Cloud and Compliance

The perfect match ?

By Tanguy Combe & Ismaël Hommani

20 novembre 2021

Compliance
Mastering risks

In short

Compliance is a set of rules to abide by in order to manage the risk and guarantee that your softwares behave as expected (is my data safe, how my production is run, ... ?).

Compliance is usually motivated by

- Legal aspects (PCI-DSS; RGPD, ...)
- Internal aspects (HR, environment, budget,...)

Compliance protect you from legal risk but can also serves as a commercial asset.

Compliance, business and innovation
Finding the right balance

Create a *win-win* situation

Compliance should never be an obstacle to your business and innovation;

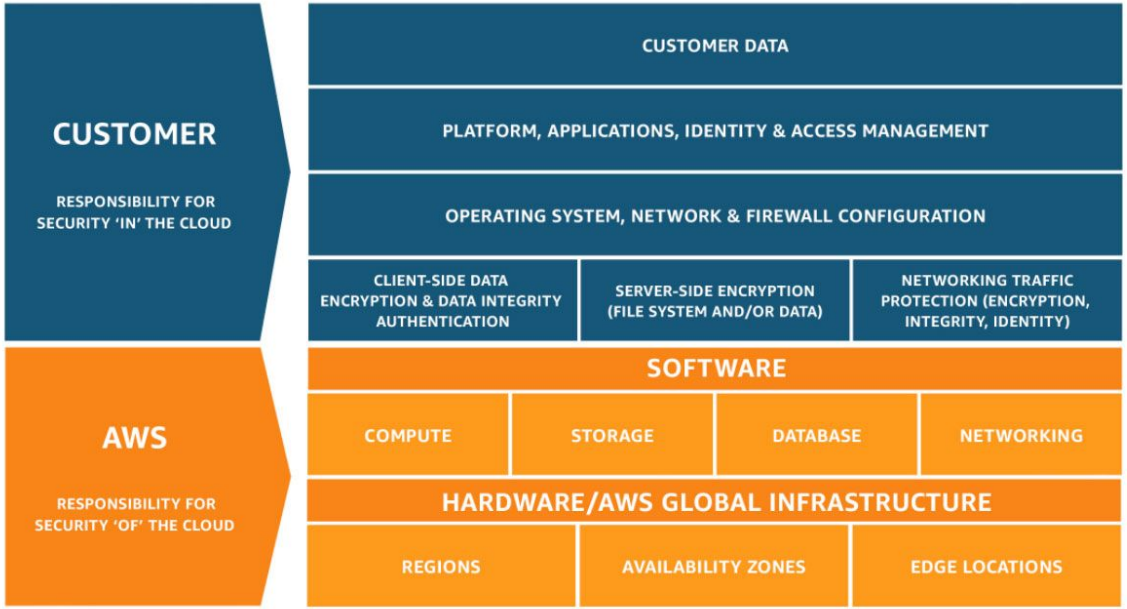
Think compliance as part of your business and embrace it.
It implies to:

- Think its implementation through proven processes and best practices
- Think it continuously and in an automatic manner

⇒ Audit is a non event through **Compliance As Service**
⇒ Ease of evolution through **Compliance As code**
⇒ **Rise of the Compliance Governance**

A shared responsibility model

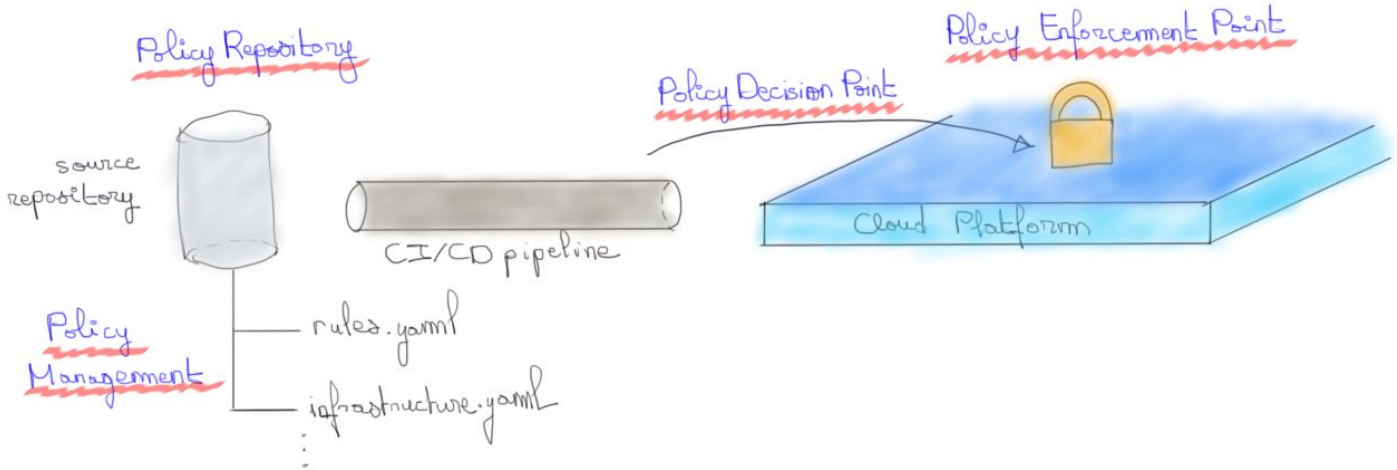
Accountability when consuming Cloud



https://aws.amazon.com/compliance/shared-responsibility-model/

Compliance As Code & As A Service

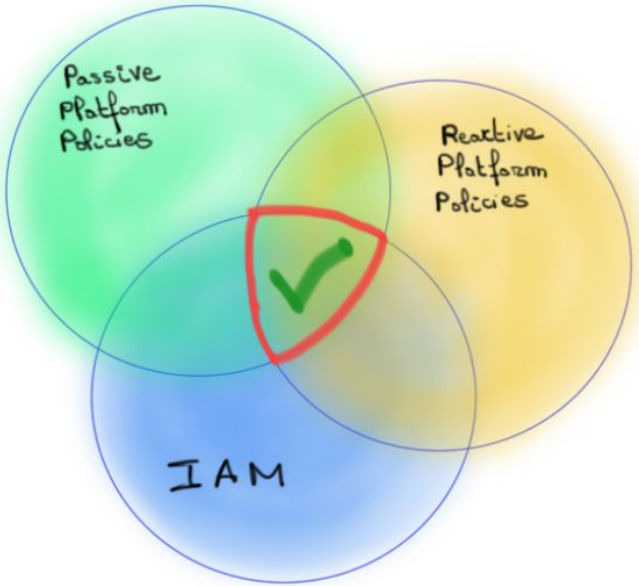
Bake the compliance into the platform rather than the soft



Overview

A three layers model

- Provided by the cloud platform as Managed services



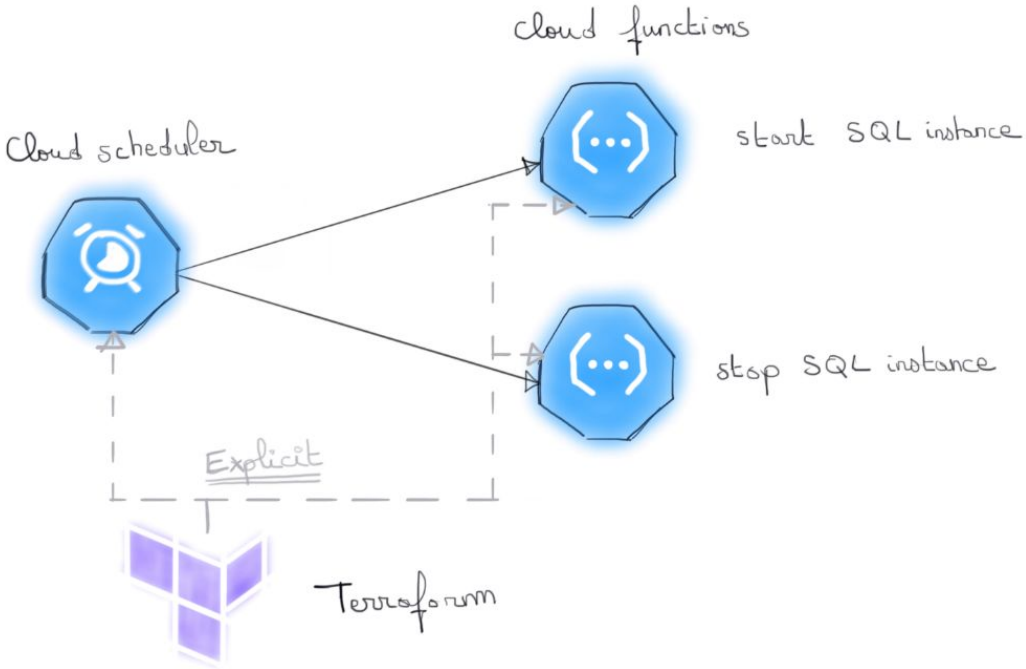
- Implemented through the instantiation of dedicated processes that react to events

- Platform provided

Reactive Platform Policies

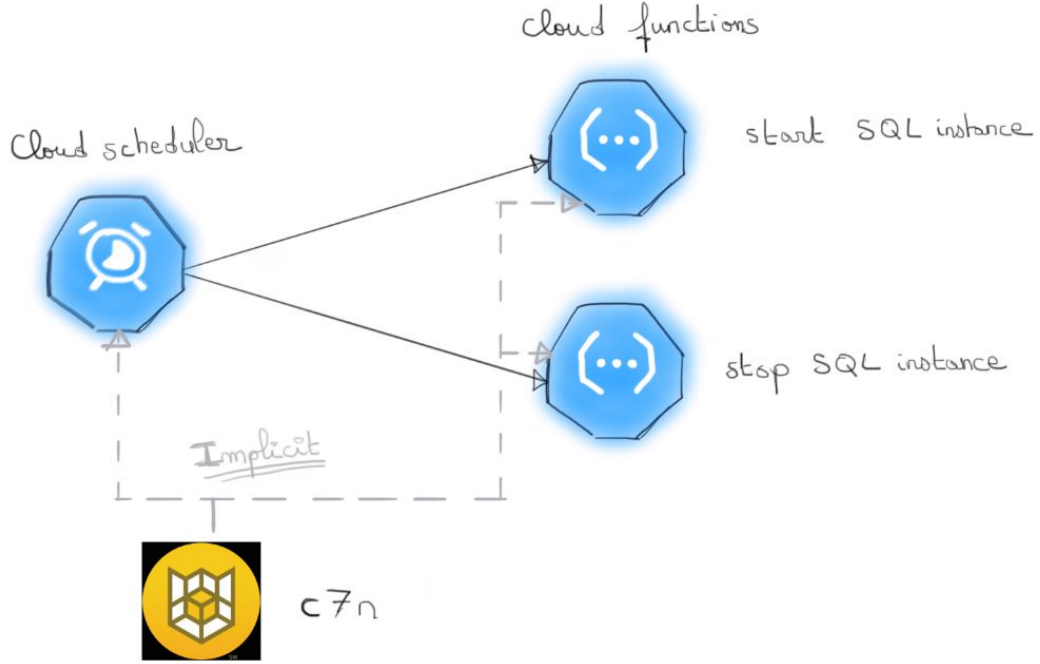
An answer to the lack of the passive approach

Hand made:



Reactive Platform Policies

Declarative approach with Cloud Custodian



Cloud custodian

A rules engine running on cloud managed services

- Simple YAML DSL
- Python library
- Run anywhere
- Multi cloud: AWS, Azure, GCP
- CNCF Sandbox
- Open source (one release a month)

Cloud custodian

Under the hood

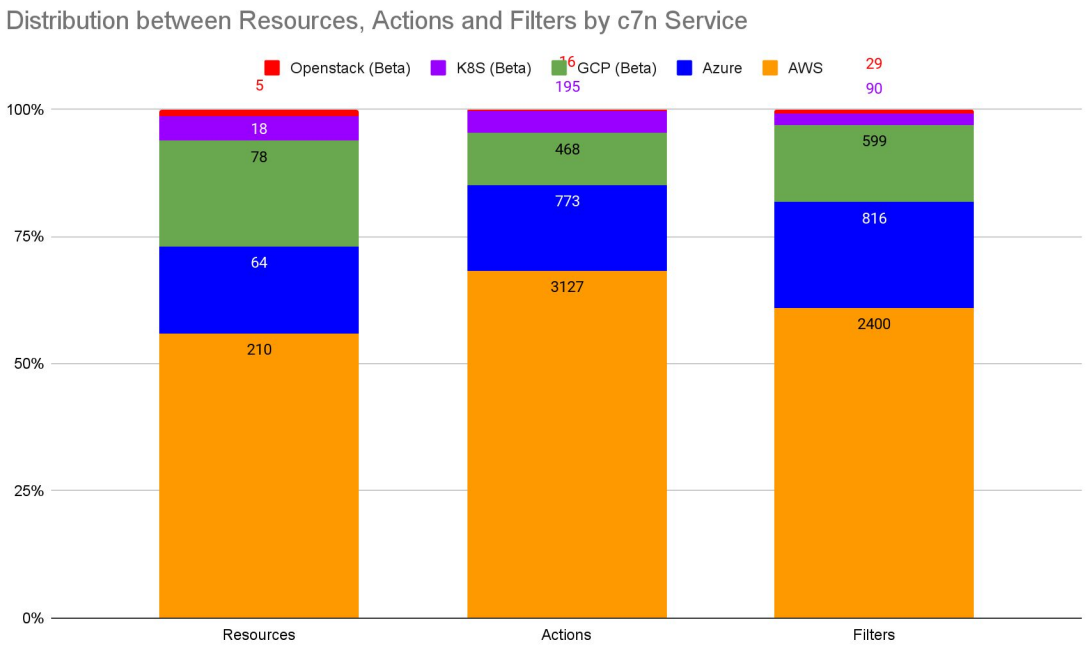
A simple YAML DSL to identify :

- The resource type targeted by the policy
- Filters to apply to match resources
- Actions on the filtered resources

```yaml
# myPolicy.yml
policies:
   - name: find-non-attached-disks
     resource: azure.disk
     filters:
      - type: value
        key: managedBy
        value: null
     actions:
      - type: delete
```

Cloud custodian

Répartition par Service



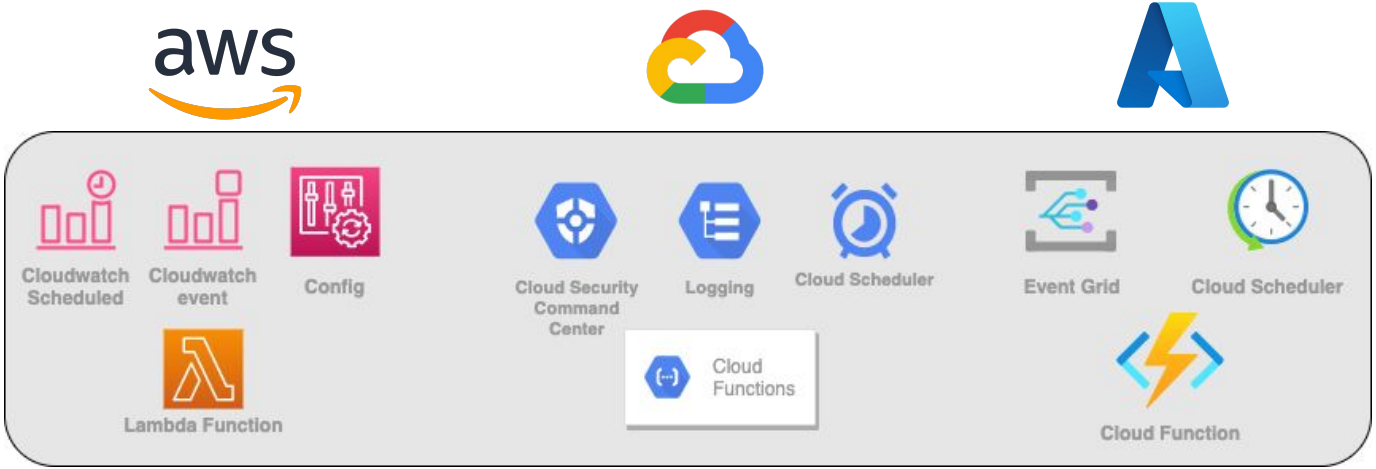
Cloud custodian

Execution modes

Local Run

Event Trigger

Periodic Run



Cloud custodian

Filters types

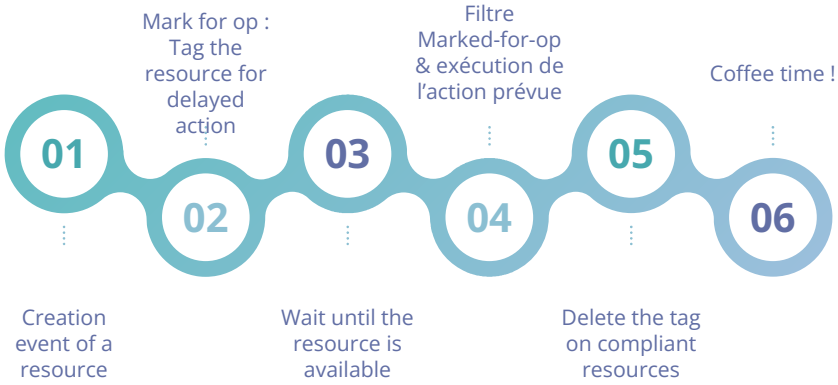
- Value Filter
- Event Filter (serverless execution only)
- Specific Filter

GitLab

Cloud custodian

A more complex example

- Link policies together
- Mark-for-op / Marked-for-op
- Delayed actions



GitLab

Cloud custodian
Usage and integration

- Bringing GitOps to manage compliance

- Different implementations for different needs :
  - FinOps : Start / Stop dev instances
  - Reactive information : Alerting through slack / splunk / datadog (cc c7n-mailer)
  - Compliance: Bake rules into the cloud platform

Cloud custodian

Open-Source and community

- Identify a need, on a new resource / action / filter
- Develop and test your feature
- Use Cloud custodian Stubber maker to record your test
- Open a pull request

https://github.com/cloud-custodian/cloud-custodian/pull/6750/files


Cloud custodian in the GCP

WeScale - Who are We?

2015

Company creation

50

Cloud passionate folks

PARIS

NANTES

FULL REMOTE

Our partnerships

CLOUD NATIVE COMPUTING FOUNDATION
SILVER MEMBER

kubernetes CERTIFIED SERVICE PROVIDER

HashiCorp

aws partner network
Advanced Consulting Partner

Partner
Google Cloud

Wescale training

Master Cloud Native technologies
Train yourself anywhere in France and remotely

OUR TRAINING PROGRAMS

aws
Google Cloud
docker
kubernetes
HashiCorp Vault
ANSIBLE
HashiCorp Terraform
DevSecOps

OUR CERTIFICATIONS

aws partner network
Training Partner

Vault ASSOCIATE
HashiCorp CERTIFIED

Datadock

Qualiopi
processus certifié

OFFICIAL PARTNER

HashiCorp

Questions ?

Thank you for your attention