



Evolving GitOps: Harnessing Kubernetes Resource Model for 5G Core

Ashan Senevirathne & Joel Studler



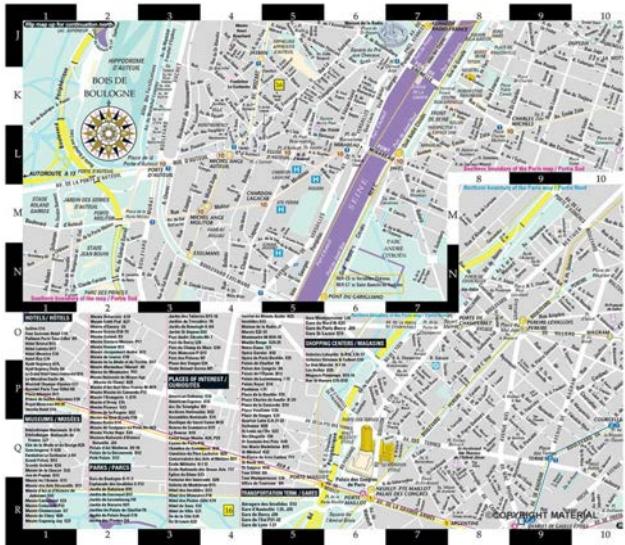


An Analogy...

Static paper map

- Fixed
- Static
- Unchanging
- Overwhelming

This is GitOps today



Apple maps

- Dynamic
- Changes on external conditions
- More focused
- Simple to navigate

This is GitOps w/ KRM





Ashan Senevirathne

Product Owner

Slack: CNCF/Kubernetes/Nephio

ashan.senevirathne@swisscom.com

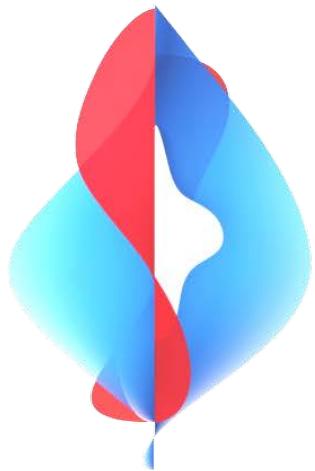


Joel Studler

Senior DevOps Engineer

Slack: CNCF/Kubernetes/Nephio

joel.studler@swisscom.com



swisscom



Brief History of Automation in Mobile Network Cores

2G	3G	4G	5G
○	○	○	●
Custom Hardware	Custom Hardware	x86 VMs	Containers+ Kubernetes
Spreadsheets	Spreadsheets + Scripts	+ Ansible	IaC + GitOps
«PNF» – physical network function	«VNF» – virtual network function	«CNF» – cloud native network function	



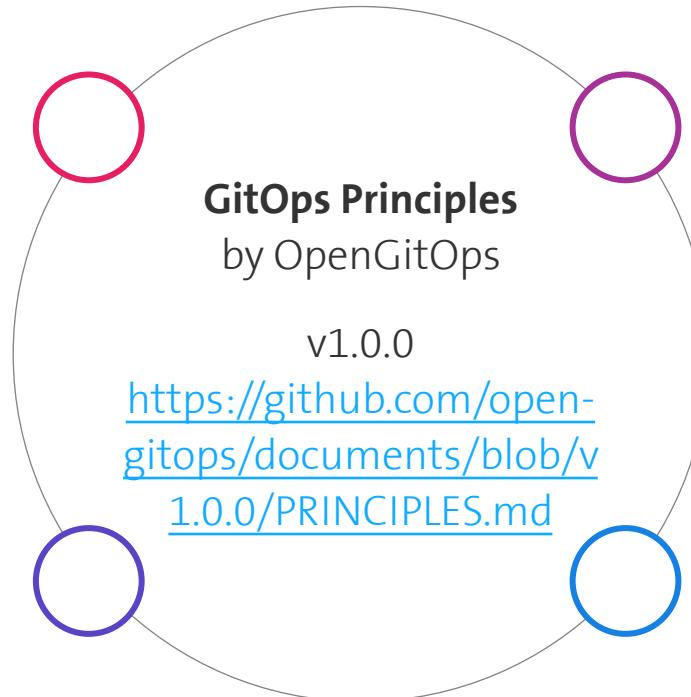
What is GitOps?

Declarative

**Continuously
Reconciled**

**Versioned and
Immutable**

Pulled Automatically





Examples of GitOps in Practice

Example

Infrastructure as Code (IaC) using Terraform, applied manually

Triggering Ansible playbooks or scripts from Jenkins pipeline

GitLab CI pipeline acting commits

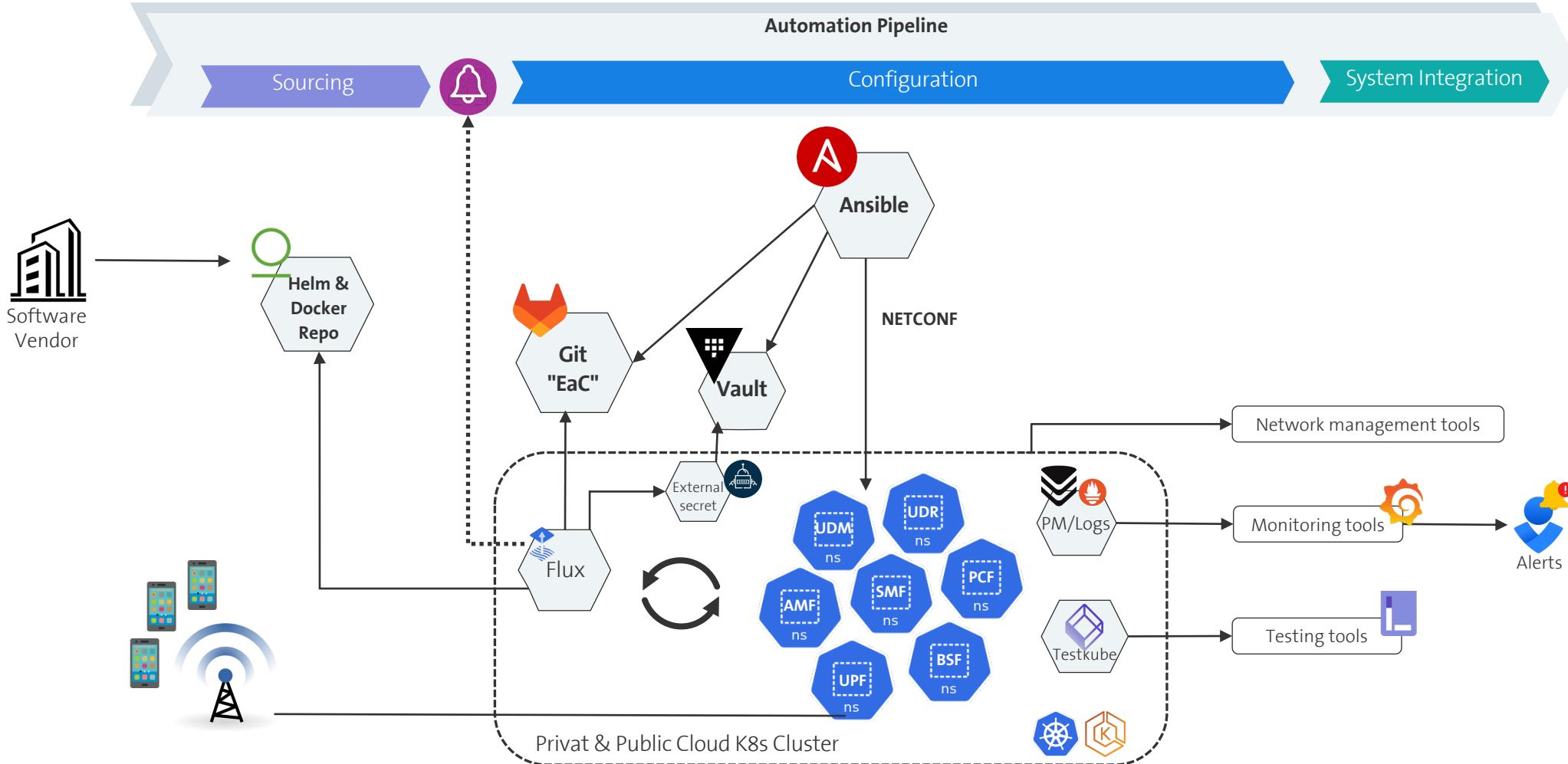
Flux or ArgoCD deployments

Declarative Versioned and Immutable Pulled Automatically Continuously Reconciled

✓	✓	✗	✗
✓	(✓)	✗	✗
✓	✓	✓	✗
✓	✓	✓	✓

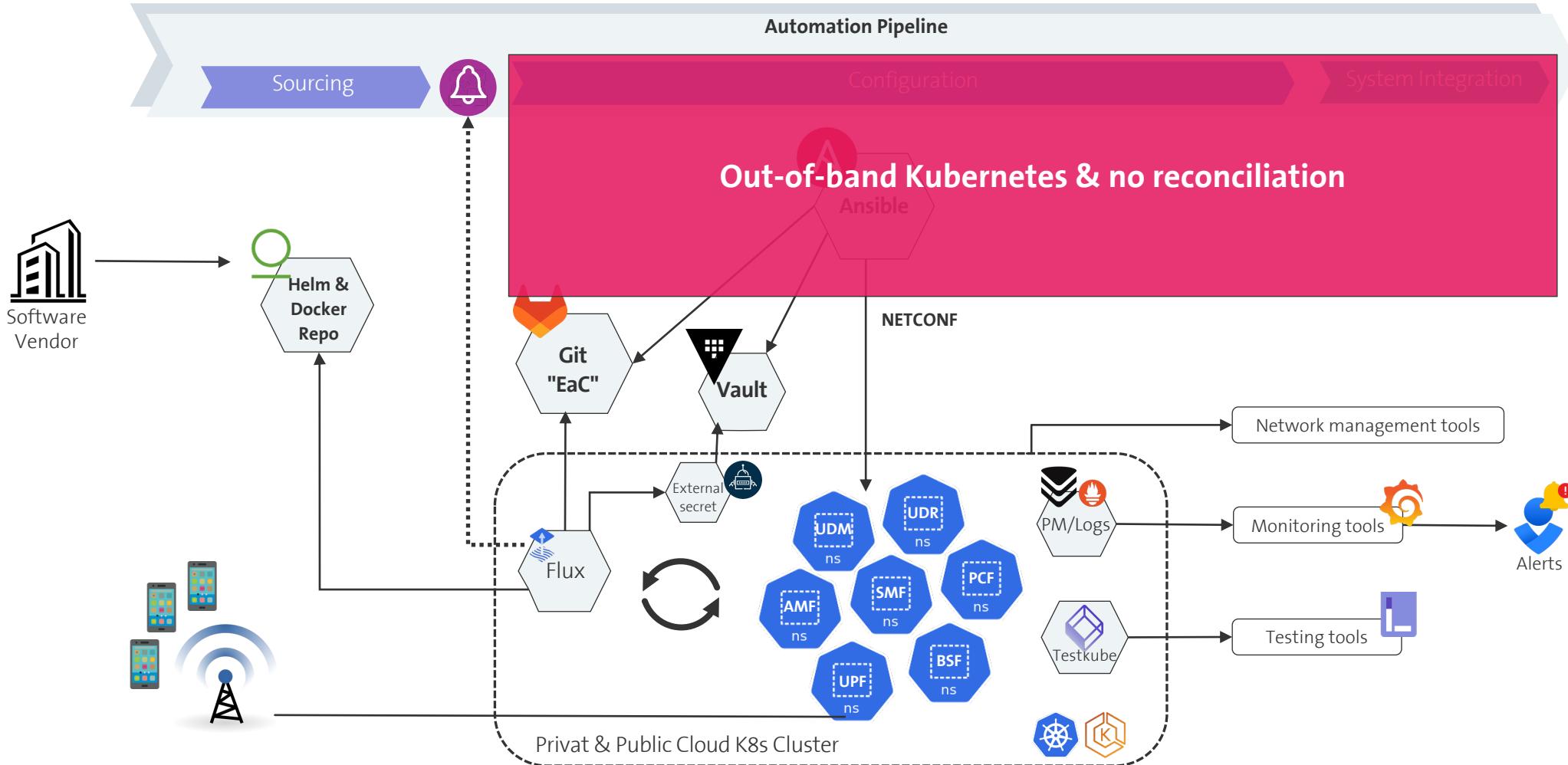


Current State of Automation



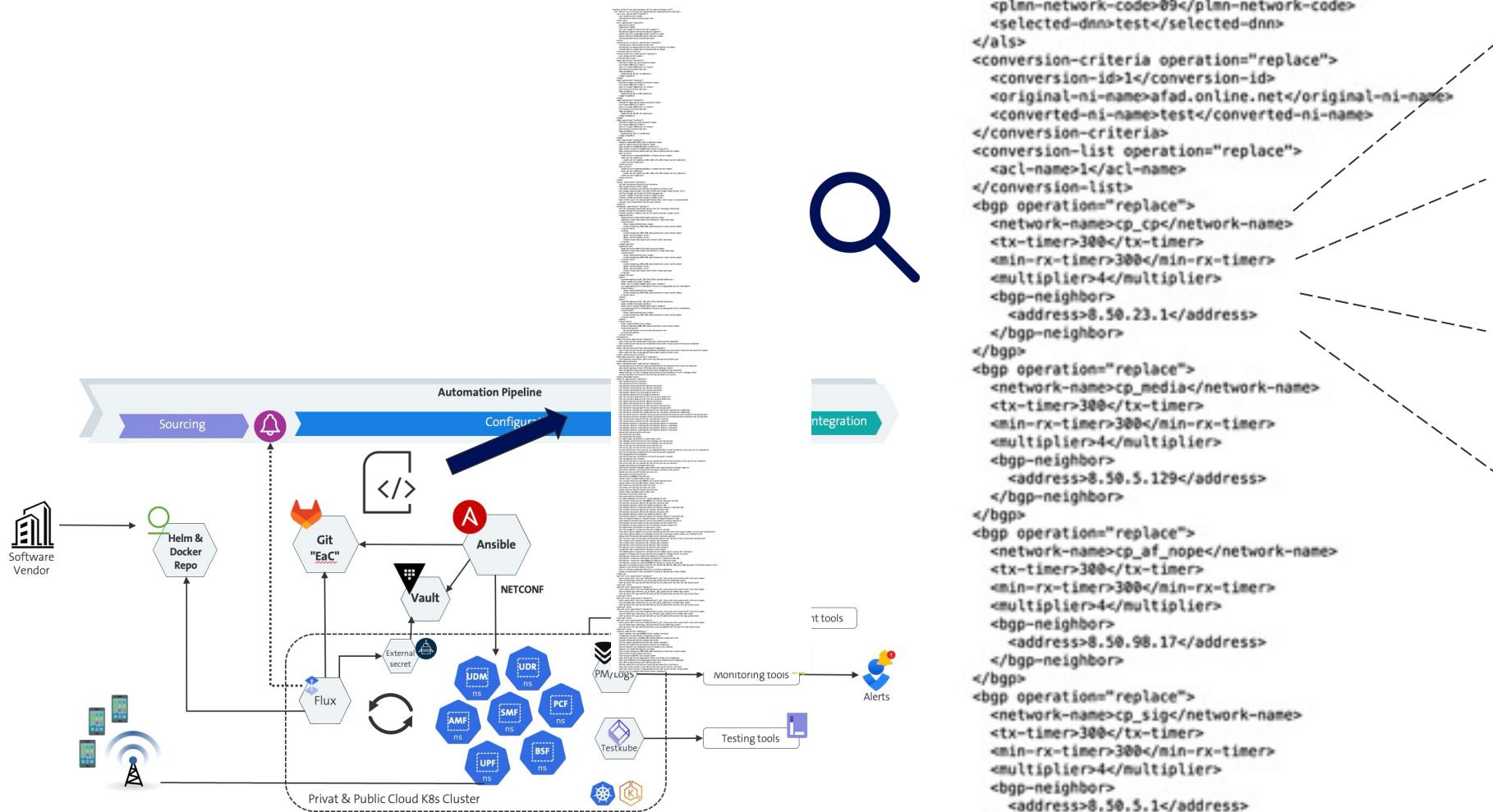


Current State of Automation





Current State of Automation



```
config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<af xmlns="urn:fiction:com:opennetworks:opennetworks-config">
  <acl-acc operation="replace">
    <acl-name>1</acl-name>
    <conversion-id>1</conversion-id>
  </acl-acc>
  <als operation="replace">
    <pei>test</pei>
    <add>test</add>
    <nf-set-support>test</nf-set-support>
    <binding-support>test</binding-support>
    <plmn-country-code>999</plmn-country-code>
    <plmn-network-code>09</plmn-network-code>
    <selected-dnn>test</selected-dnn>
  </als>
  <conversion-criteria operation="replace">
    <conversion-id>1</conversion-id>
    <original-ni-name>afad.online.net</original-ni-name>
    <converted-ni-name>test</converted-ni-name>
  </conversion-criteria>
  <conversion-list operation="replace">
    <acl-name>1</acl-name>
  </conversion-list>
  <bgp operation="replace">
    <network-name>cp_cp</network-name>
    <tx-timer>300</tx-timer>
    <min-rx-timer>300</min-rx-timer>
    <multiplier>4</multiplier>
    <bgp-neighbor>
      <address>8.50.23.1</address>
    </bgp-neighbor>
  </bgp>
  <bgp operation="replace">
    <network-name>cp_media</network-name>
    <tx-timer>300</tx-timer>
    <min-rx-timer>300</min-rx-timer>
    <multiplier>4</multiplier>
    <bgp-neighbor>
      <address>8.50.5.129</address>
    </bgp-neighbor>
  </bgp>
  <bgp operation="replace">
    <network-name>cp_af_nope</network-name>
    <tx-timer>300</tx-timer>
    <min-rx-timer>300</min-rx-timer>
    <multiplier>4</multiplier>
    <bgp-neighbor>
      <address>8.50.98.17</address>
    </bgp-neighbor>
  </bgp>
  <bgp operation="replace">
    <network-name>cp_sig</network-name>
    <tx-timer>300</tx-timer>
    <min-rx-timer>300</min-rx-timer>
    <multiplier>4</multiplier>
    <bgp-neighbor>
      <address>8.50.5.1</address>
    </bgp-neighbor>
  </bgp>
  <dns operation="replace">
    <domain-name>009.999.afad.</domain-name>
    <query-type>recursive</query-type>
    <max-cache-ttl>604230</max-cache-ttl>
    <max-local-cache-ttl>300</max-local-cache-ttl>
    <no-forwarding>true</no-forwarding>
  </dns>
</af>
```

- IP addresses
 - Subnets
 - VLANs
 - DNS Records
 - Network function variables
 - Infrastructure variables
 - Network function-Network function mapping
 - Secret references
 - Certificate references



Current State of Automation



- IP addresses
- Subnets
- VLANs
- DNS Records
- Network function variables
- Infrastructure variables
- Network function-Network function mapping
- Secret references
- Certificate references



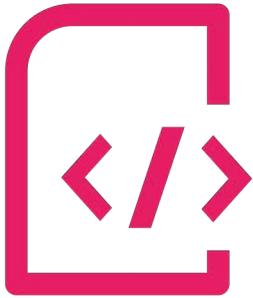
Key Issues With GitOps in Practice



Often no Reconciliation



Often out-of-band
with Kubernetes



Often no abstraction
and simplification layer



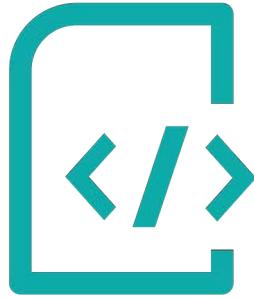
What We Like About GitOps in Practice



Source of Truth



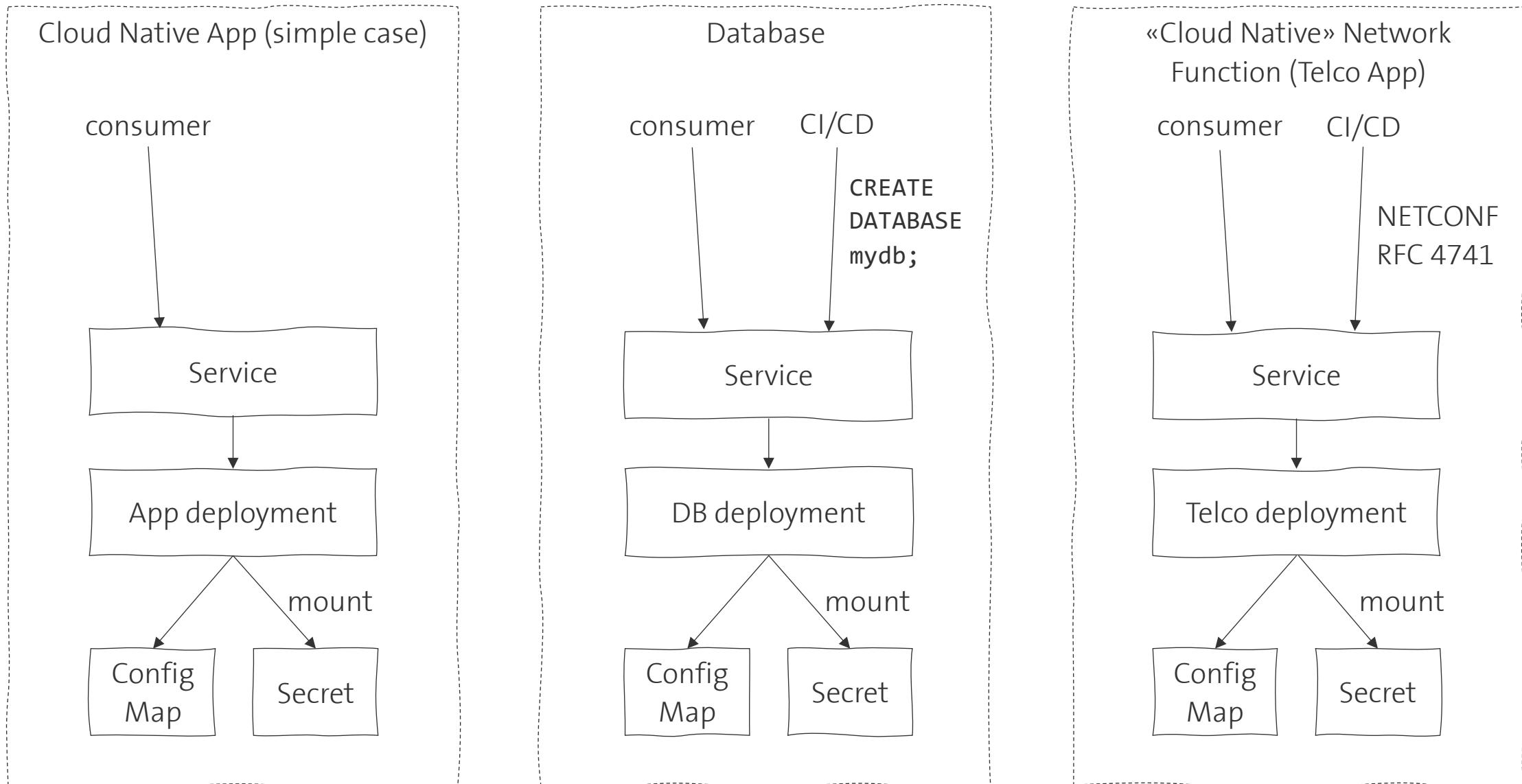
Review process



Declarative

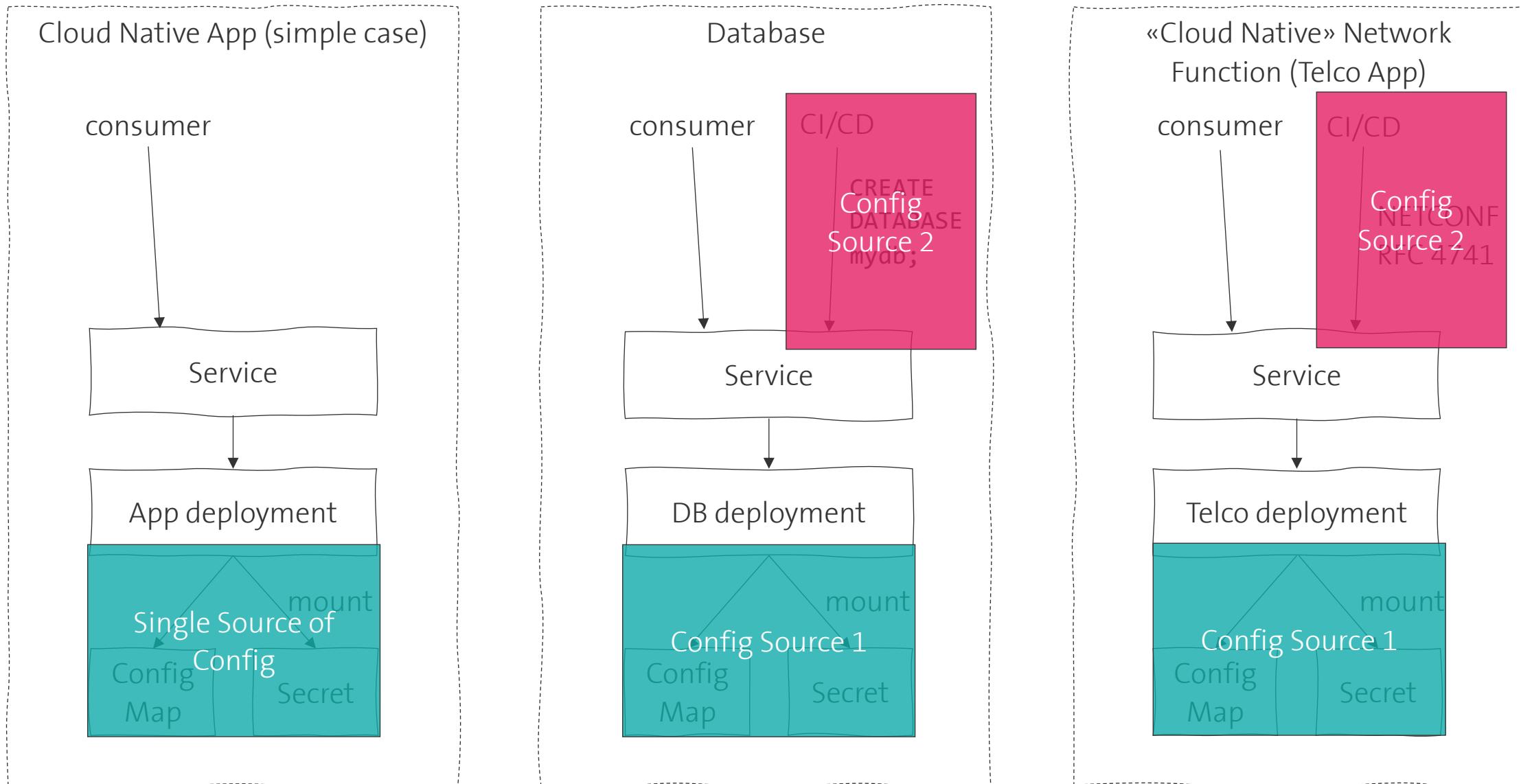


Configuration of Cloud Native Apps





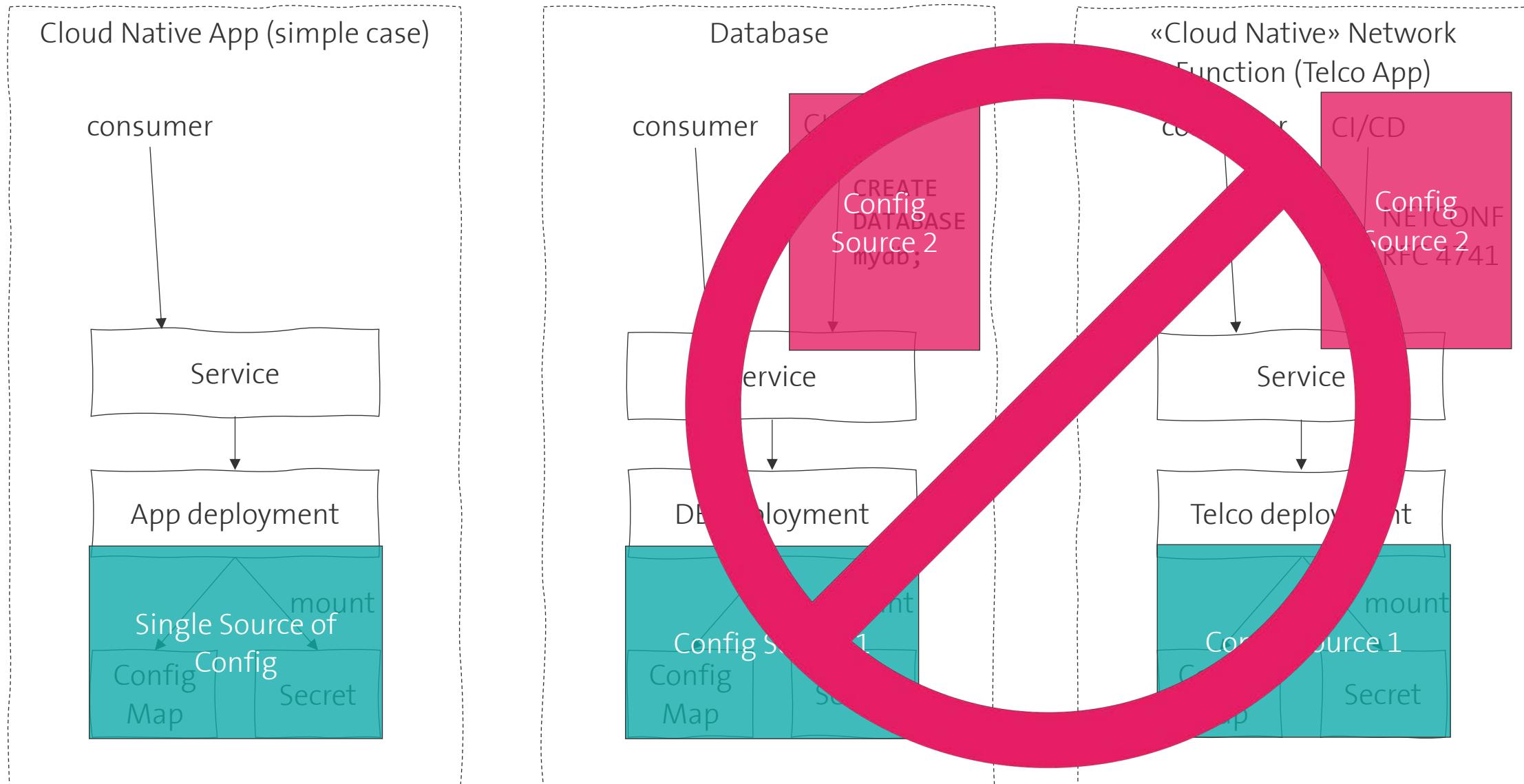
Configuration of Cloud Native Apps





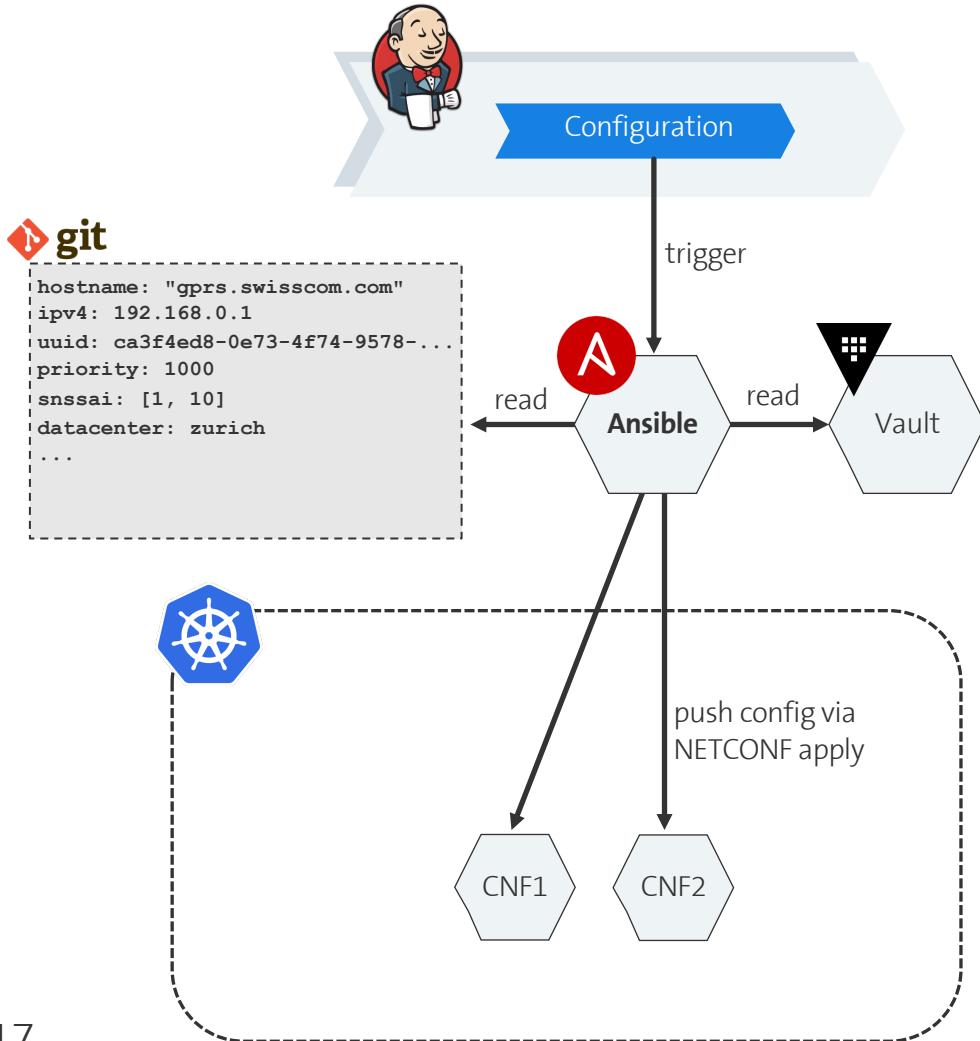
Configuration of Cloud Native Apps

Not Cloud Native!



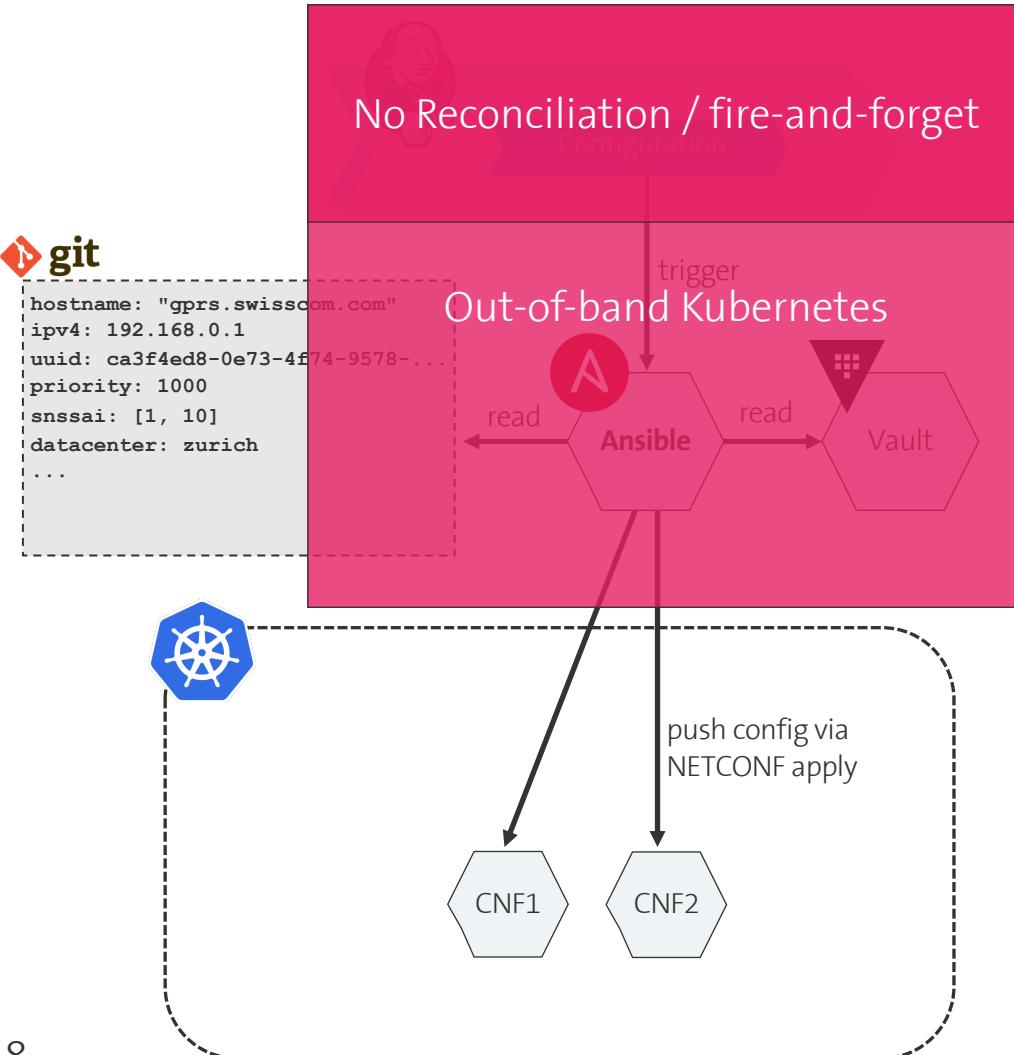


Introduce Reconciliation & K8s in-band



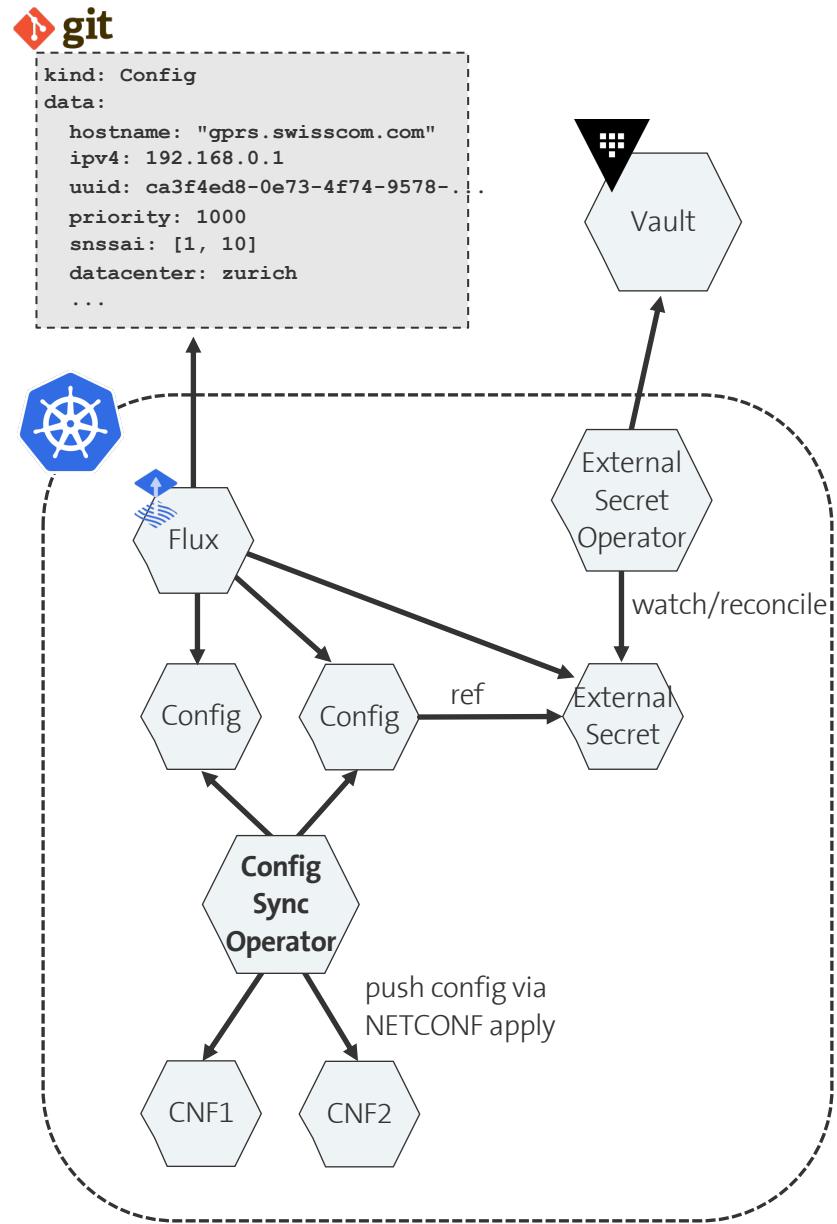
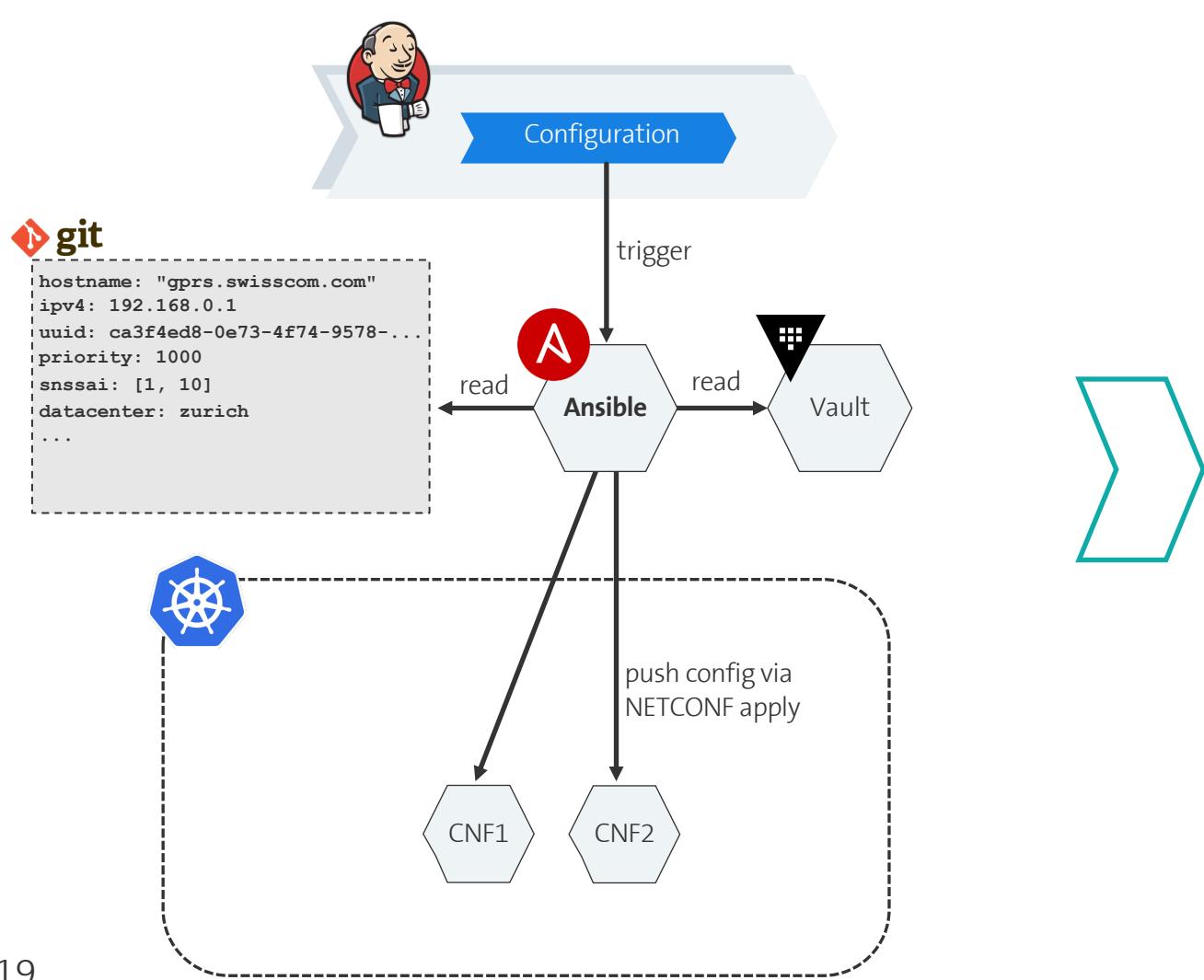


Introduce Reconciliation & K8s in-band



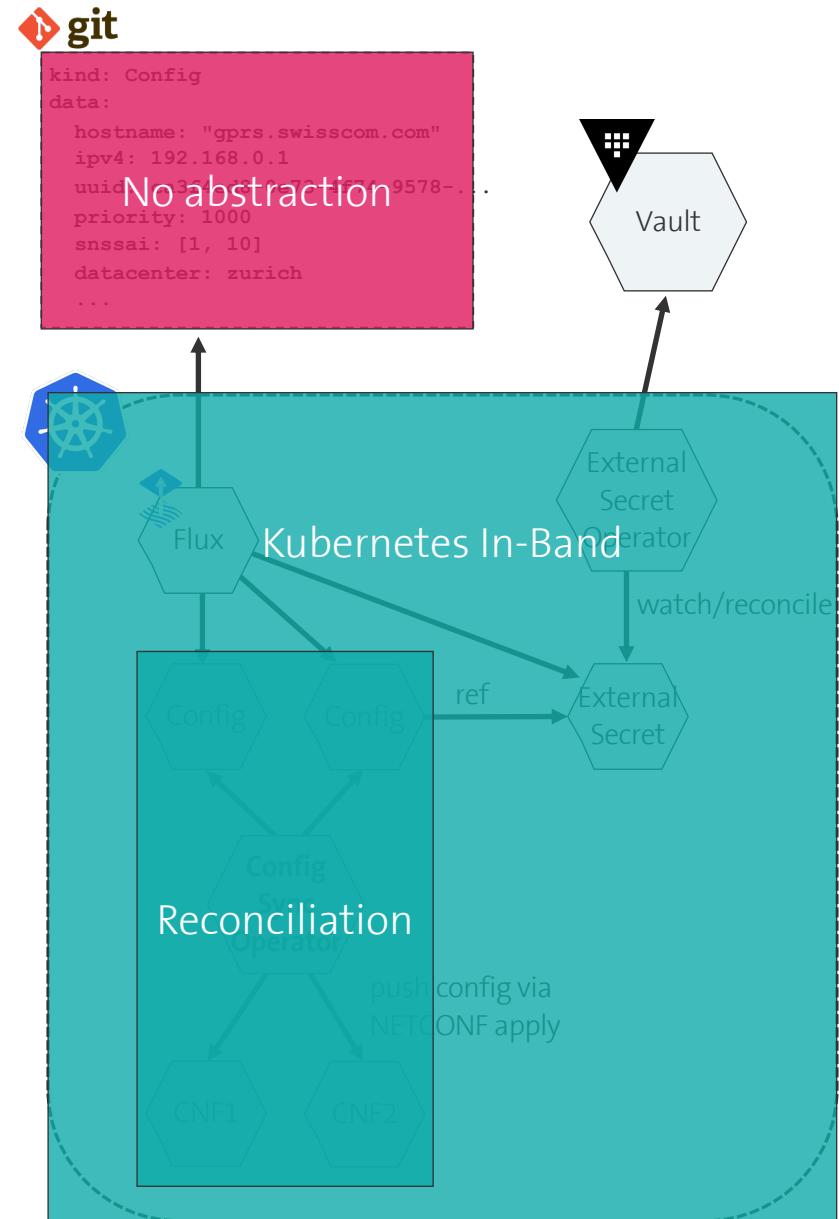
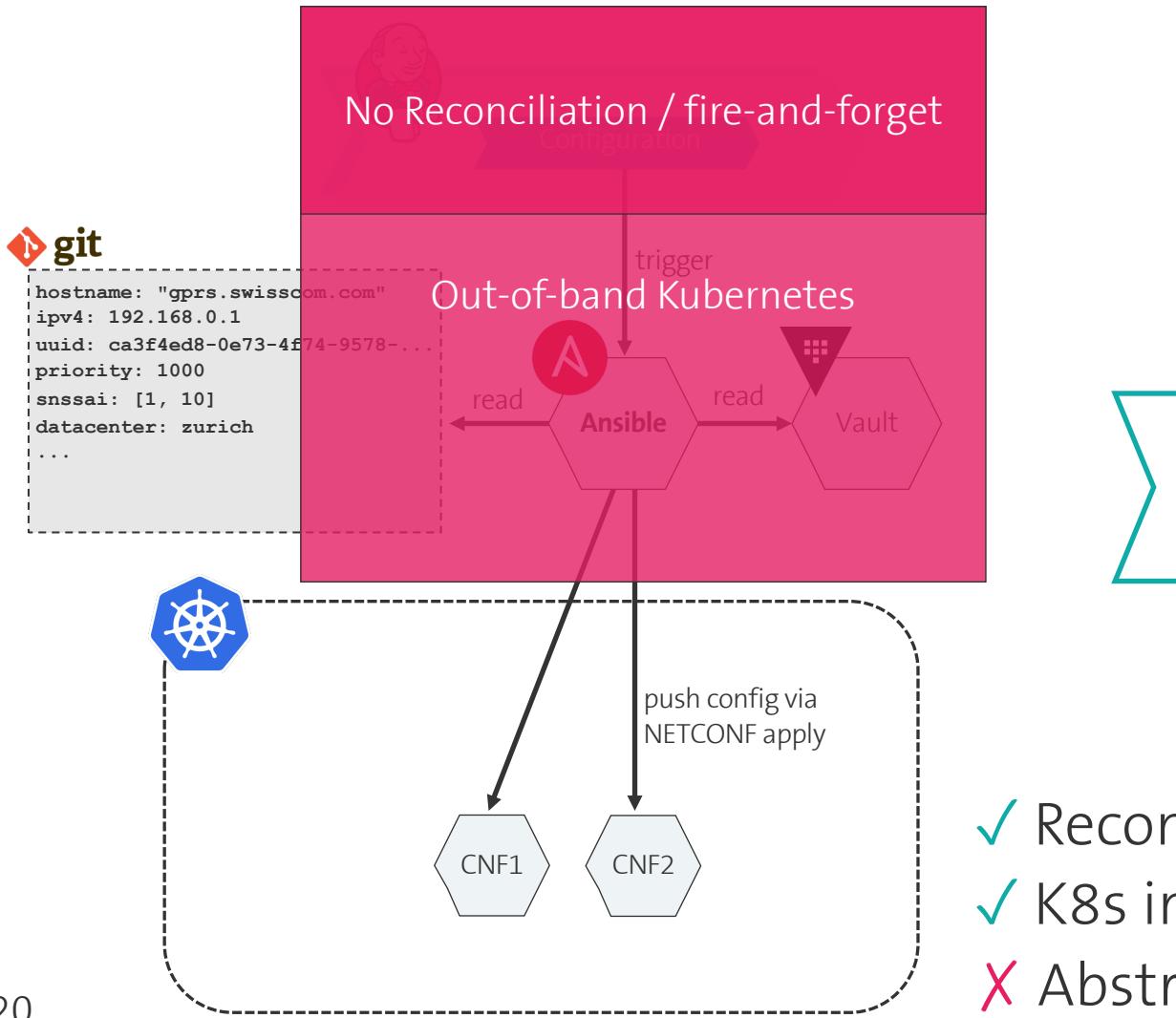


Introduce Reconciliation & K8s in-band





Introduce Reconciliation & K8s in-band





Config Sync Operator SDC

“Schema Driven Configuration” (SDC)

Protocols: gNMI, NETCONF (Telco Industry Standard)

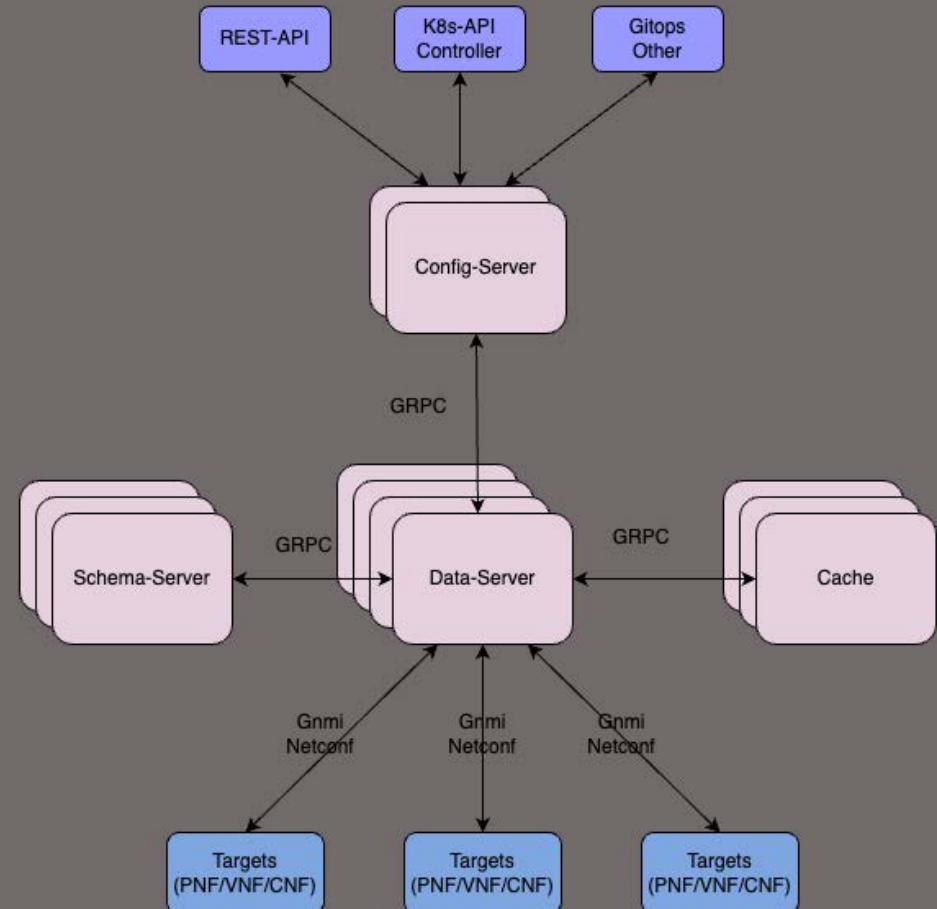
Supported Targets: Physical (PNF), Virtual Machines (VNF)
Cloud Native (CNF)

Vendor agnostic

Declarative (Kubernetes CRs, Operators, API extension)

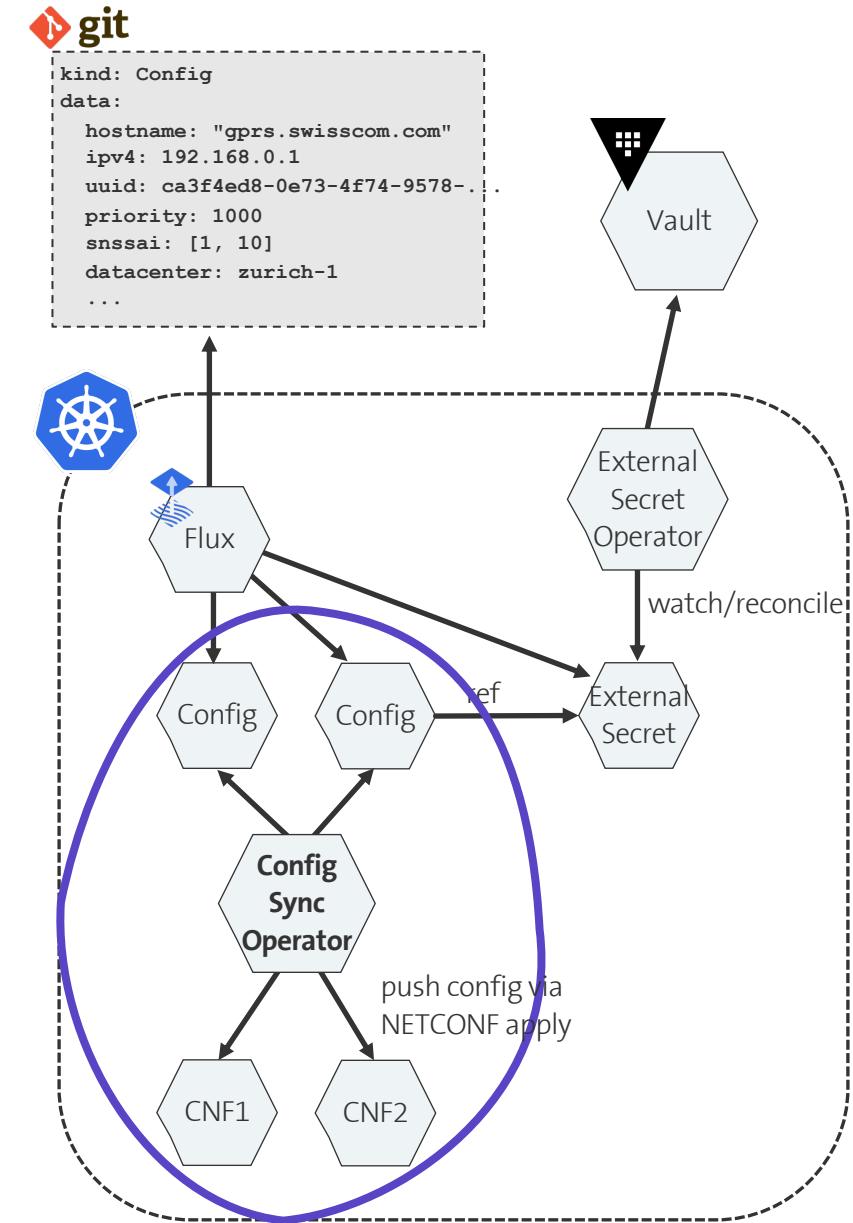
Roadmap: Schema validation using YANG (Telco Industry Standard)

Roadmap: Reconciliation and config drift fix



Demo SDC

Config Sync Operator





« The entire history of software engineering is that of the rise in levels of abstraction. »

Grady Booch



What is Kubernetes Resource Model (KRM)?



API extensions

Custom Resource Definitions
and API Services extend the
Kubernetes API



CRs as Instances

Custom Resources instantiate
a CRD / APIService

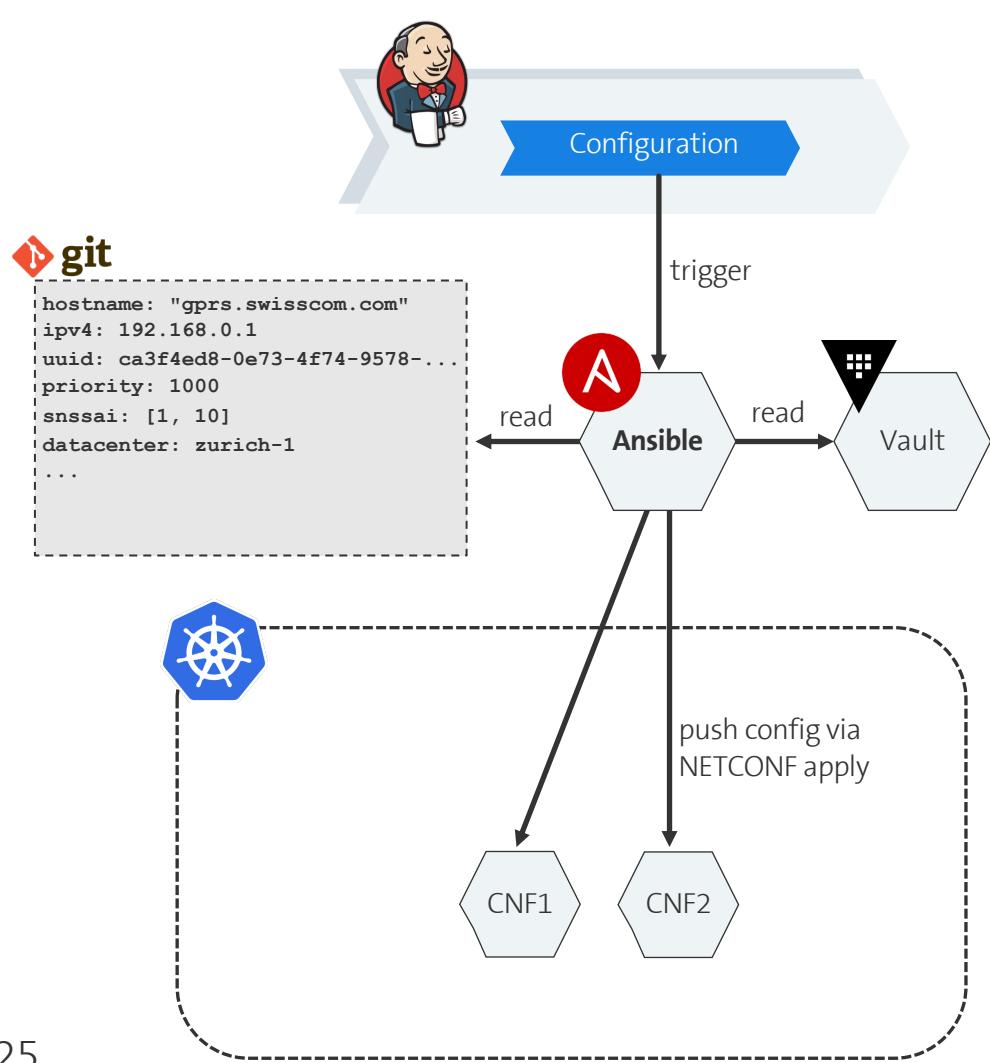


Business Logic

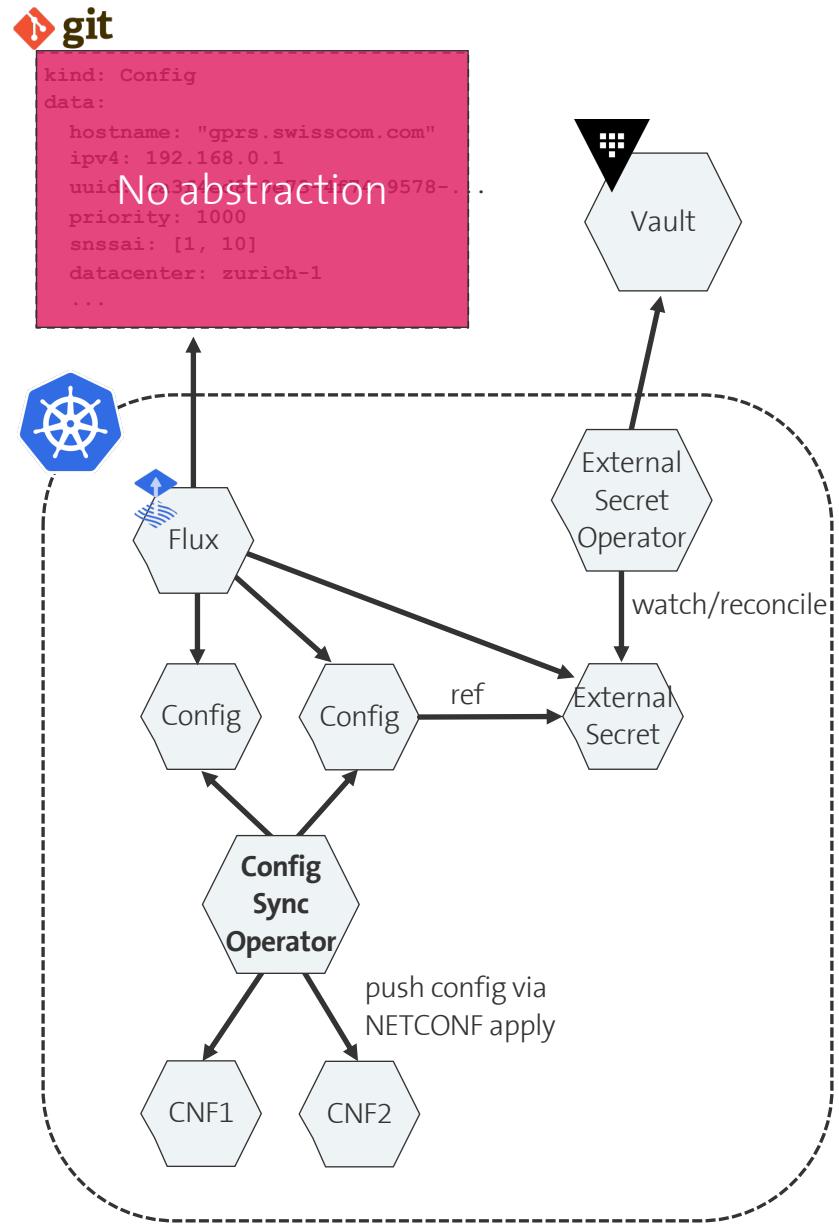
Operator custom code to
execute your business logic.
e.g. Lifecycle, Backup, Self-heal



Introduce Abstraction

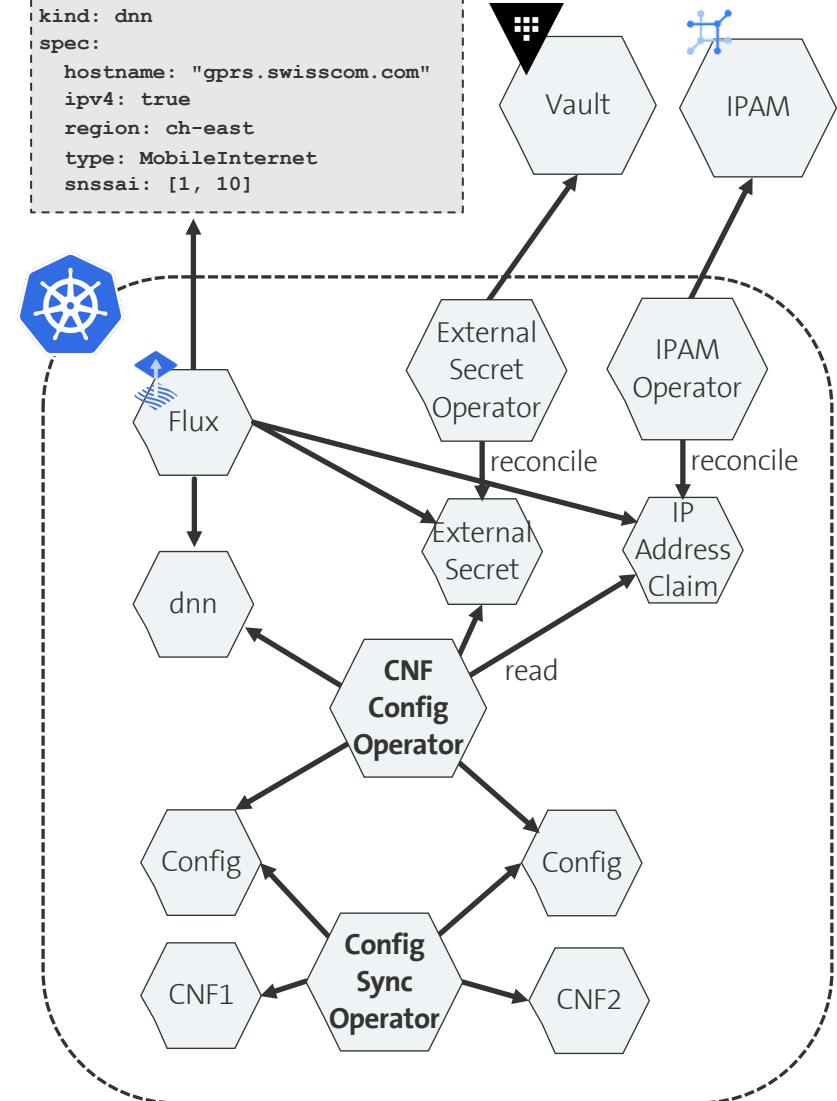
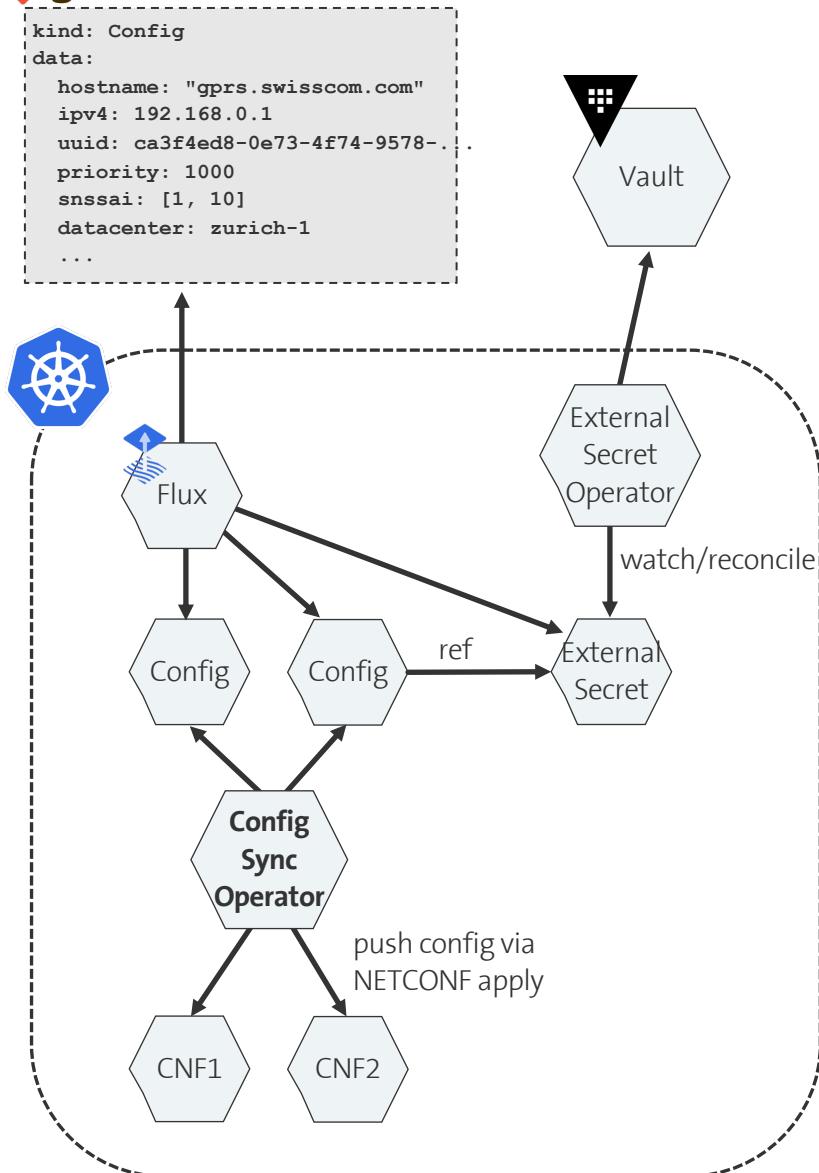


- ✓ Reconciliation
- ✓ K8s in-band
- ✗ Abstraction





Introduce Abstraction

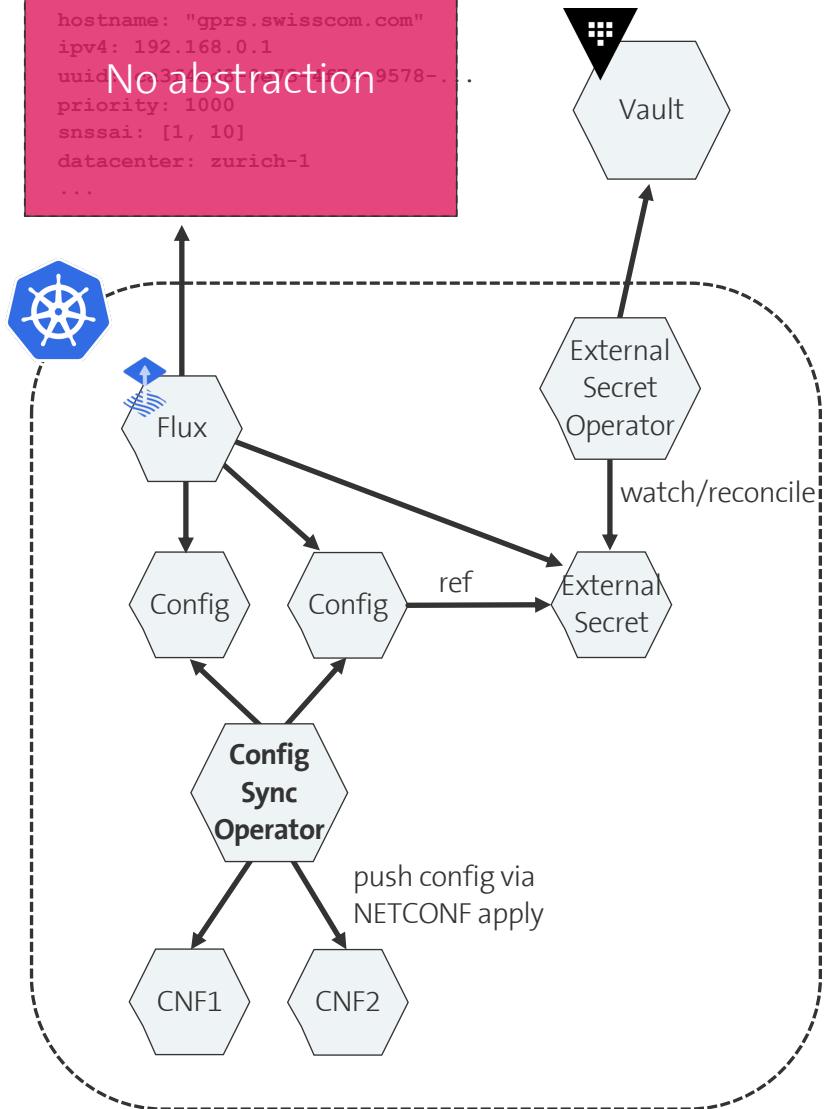




Introduce Abstraction



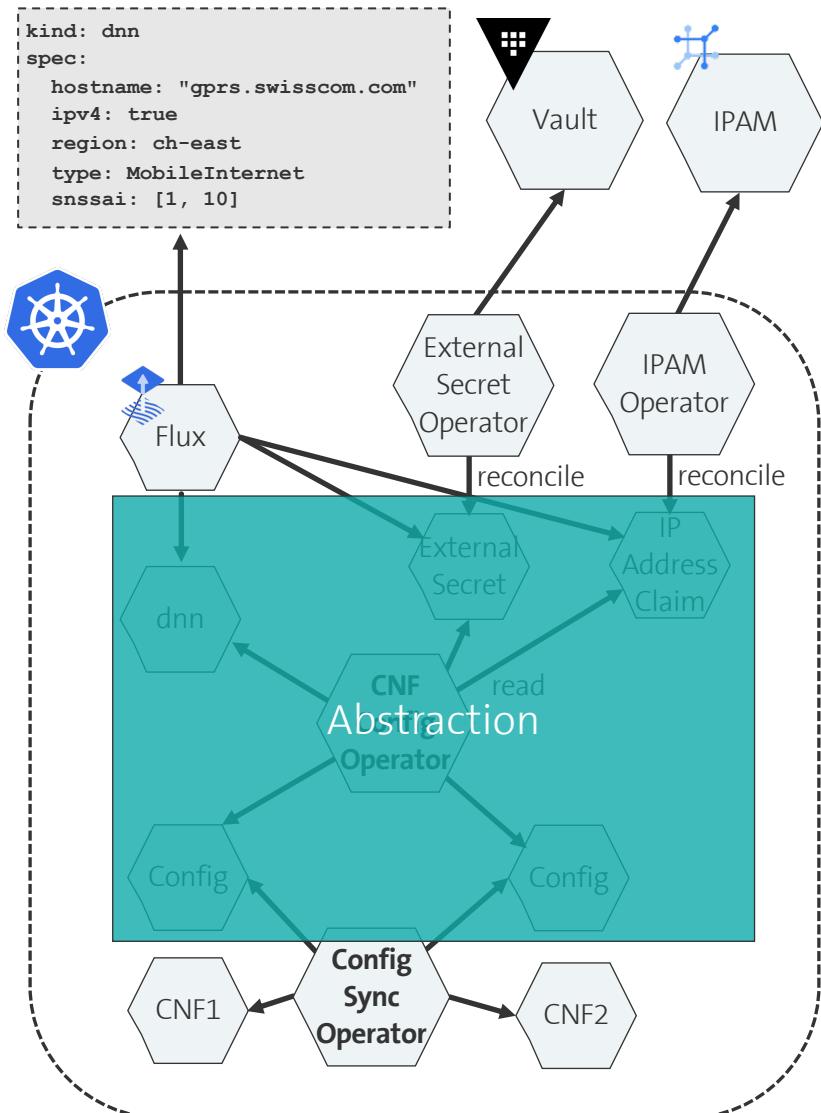
```
kind: Config  
data:  
  hostname: "gprs.swisscom.com"  
  ipv4: 192.168.0.1  
  ...  
No abstraction
```



- ✓ Reconciliation
- ✓ K8s in-band
- ✓ Abstraction

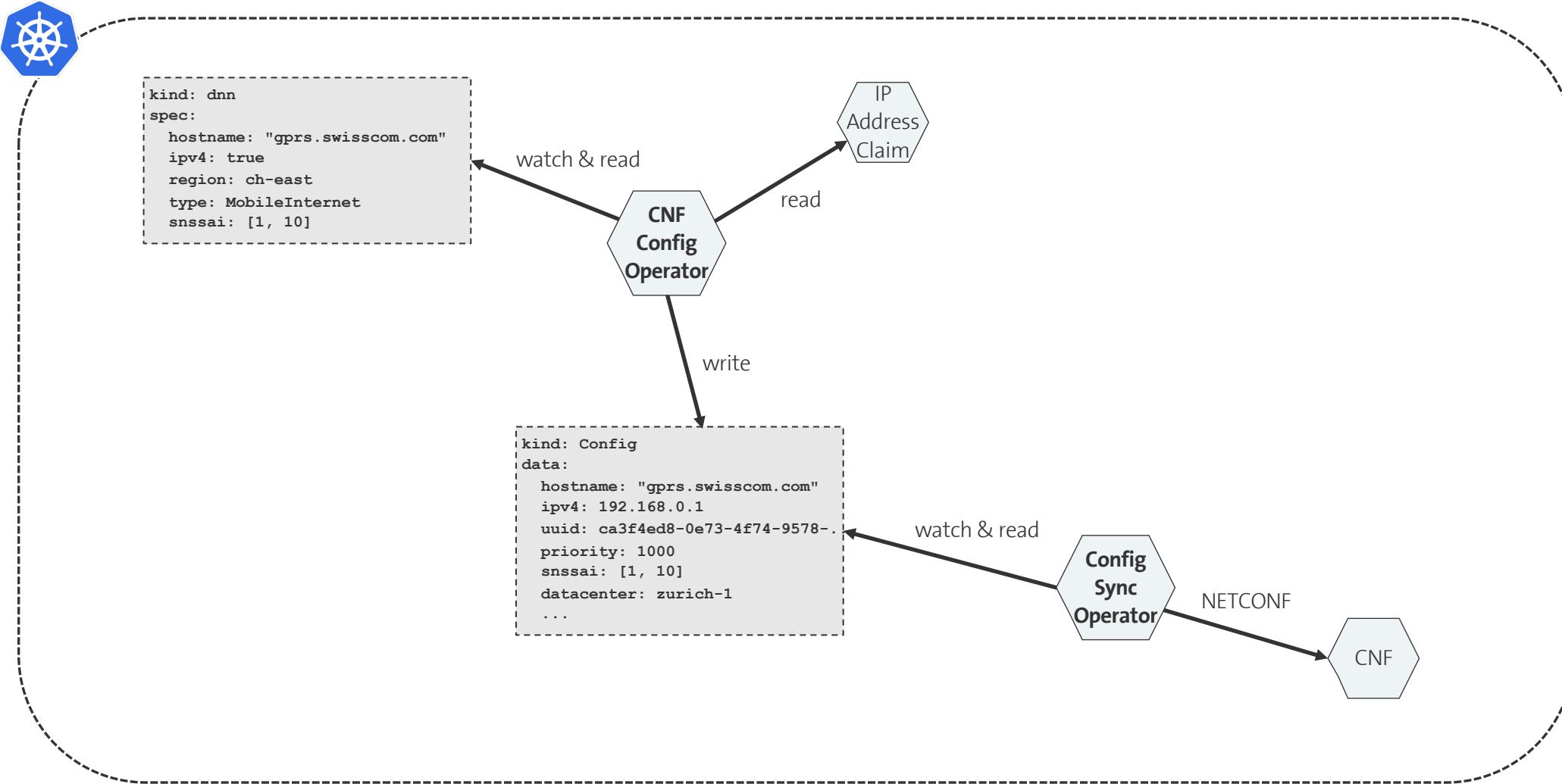


```
kind: dnn  
spec:  
  hostname: "gprs.swisscom.com"  
  ipv4: true  
  region: ch-east  
  type: MobileInternet  
  sssai: [1, 10]
```



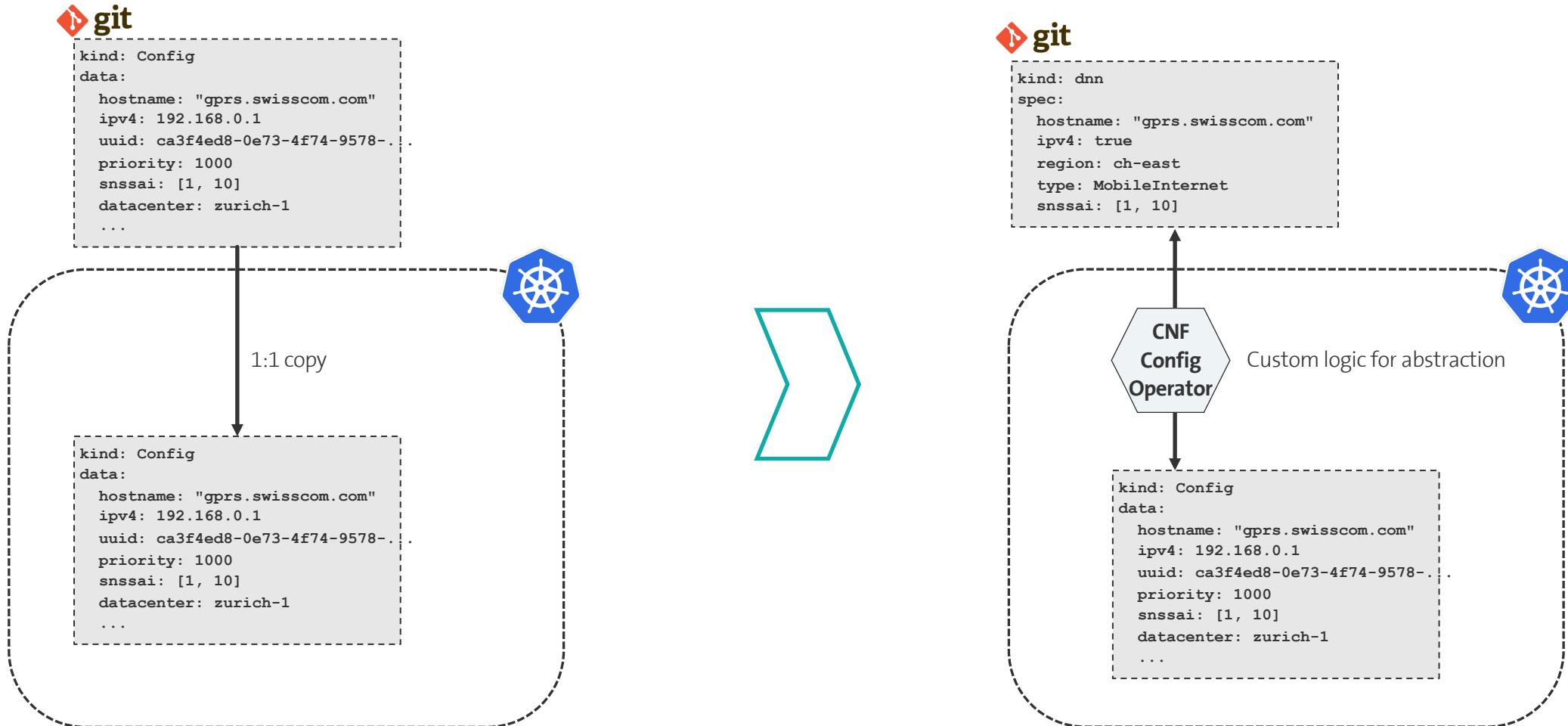


Introduce Abstraction



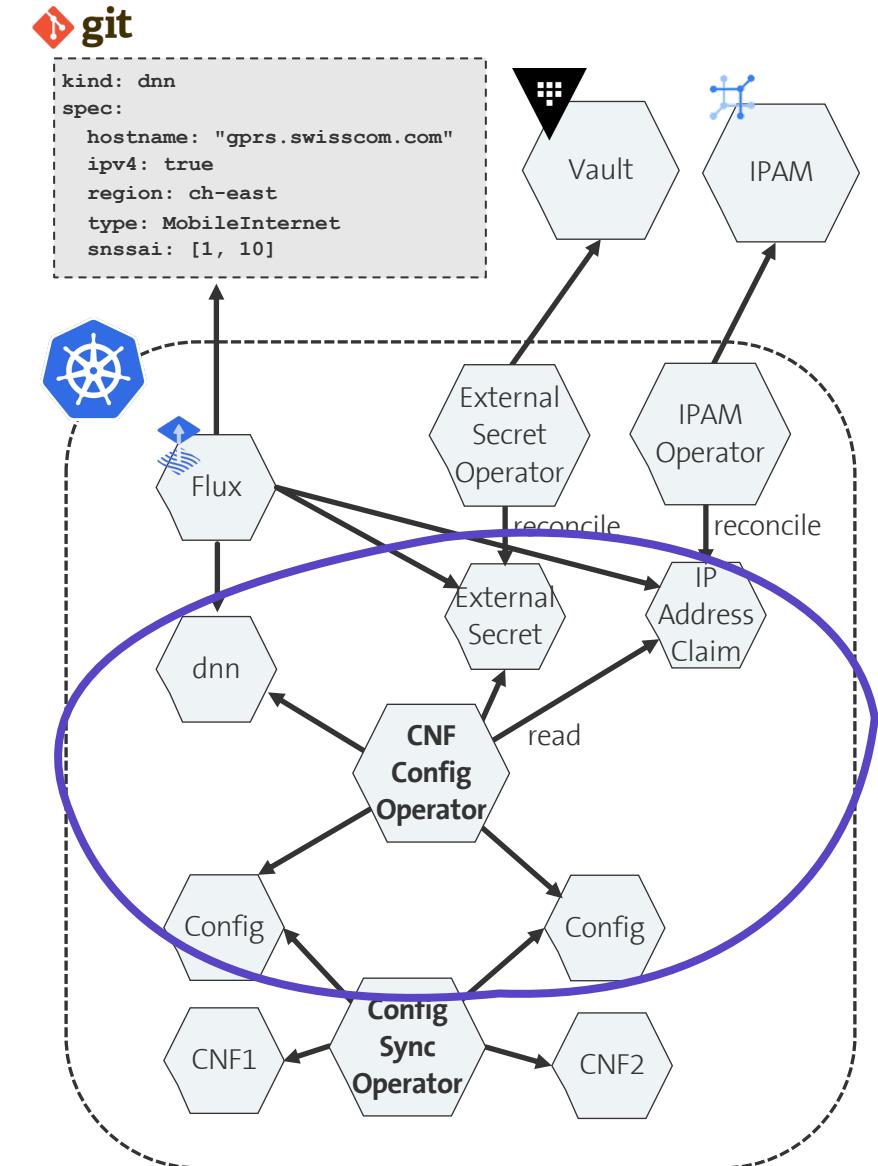


Introduce Abstraction



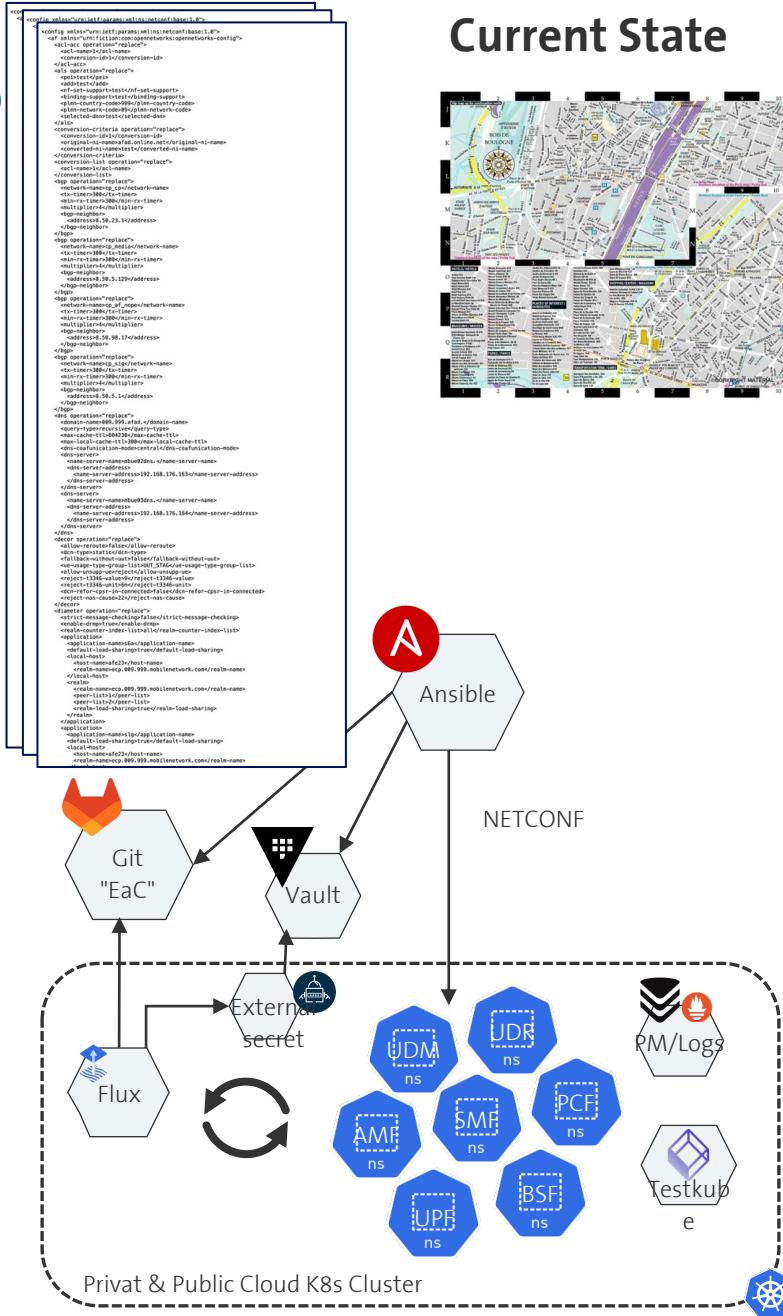
Demo Config Operator

Assembling the Configuration

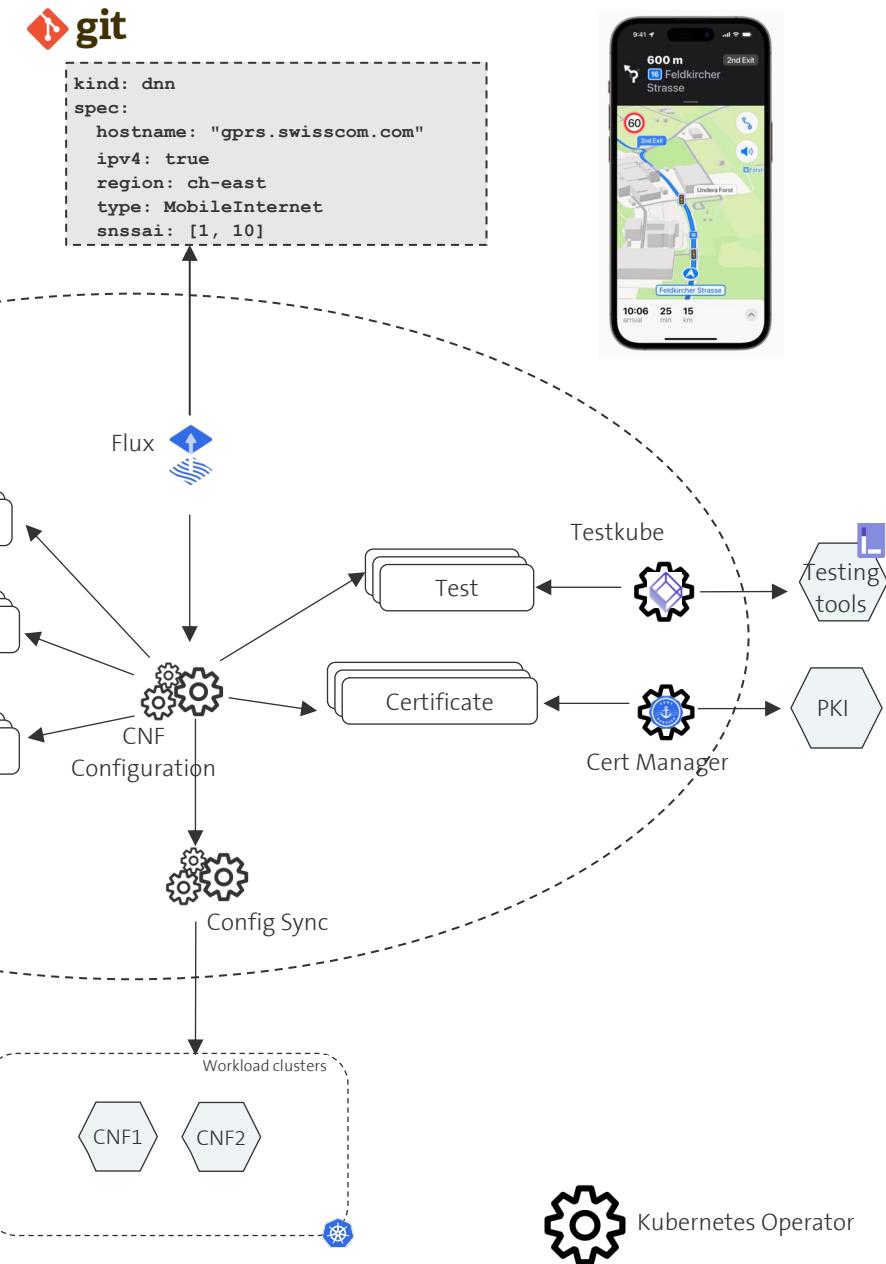




Current State

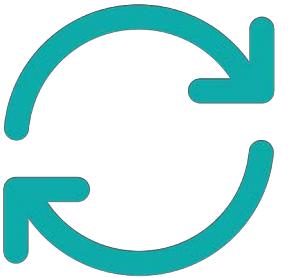


Future State



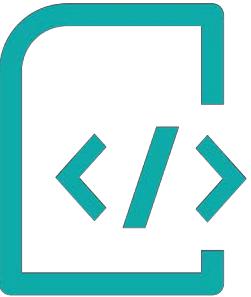


So how will we improve with the new Solution?



Reconciliation

K8s Operator
for NETCONF



Abstraction and
simplification layer

Dynamic config
generation



In-band
with Kubernetes

K8s Operators
in the cluster



Our Learnings & Suggestions

... when thinking beyond GitOps





Avoid

Using Fire-and-forget CI tools for CD

...because they usually don't reconcile

Checking in low level configurations in Git

Things like IP Addresses, VLAN IDs

Using Kubernetes out-of-band automation tools

Tools like Ansible Playbooks or Jenkins

NETCONF

we'd like to see a NETCONF-free 5G Core





Aim to

Reuse cloud native tools to be in-band with K8s

...like Flux, Argo, Testkube, cert-manager

Create your own Kubernetes Operators

...if the existing ones don't do the job

Validate all four GitOps Principles in your System

Verify that you properly implemented the principles

Implement abstractions of your configuration

Dynamically fetch low level configuration

Contribute to the ecosystem

Share your code





Further material

GitOps Principles by OpenGitOps

<https://opengitops.dev>

<https://github.com/open-gitops/documents/blob/v1.0.0/PRINCIPLES.md>

How We Are Moving from GitOps to Kubernetes Resource Model in 5G Core — Ashan Senevirathne and Joel Studler at KubeCon Europe 2024

<https://www.youtube.com/watch?v=crmTnB6Zwt8>

Accelerating Cloud Native in Telco Whitepaper

https://github.com/lfn-cnti/bestpractices/blob/main/doc/whitepaper/Accelerating_Cloud_Native_in_Telco.md

SDC – Schema Driven Configuration

<https://docs.sdcio.dev>

<https://github.com/sdcio>



Thanks!





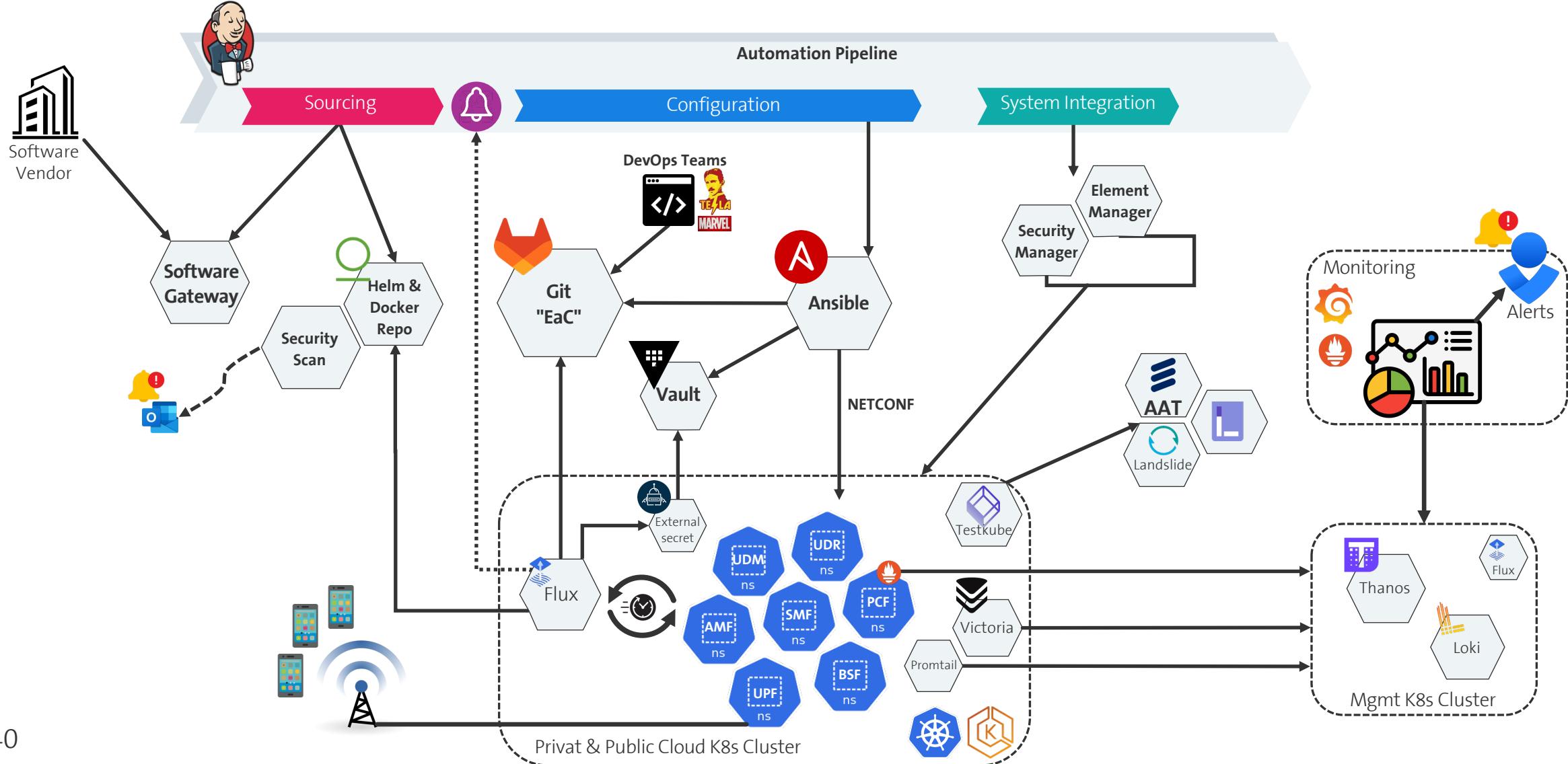
Q&A



Backup Slides

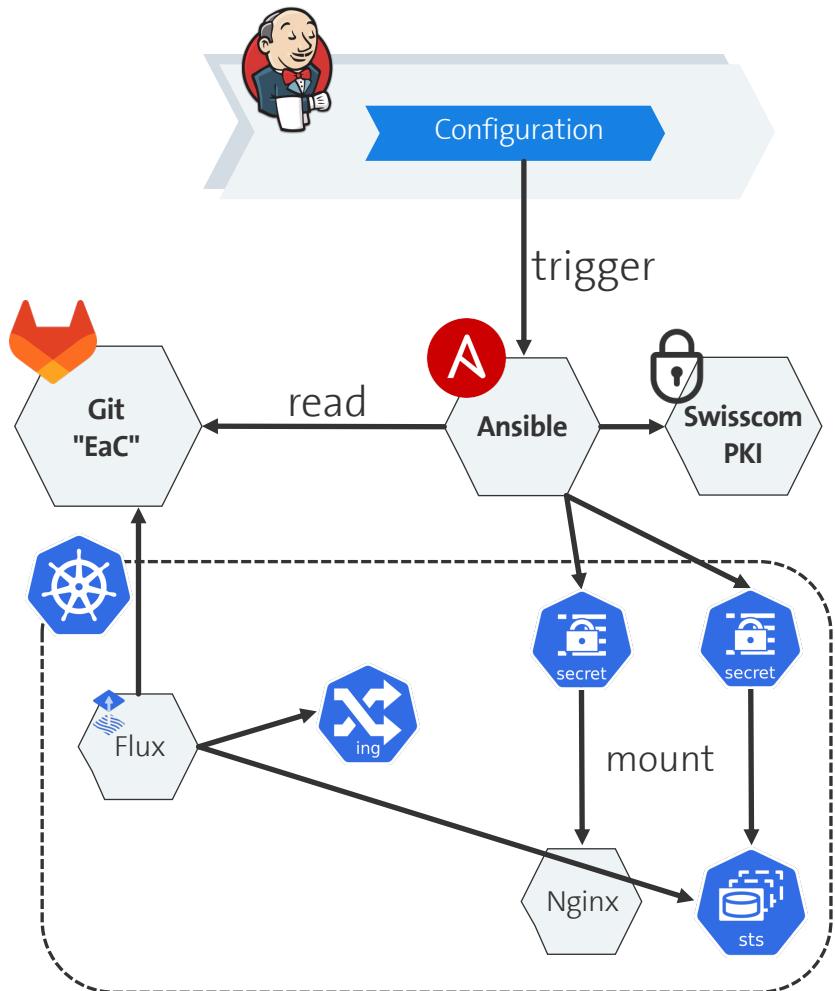


Our automation journey. Where we started

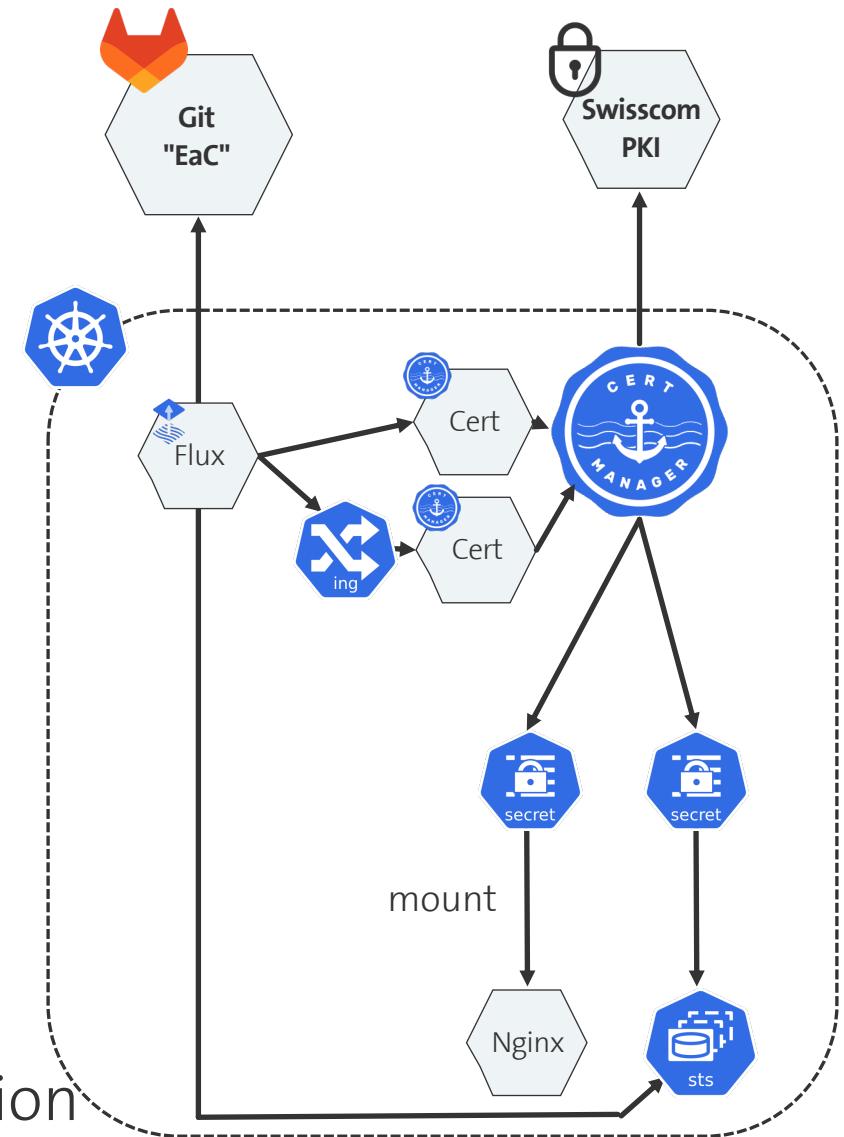




Example Certificate management

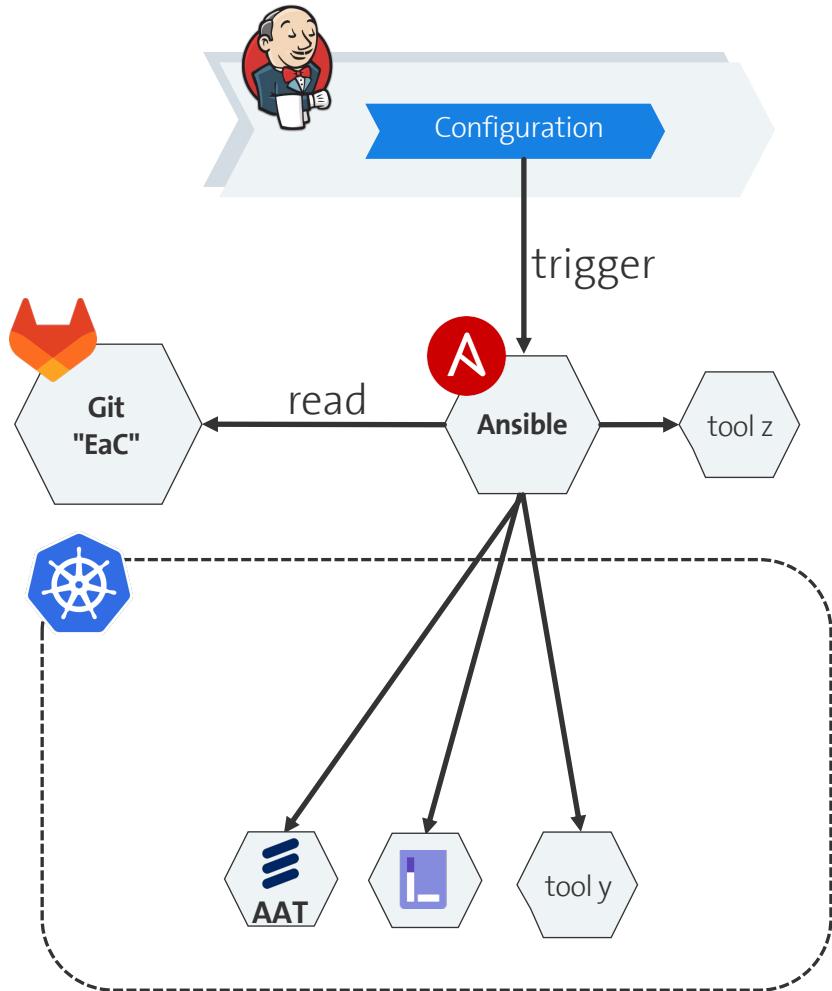


- ✓ Cert rotation
- ✓ Privat Key location





Example Testing



✓ Integrated
✓ Single Pane

