Simplify your Kubernetes setup through AKS Add-Ons

Maheshk
@MaheshKBlr

Cloud Solution Architect, Cloud-native, @Microsoft | market watcher, reader, cyclist, runner

Bengaluru, India linkedin.com/in/mfcmahesh/

Agenda

- Kubernetes on Azure
- AKS Addons & Demo
- AKS Tools
- Key takeaways

Kubernetes on Azure

Enterprise-grade by design

Development tools

- Visual Studio Code
- GitHub
- Azure Container Registry
- Azure Monitor

Platform

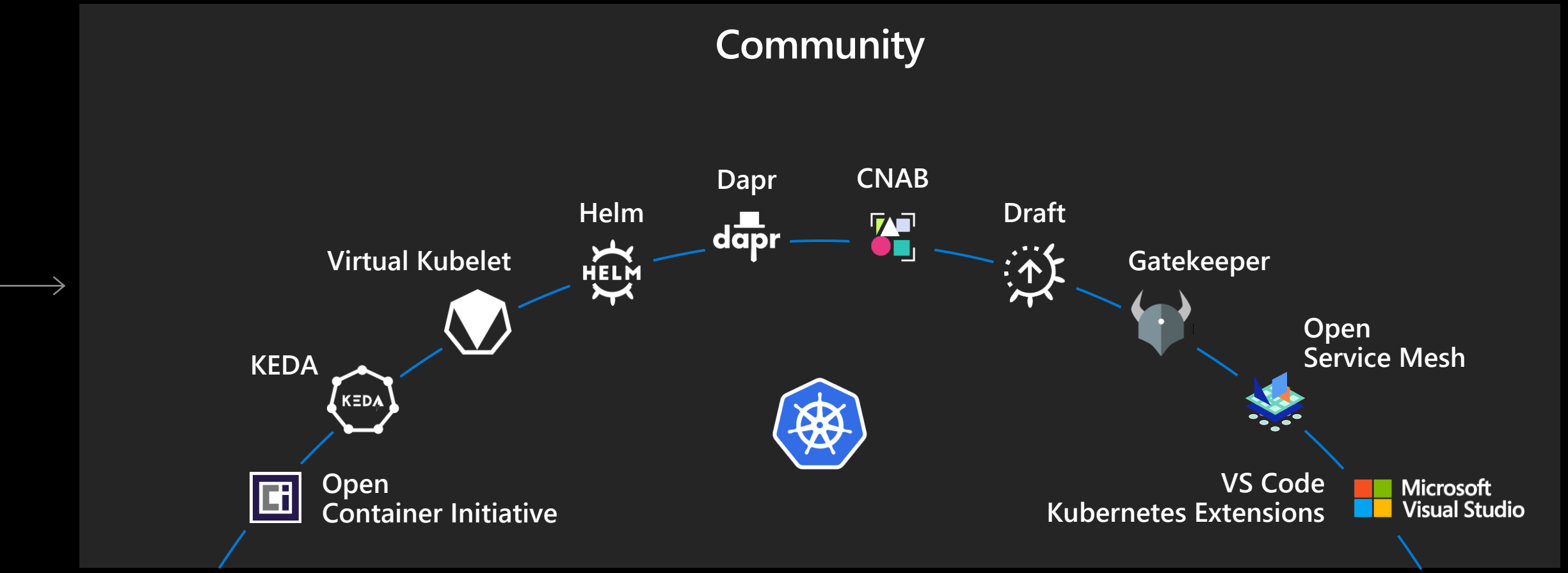
- Active Directory
- Azure Policy
- Security Center
- Key Vault
- Azure Advisor

- Azure Kubernetes Service
- Azure Container Instances
- Azure Red Hat OpenShift

Azure Arc: Management across environments

Kubernetes on Azure

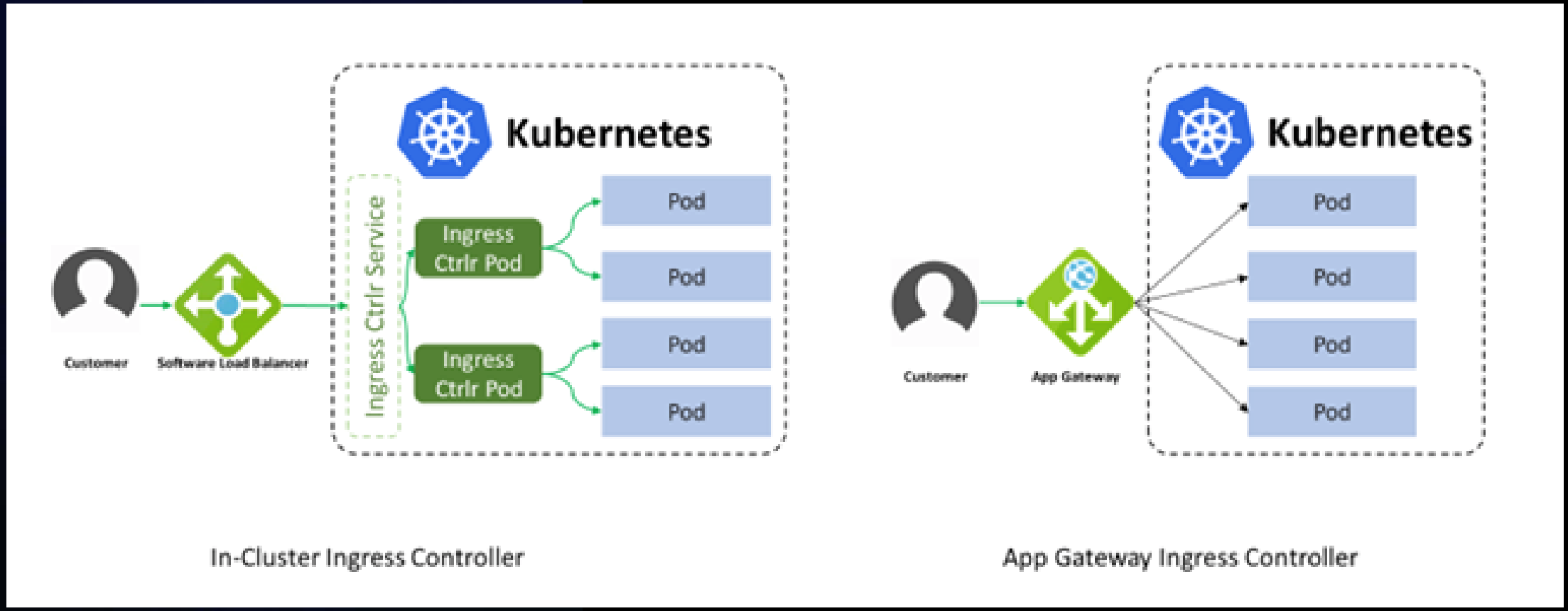
Enterprise-grade by design

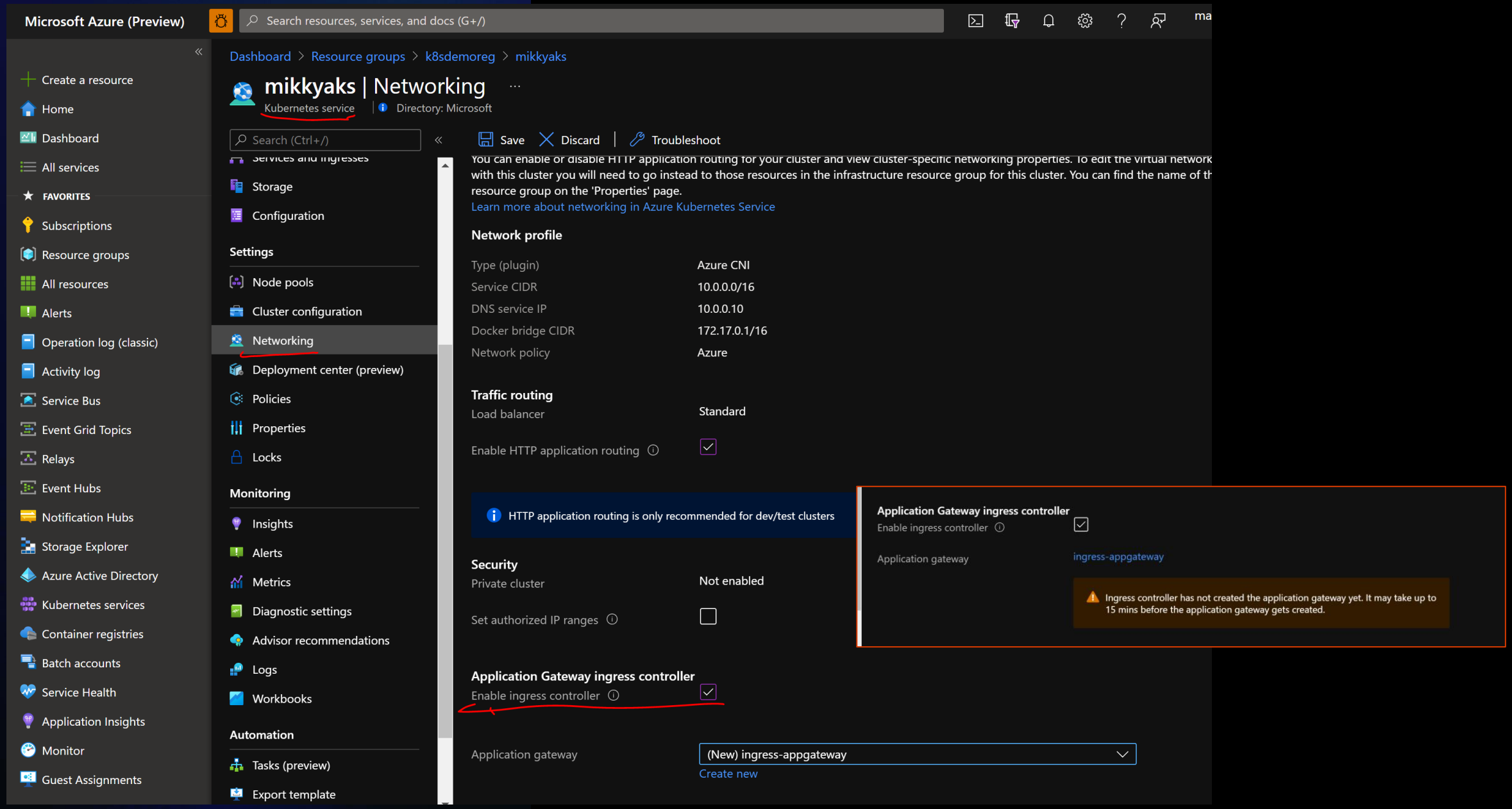


#1 – Application Gateway Ingress Controller add-on (AGIC)

- Configured via the Kubernetes Ingress resource, along with Service and Deployments/Pods.
- Leverages Application Gateway L7 load balancer

URL routing / Cookie-based affinity / TLS termination / End-to-end TLS
Support for public, private, and hybrid web sites / Integrated WAF

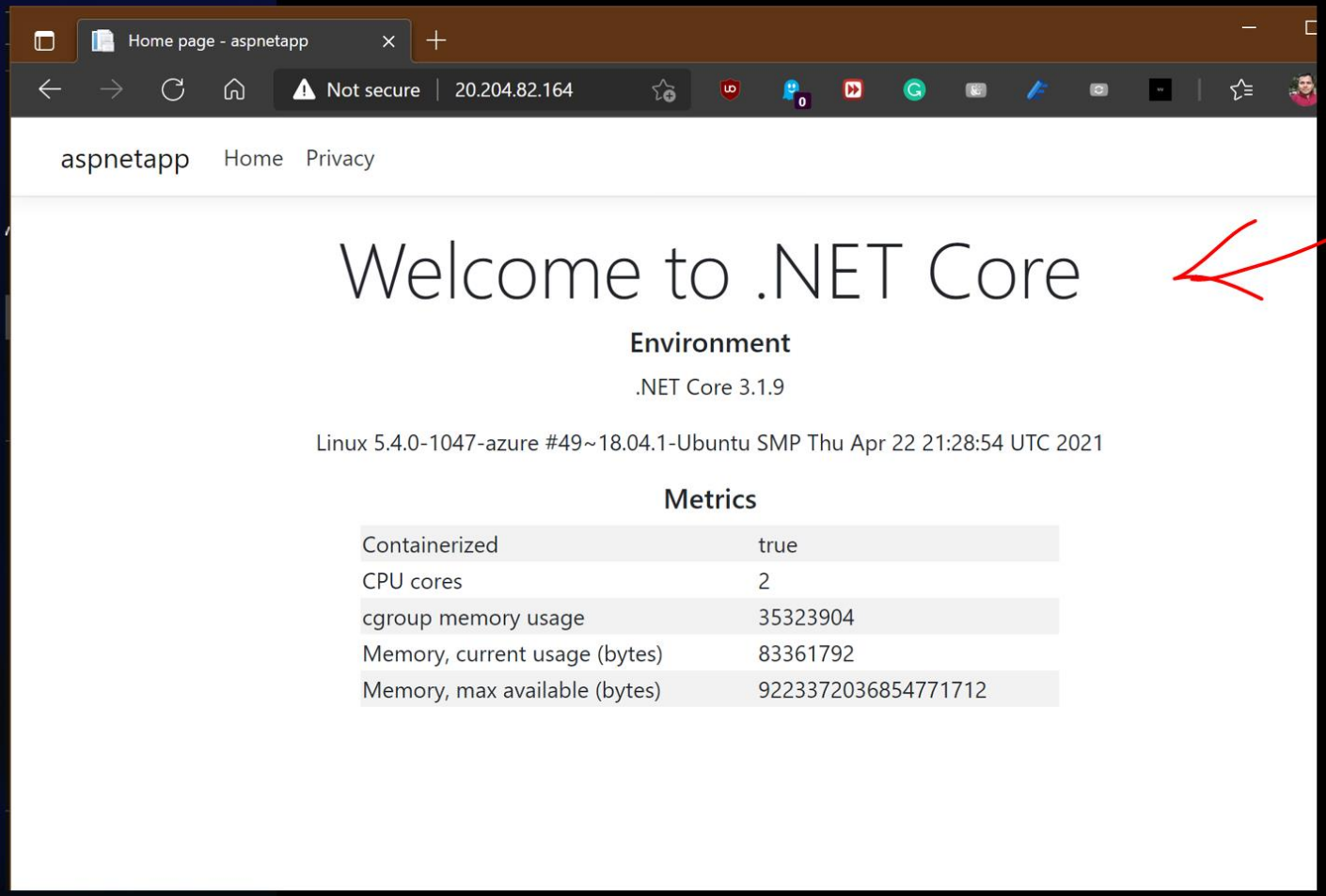



Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
Subscriptions
Resource groups
All resources
Alerts
Operation log (classic)
Activity log
Service Bus
Event Grid Topics
Relays
Event Hubs
Notification Hubs
Storage Explorer
Azure Active Directory
Kubernetes services
Container registries
Batch accounts
Service Health
Application Insights
Monitor
Guest Assignments
Dashboard > Resource groups > k8sdemoreg > mikkyaks
mikkyaks | Networking
Kubernetes service
Directory: Microsoft
Search (Ctrl+/)
Storage
Configuration
Settings
Node pools
Cluster configuration
Networking
Deployment center (preview)
Policies
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Logs
Workbooks
Automation
Tasks (preview)
Export template
Save
Discard
Troubleshoot
with this cluster you will need to go instead to those resources in the infrastructure resource group for this cluster. You can find the name of th
resource group on the 'Properties' page.
Learn more about networking in Azure Kubernetes Service
Network profile
Type (plugin)
Azure CNI
Service CIDR
10.0.0.0/16
DNS service IP
10.0.0.10
Docker bridge CIDR
172.17.0.1/16
Network policy
Azure
Traffic routing
Load balancer
Standard
Enable HTTP application routing
HTTP application routing is only recommended for dev/test clusters
Security
Private cluster
Not enabled
Set authorized IP ranges
Application Gateway ingress controller
Enable ingress controller
Application gateway
(New) ingress-appgateway
Create new
Application Gateway ingress controller
Enable ingress controller
Application gateway
ingress-appgateway
Ingress controller has not created the application gateway yet. It may take up to 15 mins before the application gateway gets created.

```
---

apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: aspnetapp
  annotations:
    kubernetes.io/ingress.class: azure/application-gateway
spec:
  rules:
  - http:
      paths:
      - path: /
        backend:
          serviceName: aspnetapp
          servicePort: 80
```

```
root:/mnt/d/k8sday/azure-voting-app-redis# k get ing
Warning: extensions/v1beta1 Ingress is deprecated in v1.14+, unavailable in v1.22+; use networking.k8s.io/v1 Ingress
NAME             CLASS    HOSTS                                                  ADDRESS         PORTS   AGE
aks-helloworld   <none>   aks-helloworld.fc97b331c1a1402e9c3c.centralindia.aksapp.io   20.204.30.160   80      30m
aspnetapp        <none>   *                                                      20.204.82.164   80      2m55s
root:/mnt/d/k8sday/azure-voting-app-redis#
```



#2 - Monitoring Addon

Helps to enable monitoring of our cluster using Azure CLI

```
$ az aks enable-addons -a monitoring -n ExistingManagedCluster -g ExistingManagedClusterRG
```

```
$ az aks enable-addons -a monitoring -n ExistingManagedCluster -g ExistingManagedClusterRG
--workspace-resource-id
"/subscriptions/<SubscriptionId>/resourceGroups/<ResourceGroupName>/providers/Microsoft.OperationalInsights/workspaces/<WorkspaceName>"
```

The output will resemble the following:

Output Copy

```
provisioningState       : Succeeded
```

https://docs.microsoft.com/en-us/azure/azure-monitor/containers/container-insights-enable-existing-clusters

#3 - Virtual Node Add on (based on Virt-Kubelet)

VNodes enable network communication between pods that run in Azure Container Instances (ACI) & AKS

$ az aks enable-addons --resource-group myResourceGroup --name myAKSCluster --addons virtual-node --subnet-name myVirtualNodeSubnet

Note: **$ az aks install-cli** must be installed before running any 'Az AKS' command

```
root:/mnt/d/k8sday/azure-voting-app-redis# kubectl get pod
NAME                                READY   STATUS    RESTARTS   AGE
aci-helloworld-59cd44f545-zhw7x     0/1     Pending   0          77s
aks-helloworld-796448fcc4-ffmh4     1/1     Running   0          10h
aspnetapp                           1/1     Running   0          9h
azure-vote-back-59d587dbb7-gf598    1/1     Running   0          11h
azure-vote-front-78dc4ff55b-s7bbw   1/1     Running   0          11h
```

```
root:/mnt/d/k8sday/azure-voting-app-redis# k get no
NAME                                STATUS   ROLES   AGE   VERSION
aks-agentpool-22028957-vmss000000   Ready    agent   12h   v1.19.11
aks-agentpool-22028957-vmss000001   Ready    agent   12h   v1.19.11
aks-agentpool-22028957-vmss000002   Ready    agent   12h   v1.19.11
```

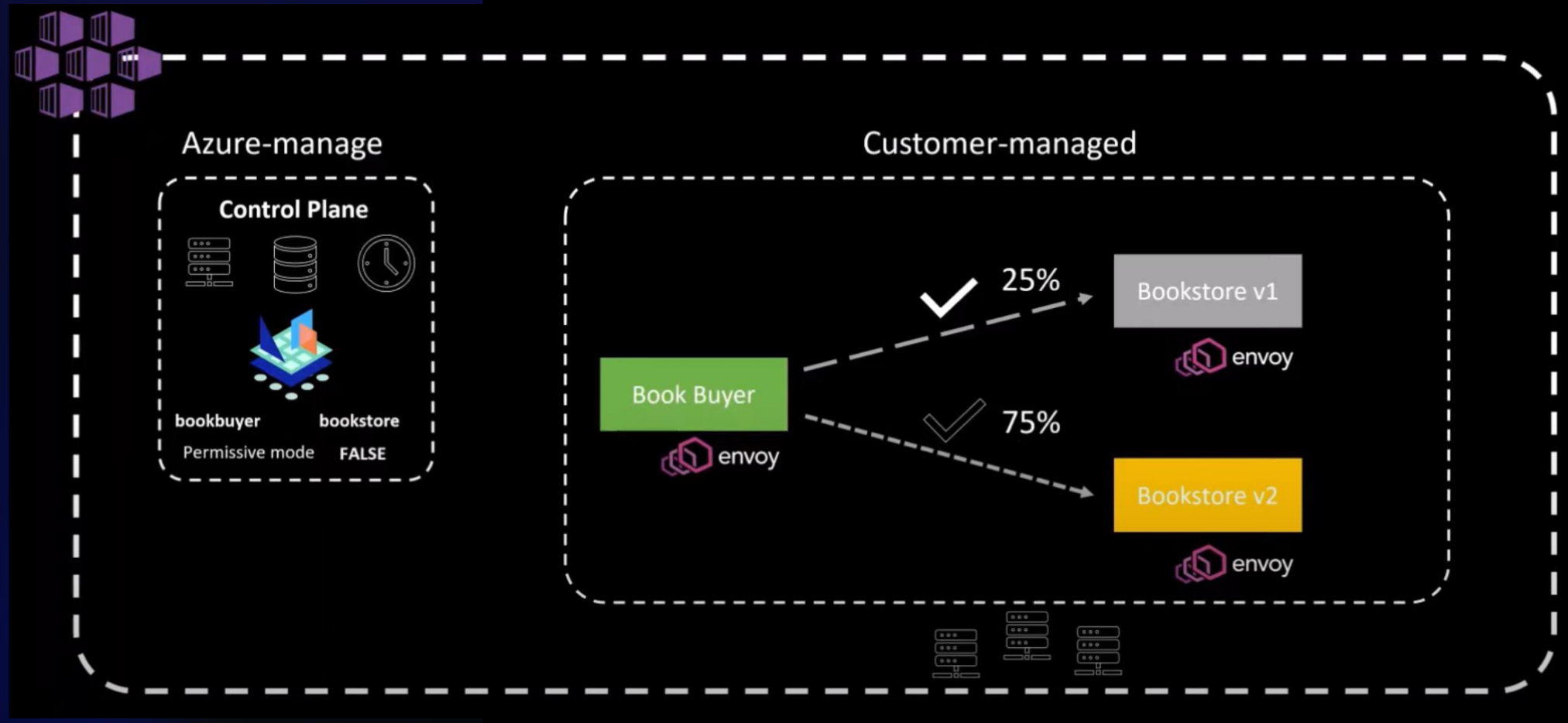
https://docs.microsoft.com/en-us/azure/aks/virtual-nodes-cli

#4 - Open Service Mesh (OSM) AKS Addon **preview*

- OSM is a robust service mesh utilizing the Envoy proxy CNCF project.
- lightweight, extensible, Cloud Native service mesh that allows users to uniformly manage, secure
- Uses Service Mesh Interface SMI and works by injecting an Envoy proxy as a sidecar
- Traffic encryption, routing, management, shifting, observability, debugging and monitoring
- secure end to end service to service communication by enabling mTLS

https://docs.openservicemesh.io/

#4 Open Service Mesh (OSM) AKS Addon **preview*



https://docs.microsoft.com/en-us/azure/aks/servicemsh-osm-about

#5 Azure-policy addon

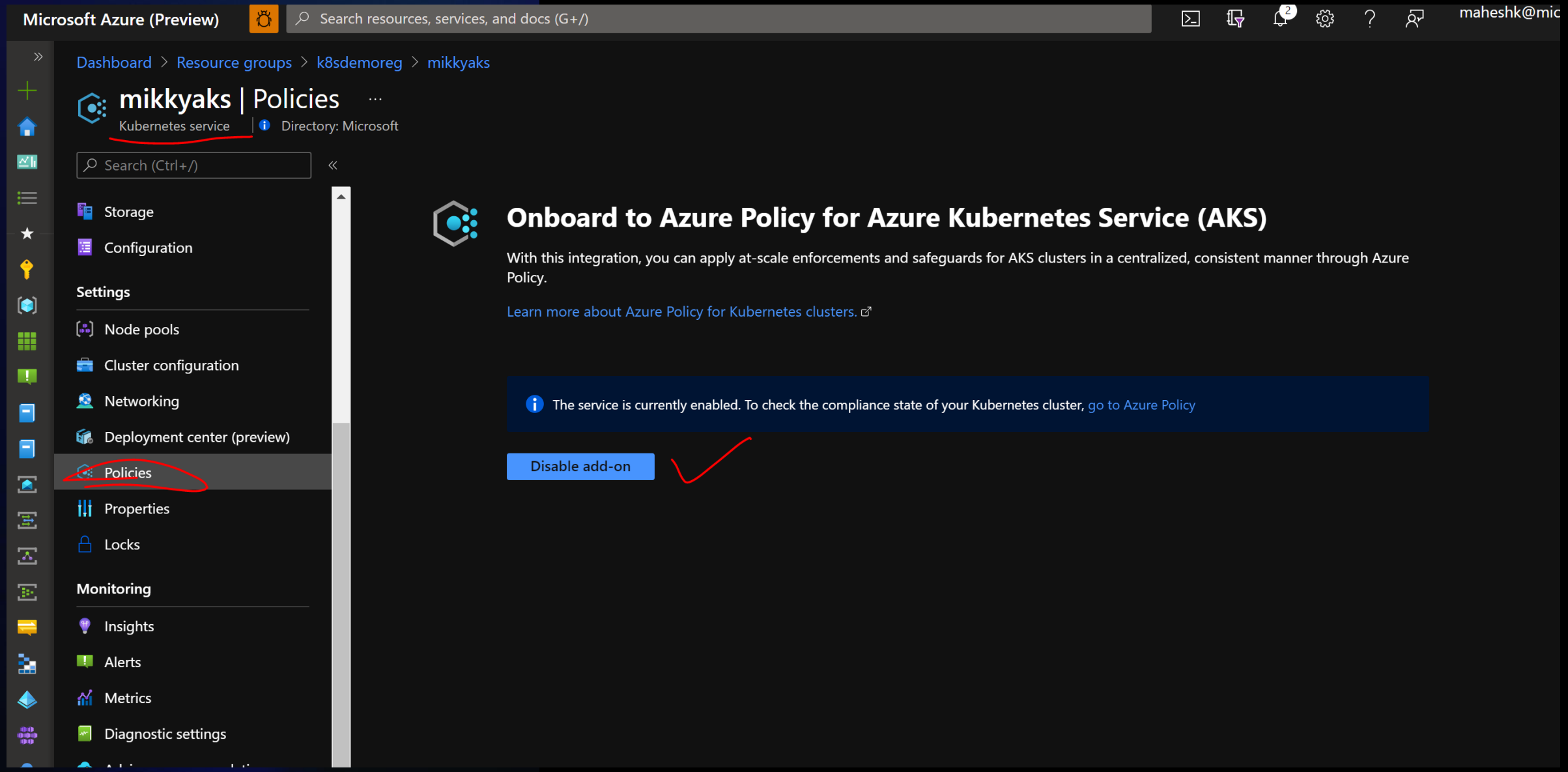
- Azure Policy extends Gatekeeper v3
- Helps to apply at-scale enforcements – Safeguards our clusters
- Manage & report the compliance from one place

```
$ az aks enable-addons --addons azure-policy --name MyAKSCluster --resource-group MyResourceGroup
```

```
root:/mnt/d/k8sday/azure-voting-app-redis# az aks enable-addons --addons azure-policy --name mikkyaks --resourc
The behavior of this command has been altered by the following extension: aks-preview
{- Finished ..
  "aadProfile": null,
  "addonProfiles": {
    "azurepolicy": {
      "config": null,
      "enabled": true,
      "identity": {
        "clientId": "1a1dc531-edaa-4dbe-b949-d3f75ef7e95d",
        "objectId": "338c7cdd-a69d-42ed-b960-0fcfe7181de5",
        "resourceId": "/subscriptions/38e1b8c4-c5bc-4dd5-a7e0-e909b45f4fad/resourcegroups/MC_k8sdemoreg_mikkyak
ntity/userAssignedIdentities/azurepolicy-mikkyaks"
      }
    },
    "httpApplicationRouting": {
      "config": {
        "HTTPApplicationRoutingZoneName": "fc97b331c1a1402e9c3c.centralindia.aksapp.io"
      },
```

```
}
root:/mnt/d/k8sday/azure-voting-app-redis# kubectl get pods -n gatekeeper-system
NAME                                     READY   STATUS    RESTARTS   AGE
gatekeeper-audit-6dcf64cf84-fqlgr        1/1     Running   0          51m
gatekeeper-controller-6dd6b7f4c9-2tsmr   1/1     Running   0          51m
gatekeeper-controller-6dd6b7f4c9-bwflf   1/1     Running   0          51m
root:/mnt/d/k8sday/azure-voting-app-redis#
```

```
      "config": {
```


Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
maheshk@mic
Dashboard > Resource groups > k8sdemoreg > mikkyaks
mikkyaks | Policies
Kubernetes service
Directory: Microsoft
Search (Ctrl+/)
Storage
Configuration
Settings
Node pools
Cluster configuration
Networking
Deployment center (preview)
Policies
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Onboard to Azure Policy for Azure Kubernetes Service (AKS)
With this integration, you can apply at-scale enforcements and safeguards for AKS clusters in a centralized, consistent manner through Azure Policy.
Learn more about Azure Policy for Kubernetes clusters.
The service is currently enabled. To check the compliance state of your Kubernetes cluster, go to Azure Policy
Disable add-on

#6 – HTTP Application routing Addon

- Help us to create an ingress controller quickly and allow access our applications

- Not designed for production environment

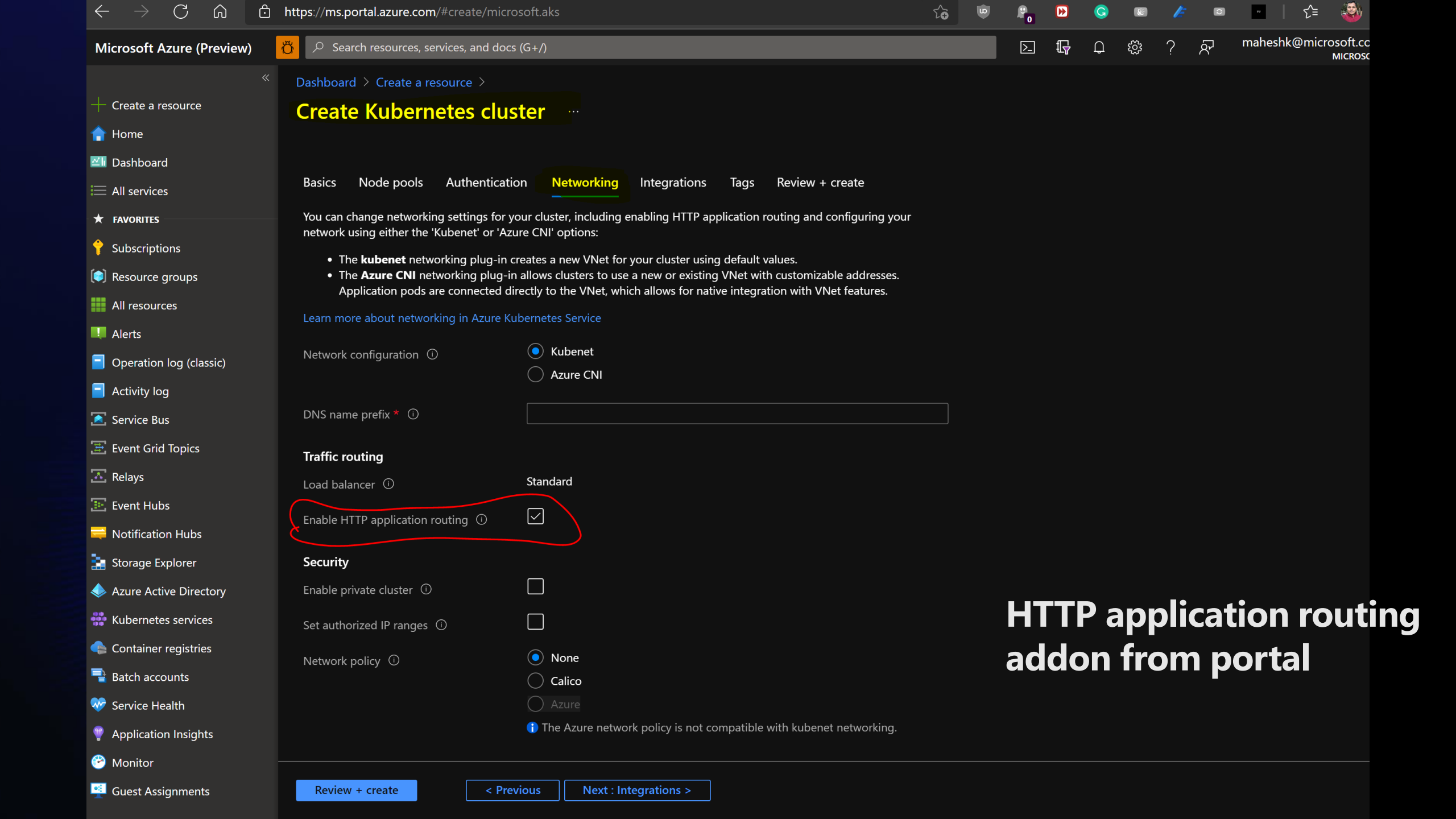
```
$ az aks create --resource-group myResourceGroup
--name myAKSCluster --enable-addons http_application_routing
```

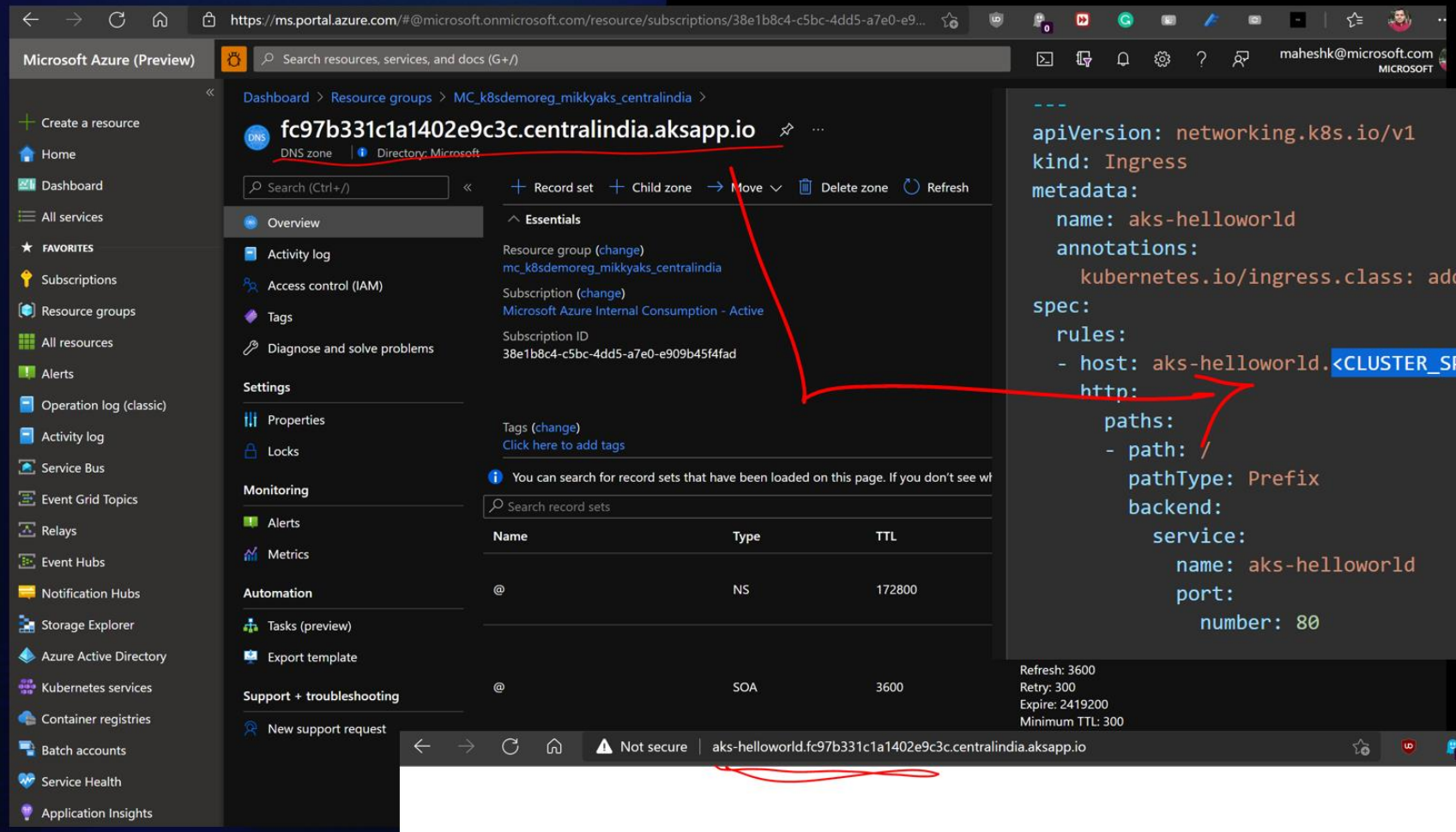
```
$ az aks enable-addons --resource-group myResourceGroup
--name myAKSCluster --addons http_application_routing
```

```
$ az aks disable-addons --addons http_application_routing --name myAKSCluster --resource-group
myResourceGroup --no-wait
```

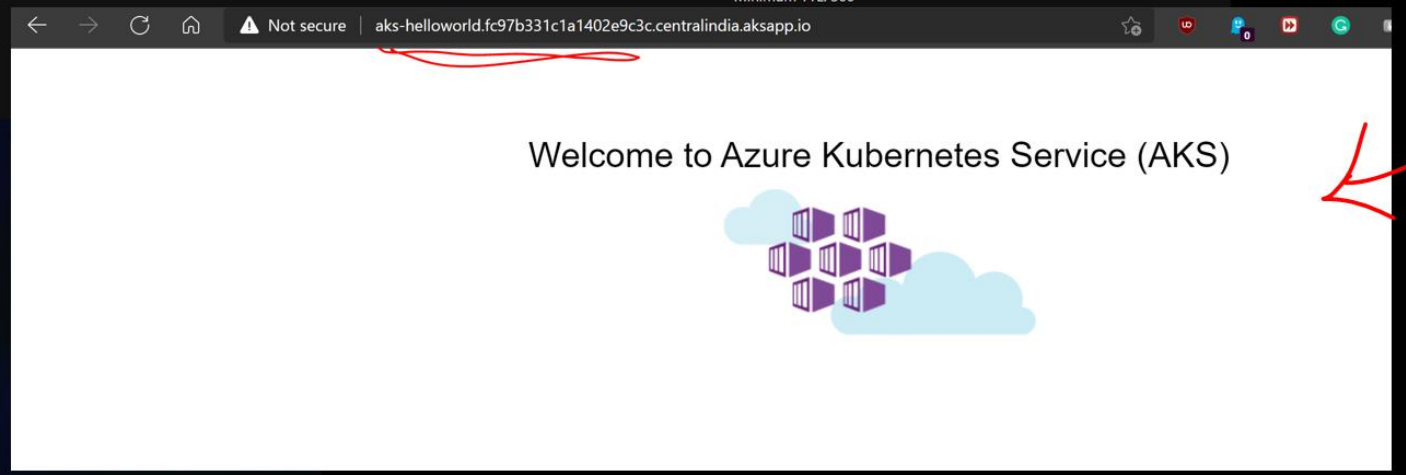
root: /mnt/d/k8sday/azure-voting-app-redis

```
root:/mnt/d/k8sday/azure-voting-app-redis# az aks show --resource-group k8sdemoreg --name mikkyaks --output table
The behavior of this command has been altered by the following extension: aks-preview
Name      Location      ResourceGroup    KubernetesVersion    ProvisioningState    Fqdn
--------  ------------  ---------------  -------------------  -------------------  ----------------------------------------------
mikkyaks  centralindia  k8sdemoreg       1.19.11              Succeeded            mikkyaks-dns-12f69bd2.hcp.centralindia.azmk8s.io
root:/mnt/d/k8sday/azure-voting-app-redis# az aks enable-addons --resource-group k8sdemoreg --name mikkyaks --addons http_application_routing
The behavior of this command has been altered by the following extension: aks-preview
{- Finished ..
  "aadProfile": null,
  "addonProfiles": {
    "azurepolicy": {
      "config": null,
      "enabled": false,
      "identity": null
    },
    "httpApplicationRouting": {
      "config": {
        "HTTPApplicationRoutingZoneName": "fc97b331c1a1402e9c3c.centralindia.aksapp.io"
      },
      "enabled": true,
      "identity": {
        "clientId": "e6fb13d0-7adb-47ad-9dad-462995785edb",
        "objectId": "396b2d84-33cf-40f0-bcb1-dca909580e95",
        "resourceId": "/subscriptions/38e1b8c4-c5bc-4dd5-a7e0-e909b45f4fad/resourcegroups/MC_k8sdemoreg_mikkyaks_centralindia/providers/Microsoft.ManagedIdentity/userAssignedIdentities/httpapplicationrouting-mikkyaks"
      }
    },
    "omsAgent": {
      "config": {
        "logAnalyticsWorkspaceResourceID": "/subscriptions/38e1b8c4-c5bc-4dd5-a7e0-e909b45f4fad/resourcegroups/defaultresourcegroup-cin/providers/microsoft.operationalinsights/workspaces/defaultworkspace-38e1b8c4-c5bc-4dd5-a7e0-e909b45f4fad-cin"
      },
      "enabled": true,
      "identity": {
        "clientId": "91c58769-532a-4bb9-a44b-cc596e135e13",
        "objectId": "8f22f28d-0156-4e8e-9bb9-7e97cc919ede",
        "resourceId": "/subscriptions/38e1b8c4-c5bc-4dd5-a7e0-e909b45f4fad/resourcegroups/MC_k8sdemoreg_mikkyaks_centralindia/providers/Microsoft.ManagedIdentity/userAssignedIdentities/omsagent-mikkyaks"
      }
    }
  },
  "agentPoolProfiles": [
    {
      "availabilityZones": null,
```


https://ms.portal.azure.com/#create/microsoft.aks
Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
maheshk@microsoft.co
MICROSO
Create a resource
Home
Dashboard
All services
FAVORITES
Subscriptions
Resource groups
All resources
Alerts
Operation log (classic)
Activity log
Service Bus
Event Grid Topics
Relays
Event Hubs
Notification Hubs
Storage Explorer
Azure Active Directory
Kubernetes services
Container registries
Batch accounts
Service Health
Application Insights
Monitor
Guest Assignments
Dashboard > Create a resource >
Create Kubernetes cluster
Basics
Node pools
Authentication
Networking
Integrations
Tags
Review + create
You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Kubenet' or 'Azure CNI' options:
The kubenet networking plug-in creates a new VNet for your cluster using default values.
The Azure CNI networking plug-in allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.
Learn more about networking in Azure Kubernetes Service
Network configuration
Kubenet
Azure CNI
DNS name prefix *
Traffic routing
Load balancer
Standard
Enable HTTP application routing
Security
Enable private cluster
Set authorized IP ranges
Network policy
None
Calico
Azure
The Azure network policy is not compatible with kubenet networking.
Review + create
< Previous
Next : Integrations >
HTTP application routing addon from portal




```yaml
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: aks-helloworld
  annotations:
    kubernetes.io/ingress.class: addon-http-application-routing
spec:
  rules:
  - host: aks-helloworld.<CLUSTER_SPECIFIC_DNS_ZONE>
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: aks-helloworld
            port:
              number: 80
```



List of AKS Addons

Maheshk
@MaheshKBlr

Add on	Purpose	Production ready?
1. App Gateway Ingress controller (AGIC)	turn on Log Analytics monitoring	Yes
2. Monitoring	Helps monitor our clusters. It supports Prometheus as well	Yes
3. Virtual Node	Enable AKS Virtual Nodes using container images for POD (based on virtual Kubelet project) https://github.com/virtual-kubelet/virtual-kubelet	Yes
4. Open Service Mesh (OSM)	Allows users to uniformly manage, secure, and get out-of-the-box observability features for highly dynamic microservice environments	In public preview
5. azure-policy	Enables at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. https://aka.ms/aks/policy	Yes
6. HTTP Application routing	Quick Ingress controller for dev environment. It helps to configure ingress with automatic public DNS name creation.	Only for dev/test cluster
7. DAPR	https://dapr.io/ Distributed Application Prog. Runtime https://github.com/Azure/AKS/projects/1	In development
8. kube-dashboard	AKS dashboard add-on. Allows to disable k8s dashboard for older version. Deprecated from 1.19+ onwards	Deprecated

```
To list all installed AKS Add-ons: $ az aks list -g myAKSResourceGroup | jq -r .[].addonProfiles
```

AKS Tools

Built-in best practices


Azure Advisor recommendations for AKS


Azure Security Center


AKS Cluster baseline


AKS Diagnostics


AKS Periscope


Kubernetes and AKS VS Code extension


AKS best practices

Azure Developer Community

Learn, Network, Upskill

Share with Azure fans!

Supported by

Microsoft Azure

Thank you

Questions?
Slide deck ->

Maheshk
@MahesKBlr