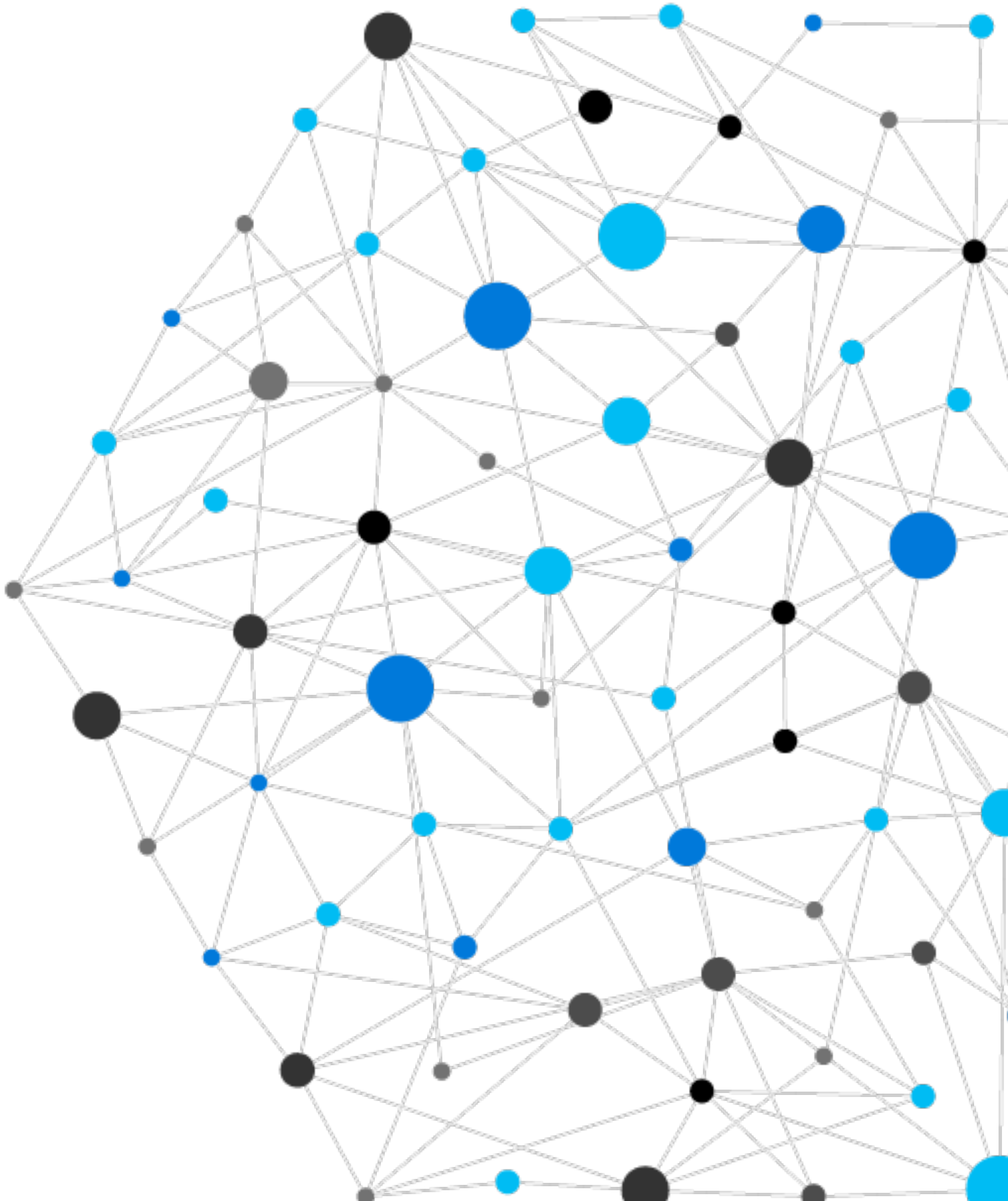
Microsoft Azure

Optimize your Kubernetes Clusters on Azure with Built-in Best Practices



Your speaker today

Jorge Palma

Senior Program Manager - Azure Container Compute

@jorgefpalma

Microsoft Azure

Kubernetes: empowering you to do more

Portable

Public, private, hybrid, multi-cloud

Extensible

Modular, pluggable, hookable, composable

Self-healing

Auto-placement, auto-restart, auto-replication, auto-scaling

Deploy your applications quickly and predictably

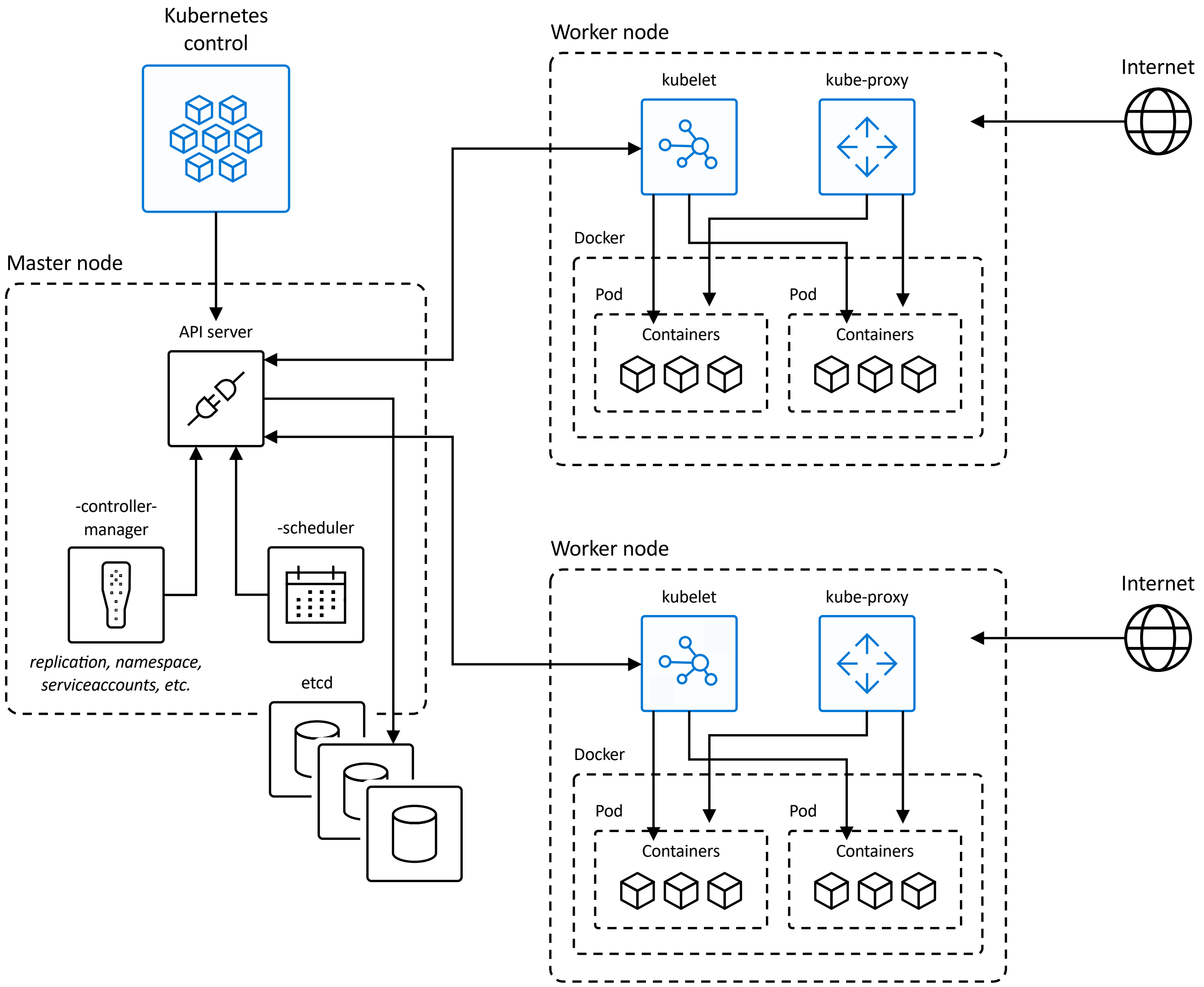
Scale your applications on the fly

Roll out new features seamlessly

Limit hardware usage to required resources only

How Kubernetes works

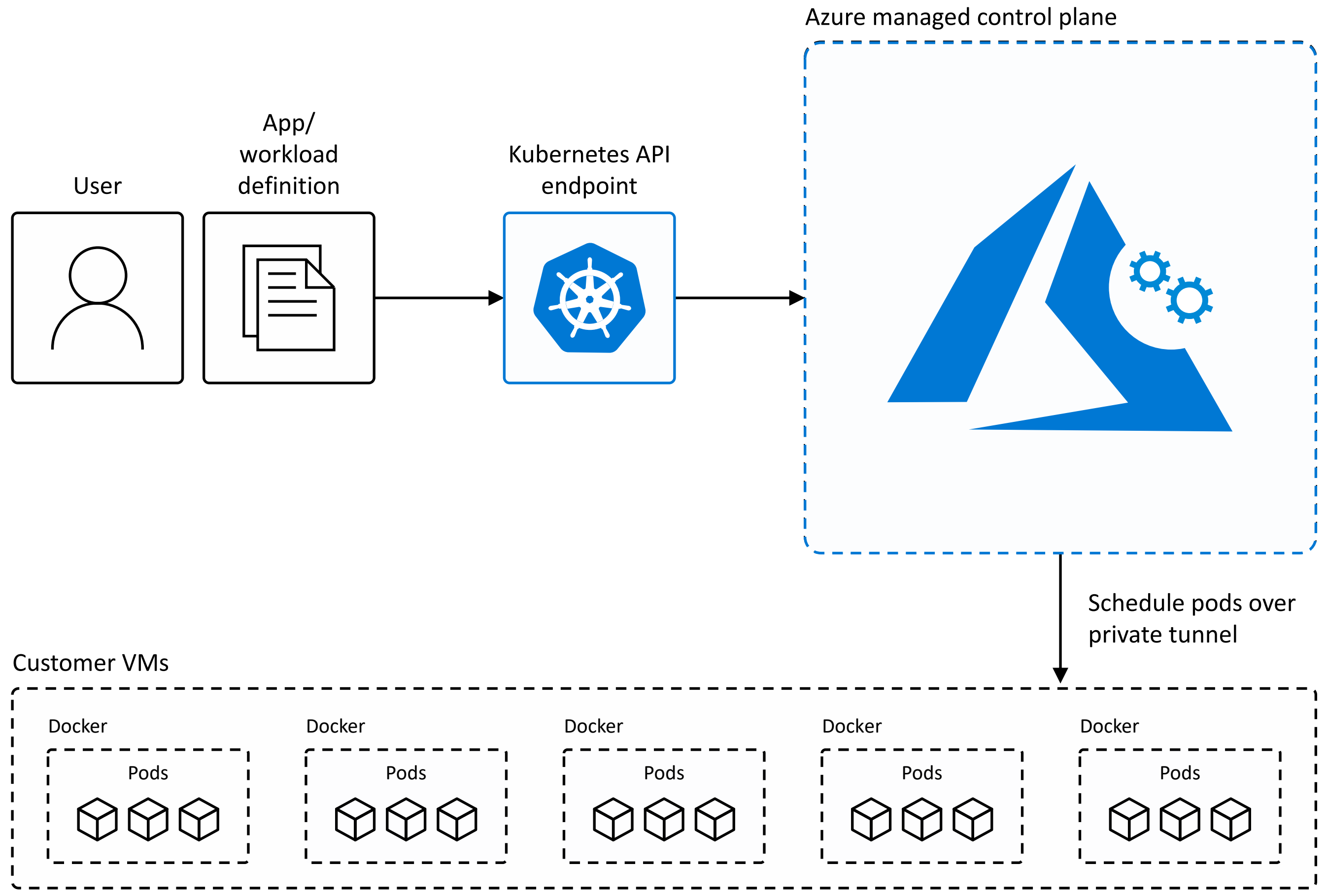
1. Kubernetes users communicate with API server and apply desired state
2. Master nodes actively enforce desired state on worker nodes
3. Worker nodes support communication between containers
4. Worker nodes support communication from the Internet



Microsoft Azure

Ok, so managed kubernetes it is

- Automated upgrades, patches
- High reliability, availability
- Easy, secure cluster scaling
- Self-healing
- API server monitoring
- At no charge



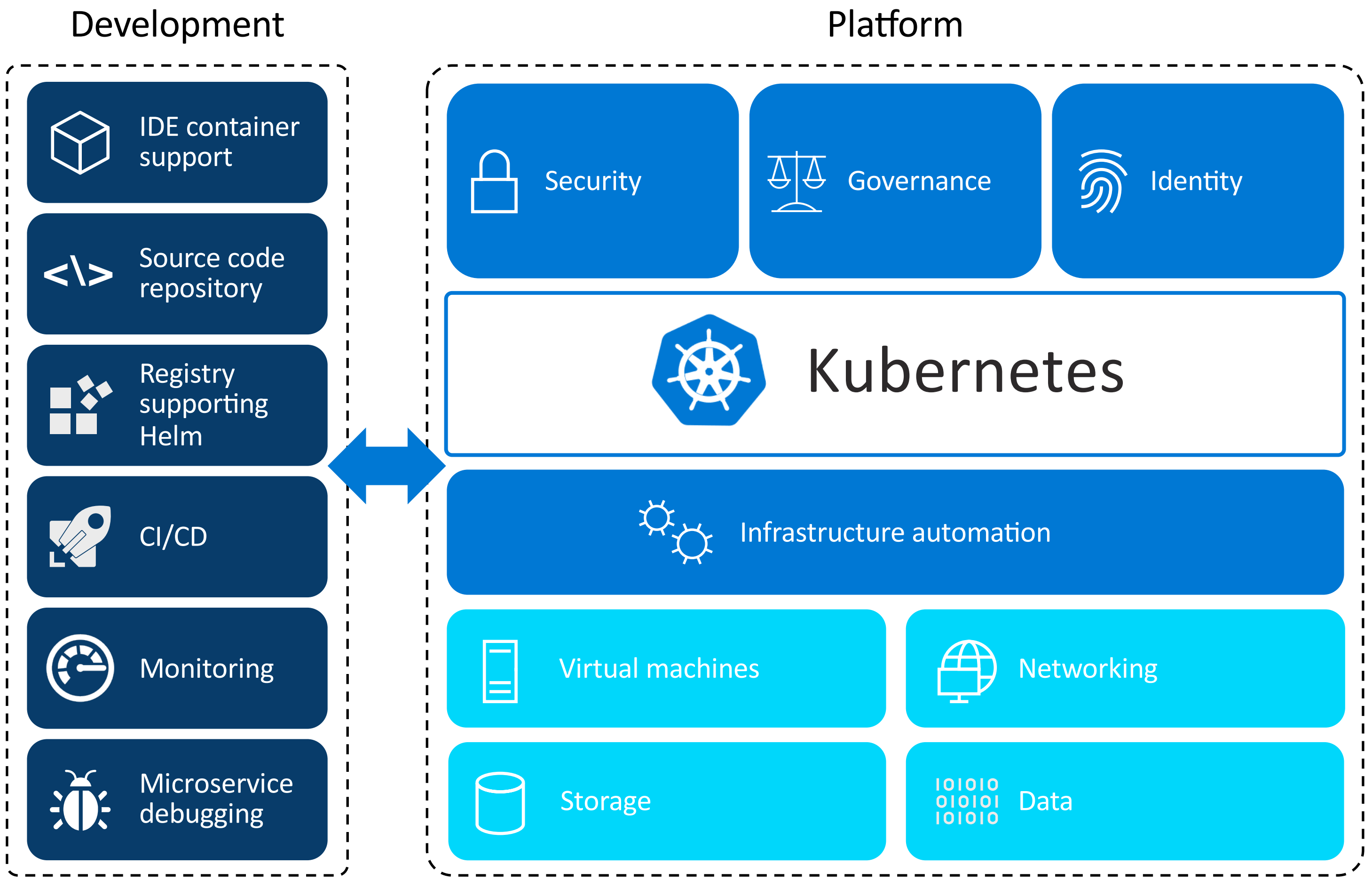
Microsoft Azure

Is that enough?

Well, depends

Unlock the agility for containerized applications using:

- Infrastructure automation that simplifies provisioning, patching, and upgrading
- Tools for containerized app development and CI/CD workflows
- Services that support security, governance, and identity and access management



Microsoft Azure

What is missing?

Common issues

1. Incorrect Kubernetes configurations
2. Permissive or insecure clusters and lack of pod security
3. Lack of governance policies
4. Lack of central authentication at scale
5. Lack of fine-grained access control at scale
6. “Voluntary” disruptions and unplanned downtime
7. Inefficiency

What can we do?

Common needs

1. Validating Kubernetes Configurations
2. Manage and harden cluster and pod security, especially at scale
3. Create and curate default secure configurations, and we need to be able to enforce them via Policies
4. Leverage central authentication directories
5. Apply fine-grained access controls at scale
6. Prevent human errors that cause down time, harden against disruption
7. How can we be more efficient
   a) Autoscalling?
   b) Different agent node groups/pools?
   c) Spot instances?

Kubernetes Configurations

Sample configuration checks

1. Configure readiness and health probes
2. Configure Resource quotas
3. Do not use “latest” image tags
4. Restrict the registries your images can come from
5. Configure pod security
6. Cluster’s Kubernetes version up to date
7. Cluster agent nodes up to date
8. Administrative access minimized, audited and API access controlled.

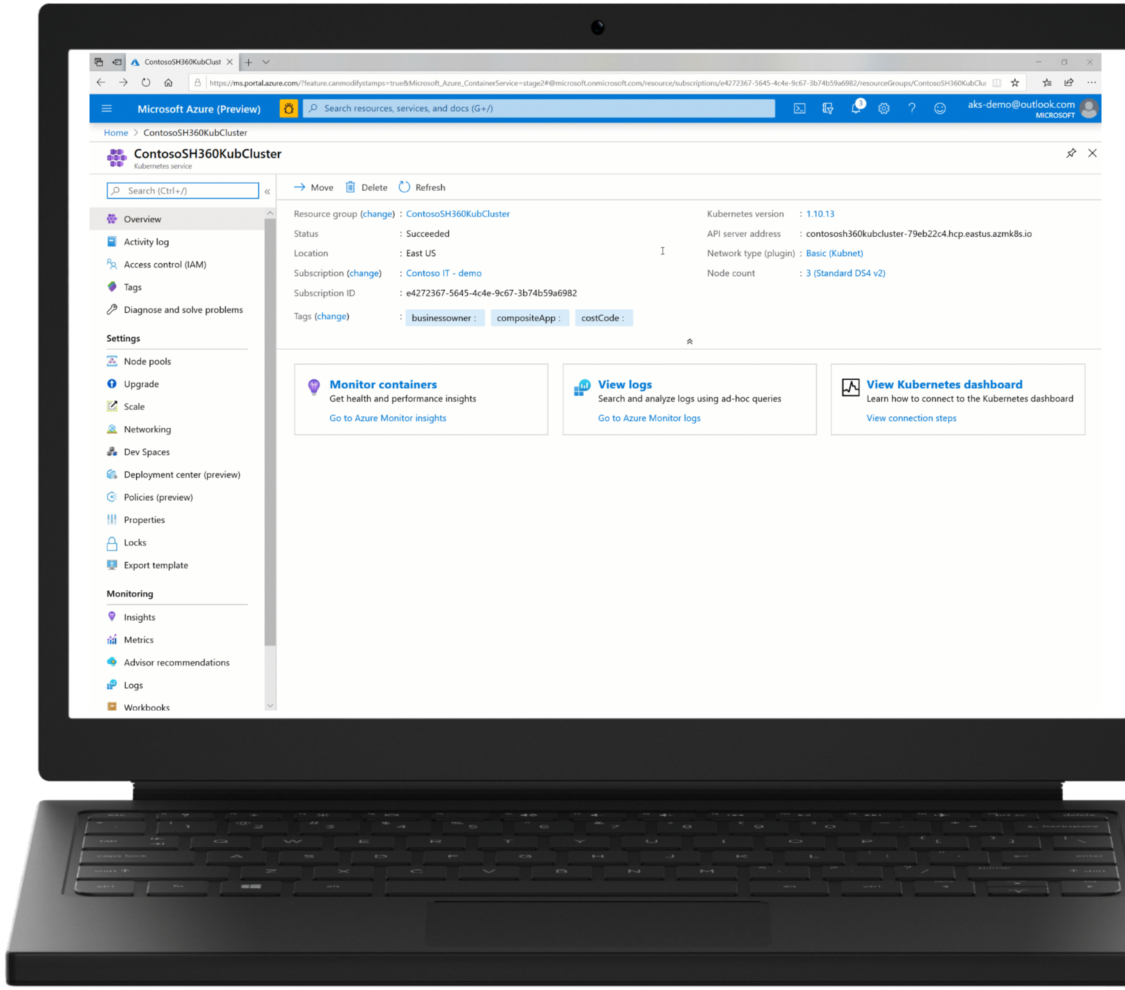
Kubernetes Configurations

Configuration recommendation and validation tools

- Polaris
- Kube-scan
- Kube-advisor
- Secure DevOps Kit

Kubernetes Built-in best practices with Azure Advisor

- Proactive and actionable recommendations from Azure Advisor based on your configuration and usage telemetry
- Grounded with knowledge from thousands of customer engagements
- Improve the performance, availability, efficiency and security of your cluster before there's a problem



ContosoSH360KubClust

https://ms.portal.azure.com/?feature.canmodifystamps=true&Microsoft_Azure_ContainerService=stage2#@microsoft.onmicrosoft.com/resource/subscriptions/e4272367-5645-4c4e-9c67-3b74b59a6982/resourceGroups/ContosoSH360KubClu

Microsoft Azure (Preview) | Search resources, services, and docs (G+/) | aks-demo@outlook.com MICROSOFT

Home > ContosoSH360KubCluster

ContosoSH360KubCluster
Kubernetes service

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Node pools
Upgrade
Scale
Networking
Dev Spaces
Deployment center (preview)
Policies (preview)
Properties
Locks
Export template

Monitoring
Insights
Metrics
Advisor recommendations
Logs
Workbooks

Move | Delete | Refresh

Resource group (change) : ContosoSH360KubCluster
Status : Succeeded
Location : East US
Subscription (change) : Contoso IT - demo
Subscription ID : e4272367-5645-4c4e-9c67-3b74b59a6982
Tags (change) : businessowner : compositeApp : costCode :

Kubernetes version : 1.10.13
API server address : contososh360kubcluster-79eb22c4.hcp.eastus.azmk8s.io
Network type (plugin) : Basic (Kubnet)
Node count : 3 (Standard DS4 v2)

Monitor containers
Get health and performance insights
Go to Azure Monitor insights

View logs
Search and analyze logs using ad-hoc queries
Go to Azure Monitor logs

View Kubernetes dashboard
Learn how to connect to the Kubernetes dashboard
View connection steps

Microsoft Azure

Tips for getting started with Advisor alerts

1. Start simple with a few high impact recommendations and email
2. Notify the person or team who can remediate the recommendations
3. Explore automation scenarios using webhooks and/or runbooks

Cloud Workload Protection for Containers

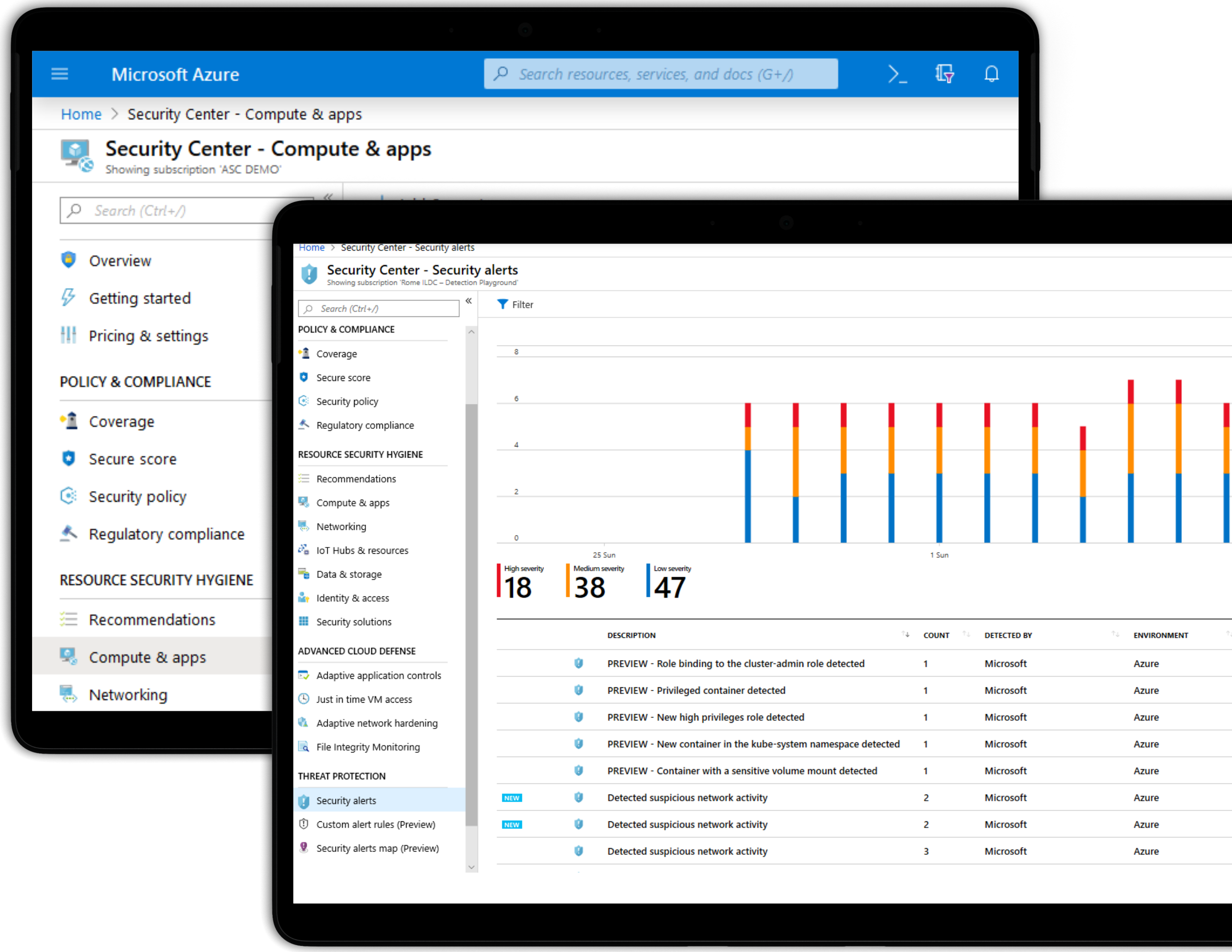
Now available in standard Azure Security Center with the new Container Service add-on

Protecting Container hosts (IaaS)

- CIS Docker Benchmark assessment
- Node Threat Protection

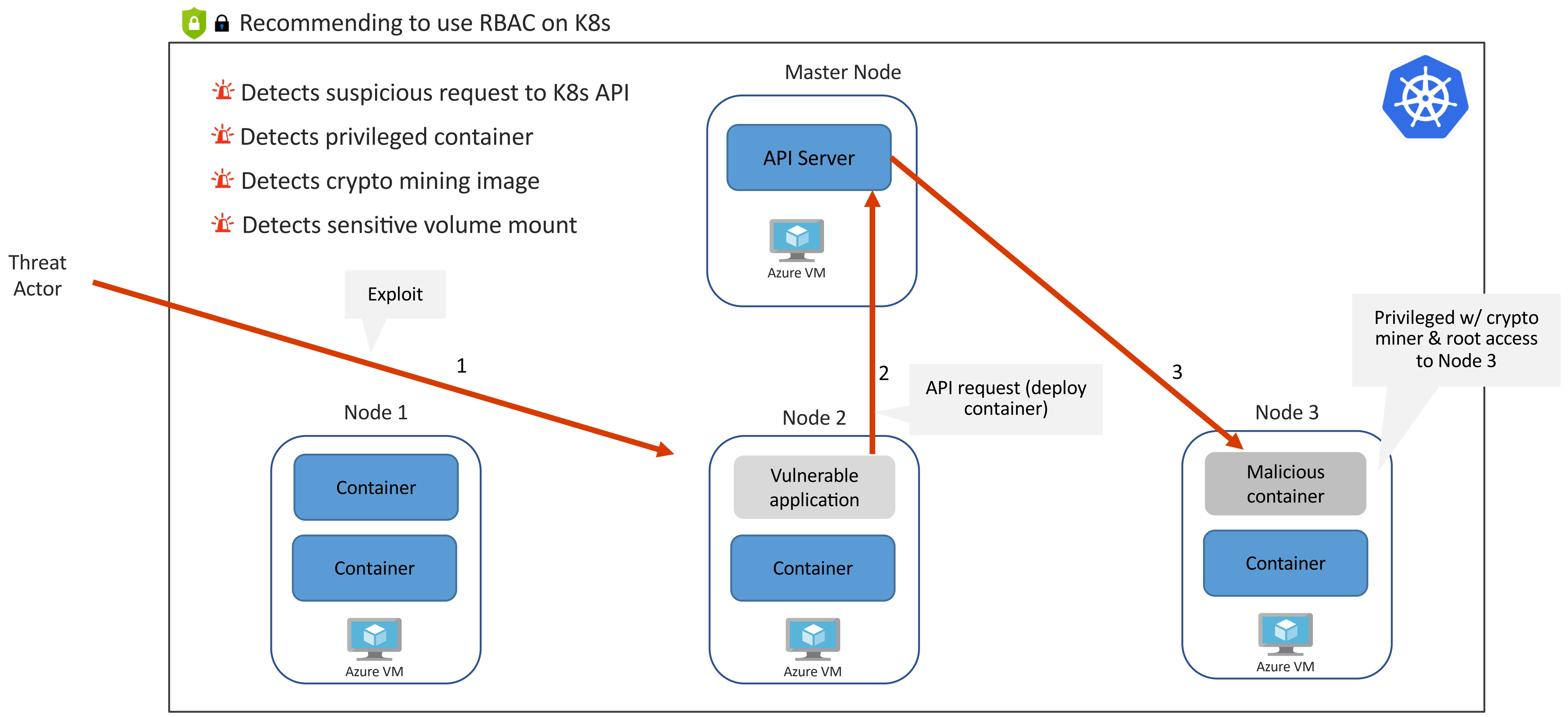
Protecting AKS

- Actionable recommendations based on AKS best practices
- Cluster and Node Threat detection based on AKS audit log and Node Auditd



	DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT
	PREVIEW - Role binding to the cluster-admin role detected	1	Microsoft	Azure
	PREVIEW - Privileged container detected	1	Microsoft	Azure
	PREVIEW - New high privileges role detected	1	Microsoft	Azure
	PREVIEW - New container in the kube-system namespace detected	1	Microsoft	Azure
	PREVIEW - Container with a sensitive volume mount detected	1	Microsoft	Azure
NEW	Detected suspicious network activity	2	Microsoft	Azure
NEW	Detected suspicious network activity	2	Microsoft	Azure
	Detected suspicious network activity	3	Microsoft	Azure

Protecting against advanced cloud threats



Recommending to use RBAC on K8s
Detects suspicious request to K8s API
Detects privileged container
Detects crypto mining image
Detects sensitive volume mount
Threat Actor
Exploit
1
Master Node
API Server
Azure VM
2
API request (deploy container)
3
Privileged w/ crypto miner & root access to Node 3
Node 1
Container
Container
Azure VM
Node 2
Vulnerable application
Container
Azure VM
Node 3
Malicious container
Container
Azure VM

Microsoft Azure

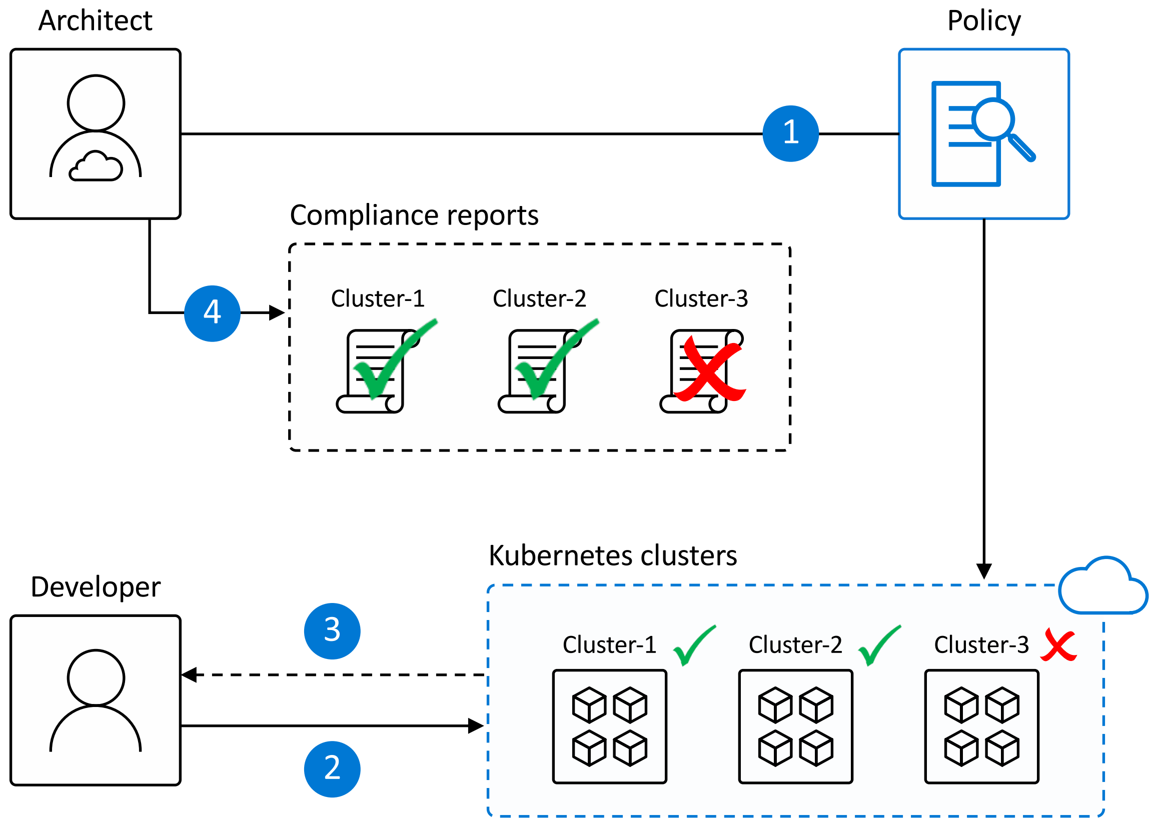
Policy Management

Policy management/enforcement tools and projects

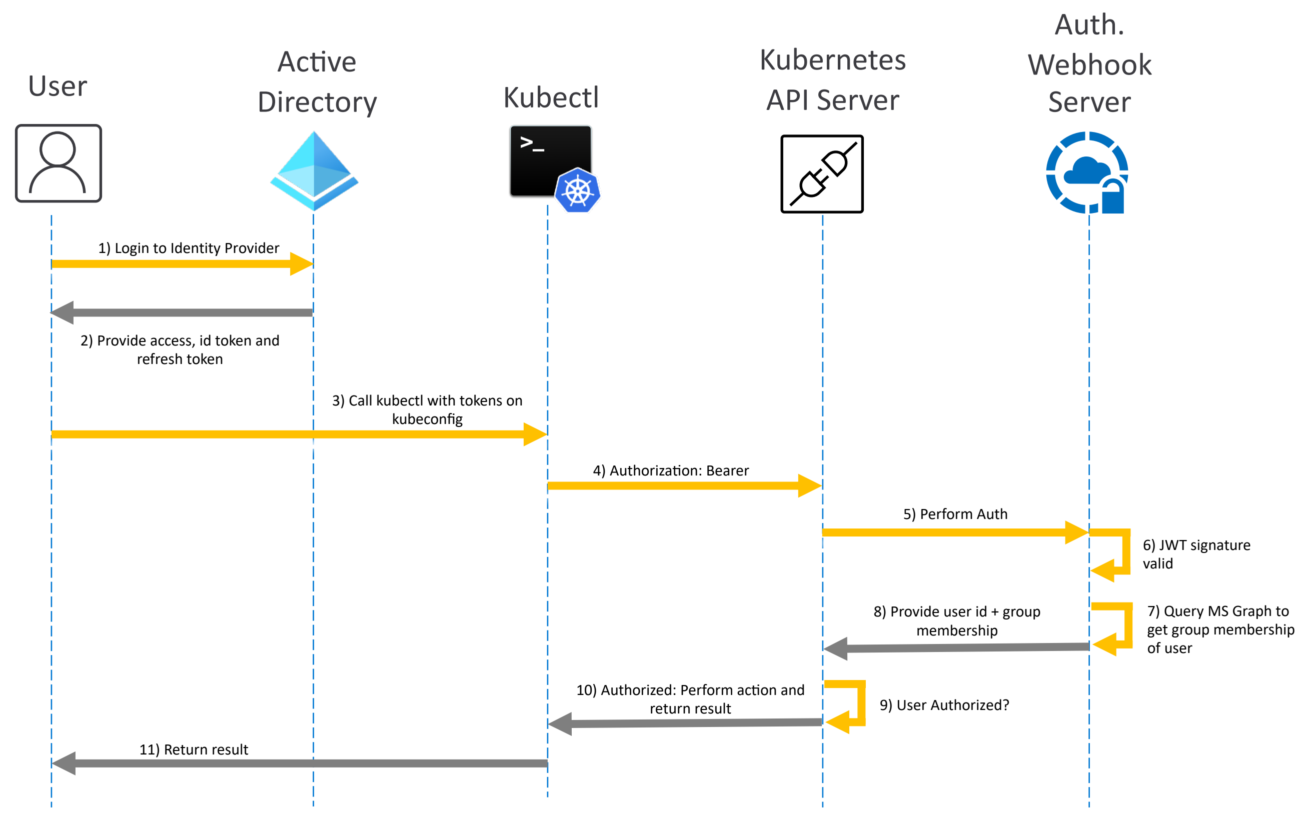
- OPA Gatekeeper
- Kyverno
- K-rail

Policy management at scale

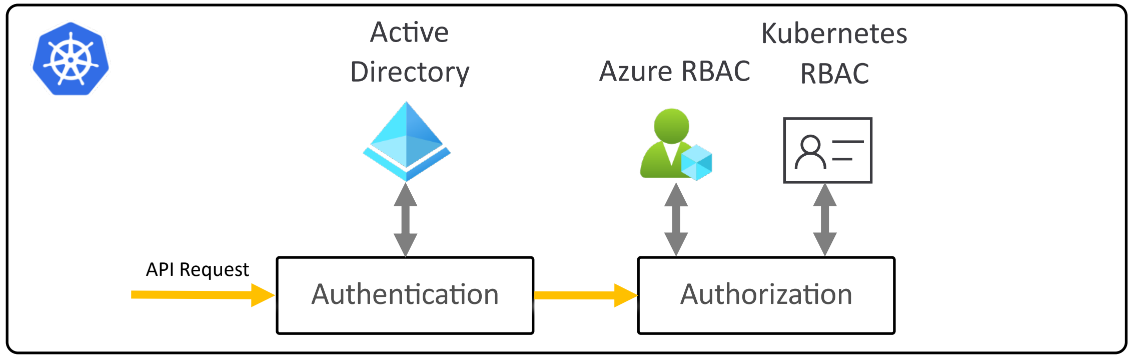
1. Architect assigns a deployment policy across cluster(s)
2. Developer uses standard Kubernetes API to deploy to the cluster
3. Real-time deployment enforcement (acceptance/denial) provided to developer based on policy
4. Cloud architect obtains compliance report for the entire environment and can drill down to individual pod level



Authentication at scale

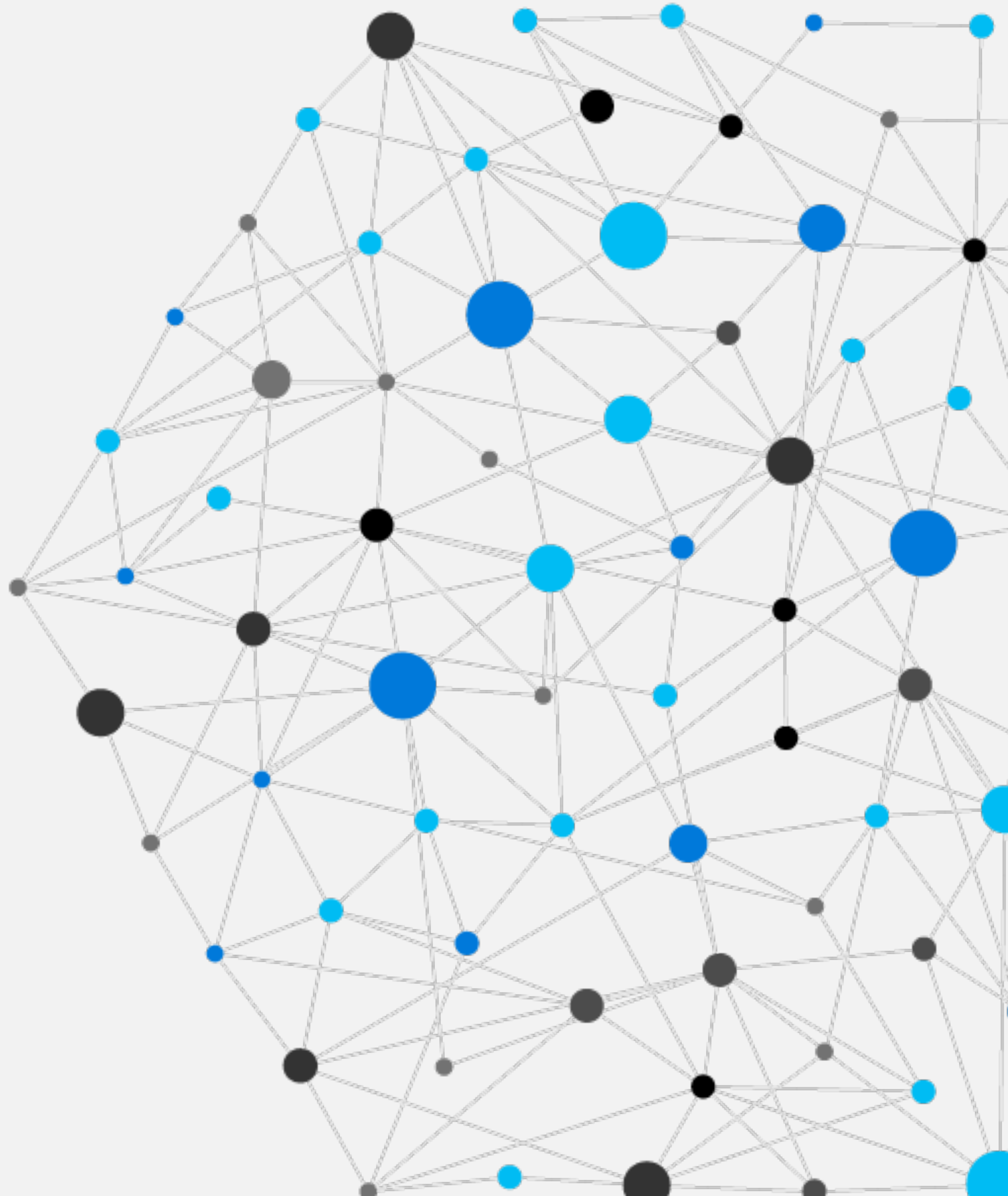

User
Active Directory
Kubectl
Kubernetes API Server
Auth. Webhook Server
1) Login to Identity Provider
2) Provide access, id token and refresh token
3) Call kubectl with tokens on kubeconfig
4) Authorization: Bearer
5) Perform Auth
6) JWT signature valid
7) Query MS Graph to get group membership of user
8) Provide user id + group membership
9) User Authorized?
10) Authorized: Perform action and return result
11) Return result

Authorization at scale



Microsoft Azure

Demo



Diagnostics and troubleshooting

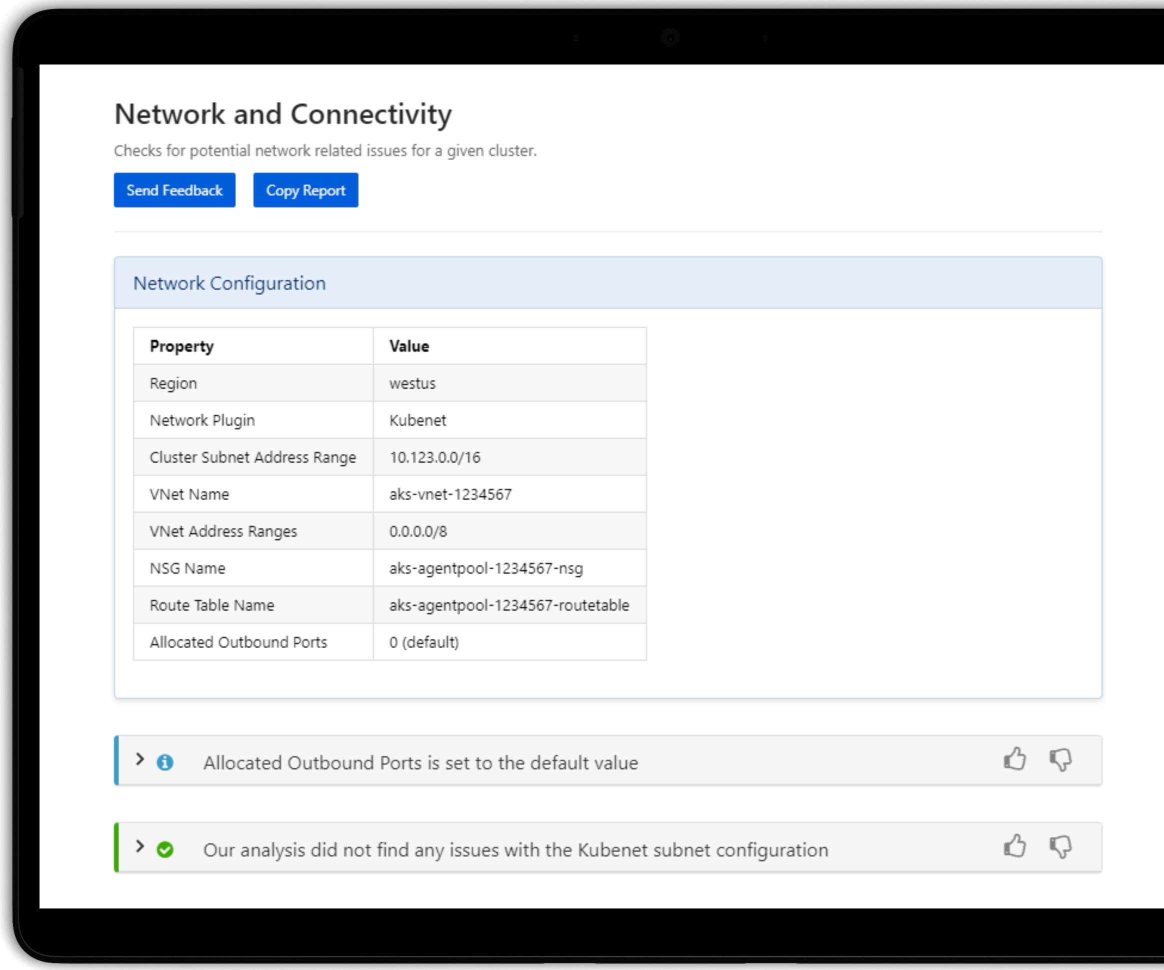
Diagnostics and troubleshooting tools

- Sysdig
- Weave Scope
- Periscope + AKS diagnostics

Built-in diagnostics and troubleshooting solutions with AKS Diagnostics

Available in the Azure Portal and via VS Code extension

- Quickly pinpoint cluster issues by analyzing backend telemetry on common issues such as networking misconfiguration, CRUD operation failures, and more
- Use red, orange, and green status icons to identify whether there is a pertinent issue
- Get recommendations for next steps and potential solutions
- Run a basic health check on your network configuration using the VS code extension or visit the portal for the deep dive



Network and Connectivity

Checks for potential network related issues for a given cluster.

Network Configuration

Property	Value
Region	westus
Network Plugin	Kubenet
Cluster Subnet Address Range	10.123.0.0/16
VNet Name	aks-vnet-1234567
VNet Address Ranges	0.0.0.0/8
NSG Name	aks-agentpool-1234567-nsg
Route Table Name	aks-agentpool-1234567-routetable
Allocated Outbound Ports	0 (default)

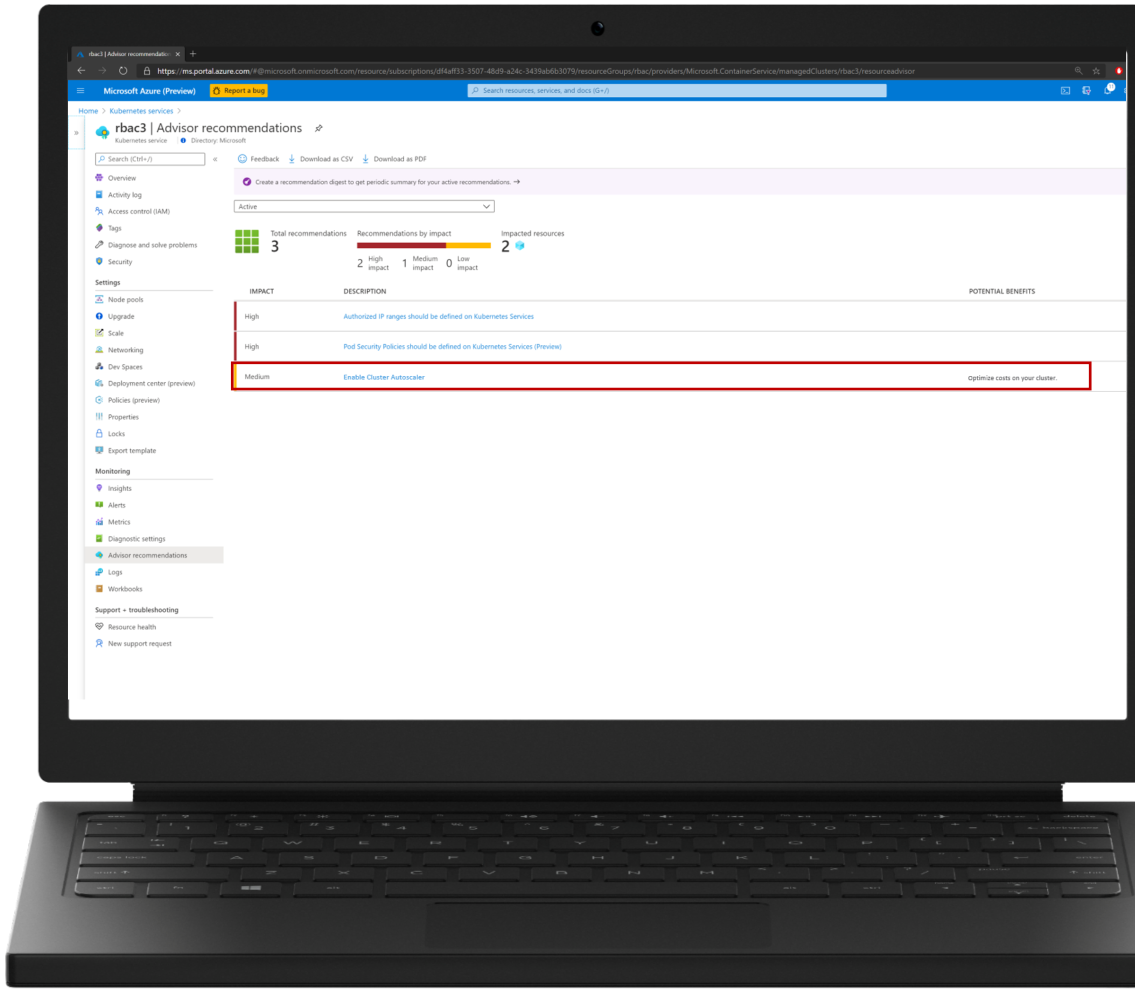
Allocated Outbound Ports is set to the default value

Our analysis did not find any issues with the Kubenet subnet configuration

Microsoft Azure

Efficiency and cost savings

- Use Node Groups/Pools with VMs right sized to the workload of that pool(s).
- Leverage Cluster Autoscaler and Horizontal Pod Autoscaler to maximize your cluster infrastructure.
- Use projects like Virtual Kubelet to quickly respond to temporaty bursts
- Use Descheduler to respond to unbalanced or unoptimized clusters.
- Use more fit for purpose scaling projects like KEDA to optimize scaling based on your workload architecture and needs.



https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/resource/subscriptions/df4aff33-3507-48d9-a24c-3439ab6b3079/resourceGroups/rbac/providers/Microsoft.ContainerService/managedClusters/rbac3/resourceadvisor

rbac3 | Advisor recommendations
Kubernetes service · Directory: Microsoft

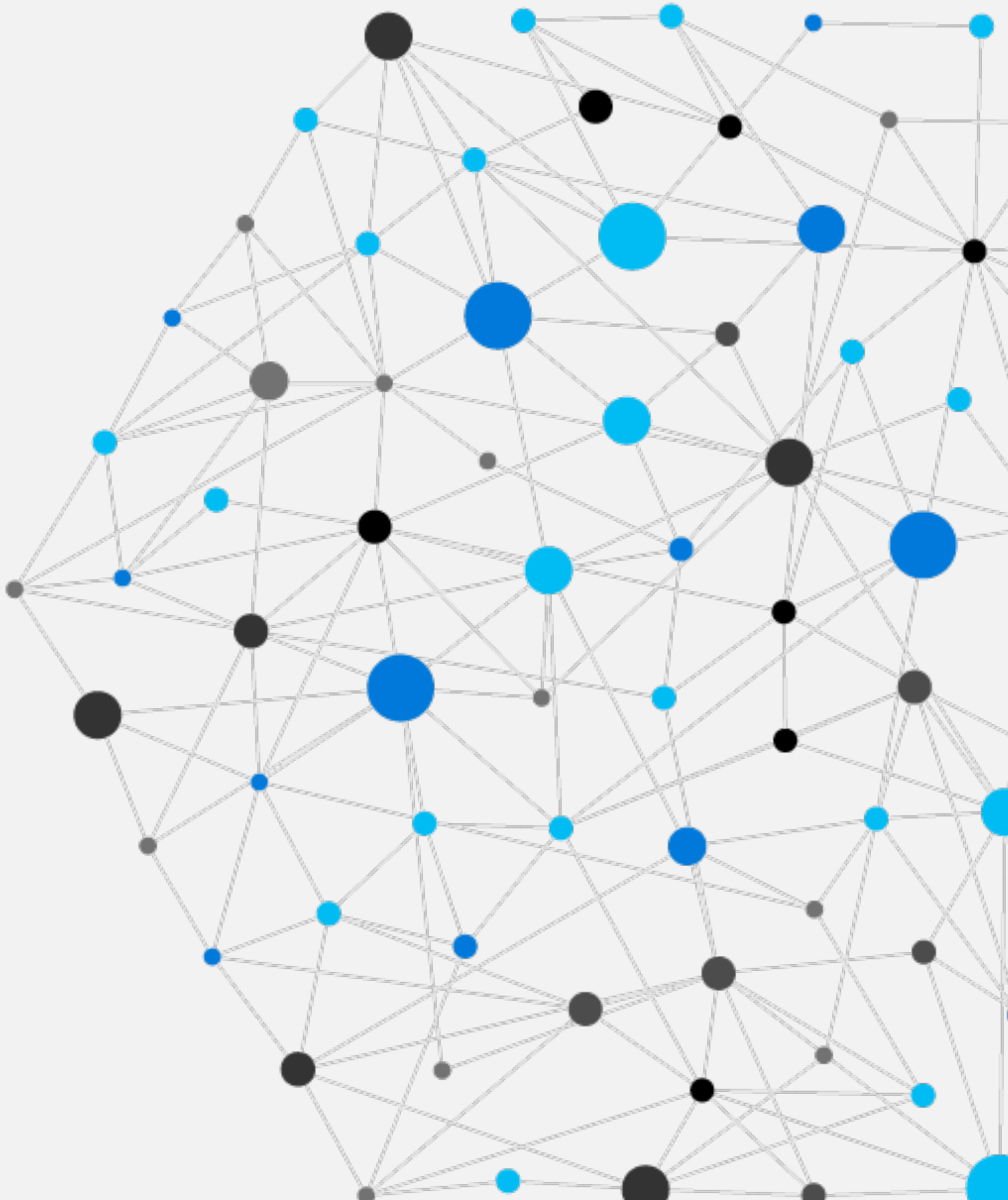
Create a recommendation digest to get periodic summary for your active recommendations. →

Total recommendations 3
Recommendations by impact: 2 High impact, 1 Medium impact, 0 Low impact
Impacted resources 2

IMPACT	DESCRIPTION	POTENTIAL BENEFITS
High	Authorized IP ranges should be defined on Kubernetes Services	
High	Pod Security Policies should be defined on Kubernetes Services (Preview)	
Medium	Enable Cluster Autoscaler	Optimize costs on your cluster.

Microsoft Azure

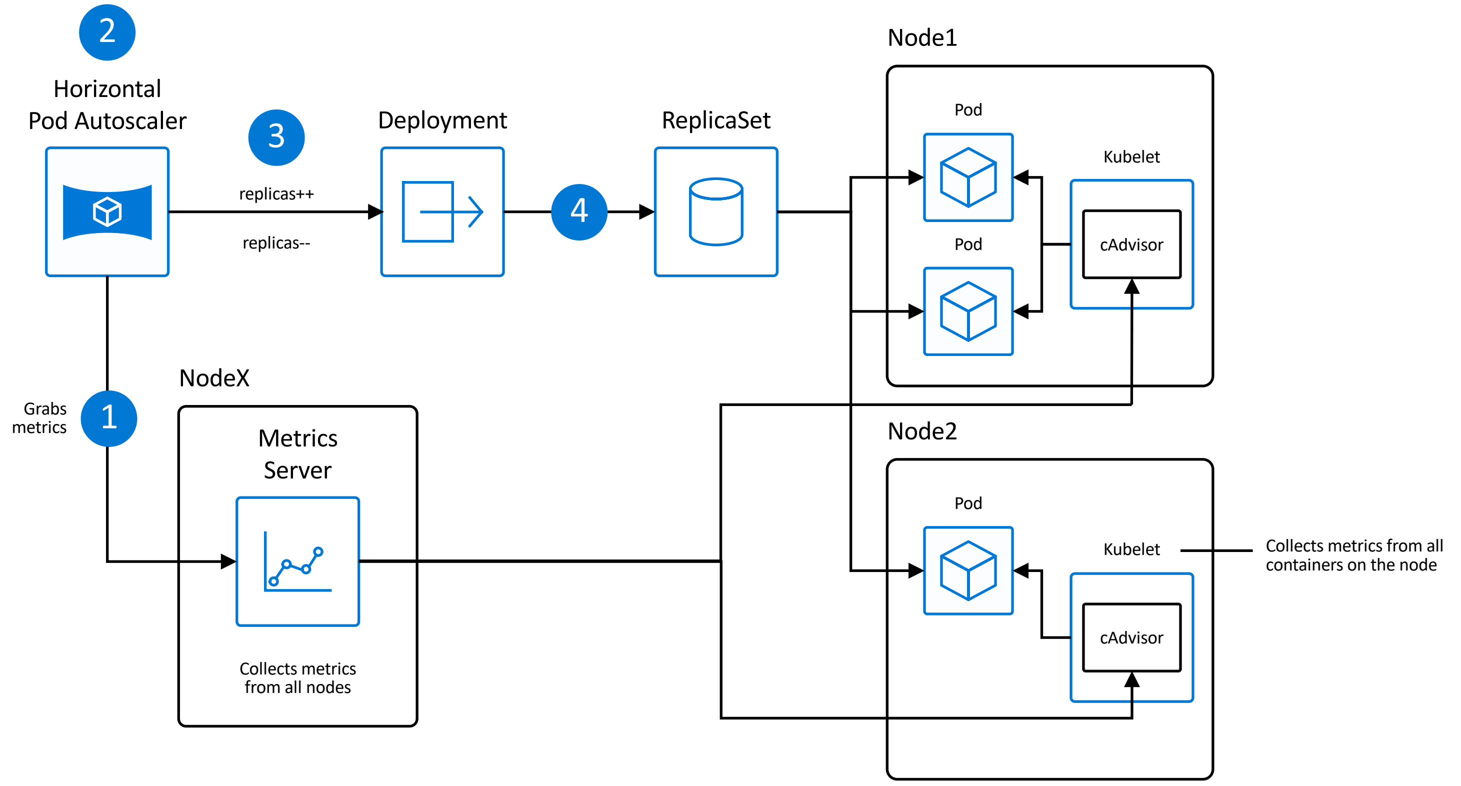
Efficiency and cost savings



Horizontal Pod Autoscaler

The horizontal pod autoscaler (HPA) uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If a service needs more resources, the number of pods is automatically increased to meet the demand.

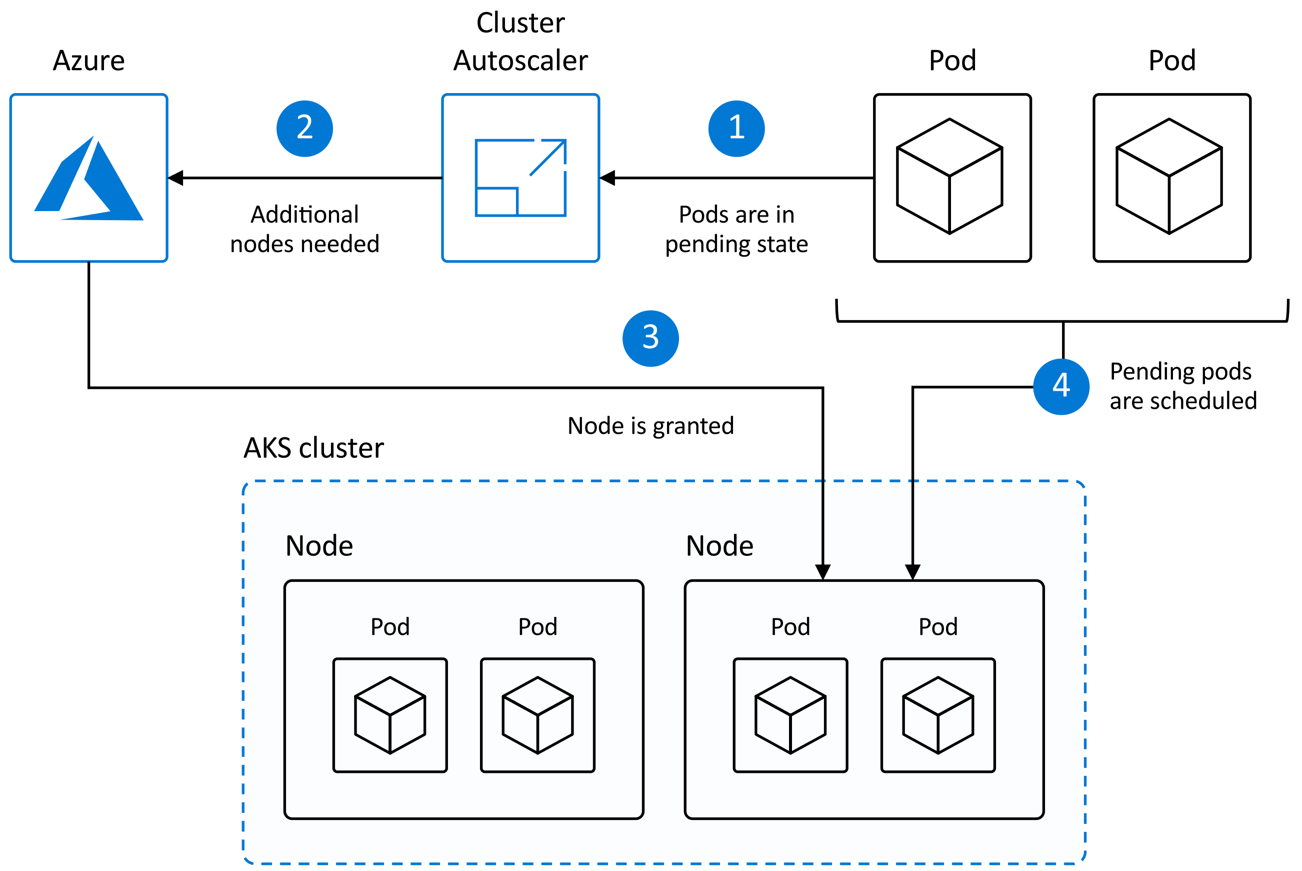
1. HPA obtains resource metrics and compares them to user-specified threshold
2. HPA evaluates whether user specified threshold is met or not
3. HPA increases/decreases the replicas based on the specified threshold
4. The Deployment controller adjusts the deployment based on increase/decrease in replicas



Cluster Autoscaler

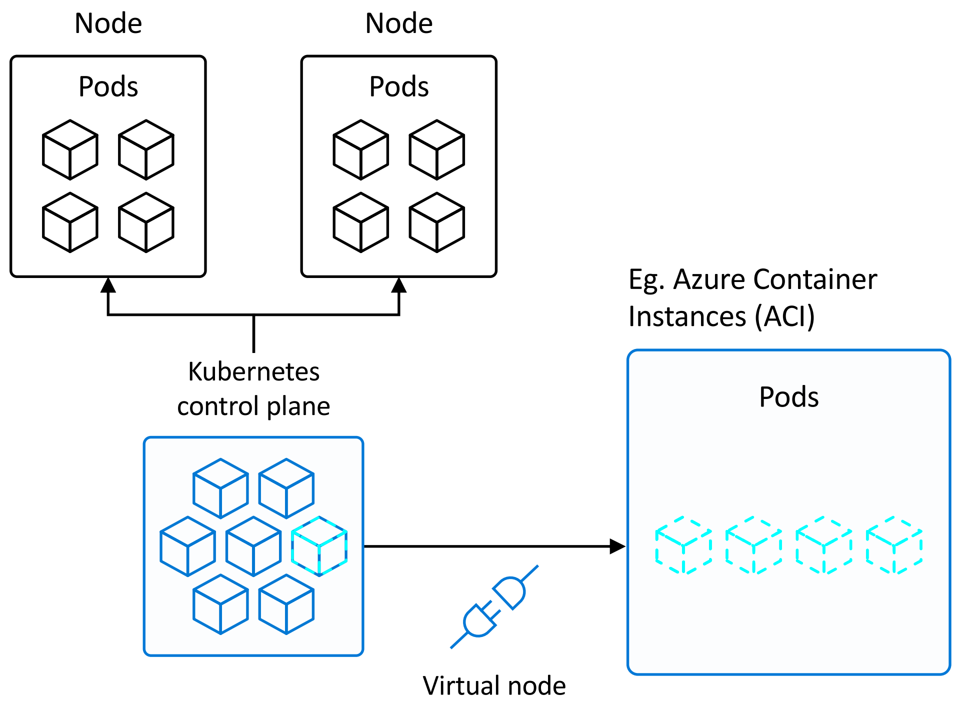
The cluster autoscaler watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.

1. HPA obtains resource metrics and compares them to user-specified threshold
2. HPA evaluates whether user specified threshold is met or not
3. HPA increases/decreases the replicas based on the specified threshold
4. The Deployment controller adjusts the deployment based on increase/decrease in replicas



Nodeless Kubernetes using Virtual Kubelet

- Elastically provision compute capacity in seconds
- No infrastructure to manage
- Built on open sourced Virtual Kubelet technology, Cloud Native Computing Foundation (CNCF) sandbox project
- Burst faster than what would normally require infrastructure to provision



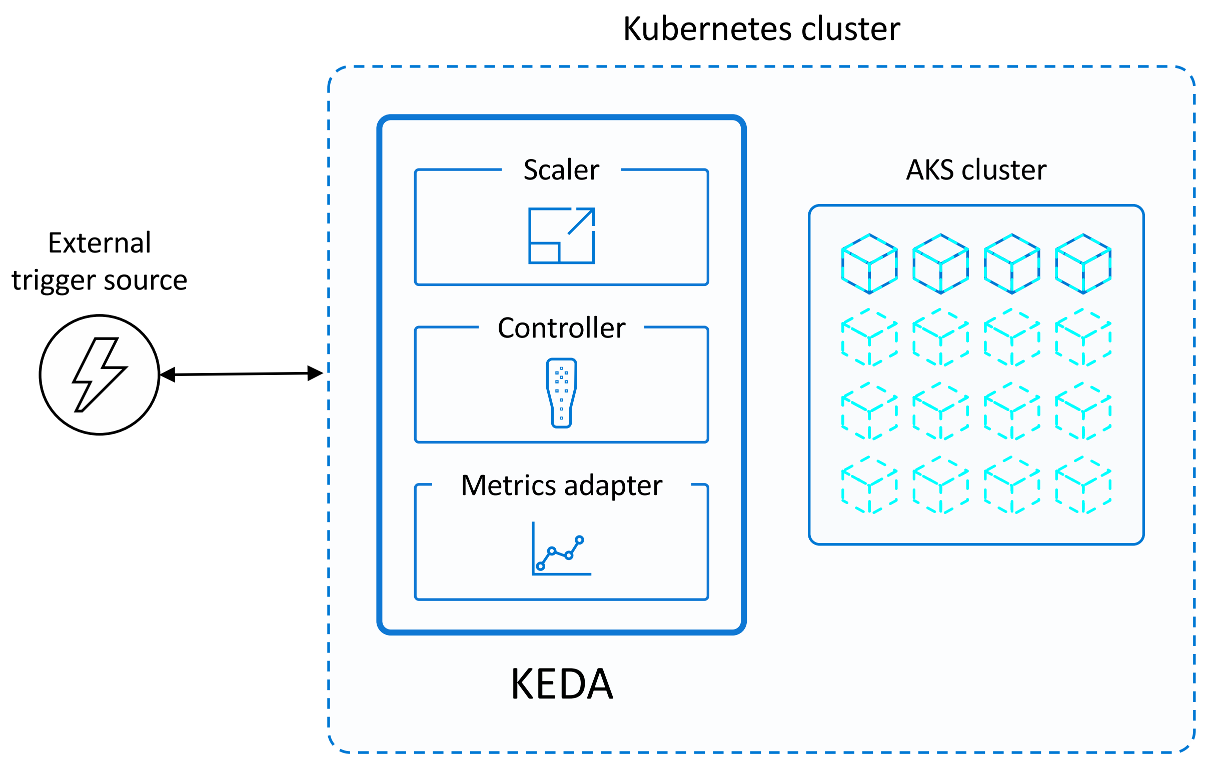
Kubernetes-based event-driven auto-scaling (KEDA)

Open-source component jointly built by Microsoft and RedHat

- Event-driven container creation & scaling
  Allows containers to “scale to zero” until an event comes in, which will then create the container and process the event, resulting in more efficient utilization and reduced costs

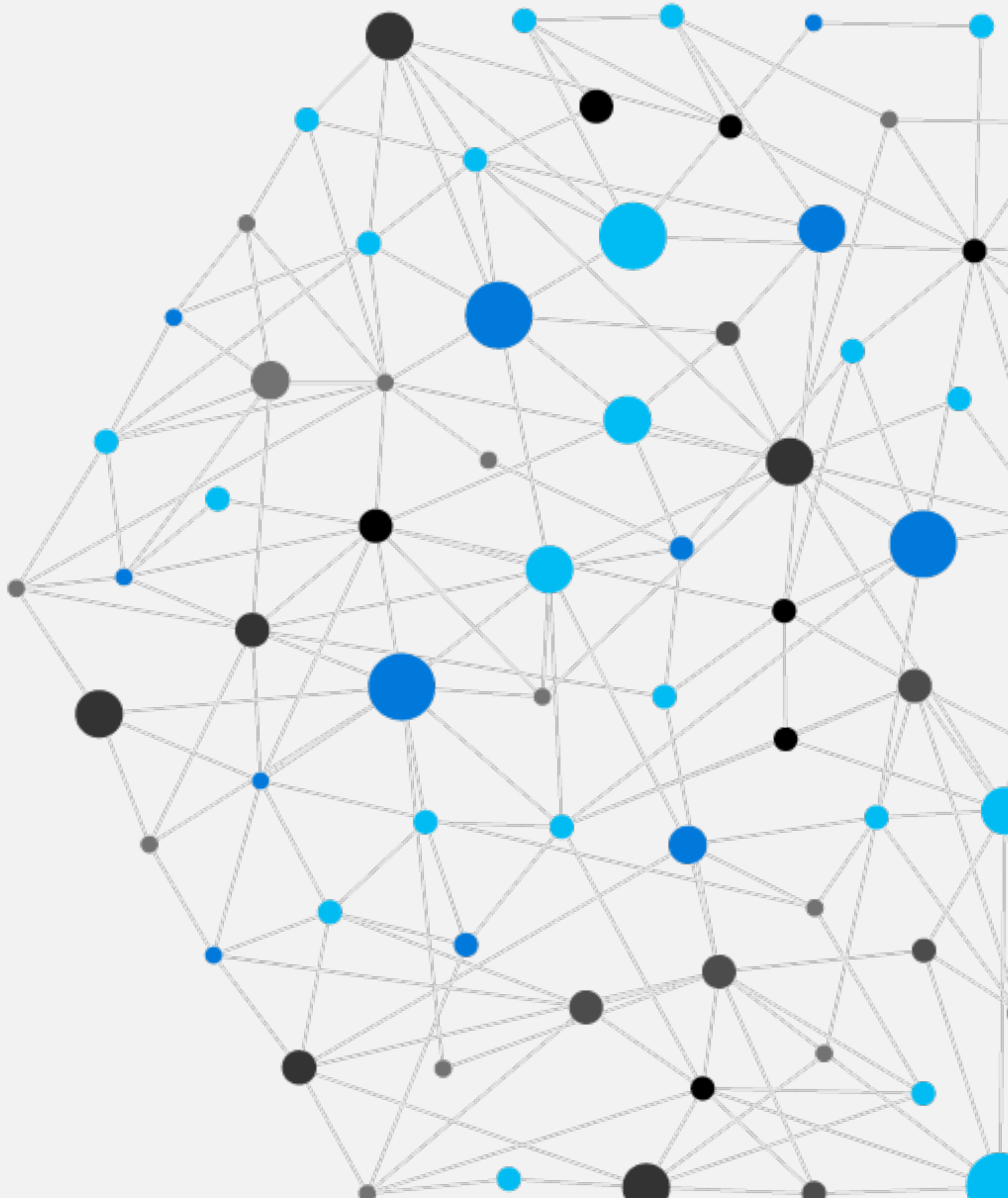
- Native triggers support
  Containers can consume events directly from the event source, instead of routing events through HTTP

- Can be used in any Kubernetes service
  This includes in the cloud (e.g., AKS, EKS, GKE, etc.) or on-premises with OpenShift—any Kubernetes workload that requires scaling by events instead of traditional CPU or memory scaling can leverage this component.



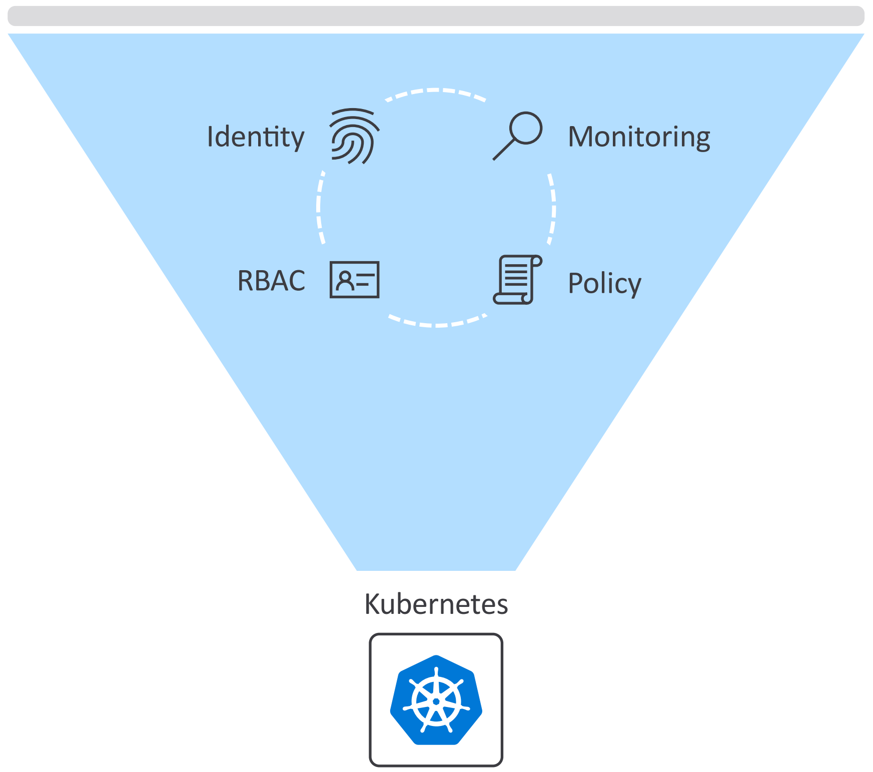
Microsoft Azure

Demo



Takeaways

- Consistently apply policies, role-based-access-controls (RBAC) for at-scale governance
- Deploy Kubernetes configuration to all clusters using a GitOps-based workflow
- Enforcing enterprise policies via Policy management tools like OPA Gatekeeper, Kyverno, etc
- Directory integration for centralized identity management at scale
- Workload-specific tuned autoscaling features and fit for purpose projects like Virtual Kubelet, Descheduler and KEDA to maximize the efficiency of clusters and resources



Resources

Kubernetes on Azure

https://azure.microsoft.com/en-us/overview/kubernetes-on-azure/

Kubernetes learnings and training

https://azure.microsoft.com/en-us/resources/kubernetes-learning-and-training/

Best Practices for Azure Kubernetes Services (AKS)

https://aka.ms/aks/bestpractices

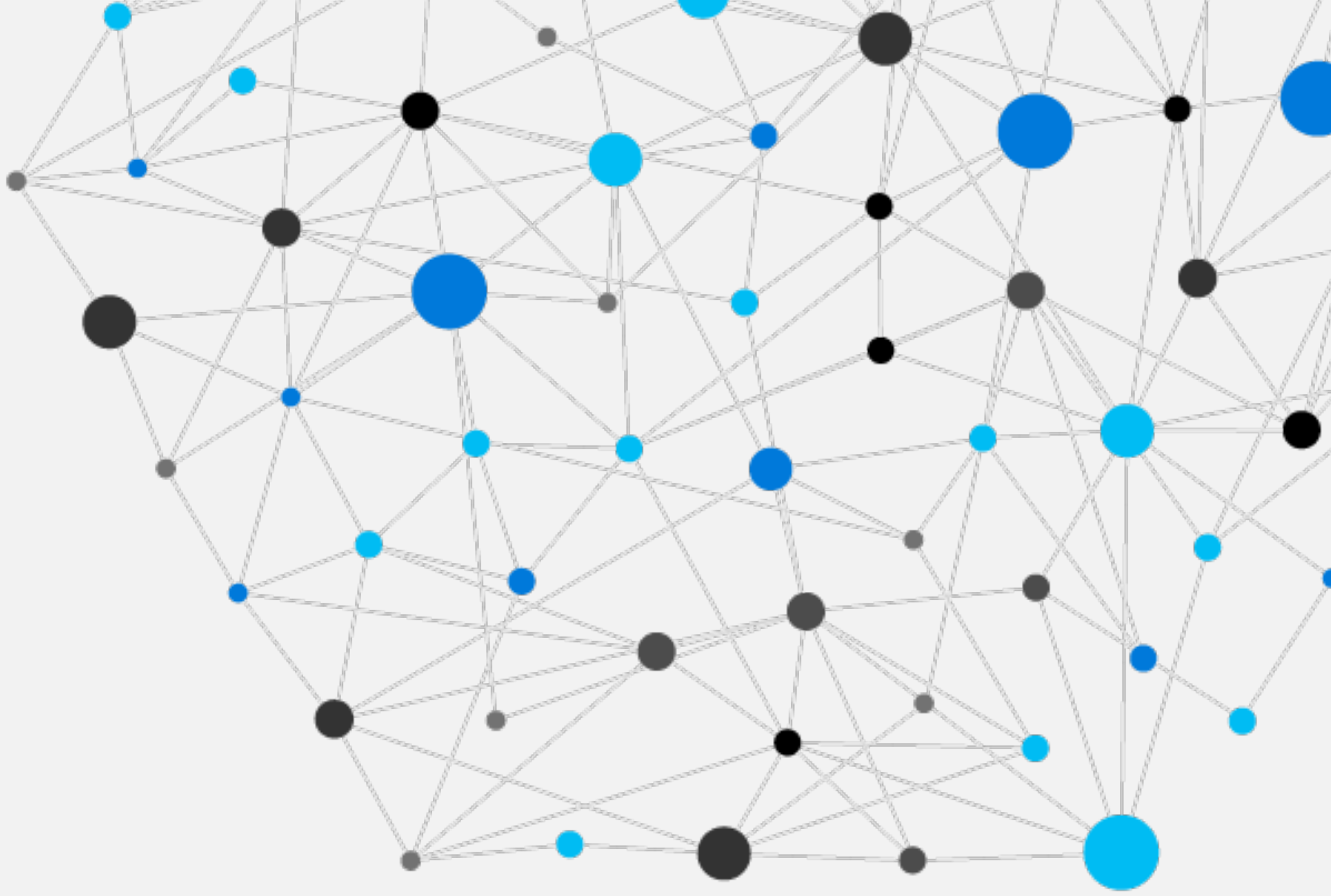
Azure Kubernetes Services (AKS) Diagnostics

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

Azure Security Center and Azure Kubernetes Service

https://docs.microsoft.com/en-us/azure/security-center/azure-kubernetes-service-integration

Q&A



Microsoft Azure

Microsoft Azure

Thank you for joining us.