sourced
cloud at scale™

Open Policy Agent

Flexibility & Security with Policy as Code

5 September 2019

Who Are We?

Ravi Nair

Consultant

Worked in the industry for over 10 years across various roles including Application Support, Build & Release, Infrastructure Operations and Application Development

Drew Taylor

Consultant

Worked in the industry for over 15 years from multi-nationals to start ups which included a diverse range of technologies; Cloud, Hosted and VOIP

sourced
cloud at scale™

Agenda

01 OPA : An Introduction

02 Rego : An Introduction

03 How and Where OPA Fits In

04 Demo

05 Other Tools in the Market

sourced
cloud at scale™

OPA : An Introduction

OPA : An Introduction – What is Policy?

- All organisations have policies
- Essential to long term success
- Comply with legal and governance requirements
- Usually applied manually
- Enforced with application logic if required
- Or statically configured at deploy time

sourced
cloud at scale™

OPA : An Introduction – What is Policy?

Definition

10. Data[2] refers to the representation of facts, figures and ideas. It is often viewed as the lowest level of abstraction from which information and knowledge are derived.

11. Data risk encompasses the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events impacting on data. Consideration of data risk is relevant regardless of whether the data is in hard copy or soft copy form. Examples include:

    (a) fraud due to theft of data;

    (b) business disruption due to data corruption or unavailability;

    (c) execution delivery failure due to inaccurate data; and

    (d) breach of legal or compliance obligations resulting from disclosure of sensitive data.

12. For the purposes of this PPG, data risk is considered to be a subset of operational risk, which includes information and information technology risk. In addition, information and information technology security risk overlaps with data risk (refer to the diagram below).[3]

objectives (including regulatory and legal requirements). Consequently, it is important that business functions understand and manage the risks associated with the data required for the successful execution of their processes. Additionally, an understanding of data risk is beneficial when managing other types of risk.

Data risk management

13. A regulated entity would typically manage data risk in alignment with the operational risk framework and, where relevant, in conjunction with other risk management frameworks (e.g. credit, market and insurance risk management frameworks), depending on the nature of the data involved.

14. A goal of data risk management is to ensure that the overall business objectives of a regulated entity continue to be met. Therefore, it is important that an individual business unit's objectives are not considered in isolation, but rather in the context of the objectives of the entity as a whole. Consequently, the design of controls for a particular data set would typically take into account all usage of that data.

15. The adequacy of data controls in ensuring that a regulated entity operates within its risk appetite would normally be assessed as part of introducing new business processes and then on a regular basis thereafter (or following material change to either the process, usage of data, internal controls or external environments). The assessment would typically take into account the end-to-end use of the data and related control environment (including compensating controls). Changes to the control environment would typically follow normal business case practices, taking into account the likelihood and impact of an event against the cost

sourced
cloud at scale™

OPA : An Introduction – What is Policy Enablement?

- Allows policies to be written as declarative code
- Updated at any time without redeploying
- Adaptable to changing requirements
- Increases consistency of policies
- Mitigates risk of human error

sourced
cloud at scale™

OPA : An Introduction

CLOUD NATIVE
COMPUTING FOUNDATION

fluentd

Prometheus

Open Policy Agent

kubernetes

etcd

sourced
cloud at scale™

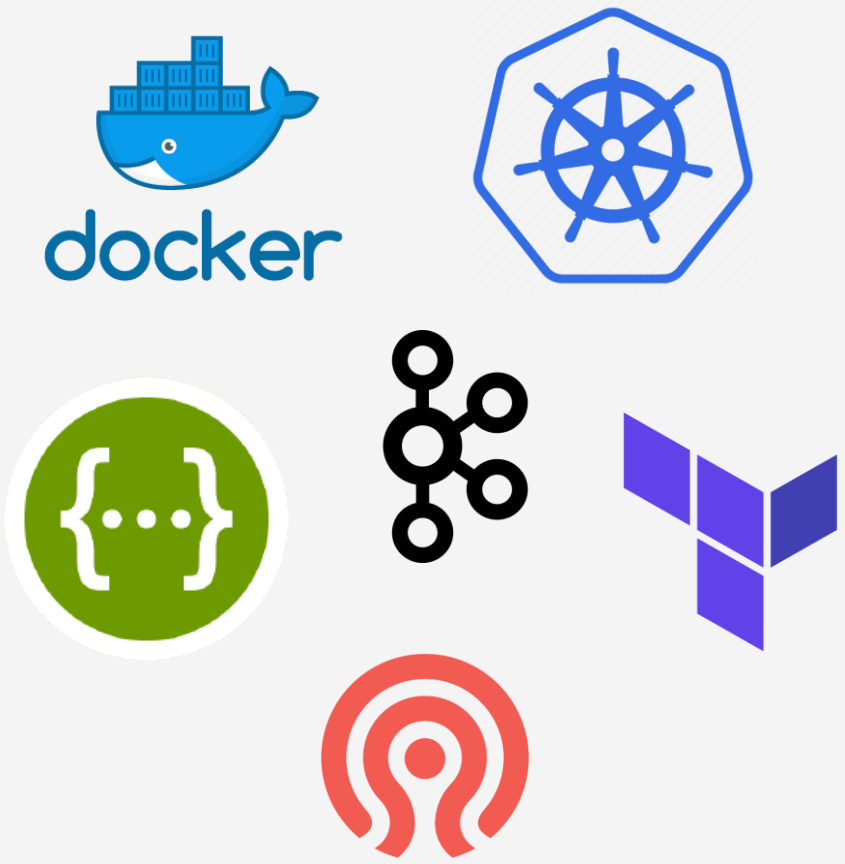
OPA : An Introduction

- Lightweight, general-purpose Policy Engine
- Integrated as a sidecar, host-level daemon or a library
- Core services can offload policy decisions to OPA
- Policy evaluation using a query-like language
- Policies written in high-level declarative language (Rego)

Open Policy Agent

sourced
cloud at scale™

OPA : An Introduction – Use cases



sourced
cloud at scale™

sourced
cloud at scale™

Rego: An Introduction

Rego : An Introduction

- Inspired by Datalog
- Supports structured documents
- Declarative
- Provides a REPL
- Built-in functions
- Variables

```
default v = false

v {
    "hello" != "world"
}
```

```
default v = false

v {
    "hello" == "world"
}
```

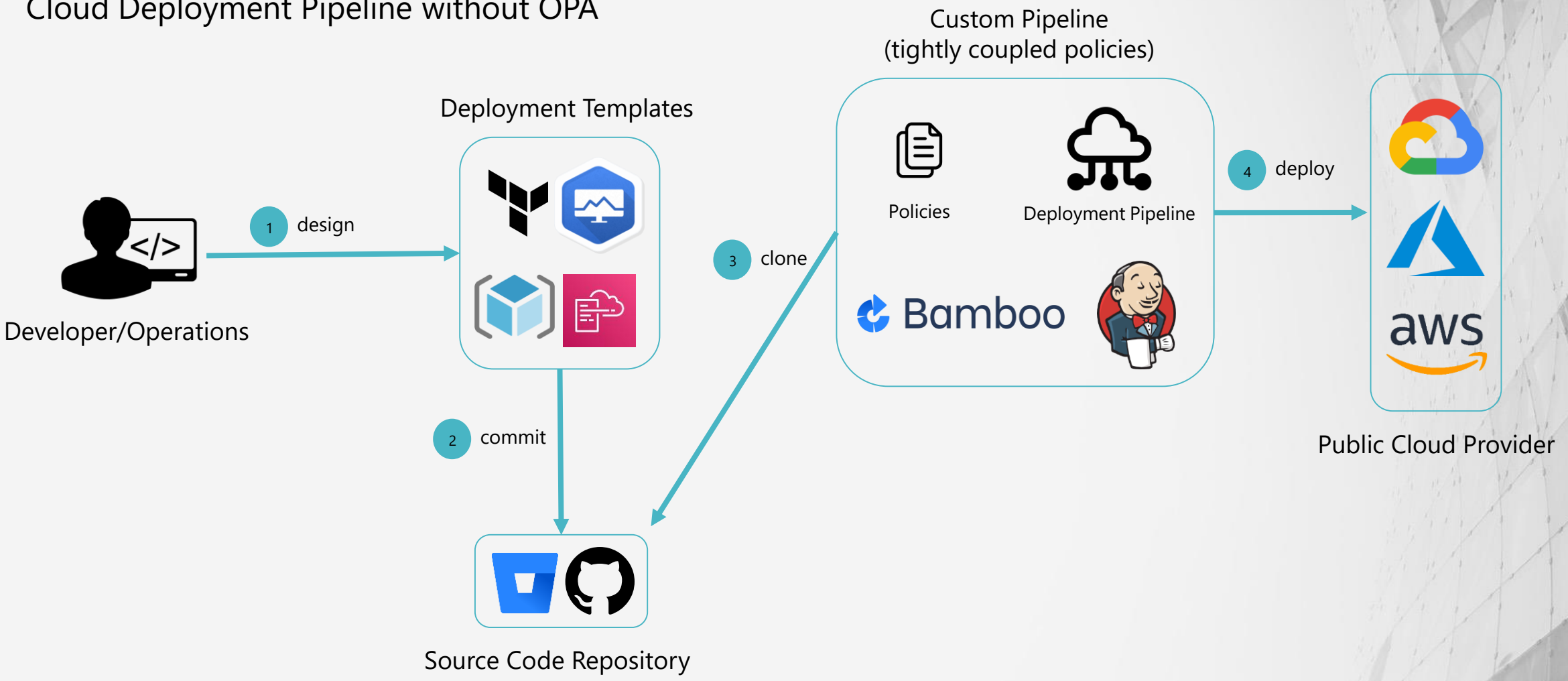

sourced
cloud at scale™

sourced
cloud at scale™

How and Where OPA Fits In

How and Where OPA Fits In

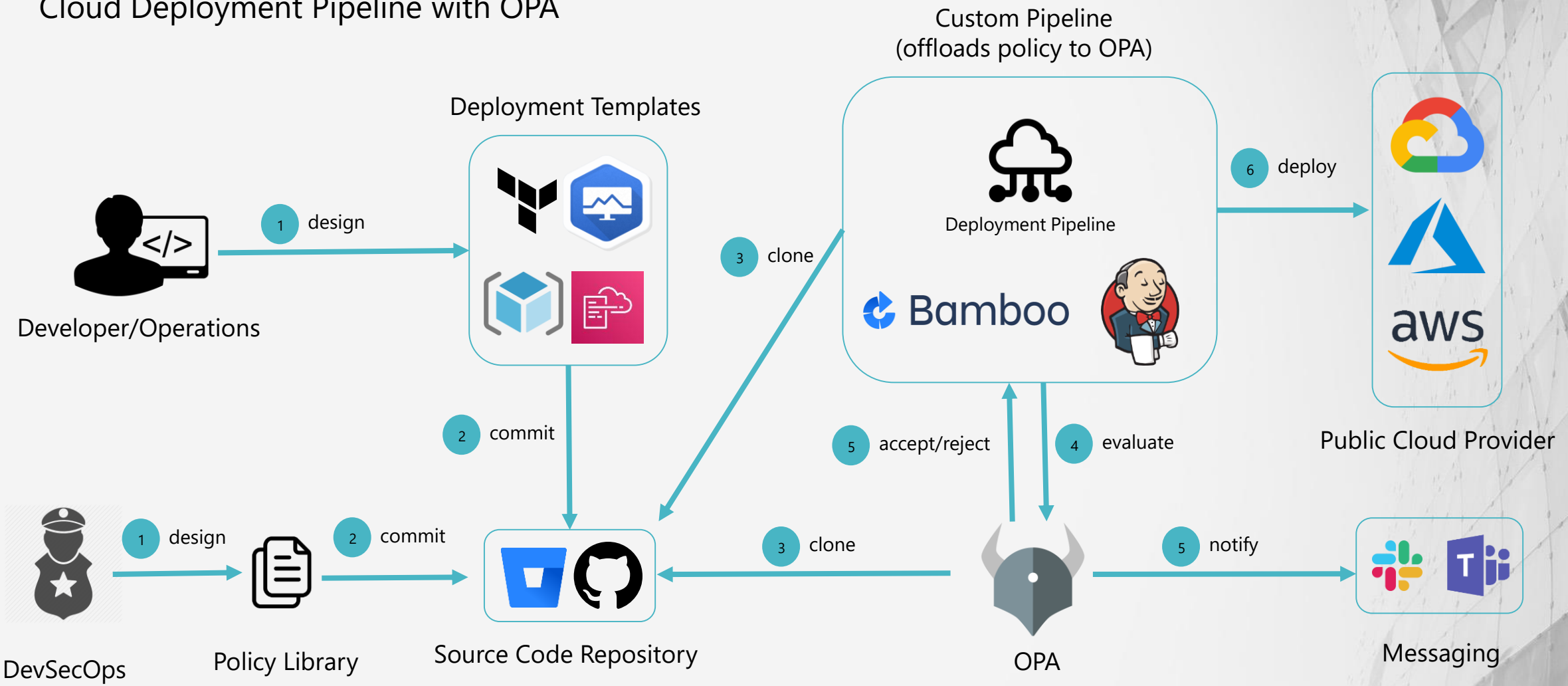
Cloud Deployment Pipeline without OPA



sourced
cloud at scale™

How and Where OPA Fits In

Cloud Deployment Pipeline with OPA



sourced
cloud at scale™

sourced
cloud at scale™

Demo

Prevent Creation of Public Bucket

Other Tools in the Market

Other Tools in the Market

- Sentinel Language
- Integrates natively with other Hashicorp tools

sourced
cloud at scale™

Other Tools in the Market

- Open source toolset (written by Google)
- Provides a config-validator (uses Rego)
- Provides a policy library that has prebuilt policies
- Forseti Scanner can reuse policies written for config-validator (detection)

Forseti

sourced
cloud at scale™

Who Are We?


SINGAPORE
AIRLINES


RHB


CERTIS


QANTAS


sourced
cloud at scale™


aws
partner
network
Premier
Consulting
Partner
Migration Competency
DevOps Competency
Channel Partner
Public Sector Partner


Microsoft
Gold Partner


Premier Partner
Google Cloud

Who Are We?

Enterprise Cloud Computing Consultants

We work with some of the largest and most security conscious organisations around the world to help them unlock innovation through cloud computing.

sourced
cloud at scale™

Thank You

sourcedgroup.com

linkedin.com/company/sourced-group/

@sourcedgroup

sourced
cloud at scale™