Security on Azure Kubernetes Services with open-source tools

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

About Me

2019 Global Azure BOOTCAMP

NASH TECH
The Power to Innovate

Microsoft

Lai Trung Minh Duc

- Data Scientist @ Unilever Vietnam
- Solution Architect @ Savills Vietnam
- Full-stack Developer @ Pizitech
- Tech Trainer @ Microsoft Student Partners

ASP.NET Core 2+ | Microsoft Azure |

Azure DevOps | Docker | Kubernetes |

Power BI | Excel | MS SQL | Python

Story

- Tèo is a system engineer want to test Kubernetes on Azure
- After 3 days using AKS, he realized that his MySQL database was overload, and bad inserted inside the database.
- He said… “I need to find a way to know what happened on my system. Then protect it with… my small budget”.

Agenda

Duration	Content
5 min	Overview Azure security solutions for Azure Kubernetes Services
25 min	Open-source Web Application Firewall | Layer-7 Load Balancer | HTTPS • Kubernetes NGINX Ingress Controller. • cert-manager: SSL certificate manager on Kubernetes • Demo: Deploy NGINX Ingress Controller and cert-manager • Write YAML config files to activate WAF | L7 LB | HTTPS • Security Test
5 min	Log Management for Azure Kubernetes Services
5 min	Attack alerting to Slack with Azure Logic App

Scope of this presentation

- Azure AKS = managed Kubernetes service by Azure
- Protect AKS cluster from outside – at application layer (L7).

- ~~Identity protection (Azure AD)~~
- ~~Secured networking inside AKS cluster~~
- ~~Backup | Disaster Recovery for AKS cluster~~

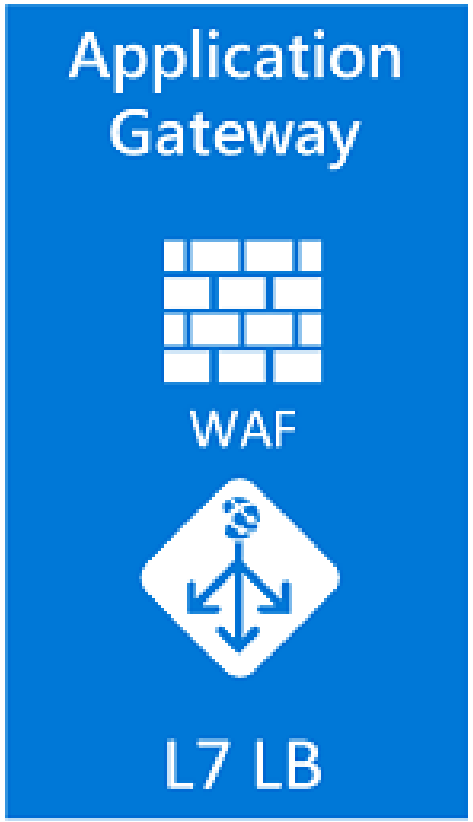
Overview Azure security solutions for Azure Kubernetes Services

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

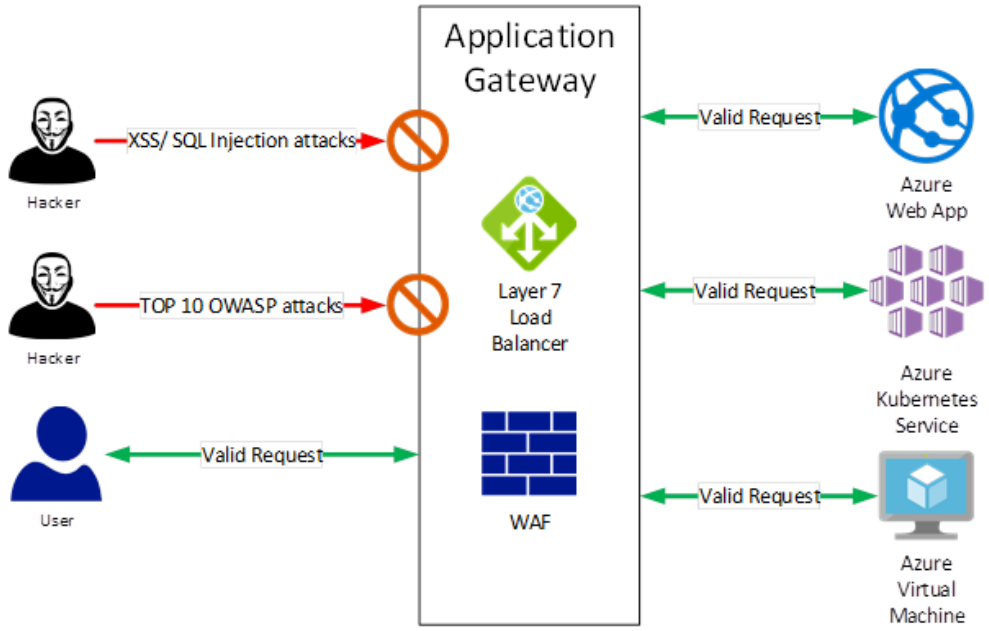
Overview Azure security solutions

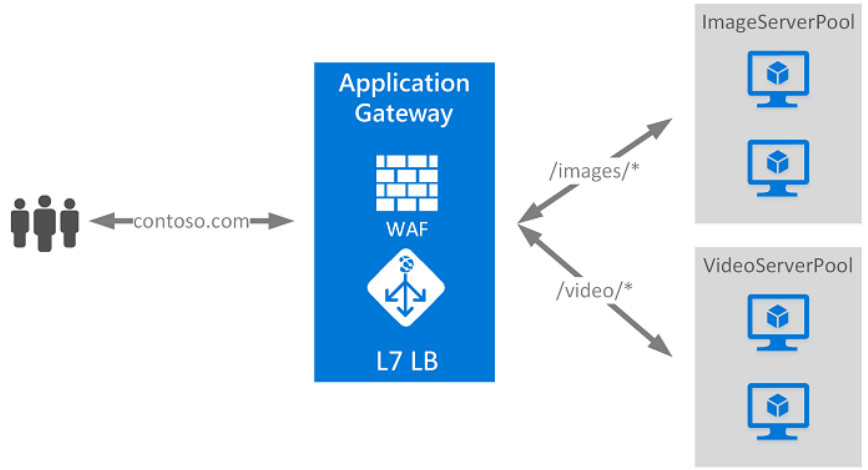
- Azure Application Gateway
- Azure Log Analytics
- Azure Monitor



Azure Application Gateway

- Web Application Firewall:
  - Block malicious traffic
- Layer-7 Load Balancer
  - Route traffic based on URL
- Friendly management dashboard.

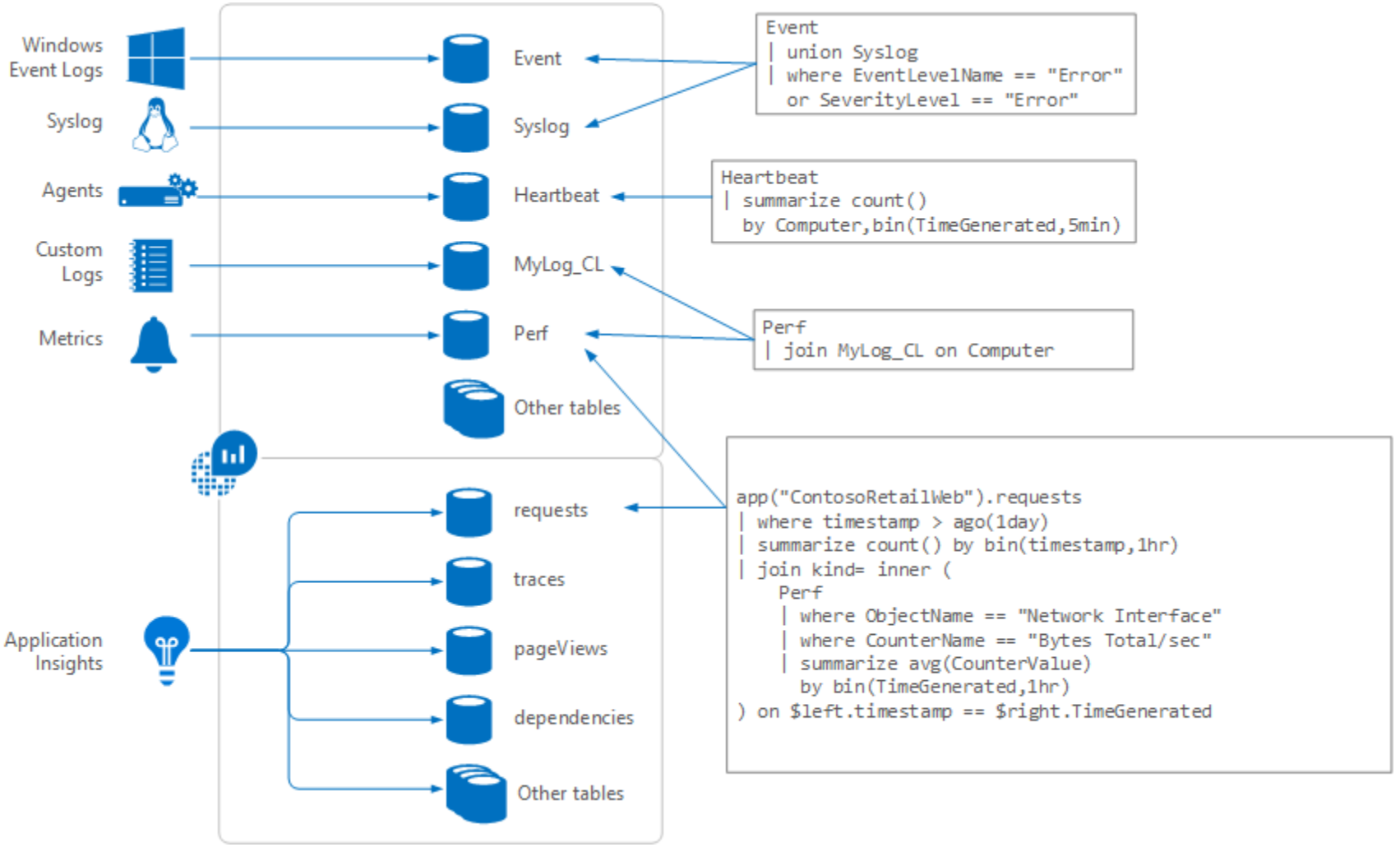




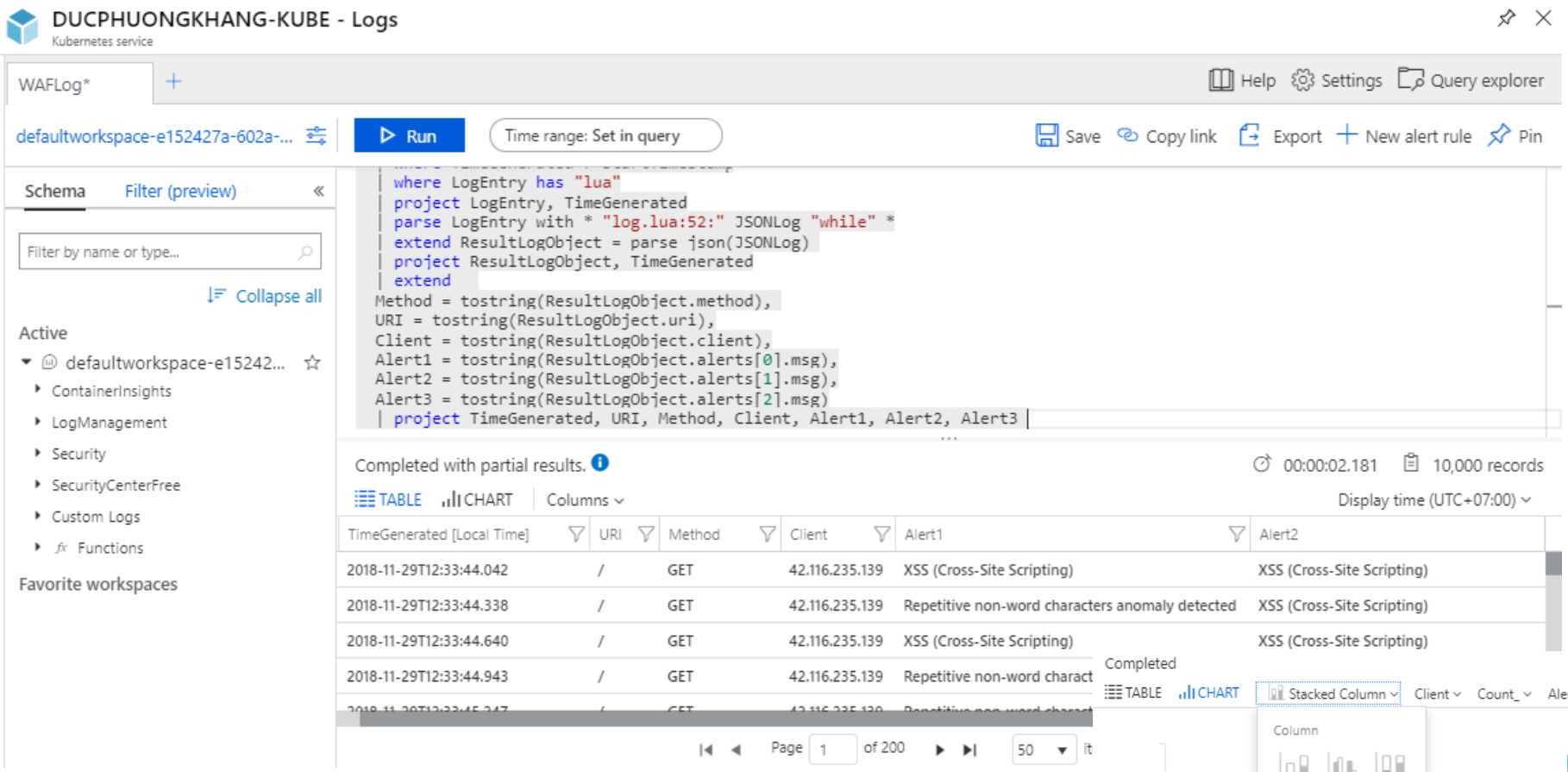
Azure Log Analytics

- Log storage
- Log digestion
- Log visualization
- Log retention

Using Kusto query language

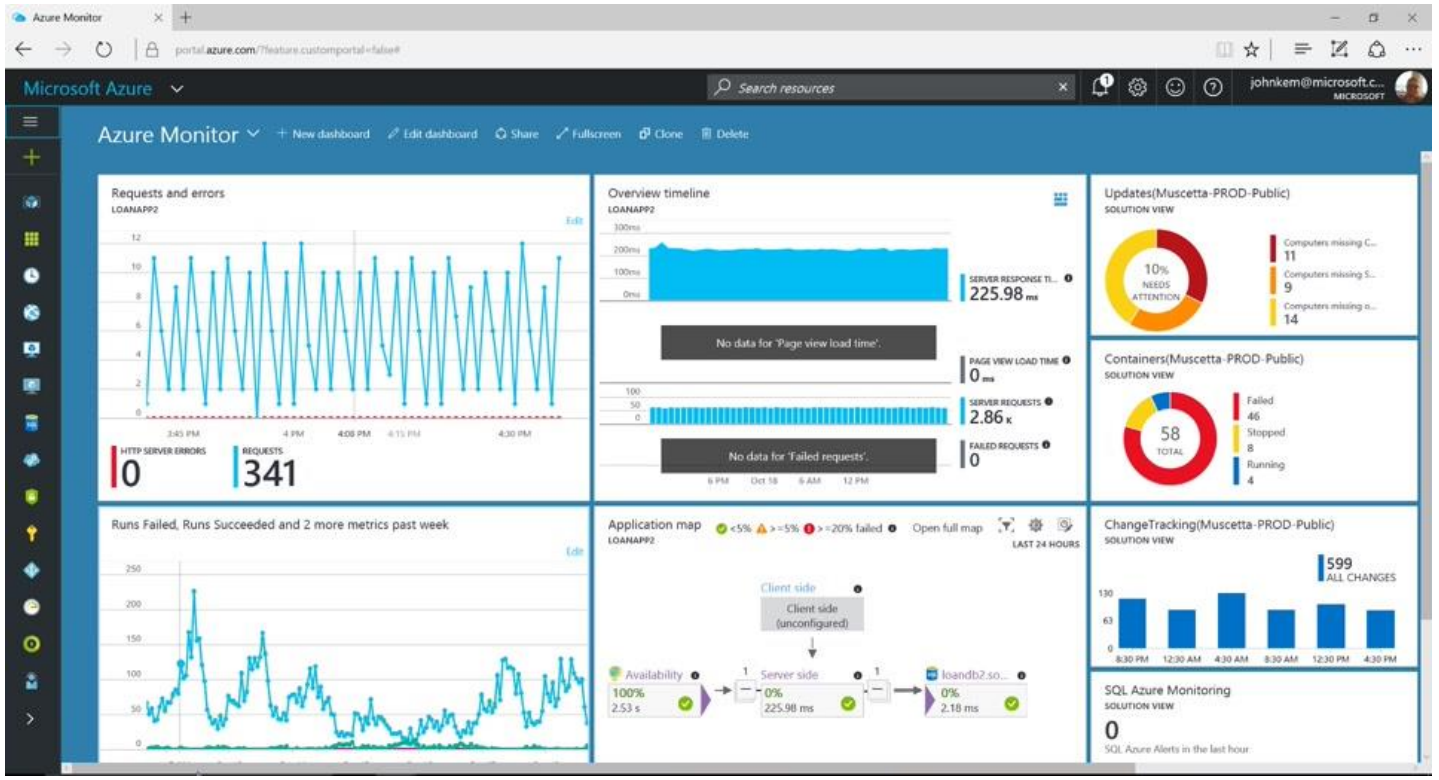


Azure Log Analytics



Azure Monitor

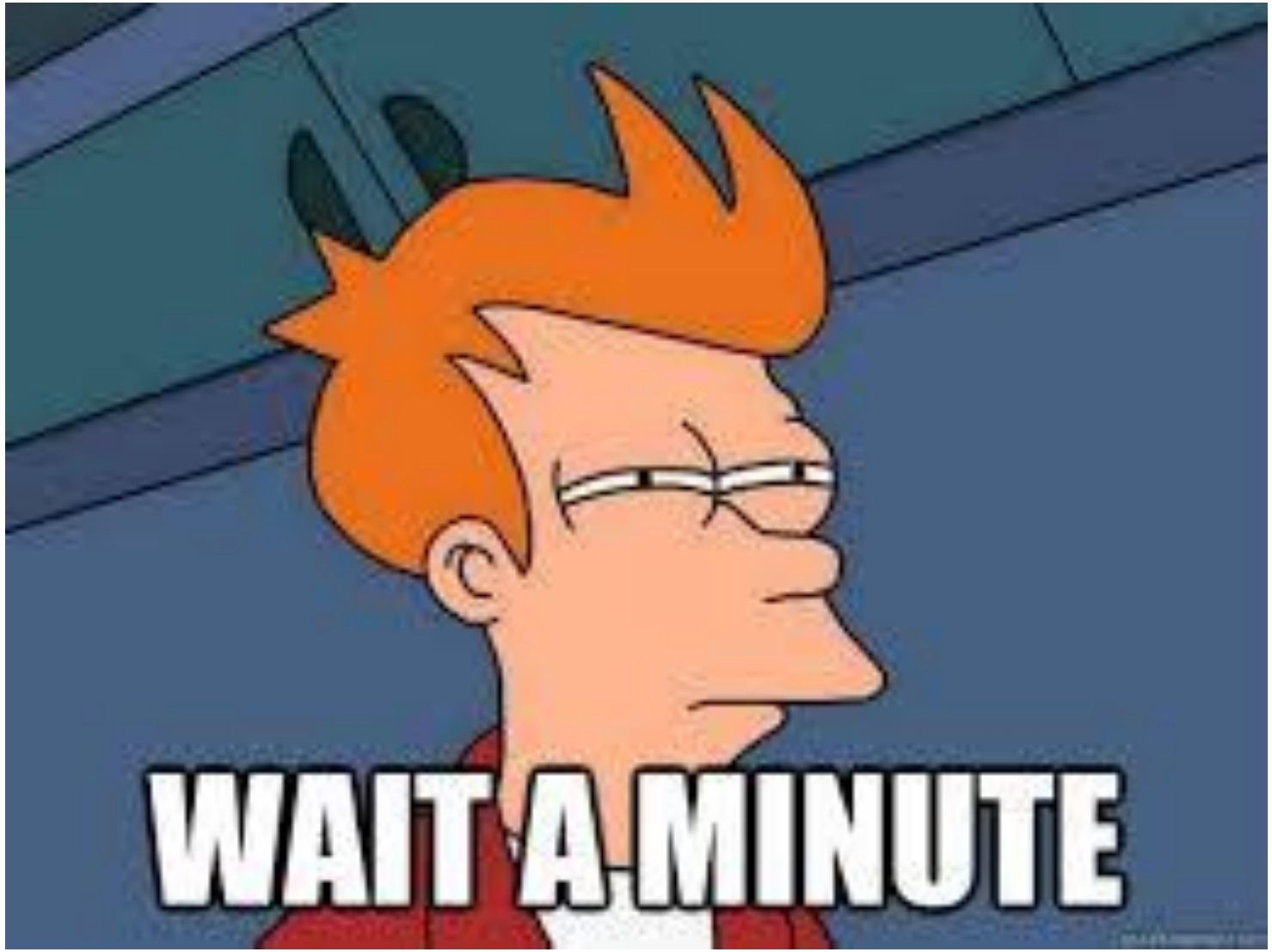
- Log Analytics is a part of Azure Monitor
- Support on monitoring CPU, network, virtual machines,…
- Support alert with rules via email, webhook,…



2019 Global Azure BOOTCAMP

NASH TECH
The Power to Innovate

Microsoft



Monthly Cost

Azure Application Gateway	Azure Log Analytics	Azure Monitor
Microsoft: from **$103.018**	Free: 5GB	Standard metrics: FREE
Others (F5, Barracuda): BYOL	Ingestion: **$2.99**/GB	Alert from log: from **$0.5**
	Retention: $0.13/GB	Notification from alert: **$2**

https://azure.microsoft.com/en-us/pricing/details/monitor/

https://azure.microsoft.com/en-us/pricing/details/application-gateway/

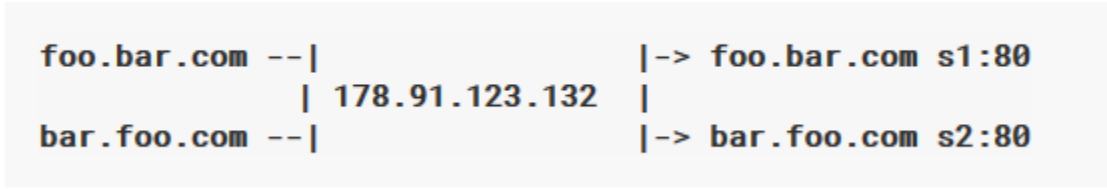
Opensource WAF | L7 LB | HTTPS: Kubernetes NGINX Ingress controller

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

What is Ingress?

- Ingress, added in Kubernetes v1.1, **exposes HTTP and HTTPS routes from outside the cluster to services within the cluster.** Traffic routing is controlled by rules defined on the Ingress resource.
- An Ingress can be configured to **give services externally-reachable URLs, load balance traffic, terminate SSL,** and offer name based virtual hosting
- An Ingress **does not expose arbitrary ports or protocols.** Exposing services other than HTTP and HTTPS to the internet typically uses a service of type Service.Type=NodePort or Service.Type=LoadBalancer



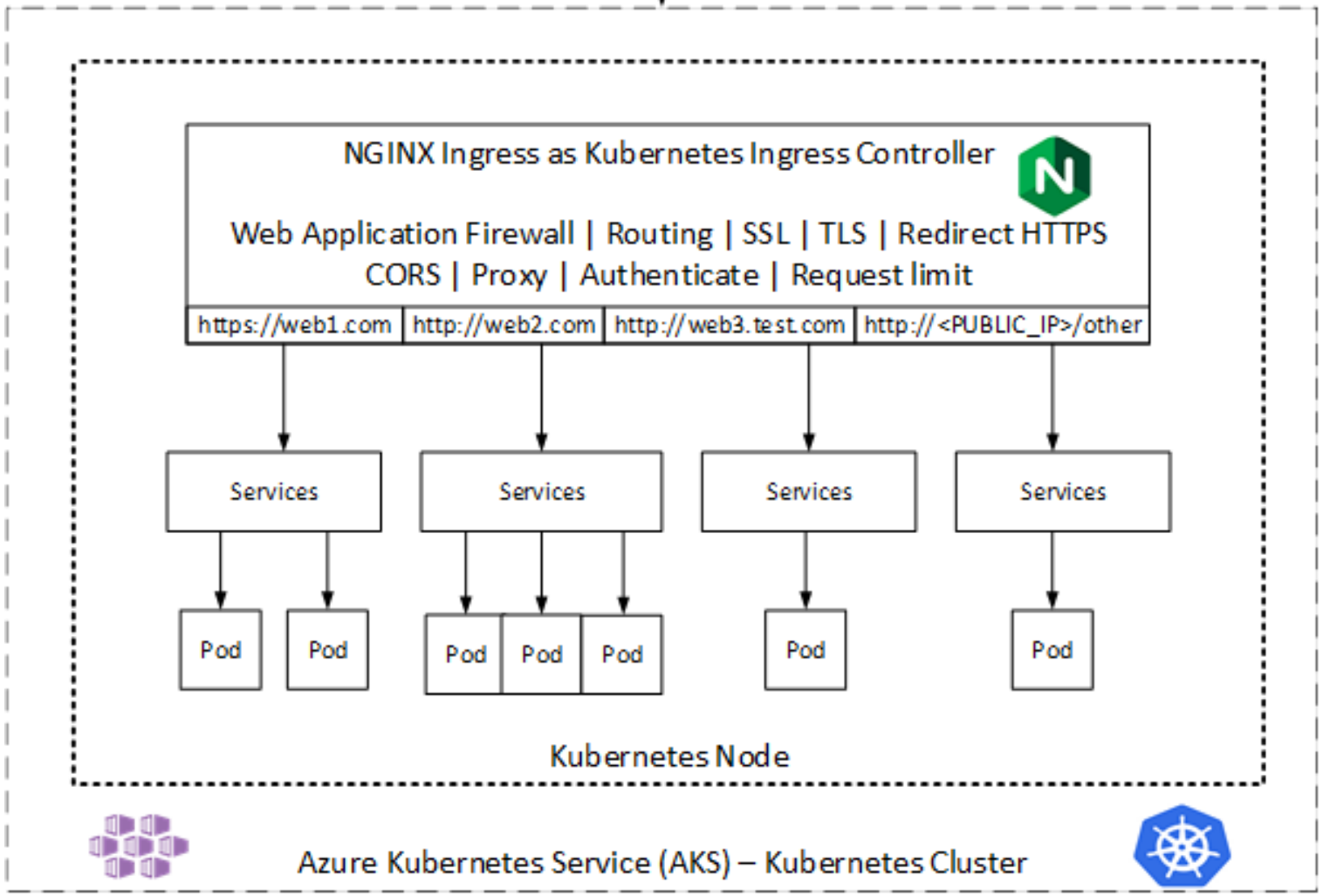

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: name-virtual-host-ingress
spec:
  rules:
  - host: foo.bar.com
    http:
      paths:
      - backend:
          serviceName: service1
          servicePort: 80
  - host: bar.foo.com
    http:
      paths:
      - backend:
          serviceName: service2
          servicePort: 80
```

Ingress Controller

Implementation:

- NGINX Ingress
- HAProxy
- Istio
- Traefik

https://kubernetes.io/docs/concepts/services-networking/ingress-controllers/



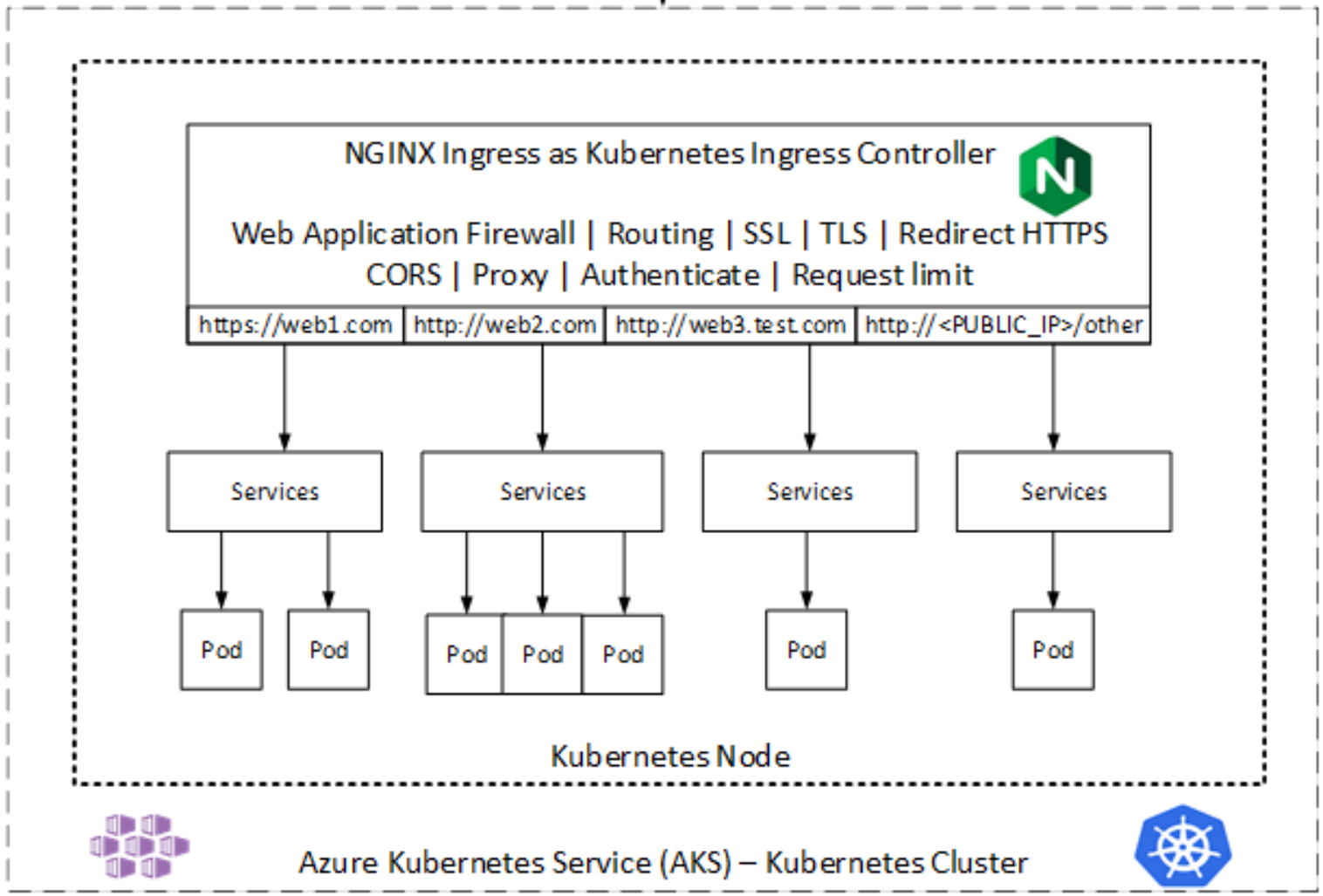
NGINX Ingress Controller

- Opensource project maintained by Kubernetes community based on NGINX Product. Integrate with *Resty WAF (ModSecurity)*.

  https://github.com/kubernetes/ingress-nginx

- Different from NGINX product:

  https://github.com/nginxinc/kubernetes-ingress/blob/master/docs/nginx-ingress-controllers.md



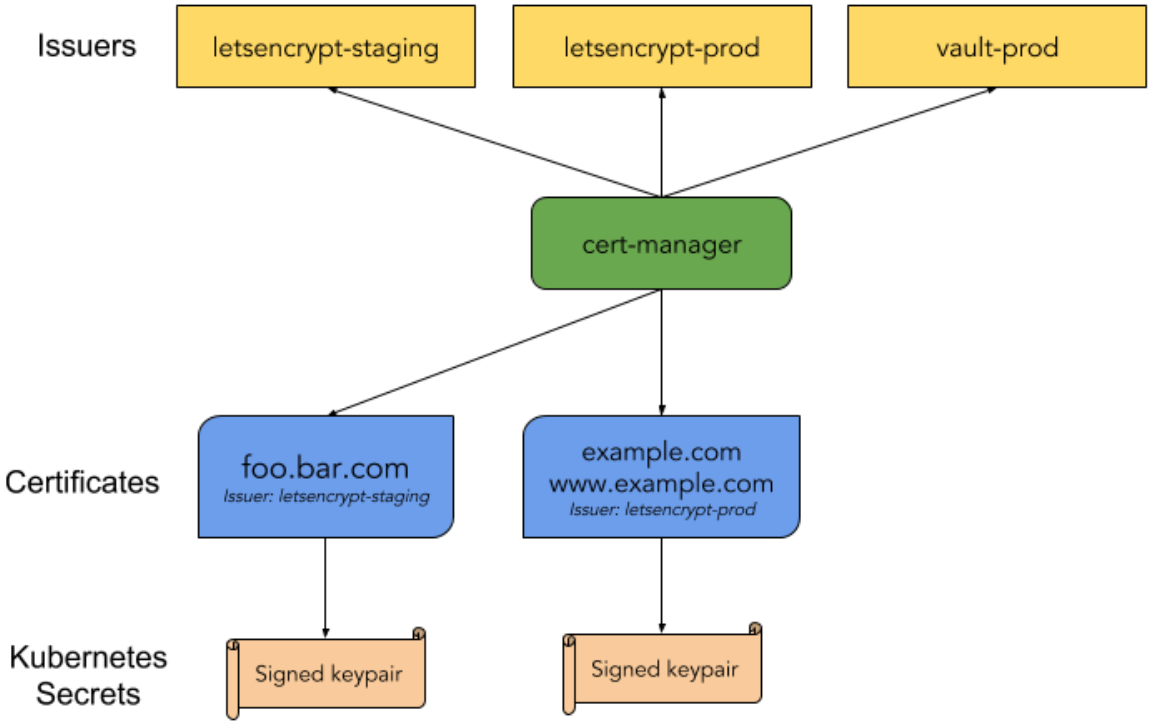
Opensource WAF | L7 LB | HTTPS: cert-manager: SSL certificate manager on Kubernetes

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

cert-manager

- cert-manager is a Kubernetes **add-on to automate the management and issuance of TLS certificates** from various issuing sources.
- It will ensure **certificates are valid and up to date** periodically, and **attempt to renew certificates** at an appropriate time **before expiry**.



https://github.com/jetstack/cert-manager

Opensource WAF | L7 LB | HTTPS: Deploy NGINX Ingress Controller and cert-manager

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Instruction steps

NGINX Ingress Controller

- Install HELM
- Install NGINX Ingress controller by using HELM
- Assign IP of Ingress to AKS DNS
- Config Ingress controller to record external IP to log file.

cert-manager

- Install cert-manager by using HELM.
- Config SSL Issuer (YAML)
- Config domain name for SSL certificate (YAML)

DEMO

Deploy NGINX Ingress Controller and Cert Manager

Opensource WAF | L7 LB | HTTPS: Write YAML files to activate WAF | L7 LB | HTTPS

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Ingress YAML Annotations

2019 Global Azure BOOTCAMP

NASH TECH The Power to Innovate

Microsoft

- Resty WAF
- Force SSL
- SSL Issuer

https://github.com/kubernetes/ingress-nginx/blob/master/docs/user-guide/nginx-configuration/annotations.md

```yaml
annotations:
  kubernetes.io/ingress.class: nginx
  certmanager.k8s.io/cluster-issuer: letsencrypt-prod
  nginx.ingress.kubernetes.io/ssl-redirect: "true" # Force redirect HTTPS
  nginx.ingress.kubernetes.io/rewrite-target: /
  nginx.ingress.kubernetes.io/lua-resty-waf: "active" # Turn on WAF
  nginx.ingress.kubernetes.io/lua-resty-waf-score-threshold: "10"
```

Ingress YAML Specs

- SSL Domain and Secret
- Mapping domain to service

```yaml
spec:
  tls:
  - hosts: # Replace your domains in here
    - shop.thesis.analyticsvn.com
    secretName: tls-secret
  rules:
  - host: shop.thesis.analyticsvn.com # Replace your domain in here
    http:
      paths:
      - path: /
        backend:
          serviceName: dpk-shop # Replace your service name
          servicePort: 80 # Replace your service port
```

2019 Global Azure BOOTCAMP

NASH TECH
The Power to Innovate

Microsoft

DEMO

Write Ingress config to activate WAF | HTTPS | L7 LB

Pen-test

Log Management on Azure Kubernetes Service

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Log Management solution

Open source tools

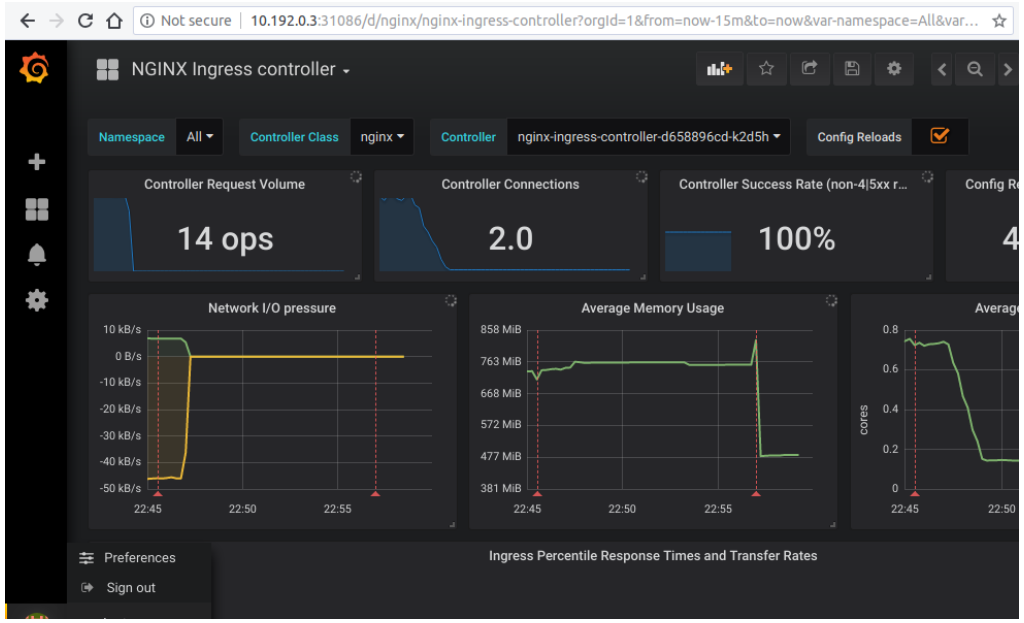
- kubectl logs
- ELK (Elasticsearch, Logstash, Kibana) Stack
- Prometheus + Grafana
- InfluxDB with NGINX Ingress plugin

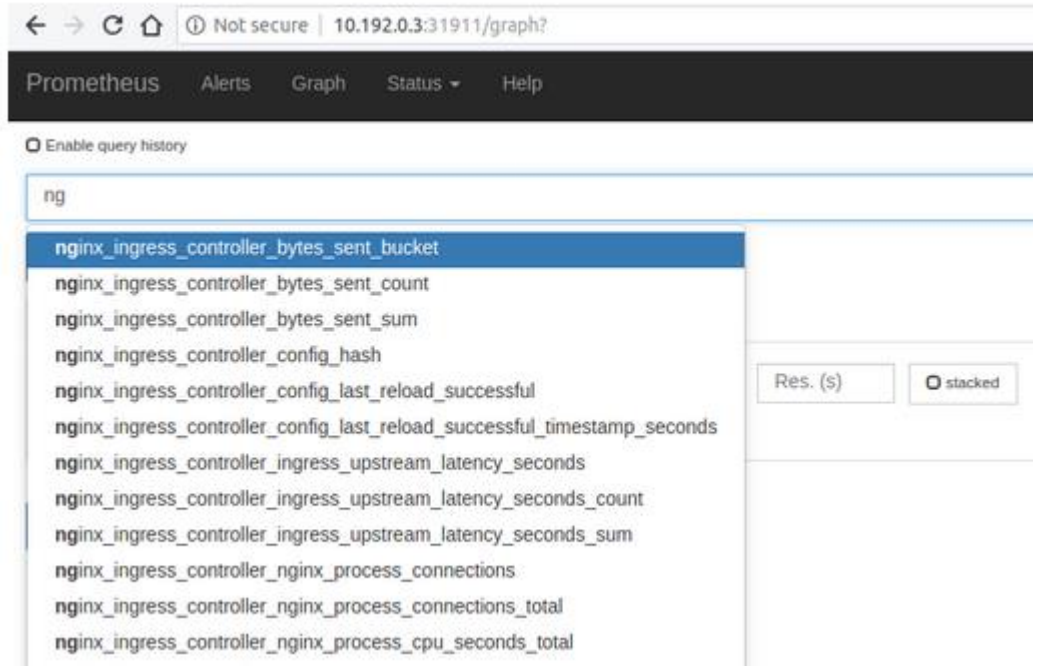
Microsoft Azure services

- Azure Log Analytics from Azure Monitor workspace. (Log collect status: ON – by default)

Prometheus + Grafana

- Official supported by NGINX Ingress controller
- Follow tutorial at: https://kubernetes.github.io/ingress-nginx/user-guide/monitoring/





DEMO

Prometheus + Grafana (UI only | not included installed steps)

Azure Log Analytics (query)

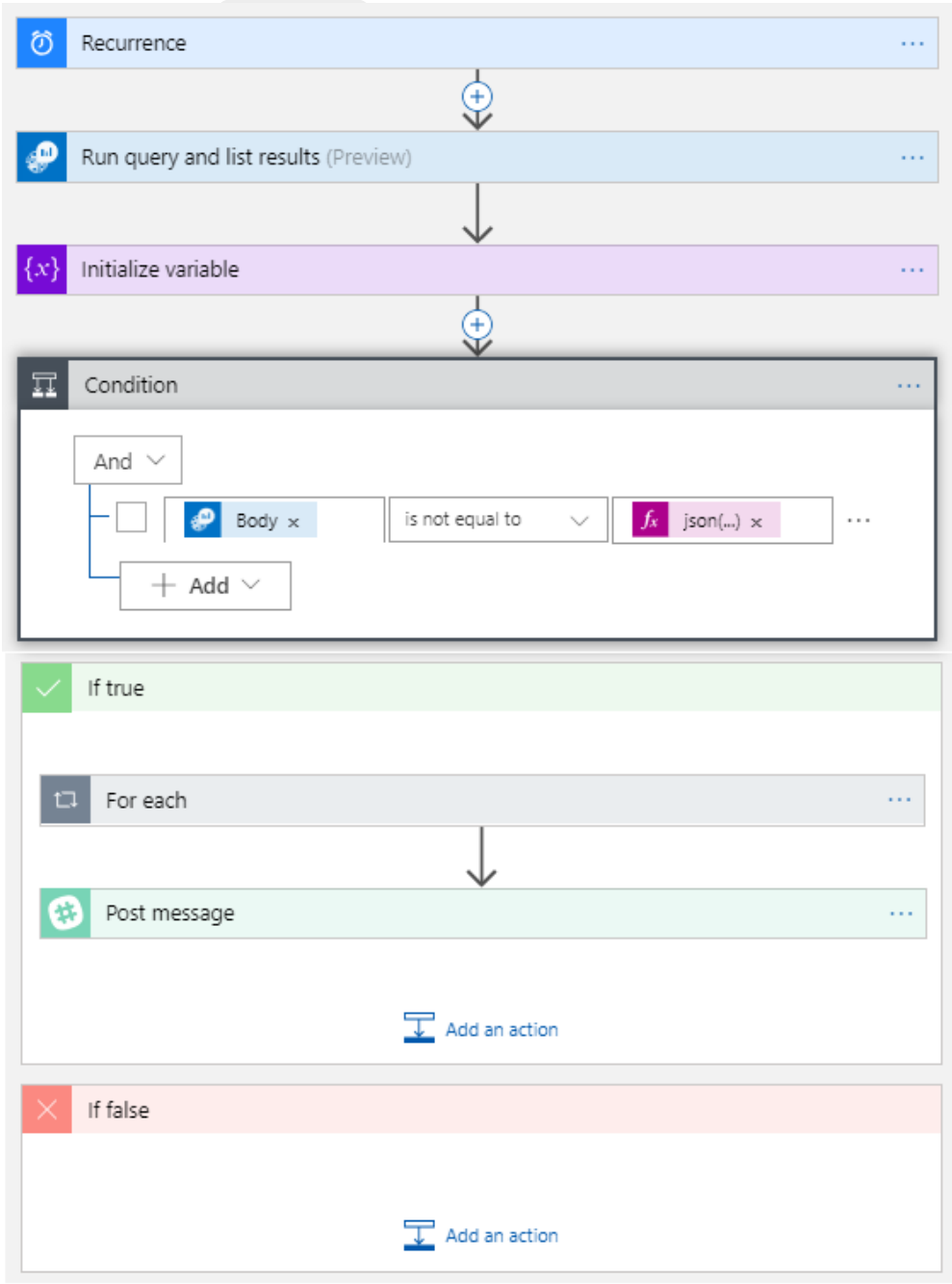
Alert to Slack with Azure Logic App

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Azure Logic App + Slack

- Azure Logic App: platform for workflow and automation tasks with less-code approach.
- Slack: communication channel
- Logic App scan log in Log Analytics → Alert to Slack if detect attacks.



2019 Global Azure BOOTCAMP

NASH TECH
The Power to Innovate

Microsoft

DEMO

Azure Logic App and Slack for Attack Alert

(result demo only)

THANK YOU

Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Reference

- Deploy-code Github:
- … (will filled in later) …