



NGINX



Security on Azure Kubernetes Services with open-source tools



Sat, Apr-27 @ NashTech

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

DucLTM@outlook.com

About Me

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	<p>Open-source Web Application Firewall Layer-7 Load Balancer HTTPS</p> <ul style="list-style-type: none">• 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



Sat, Apr-27 @ NashTech

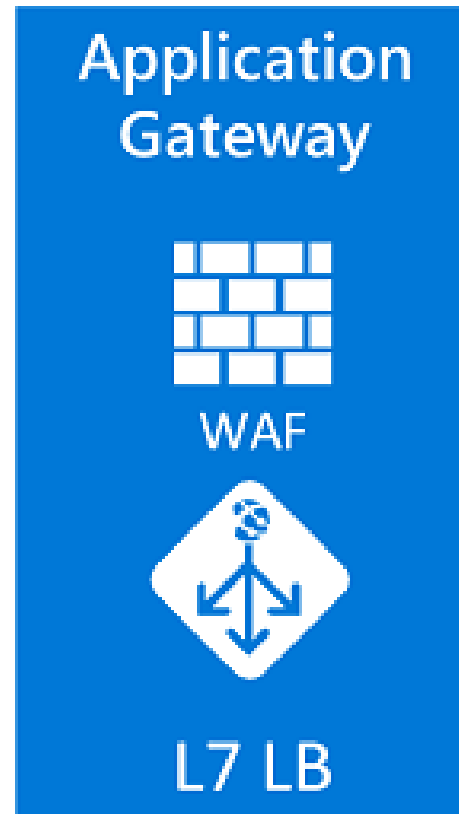
Lai Trung Minh Duc | Supply Chain Data Scientist, Unilever Vietnam

DucLTM@outlook.com

Overview Azure security solutions

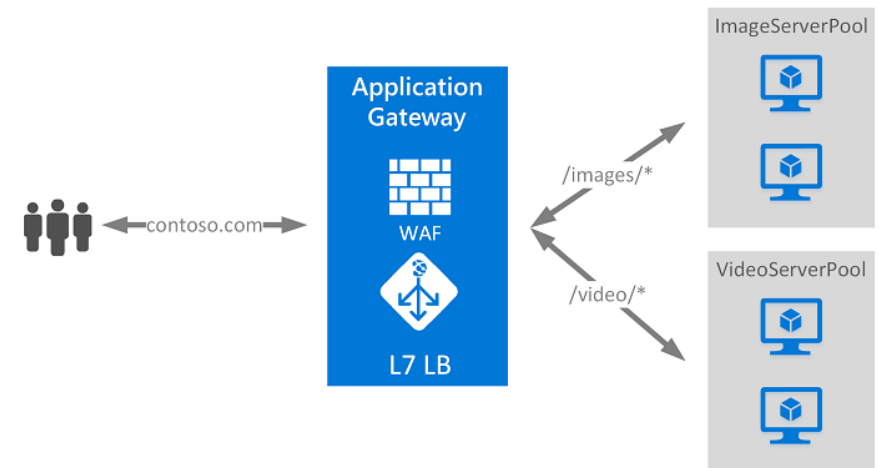
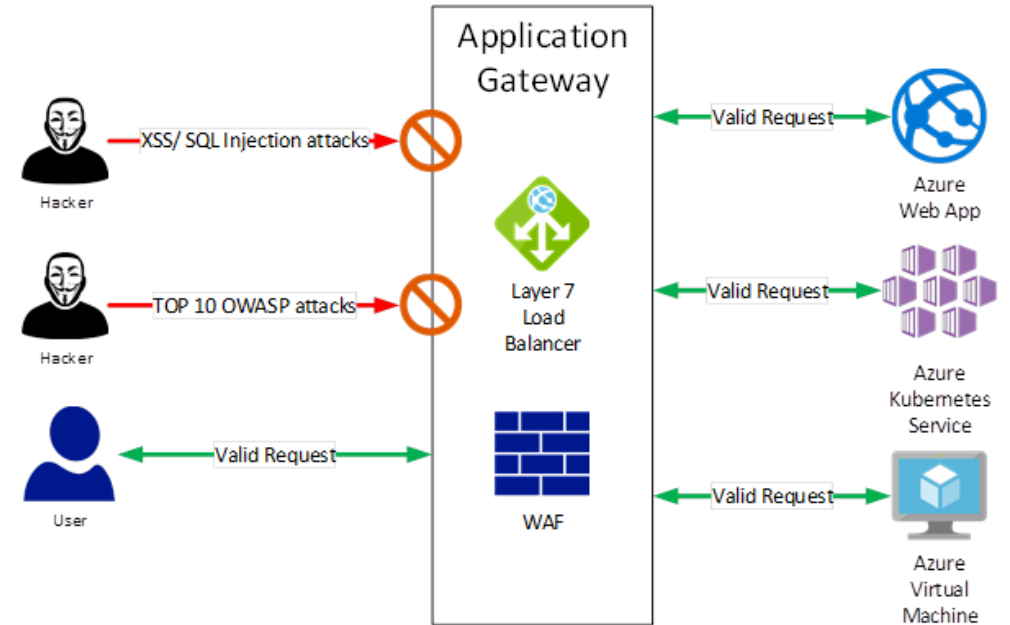


- Azure Application Gateway
- Azure Log Analytics
- Azure Monitor



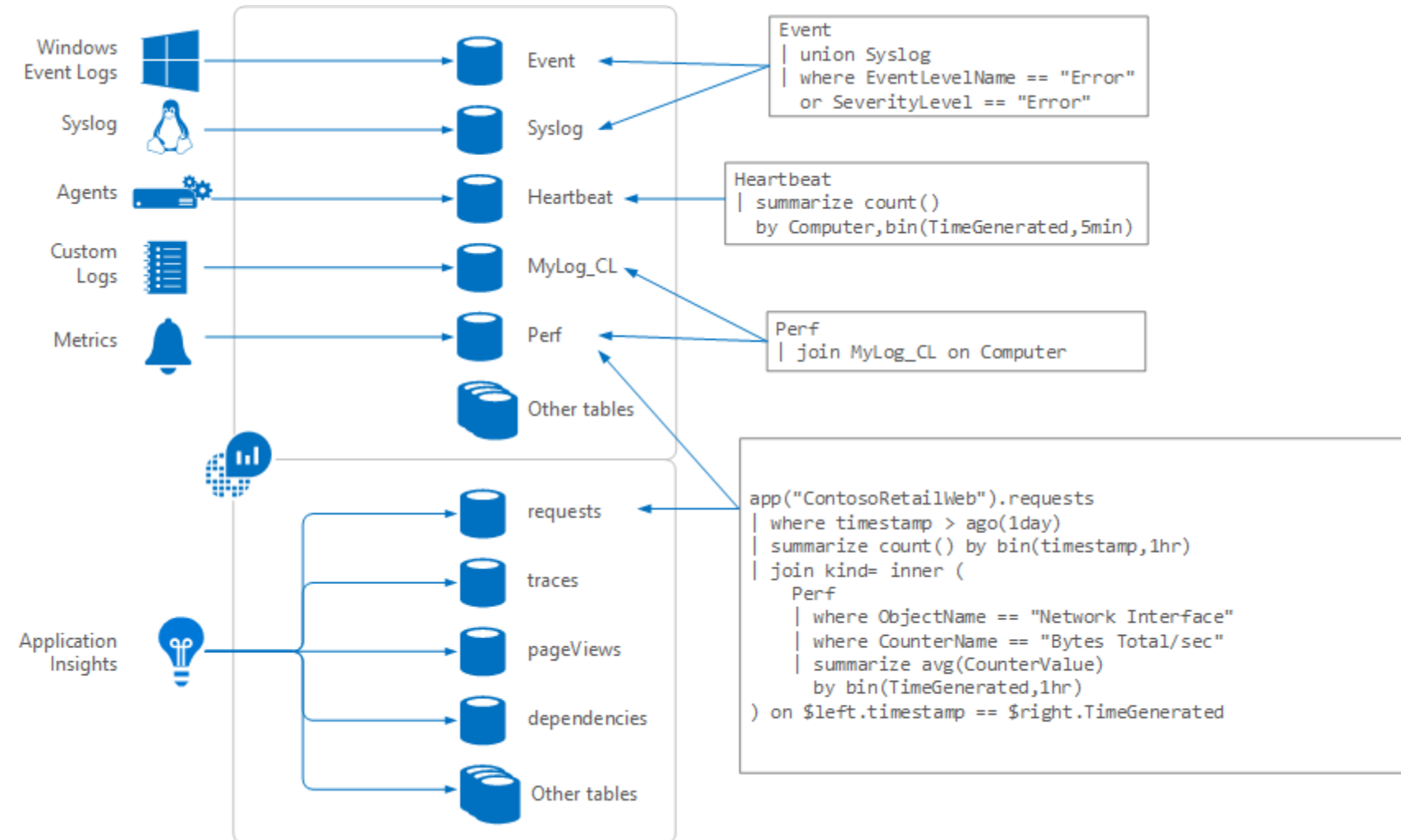
Azure Application Gateway

- 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

2019
Global Azure
BOOTCAMP

NASH
TECH
The Power to Innovate



DUCPHUONGKHANG-KUBE - Logs
Kubernetes service

WAFLog* + Help Settings Query explorer

defaultworkspace-e152427a-602a-... Run Time range: Set in query Save Copy link Export New alert rule Pin

Schema Filter (preview) <<

Filter by name or type...

Collapse all

Active

- defaultworkspace-e15242...
 - ContainerInsights
 - LogManagement
 - Security
 - SecurityCenterFree
 - Custom Logs
 - Functions

Favorite workspaces

```
where LogEntry has "lua"
project LogEntry, TimeGenerated
parse LogEntry with * "log.lua:52:" JSONLog "while" *
extend ResultLogObject = parse json(JSONLog)
project ResultLogObject, TimeGenerated
extend
Method = tostring(ResultLogObject.method),
URI = tostring(ResultLogObject.uri),
Client = tostring(ResultLogObject.client),
Alert1 = tostring(ResultLogObject.alerts[0].msg),
Alert2 = tostring(ResultLogObject.alerts[1].msg),
Alert3 = tostring(ResultLogObject.alerts[2].msg)
project TimeGenerated, URI, Method, Client, Alert1, Alert2, Alert3
```

Completed with partial results. 00:00:02.181 10,000 records

Display time (UTC+07:00)

TimeGenerated [Local Time]	URI	Method	Client	Alert1	Alert2
2018-11-29T12:33:44.042	/	GET	42.116.235.139	XSS (Cross-Site Scripting)	XSS (Cross-Site Scripting)
2018-11-29T12:33:44.338	/	GET	42.116.235.139	Repetitive non-word characters anomaly detected	XSS (Cross-Site Scripting)
2018-11-29T12:33:44.640	/	GET	42.116.235.139	XSS (Cross-Site Scripting)	XSS (Cross-Site Scripting)
2018-11-29T12:33:44.943	/	GET	42.116.235.139	Repetitive non-word charact	

Completed 00:00:00.383 19 records

TABLE CHART Columns

Stacked Column Client Count_ Alert2 Sum

Column

Line

Pie

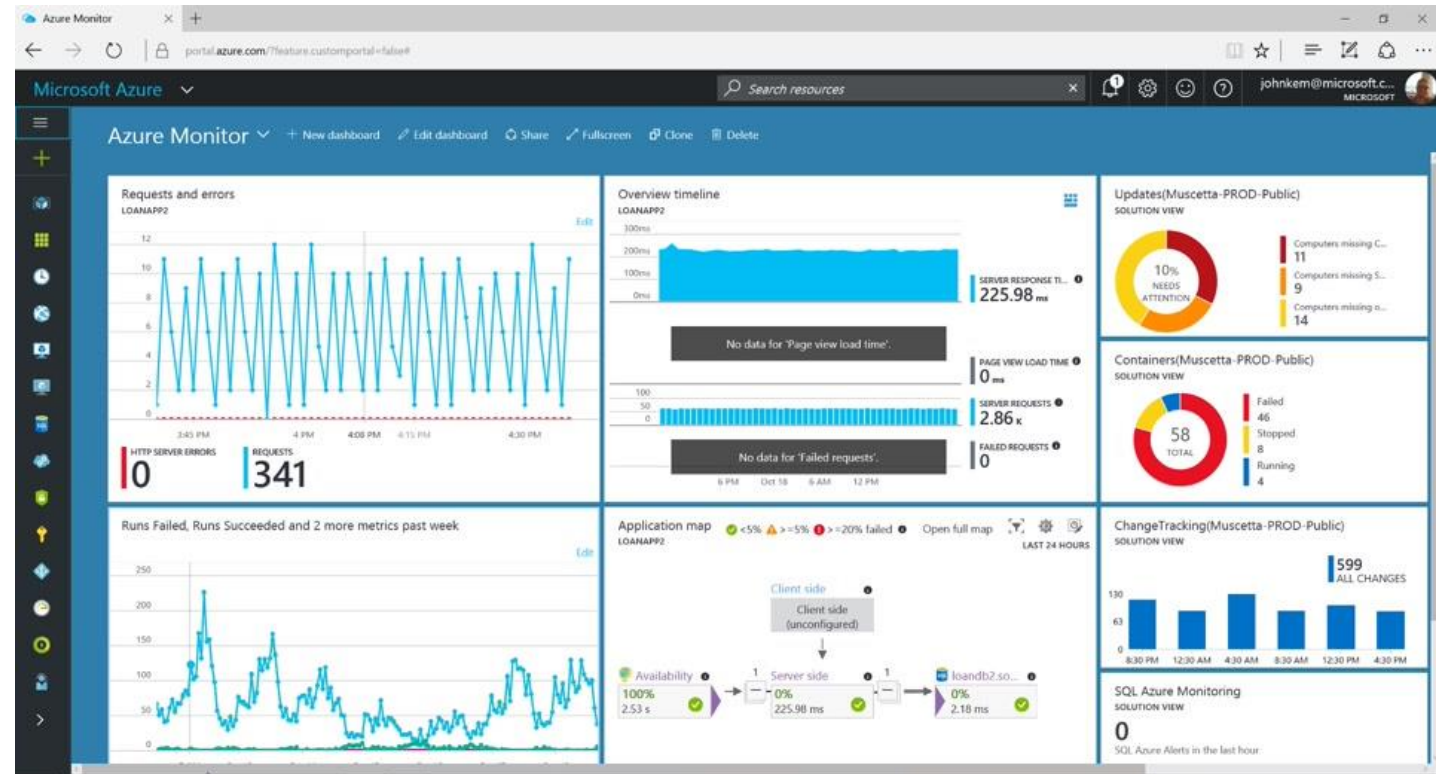
Area

Legend

- HTTP Response Splitting
- Repetitive non-word ch...
- SQL Comment Sequence
- SQL Injection attempt
- SQL Injection character ...
- SQL Operators
- SQL String Termination
- SQL Tautologies
- System file access atte...
- XSS (Cross-Site Scripting)
- XSS (Cross-Site Scriptin...

Azure Monitor

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





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/>



NGINX



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



Sat, Apr-27 @ NashTech

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](#)

```
foo.bar.com --|                               |-> foo.bar.com s1:80
                | 178.91.123.132             |
bar.foo.com  --|                               |-> bar.foo.com s2:80
```

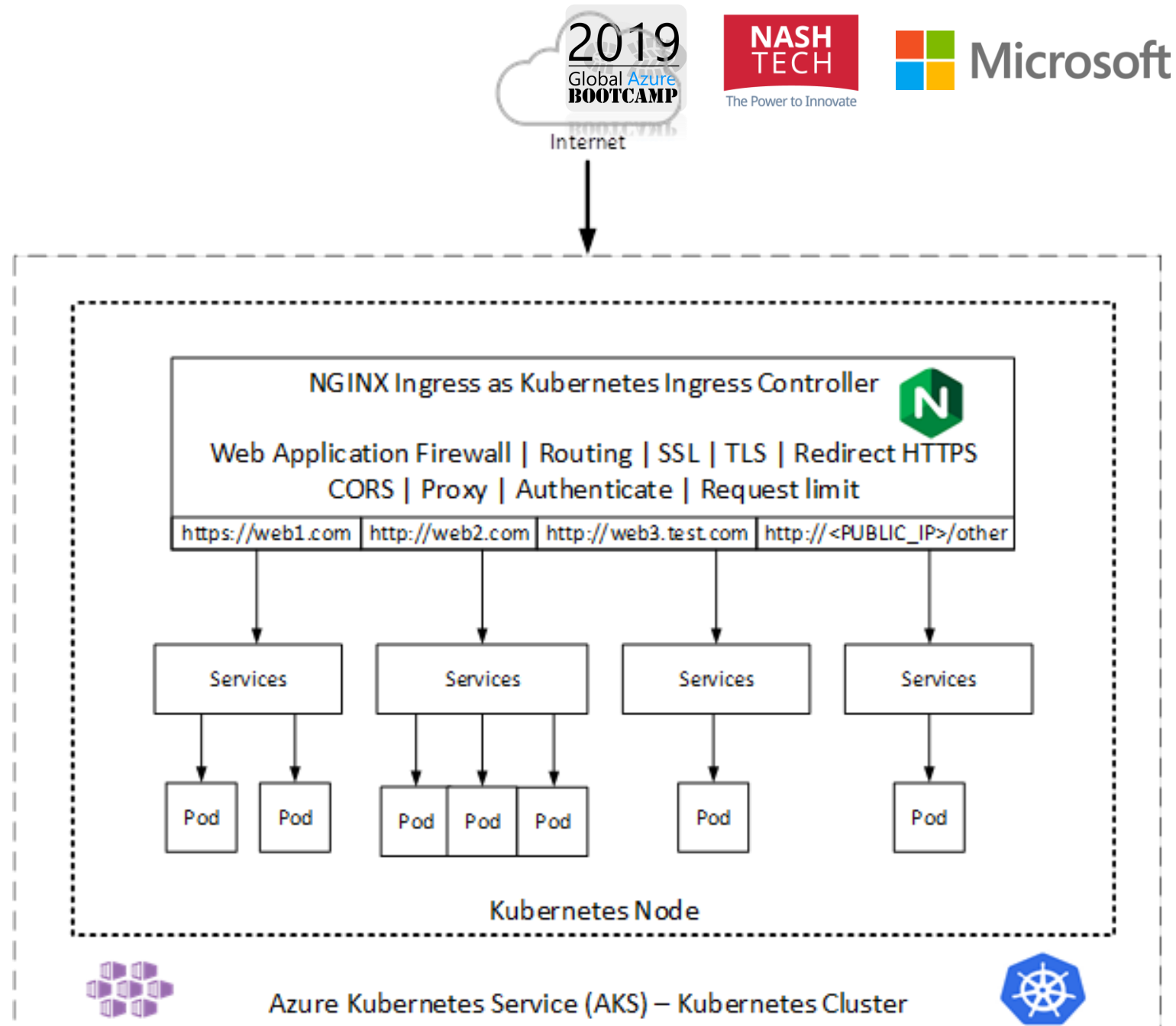
```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: name-virtual-host-ingress
spec:
  rules:
    - host: foo.bar.com
      http:
        paths:
          - backend:
              serviceName: service1
              servicePort: 80
    - host: bar.foo.com
      http:
        paths:
   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

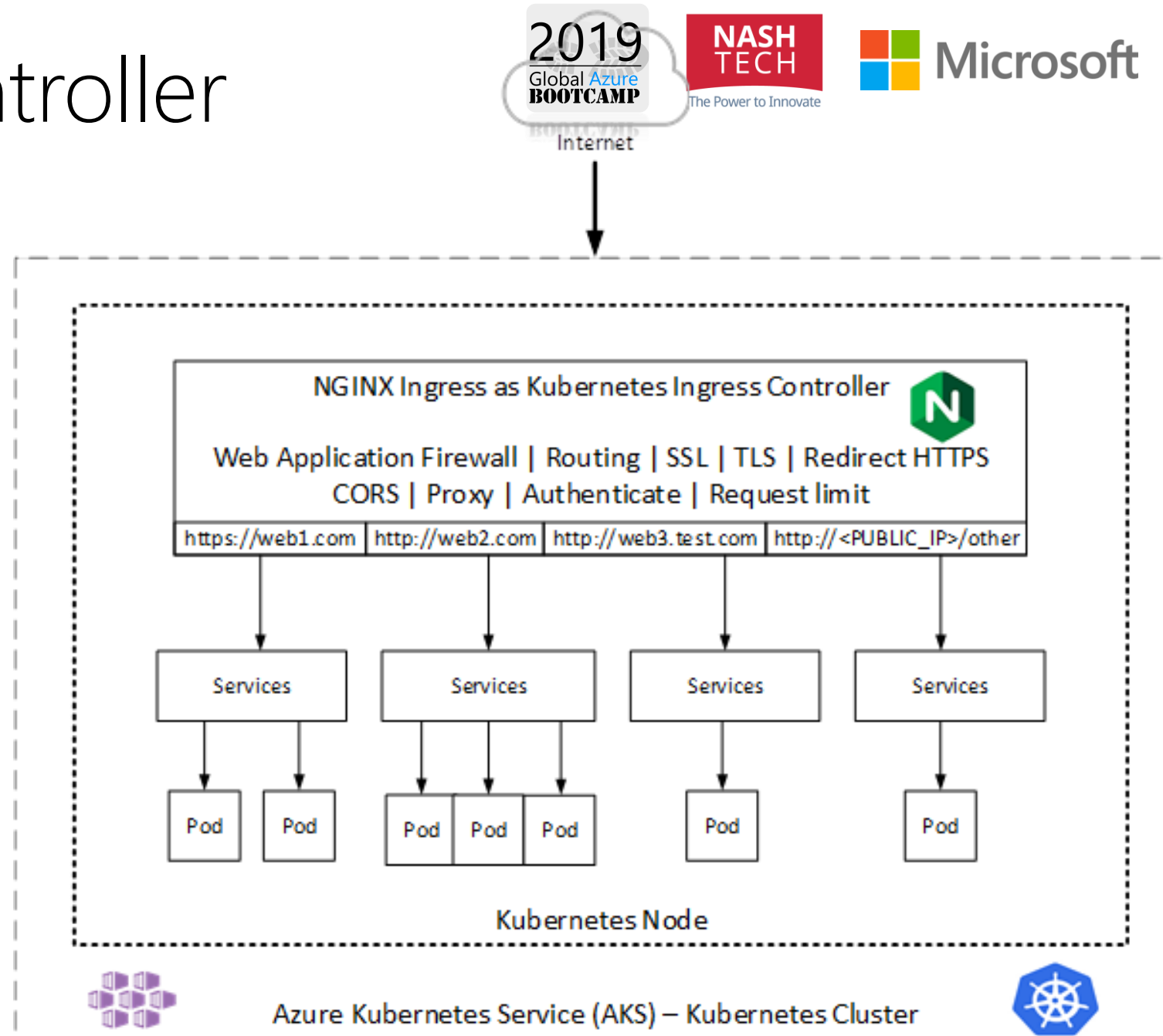


- Opensource project maintained by Kubernetes community based on NGINX Product. Integrate with *Resty WAF* (*ModSecurity*).

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

- Different from NGINX product:

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





NGINX



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



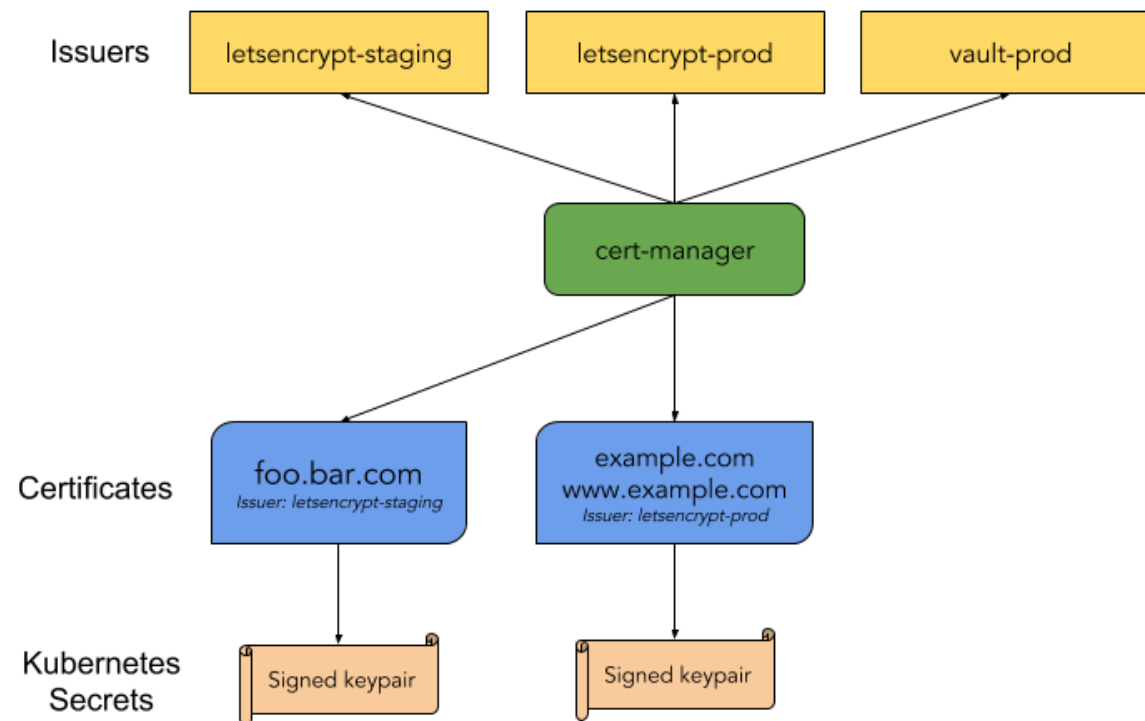
Sat, Apr-27 @ NashTech

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>



NGINX



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



Sat, Apr-27 @ NashTech

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



Sat, Apr-27 @ NashTech

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

DucLTM@outlook.com

Ingress YAML Annotations



- Resty WAF
- Force SSL
- SSL Issuer

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

`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

```
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
```



DEMO

Write Ingress config to activate WAF | HTTPS | L7 LB

Pen-test



Log Management on Azure Kubernetes Service



Sat, Apr-27 @ NashTech

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

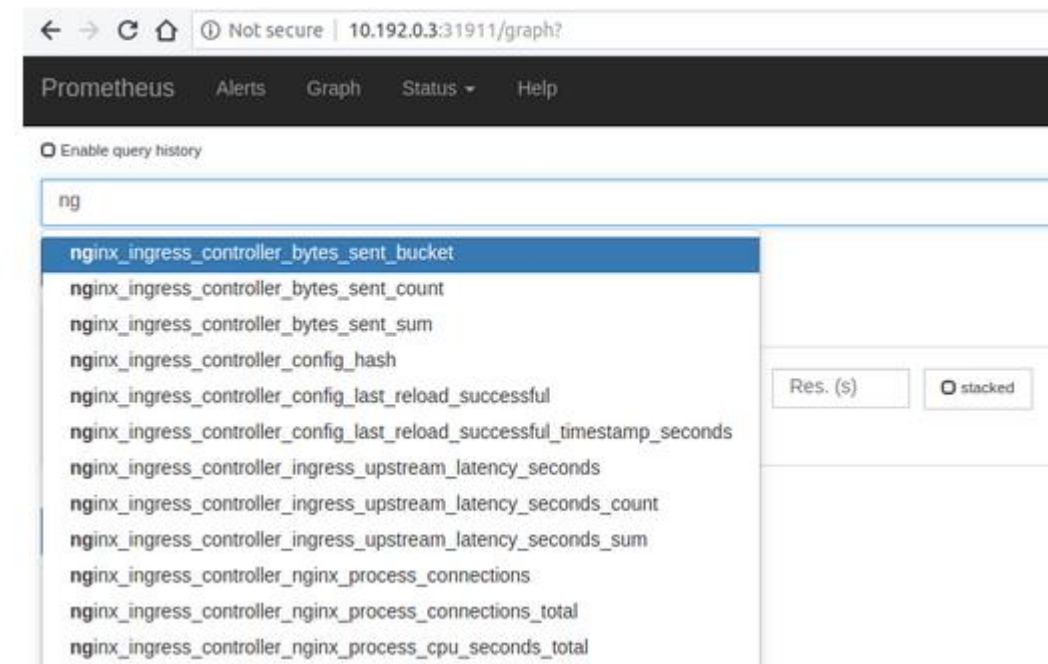
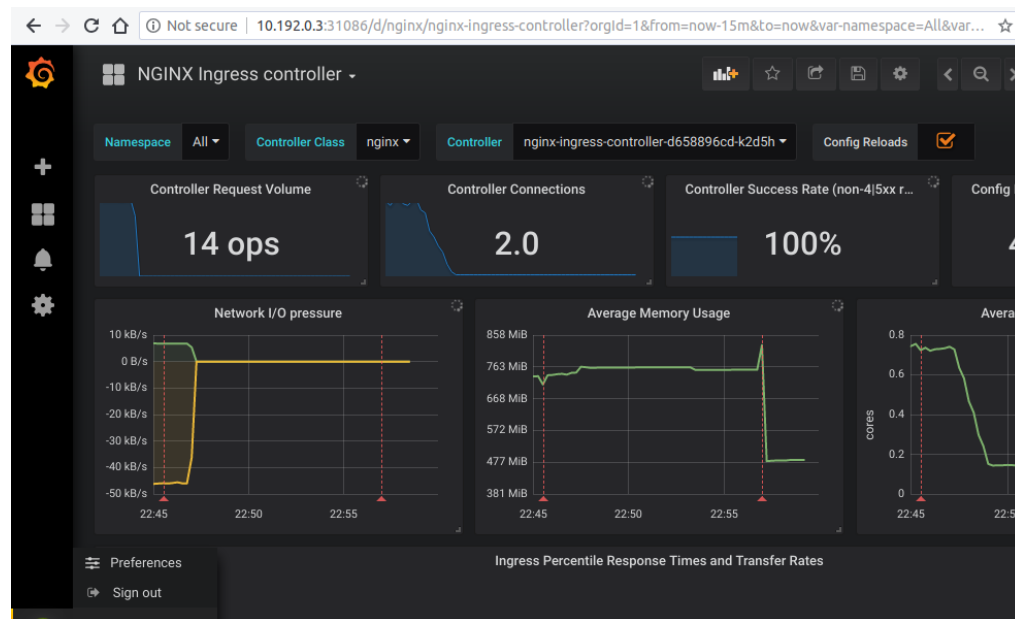
Microsoft Azure services

- 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)



NGINX



Alert to Slack with Azure Logic App



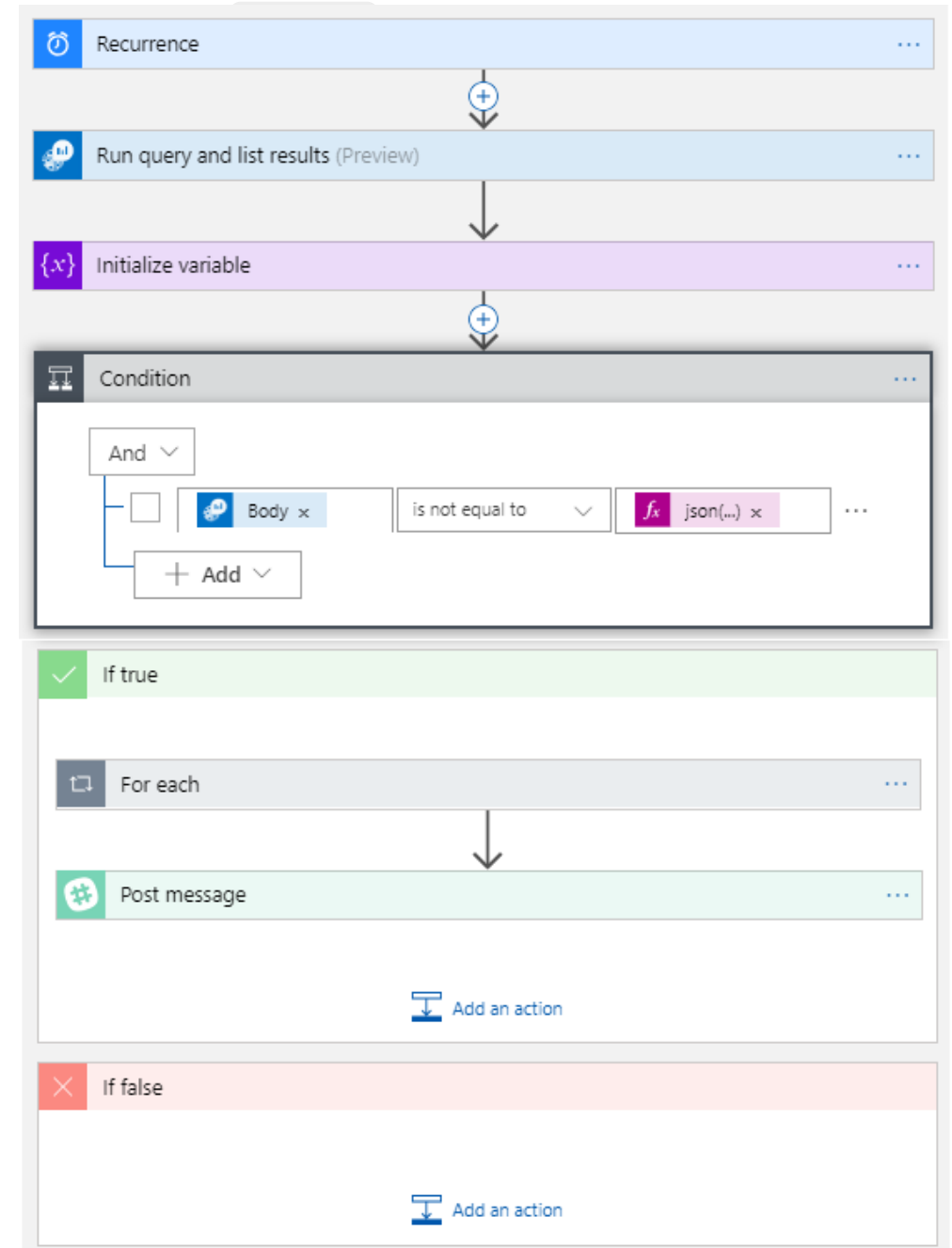
Sat, Apr-27 @ NashTech

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.





DEMO

Azure Logic App and Slack for Attack Alert
(result demo only)



THANK YOU



Sat, Apr-27 @ NashTech

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

DucLTM@outlook.com

Reference

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

