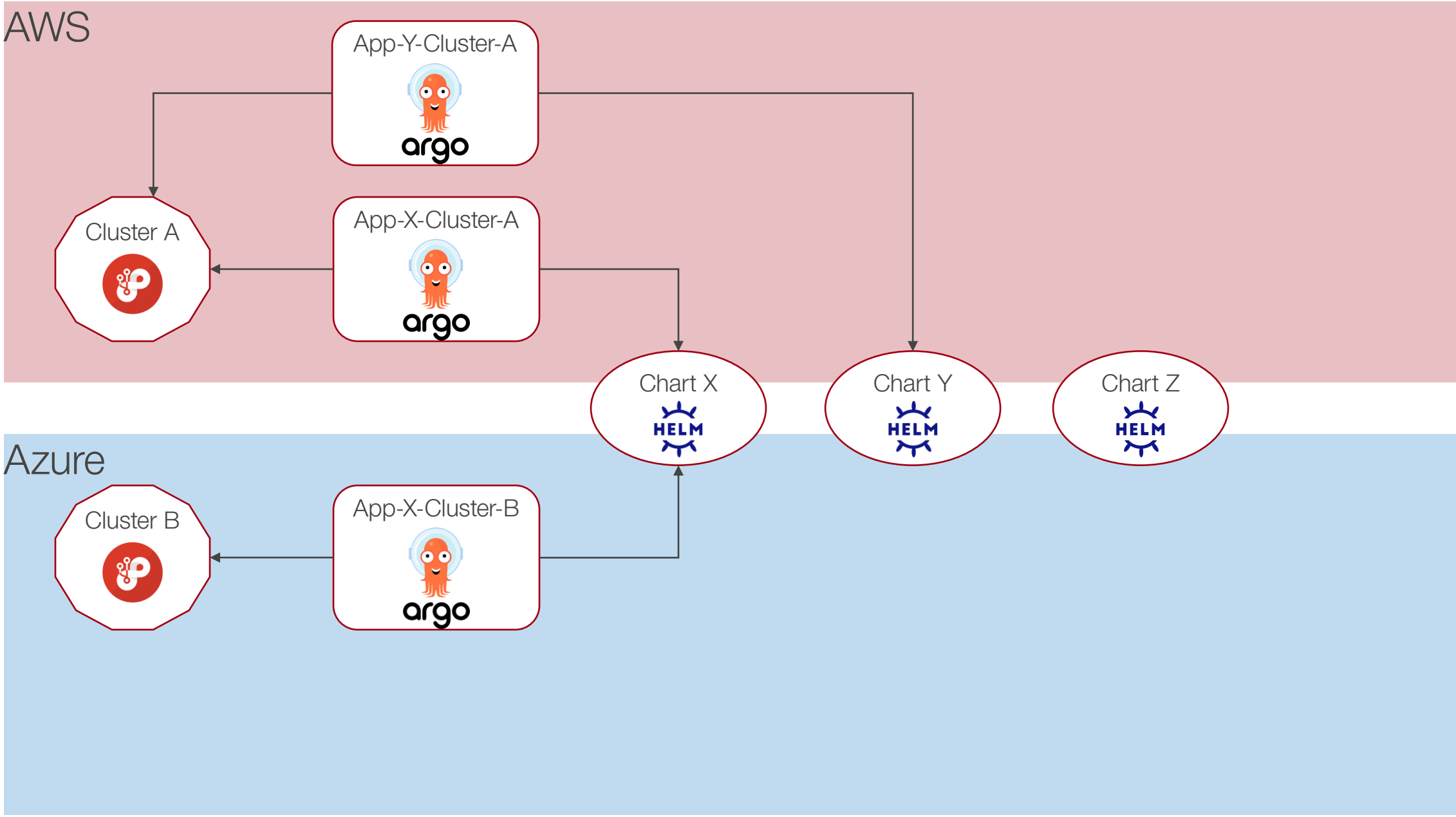

AWS
cluster-A-app-X-values.yaml
Cluster A
App-X-Cluster-A
argo
Chart X
values.yaml
HELM

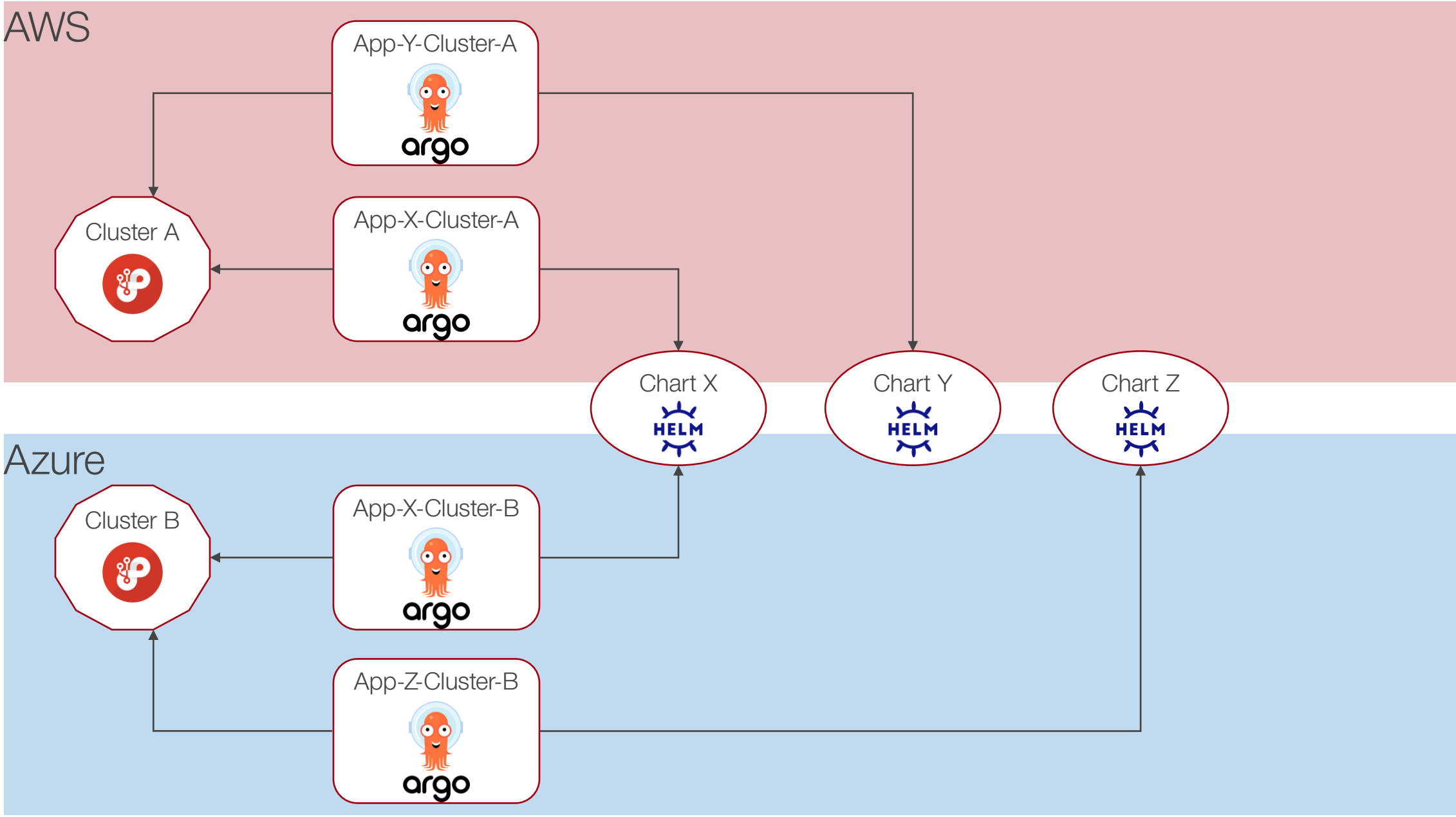

AWS
cluster-A-app-X-values.yaml
Cluster A
App-X-Cluster-A
argo
Chart X
values.yaml
HELM
Azure
Cluster B
App-X-Cluster-B
argo
cluster-B-app-X-values.yaml

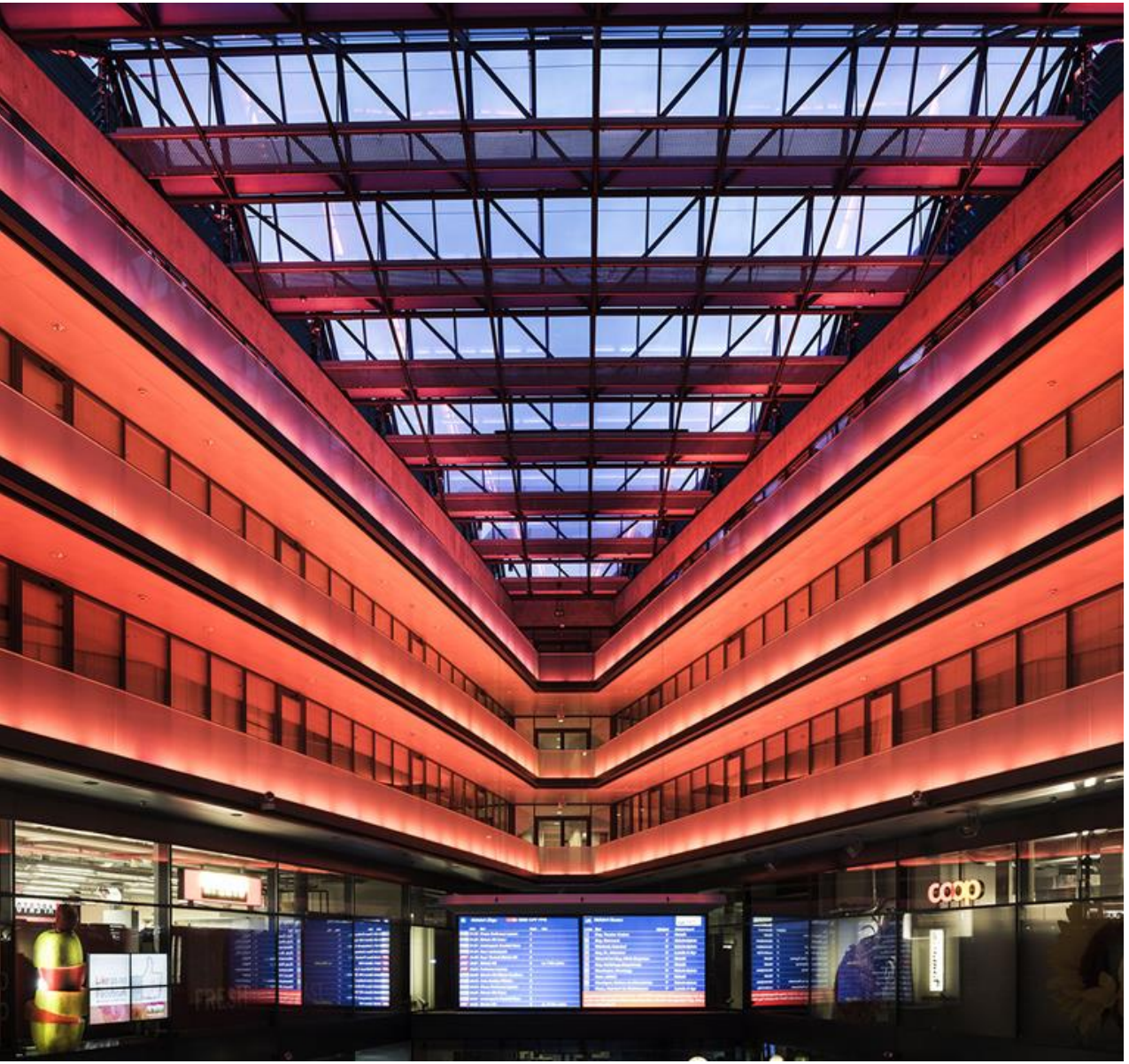

AWS
cluster-A-app-X-values.yaml
Cluster A
App-X-Cluster-A
argo
Chart X
values.yaml
HELM
Azure
Cluster B
App-X-Cluster-B
argo
App-X-Cluster-C
argo
Cluster C
cluster-B-app-X-values.yaml
cluster-C-app-X-values.yaml


AWS
Cluster A
Chart X
HELM
Chart Y
HELM
Chart Z
HELM
Azure
Cluster B


AWS
Cluster A
App-X-Cluster-A
argo
Chart X
HELM
Chart Y
HELM
Chart Z
HELM
Azure
Cluster B
App-X-Cluster-B
argo

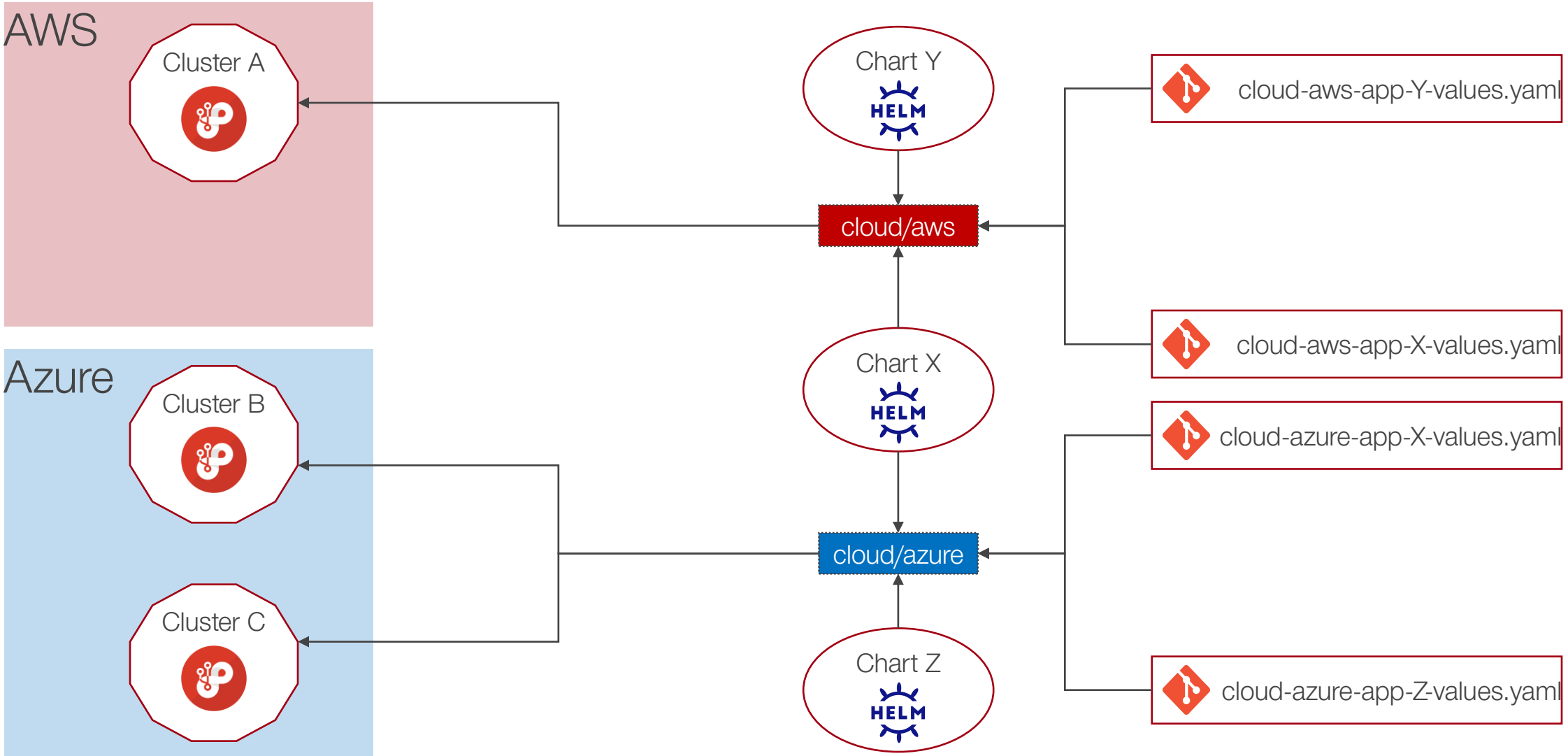

AWS
App-Y-Cluster-A
argo
Cluster A
App-X-Cluster-A
argo
Chart X
HELM
Chart Y
HELM
Chart Z
HELM
Azure
Cluster B
App-X-Cluster-B
argo


AWS
App-Y-Cluster-A
argo
Cluster A
App-X-Cluster-A
argo
Chart X
HELM
Chart Y
HELM
Chart Z
HELM
Azure
Cluster B
App-X-Cluster-B
argo
App-Z-Cluster-B
argo

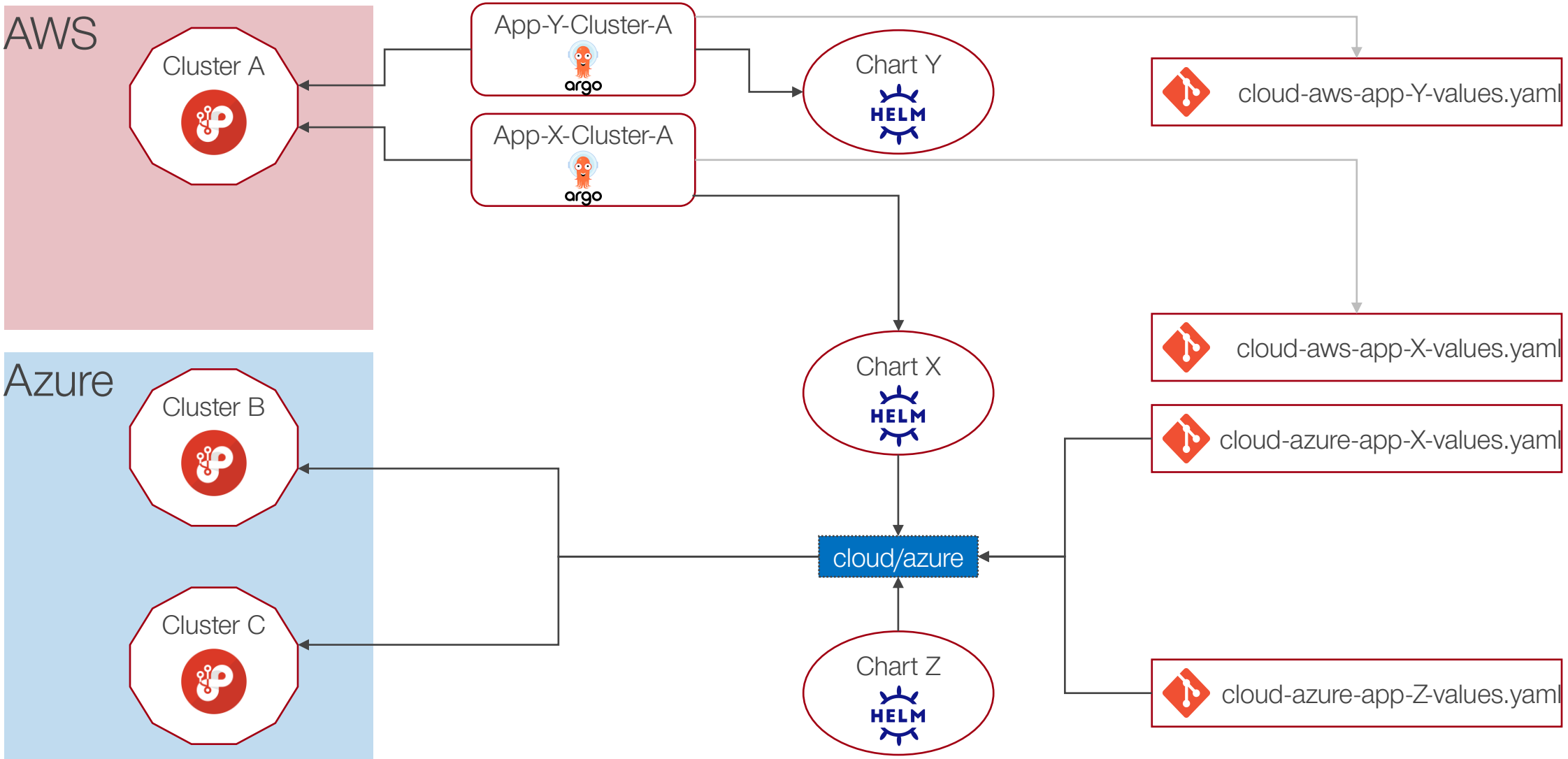


The Concept

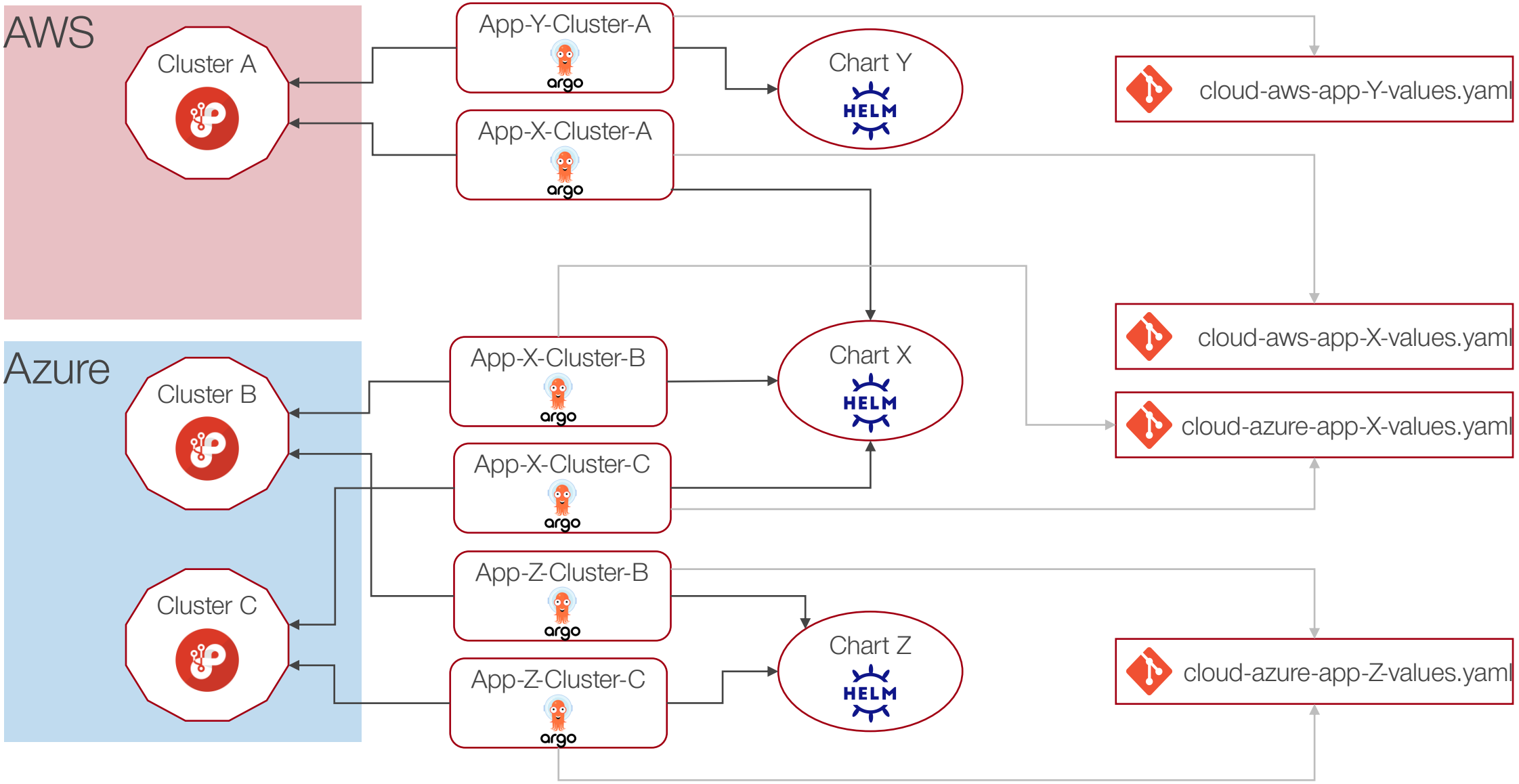
Introducing: Groups



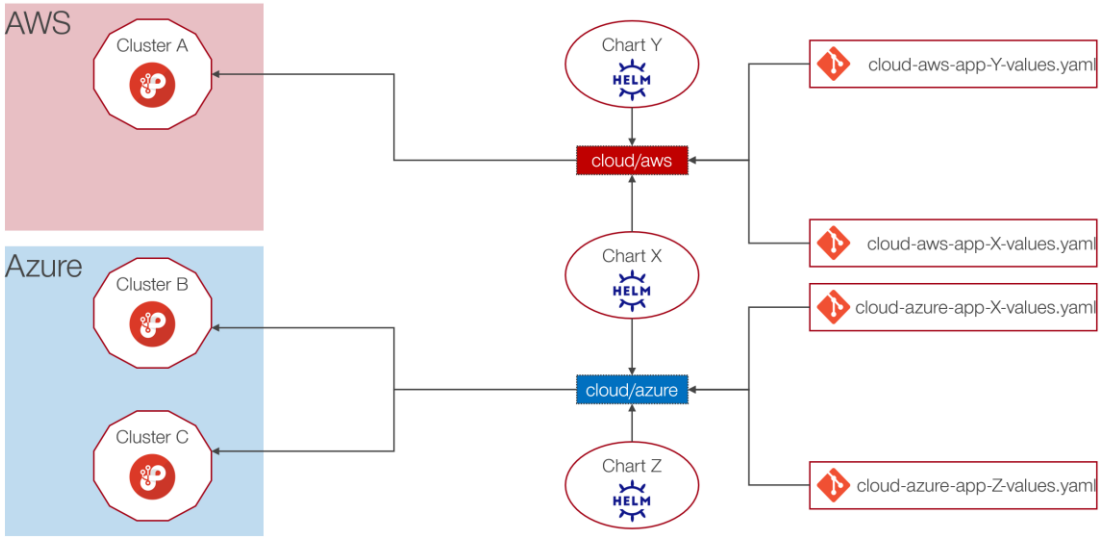
Introducing: Groups



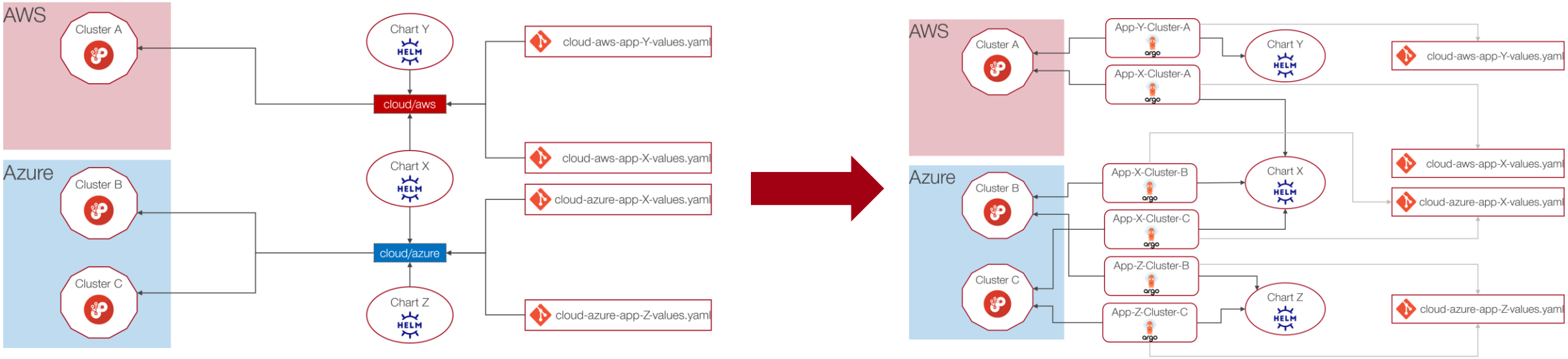
Introducing: Groups



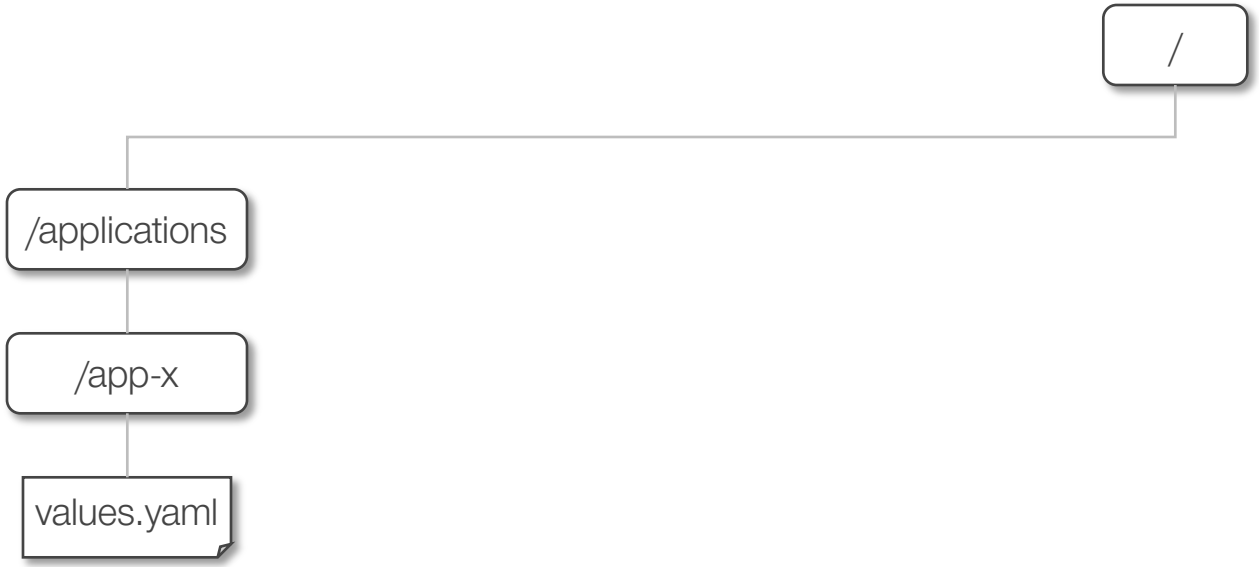
Introducing: Groups

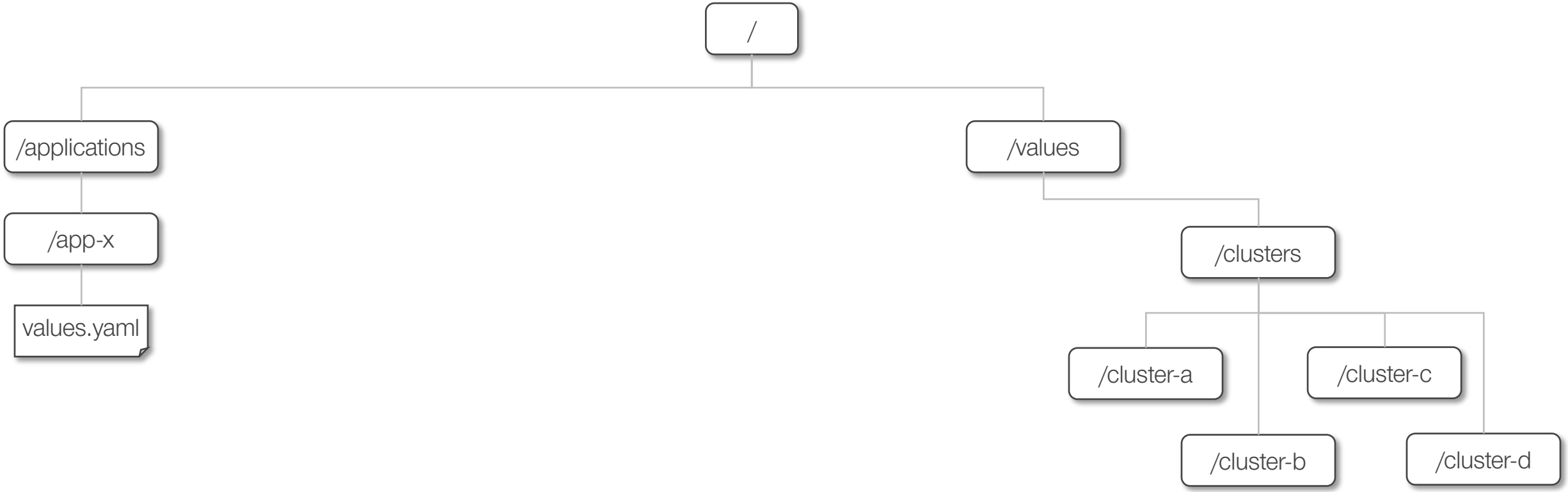


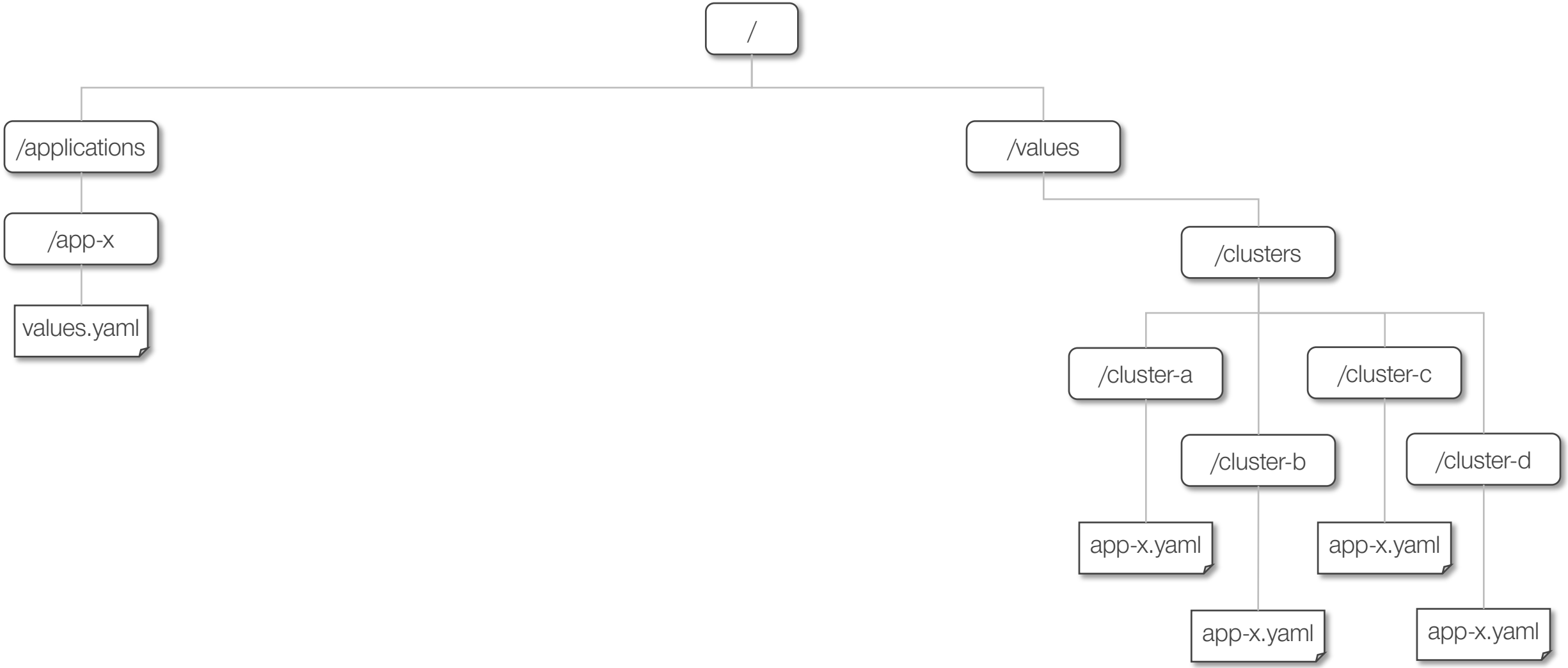
Introducing: Groups

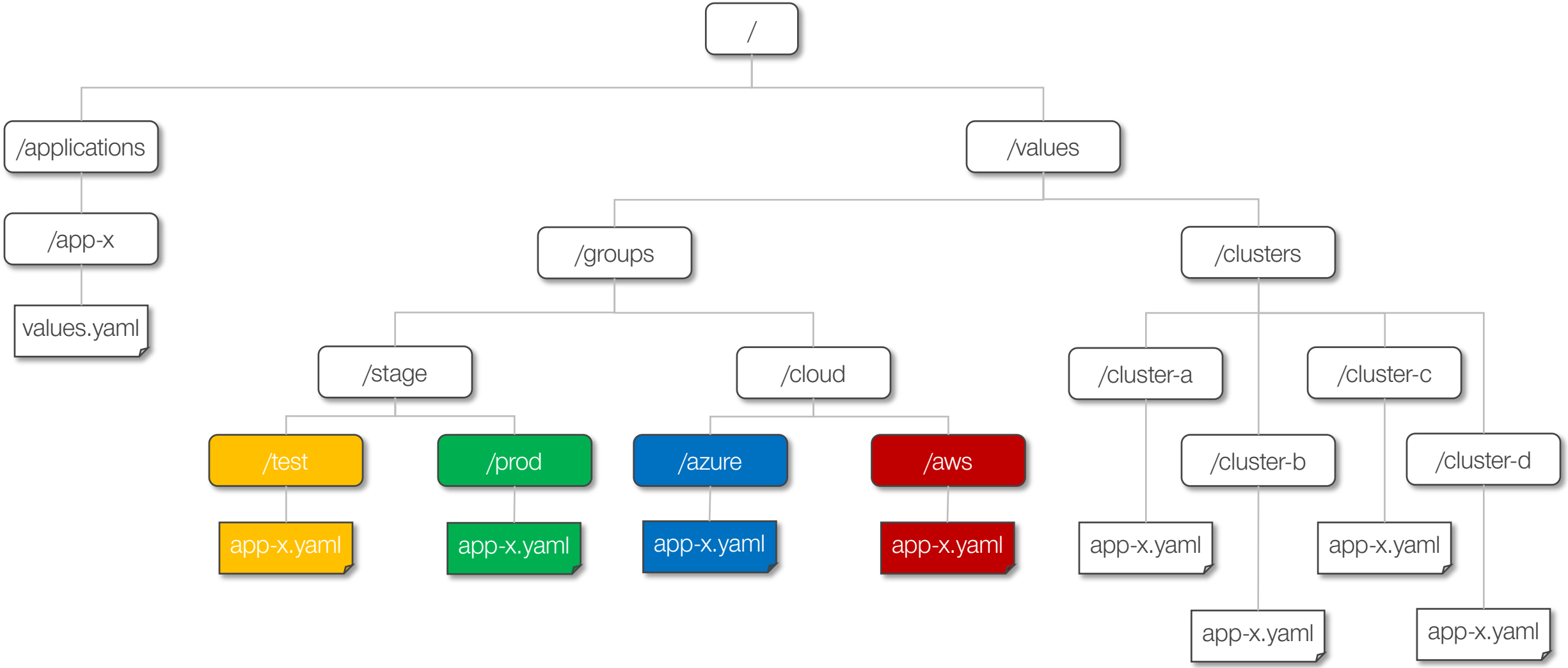


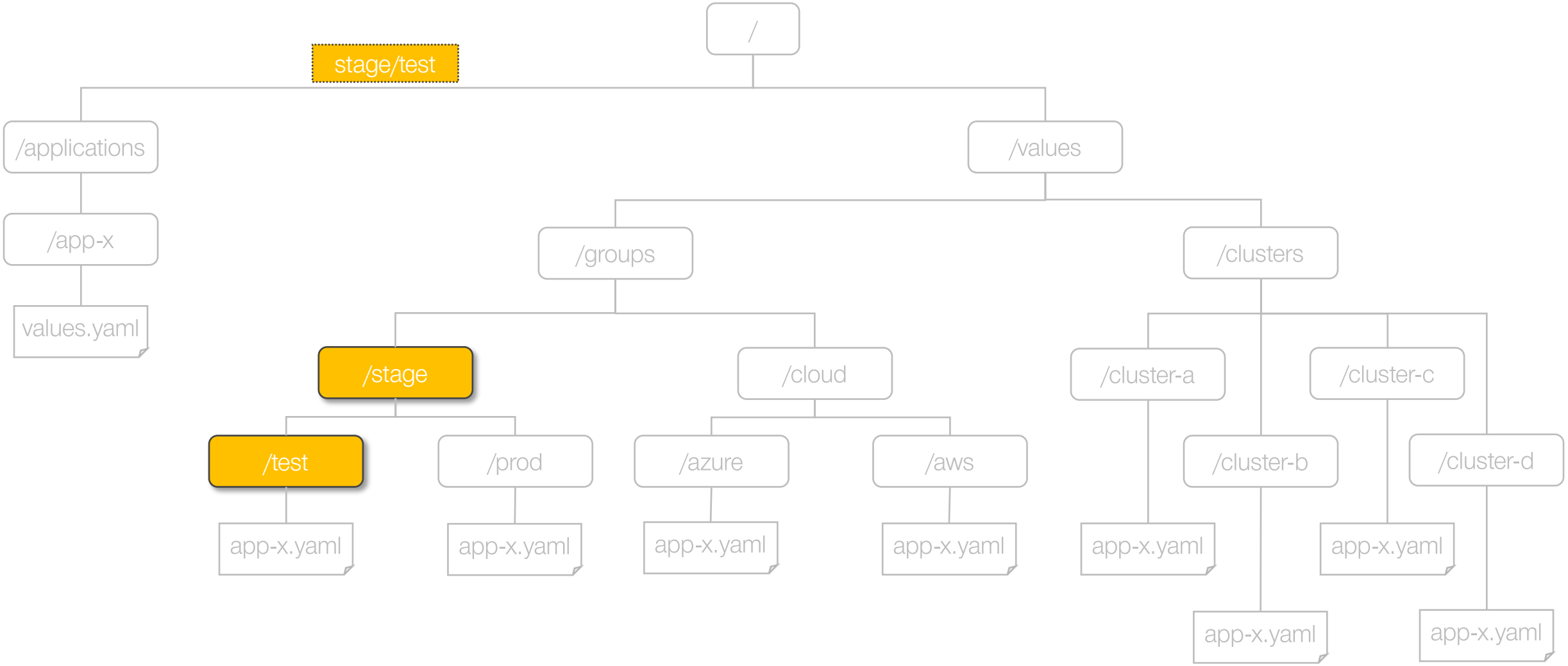
The Implementation

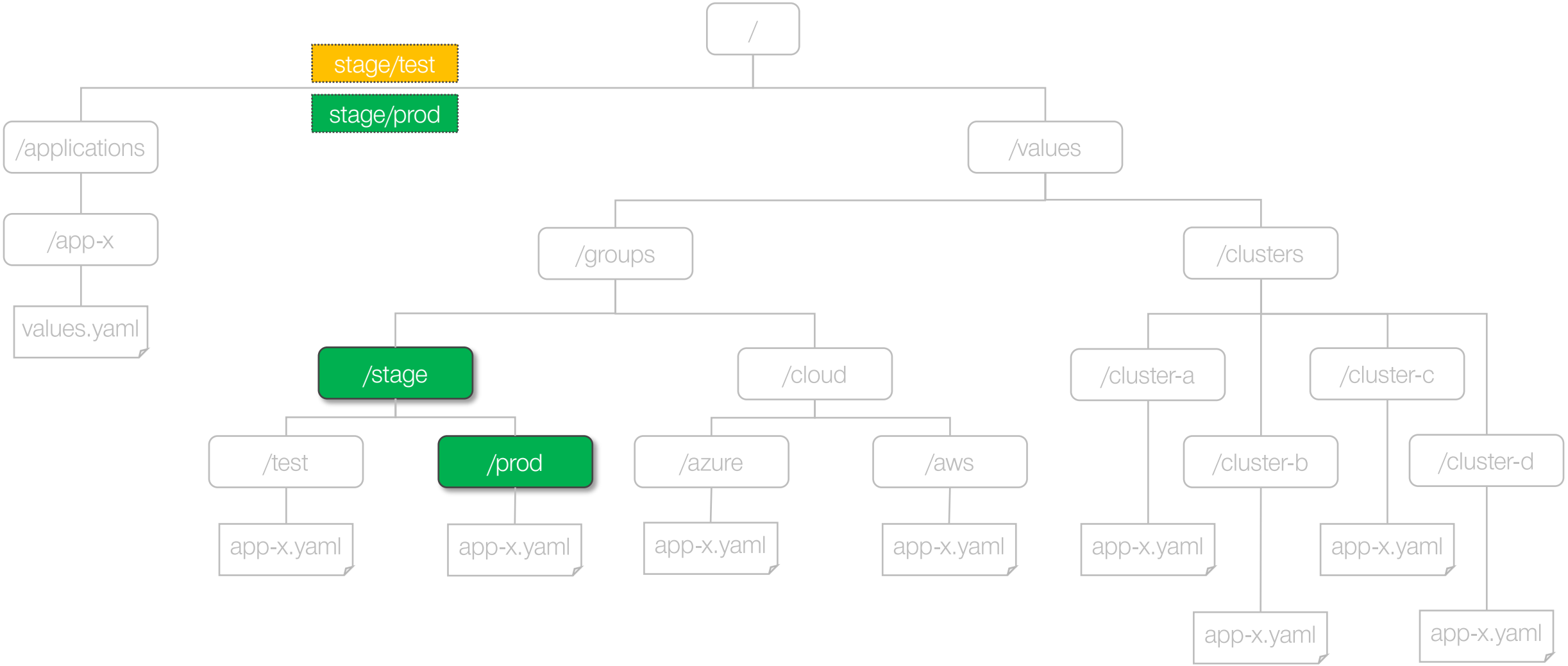

/
/applications
/app-x
values.yaml

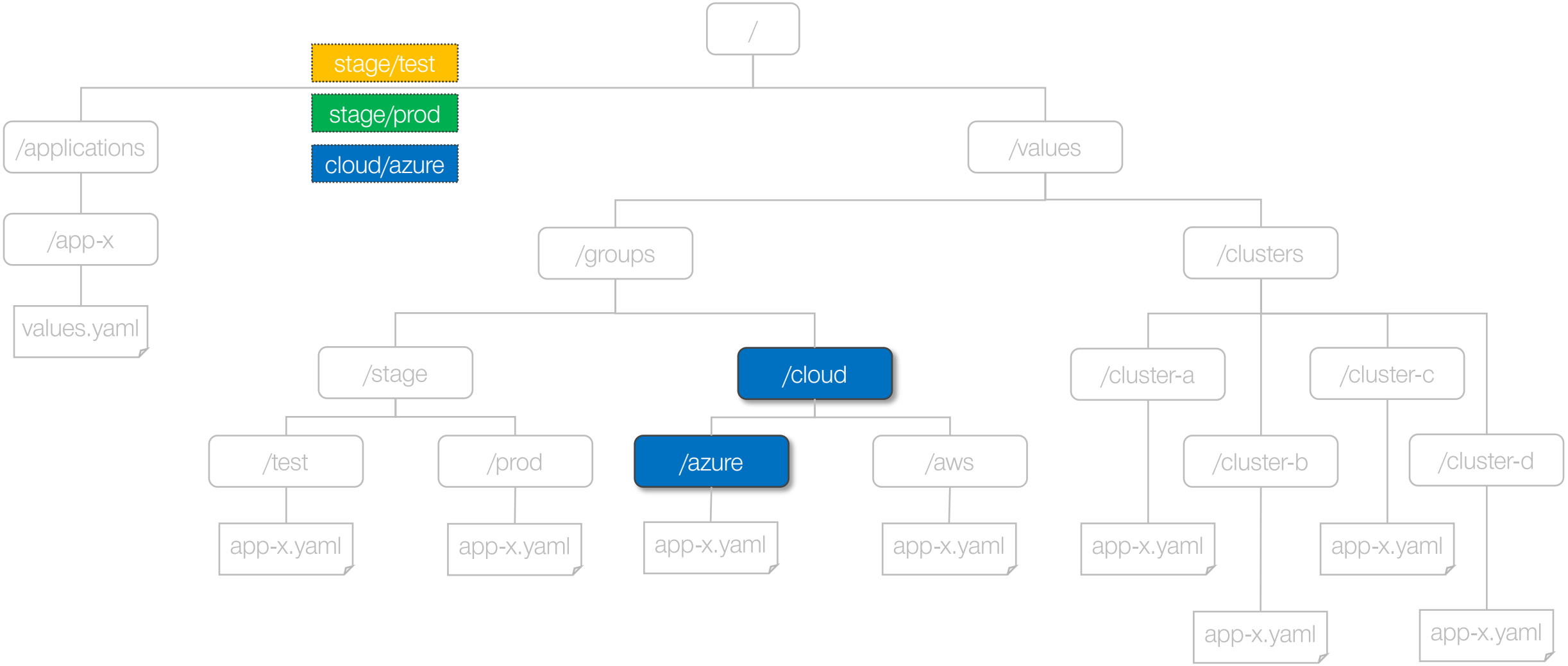

/
/applications
/app-x
values.yaml
/values
/clusters
/cluster-a
/cluster-b
/cluster-c
/cluster-d

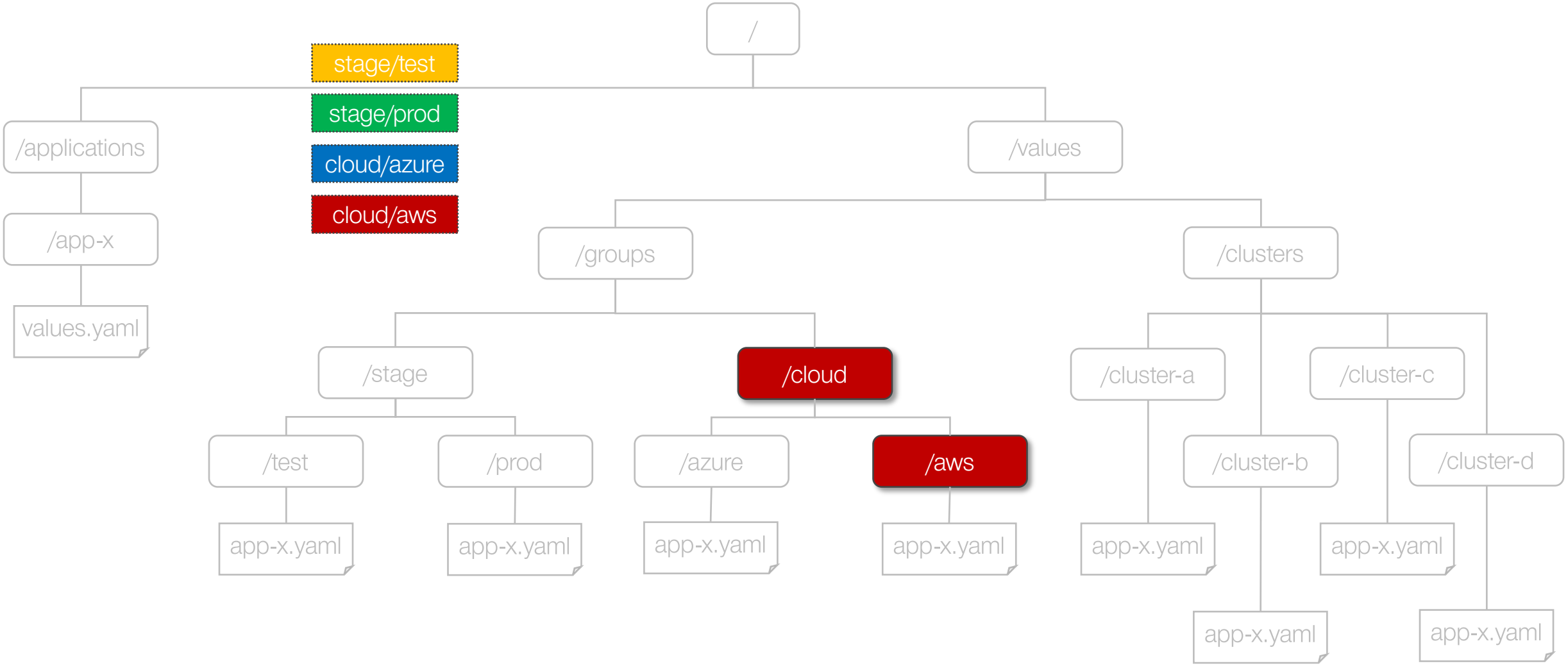

/
/applications
/app-x
values.yaml
/values
/clusters
/cluster-a
/cluster-b
/cluster-c
/cluster-d
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml


/
/applications
/app-x
values.yaml
/values
/groups
/stage
/test
app-x.yaml
/prod
app-x.yaml
/cloud
/azure
app-x.yaml
/aws
app-x.yaml
/clusters
/cluster-a
app-x.yaml
/cluster-b
app-x.yaml
/cluster-c
app-x.yaml
/cluster-d
app-x.yaml

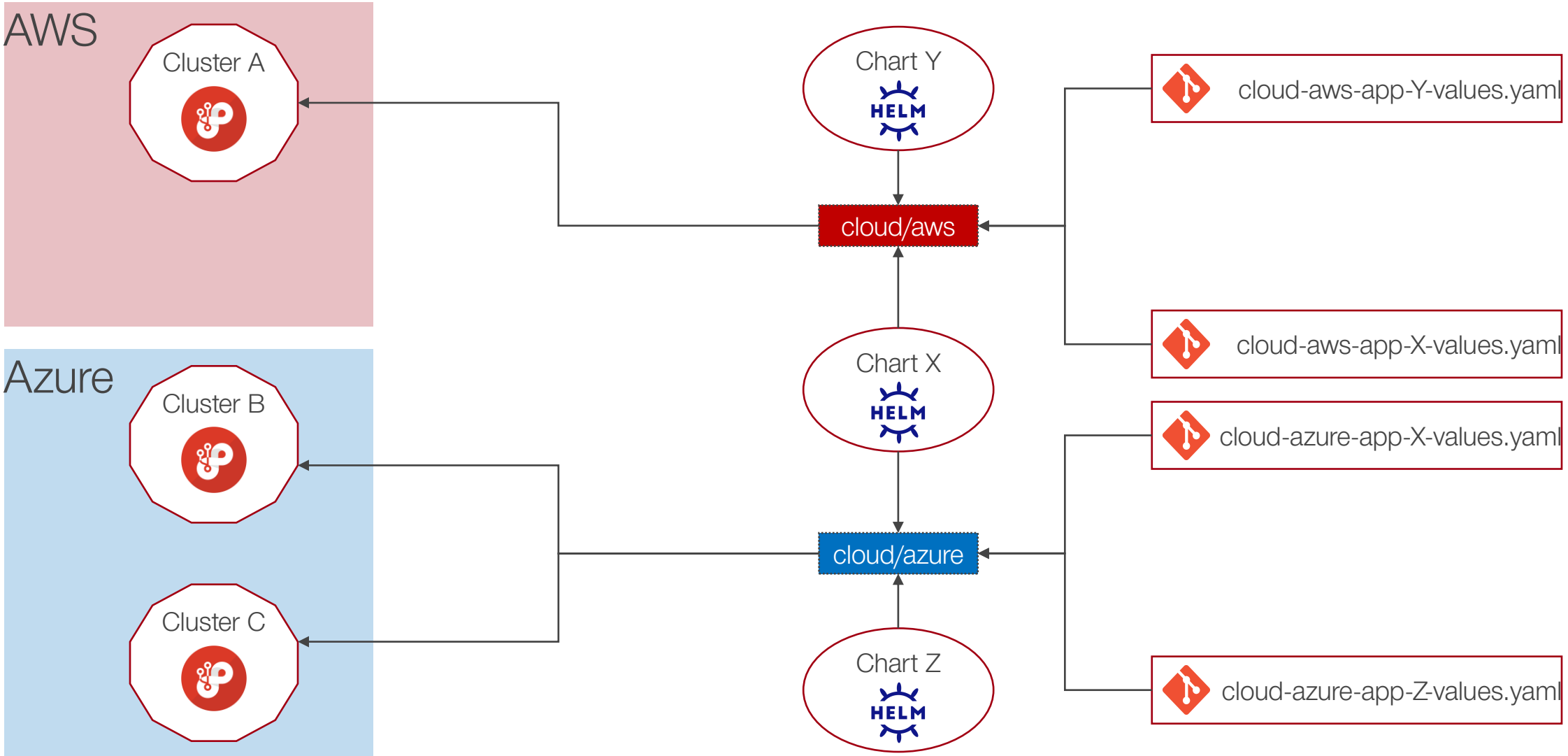

/
stage/test
/applications
/values
/app-x
values.yaml
/groups
/clusters
/stage
/cloud
/cluster-a
/cluster-c
/test
/prod
/azure
/aws
/cluster-b
/cluster-d
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml


/
stage/test
stage/prod
/applications
/app-x
values.yaml
/values
/groups
/clusters
/stage
/cloud
/cluster-a
/cluster-c
/test
/prod
/azure
/aws
/cluster-b
/cluster-d
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml

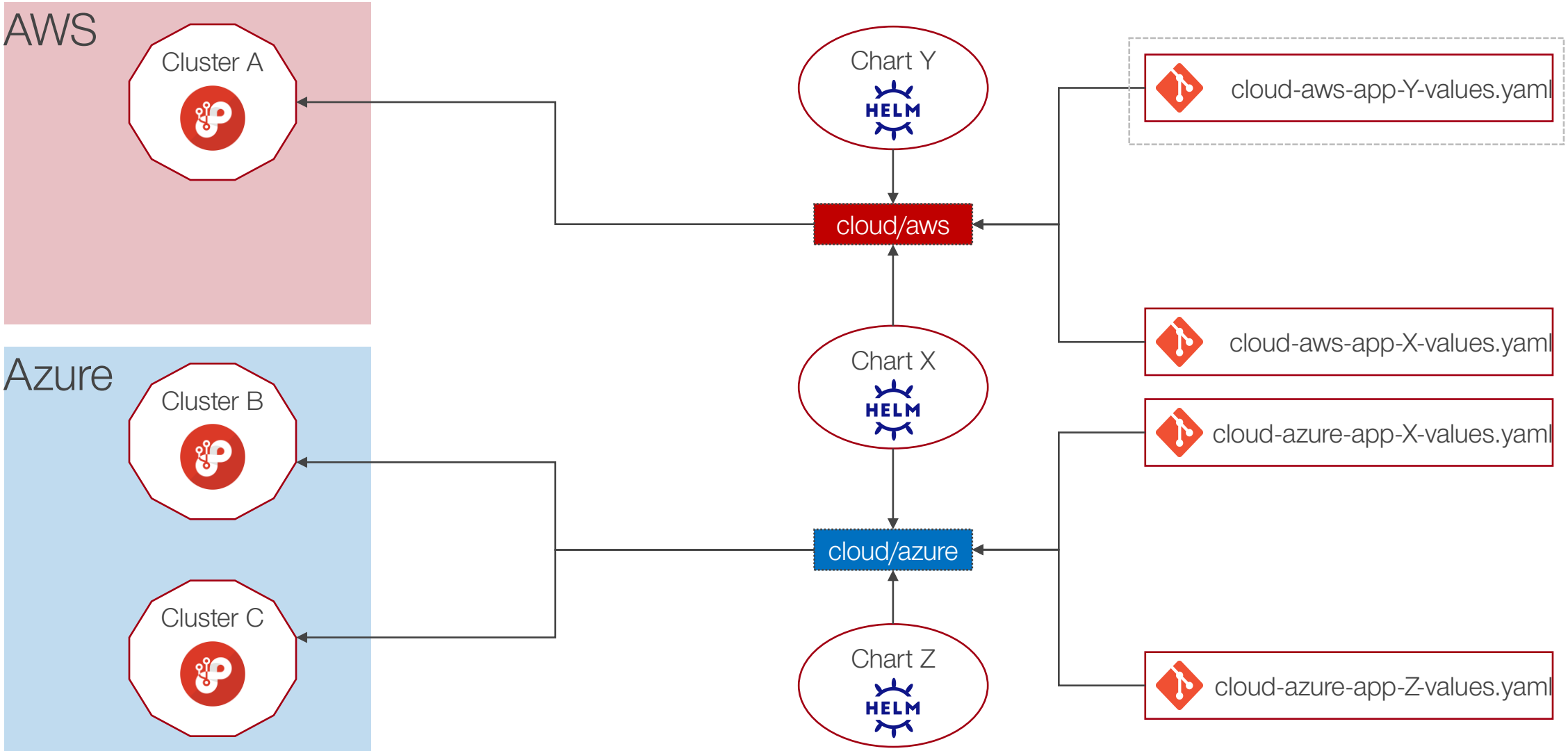

/
stage/test
stage/prod
cloud/azure
/applications
/app-x
values.yaml
/values
/groups
/clusters
/stage
/cloud
/test
/prod
/azure
/aws
/cluster-a
/cluster-b
/cluster-c
/cluster-d
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml

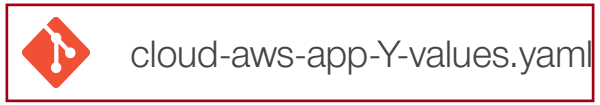

/
stage/test
stage/prod
cloud/azure
cloud/aws
/applications
/app-x
values.yaml
/values
/groups
/clusters
/stage
/cloud
/test
/prod
/azure
/aws
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml
/cluster-a
/cluster-c
/cluster-b
/cluster-d
app-x.yaml
app-x.yaml
app-x.yaml
app-x.yaml

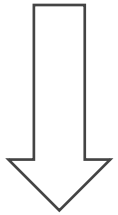
Introducing: Groups



Introducing: Groups




cloud-aws-app-Y-values.yaml



cloud/aws

values/groups/**cloud/aws**/app-y.yaml

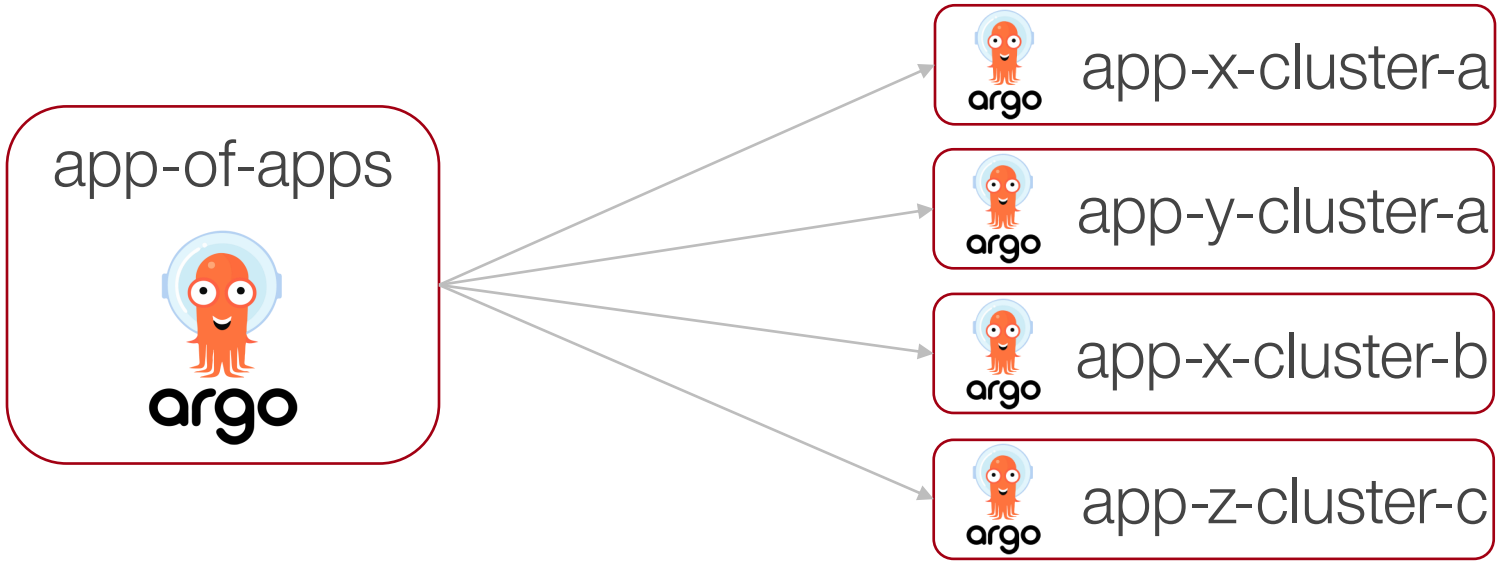
FANCY!

cloud/aws

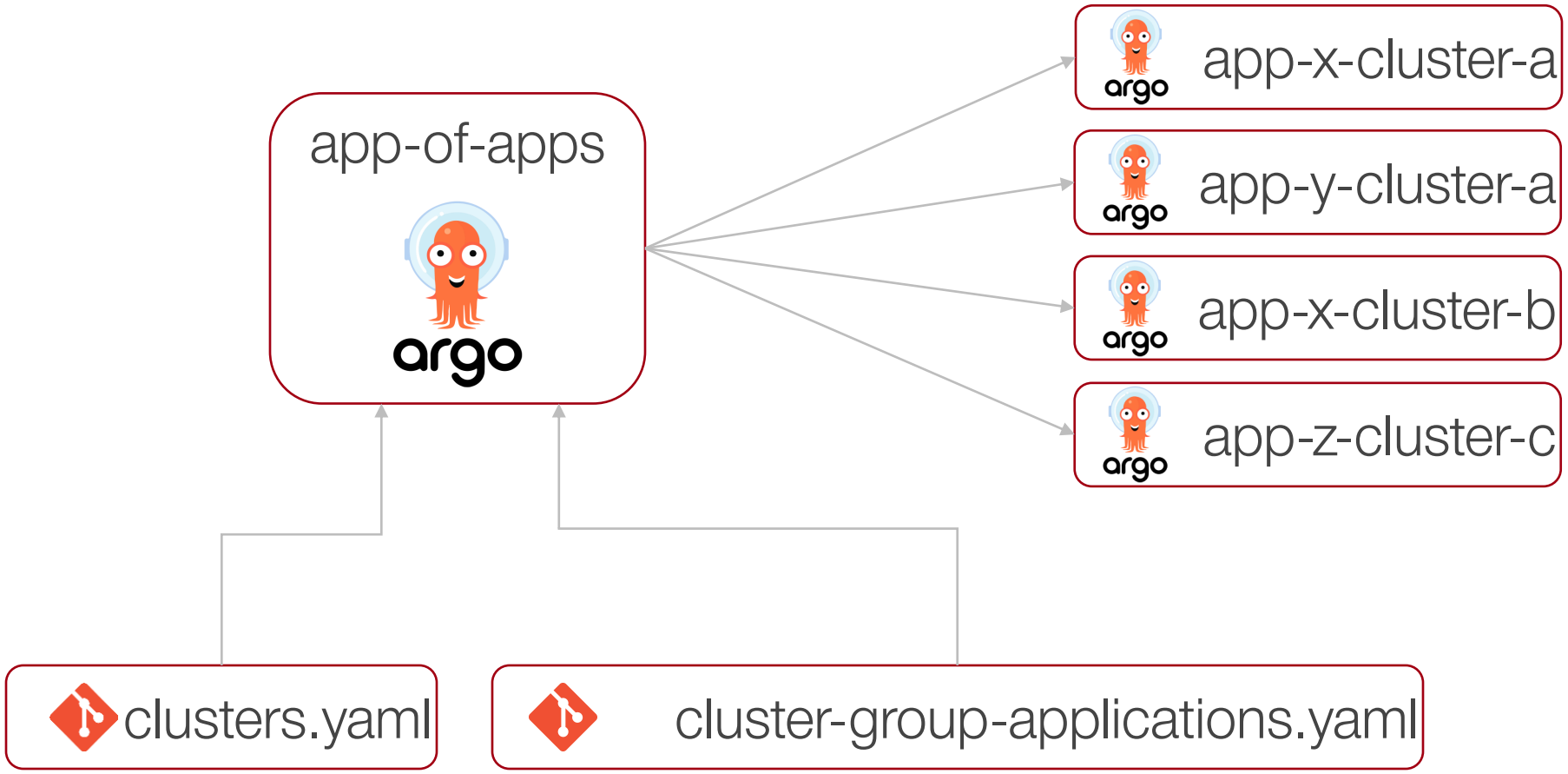
values/groups/**cloud/aws**/app-y.yaml

App-Of-Apps Pattern

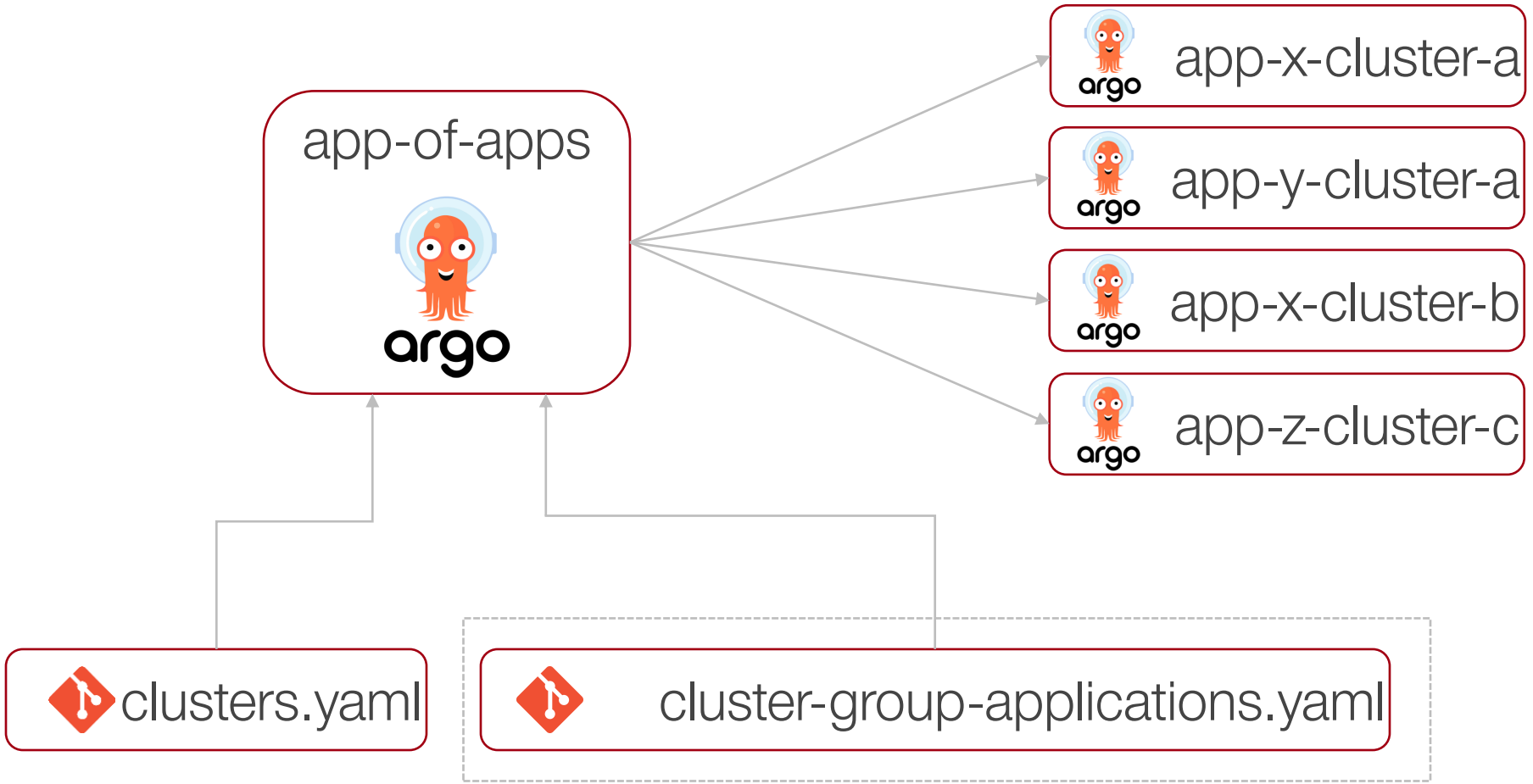
App-Of-Apps Pattern



App-Of-Apps Pattern



App-Of-Apps Pattern



cluster-group-applications.yaml

```yaml
cloud/azure:
  applications:
    - name: "app-u"
      namespace: "app-u"
    - name: "app-v"
      namespace: "app-v"
  excludes: []
```

cloud/azure

cluster-group-applications.yaml

```
cloud/azure:
  applications:
    - name: "app-u"
      namespace: "app-u"
    - name: "app-v"
      namespace: "app-v"
  excludes: []
```

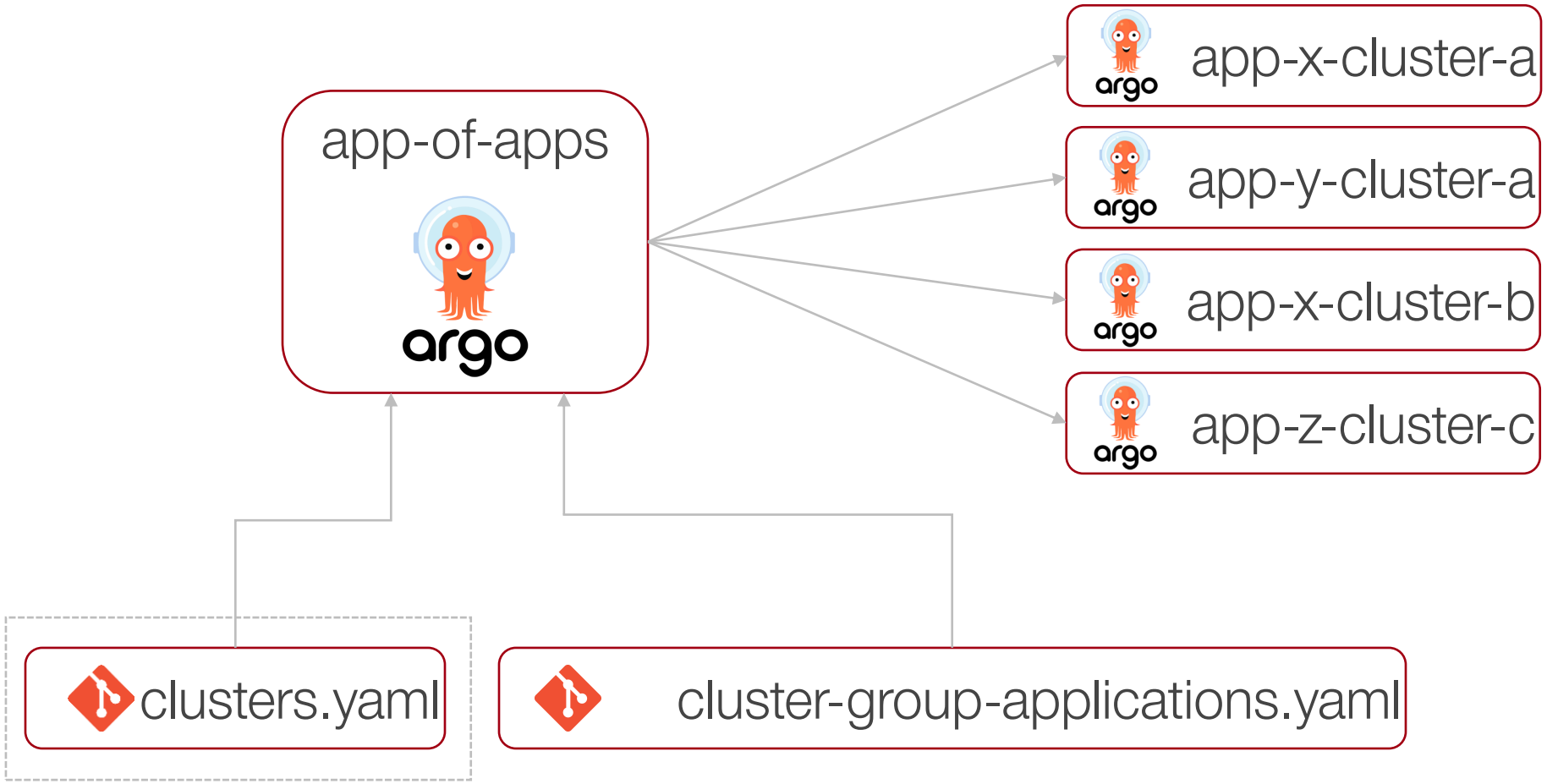
cloud/azure

cluster-group-applications.yaml

```
cloud/azure:
  applications:
    - name: "app-u"
      namespace: "app-u"
    - name: "app-v"
      namespace: "app-v"
  excludes: []
```

cloud/azure

App-Of-Apps Pattern



clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - cloud/azure
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications: []
```

stage/prod

cloud/azure

clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - cloud/azure
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications: []
```

stage/prod

cloud/azure

clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - cloud/azure
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications: []
```

stage/prod

cloud/azure

clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - cloud/azure
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications: []
```

stage/prod

cloud/azure

clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - cloud/azure
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications: []
```

stage/prod

cloud/azure

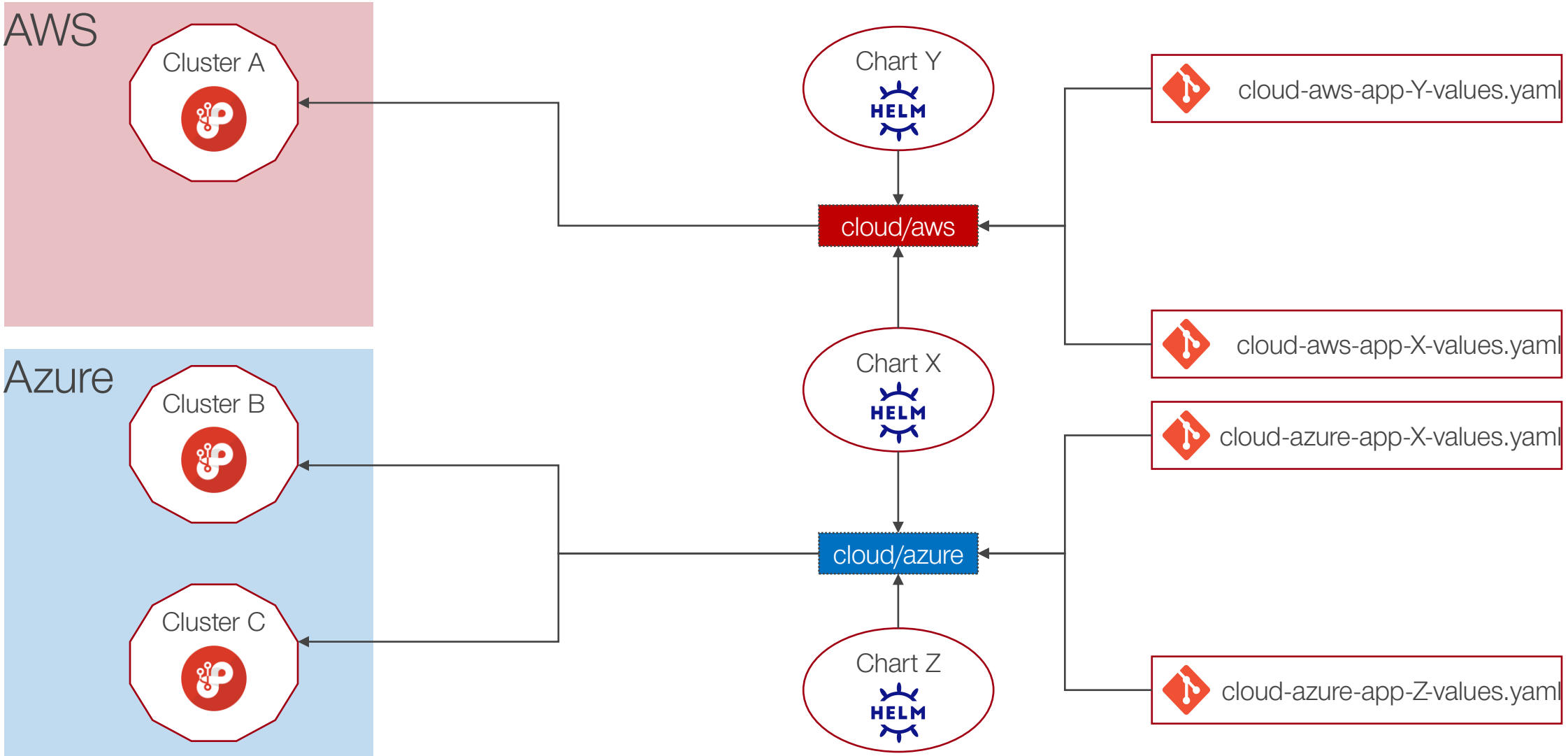
clusters.yaml

```yaml
name: cluster-c
api: ...
groups:
  - stage/prod
  - stage/prod/update-group-b
  - cloud/azure
  - cloud/aws/ocp-prod-account
  - platform/ocp4
  - cluster/shared
  - cluster/batch-nodes
  - cluster/network-ingress-azure
  - applications/argo-workflows
  - applications/instana
  - applications/3scale
  - applications/kafka-operator
applications:
  - name: app-x
    namespace: app-x
  - name: app-y
    namespace: app-y
excludeApplications:
  - someapp
```

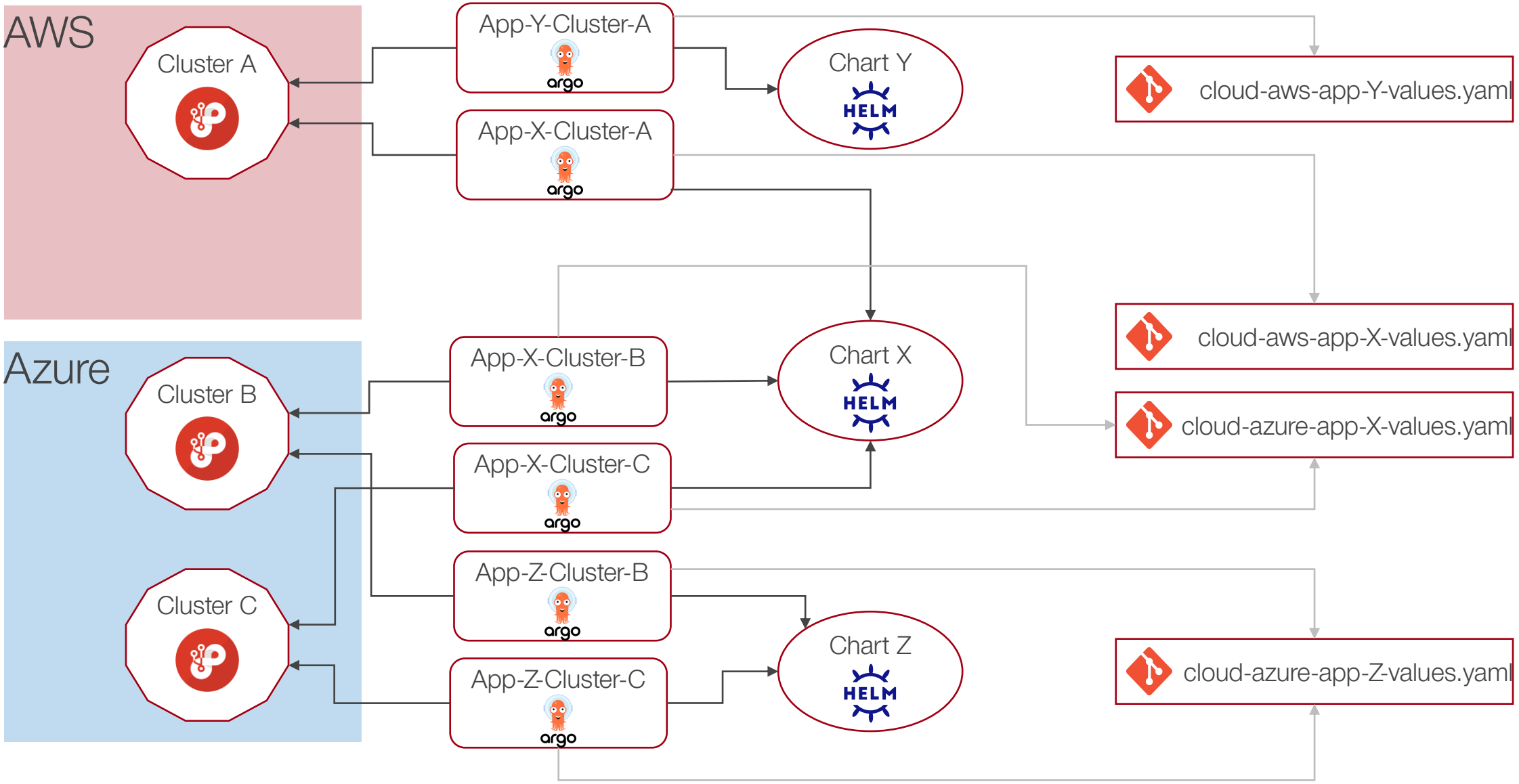
stage/prod

cloud/azure

Groups


AWS
Cluster A
Azure
Cluster B
Cluster C
Chart Y
HELM
Chart X
HELM
Chart Z
HELM
cloud/aws
cloud/azure
cloud-aws-app-Y-values.yaml
cloud-aws-app-X-values.yaml
cloud-azure-app-X-values.yaml
cloud-azure-app-Z-values.yaml

Introducing: Groups



There is more …

- Cluster Admin delegation with ArgoCD Projects
- Common values
- Secrets-handling with mozilla/sops
- “Shared” app charts
- Cluster inventory
- ArgoCD application labels

There is mo

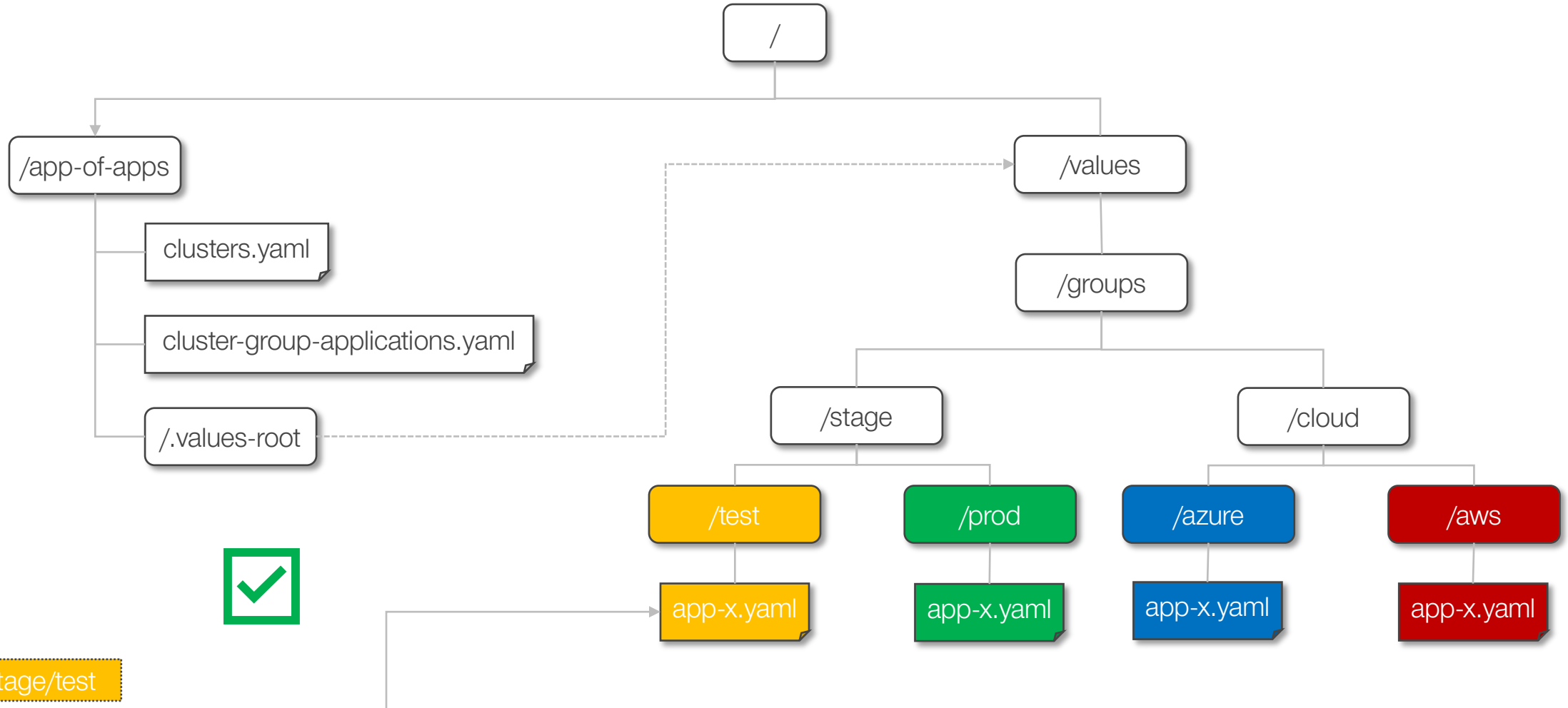
- Cluster Ad
- mon
- h
- Shared”
- Cluster inv
- ArgoCD a

GitHub

https://github.com/SchweizerischeBundesbahnen/container-platform-base

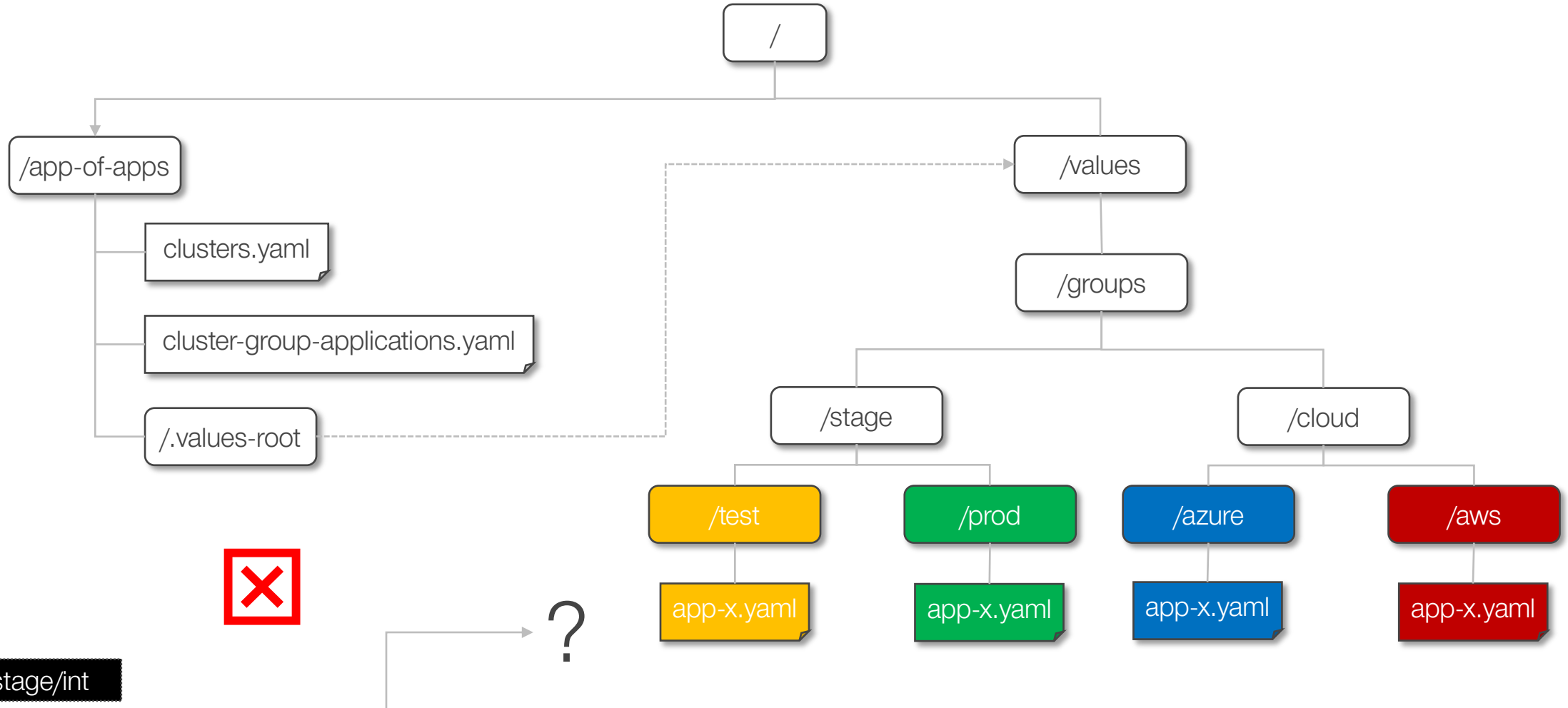

SBB CFF FFS
Thanks,
danke,
merci
& grazie.

Automatic values yaml detection




```
.Files.Get ".values-root/groups/stage/test/app-x.yaml"
```

Automatic values yaml detection




```
.Files.Get ".values-root/groups/stage/int/app-x.yaml"
```

Automatic values yaml detection