Microsoft

# Self Managed vs Managed Cluster

**Hemant Rathore**
Technology Specialist –App Innovation
https://www.linkedin.com/in/hmntrathore/

# Agenda

- DIY Kubernetes
- AKS: Managed Kubernetes
- Developer Experience
- Instrumentation, observability & alerting
- Reduce cost and streamline operations
- AI
- Security

# From infrastructure to **innovation**

## Managed Kubernetes empowers you to do more

Focus on your containers and code, not the plumbing of them.

| Responsibilities | DIY with Kubernetes | Managed Kubernetes on Azure |
|---|---|---|
| Containerization | Customer | Customer / Microsoft |
| Application iteration, debugging | Customer | Customer / Microsoft |
| CI/CD | Customer | Customer / Microsoft |
| Cluster hosting | Customer | Microsoft |
| Cluster upgrade | Customer | Microsoft |
| Patching | Customer | Microsoft |
| Scaling | Customer | Microsoft |
| Monitoring and logging | Customer | Microsoft |

Customer

Microsoft

# DIY Kubernetes

## Strengths

- Greater control on configuration, customization, deployment and security options
- No lock-in
- Can mix and match best in class management tools
- Potentially cost effective in some scenarios at scale if internal resources are already accounted for

## Weaknesses

- Difficult to set-up and maintain for internal teams
- Many integration points
- Potentially a weaker solution than off the shelf
- Less documentation, templates and support
- Higher TCO when fully counting costs
- Landing Zone and Baseline is cumbersome
- Complex upgrade process

# Achieve more with Azure Kubernetes Service

Achieve efficiency and operational excellence

Build resilient, global applications

Enhance developer productivity

Differentiate with innovation and open source

# AKS provides a modern platform for intelligent apps

## Choice

Integrated with IDEs for your favorite framework/language, bring your code or container

## Integrated CI/CD

Delivery w/ GitHub AS, GitHub Actions, Azure DevOps, and others

## Blue-green deploys

Seamlessly rollout new versions of apps for user testing or change management while maintaining uptime

## Reliability and scale

Autoscale, high availability with a service-level agreement (SLA)-backed uptime, continuous backups

## Patching/upgrade

Automatic platform maintenance and security patching. Rolling updates w/o downtime, version pinning, rollbacks

## Observability

System insights for faster issue resolution, health checks

## Security

Policy enforcement, RBAC, secrets management, authN and authZ, secure container supply chain

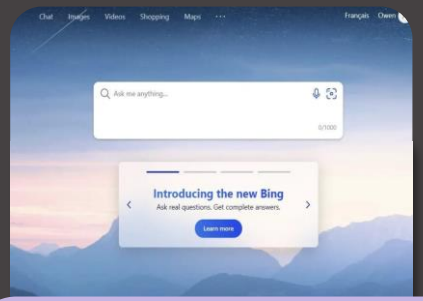
## Self healing and resilience

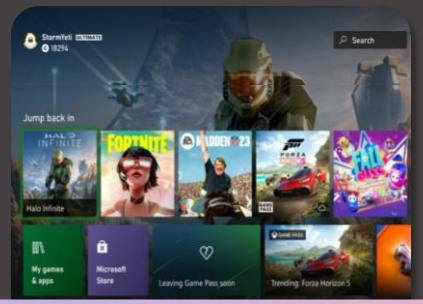
Health checks and self healing of unhealthy apps, harden using chaos engineering principles, and load testing tools

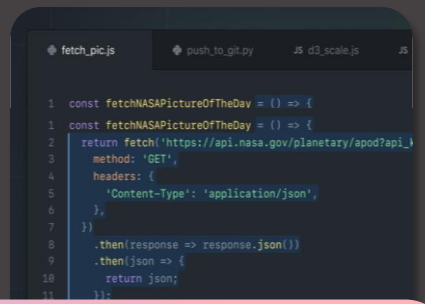
## Managed operations

Opinionated and simplified operations through a fully managed service. Managed addons, nodes & lifecycle

# Innovate on a pressure tested platform




**Microsoft modernized our own flagship apps and services for highly differentiated experiences**

| AI-based search with ChatGPT | Modern work across Office 365 | AI-powered meeting recaps | Personalized recommendations | Copilot assisted coding |
|---|---|---|---|---|
| Bing | Office | Microsoft Teams | XBOX | GitHub |

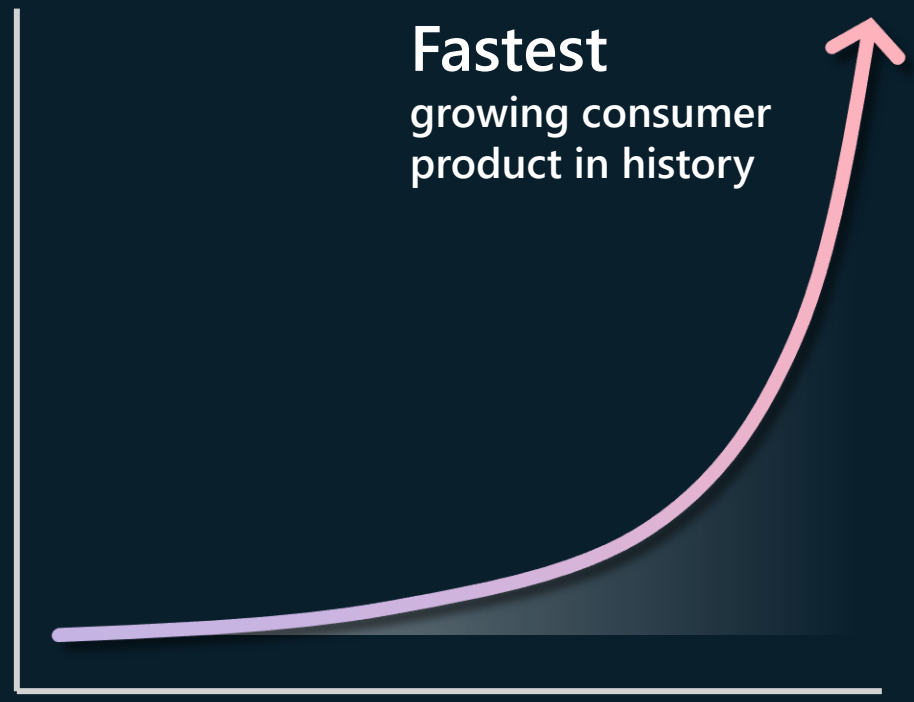
# Azure powers OpenAI and ChatGPT

ChatGPT

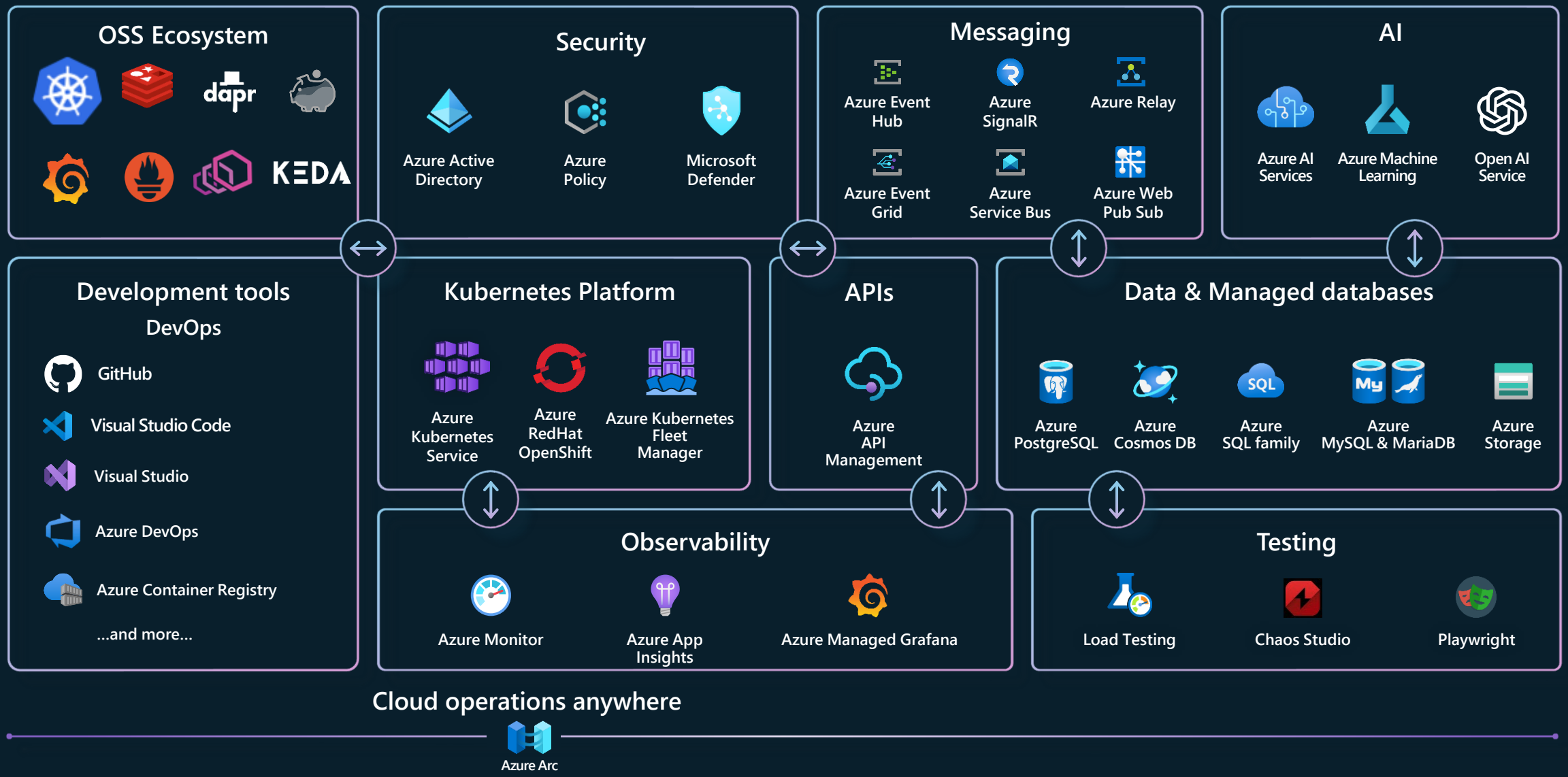
Runs on Azure Kubernetes Service (AKS)

Backed by Azure Cosmos DB

Developed on GitHub



# End to End Cloud Native Platform



# Developer experience

# What does it look like for developers on Kubernetes?

Bootstrapping and development

Continuous deployment

Observability, testing, and scaling

# Code-to-cloud with AKS

## Zero to sixty in seconds

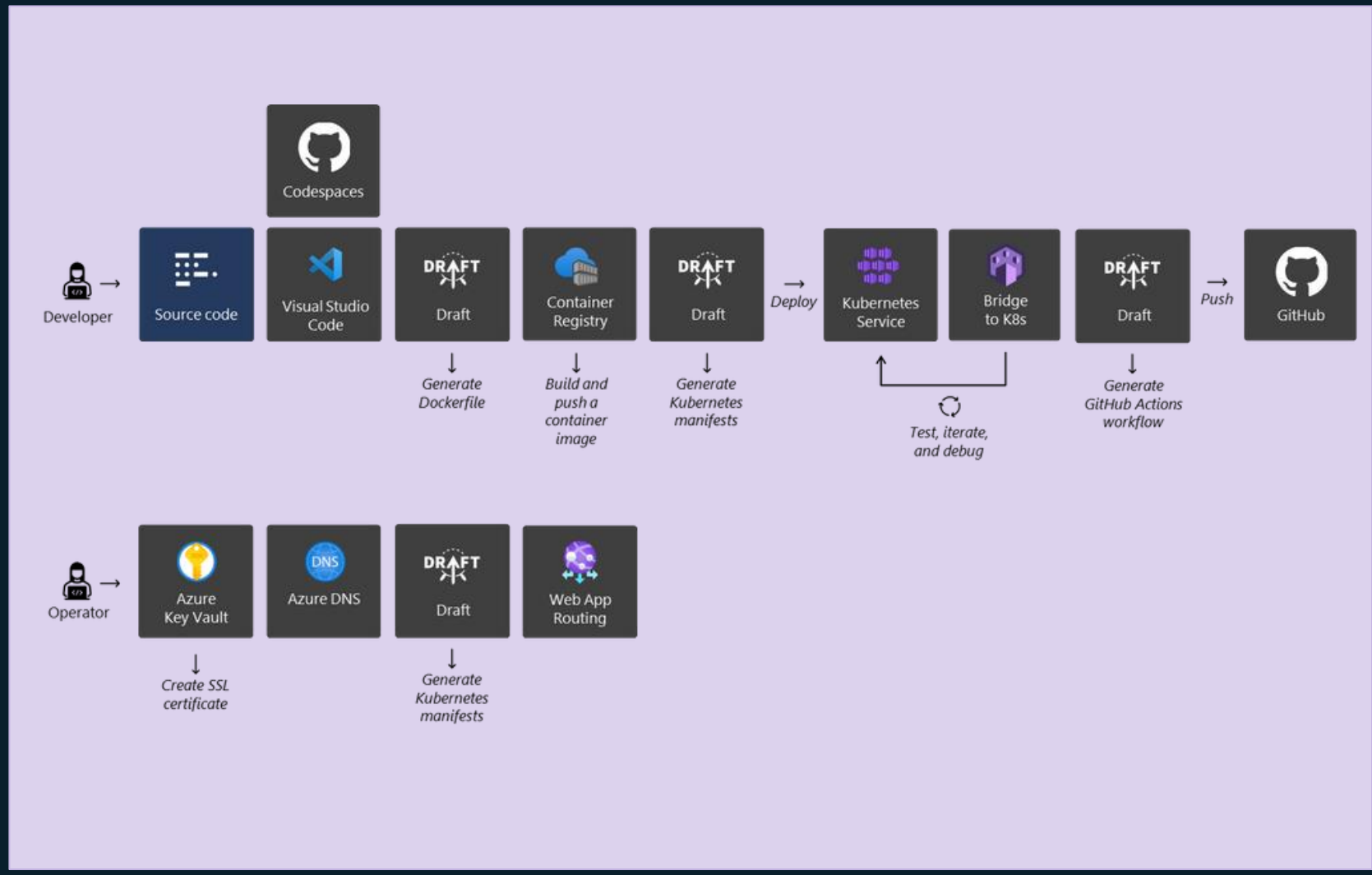
- Quickly bootstrap containerized applications with Automated Deployments (w/ Draft)
- Easily create extensible CI/CD pipelines with GitHub actions

## Common tasks made simple

- Auto-complete K8s manifests in VS Code
- Easily and securely expose endpoints with App Routing
- Scale on app-centric metrics via KEDA

## Optimized for microservices

- Leverage hardened microservice patterns with Dapr
- Debug microservices locally without mocks using Bridge to Kubernetes



Work | Create a resource - Microsoft Az | https://ms.portal.azure.com/#create/hub

Microsoft Azure (Preview) | Search resources, services, and docs (G+/) | MICROSOFT (MICROSOFT.ONMI...

Home >

# Create a resource

...

Get Started

Recently created

**Categories**

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

IT & Management Tools

Media

Migration

Mixed Reality

Monitoring & Diagnostics

Networking

Security

Storage

Search services and marketplace

Getting Started? Try our Quickstart center

## Popular Azure services

See more in All services

**Azure Kubernetes Service (AKS)**
Create | Docs | MS Learn

**Web App for Containers**
Create | Docs | MS Learn

**Batch Service**
Create | Docs | MS Learn

**Kubernetes - Azure Arc**
Create | Docs | MS Learn

**Container App**
Create | Docs

**Container Instances**
Create | Learn more | MS Learn

**Container Registry**
Create | Docs | MS Learn

**Service Fabric Cluster**
Create | Docs

## Popular Marketplace products

See more in Marketplace

**Windows Server 2022 Core Datacenter Minimal OS**
Create | Learn more

**Basic**
Create | Learn more

**Hyper-V Server on Windows Server 2016**
Create | Learn more

**Docker Engine Community on Ubuntu 20.04 LTS**
Create | Learn more

**Docker Compose Server on Windows Server 2016**
Create | Learn more

**Pay-as-You-Go**
Set up + subscribe | Learn more

**Docker 20.10 with Portainer 2.6 on Ubuntu 20.04**
Create | Learn more

**Docker Compose Server on Ubuntu Server 20.04**
Create | Learn more

**container**
Create | Learn more

**Docker on Ubuntu 20.04 LTS**

17°C Cloudy

# Dealing with Upgrade Complexities

Staying within a supported K8s version

Keep upgrade success rate high

Avoiding workload disruptions

# AKS Upgrade Strategy

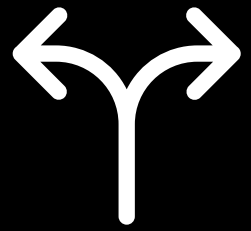
| | |
|---|---|
| Staying within a supported K8s version | • Automated upgrade framework<br>• OS Upgrade Channel<br>• Long Term Support (LTS)<br>• Platform Support up to N-3 (Coming: AKS-initiated auto-upgrades) |
| Keep upgrade success rate high | • Upgrade Dry-run, PDB validation<br>• Upgrade groups<br>• Soak time, maxSurge default<br>• AKS Release Tracker |
| Avoiding workload disruptions | • Breaking change detection and Pre-flight checks<br>• Clear status updates<br>• Planned maintenance<br>• Upgrade Rollback / Reset<br>• Workload metrics-based upgrade |

# AKS Kubernetes version Long Term Support (LTS)

Two years of Microsoft support, including CVEs and critical bugs

Upgrade available to the next AKS Kubernetes LTS

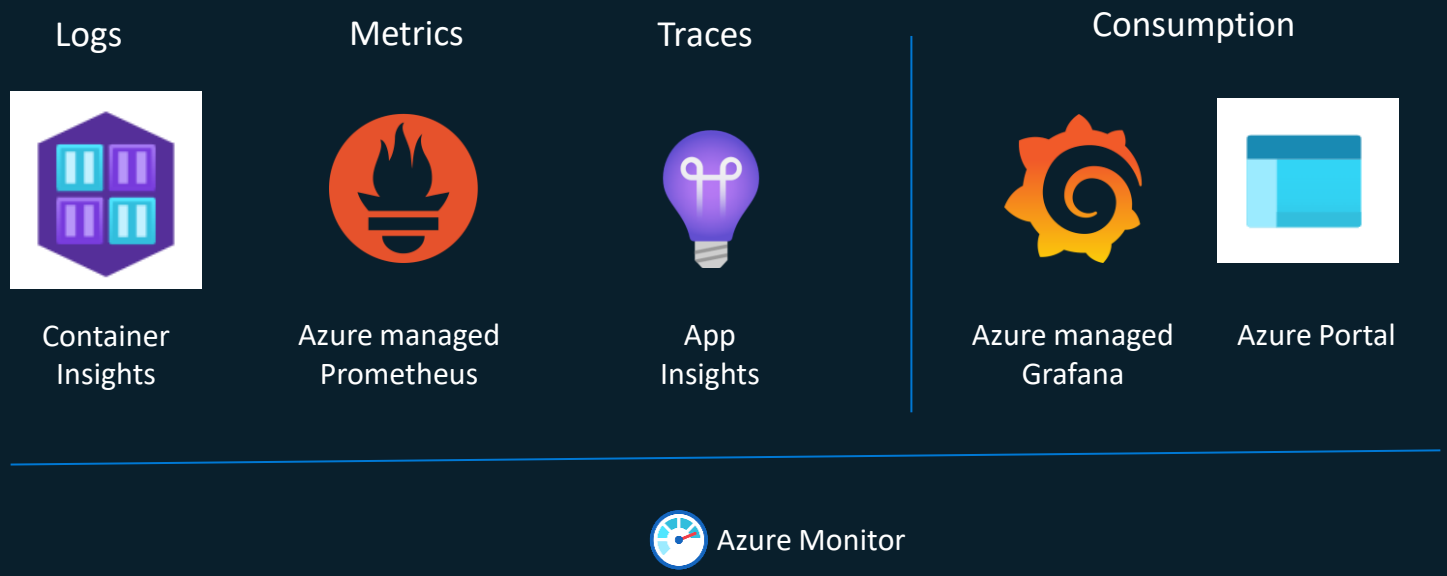
Ability to return to the upstream version train



Forked after upstream EOL, maintained by Microsoft

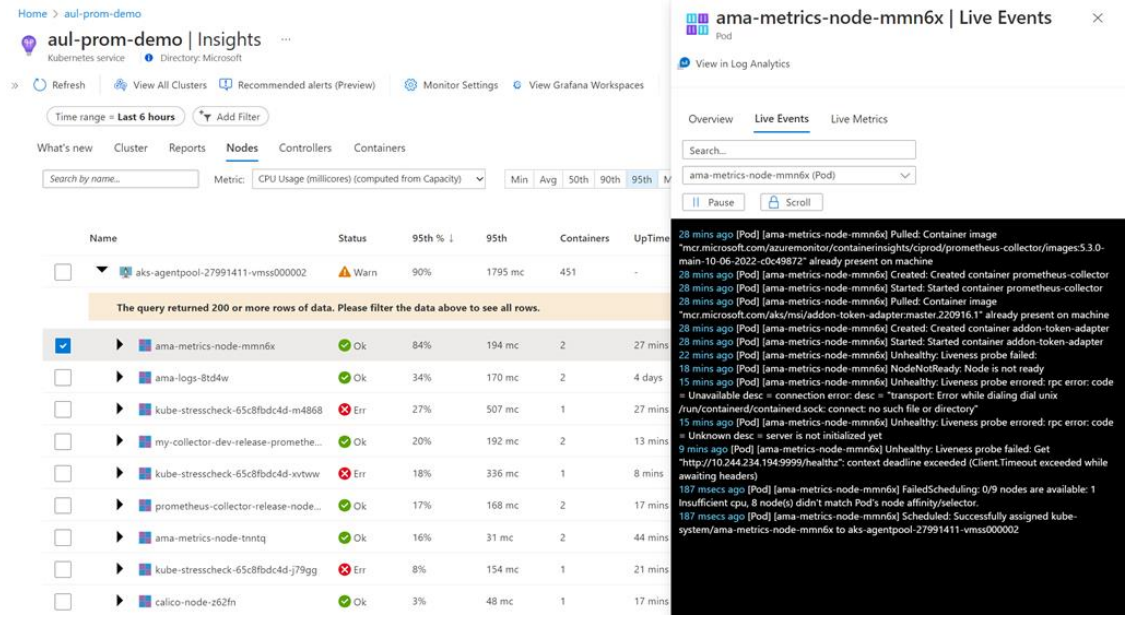
# Instrumentation, observability & alerting

# Instrumentation, observability & alerting



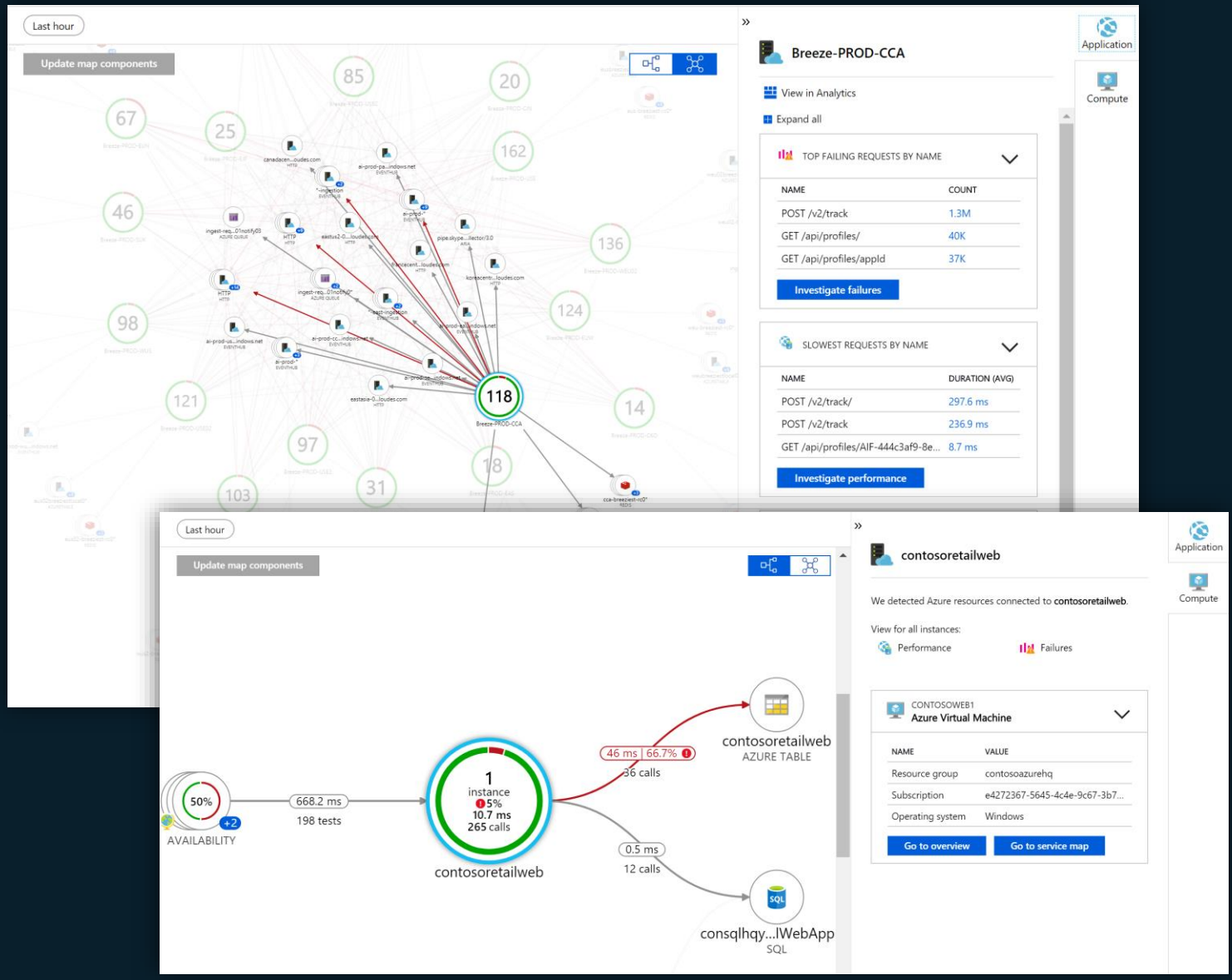
# Container Insights

- Collects troubleshooting logs and Live cluster events
- Recommended alerts to proactively identify
- Visualizations to monitor health and performance of your cluster
- Complements Prometheus and Grafana for end-to-end Kubernetes monitoring across microservices and infrastructure



# Application Insights

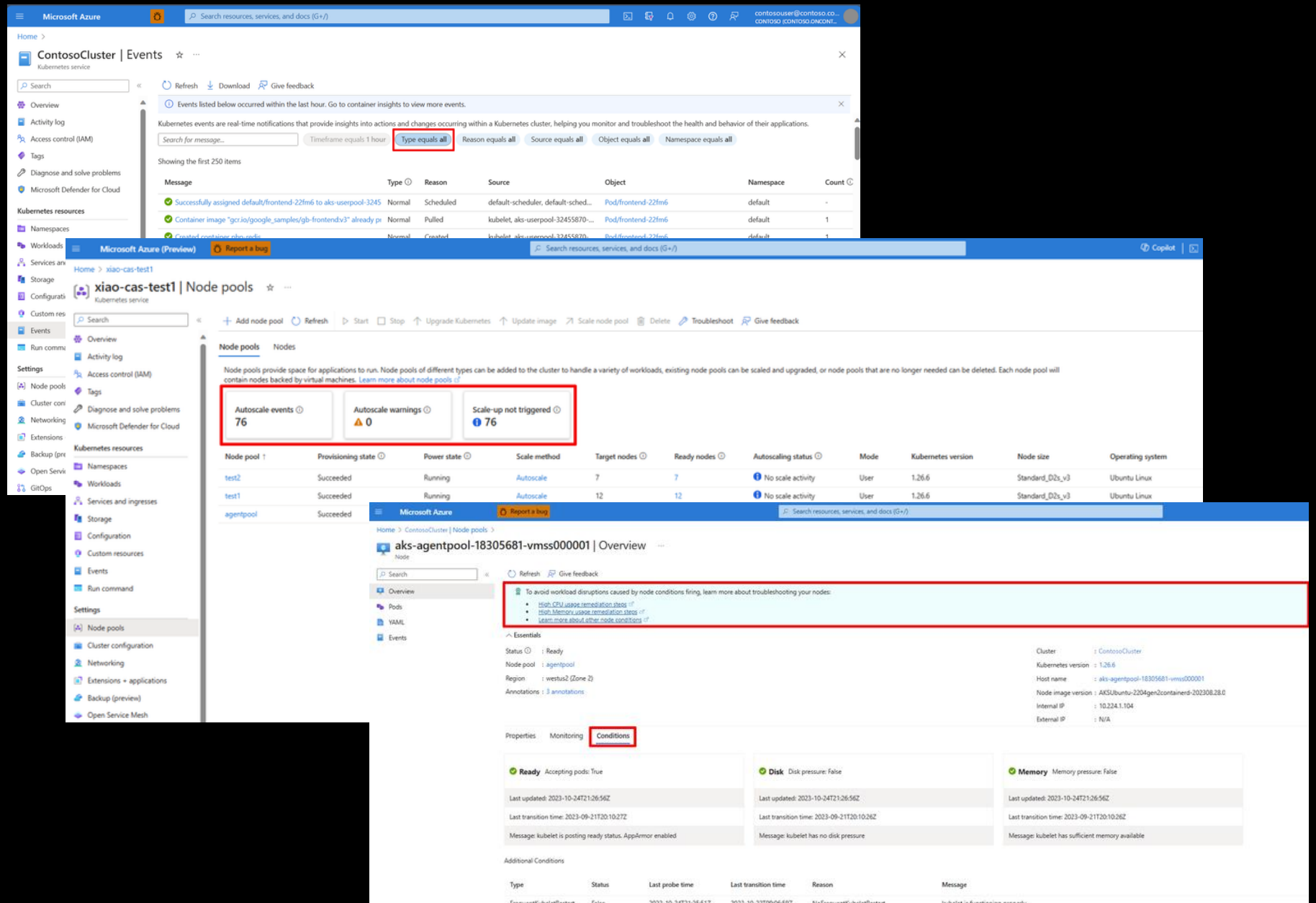
- Available on all major RPs – AKS, App Services, Functions and more.
- Monitor apps in .NET, Python, Java, Node.js or any other language with OSS SDKs
- Ditsributed tracing via App Map and End to End transaction details
- Transition with 1-click from App Map to VM Map for diagnostics
- Monitor calls to SQL, Eventhub, Cosmos Db, etc.
- Visualize events & metrics in real time with Live Metrics Stream



# Enhanced Cluster Troubleshooting

*In the portal today*

- Kubernetes Events: Real-time Cluster Signals
- Cluster Autoscaler Metrics: Resource Allocation Fine-Tuning
- Optimizing Node Performance with Node Saturation Metrics



# AKS Monitoring

## Optimized for cost and streamlined operations

### Frequency

Specify how often to collect data between 1 and 30min

### Namespace

Include or exclude specific namespaces from data ingestion

### Per-table config

Individually select which data tables to ingest into your Log Analytics workspace

### Basic logs

Reduced ingestion cost with basic query capabilities, ideal for verbose logs and sporadic troubleshooting cases

# Reduce cost and streamline operations

# AKS Cost Analysis

*aka.ms/aks/cost-analysis*

Azure native experience for cost visibility and allocation

Built on top of open source, vendor neutral CNCF sandbox project OpenCost

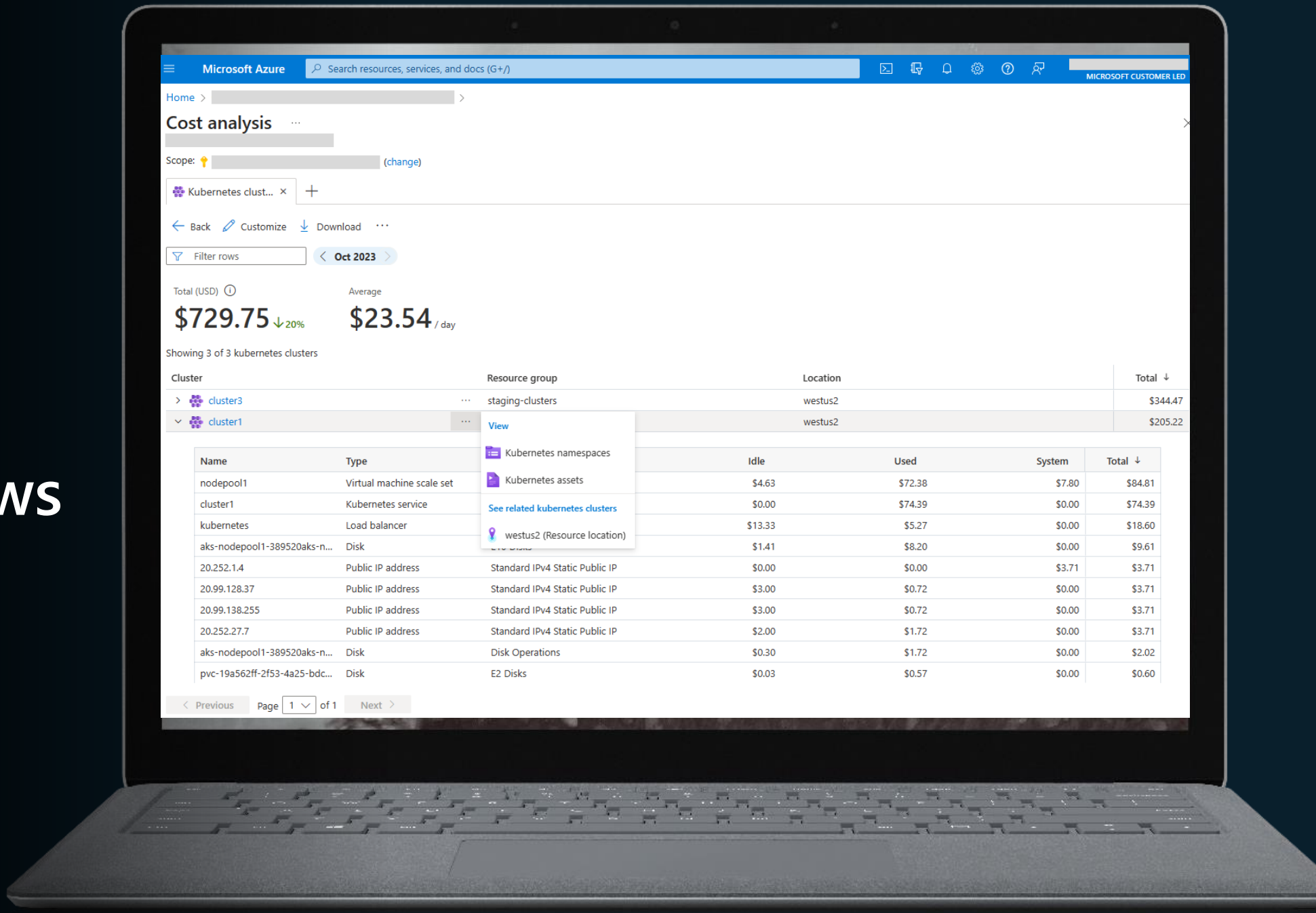
Available for Standard and Premium tier AKS clusters at no additional cost

Ensure costs are allocated to the right teams to drive accountability

Identify high spend areas and opportunities to optimize costs

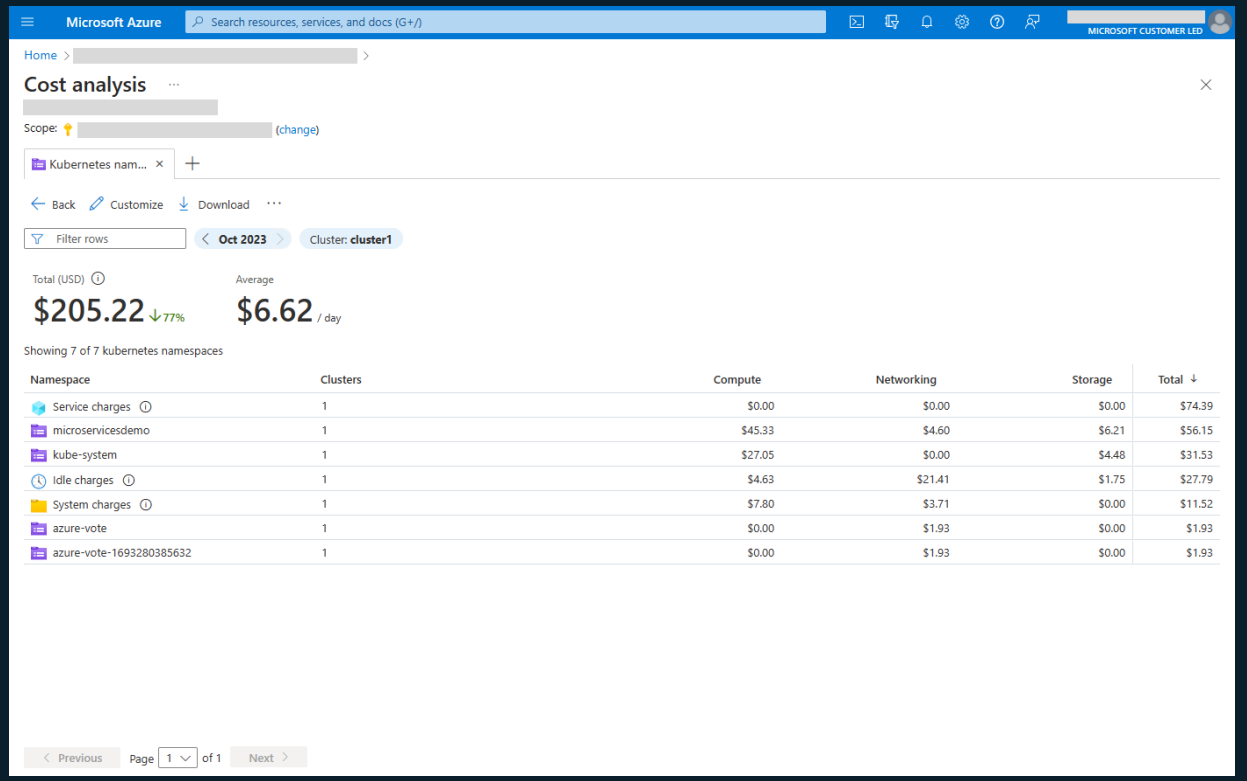
Proactively identify cost anomalies to prevent unanticipated overspending

# Kubernetes specific views

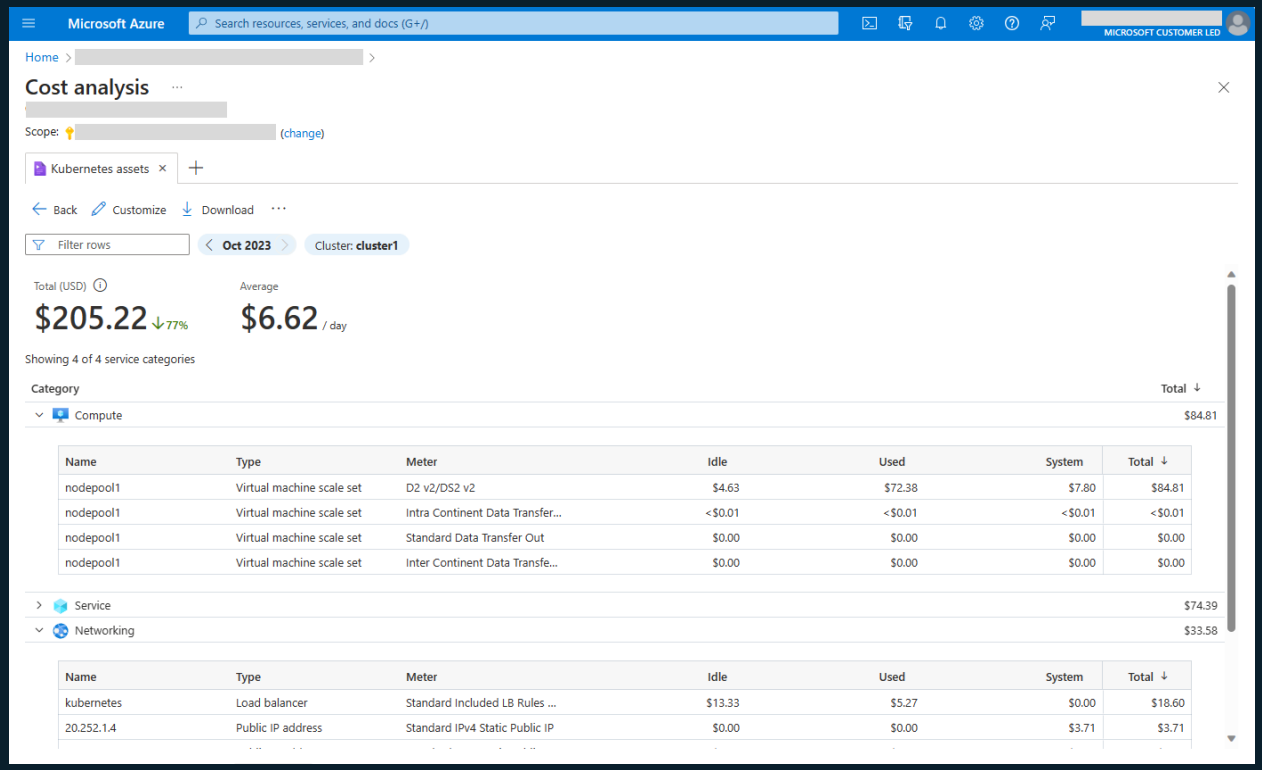



*Kubernetes cluster view*

## *Kubernetes namespace view*




## *Kubernetes assets view*



# AI everywhere

# Microsoft Copilot for Azure

An AI companion that simplifies how you design, operate, optimize, and troubleshoot both apps and infrastructure from cloud to edge.

Available initially in Azure portal. Expanding to Azure mobile app and CLI.

# Microsoft Copilot for Azure

## Generate deep insights instantly

Find personalized solutions for your workloads with an AI assistant that knows your environment.

## Discover new cloud functionality

Ask Copilot questions using natural language to discover and utilize the full functionality of Azure services.

## Do complex tasks faster

Optimize processes, resources, and workloads with AI orchestration and analysis.

**aka.ms/MSCopilotforAzurePreview**

store-front | store-admin | ws75043a084 - Microsoft Azure

https://ms.portal.azure.com/?feature.drilldown=true&feature.apiversion=2023-04-01-preview&feature.aksview=true&feature.canmodifystamps=true&microsoft_azure_costm...

Microsoft Azure (Preview) | Search resources, services, and docs (G+/) | Copilot | MICROSOFT (MICROSOFT.ONMI...

Dashboard > petsupply-1 | Node pools >

# ws75043a084 | Overview

Node pool

Search

- Overview
- Nodes
- Configuration

Start | Stop | Upgrade Kubernetes | Update image | Scale node pool | Delete | Refresh | Give feedback

## Essentials

| | | | |
|---|---|---|---|
| Provisioning state | : Succeeded | Cluster | : petsupply-1 |
| Power state | : Running (1/1 nodes ready) | Operating system | : Ubuntu Linux |
| Availability zones | : None | Kubernetes version | : 1.27.3 |
| Mode | : User | Node count | : 1 node |
| | | Node size | : Standard_NC12s_v3 |

Properties | Monitoring

### Node pool

| | |
|---|---|
| Max pods per node | 250 |
| Public IPs per node | Disabled |
| Autoscaling | Disabled |
| Azure Spot Instance | Disabled |
| Maximum price | N/A |
| Scale eviction policy | N/A |
| Node image version | AKSUbuntu-2204gen2containerd-202310.31.0 |
| Proximity placement group | N/A |

### Taints and labels

Taints: sku=gpu:NoSchedule

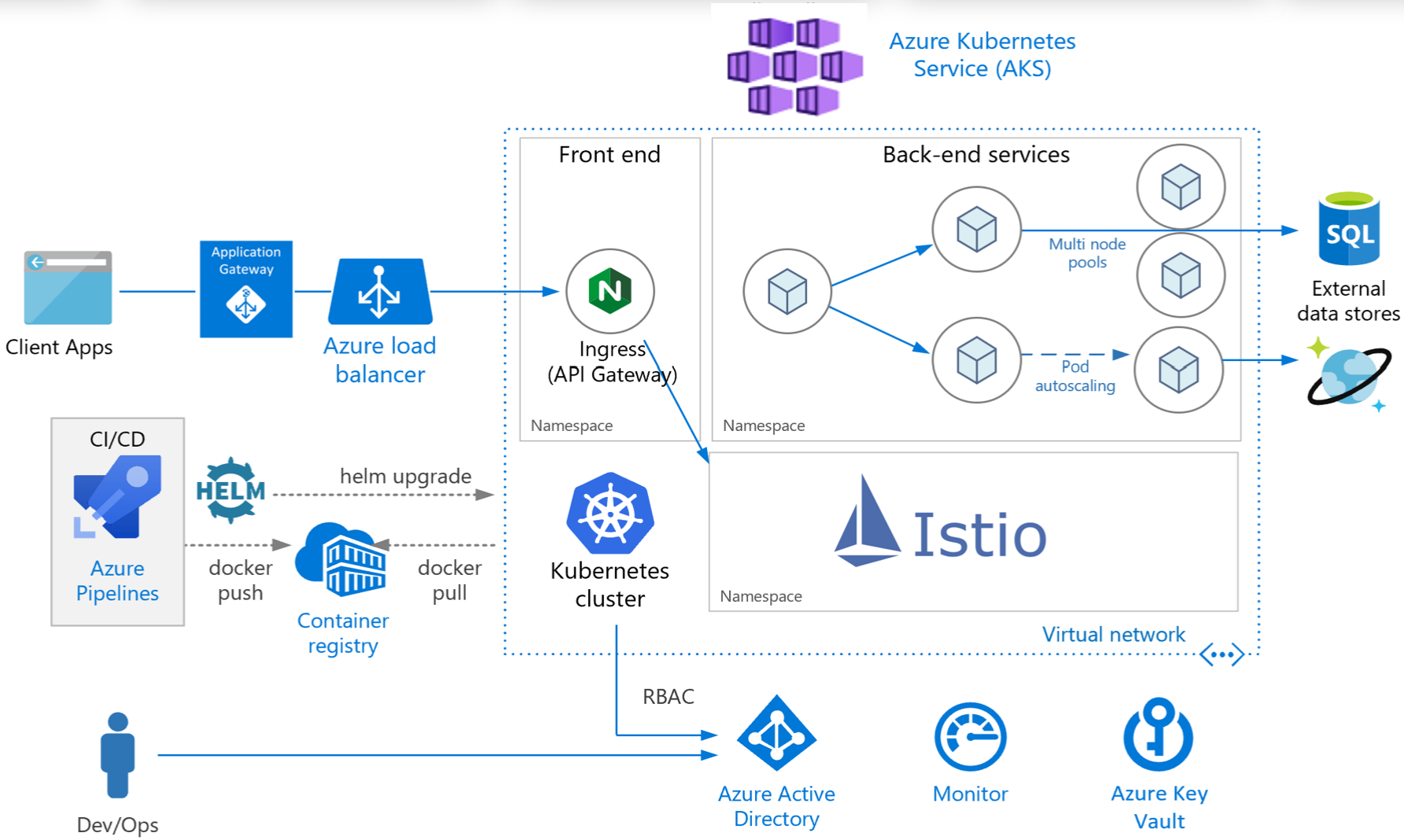
Labels:
- apps : falcon-7b
- kaito.sh/machine-type : gpu
- kaito.sh/workspace : workspace-falcon-7b
- kaito.sh/workspacenamespace : store
- karpenter.sh/provisioner-name : default

### Configuration

| | |
|---|---|
| Mode | User |
| Maximum surge | Default |
| Node drain timeout | 30 |
| OS disk size | 128 GB |
| OS disk type | Ephemeral |

# security

Build Security | Registry Security | Cluster Security | Infrastructure Security | Application Security



# Azure Policy

AKS Built-in policy to harden cluster and applications

Leverage Custom Policy to craft your own policies

## Azure Policy built-in definitions for Azure Kubernetes Service

Article • 11/15/2023 • 6 contributors

Feedback

### In this article



This page is an index of Azure Policy built-in policy definitions for Azure Kubernetes Service. For additional Azure Policy built-ins for other services, see Azure Policy built-in definitions.

The name of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Version** column to view the source on the Azure Policy GitHub repo.

## Initiatives

| Name | Description | Policies | Version |
|---|---|---|---|
| [Preview]: Use Image Integrity to ensure only trusted images are deployed | Use Image Integrity to ensure AKS clusters deploy only trusted images by enabling the Image Integrity and Azure Policy Add-Ons on AKS clusters. Image Integrity Add-On and Azure Policy Add-On are both pre-requisites to using Image Integrity to verify if image is signed upon deployment. For more info, visit https://aka.ms/aks/image-integrity. | 3 | 1.1.0-preview |
| [Preview]: AKS Guardrails should help guide developers towards AKS recommended best practices | A collection of Kubernetes best practices that are recommended by Azure Kubernetes Service (AKS). For the best experience, use AKS Guardrails to assign this policy initiative: https://aka.ms/aks/guardrails. | 11 | 1.3.1-preview |
| Kubernetes cluster pod security baseline standards for Linux-based workloads | This initiative includes the policies for the Kubernetes cluster pod security baseline standards. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For instructions on using this policy, visit https://aka.ms/kubepolicydoc. | 5 | 1.4.0 |
| Kubernetes cluster pod | This initiative includes the policies for the Kubernetes cluster pod | 8 | 2.4.0 |


question