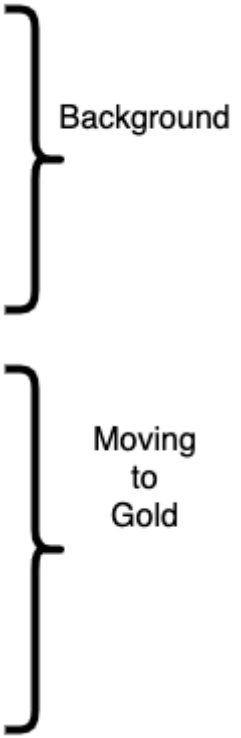
API Programme Services

Road to Gold

Agenda

1. What is API Programme Services?
2. Infrastructure as Code
3. Continuous Delivery
4. Metrics and Alerting
5. Disaster Recovery Terminology
6. Architecture Decisions for DR
7. Global Server Load Balancer (GSLB)
8. Patroni Postgres Failover
9. What, no writes?
10. Switchover Agent
11. Isolated DR Testing
12. Kong Data Planes
13. Our Data and Service Objectives
14. Community Contributions



What is API Programme Services?

At the core, it is a team that champions the benefits and best practices of APIs across government, fosters a community, and offers an API Gateway for configuring and securing access to data.

15M	6	75	12
REQUESTS PER DAY	MINISTRIES	ACTIVE SERVICES	TEAM MEMBERS

Online Services:

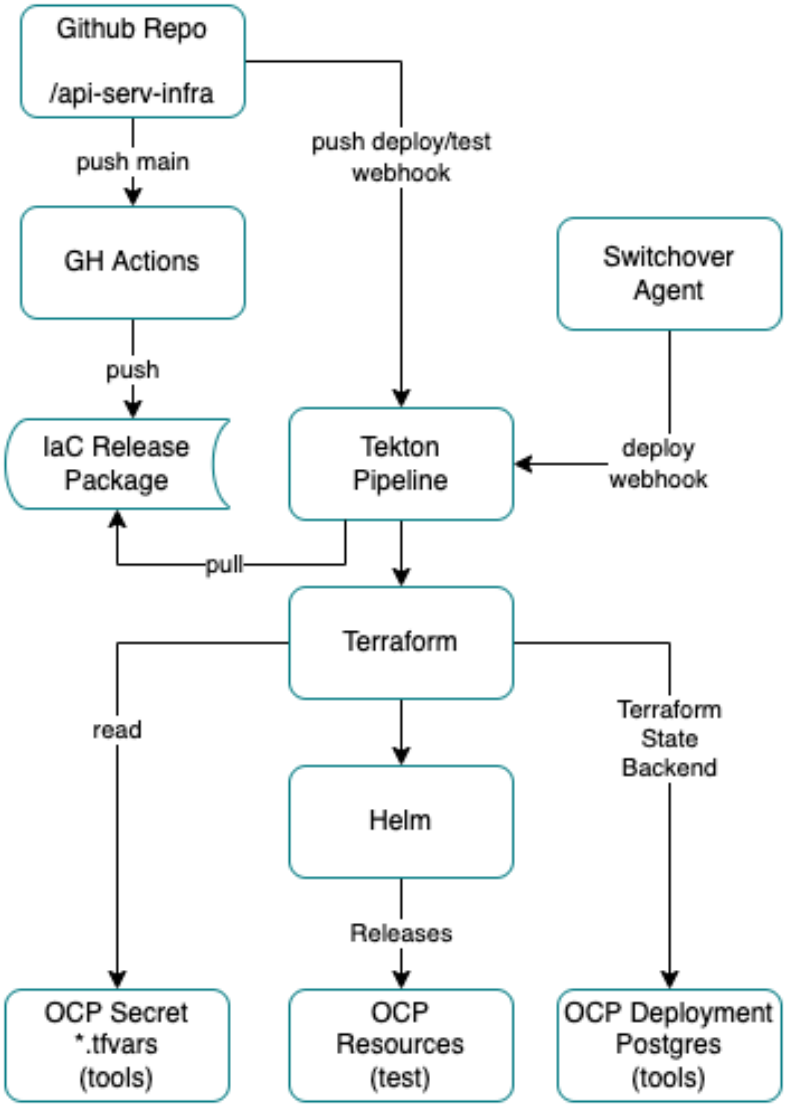
- API Gateway (Kong CE)
- API Services Portal (BC Gov)
  - Community to discover and request access to APIs
  - Ministries to publish APIs, monitor traffic and manage Consumer access

Infrastructure as Code (IaC)

Guiding principle:
Container-Platform Agnostic

Where possible, using `Kubectl`, `Terraform` and `Helm`

- Private Repository: https://github.com/bcgov-dss/api-serv-infra
- `dev` and `main` branches
- `deploy/dev`, `deploy/test` and `deploy/prod` branches containing a `package-tag` file with Release tag



Continuous Delivery

- IaC updates to `dev` and `main` triggers deployment to `dev` and `test`
- Same Tekton Pipeline deployed in Silver, Gold and Gold DR and used for `dev`, `test` and `prod`
  - https://github.com/bcgov/helm-charts/tree/master/charts/ocp-tkn-terraform-pipeline
- All Container Images stored in Github Package Registry
- Aqua scanning (https://aqua.apps.silver.devops.gov.bc.ca)
- Wildcard Certificates stored in Vault (https://vault.developer.gov.bc.ca)

> Roadmap:
>
> - Tekton metrics in Sysdig Cloud
> - Transitioning to Vault for external dependency config
> - Transitioning to Artifactory for Package Registry

Metrics and Alerting

Standardized on Prometheus format for metrics

Multiple sources scraped:

- Kong, FluentD, Postgres, Switchover Agent

Features:

- Use for our own Ops and for Clients
- Metrics to our Clients via Prometheus and Grafana
- Federate to Gold/GoldDR from Silver
- Alerts: Grafana and Sysdig Cloud
  - `APS_ALERTS` MS Teams and `Email` distribution lists
- Uptime Robot https://stats.uptimerobot.com/KZ3Nvh29l1/787465259

> Roadmap:
>
> - Ops metrics and Client metrics in Sysdig Cloud
> - OpsGenie and Uptime.com

Disaster Recovery Terminology

Term	Values
Data Center	Kamloops (kdc) and Calgary (cdc)
OCP Cluster	Gold and GoldDR
Project	`b8840c`
Environment	Dev, Test, Prod
LB Site	Active, Passive
Storage	Master, Standby
DR Role	Primary, Standby
Cluster	`Gold` =Project `b8840c` in Kamloops/Gold/Active `GoldDR` =Project `b8840c` in Calgary/GoldDR/Passive

Key Architecture Decisions

Decision	Primary Driver
Move to Gold	Client Requirement
Implement Kong Hybrid	Minimize Client Impact
Switchover Automation	Role and behavior of GSLB Automated vs Managed
Terraform Postgres State	Kubernetes was an option
Upgrade Patroni Spilo	From 1.6 to 2.1 - Postgres 12
Jenkins to Tekton	Excessive resources

> Potential Updates:
>
> - Artifactory - Move Images from Github Package Registry
> - Adoption of Crunchy DB (Operator)
> - Consolidate Alerting to Sysdig Cloud
> - Public Cloud Data Planes
> - Improve availability of Keycloak Authorization Services (Keycloak X?)

Global Server Load Balancer

`F5 BIG-IP DNS` is a system that monitors the availability and performance of global resources and uses that information to manage network traffic patterns.

What the GSLB is calling

```
curl -k "https://142.34.229.4/health" -H "Host: ggw.api.gov.bc.ca"
<html><body>iamalive</body></html>
```

What the GSLB adjusts

```
dig "ggw.api.gov.bc.ca.glb.gov.bc.ca"

;; ANSWER SECTION:
ggw.api.gov.bc.ca.glb.gov.bc.ca. 30 IN    A    142.34.229.4
```

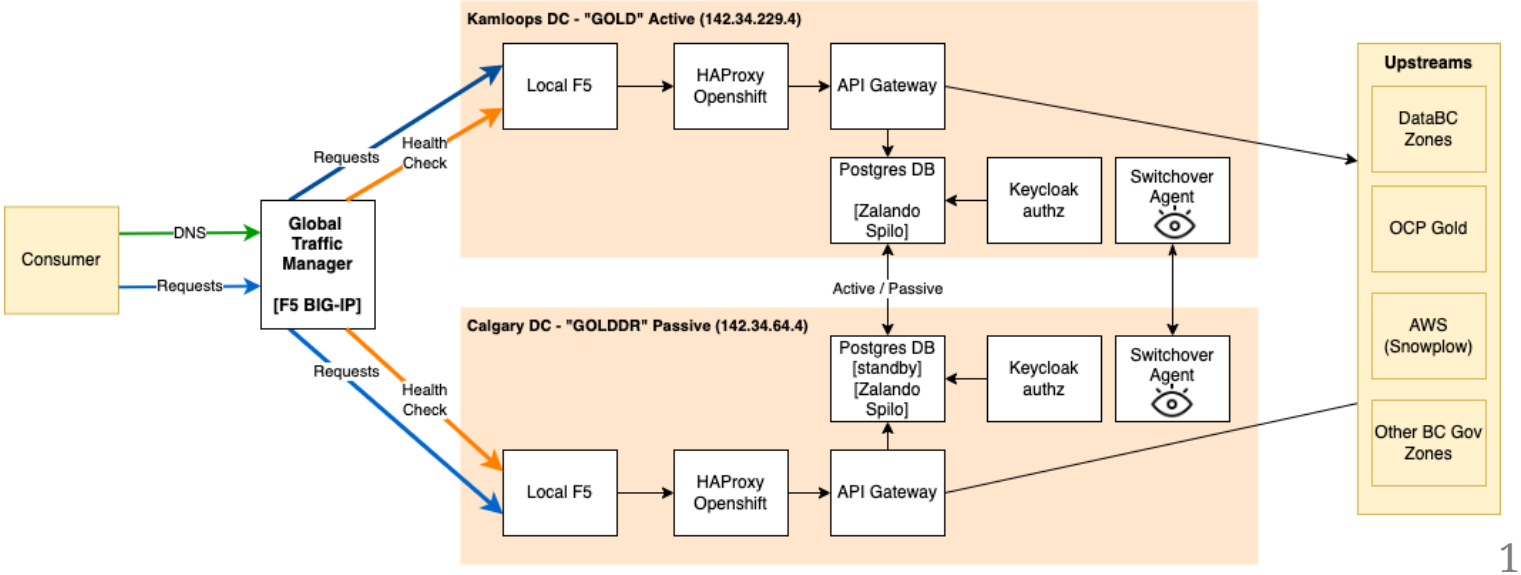
How our DNS is configured

```
CNAME *.api.gov.bc.ca  -> ggw.api.gov.bc.ca.glb.gov.bc.ca
```

Global Server Load Balancer - Unit Testing

GSLB Testing suite https://github.com/bcgov/aps-testing

```
baseline_all_down
test_happy_path
test_switch_to_dr
test_total_outage
test_switch_to_primary
test_dr_down
test_dr_then_recovery
test_dr_maintenance_with_outage
```



Patroni Postgres Failover

We use `patroni` clustering solution to provide In-Cluster failover.

There is a Patroni Cluster on `Gold` running as a `Master` and on `GoldDR` running as a `Standby` (can be vice-versa if in a Recovery scenario).

A Patroni Standby Leader connects directly to a Patroni Master for replication.

```
{
  "standby_cluster": {
    "host": "patroni-spilo-transport-patroni-gold",
    "port": 8424
  }
}
```

> Roadmap - Assessing Crunchy DB Operator and using incremental backups to ObjectStore S3 for recovery

What, no writes?

Three services use Postgres:

`API Services Portal` can run ok with unauthenticated users, so part of the site will function. Logging into the portal writes information to the database and it relies on Keycloak.

`Keycloak` fails to start.

`Kong Control Plane` starts but is quite unhappy about it.

The `Kong Data Plane` depends on the Kong Control Plane but can run safely without for a period of time.

> How these services interact with each other, and how they behave in a failure situation will impact the approach for automating failover.

Switchover Agent

A new service run in both Gold and Gold DR, that makes decisions about whether or not to switch traffic to the DR site, and actions those decisions.

https://github.com/bcgov/switchover-agent

Connects to each other via mTLS using a `TransportServerClaim` tunnel

Observers:

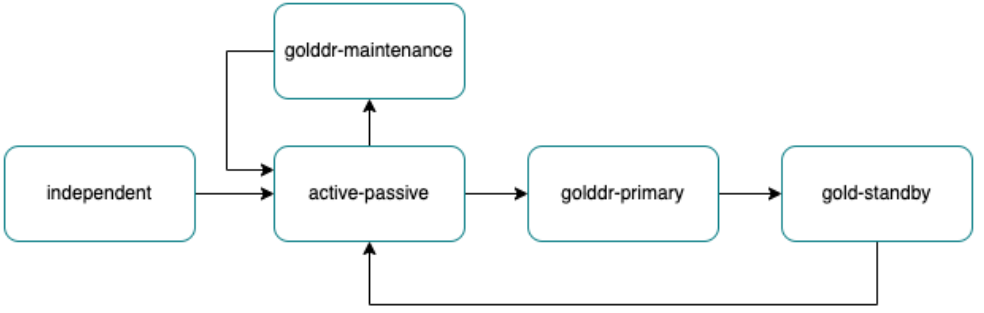
- GSLB Domain Resolution (`ggw.api.gov.bc.ca.glb.gov.bc.ca`)
- Patroni Health
- Peer Connectivity
- 'switchover-state' ConfigMap
- Tekton Pipelines

Switchover Agent - States

State	Description
active-passive	Healthy state where traffic is going to Gold Cluster
golddr-primary	In Recovery where traffic is going to GoldDR Cluster
gold-standby	In Recovery still, but Gold is ready to return to `active-passive`
golddr-maintenance	Healthy state (traffic on Active), with GoldDR Cluster taken offline to do isolated testing

The `Switchover Agent` only automates the transition to **golddr-primary** - all others are human initiated via the 'switchover-state' ConfigMap.

State model



Switchover Agent - Testing

In our Development environment, we have a set of Cron Jobs that cycle through the states automatically throughout the day, every day.

We do this to better understand the impacts during these transitions. We also work in `dev` all the time, so any unusual behavior can be investigated.

Time	Outcome	Transition To
Midnight	Failover to `Passive site` - "in recovery"	`golddr-primary`
4 am	`Active site` is back online, make it Standby	`gold-standby`
5 am	Make `Active site` Primary and `Passive` site Standby	`active-passive`
8 am	Failover to `Passive site` - "in recovery"	`golddr-primary`
Noon	`Active site` is back online, make it Standby	`gold-standby`
1 pm	Make `Active site` Primary and `Passive` site Standby	`active-passive`
4 pm	Failover to `Passive site` - "in recovery"	`golddr-primary`
8 pm	`Active site` is back online, make it Standby	`gold-standby`
9 pm	Make `Active site` Primary and `Passive` site Standby	`active-passive`

Switchover Agent - Example

Transition: `active-passive` to `golddr-primary`

Observation: GSLB is resolving domain to the `Calgary/GoldDR/Passive` IP

Kamloops/Gold/Active:

- set `in_recovery` to `True` in `.tfvars`
- maintenance mode is on
- health api is scaled down
- notify Peer (if possible but not necessary)

Calgary/GoldDR/Passive:

- set `in_recovery` to `True` in `.tfvars`
- maintenance mode is on
- health api is scaled up (should already be)
- enable patroni as Master
- trigger deployment (will scale up Keycloak, Kong Control Plane)
- wait for deployment to complete (Tekton Event ID)
    - then turn maintenance mode off

Switchover Agent - Maintenance Mode

The Maintenance logic affects two services: API Services Portal and the `authz` Keycloak service.

When it is turned ON:

1) API Services Portal's Maintenance banner is displayed

2) The `keycloak-http` service has its Pod Selector changed to a `Maintenance Service` that always returns 302 redirect to the Portal

When it is turned OFF:

1) API Services Portal's Maintenance banner is removed

2) The `keycloak-http` service has its Pod Selector changed back to Keycloak.

3) `Maintenance Service` deployment is cycled (force closes any keep-alive connections)

Isolated DR Testing

On a scheduled (yearly?) basis, there is a need to isolate the `GoldDR` Cluster so that it can be tested without impacting production.

Transition: `active-passive` to `golddr-maintenance`

Kamloops/Gold/Active:

- `in_recovery` must be `False`

Calgary/GoldDR/Passive:

- `in_recovery` must be `False`
- set `in_maintenance` to `True` in `.tfvars`
- health api is scaled down (no traffic is sent to `Calgary/GoldDR/Passive`)
- initiate work to make `Calgary/GoldDR/Passive` detached and "healthy"
  - maintenance mode is on
  - enable patroni as Master
  - trigger deployment (will scale up Keycloak, Kong Control Plane)
  - wait for deployment to complete (Tekton Event ID)
  - then turn maintenance mode off

Isolated DR Testing - Local Setup

`in_maintenance` is used in the Terraform configuration to add in `hostAliases` to the Kong Control Plane and API Services Portal for the `authz` service.

This is necessary because these services internally use the GSLB Url and it needs to route to the `GoldDR` Cluster.

https://authz.cdc.api.gov.bc.ca/.../.well-known/openid-configuration

```
{
  "authorization_endpoint":"https://authz.cdc.api.gov.bc.ca/auth/realms/.../auth",
  "token_endpoint":"https://authz.apps.gov.bc.ca/auth/realms/.../token",
}
```

Locally, static name resolution can be added (example for `dev`):

`142.34.64.4 api-gov-bc-ca.dev.api.gov.bc.ca`

`142.34.64.4 authz-apps-gov-bc-ca.dev.api.gov.bc.ca`

In a local browser, can then go to: https://api-gov-bc-ca.dev.api.gov.bc.ca

After completion, the system can be transitioned back to `active-passive`.

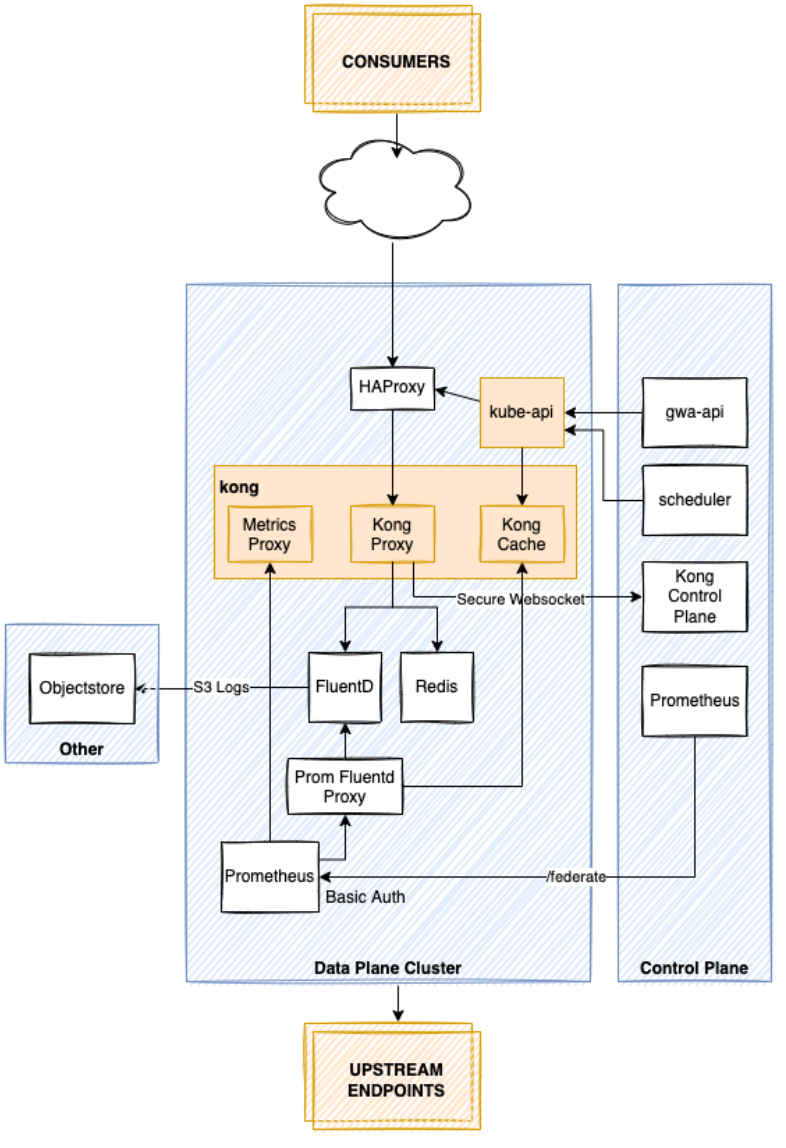
Kong Data Planes

Kong Hybrid supports the separation of a Control Plane supporting multiple Data Planes.

We deploy a Data Plane in each Cluster, including Silver.

They each connect to the GSLB Url of the Control Plane `gwcluster.api.gov.bc.ca` over an mTLS connection.

They remain available for a period of time, even with connection failures to the Control Plane.



Our Data and Service Objectives

Our Data on Postgres:

- Keycloak - Authorization Services (~15MB)
- API Services Portal (~100MB)
- Kong API Gateway (~15MB)

Recovery Point Objectives (RPO) : *Time between Last Backup and Event*

- Continual connection to Master; less than 1 minute
- If restore from backup required, then ~5 minutes

Recovery Time Objectives (RTO) : *Time between Event and Data Restored*

- Less than 1 minute
- Restore using BC Gov Objectstore S3 (if from backup)

Service Objectives:

Online Service	**RTO**
Kong API Gateway	0 seconds
API Services Portal	20 minutes

Community Contributions

The APS team created these projects to support our service on Gold:

- https://github.com/bcgov/aps-testing
- https://github.com/bcgov/helm-charts/generic-api
- https://github.com/bcgov/helm-charts/ocp-tkn-terraform-pipeline
- https://github.com/bcgov/helm-charts/ocp-transport-claim
- https://github.com/bcgov/helm-charts/patroni-spilo
- https://github.com/bcgov/switchover-agent

BC Gov Open source projects:

- https://github.com/bcgov/gwa-cli
- https://github.com/bcgov/gwa-api
- https://github.com/bcgov/api-services-portal

Thank You!

Reach out on Rocket.Chat #aps-ops

FD	Aidan	PO	Jonathan
TW	Carol-Anne	FD	Joshua
BA	Chris	TA	Justin
UX	Elisa	SM	Mariel
BA	Graeme	QA	Niraj
CE	Hannah	TA	Nithin