Elasticsearch7.x cluster in Azure
Terraform infrastructure as code challenge
(with the Free Tier twist)

Apr 20, 2020

Marek Fengler

https://github.com/mf2012/es7-azure

About me

- IT Linux professional since 2000
- AWS, Openstack, DevOps, Automation, Azure
- 13 years operational experience (24/7 environments)
- Lifelong learner
- Musician

Challenge 1

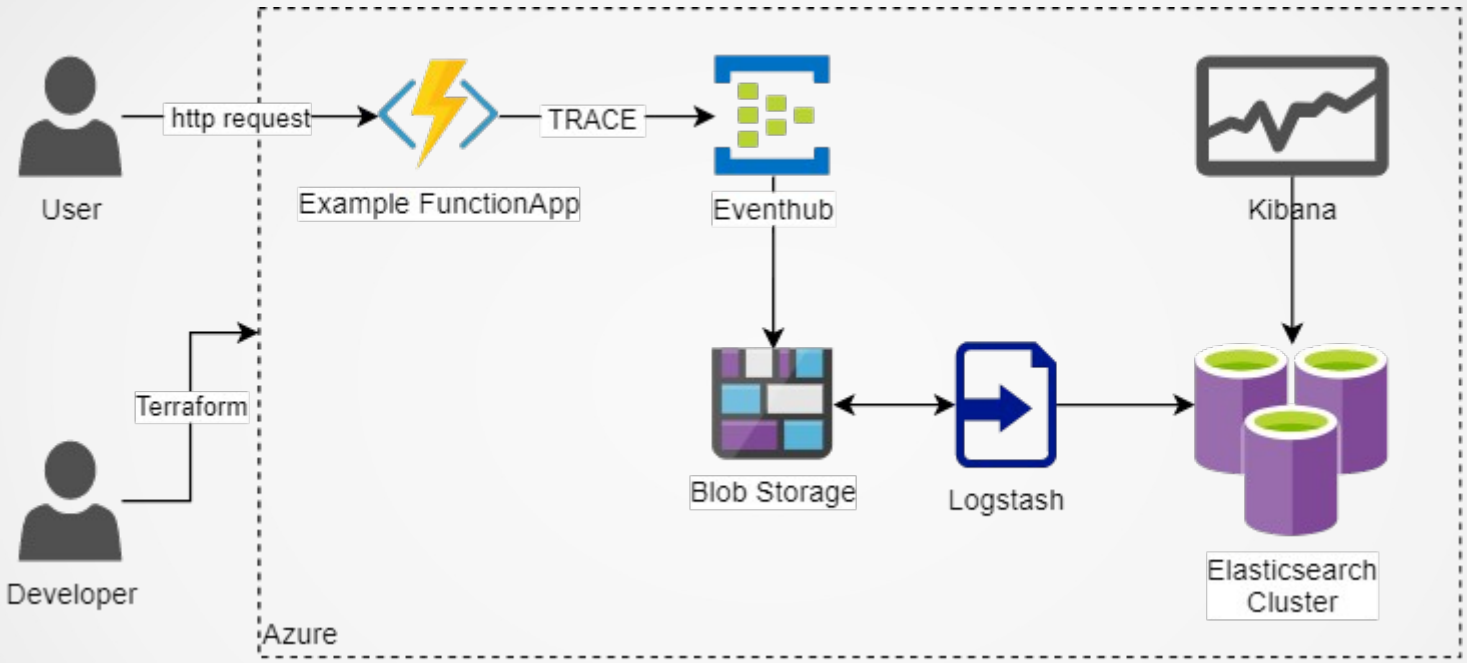
- Stand up an Elasticsearch
- Stand up Azure Event Hubs
- Single Azure Function sending stack traces into Elasticsearch every time it is invoked
- Test scripts for all services which can be intergrated in CI/CD
- Terraform with azurerm_provider
- Time limit 18h
- Azure Free Tier subscription*

  * - Tier is chosen to see what the limitations are

Possible Solutions

- Production ready multi-node ES cluster (3xmaster, 2xdata, 2x client) + Eventhub + FunctionApp
- Production ready multi-node ES cluster on K8s with Helm Charts + Eventhub + FunctionApp
- Minimal ES cluster on 3x nodes + Eventhub + FunctionApp

What is the solution?



Limitation only allow solution with simple 3 node cluster

What we've learned in 18h?

- How to use Terraform with Azure (we like it!)
- Bootstrap Elasticsearch cluster on 3 x Standard_D1 nodes, Logstash, Kibana (ELK)
- Azure's Eventhub, Analytics
- Write an Azure FunctionApp and monitor it
- Flow of events in Azure cloud
- Wisdom of Azure's Free Tier limitations – great for PoC and prototyping, not so great for production workloads
- 80% done, still 20% remaining

Way forward

- Finish the tests
- Confirm the data pipeline actually is working
- Use paid tier for production workloads in Azure

Code:

- https://github.com/mf2012/es7-azure