Microsoft

Cloud Native Night Munich

AKS best practices

Jose Moreno

Azure FastTrack Engineer
jose.moreno@microsoft.com

Microsoft FastTrack für Azure

Arbeiten Sie gemeinsam mit Azure-Technikern am Onboarding der Kunden. Erweitern Sie Ihr Business durch schnellere Wertschöpfung und Erweiterung Ihrer Kenntnisse.

Direkte Unterstützung durch Azure-Techniker.

Zugang zu Tools und realen Kundenumgebungen

Zusammenarbeit mit Ihren internen Ressourcen und Partnern

Infos: https://azure.microsoft.com/de-de/programs/azure-fasttrack/
Nominierung: https://azfasttrack.azurewebsites.net/

Agenda

- Cluster Isolation and Resource Management
- Storage
- Networking
- Network Policies
- Securing your Environment
- Scaling your Applications and Cluster
- Logging and Monitoring

What is AKS?

Kubernetes is not the thing.
It is the thing that gets us to
the thing.

Kubernetes offerings in Azure

	Do It Yourself	acs-engine	Azure Kubernetes Service
Description	Create your VMs, deploy k8s	acs-engine generates ARM templates to deploy k8s	Managed k8s
Possibility to modify the cluster	Highest	Highest	Medium
You pay for	Master+Node VMs	Master+Node VMs	Node VMs
Supports internal clusters (no Internet connectivity)	Yes	Yes	Yes (master VMs with public IPs today)

az aks overview

```
$ az aks -h
Commands:
    browse            : Show the dashboard for a Kubernetes cluster in a web browser.
    create            : Create a new managed Kubernetes cluster.
    delete            : Delete a managed Kubernetes cluster.
    disable-addons    : Disable Kubernetes addons.
    enable-addons     : Enable Kubernetes addons.
    get-credentials   : Get access credentials for a managed Kubernetes cluster.
    get-upgrades      : Get the upgrade versions available for a managed Kubernetes cluster.
    get-versions      : Get the versions available for creating a managed Kubernetes cluster.
    install-cli       : Download and install kubectl, the Kubernetes command-line tool.
    install-connector : (PREVIEW) Install the ACI Connector on a managed Kubernetes cluster.
    list              : List managed Kubernetes clusters.
    remove-connector  : (PREVIEW) Remove the ACI Connector from a managed Kubernetes cluster.
    remove-dev-spaces : (PREVIEW) Remove Azure Dev Spaces from a managed Kubernetes cluster.
    scale             : Scale the node pool in a managed Kubernetes cluster.
    show              : Show the details for a managed Kubernetes cluster.
    upgrade           : Upgrade a managed Kubernetes cluster to a newer version.
    upgrade-connector : (PREVIEW) Upgrade the ACI Connector on a managed Kubernetes cluster.
    use-dev-spaces    : (PREVIEW) Use Azure Dev Spaces with a managed Kubernetes cluster.
    wait              : Wait for a managed Kubernetes cluster to reach a desired state.
```

AKS provisioning

Day 0:

```
az aks create -n myakscluster -g aksrg --node-count 2 -k 1.11.3 -s Standard_DS2_v2
az aks get-credentials –myakscluster -g aksrg
kubectl get nodes
```

Day 1:

```
az aks enable-addons –myakscluster -g aksrg -a monitoring,http_application_routing
kubectl all the things!
```

Day 2:

```
az aks upgrade –myakscluster -g aksrg -k 1.11.4
```

I have a cluster, now what?

Some Kubernetes best practices

- Use namespaces, do not deploy to default
- Optionally, use different clusters for different apps/environments (remember, you do not pay for the master nodes!)
- Use resource quotas
- Use at least 3 nodes, that will give you enough capacity during upgrades (especially if using disks as persistent volumes)

Kube-advisor

- Diagnostic tool for Kubernetes clusters. At the moment, it returns pods that are missing resource and request limits.
- More info can be found at https://github.com/Azure/kube-advisor

```
|                                  |                                          | CPU Request Limits Missing     |
+                                  +                                          +--------------------------------+
|                                  |                                          | Memory Request Limits Missing  |
+----------------------------------+------------------------------------------+--------------------------------+
| zipkin-zipkin                    | zipkin                                   | CPU Resource Limits Missing    |
+                                  +                                          +--------------------------------+
|                                  |                                          | Memory Resource Limits Missing |
+                                  +                                          +--------------------------------+
|                                  |                                          | CPU Request Limits Missing     |
+                                  +                                          +--------------------------------+
|                                  |                                          | Memory Request Limits Missing  |
+----------------------------------+------------------------------------------+--------------------------------+
+--------------------------------+-------------------------------------------------------------------------------+
|            ISSUE               |                                REMEDIATION                                    |
+--------------------------------+-------------------------------------------------------------------------------+
| CPU Request Limits Missing     | Consider setting resource and request limits to prevent resource starvation:  |
|                                | https://kubernetes.io/docs/concepts/configuration/manage-compute-resources-container/ |
| Memory Request Limits Missing  |                                                                               |
|                                |                                                                               |
| CPU Resource Limits Missing    |                                                                               |
|                                |                                                                               |
| Memory Resource Limits Missing |                                                                               |
|                                |                                                                               |
+--------------------------------+-------------------------------------------------------------------------------+
```

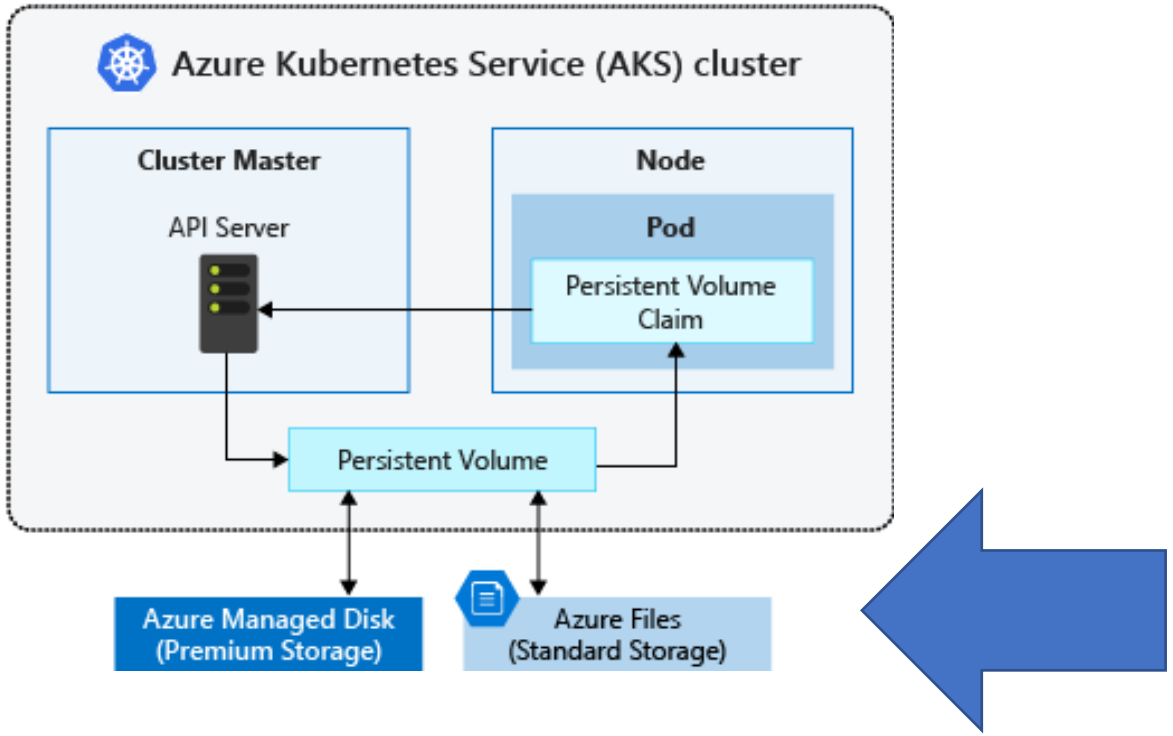
VS Code extension for warnings

- Kubernetes VS Code extension adding warnings for resource request/limits

```
35      containers:
36        - image: itowlson/biscuit2:latest
37          imagePullPolicy: Always
38          name: biscuit2
39  No CPU limit specified for this container - this could starve o
40  ther processes
41              memory: 12345
```

Storage

AKS Persistent Volumes



- You can use AAD-based access to Azure Files
- Managed Disks encrypted with Storage Service Encryption

https://docs.microsoft.com/mt-mt/azure/aks/concepts-storage

Persistent Volumes

- Dynamic Azure Disks
- Static Azure Disks
- Dynamic Azure Files
- Static Azure Files
- Disks are ReadWriteOnce, Files are ReadWriteMany
- Only Disks support Premium storage
- Faster disk attachment: https://github.com/khenidak/dysk

```
$ kubectl get sc

NAME                    PROVISIONER                    AGE
default (default)       kubernetes.io/azure-disk       1h
managed-premium         kubernetes.io/azure-disk       1h
```

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: azure-managed-disk
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: managed-premium
  resources:
    requests:
      storage: 5Gi
```

Azure Premium SSD Managed Disks specs

	P4	P6	P10	P15	P20	P30	P40	P50	P60 (PREVIEW)*	P70 (PREVIEW)*	P80 (PREVIEW)*
Disk Size	32 GiB	64 GiB	128 GiB	256 GiB	512 GiB	1 TiB	2 TiB	4 TiB	8 TiB	16 TiB	32 TiB (32767 GiB)
Price per month	$5.81	$11.23	$21.68	$41.82	$80.54	$148.68	$284.94	$545.10	$520.32	$991.09	$1,982.18
IOPS per disk	120	240	500	1,100	2,300	5,000	7,500	7,500	12,500	15,000	20,000
Throughput per disk	25 MB/second	50 MB/second	100 MB/second	125 MB/second	150 MB/second	200 MB/second	250 MB/second	250 MB/second	480 MB/second	750 MB/second	750 MB/second

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

Verify your VM size

Size	vCPU	Memory: GiB	Temp storage (SSD) GiB	Max data disks	Max cached and temp storage throughput: IOPS / MBps (cache size in GiB)	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
Standard_E2s_v3	2	16	32	4	4,000 / 32 (50)	3,200 / 48	2 / 1,000
Standard_E4s_v3 [2]	4	32	64	8	8,000 / 64 (100)	6,400 / 96	2 / 2,000
Standard_E8s_v3 [2]	8	64	128	16	16,000 / 128 (200)	12,800 / 192	4 / 4,000
Standard_E16s_v3 [2]	16	128	256	32	32,000 / 256 (400)	25,600 / 384	8 / 8,000
Standard_E20s_v3 [2]	20	160	320	32	40,000 / 320 (400)	32,000 / 480	8 / 10,000
Standard_E32s_v3 [2]	32	256	512	32	64,000 / 512 (800)	51,200 / 768	8 / 16,000
Standard_E64s_v3 [2]	64	432	864	32	128,000/1024 (1600)	80,000 / 1200	8 / 30,000
Standard_E64is_v3 [3]	64	432	864	32	128,000/1024 (1600)	80,000 / 1200	8 / 30,000

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

Backups with Heptio Ark

- https://heptio.github.io/ark/v0.10.0/
- Complete backup including resource definitions and persistent volumes
- Azure Disks supported natively, Azure Files supported over restic

Leveraging Azure managed databases

- Great way to keep your containers stateless
- Leverage the embedded HA/DR capabilities of Azure DBaaS offerings…
- …as well as security, scalability, etc

Azure SQL Database
Managed relational SQL Database as a service

Azure Cosmos DB
Globally distributed, multi-model database for any scale

SQL Data Warehouse
Elastic data warehouse as a service with enterprise-class features

Data Factory
Orchestrate and manage data transformation and movement

Redis Cache
Power applications with high-throughput, low-latency data access

SQL Server Stretch Database
Dynamically stretch on-premises SQL Server databases to Azure

SQL Server on Virtual Machines
Host enterprise SQL Server apps in the cloud

Table Storage
NoSQL key-value store using semi-structured datasets

Azure Database for PostgreSQL
Managed PostgreSQL database service for app developers

Azure Database for MySQL
Managed MySQL database service for app developers

Azure Database for MariaDB
Managed MariaDB database service for app developers

Azure Database Migration Service
Reduce the complexity of your cloud migration

Networking

AKS Basic Networking

- Done using **Kubenet** network plugin and has the following features
  - Nodes and Pods are placed on **different** IP subnets
  - User Defined Routing and IP Forwarding is for connectivity between Pods across Nodes.

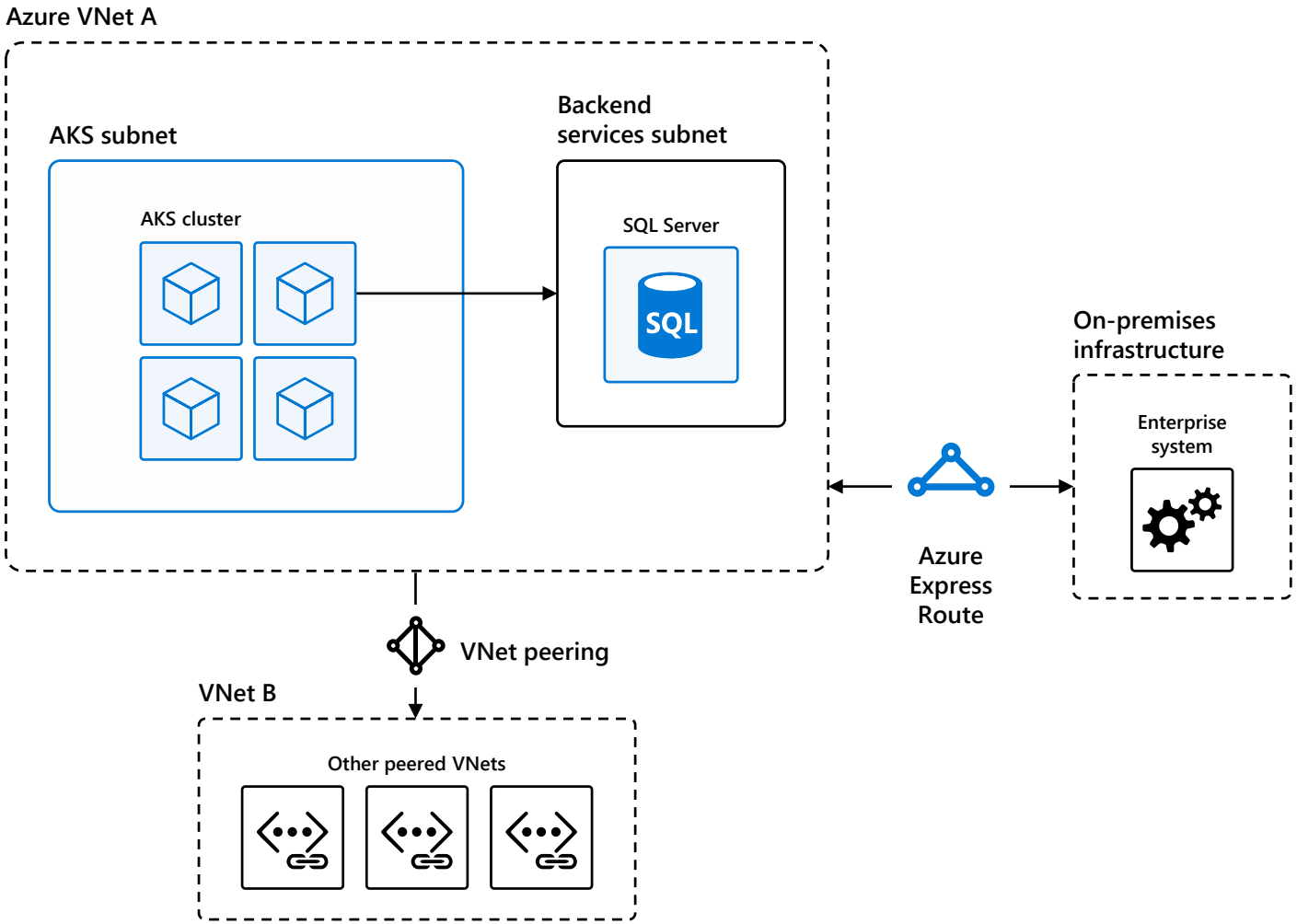
- Drawbacks
  - 2 different IP CIDRs to manage
  - Performance impact
  - Peering or On-Premise connectivity is hard to achieve

AKS Advanced Networking

- Done using the Azure CNI (Container Networking Interface)
  - **CNI** is a vendor-neutral protocol, used by container runtimes to make requests to Networking Providers
  - **Azure CNI** is an implementation which allows you to integrate Kubernetes with your VNET

- Advantages
  - Single IP CIDR to manage
  - Better Performance
  - Peering and On-Premise connectivity is out of the box
  - Network Policy coming soon to Azure CNI plugin on AKS, already available in acs-engine! (https://github.com/Azure/azure-container-networking/)

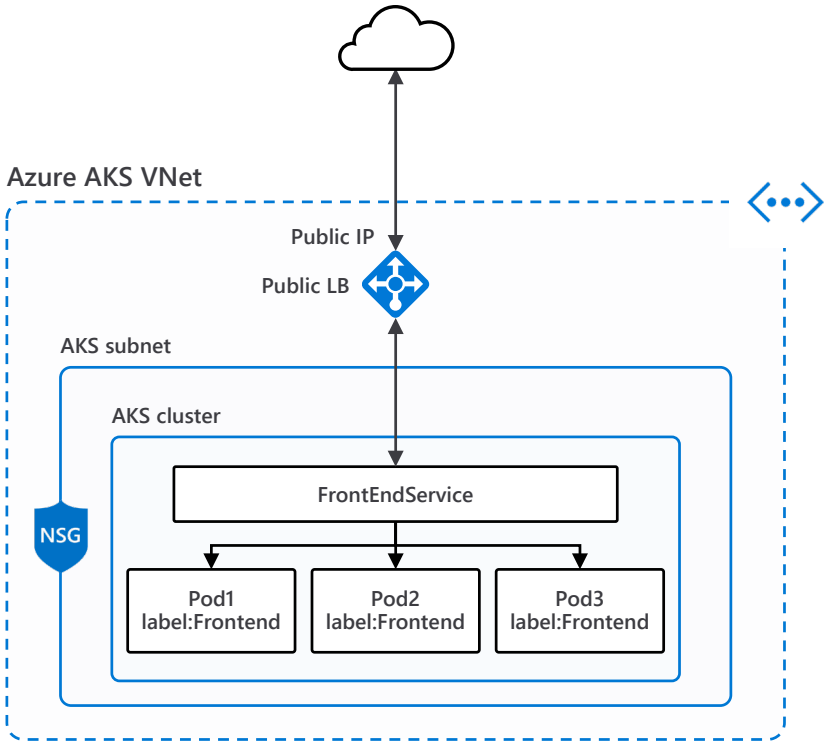
AKS with Advanced Networking



Public Service

- Service Type LoadBalancer
- Basic Layer4 Load Balancing (TCP/UDP)
- Each service as assigned an IP on the ALB (Azure Load Balancer)

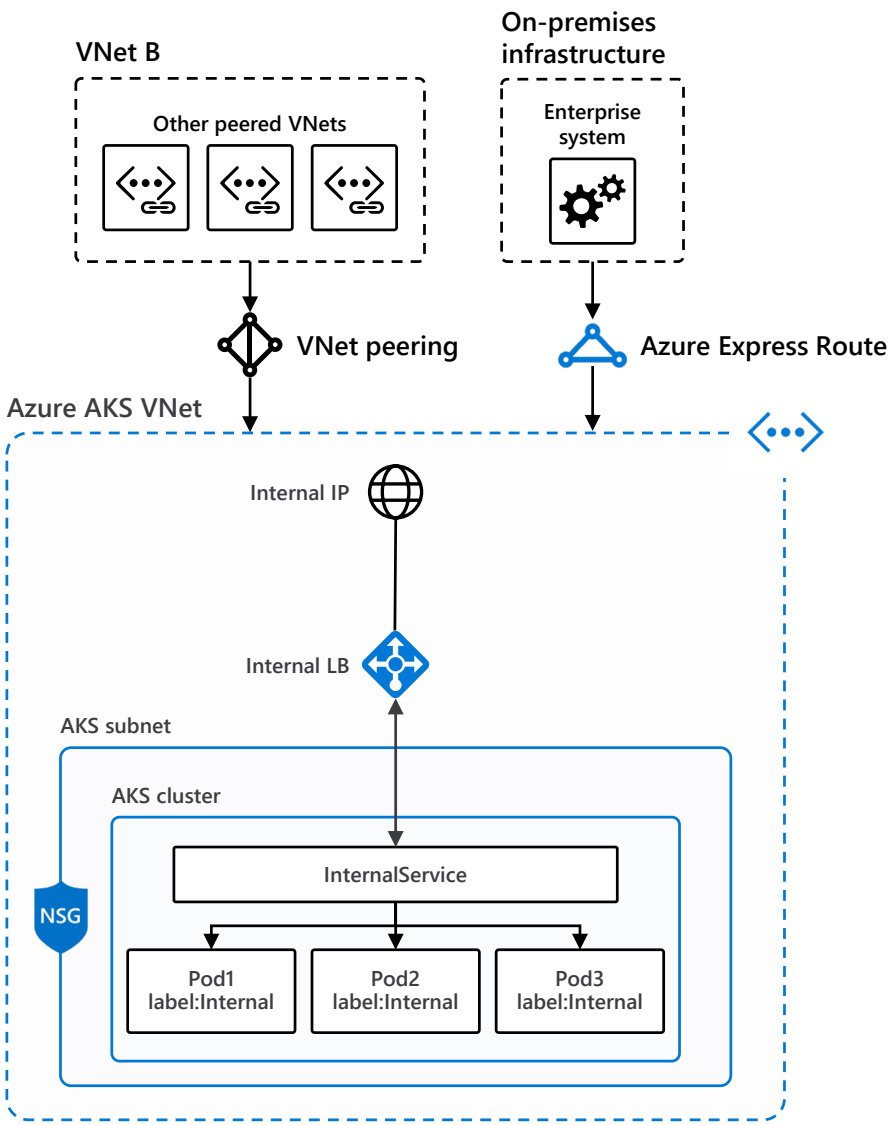
```yaml
apiVersion: v1
kind: Service
metadata:
  name: frontendservice
spec:
  loadBalancerIP: X.X.X.X
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: frontend
```



Internal Service

- Used for internal services that should be accessed by other VNETs or On-Premise only

```yaml
apiVersion: v1
kind: Service
metadata:
  name: internalservice
  annotations:
    service.beta.kubernetes.io/azure-load-balancer-internal:
"true"
spec:
   type: LoadBalancer
   loadBalancerIP: 10.240.0.25
   ports:
   - port: 80
   selector:
    app: internal
```



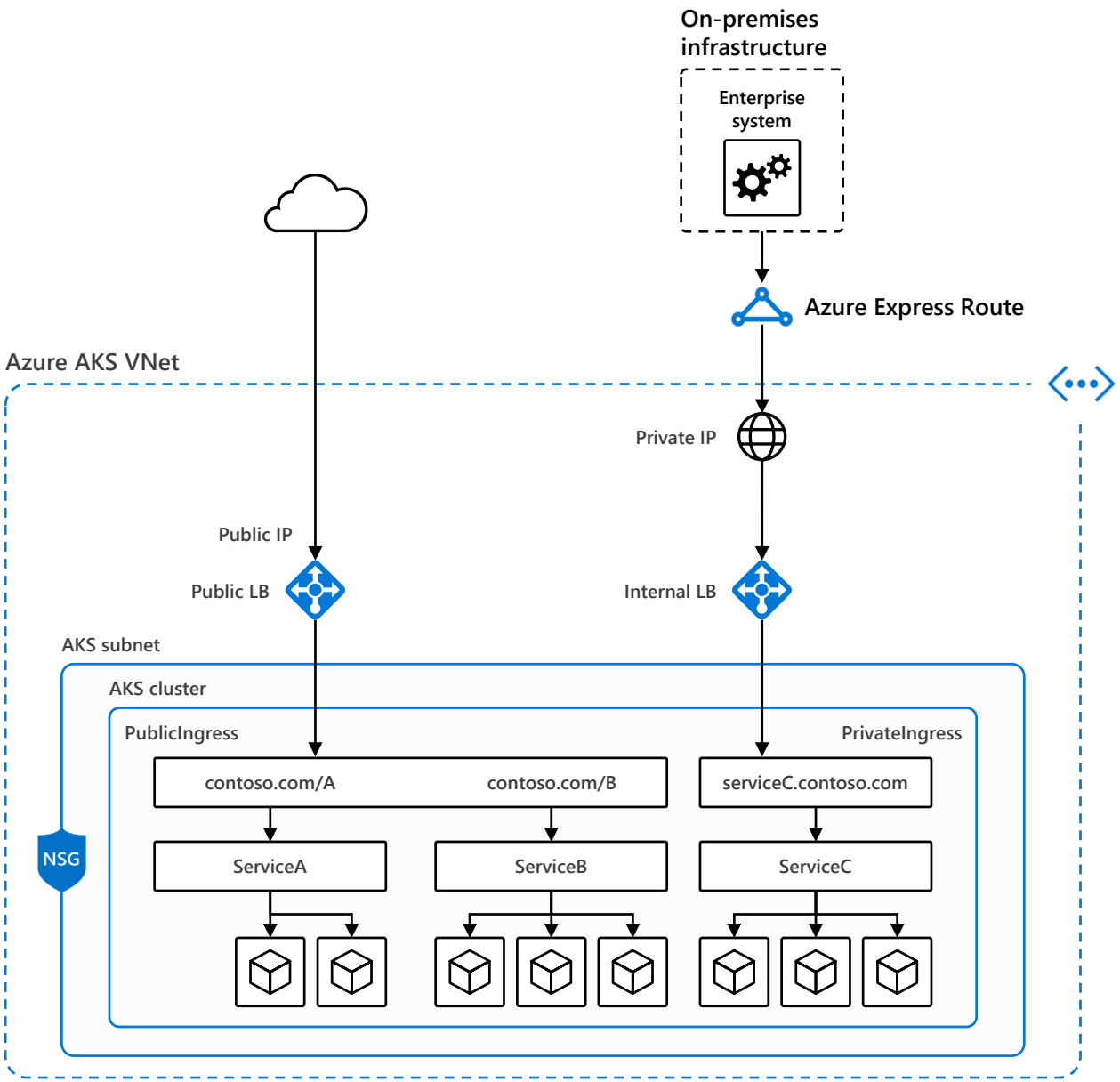
Ingress and Ingress Controllers

- **Ingress** is a Kubernetes API that manages external access to the services in the cluster
  - Supports HTTP and HTTPs
  - Path and Subdomain based routing
  - SSL Termination
  - Save on public Ips

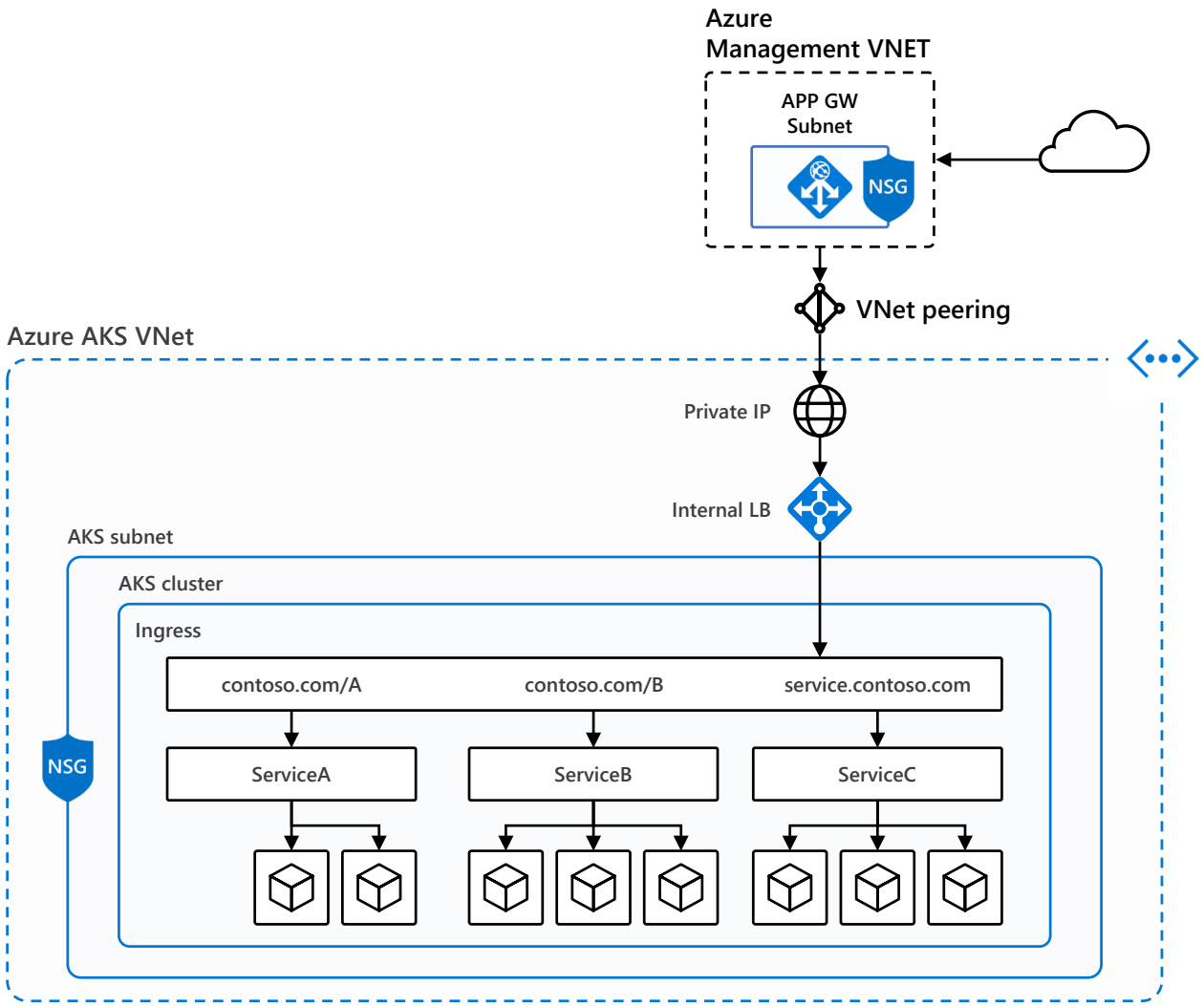
- **Ingress controller** is a daemon, deployed as a Kubernetes Pod, that watches the Ingress Endpoint for updates. Its job is to satisfy requests for ingresses. Most popular one being **Nginx**.

Ingress

```yaml
kind: Ingress
metadata:
 name: contoso-ingress
  annotations: kubernetes.io/ingress.class:
”PublicIngress"
spec:
 tls:
 - hosts:
  - contoso.com
  secretName: contoso-secret
 rules:
  - host: contoso.com
   http:
    paths:
    - path: /a
     backend:
      serviceName: servicea
      servicePort: 80
    - path: /b
     backend:
      serviceName: serviceb
      servicePort: 80
```

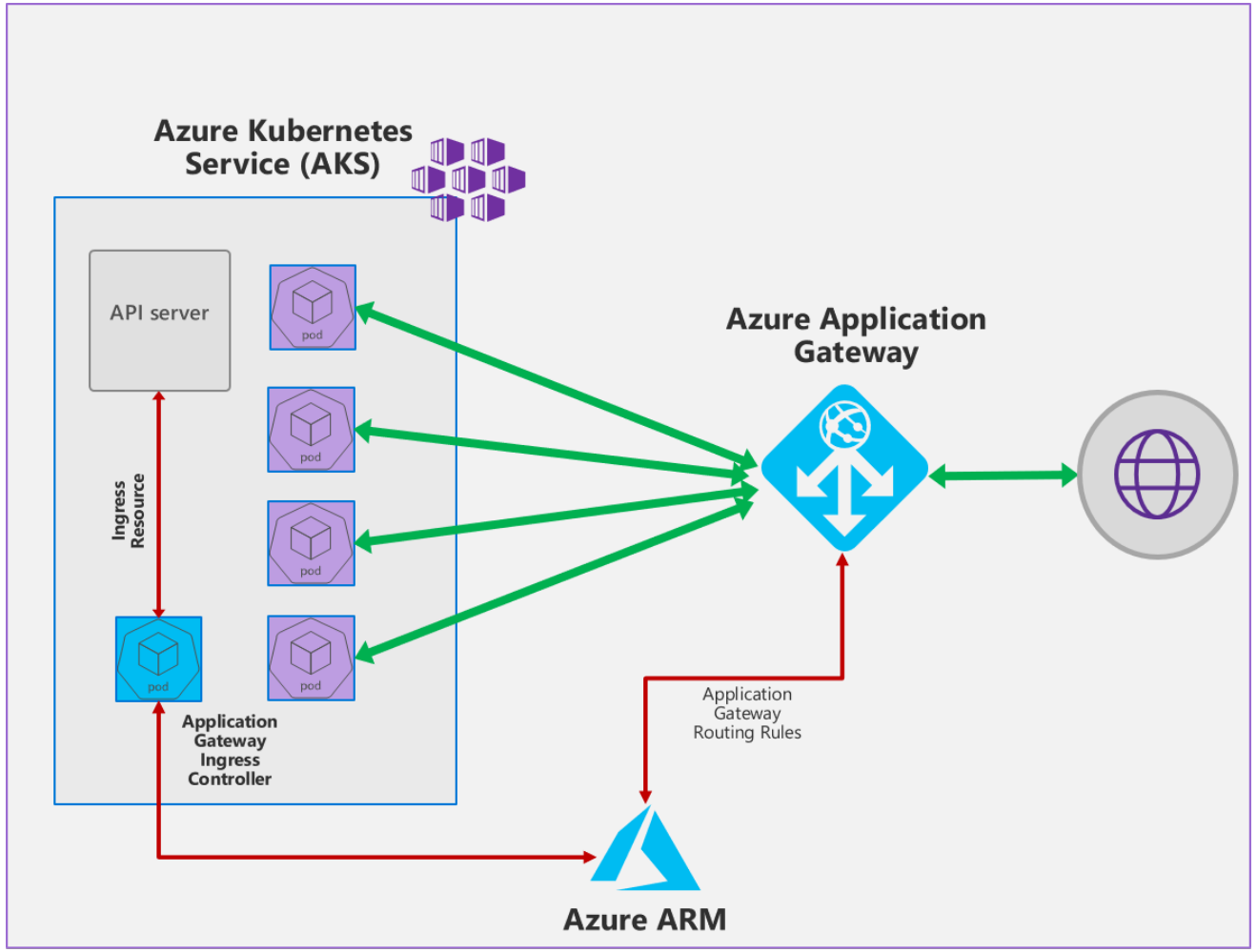


Securing Kubernetes Services with a WAF

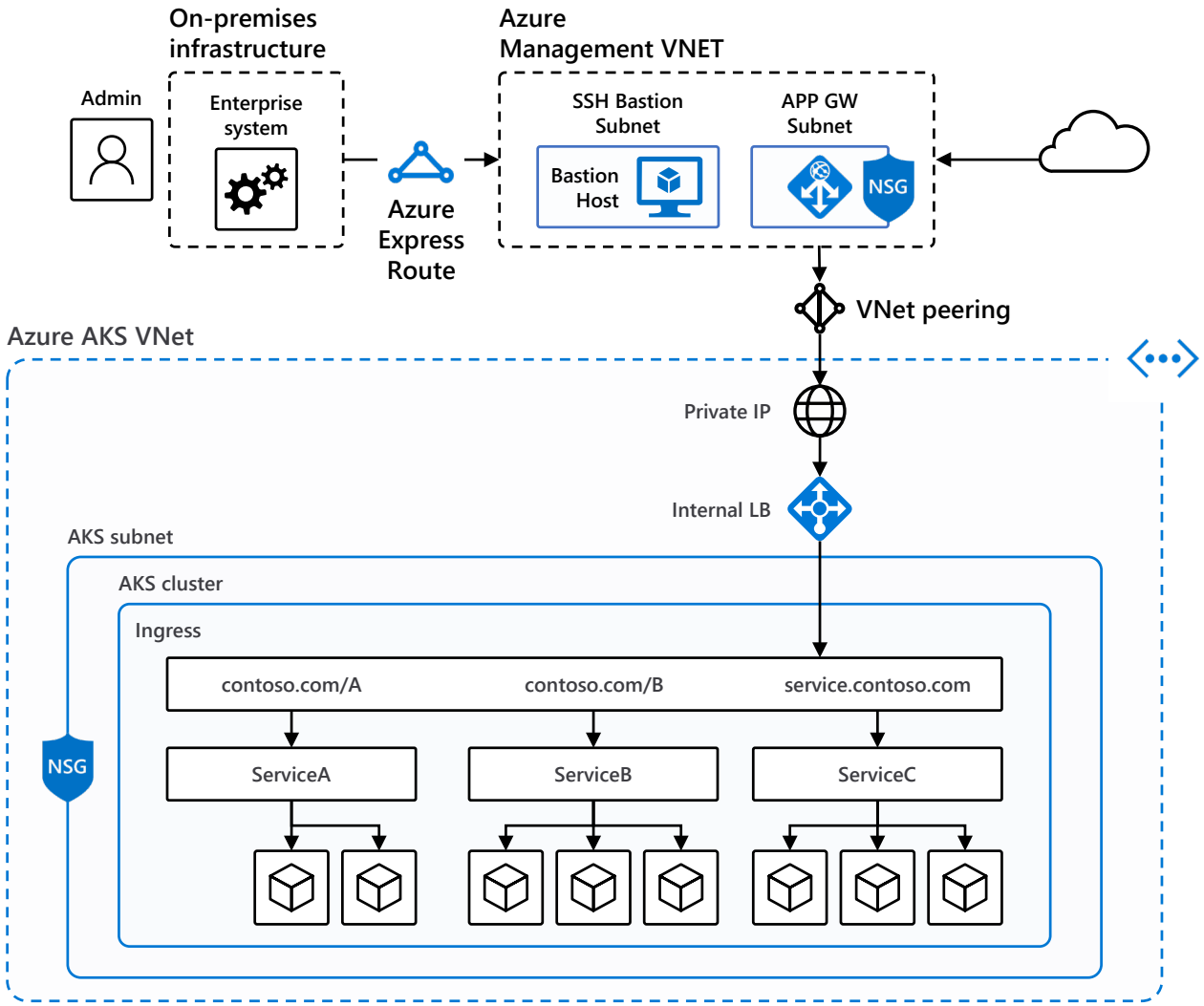


Azure Application Gateway Ingress Controller

- Alternatively deploy an Azure Application Gateway with an ingress controller
- https://azure.github.io/application-gateway-kubernetes-ingress/



Cluster Management Through Bastion Host



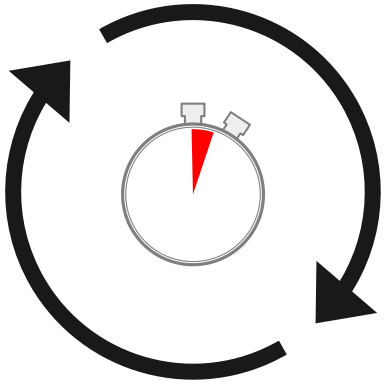
Tip: deploy SSH keys at creation time, and store them in a KMS such as Azure Key Vault

Network Policies

Network policies

Label-based

Declarative



Dynamic

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
    ports:
    - protocol: TCP
      port: 6379
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
```

https://kubernetes.io/docs/concepts/services-networking/network-policies/

A Network Security Stack for Azure Kubernetes Service

Tigera Secure Enterprise

Controls, Compliance, & Visibility

Tigera Calico

Industry standard for Network Policy, integrates with Istio for multi-factor auth

Azure CNI

Azure-native VNET Networking

Calico already available in acs-engine: https://github.com/Azure/acs-engine/blob/master/docs/kubernetes/features.md

Securing your environment

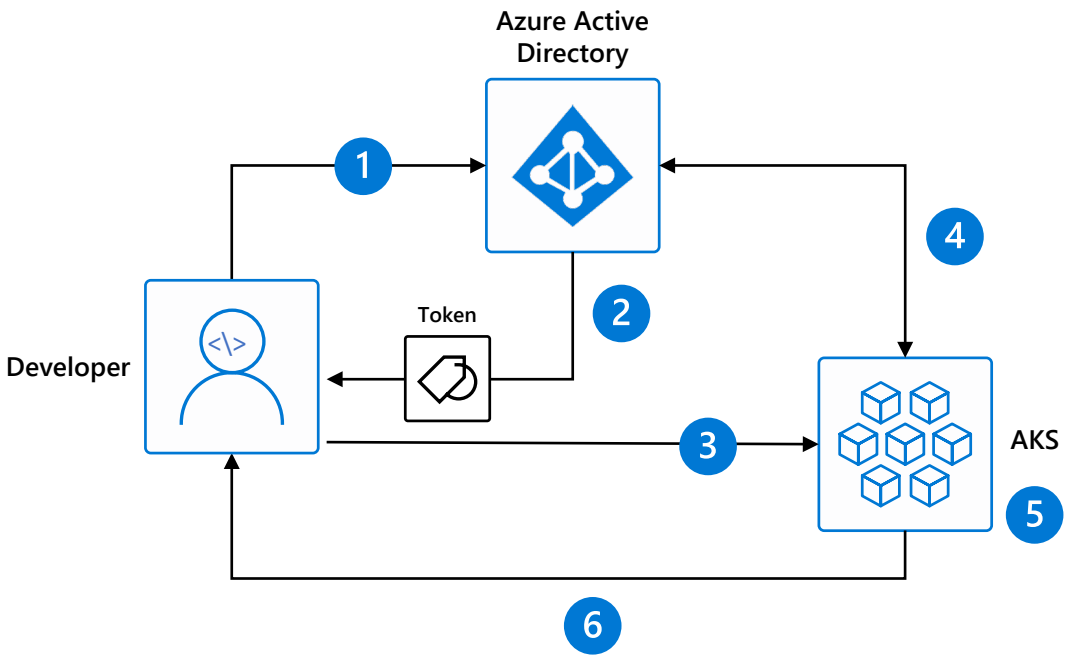
Cluster Level Security

Cluster Level Security

- Securing endpoints for API server and cluster nodes
  - Ensuring authentication and authorization (AAD + RBAC)
  - Setting up & keeping least privileged access for common tasks

Cluster Level - Identity and Access Management through AAD and RBAC

1. Kubernetes Developer authenticates with AAD
2. The AAD token issuance endpoint issues the access token
3. Developer performs action w/ AAD token.
   Eg. *kubectl create pod*
4. Kubernetes validates token with AAD and fetches the Developer's AAD Groups
   Eg. Dev Team A, App Group B
5. Kubernetes RBAC and cluster policies are applied
6. Request is successful or not based on the previous validation



AAD-authentication experience in AKS (non admin user)

```
$ az aks get-credentials --resource-group myAKSCluster --name myAKSCluster

$ kubectl get nodes

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and
enter the code BUJHWDGNL to authenticate.

NAME                        STATUS    ROLES     AGE       VERSION
aks-nodepool1-42032720-0    Ready     agent     1h        v1.9.6
aks-nodepool1-42032720-1    Ready     agent     1h        v1.9.6
aks-nodepool1-42032720-2    Ready     agent     1h        v1.9.6
```

Or

```
Error from server (Forbidden): nodes is forbidden: User baduser@contoso.com cannot
list nodes at the cluster scope
```

Provisioning AD-enabled AKS (admin user)

```
$ az aks create --resource-group myAKSCluster --name myAKSCluster --generate-ssh-keys \
  --aad-server-app-id <Azure AD Server App ID> \
  --aad-server-app-secret <Azure AD Server App Secret> \
  --aad-client-app-id <Azure AD Client App ID> \
  --aad-tenant-id <Azure AD Tenant>
```

```
$ az aks get-credentials --resource-group myAKSCluster –name  myAKSCluster --admin
Merged "myCluster" as current context ..
```

```
$ kubectl get nodes

NAME                        STATUS    ROLES     AGE       VERSION
aks-nodepool1-42032720-0    Ready     agent     1h        v1.9.6
aks-nodepool1-42032720-1    Ready     agent     1h        v1.9.6
aks-nodepool1-42032720-2    Ready     agent     1h        v1.9.6
```

https://docs.microsoft.com/en-us/azure/aks/aad-integration

Provisioning AD-enabled AKS (admin user)

Setting up a Cluster Role

```yaml
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: ClusterRole
metadata:
  labels:
   kubernetes.io/cluster-service: "true"
  name: cluster-admin
rules:
- apiGroups:
  - extensions
  - apps
  resources:
  - deployments
  verbs:
  - get
  - list
  - watch
  - update
  - patch
- apiGroups:
  - ""
  resources:
  - events
  - namespaces
  - nodes
  - pods
  verbs:
  - get
  - list
  - watch
```

Bind the Cluster Role to a user

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: contoso-cluster-admins
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
kind: User
name: "user@contoso.com"
```

Bind the Cluster Role to a group

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: contoso-cluster-admins
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
kind: Group
name: "894656e1-39f8-4bfe-b16a-510f61af6f41"
```

Cluster Level Security

- Securing endpoints for API server and cluster nodes
  - Ensuring authentication and authorization (AAD + RBAC)
  - Setting up & keeping least privileged access for common tasks
  - Admission Controllers
    - *NamespaceLifecycle*
    - *LimitRanger*
    - *ServiceAccount*
    - *DefaultStorageClass*
    - *DefaultTolerationSeconds*
    - *MutatingAdmissionWebhook*
    - *ValidatingAdmissionWebhook*
    - *ResourceQuota*
    - *DenyEscalatingExec*
    - *AlwaysPullImages*

- Coming soon:
  - NodeRestriction
  - PodSecurityPolicy

https://docs.microsoft.com/en-us/azure/aks/faq#what-kubernetes-admission-controllers-does-aks-support-can-admission-controllers-be-added-or-removed

ValidatingAdmissionWebhook

```yaml
apiVersion: admissionregistration.k8s.io/v1beta1
kind: ValidatingWebhookConfiguration
metadata:
  name: denyuntrustedreg
webHooks:
  - name: denyregistry.palma.sh
    rules:
      - apiGroups:
          - ""
        apiVersions:
          - v1
        operations:
          - CREATE
        resources:
          - pods
    failurePolicy: Fail
    clientConfig:
      url:
“https://denyregistry.azurewebsites.net/api/HttpTriggerJS1?code=NeZuU87adO
ayXyoTWphGECUJj7cAi4PDyaG8oDEGzWeZAU63mnvX6Q==&name=Ignite"
```

MutatingAdmissionWebhook

```yaml
apiVersion: admissionregistration.k8s.io/v1beta1
kind: MutatingWebhookConfiguration
metadata:
  name: label-injector-webhook-cfg
  labels:
    app: label-injector
webhooks:
  - name: label-injector.palma.sh
    clientConfig:
      service:
        name: label-injector-webhook-svc
        namespace: default
        path: "/mutate"
      caBundle: ${CA_BUNDLE}
    rules:
      - operations: [ "CREATE" ]
        resources: ["pods"]
        apiGroups: [""]
        apiVersions: ["v1"]
    namespaceSelector:
      matchLabels:
        label-injector: enabled
```

Cluster Level – Nodes, Upgrade and Patches

- Regular maintenance, security and cleanup tasks
  - Maintain, update and upgrade hosts and kubernetes
  - Monthly ideal, 3 months minimum
  - Security patches
    - AKS automatically applies security patches to the nodes on a nightly schedule
    - You're responsible to reboot as required
    - Kured DaemonSet: https://github.com/weaveworks/kured

Upgrade to version 1.10.6

```
$ az aks upgrade --name myAKSCluster \
--resource-group myResourceGroup \
--kubernetes-version 1.10.6
```

- **SSH Access**
  - DenyEscalatingExec
- **Running benchmarks and tests to validate cluster setup**
  - Kube-bench
  - Aqua Hunter
  - Others

https://docs.microsoft.com/en-us/azure/aks/faq#are-security-updates-applied-to-aks-agent-nodes
https://docs.microsoft.com/en-us/azure/aks/node-updates-kured

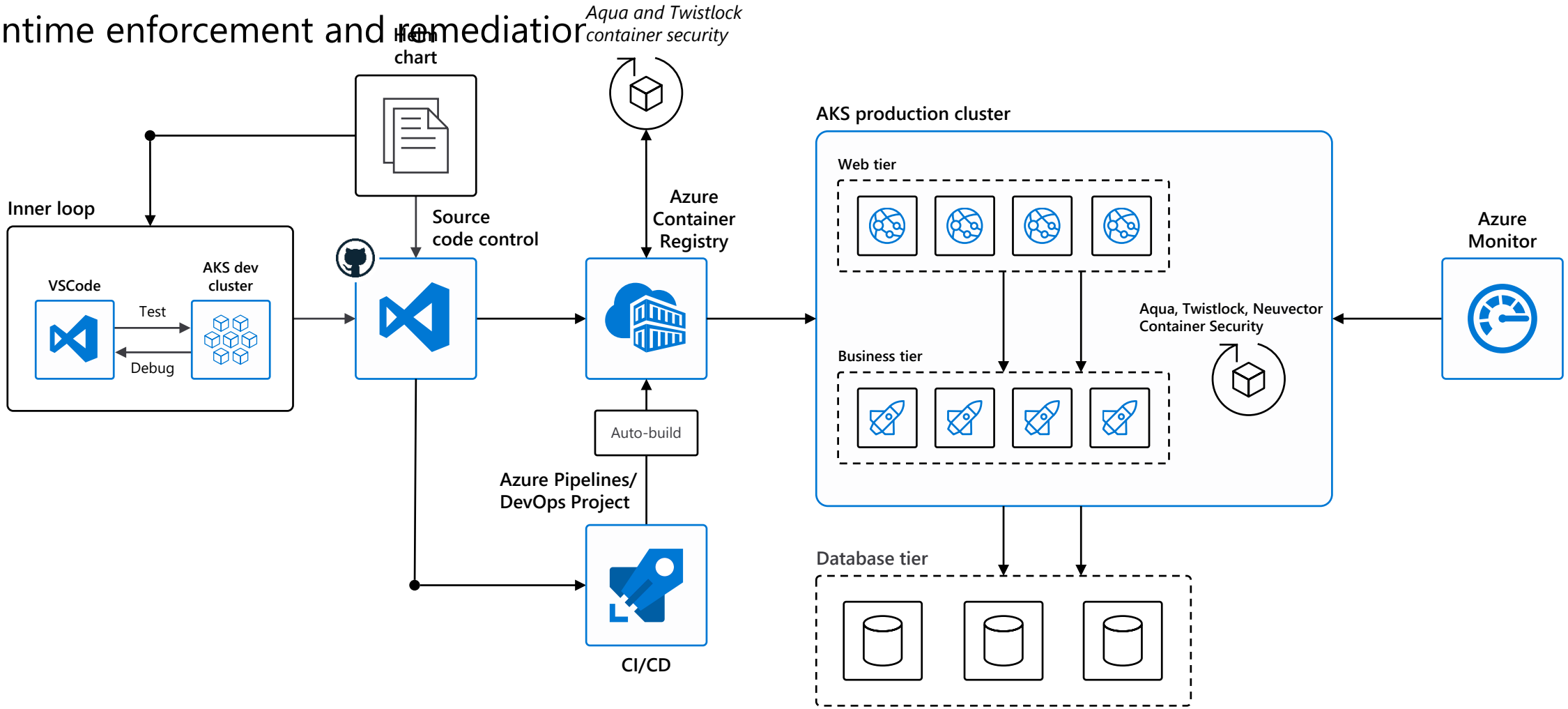
Container Level Security and Isolation

Container Level – The images

- Trusted Registry
- Regularly apply security updates to the container images

Container Level – Images and Runtime

- Scan your images, scan your containers
- Runtime enforcement and remediation



Container Level – The access

- Avoid access to HOST IPC namespace - only if absolutely necessary
- Avoid access to Host PID namespace - only if absolutely necessary
- Avoid root / privileged access
    - Consider Linux Capabilities

Container Level – apparmor profiles

```
$ kubectl exec hello-apparmor touch /tmp/test

touch: /tmp/test: Permission denied
error: error executing remote command: command terminated with non-zero exit
code: Error executing in Docker Container: 1
```

Container Level – seccomp profiles

```
$ kubectl create -f seccomp-pod.yaml
pod "chmod-prevented" created

$ kubectl get pods
NAME                    READY       STATUS      RESTARTS    AGE
chmod-prevented         0/1         Error       0           8s
```

Pod Level Security

Pod Level – Pod Security Context

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    runAsUser: 1000
    fsGroup: 2000
  volumes:
  - name: sec-ctx-vol
    emptyDir: {}
  containers:
  - name: sec-ctx-demo
    image: ignite.azurecr.io/nginx-demo
    volumeMounts:
    - name: sec-ctx-vol
      mountPath: /data/demo
    securityContext:
      runAsUser: 2000
      allowPrivilegeEscalation: false
      capabilities:
        add: ["NET_ADMIN", "SYS_TIME"]
      seLinuxOptions:
        level: "s0:c123,c456"
```

https://kubernetes.io/docs/tasks/configure-pod-container/security-context/

Pod Level – Pod Security Policies

Coming soon!

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: restricted
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: 'docker/default’
    apparmor.security.beta.kubernetes.io/allowedProfileNames: 'runtime/default’
    seccomp.security.alpha.kubernetes.io/defaultProfileName: 'docker/default’
    apparmor.security.beta.kubernetes.io/defaultProfileName: 'runtime/default’
spec:
  privileged: false
  allowPrivilegeEscalation: false # Required to prevent escalations to root.
  requiredDropCapabilities: # This is redundant with non-root + disallow privilege escalation, but we can provide it for defense in depth.
    - ALL
  volumes: # Allow core volume types.
    - 'configMap’
    - 'emptyDir’
    - 'projected’
    - 'secret’
    - 'downwardAPI’
    - 'persistentVolumeClaim’ # Assume that persistentVolumes set up by the cluster admin are safe to use.
  hostNetwork: false
  hostIPC: false
  hostPID: false
  runAsUser:
    rule: 'MustRunAsNonRoot’ # Require the container to run without root privileges.
  seLinux:
    rule: 'RunAsAny’ # This policy assumes the nodes are using AppArmor rather than SELinux.
  supplementalGroups:
    rule: 'MustRunAs’
    ranges:
      - min: 1      # Forbid adding the root group.
        max: 65535
  fsGroup:
    rule: 'MustRunAs’
    ranges:
      - min: 1     # Forbid adding the root group.
        max: 65535
  readOnlyRootFilesystem: false
```

Pod level

- Pod Security Context
- Pod Security Policies
- AlwaysPull Images

Securing Workloads

Storing your secrets in Azure Key Vault

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx-flex-kv
spec:
  containers:
  - name: nginx-flex-kv
    image: nginx
    volumeMounts:
    - name: test
      mountPath: /kvmnt
      readOnly: true
  volumes:
  - name: test
    flexVolume:
      driver: "azure/kv"
      secretRef:
        name: kvcreds # k8s secret with KV credentials
      options:
        usepodidentity: "false"
        keyvaultname: "testkeyvault"
        keyvaultobjectname: "testsecret"
        keyvaultobjecttype: secret # OPTIONS: secret, key, cert
        resourcegroup: "testresourcegroup"
        subscriptionid: "testsub"
        tenantid: "testtenant"
```

https://github.com/Azure/kubernetes-keyvault-flexvol

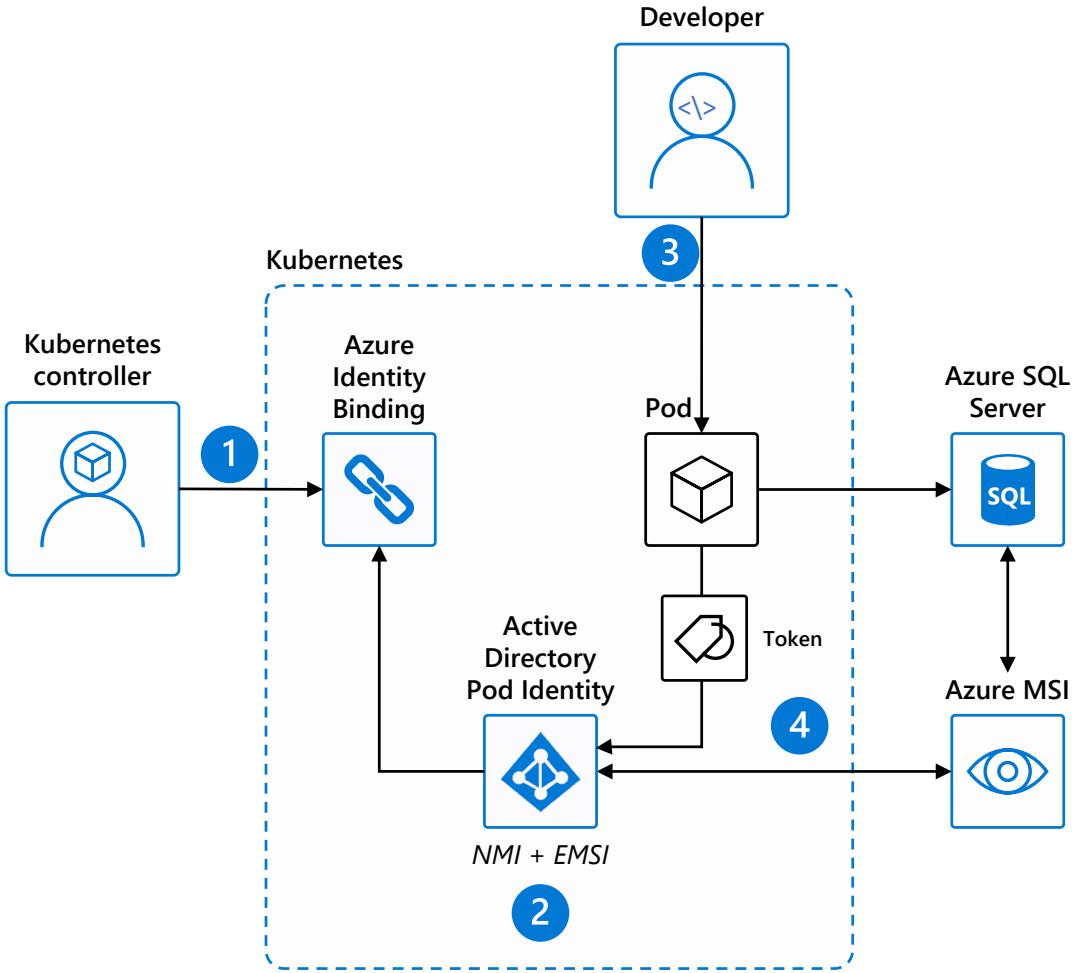
Pod Identity

1. Kubernetes operator defines an identity map for K8s service accounts

2. Node Managed Identity (NMI) watches for mapping reaction and syncs to Managed Service Identify (MSI)

3. Developer creates a pod with a service account. Pod uses standard Azure SDK to fetch a token bound to MSI

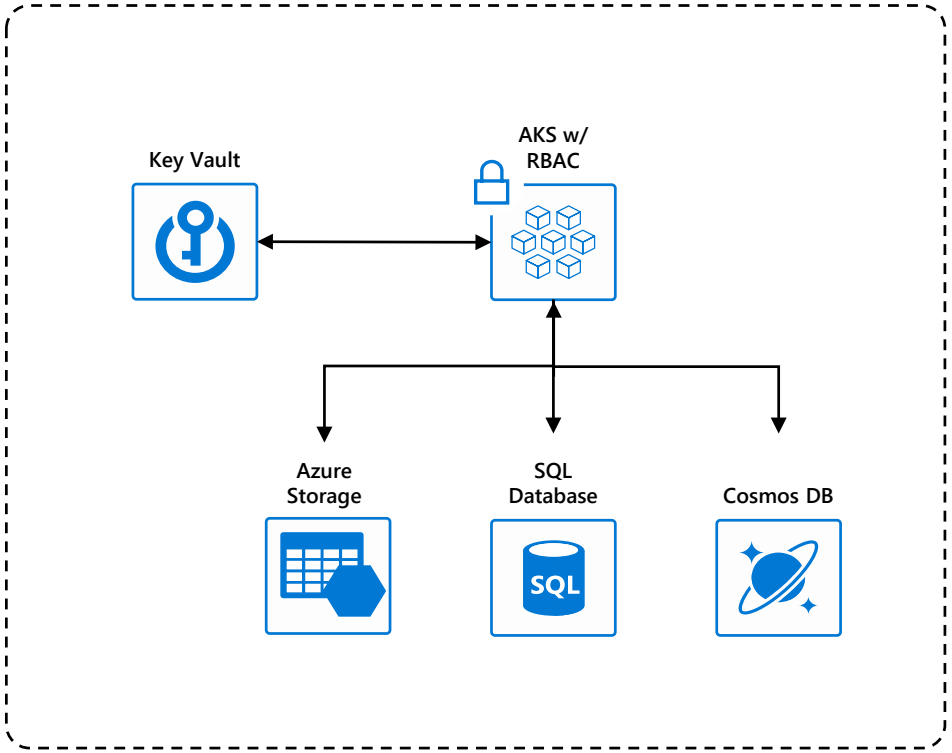
4. Pod uses access token to consume other Azure services; services validate token



https://github.com/Azure/aad-pod-identity

Securing workloads

- Managing secrets and privileged information
  - Azure Key Vault



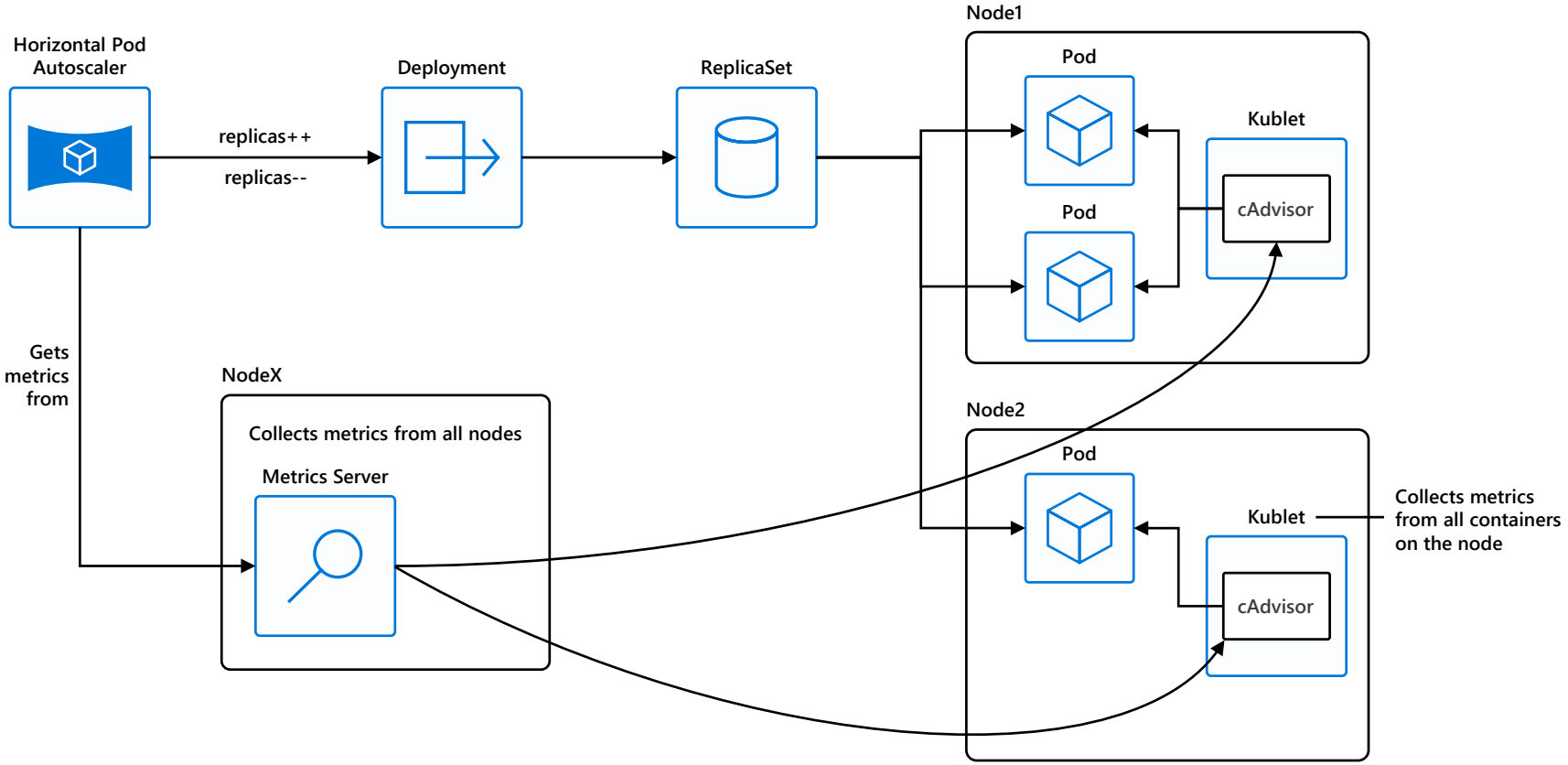
https://github.com/Azure/kubernetes-kms

Compliance

- AKS is SOC 1/2 , PCI , HIPPA and ISO certified
- All the details are listed in the Azure Trust Center

Autoscaling Applications and Clusters

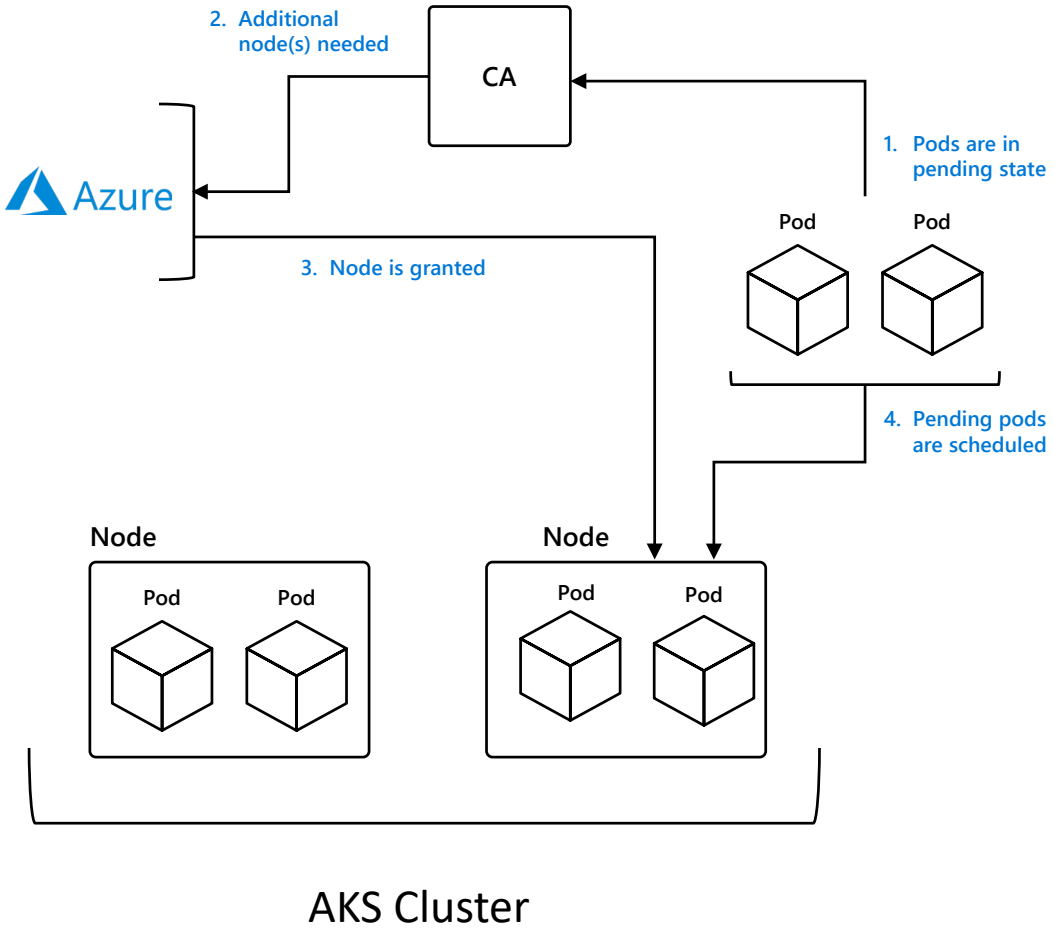
Horizontal Pod Autoscaler



https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/

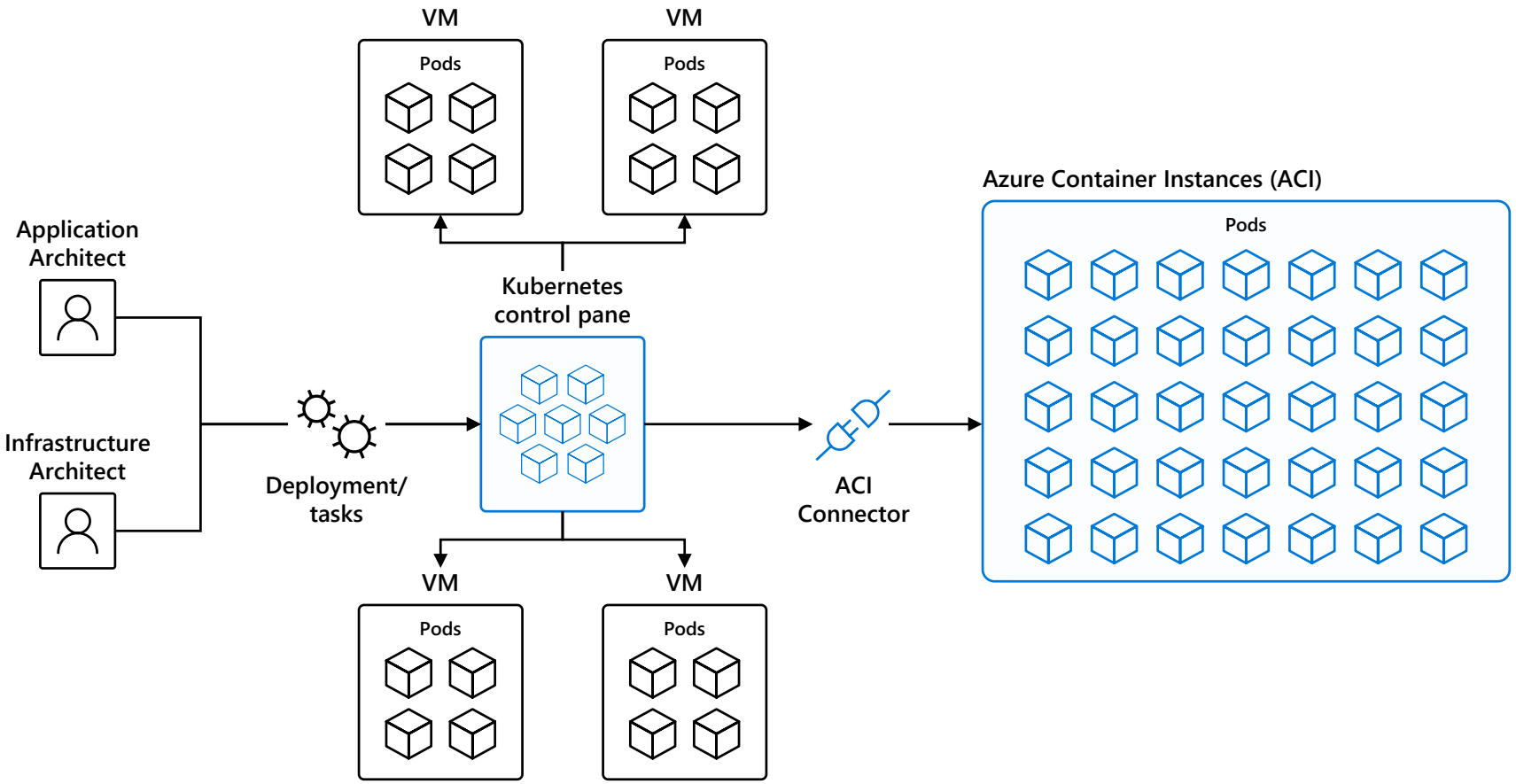
AKS Cluster Autoscaler

- Scales nodes based on pending pods
- Scale up and scale down
- Reduces dependency on monitoring
- Removes need for users to manage nodes and monitor service usage manually



https://docs.microsoft.com/en-us/azure/aks/autoscaler

Bursting with the ACI Connector/ Virtual Kubelet

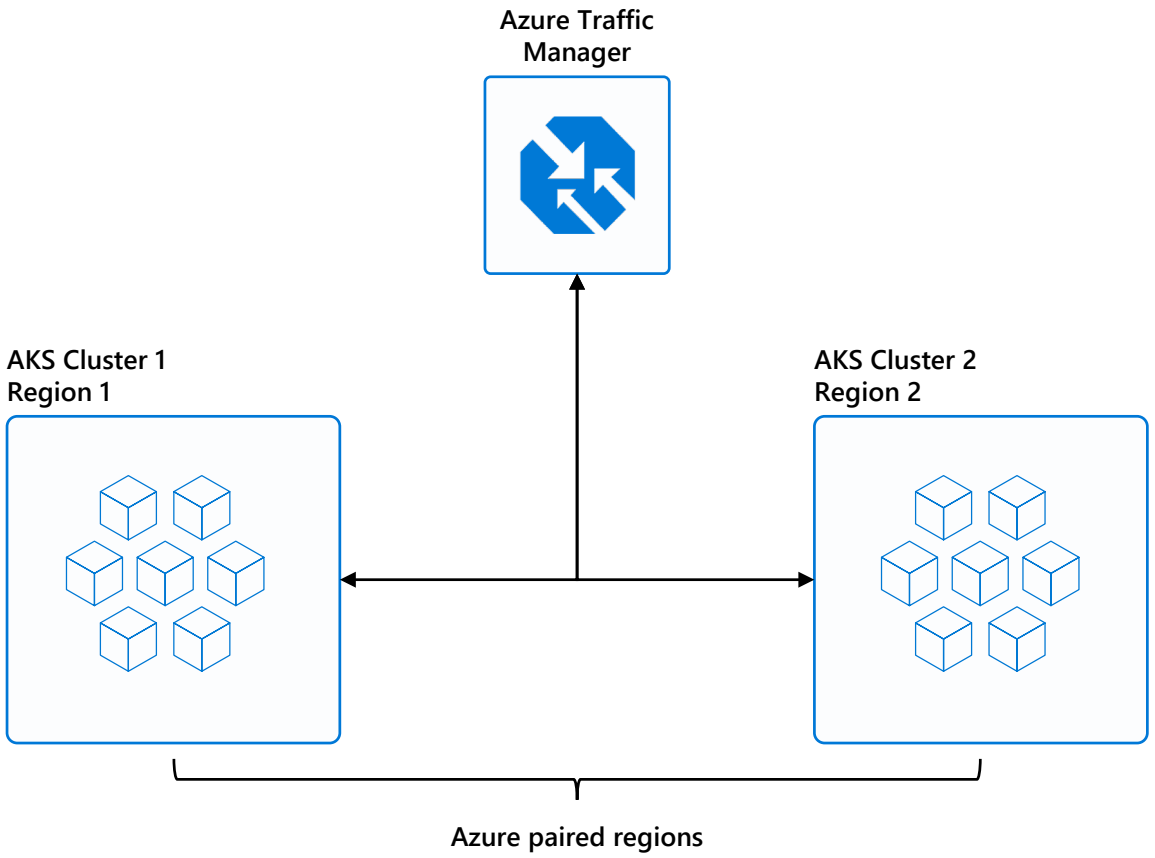


https://docs.microsoft.com/en-us/azure/aks/virtual-kubelet

Multi-Region

Multi-Region Clusters

- Minimize downtime risk
- One live region
  - Another backup
  - Or weighted traffic
- A/B testing



Logging and Monitoring

Monitoring/Logging your cluster

- Log Everything to stdout / stderr
- Key Metrics:
  - Node metrics (CPU Usage, Memory Usage, Disk Usage, Network Usage)
  - Kube_node_status_condition
  - Pod memory usage / limit; memory_failures_total
    - container_memory_working_set_bytes
  - Pod CPU usage average / limit
  - Filesystem Usage / limit
  - Network receive / transmit errors
- Azure Monitor for Containers

In the roadmap

Overview health of AKS cluster

Node event Logs

Home > Kubernetes services > monclu - Insights (preview) > Logs

Logs
defaultworkspace-5abfd9c4-ec8c-4db9-acd4-c762dce93508-cca

New Query 1* +

Help | Settings | Query explorer

defaultworkspace-5abfd9c4-ec8c-4... | Run | Time range: **Set in query** | Save | Copy link | Export | Set alert | Pin

```
let startDateTime = datetime('2018-09-15T08:30:00.000Z');
let endDateTime = datetime('2018-09-26T14:31:46.659Z');
let EmptyKubeEvents_CLTable = datatable(TimeGenerated: datetime, Name_s: string, ObjectKind_s: string,                Type_s: string, Reason_s: string, Message: string, Namespace_s:
string)[];
let KubeEvents_CLTable = union isfuzzy = true EmptyKubeEvents_CLTable, KubeEvents_CL
| where TimeGenerated >= startDateTime and TimeGenerated < endDateTime
| where ObjectKind_s =~ 'Node'
| where Name_s =~ 'aks-agentpool-41197944-0'
| project TimeGenerated, Name_s , ObjectKind_s , Type_s, Reason_s , Message , Namespace_s
| order by TimeGenerated desc;
KubeEvents_CLTable
```

Completed | 00:00:01.608 | 7 records

TABLE | CHART | Columns | Display time (UTC+00:00)

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	Name_s	ObjectKind_s	Type_s	Reason_s	Message	Namespace_s
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	Starting	Starting kubelet.	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	NodeHasSufficientDisk	Node aks-agentpool-41197944-0 status is now: NodeHasSufficientDisk	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	NodeHasSufficientMemory	Node aks-agentpool-41197944-0 status is now: NodeHasSufficientMe...	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	NodeHasNoDiskPressure	Node aks-agentpool-41197944-0 status is now: NodeHasNoDiskPressure	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	NodeHasSufficientPID	Node aks-agentpool-41197944-0 status is now: NodeHasSufficientPID	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	NodeAllocatableEnforced	Updated Node Allocatable limit across pods	
2018-09-17T19:19:28.000	aks-agentpool-41197944-0	Node	Normal	Starting	Starting kube-proxy.	

Pod usage and details

Home > Kubernetes services > monclu - Insights (preview)

monclu - Insights (preview)
Kubernetes service

TimeRange = **Last 7 days** | Add Filter

Cluster | Nodes | Controllers | Containers

Monitor resource group | Learn more | Feedback

Search by name... | Metric: CPU Usage (millicores) | Min | Avg | 50th | 90th | 95th | Max

All 44 item(s)

NAME	STATUS	95TH %	95TH	POD	NODE	RESTARTS	UPTIME	TREND 95TH % (1 BAR = 8H)
cpu-demo-ctr	Ok	50%	1001 mc	cpu-demo-679b7...	aks-agentpool-4...	0	5 days	
omsagent	Ok	11%	16 mc	omsagent-h4v6l	aks-agentpool-4...	0	8 days	
omsagent	Ok	4%	6 mc	omsagent-rs-57f...	aks-agentpool-4...	0	8 days	
tunnel-front	Ok	2%	47 mc	tunnelfront-85c6...	aks-agentpool-4...	0	8 days	
memory-demo-ctr	Ok	2%	41 mc	memory-demo	aks-agentpool-4...	0	6 days	
addon-http-application-routi...	Ok	1%	0.1 mc	addon-http-appli...	aks-agentpool-4...	0	8 days	
heapster-nanny	Ok	0.9%	0.4 mc	heapster-5457df...	aks-agentpool-4...	0	8 days	
heapster	Ok	0.8%	0.7 mc	heapster-5457df...	aks-agentpool-4...	0	8 days	
main	Ok	0.5%	0.5 mc	kubernetes-dash...	aks-agentpool-4...	0	8 days	
redirector	Ok	0.2%	4 mc	kube-svc-redirect...	aks-agentpool-4...	0	8 days	
kube-proxy	Ok	0.2%	3 mc	kube-proxy-jx6kw	aks-agentpool-4...	0	8 days	
influxdb	Ok	0.2%	3 mc	influxdb-jmeter-...	aks-agentpool-4...	0	8 days	
azureproxy	Ok	0.2%	3 mc	kube-svc-redirect...	aks-agentpool-4...	0	8 days	

View container logs

Container Name
cpu-demo-ctr

Container ID
ac13d52d72eb0d348006804787e42d6dffe6ce08ef9d99131836274974d23b61

Container Status
running

Image
stress

Image Tag
latest

Container Creation Time Stamp
9/20/2018, 1:48:58 PM

Start Time
9/20/2018, 1:48:58 PM

Finish Time
-

CPU Limit
2000 mc

CPU Request
1000 mc

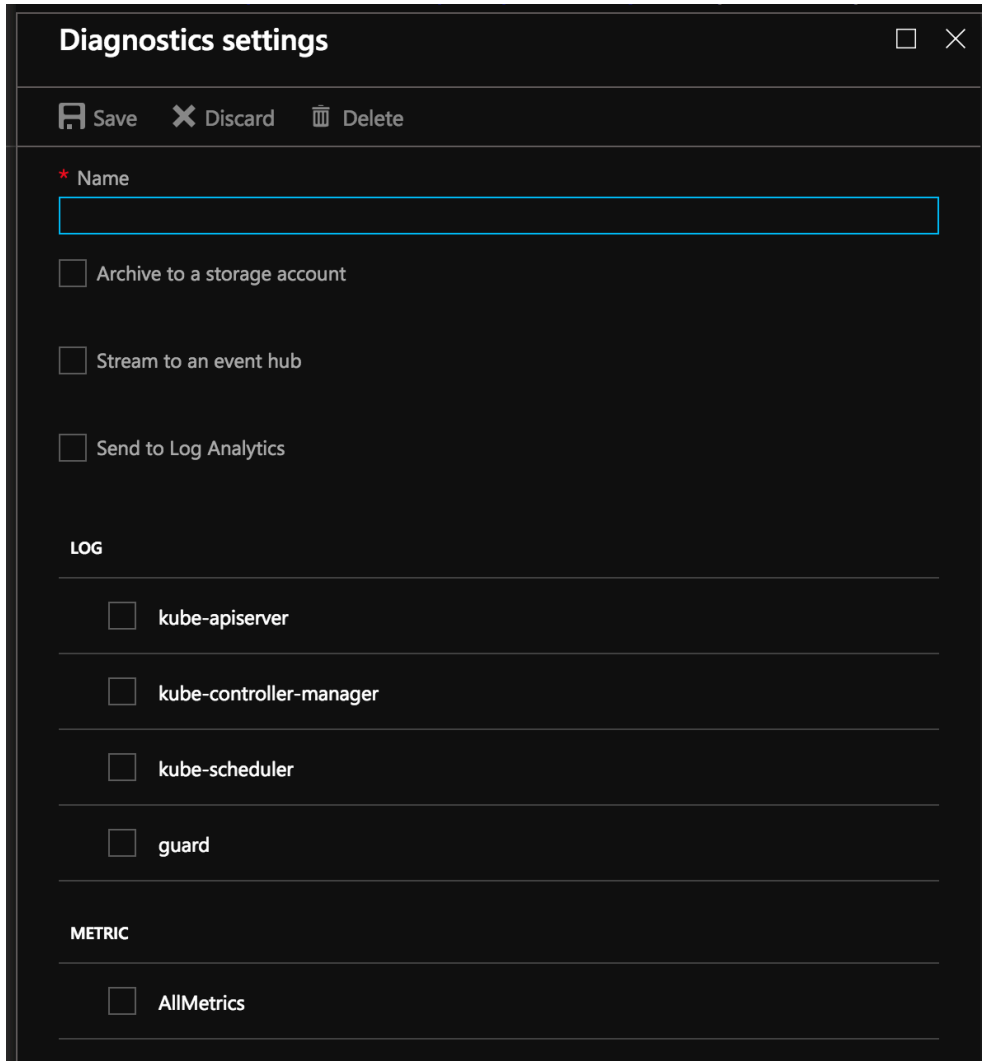
Memory Limit
5.31 GB

Memory Request
0 KB

Environment Variables

Customer control plane logs

- Use the Azure portal to enable diagnostics logs
- Pipe logs to log analytics, event hub or a storage account
- Metrics available today
  - Kube-controller-manager
  - Kube-api-server
  - Kube-scheduler
  - Audit logs on the roadmap



Example control plane logs

monclu - Logs
Kubernetes service

New Query 1*

Help Settings Query explorer

defaultworkspace-5abfd9c4-ec8c-4... Run Time range: **Last 24 hours** Save Copy link Export Set alert Pin

```
AzureDiagnostics
| where Category == "kube-controller-manager"
| where log_s contains "my-nginx"
| project log_s
```

Completed. Showing results from the last 24 hours. 00:00:01.117 11 records

TABLE CHART Columns

Drag a column header and drop it here to group by that column

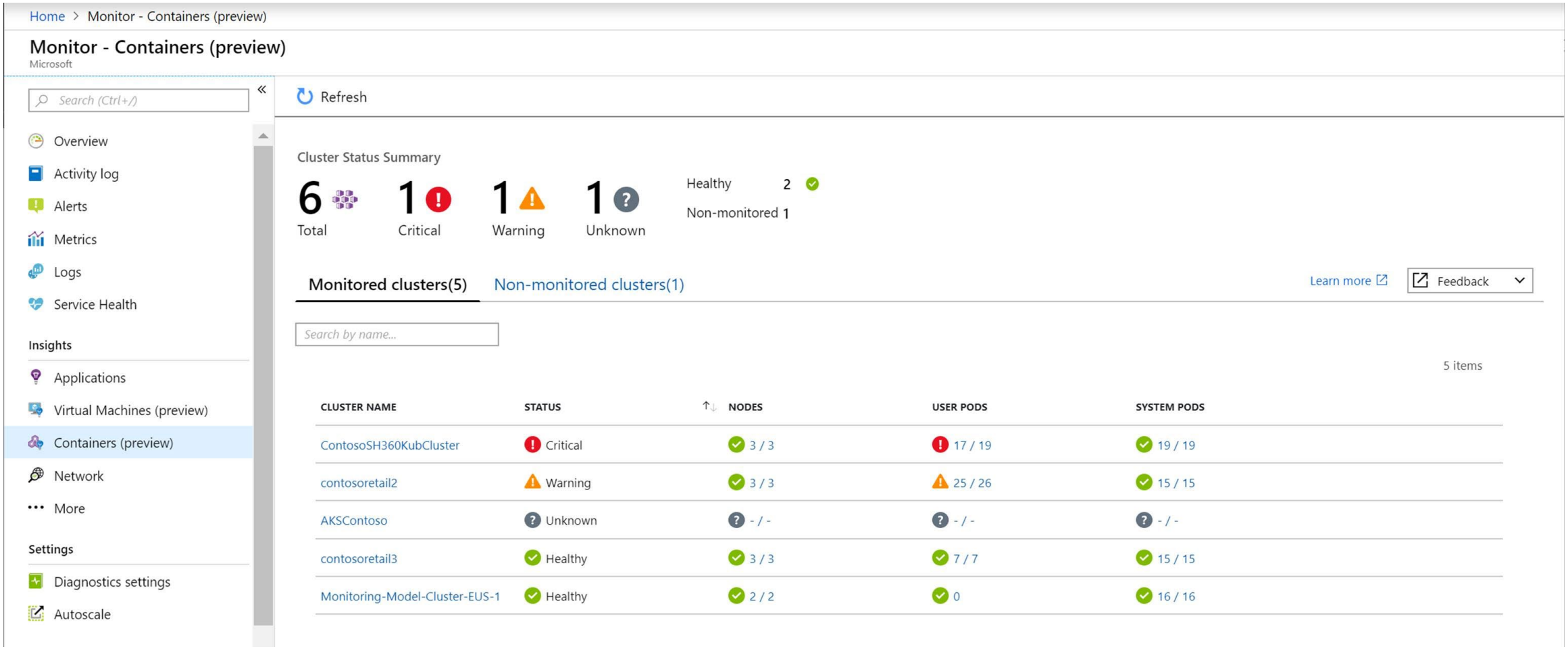
log_s

```
I0919 03:26:57.353133 1 event.go:221] Event(v1.ObjectReference{Kind:"Deployment", Namespace:"default", Name:"my-nginx", UID:"dcd7d703-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161662", FieldPath:""})...
I0919 03:26:57.418072 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.451023 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.476133 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.505592 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.505841 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.507912 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.508195 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.575581 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.576071 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
I0919 03:26:57.577221 1 event.go:221] Event(v1.ObjectReference{Kind:"ReplicaSet", Namespace:"default", Name:"my-nginx-59497d7745", UID:"dcdb4095-bbbb-11e8-a78d-06cd4d8a83f2", APIVersion:"apps/v1", ResourceVersion:"161663", Fi...
```

ery_data (1).csv

Page 1 of 1 50 items per page 1 - 11 of 11 items

Multi cluster monitoring



Resources

Resources

- AKS Best Practices GitHub: https://github.com/Azure/k8s-best-practices
- AKS Hackfest: aka.ms/k8s-hackfest & https://github.com/Azure/kubernetes-hackfest
- Distributed systems Labs by Brendan Burns
- Kube Advisor: https://github.com/Azure/kube-advisor
- VSCode Kubernetes Extension
- Documentation resources
  - Regions and limits
- Ebook for distributed systems
- AKS HoL

Thank You!

Azure Dev Spaces

- Run and debug containers directly in Azure Kubernetes Service (AKS)
- VS and Vscode
- Java, .NET core, Node.js

Azure Dev Spaces

A rapid, iterative Kubernetes development experience for teams

With minimal dev machine setup, you can iteratively run and debug containers directly in Azure Kubernetes Service (AKS). You can also collaborate with your team in a shared Kubernetes cluster, and do end-to-end testing with other components without replicating or mocking up dependencies. With Azure Dev Spaces, you can develop on Windows, Mac, or Linux using familiar tools like Visual Studio, Visual Studio Code, or the command line.

Important

Azure Dev Spaces is currently in preview, and is supported only by AKS clusters in the **East US**, **East US 2**, **Central US**, **West US 2**, **West Europe**, **Southeast Asia**, **Canada Central**, and **Canada East** regions. Previews are made available to you on the condition that you agree to the supplemental terms of use. Some aspects of this feature may change prior to general availability (GA).

Get Started on Azure Dev Spaces

Please select a language-specific guide to get started:

Java | .NET and VS Code | .NET and Visual Studio | Node.js

https://docs.microsoft.com/en-us/azure/dev-spaces/

Microsoft

© Copyright Microsoft Corporation. All rights reserved.