

Terraform Deep Dive

오랫동안 테라포밍해본 결론

얼마까지 알아보고 오셨어요?

무언가를 만들때는?

1. 손으로 처음부터 만든다.
2. 기존에 있던 것을 수정해서 만든다.
3. 기존에 있던 것을 삭제하고 다시 만든다.
4. 위에서 만든 것을 손으로 또 만든다.
5. 뭔가를 만들어서 그것이 만들게 하고 손을 쉬게 한다.

But!

그 뭔가를 만드는데 너무 힘들다.

IaC != Terraform

Chef

Puppet

Saltstack

Ansible

Terraform

Pulumi

CDK / CloudFormation

Crossplane

IaC != Terraform

Chef

Puppet

Saltstack

Ansible

Terraform

Pulumi

CDK / CloudFormation

Crossplane

Infrastructure as Code (IaC)

- 개요
 - 인프라를 코드로 관리하여 일관성을 제공하는 방법론
 - 수동 설정의 오류와 비효율성을 개선하기 위해 등장
- 장점
 - 일관성 확보 : 동일한 환경을 반복적으로 구축 가능
 - 버전 관리 : 인프라 변경사항 추적 및 롤백 지원
 - 자동화 : 배포 속도 향상 과 휴먼 에러 방지
 - 협업 강화 : 코드 기반으로 팀간 협업 용이
- 단점
 - 학습 필요 : 새로운 도구와 언어, 개념에 대한 학습 필요
 - 복잡성 증가 : 작은 프로젝트에는 복잡성 유발 가능
 - 초기비용 : 도입 및 설정에 시간과 자원 필요
 - 디버깅 어려움 : 문제 발생시 원인 파악이 어려울 수 있음

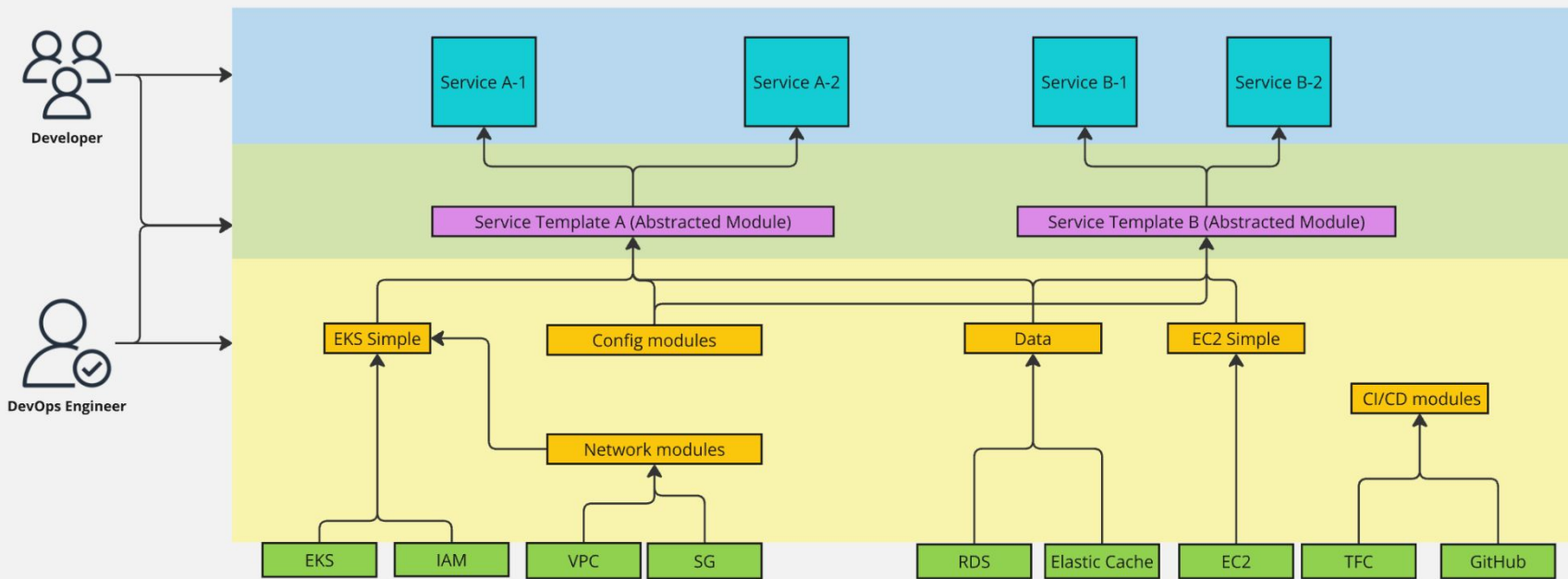
Terraform 을 선택해야 하는 이유, 선택하지 않아야 하는 이유

- 멀티 클라우드 및 다양(?)한 프로바이더를 통한 다양한 지원 가능
- 선언적 언어로 간단(?)하고 명확한 인프라 정의
- 커뮤니티와 에코시스템 활발(?)함 (활발하다고 했지, 문제가 해결된다고는 안했음)
- HCL 구림
- 간단한 프로젝트에는 복잡성을 더함
- 상태 관리 쉽지(?)만 어려움
- 다이나믹 프로바이더 미지원으로 크로스 어카운트, 리전 지원시 복잡 (OT 1.9 지원예정)
- Plan 을 믿을 수 없음
- TFE, TFC 도 별로임, 심지어 유료

Terraform 구성요소

- **Provider** : Terraform 이 인프라 플랫폼과 상호작용하기 위한 플러그인
- **Resource** : 생성하고 관리할 개별적인 인프라 요소를 나타내는 객체
- **Data** : 기존 리소스를 읽어오거나, 임시로 정보를 활용하기 위한 객체
- **Module** : 복잡한 구성을 구조화하여 관리하기 위한 테라폼 객체의 집합
- **Variable / local / Output** : 변수 입출력을 위한 객체
- **Backend** : 상태 저장을 위한 설정 블록
- **Workspace** : 여러개의 독립된 상태를 유지하기 위한 기능
- **tfstate** : 인프라의 현재 상태를 저장하여 변경사항을 추적하는 파일
- **Provisioner (local-exec)** : 리소스 생성후 추가 구성을 위한 스크립트 실행 블록
- **Lifecycle** : 리소스의 생성, 업데이트, 삭제를 제어하는 설정
- **Expressions and Functions** : 값의 계산과 조작을 위한 표현식과 함수
- **File (templatefile)** : 외부 파일을 읽어와 활용하기 위한 함수
- **Dependencies (depends_on)** : 리소스간 의존성을 정의하여 생성 순서를 관리하기 위한 설정

DevOps Engineer 와 Developer 가 공생하는 IaC



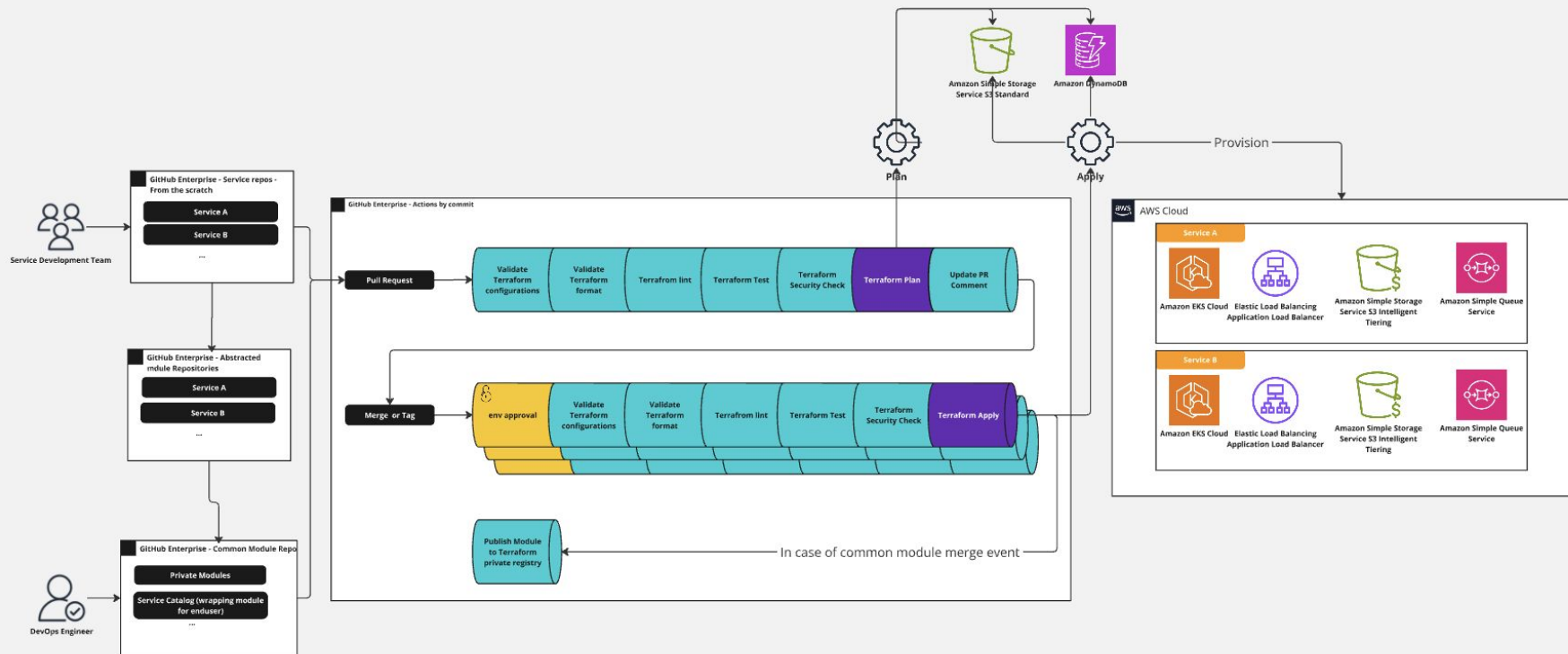
DevOps Engineer 와 Developer 가 공생하는 IaC

```
~/Developments/bitbucket/org/tidesquare/terraform-tidesquare-infra/cell
> make init
init terraform
Available configs
-----
1) halo-p-an2-hub-ICN01
2) halo-p-an2-hub-KOR
3) halo-p-an2-link-ICN01
4) halo-p-an2-link-KOR
-----
Enter the number of the config you want to use, or press 'c' to cancel:
_
```

```
▼ TERRAFORM-TIDESQUARE-MODULES
> _backup
▼ modules
> aws
> halo
> tidesquare
> templates
> .gitignore
> README.md
```

```
▼ TERRAFORM-TIDESQUARE-INFRA
> _deprecated
> cell
> cell-cp
> cell-resource
> cell-resource-cp
> cell-toolchain
> cell-toolchain-target
> global-network
> global-network-dp-acm-only
> global-resource
> init
> pipeline-trigger
> region-network
> region-resource
> samples
> .gitignore
> bitbucket-pipelines.yml
> README.md
> temp.sh
> war
```

누구나 Infra를 생성할 수 있는 Pipeline



Terraform + Github action

add test variable #1

Merged xhoto merged 1 commit into `main` from `feature/add-test-variables` on Sep 6, 2023

Conversation **6** Commits **1** Checks **6** Files changed **1**



xhoto commented on Sep 6, 2023

Add test variable



add test variable

xhoto temporarily deployed to pr last year — with GitHub Actions Inactive

xhoto temporarily deployed to pr last year — with GitHub Actions Inactive



github-actions bot commented on Sep 6, 2023

Terraform Format and Style success

Terraform Initialization success

Terraform Plan success

Terraform Validation success

Terraform TfSec failure

Show Plan

Show TFSEC

Failed: 10 issue(s)


#	ID	Severity	Title	Location	Description
1	aws-ec2-no-public-egress-sgr	CRITICAL	An egress security group rule allows traffic to /0.	<code>terraform-aws-modules/eks/aws/home/runner/work/terraform-coupang-eks/terraform-coupang-eks/examples/simple/.terraform/modules/coupang-eks-simple.eks/node_groups.tf:223</code>	Security group rule allows egress to multiple public internet addresses.
2	aws-ec2-no-public-	CRITICAL	An egress security group	<code>git:https://github.com/terraform-aws-</code> <code>modules/terraform-aws-eks?</code>	Security group rule allows egress to

<https://github.com/poc-coupang/terraform-coupang-eks/pull/1>

Terraform + Github Issue = Self-service

Issue: Resource Request - s3

Resource Request - s3. If this doesn't look right, [choose a different type](#).

**Add a title**

[Resource Request - s3]:

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Bucket name

Bucket name must be unique within the global namespace and follow the bucket naming rules.

ex. mybucket

AWS Account (environment)

Which account should the created resource be deployed into?

✓ None

029033808317 (dev)

029033808318 (pr)

029033808319 (stg)

029033808320 (qa)

029033808321 (prd)

dumpfiles


Resource deployment agreement


By submitting this form, you agree to follow our [guide](#)

☐ I agree to follow this project's guide


Submit new issue

[Resource Request - s3]: aaaaa #10

 Open

 1 task

xhoto opened this issue on Sep 19 · 0 comments

**xhoto** commented on Sep 19

Bucket name

jaewoong

AWS Account (environment)



029033808317 (dev)


Purpose of resource

ex. s3 bucket for saving dumpfiles

Resource deployment agreement

☐ I agree to follow this project's guide

  **xhoto** added the **s3** label on Sep 19

  **xhoto** self-assigned this on Sep 19

<https://github.com/tving-proserve/issue-parser/issues/new/choose>



다시 보니 선녀 같다.

튜닝의 끝은 순정! CDK 짱!

감사합니다.