Platformising DevOps with the HashiCorp Stack

HashiCorp

SETU

About me

- I have been building stuff for the last 5 years.
- Currently DevOoopsing at Setu.
- I design and develop HA, Reliable and secure architectures on the cloud.
- Help teams develop and mature in the DevOps culture.
- Love participating in discussions on Distributed Systems.

yashshanker

yashshanker

@DevOoopsEngnr

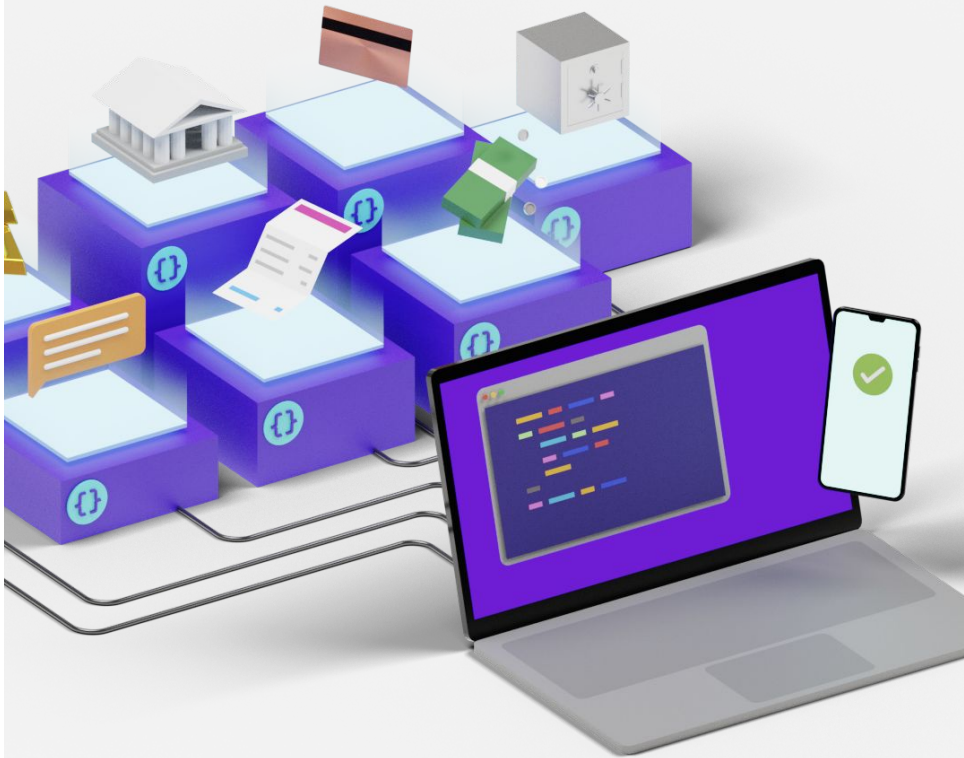
API banking infrastructure for India's financially-excluded millions

Our mission

We want to accelerate India's GDP growth by making digital financial services affordable and accessible to all.

Our vision

APIs for anything fintech—and that's the only way to scale.



Traditional DevOps Practice

- Having an army of “DevOps Engineers”
- Serve Operational Requests
    - Write configurations/scripts to generate deployable artifacts, like Dockerfiles and yaml files
    - Provision Infrastructure
    - Do production deployments
    - Resolve errors in CI/CD pipelines
    - Perform manual scaling of infrastructure
- Use a set of tools and platforms, to perform the above tasks.

DevOps at Setu : An Engineering Culture

- Tiny DevOps Team
- Distributed Ownership of Infrastructure
- Minimal overhead for Operations
- Release Self Serve Platforms
- Grow horizontally faster, building up on standardization
- Minimal involvement in Dev Teams' daily code operations, but available for support

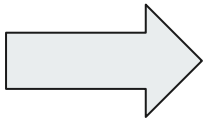
    - Infrastructure Provisioning
    - CI/CD Pipelines
    - Monitoring
    - Incidents
    - Deployments
    - Information Security

- Feedback Loops

The Short Story of DevOps at Setu

April 2020

- 1 Live Product.
- 3 micro services.
- A few thousand API requests per month.
- A few GBs of data processing per month.
- 1 team of total 5 Engineers.
- 1 DevOps Engineer.



June 2021

- 5 Live Products.
- Over 30 micro services.
- Tens of millions of API requests per month.
- Over 50 TBs of data processing per month.
- 7 teams of over 30 Engineers.
- 1 DevOps Engineer.

How we started with DevOps at Setu ?

- April 2020
  - 3 microservices deployed across, 1 Live Product, serving a few thousand requests a month
  - Deployed on AWS
  - Containerized Microservices Deployments orchestrated using Elastic Beanstalk
  - Infrastructure written in Terraform
  - AMIs built using Packer
  - Dev Teams responsible for Application Deployment
  - DevOps Team took care of Infrastructure changes, Deployments and Peripherals
  - Automated Deployments using scripts
  - 1 DevOps Engineer

How we started with DevOps at Setu ?

- May 2020
  - Launching the second product
    - Write new Infrastructure and deployment scripts, from scratch

- June 2020
  - Plans to launch 5 more products rapidly
  - The Engineering Team faced multiple challenges with the way we went about Releases

How we started with DevOps at Setu ?

Rebooting

- Problems
  - Deployments involved downtimes.
  - Change Management and Patches were challenging
  - Lack of Standardization
  - Writing new infrastructure for every product was boring and time taking.
  - Multiple Regulatory and Compliance Audits
    - API Security Testing
    - Full Infrastructure VAPT
  - Decentralised flow of Architectural Decisions were challenging to standardise
  - Missing components.

How we started with DevOps at Setu ?

Birth of the DevOps Platform

- Standardised DevOps platform to be used across Setu
    - Self Serve Low Code Infrastructure as Code in Terraform
    - Feature packed Packer based AMIs
    - Canary Deployments facilitated with CD
    - Centralised extensive Observability
    - Information Security Compliance

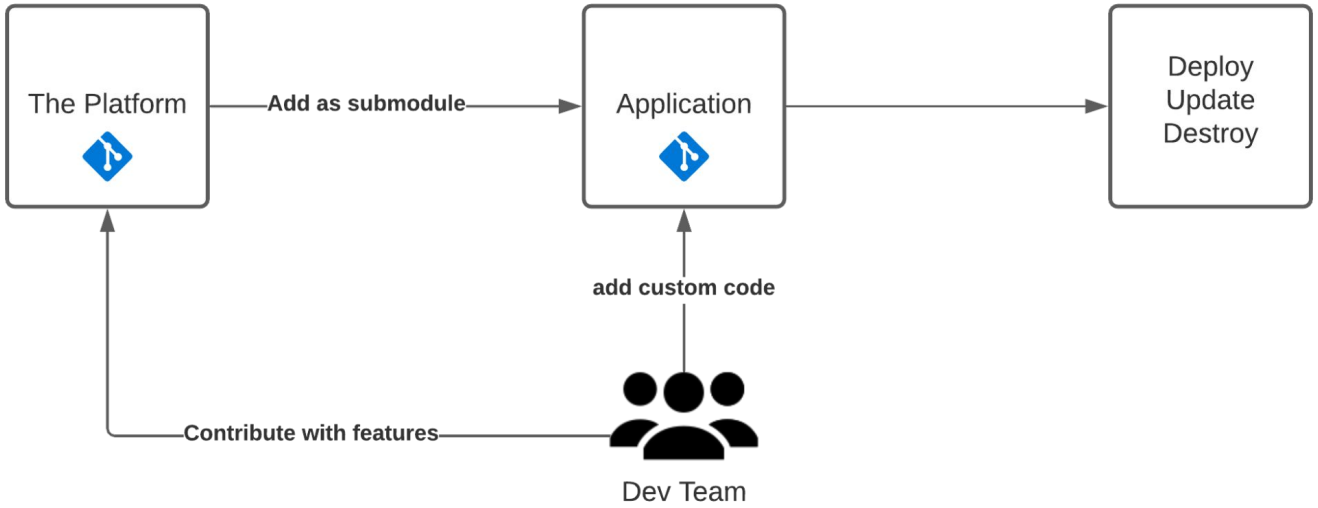
The Infrastructure Platform

- Self Serve Low Code Infrastructure as Code using Terraform
    - Includes AWS Services :
        - VPC, ASG, ALB, NLB, ECS, RDS, DynamoDB, EC2, Lambda, API GateWay, WAF, CloudFront, EFS, Site-Site VPN, SQS, AMQ(RabbitMQ and ActiveMQ), S3, Elasticache (Redis), CloudWatch, IAM, Athena, Glue, ElasticSearch, etc
    - Built in Alerting on PagerDuty and Slack, well, anything which has a webhook.
    - Grafana Dashboards for visualizations across Data Sources
    - Adheres to the AWS Well Architected Framework
    - Certified ISO 27001:2017 compliant
    - Cloud Security Alliance - Start Level One certified
    - Compliant with all of RBI and NPCI regulatory InfoSec Compliances and Guidelines, including RBI SAR

The Infrastructure Platform

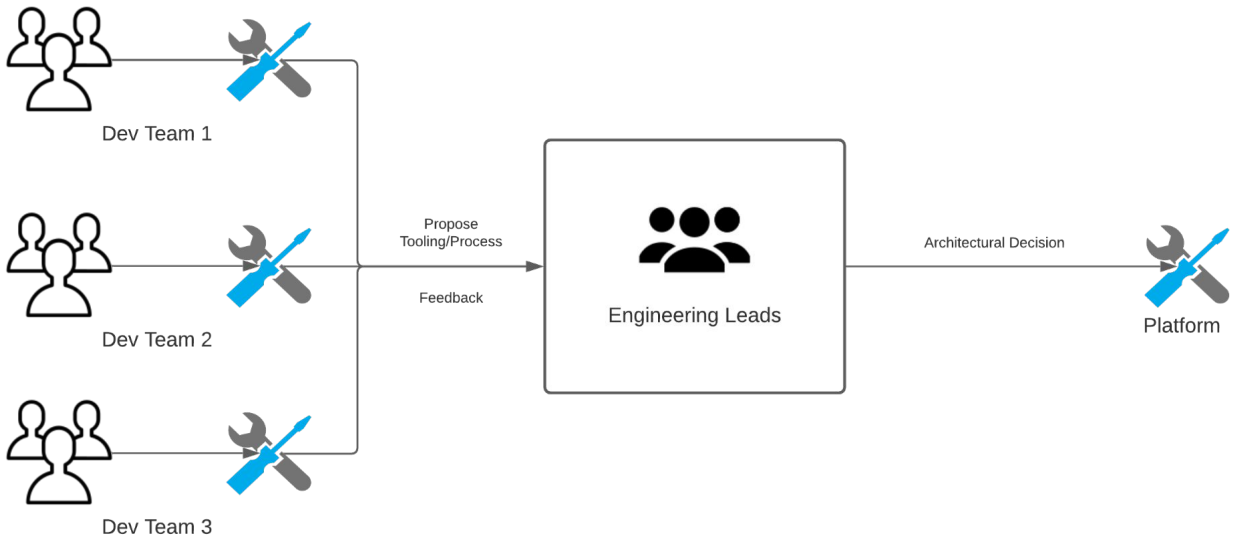
- Automated Hardened AMIs provisioning and updates using Packer
    - Includes
        - Docker setup along with secure networking.
        - Setup of ecs-init service (ecs-agent and ecs-pause containers) to enable running ECS tasks.
        - Host IDS - Ossec.
        - FIM - OSQuery
        - Network IDS and IPS - Snort.
        - MetricBeat, Filebeat and elastic-logging-plugin for docker.
        - SSH Hardening.
        - Antivirus with automated virus definition updates.

How Dev Teams use the Platform ?



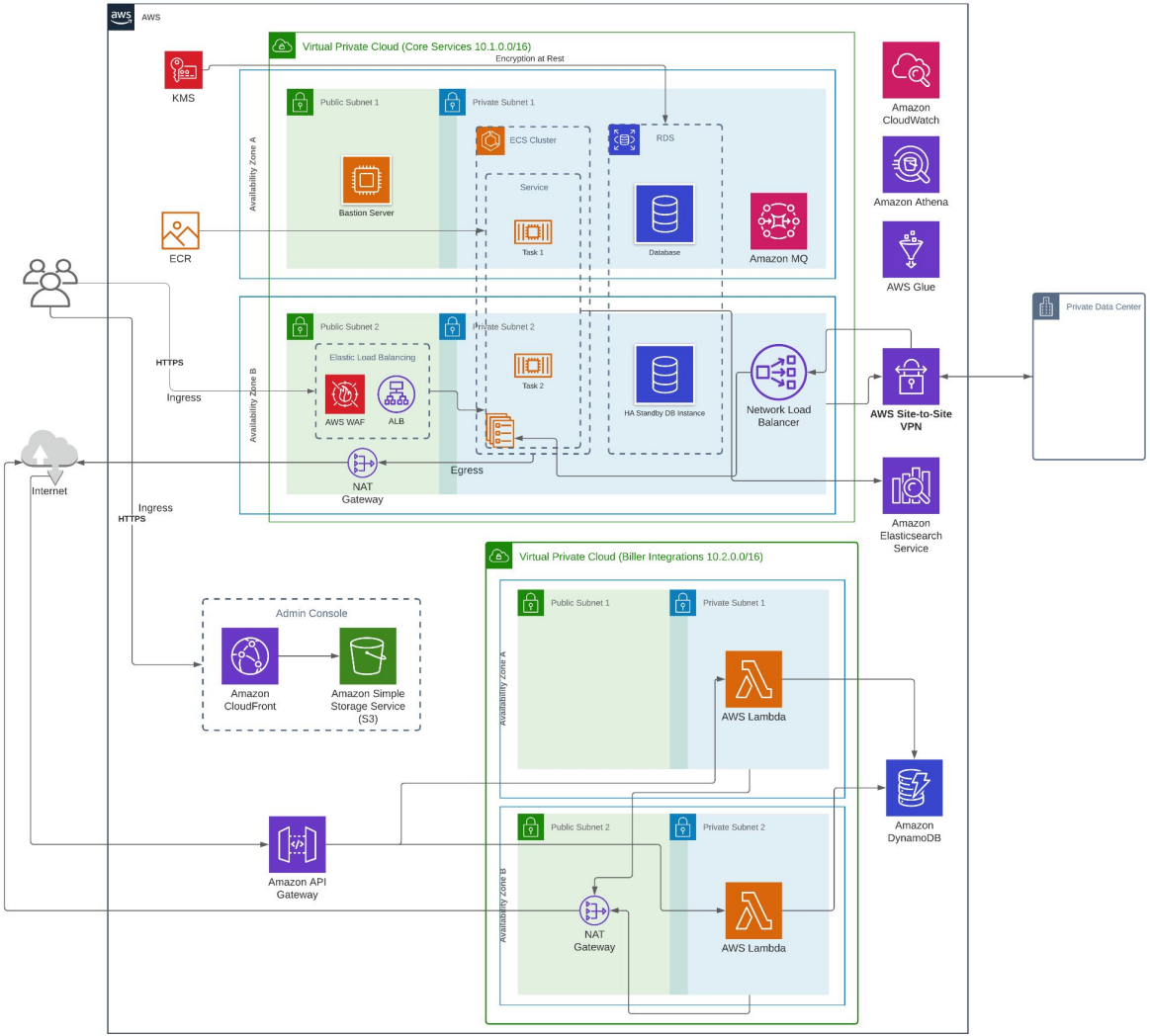

WELL-UNDERSTOOD,
PROPERLY-APPLIED
AND GOAL-ENABLING DEVOPS
BUT IS IT "DEV*SEC*OPS"?
imgflip.com

How Architectural Decisions reach DevOps ?



How about now ?

- June 2021
  - The infrastructure is now used across 7 Development Teams across 5 live Products
    - serves tens of millions of API requests
    - processes over 50 TB of data per month
    - comprising over 30 microservices
  - Containerized Microservices Deployments orchestrated using AWS EC2 Container Service
  - Infrastructure written in Terraform
  - AMIs built using Packer
  - Dev Teams responsible for Application Deployment
  - Have to undergo at least 20 InfoSec and Compliance Audits in a year
  - 1 DevOps Engineer and 1 Platform Engineer


AWS
Virtual Private Cloud (Core Services 10.1.0.0/16)
Encryption at Rest
KMS
Amazon CloudWatch
Public Subnet 1
Private Subnet 1
ECS Cluster
RDS
Availability Zone A
Bastion Server
Service
Amazon Athena
ECR
Task 1
Database
Amazon MQ
AWS Glue
Private Data Center
Public Subnet 2
Private Subnet 2
Elastic Load Balancing
HTTPS
Ingress
Availability Zone B
Task 2
AWS WAF
ALB
HA Standby DB Instance
Network Load Balancer
AWS Site-to-Site VPN
Internet
Egress
NAT Gateway
Amazon Elasticsearch Service
Ingress
HTTPS
Virtual Private Cloud (Biller Integrations 10.2.0.0/16)
Admin Console
Public Subnet 1
Private Subnet 1
Availability Zone A
Amazon CloudFront
Amazon Simple Storage Service (S3)
AWS Lambda
Amazon DynamoDB
Public Subnet 2
Private Subnet 2
Amazon API Gateway
Availability Zone B
NAT Gateway
AWS Lambda

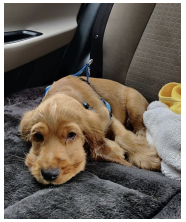
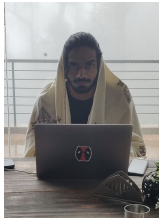
Benefits

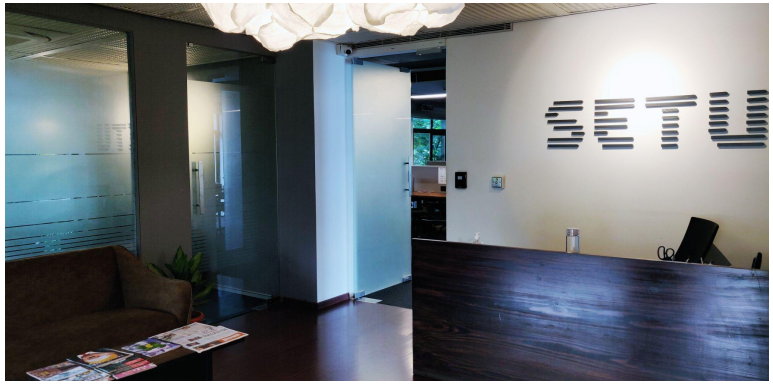
- Standardization of platform and processes across Organization.
- Provisions entire Production Infrastructure without writing a single LOC in just 20 minutes.
- InfoSec Audits take 1-3 days.
- Ownership with Dev Teams.
- Faster iterations and more reliable releases, with lesser risks per release.
- Automated Canary Deployments based on CD.

Future of the Platform

- Extending the platform around Kubernetes.
- Making the platform Cloud agnostic and support bare metal.
- Open Source ? Too insecure to release right now without cleaning up.

Let’s build something incredible together






Apply by API!
Do a GET call at
https://join.setu.co/apply

setu.co/careers
hello@setu.co

Questions