



WorkshopPLUS - Containers as Infrastructure

Containers Solutions Monitoring

Microsoft Services



Objectives

- Learn about Azure Monitor
- Understanding Azure Monitor Agents
- Learning to use Azure Monitor Search, Alerts and related services
- Using Azure Monitor with Containers, Kubernetes and Service Fabric
- Learning Kubernetes Security Best Practices



Containers Solutions Monitoring

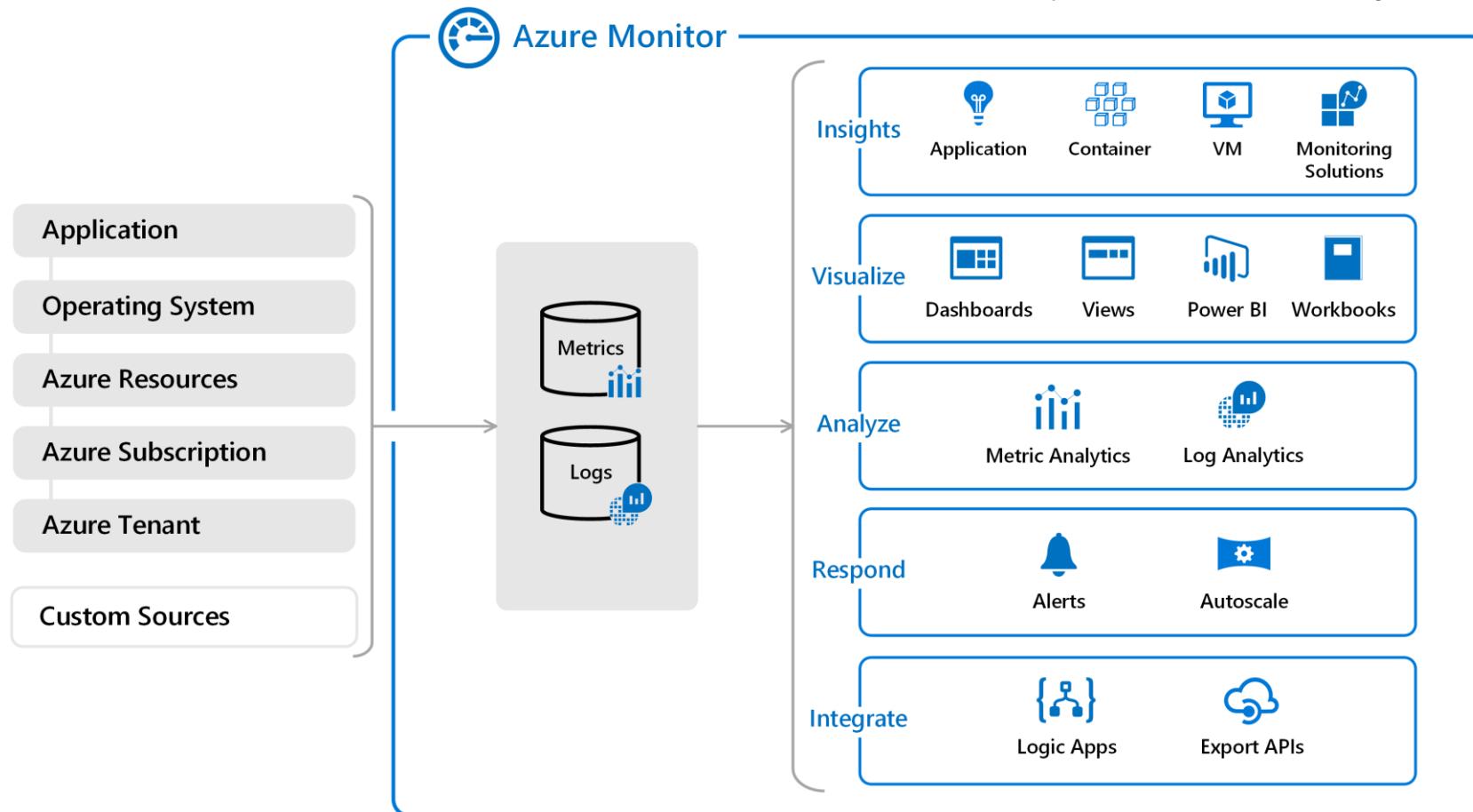
Azure Monitoring High Level View

Microsoft Services



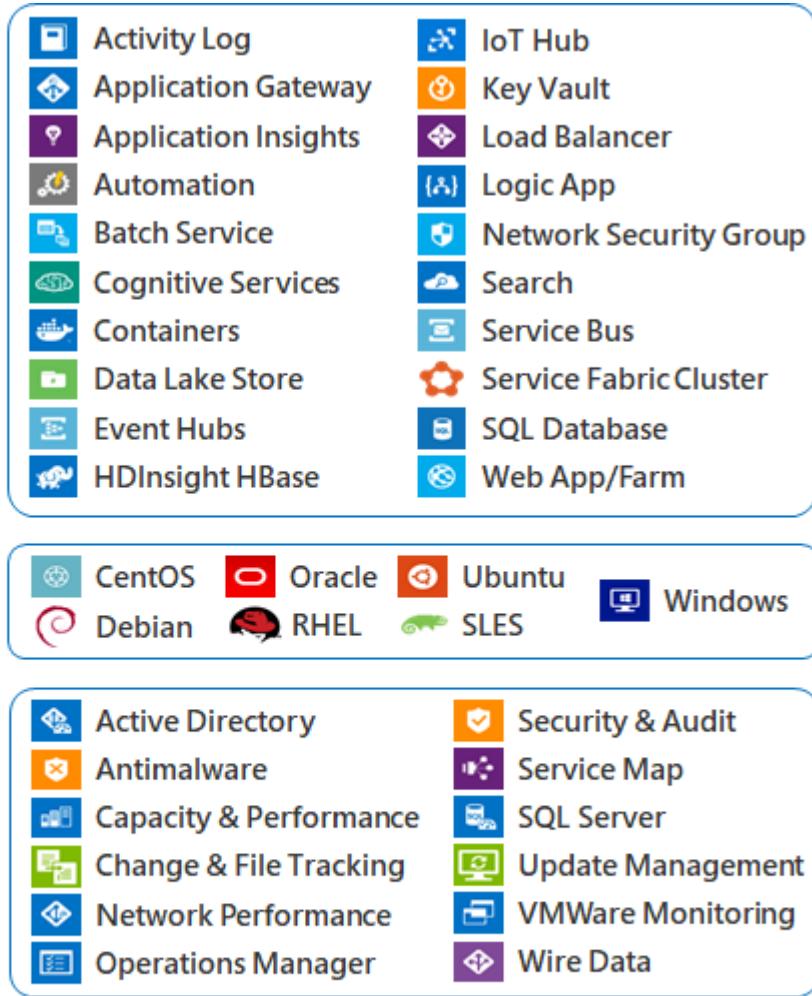
Azure Monitor

Log Analytics and Application Insights have been consolidated into Azure Monitor to provide a single integrated experience for monitoring Azure resources and hybrid environments. No functionality has been removed from these services, and you can perform the same scenarios as before with no loss or compromise of any features.

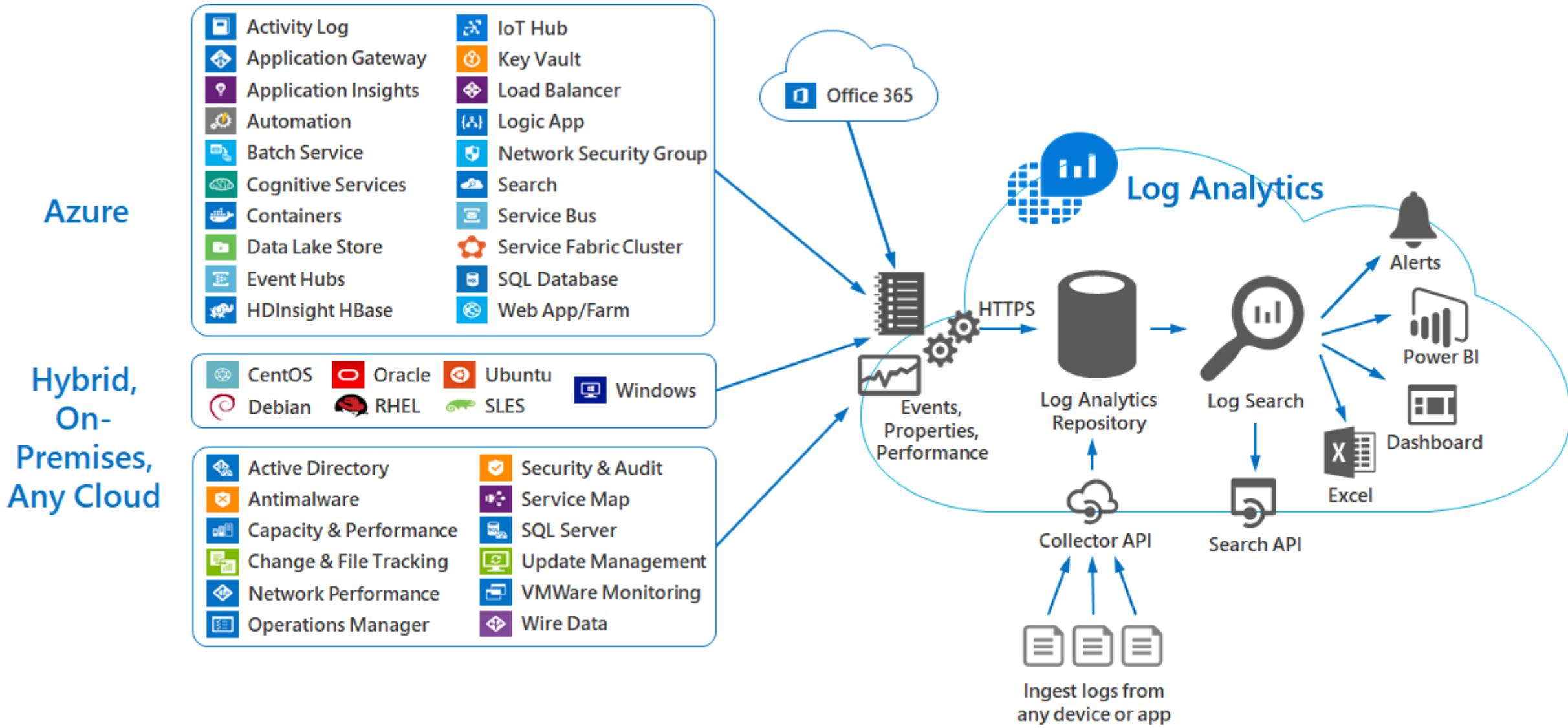


The view from above – custom logs

Azure
Hybrid,
On-
Premises,
Any Cloud

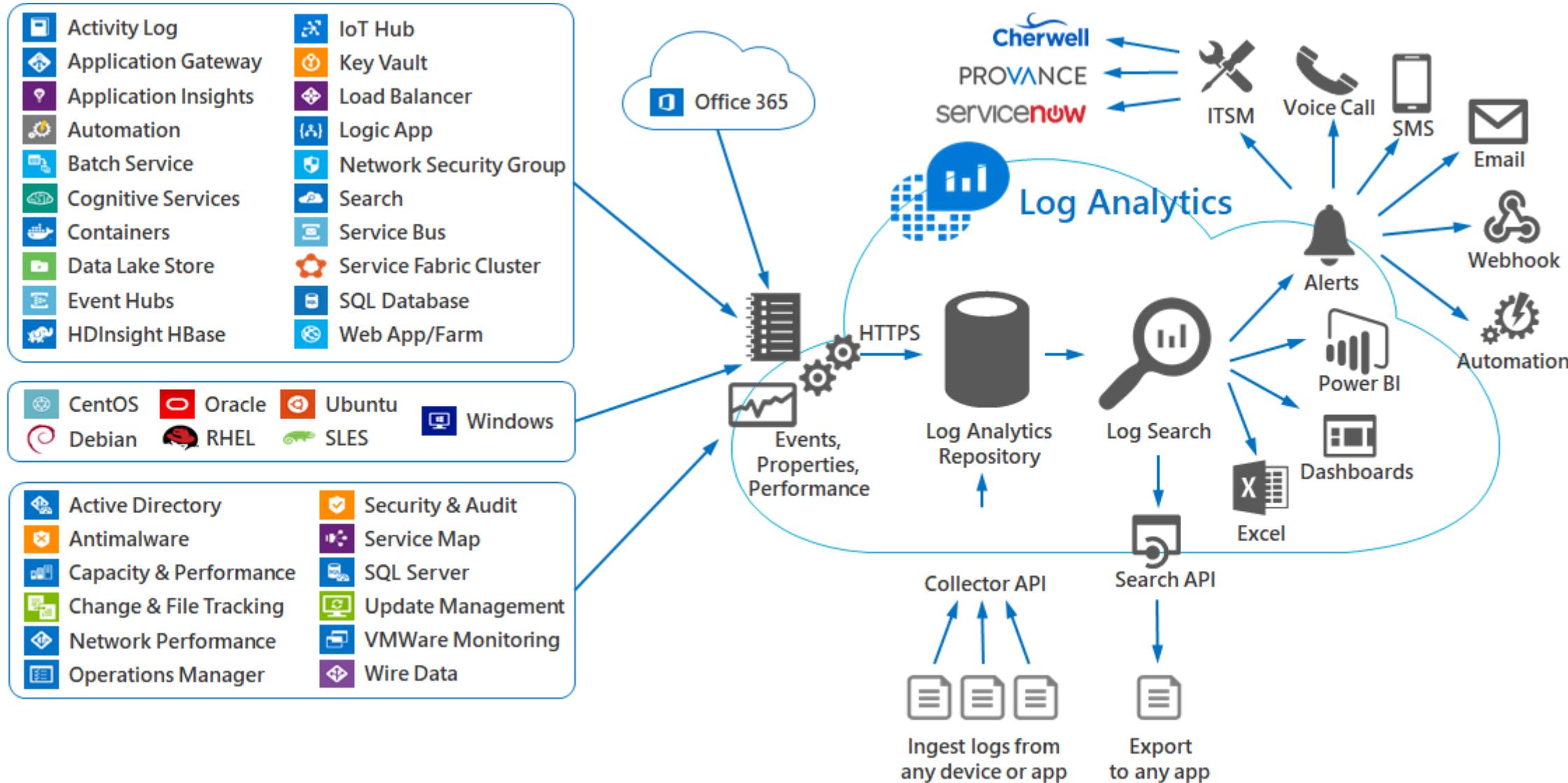


The view from above – extracting data



The view from above – alert remediation

Azure
Hybrid,
On-
Premises,
Any Cloud



Log Analytics – Data Retention

- Default is a 30 days retention (extendable for up to 2 years)
- Azure Activity Log is 90 days default (extendable up to 2 years)



Containers Solutions Monitoring

Azure Monitor Agents

Microsoft Services



Log Analytics Agent

- Developed for comprehensive management across on-premises machines, computers monitored by SCOM, and virtual machines in any cloud
- Windows and Linux agents attach to Azure Monitor, storing collected log data from different sources in your Log Analytics workspace
- Additionally stores unique logs or metrics as defined in a monitoring solution
- Both Linux and Windows agents communicate outbound to the Azure Monitor service over TCP port 443
- Agent is only available for Azure Kubernetes Service and Service Fabric; it can't be used with Azure Container Instance

Agent Deployment

- Azure Security Center: when data collection is enabled, the Log Analytics Agent is automatically provisioned on all existing and any new supported virtual machines that are deployed in the subscription.
- Azure CLI: for Service Fabric and AKS cluster using Virtual Machine Scale Set you deploy the agent by targeting the VMSS.
- Azure Resource Manager: you can also use an ARM template to deploy the agent during the cluster creation.



Containers Solutions Monitoring

Azure Monitor Logs Search

Microsoft Services

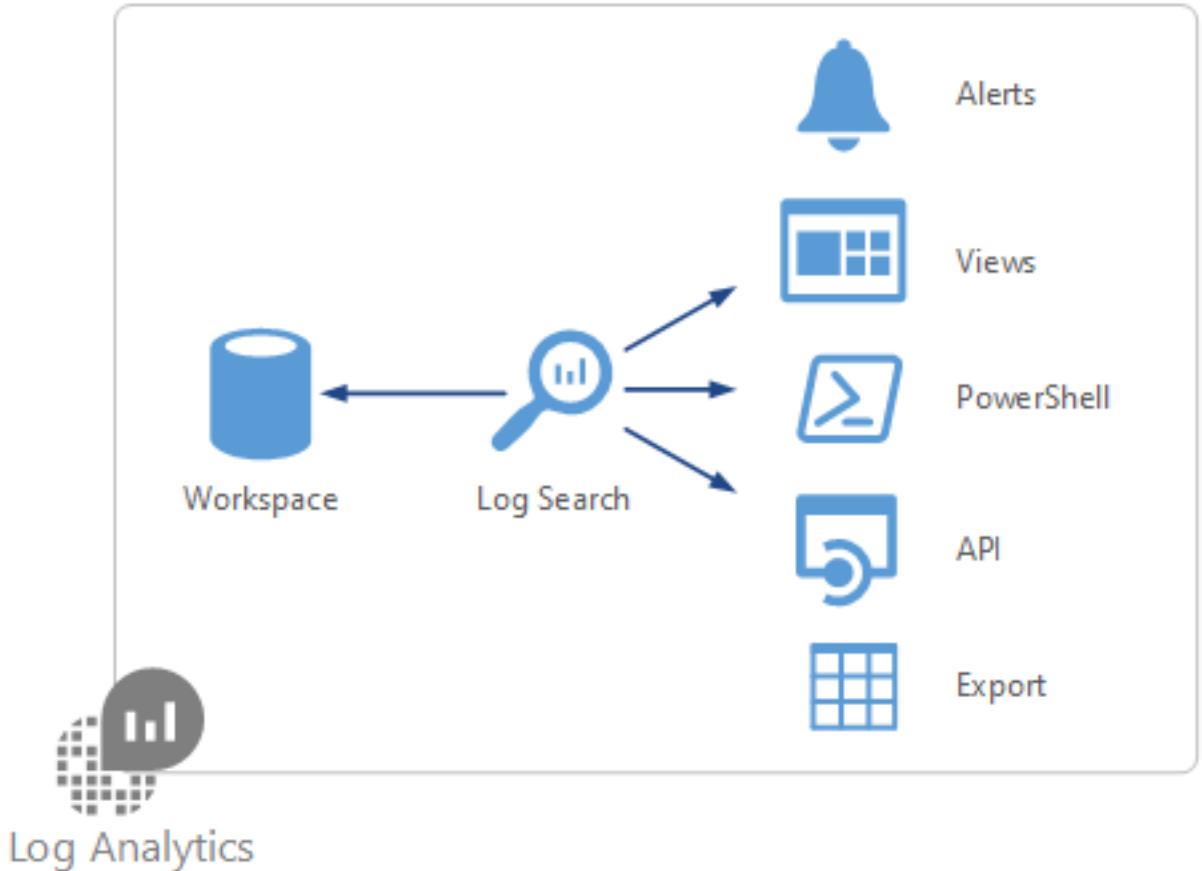


Log Search Overview

- Simple and powerful
- Full piping language
- Search-time field extractions
- Advanced queries (joins, multiline queries, advanced date/time functions)
- Smart Analytics (Advanced algorithms)
- Consistency with other applications (Application Insights)
- Integration with Power BI

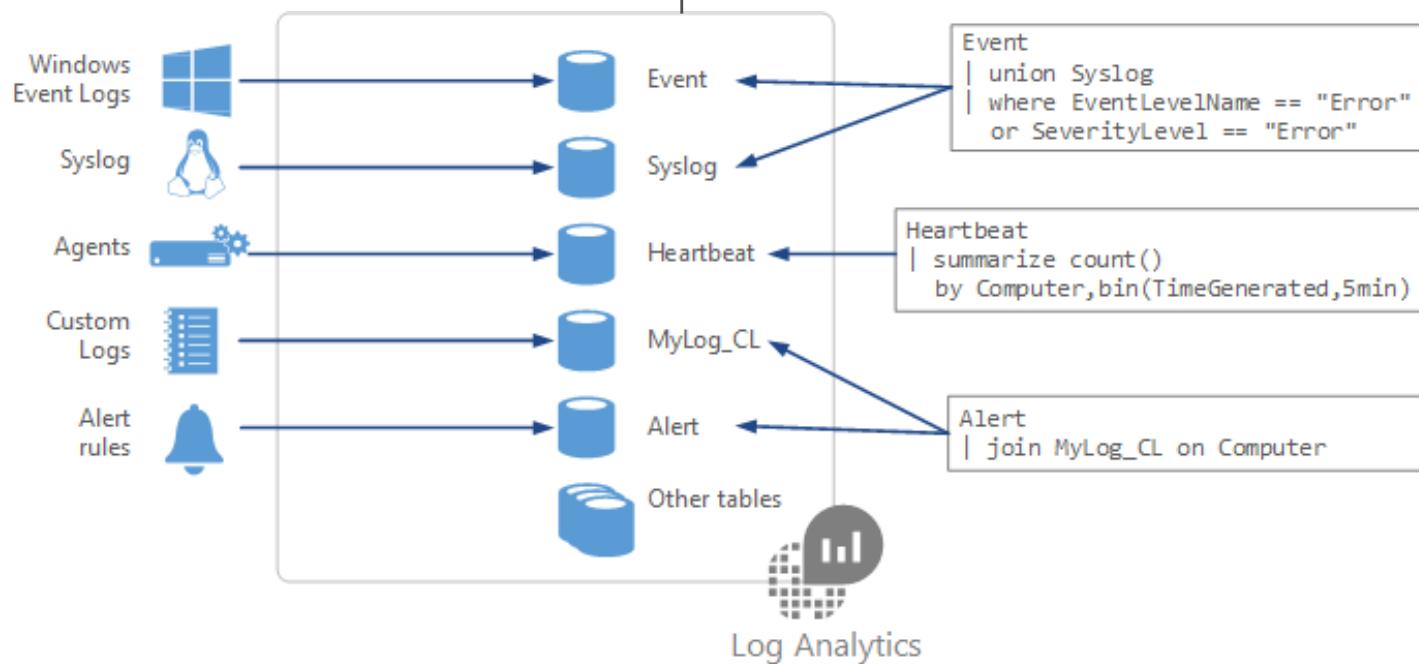
Where Log Searches are Used

- Portals
- Alert Rules
- Views
- Export
- PowerShell
- Log Analytics Search API



How Log Analytics Data is Organized

- When writing a query
 - Determine which tables have the data that you're looking for
 - Each data source and solution stores its data in dedicated tables
 - Each data source and solution includes the name of the data type and a description of each of its properties.
- Each query can include data from multiple tables



Viewing and analyzing data - Log Analytics page

- Open the Log Analytics page from Logs in the Log Analytics menu
- The Log Analytics page provides:
 - Multiple tabs
 - Rich visualizations
 - Intellisense and language auto-completion
 - Syntax highlighting
 - Query explorer
 - Schema view
 - Share
 - Smart Analytics
 - Column selection

The screenshot shows the Azure Log Analytics interface. At the top, there's a search bar with the text "contosoretail-it", a "RUN" button, and a time range selector set to "Last 24 hours". Below the search bar is a schema view on the left, listing various log types under the "ACTIVE" section. The main area displays a table of event logs. The table has columns: TimeGenerated [Local Time], Computer, EventLevelName, Source, and EventID. The data shows several error events from different sources like ContosoAzADDS1, sqlserver-1, and mycon. The table includes pagination controls at the bottom.

TimeGenerated [Local Time]	Computer	EventLevelName	Source	EventID
2018-08-15T08:28:34.953	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:28:44.000	sqlserver-1.contoso.com	Error	MSSQLSERVER	9,642
2018-08-15T08:09:32.093	ContosoAzADDS1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031
2018-08-15T08:10:10.703	mycon	Error	Microsoft-Windows-Perflib	1,023
2018-08-15T07:50:09.190	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T07:50:15.447	ContosoWeb1.ContosoRetail.com	Error	Microsoft-Windows-CAPI2	513
2018-08-15T08:02:32.517	On-Premise-16S	Error	Microsoft-Windows-Perflib	1,008
2018-08-15T07:39:30.017	ContosoMABSV1.ContosoRetail.com	Error	Microsoft-Windows-COMRuntime	10,031



Containers Solutions Monitoring

Azure Monitor Alerts

Microsoft Services



Azure Monitor - Alerts

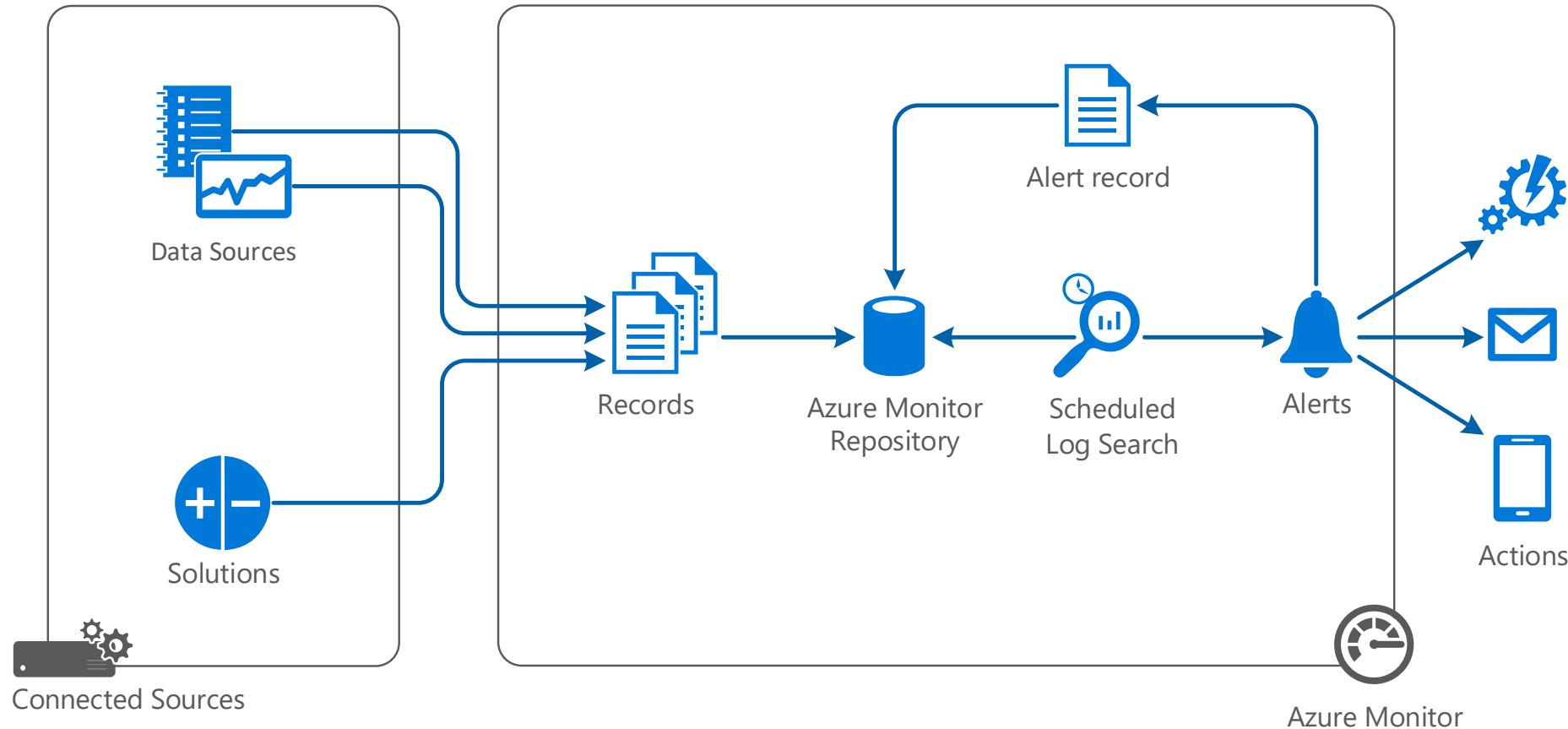
Alert on your Azure services:

- Metric values: Triggers when value of a specified metric crosses threshold
- Activity log events: Trigger on every event or only when certain events occurs

Alert based on an Azure Log Analytics Search:

- Custom Search
- Saved Search Query

Alerts - Flow



Alerts – General

Alert rule has three parts:

- Target Resource defines the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace or an Application Insights resource.
 - Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.
- Criteria is the combination of Signal and Logic applied on a Target resource, e.g.:
 - Percentage CPU > 70%
 - Server Response Time > 4 ms
 - Result count of a log query > 100
- Action is a specific call sent to a receiver of a notification - email, SMS, webhook etc.

Alerts – Create Rule

1. Define alert condition

- Alert Target (Log Analytics WS)
- Target Criteria

2. Define alert details

- Alert rule name
- Description
- Severity

3. Define action group

- Action Group
- Customize Actions

Create rule

Rules management



* RESOURCE

MIPDemo1-LA

HIERARCHY

Microsoft AIC - jp > MIPDemo-RG



* CONDITION

No condition defined, click on 'Add condition' to select a signal and define its logic

Add



ACTIONS

ACTION GROUP NAME

CONTAIN ACTIONS

No action group selected

Select action group

Create action group

ALERT DETAILS

* Alert rule name 

Specify alert rule name. Sample: 'Percentage CPU greater than 70'

Description

Specify alert description here...

Enable rule upon creation

Yes

No

Create alert rule

Alerts – Target criteria

- Search query
- Alert logic
 - Number of Results
 - Metric Measurement
- Evaluated based on
 - Period (in minutes)
 - Value of 5 minutes to 24 hours
 - Should be greater than or equal to how often the query runs
 - Frequency

Configure signal logic

[Back to signal selection](#)

Custom log search

Pivoted on ClusterName=MIPDemoAKS Time range last 15 minutes

Time	Value
7:38 PM	100
7:43 PM	100
7:48 PM	100

* Search query

```
let clusterName = 'MIPDemoAKS';
KubeNodeInventory
| where ClusterName == clusterName
```

View result of query in Azure Monitor - Logs

Query to be executed : `let clusterName = 'MIPDemoAKS'; KubeNodeInventory | where ClusterName == clusterName | summarize AggregatedValue=(sumif(1, Status contains ('Ready'))* 100.0) / count() by ClusterName , bin_at(TimeGenerated, 5min, now())`
For time window : 9/30/2019, 7:33:08 PM - 9/30/2019, 7:48:08 PM

ⓘ It may take in the range of 3 minutes, to have the logs available for provided query [Learn more](#)

Alert logic

Based on Metric measurement Operator Less than Threshold value 75

Trigger Alert Based On

Consecutive breaches Equal to 2

Aggregate on ClusterName

Condition preview

Whenever aggregated value metric in **Custom log search** log query for last 15 minutes is less than 75 and occurring in consecutive equal to 2 bins, pivoted on clustername. Evaluated every 5 minutes.

Evaluated based on

* Period (in minutes) 15 Frequency (in minutes) 5

[Done](#)

Alerts – Add action group

- Action group name (Unique in subscription)
- Short name (<12 char)
- Subscription
- Resource group
- Actions
 - Action Name
 - Action Type

Add action group X

* Action group name i	Contact AKS Admin.	✓
* Short name i	AKSAdmin	✓
* Subscription i	Microsoft AIC - jp	▼
* Resource group i	MIPDemo-RG	▼

Actions

ACTION NAME	ACTION TYPE	STATUS	DETAILS	ACTIONS
<input type="text" value="Unique name for the action"/>	Select an action type ^			
Privacy Statement	Automation Runbook			
Pricing	Azure Function			
	Email Azure Resource Manager Role			
	Email/SMS/Push/Voice			
	ITSM			
	LogicApp			
	Secure Webhook			
	Webhook			

i Have a consistent format in emails, notifications. [Learn more](#)

e of monitoring source. You can enable per action by editing details.

Alerts – Define alert details

- Alert rule name
- Alert Description
- Severity
 - Critical (Sev 0)
 - Warning (Sev 1)
 - Informational (Sev 2)
- Enable rule upon creation
- Suppress Alerts

ALERT DETAILS

* Alert rule name i

Specify alert rule name. Sample: 'Percentage CPU greater than 70'

Description

Specify alert description here...

* Severity i

Sev 3

Enable rule upon creation

Yes No

Suppress Alerts i

* Suppress alerts for (in minutes)

20

Alerts – View Alerts

Total alerts 18 Since 9/23/2019, 8:30:20 PM	Smart groups (Preview) ⓘ 2 88.89% Reduction	Total alert rules 8 Enabled 8	Action rules (preview) ⓘ 0 Enabled 0	Learn More About Alerts ↗
SEVERITY	TOTAL ALERTS	NEW	ACKNOWLEDGED	CLOSED
Sev 0	0	0	0	0
Sev 1	14 	13	0	1
Sev 2	0	0	0	0
Sev 3	0	0	0	0
Sev 4	4 	4	0	0



Containers Solutions Monitoring

Related Azure Services

Microsoft Services



Azure Security Center

Azure Security Center helps you identify and perform the hardening tasks recommended as security best practices and implement them across your machines, data services and apps.

Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL databases and storage accounts. These are monitored and protected by Security Center without necessitating any deployment.

The events collected from the agents and from Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks), that you should follow to make sure your workloads are secure, and gives you threat detection alerts.

Azure Security Center - Overview

Security Center - Overview
Showing subscription 'Microsoft AIC - jp'

Documentation X

Search (Ctrl+ /) Subscriptions What's new

Overview Getting started Pricing & settings

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

THREAT PROTECTION

- Security alerts

Policy & compliance

Secure score: 467 OF 610

Regulatory compliance:

- ISO 27001: 15 of 20 passed controls
- Azure CIS 1.1.0: 15 of 18 passed controls
- PCI DSS 3.2.1: 37 of 43 passed controls

Subscription coverage:

- Fully covered: 1
- Partially covered: 0
- Not covered: 0

Resource security hygiene

Recommendations:

- High Severity: 7
- Medium Severity: 0
- Low Severity: 2

Unhealthy resources: 9

Resource health by severity:

- Compute & apps resources: 4
- Data & storage resources: 3
- Networking resources: 4
- Identity & access resources: 3

Threat protection

Security alerts by severity:

- High Severity: 0
- Medium Severity: 0
- Low Severity: 0

No security alerts

Attacked resources: 0

Security alerts over time:

- High severity: 0
- Medium severity: 0
- Low severity: 0

No security alerts

Regulatory compliance

View your compliance posture relative to regulations that are important to you. Review assessments to watch your compliance.

Review and improve your secure score

Review and resolve security vulnerabilities to secure score and secure your workload.

New - Advanced threat protection for Storage accounts

Security Center can now protect your Storage accounts from detecting unusual and potentially harmful or exploit Storage accounts.

Azure Security Center – Compute & Apps Overview

Security Center - Compute & apps
Showing subscription 'Microsoft AIC - jp'

Search (Ctrl+/
Add Computers

Overview VMs and Computers VM scale sets Cloud services App services Containers (Preview)

Search recommendations

RECOMMENDATION	SECURE SCORE IMPROVEMENT	FAILED RESOURCES	SEVERITY
Pod Security Policies should be defined on Kubernetes Services (Preview)	+20	1 of 1 managed clusters	High
Authorized IP ranges should be defined on Kubernetes Services (Preview)	+20	1 of 1 managed clusters	High
Monitoring agent should be installed on virtual machine scale sets	1-Click Fix ! +15	1 of 2 virtual machine scale sets	Medium
Client authentication should use Azure Active Directory	+10	1 of 1 service fabric clusters	High
Diagnostic logs in Virtual Machine Scale Sets should be enabled	+3	1 of 2 virtual machine scale sets	Medium

Coverage Secure score Security policy Regulatory compliance

Recommendations Compute & apps Networking IoT Hubs & resources Data & storage Identity & access Security solutions

Azure Security Center - Recommendations

Pod Security Policies should be defined on Kubernetes Services (Preview)

^ Description

Define Pod Security Policies to reduce the attack vector by removing unnecessary application privileges. It is recommended to configure Pod Security Policies to only allow pods to access the resources which they have permissions to access.

^ General Information

Recommendation score	 ⓘ 0/20
Recommendation impact	 ⓘ +20
User impact	 ⓘ High
Implementation effort	 ⓘ Moderate

LEARN MORE

[Learn more about recommendations](#) ⓘ

[Learn how to disable the recommendation](#) ⓘ

^ Threats

- Elevation of privilege
- Data exfiltration

^ Remediation steps

Manual remediation:

To configure Pod Security Policies, follow the steps described here [Secure your cluster using pod security policies in Azure Kubernetes Service \(AKS\)](#).

^ Effected resources

[Unhealthy resources \(1\)](#) [Healthy resources \(0\)](#) [Unscanned resources \(0\)](#)

🔍 Search managed clusters

NAME

↑↓ SUBSCRIPTION

 **mipdemoaks**

Microsoft AIC - jp

Azure Sentinel - Overview

- Scalable, cloud-native security information event management (SIEM) and security orchestration automated response (SOAR) solution
- Delivers intelligent security analytics and threat intelligence across the enterprise
- Single solution for alert detection, threat visibility, proactive hunting, and threat response

Azure Sentinel

Azure Sentinel - Overview
Selected workspace: 'MIPDemo1-LA'

Search (Ctrl+ /) Refresh Last 24 hours

Currently there are no charges for using Azure Sentinel. On November 1, 2019, charges for Azure Sentinel will go into effect. Click to learn more about Azure Sentinel pricing.

Events 17.8M ↗ 1.4M **Alerts** 0 **Incidents** 0

INCIDENTS BY STATUS

NEW (0) IN PROGRESS (0) CLOSED (TRUE POSITIVE) (0) CLOSED (FALSE POSITIVE) (0)

Events and alerts over time

Events

Alerts

Category	Count
ALERTS	0
AZUREDIAGNO...	17.8M
PERF	12.6K
AZUREMETRICS	7.4K
OTHERS (13)	9.8K

Potential malicious events

POTENTIAL MALICIOUS EVENTS: 0

OUTBOUND: 0 ▲

INBOUND AND UNKNOWN: 0 ▼

Bing © 2019 Microsoft Corporation Terms

Recent incidents

No data was found

Data source anomalies

AzureMetrics

Usage

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Learn More >



Containers Solutions Monitoring

Azure Monitoring for Containers

Microsoft Services



Monitoring Containers in Azure

Monitoring containers can be divided in two categories:

- Application
 - Application Insights monitors the availability, performance, and usage of your web applications
- Infrastructure
 - Log Analytics Agent
 - Cluster's Dashboard
 - Azure Monitor for containers for AKS platform
 - Service Fabric Analytics



Containers Solutions Monitoring

Azure Monitoring for Azure Kubernetes Service

Microsoft Services



Kubernetes Web Dashboard

- Kubernetes includes a web dashboard that can be used for basic management operations
- View basic health status and metrics for clusters and applications, create and deploy services, and edit existing applications
- Does not allow alerting, storage of metrics or querying data

Kubernetes Web Dashboard – Dashboard Overview

Screenshot of the Kubernetes Web Dashboard showing the Overview page.

The dashboard has a top navigation bar with the Kubernetes logo, a search bar, and a "CREATE" button.

The left sidebar shows a navigation tree:

- Cluster
 - Namespaces
 - Nodes
 - Persistent Volumes
 - Roles
 - Storage Classes
- Namespace
 - default
- Overview (selected)
- Workloads
 - Cron Jobs
 - Daemon Sets
 - Deployments
 - Jobs
 - Pods
 - Replica Sets
 - Replication Controllers
 - Stateful Sets
- Discovery and Load Balancing
 - Ingresses
 - Services
- Config and Storage
 - Config Maps

The main content area displays the following sections:

Workloads

Workloads Statuses

- Deployments: 100.00%
- Pods: 100.00%
- Replica Sets: 100.00%

Deployments

Name	Labels	Pods	Age	Images
webapp2	app: webapp2	1 / 1	3 days	democcacr.azurecr.io/webapplicatio...

Pods

Name	Node	Status	Restarts	Age
webapp2-6fbc7466c4-m99hj	aks-nodepool1-36320020-vmss000001	Running	2	2 days

Replica Sets

Name	Labels	Pods	Age	Images
webapp2-6fbc7466c4	app: webapp2 pod-template-hash: 6fbc7466c4	1 / 1	3 days	democcacr.azurecr.io/webapplicatio...

Azure Monitor for Containers

- Azure Monitor for containers is designed to monitor the performance of container workloads deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS)
- Provides performance visibility by collecting container logs, memory and processor metrics from controllers, nodes and containers available in Kubernetes through the Metrics API

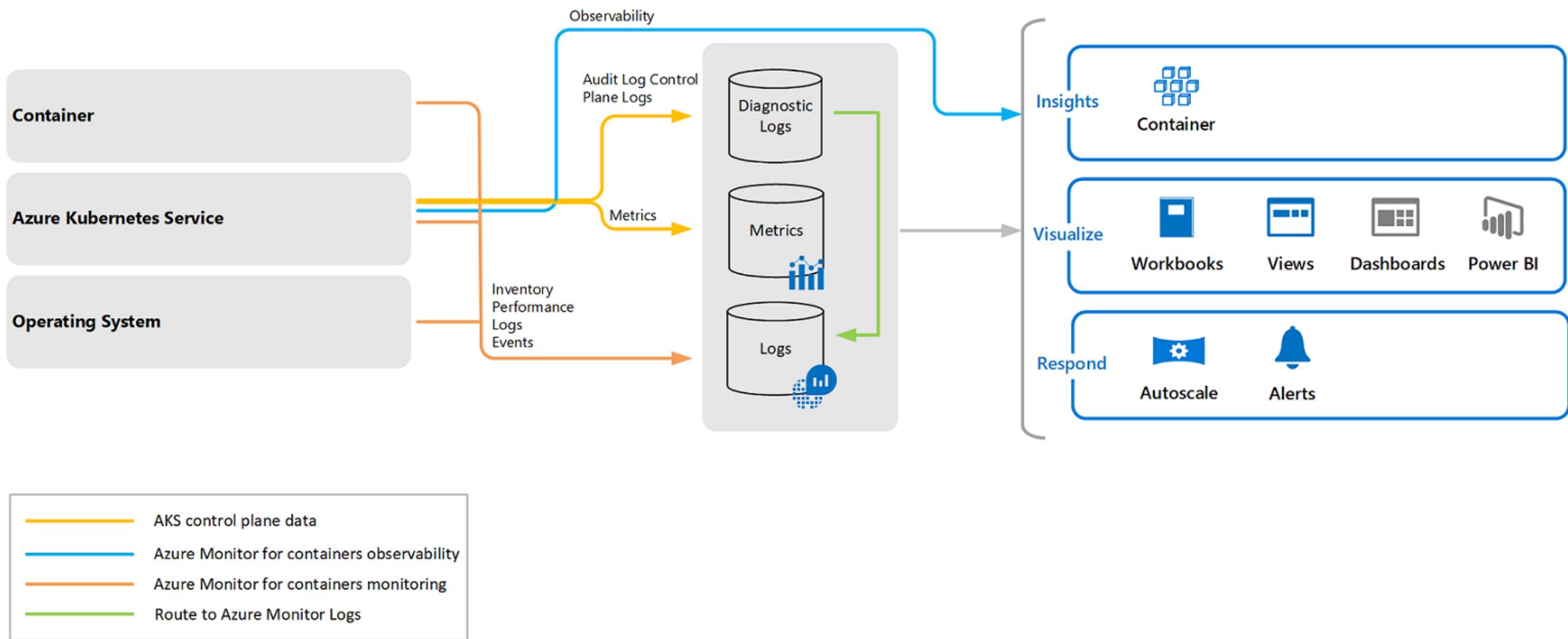
Azure Monitor for Containers

- Can be added during the creation of a cluster or to an existing cluster
- Once monitoring is enabled on Kubernetes clusters, metrics and logs are automatically collected through a containerized version of the Log Analytics agent for Linux
- Metrics are written to the metrics store and log data is written to the logs store associated with your Log Analytics workspace

Azure Monitor for Containers

- Identify AKS containers that are running on the node and their average processor and memory utilization
- Identify where the container resides in a controller or a pod
- Review the resource utilization of workloads running on the host that are unrelated to the standard processes that support the pod
- Understand the behavior of the cluster under average and heaviest loads
- Configure alerts to proactively notify you or record them, e.g. when CPU and memory utilization on nodes or containers exceed your thresholds.

Azure Monitor for Containers - Flow



Azure Monitor for Containers – Clusters Overview

 **Monitor - Containers**
Microsoft

« ⟳ Refresh ↗ Feedback

 Overview
 Activity log
 Alerts
 Metrics
 Logs
 Service Health
 Workbooks (preview)

Cluster Status Summary

1	0	0	0	1	0
Total	Critical	Warning	Unknown	Healthy	Non-monitored

Monitored clusters (1) Non-monitored clusters (0) Forums

CLUSTER NAME	CLUSTER TYPE	VERSION	STATUS	↑↓ NODES	USER PODS	SYSTEM PODS
 MIPDemoAKS	AKS	1.14.6	Healthy	2 / 2	10 / 10	12 / 12

 **Containers**
 Network

Azure Monitor for Containers – Cluster Insights

MIPDemoAKS - Insights
Kubernetes service | Directory: Microsoft

Search (Ctrl+/
Refresh | View All Clusters | Feedback | Time range = Last hour | Add Filter | View Workbooks | Forums | Learn more

Overview Activity log Access control (IAM) Tags Settings Node pools (preview) Upgrade Scale Networking Dev Spaces Deployment center (preview) Policies (preview) Properties Locks Export template Monitoring Insights Metrics (preview) Logs Support + troubleshooting New support request

Cluster Nodes Controllers Containers

Node CPU utilization %
1m granularity

Avg Min 50th 90th 95th Max

Average MIPDemoAKS **22.89 %**
Maximum MIPDemoAKS **71.27 %**

Node memory utilization %
1m granularity

Avg Min 50th 90th 95th Max

Average MIPDemoAKS **8.48 %**
Maximum MIPDemoAKS **12.86 %**

Node count
1m granularity

Total Ready Not Ready

Ready MIPDemoAKS **2**
Not Ready MIPDemoAKS **0**

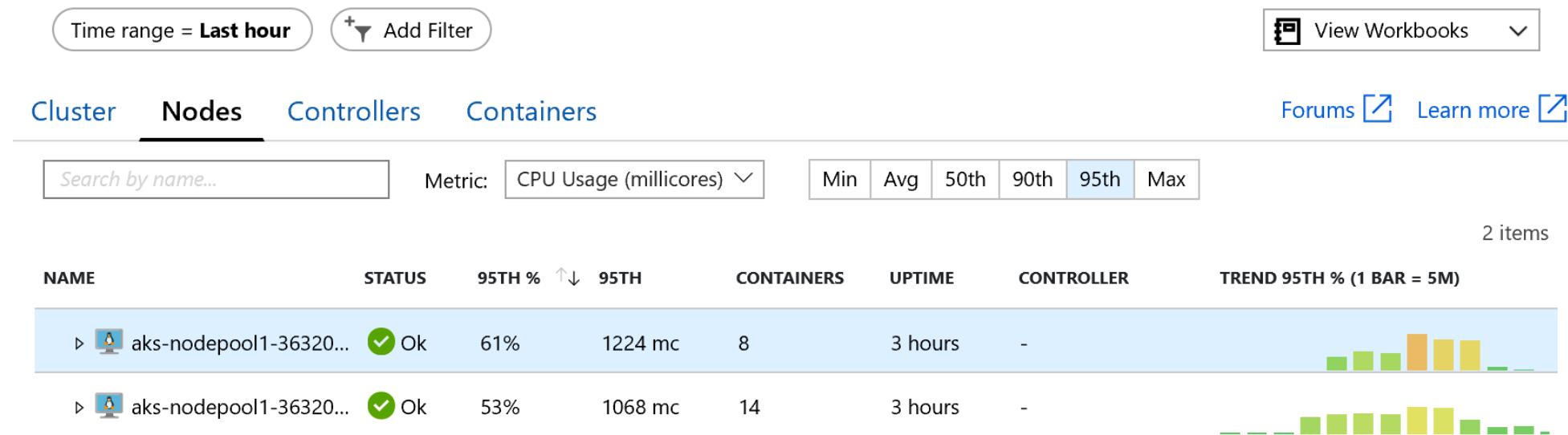
Active pod count
1m granularity

Total Pending Running Unknown Succeeded Failed

Pending MIPDemoAKS **50 m**
Running MIPDemoAKS **17.40**
Unknown MIPDemoAKS **0**
Succeeded MIPDemoAKS **0**
Failed MIPDemoAKS **0**

Azure Monitor for Containers – Nodes Insights

From the Insights blade, you can select and see directly the metrics for each of the nodes, controllers and containers.



Azure Monitor for Containers – Controllers and Containers Insights

Time range = **Last hour** [+ Add Filter](#) [View Workbooks](#)

Cluster Nodes **Controllers** Containers [Forums](#) [Learn more](#)

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

10 items

NAME	STATUS	95T...	95TH	CONTAIN...	RESTA...	UPTIME	NODE	TREND 95TH % (1 BAR = 5M)
▶ 🏛️ webapp2-6fbc7466c4 ...	10 ✓	54%	270 mc	10	0	38 mins	-	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	94%	470 mc	1	0	3 hours	aks-nodepo...	
▶ 🏛️ webapp2	✓ Ok	94%	470 mc	1	0	3 hours	aks-nodep...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	68%	341 mc	1	0	44 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	65%	325 mc	1	0	44 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	60%	299 mc	1	0	44 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	45%	223 mc	1	0	38 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	43%	215 mc	1	0	38 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	41%	207 mc	1	0	38 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	41%	207 mc	1	0	39 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	41%	206 mc	1	0	38 mins	aks-nodepo...	
▶ 🏛️ webapp2-6fbc7466...	✓ Ok	41%	206 mc	1	0	38 mins	aks-nodepo...	
▶ 🏛️ omsagent-rs-5bc7869c...	1 ✓	6%	9 mc	1	0	3 hours	-	

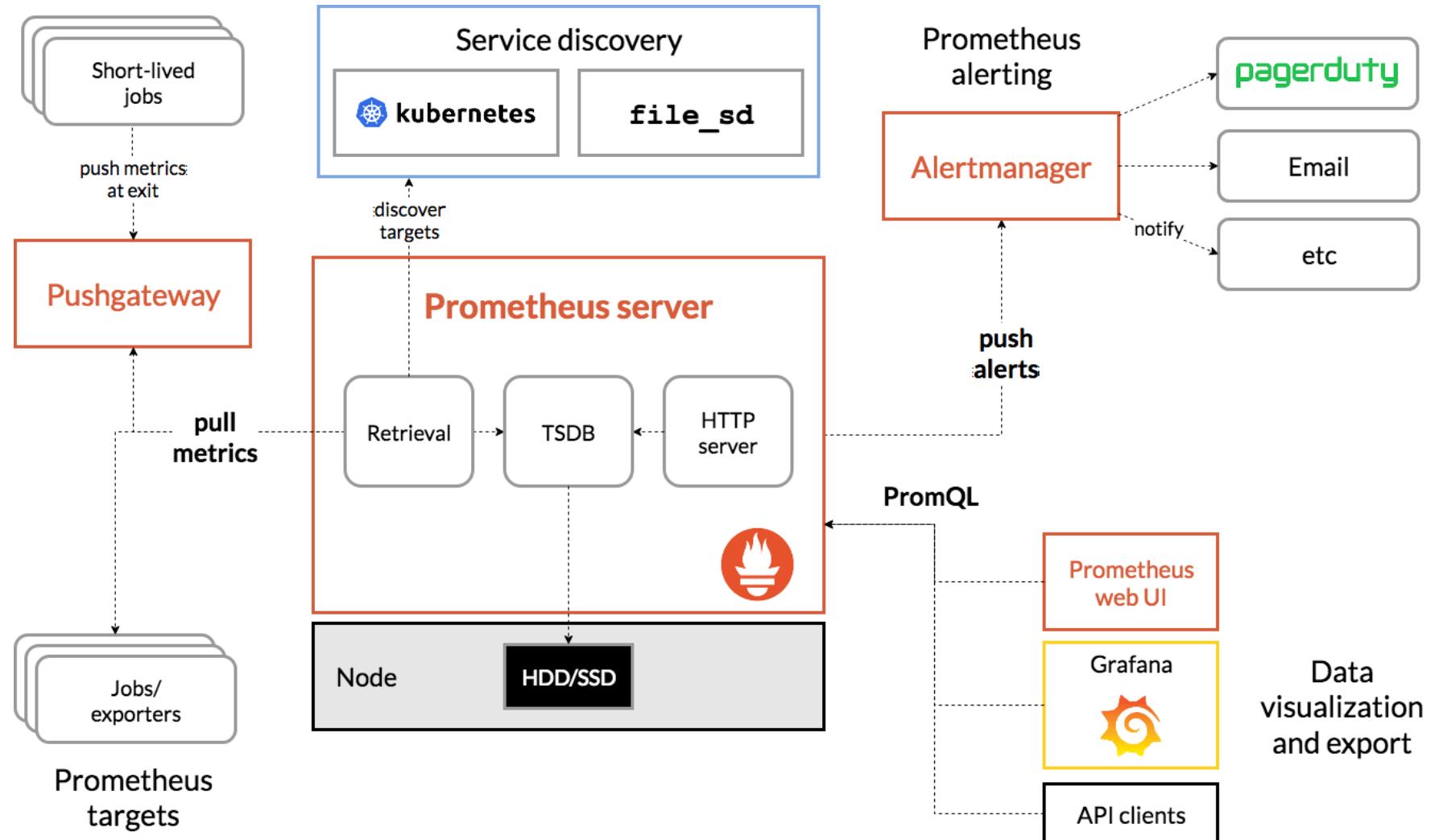
Kubernetes Master Node Logs

- Master components such as kube-apiserver and kube-controller-manager provided as a managed service
- Logs are enabled via the portal and can be sent to a Logs Analytics workspace
- Can be analyzed by a different platform by sending diagnostic logs to an Azure storage account or event hub

Prometheus & Grafana

Prometheus is a popular open source metric monitoring provides extensive metrics on Kubernetes.

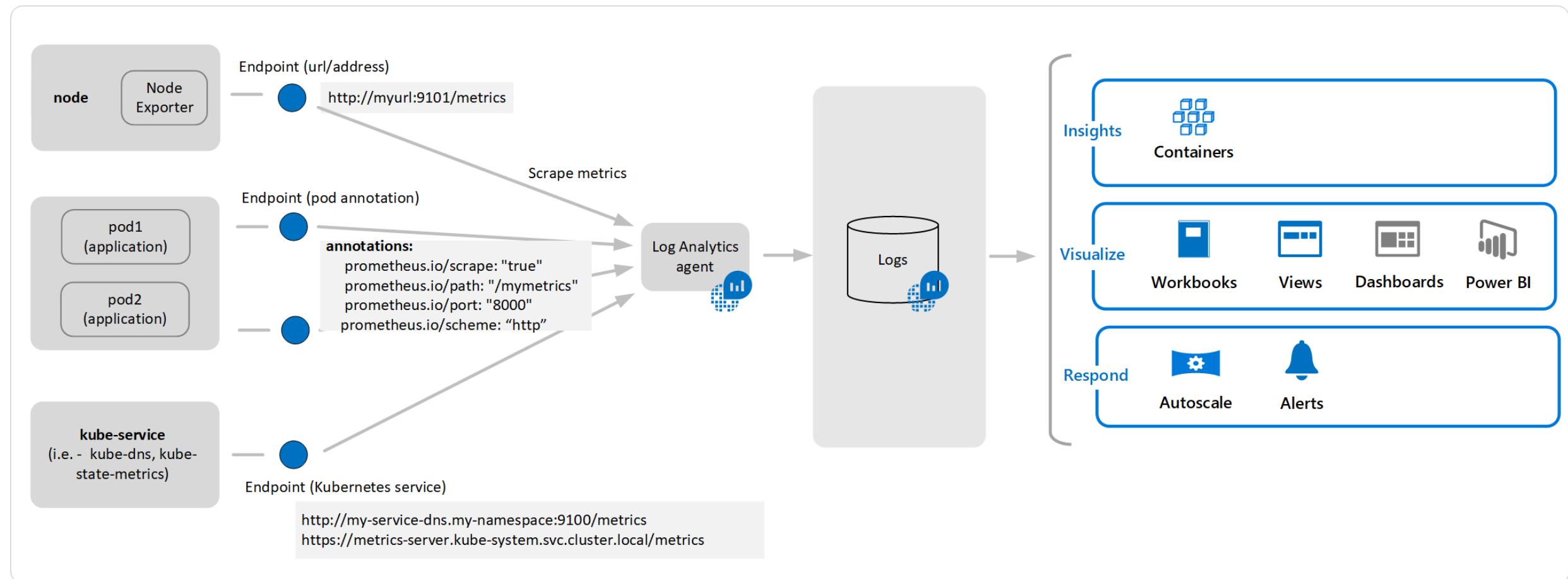
Grafana allows you to query and visualize alerts to help understand your metrics.



Azure Monitor for Containers with Prometheus

- Provides out of the box telemetry at the platform, container, orchestrator levels and to an extent the workload level
- Full stack, end to end monitoring view for Azure Kubernetes Services (AKS) in Azure Monitor for containers
- No Prometheus server is needed, just expose the Prometheus end-point through your exporters or pods (application), and the containerized agent for Azure Monitor for containers can scrape (collect) the metrics for you.

Azure Monitor for Containers with Prometheus





Containers Solutions Monitoring

*Best Practices for Customers' Security
and Management*

Microsoft Services



Security – Common Best Practices

- **Use a private registry** : A publicly available container image does not guarantee security. You should store and retrieve images from a private registry, such as Azure Container Registry or Docker Trusted Registry.
- **Monitor and scan container images** : Security monitoring and scanning solutions such as Twistlock and Aqua Security are available through the Azure Marketplace.
- **Protect credentials** : Containers can spread across several clusters and Azure regions. Make sure to secure credentials required for logins or API access, such as passwords or tokens.

Security – Common Best Practices

Image and container level security

- AAD authenticated Container registry access
- ACR image scanning and content trust for image validation

Node and cluster level security

- Automatic security patching nightly
- Nodes deployed in private virtual network subnet w/o public addresses
- Network policy to secure communication paths between namespaces (and nodes)
- Pod Security Policies
- K8s RBAC and AAD for authentication

Security – Common Best Practices

Pod level security

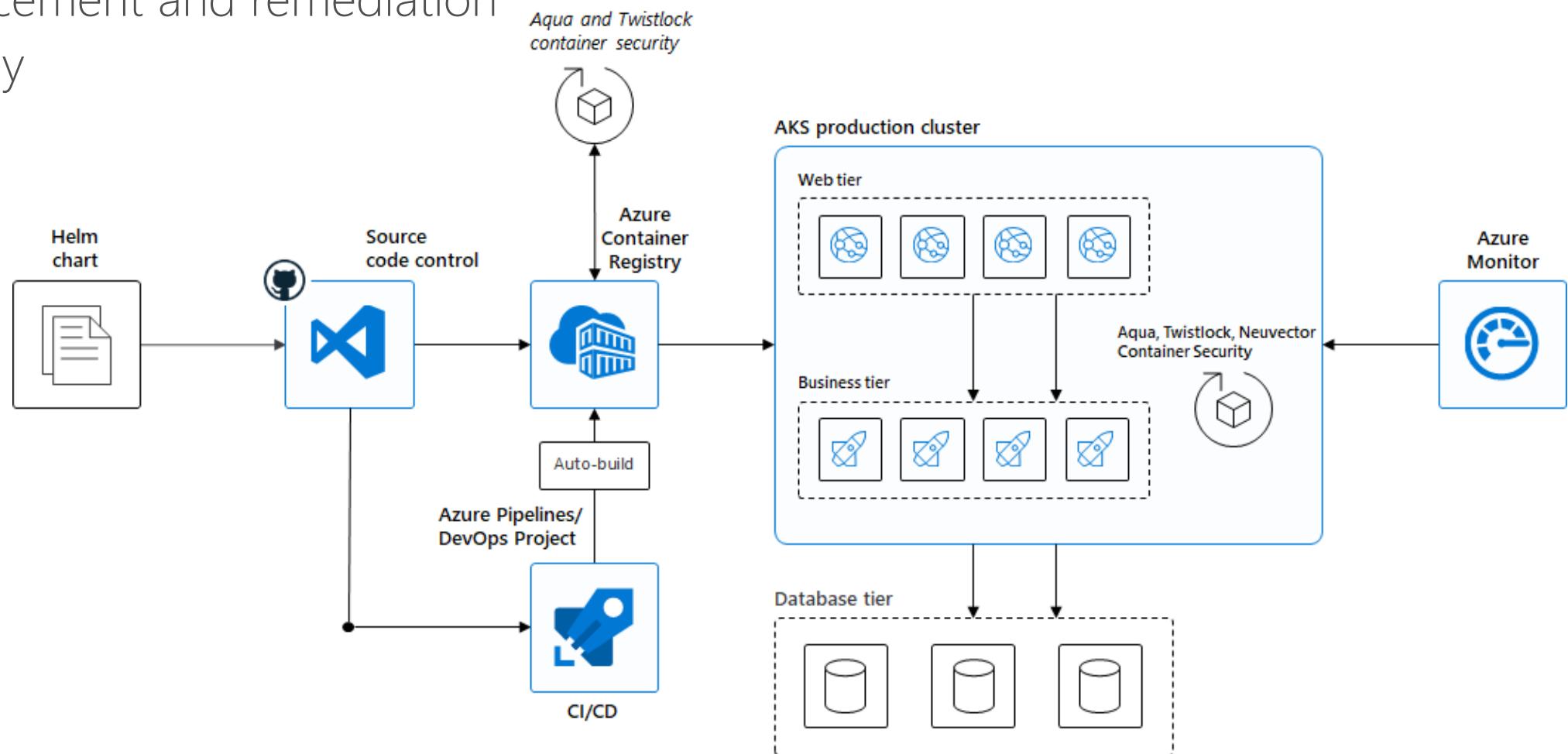
- Pod level control using AAD Pod Identity
- Pod Security Context

Workload level security

- Azure Role-based Access Control (RBAC) & security policy groups
- Secure access to resources & services
(e.g. Azure Key Vault) via Pod Identity
- Storage Encryption
- App Gateway with WAF to protect against threats and intrusions

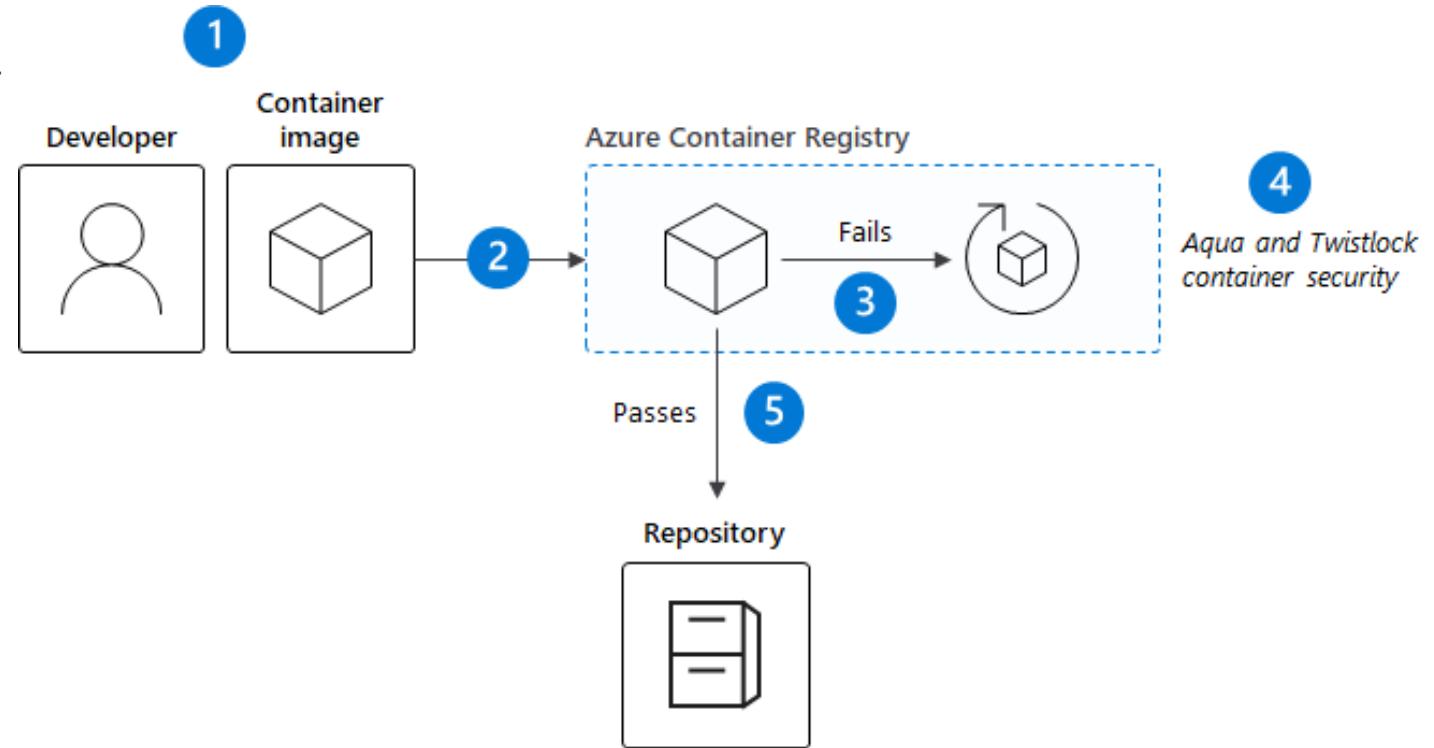
Container Level – Securing Images and Runtime

- Regularly apply security updates to the container images
- Scan your images, scan your containers
- Runtime enforcement and remediation
- Trusted Registry



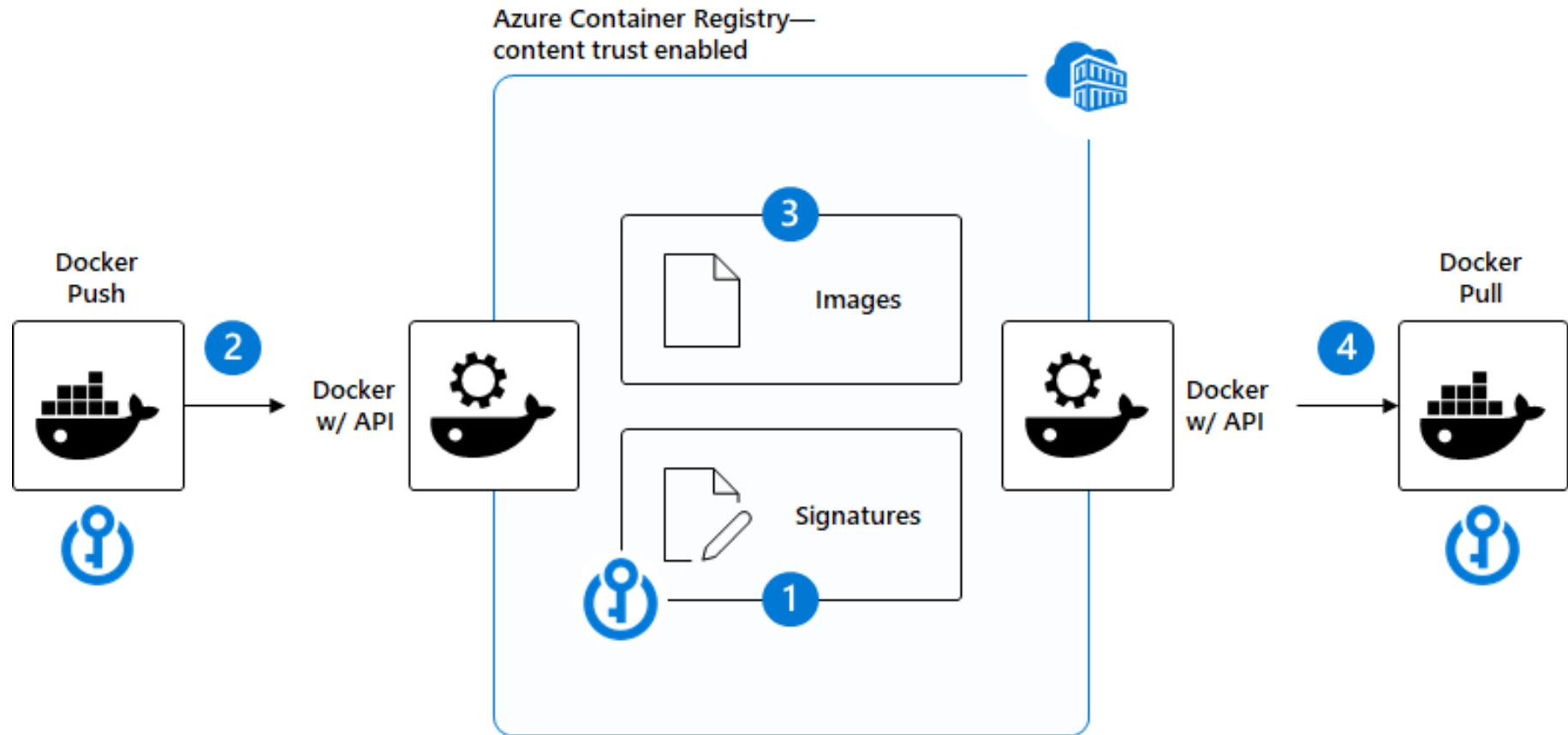
Azure Container Registry - vulnerability scanning

1. Developer/CI system builds container image
2. Image pushed to Azure Container Registry
3. Azure Container Registry quarantines image until scanning passes
4. Azure Container Registry scans content leveraging Aqua, Twistlock
5. Azure Container Registry publishes the image to the repository

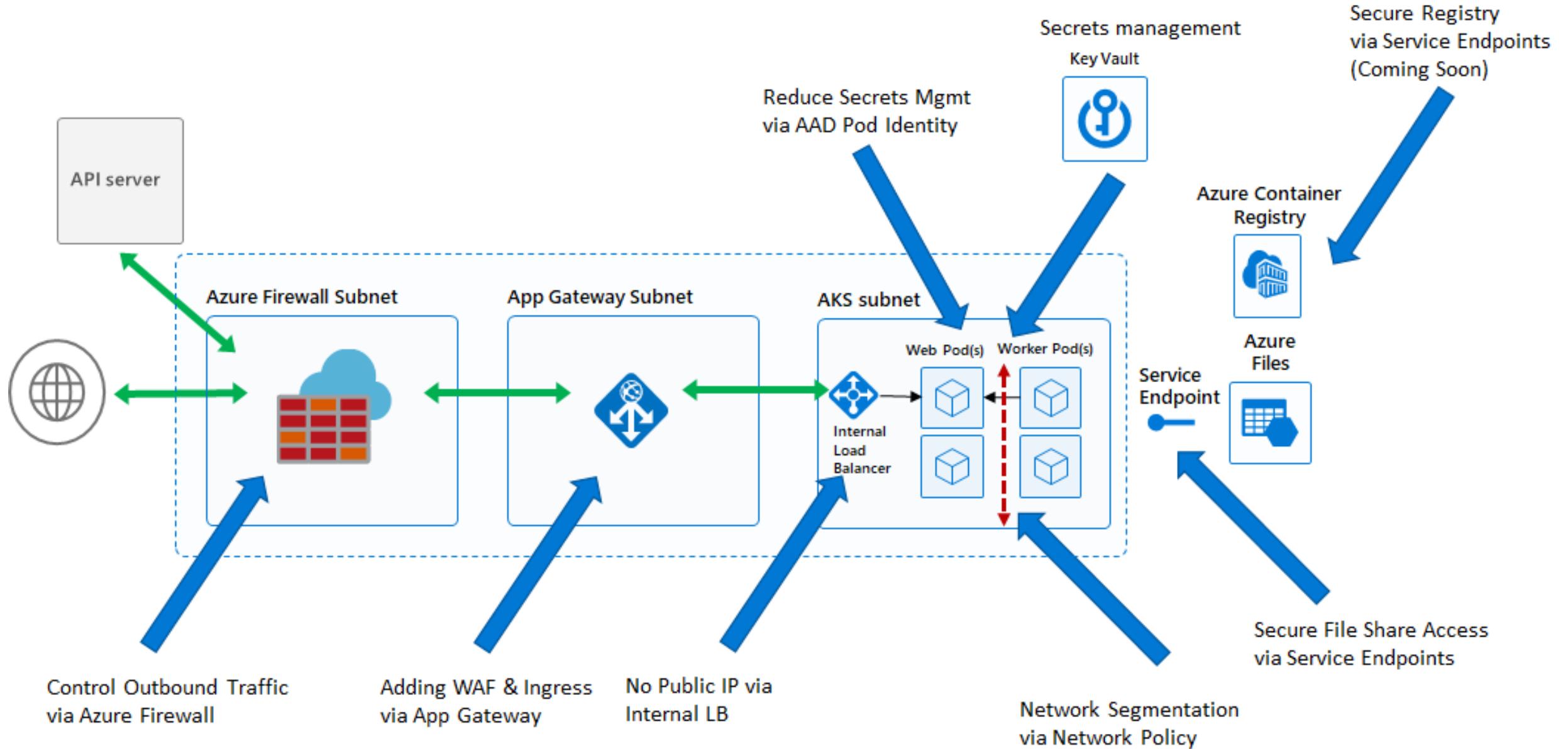


ACR - securing images from source to destination

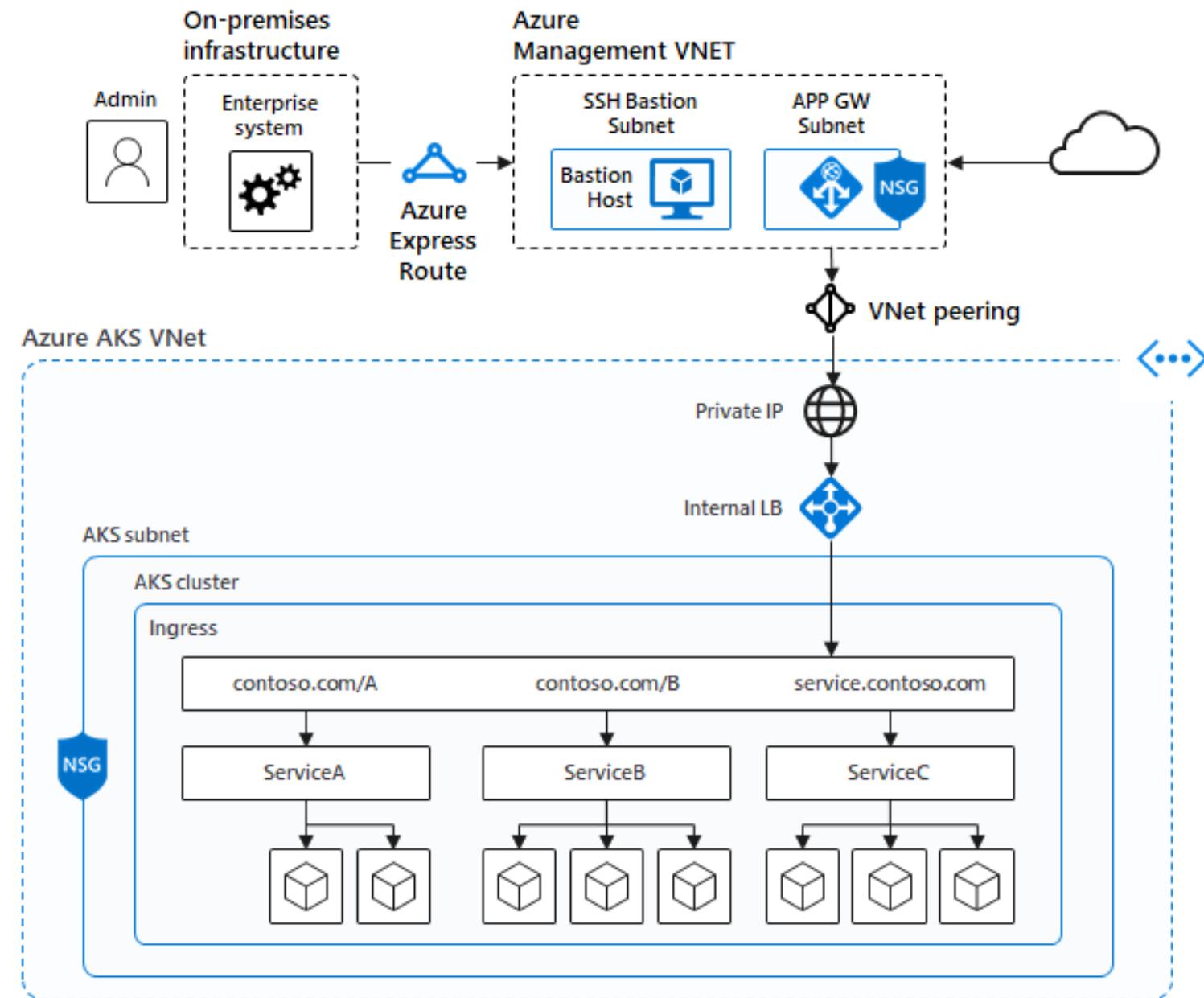
1. A set of cryptographic signing keys are associated with ACR and used for image signing
2. Image publisher signs the image and pushes to the ACR
3. Signed image is stored in Azure Container Registry
4. When an image consumer pulls a signed image, their Docker client verifies the integrity of the image



Basic example of AKS end to end security



Cluster Management Through Bastion Host





Containers Solutions Monitoring

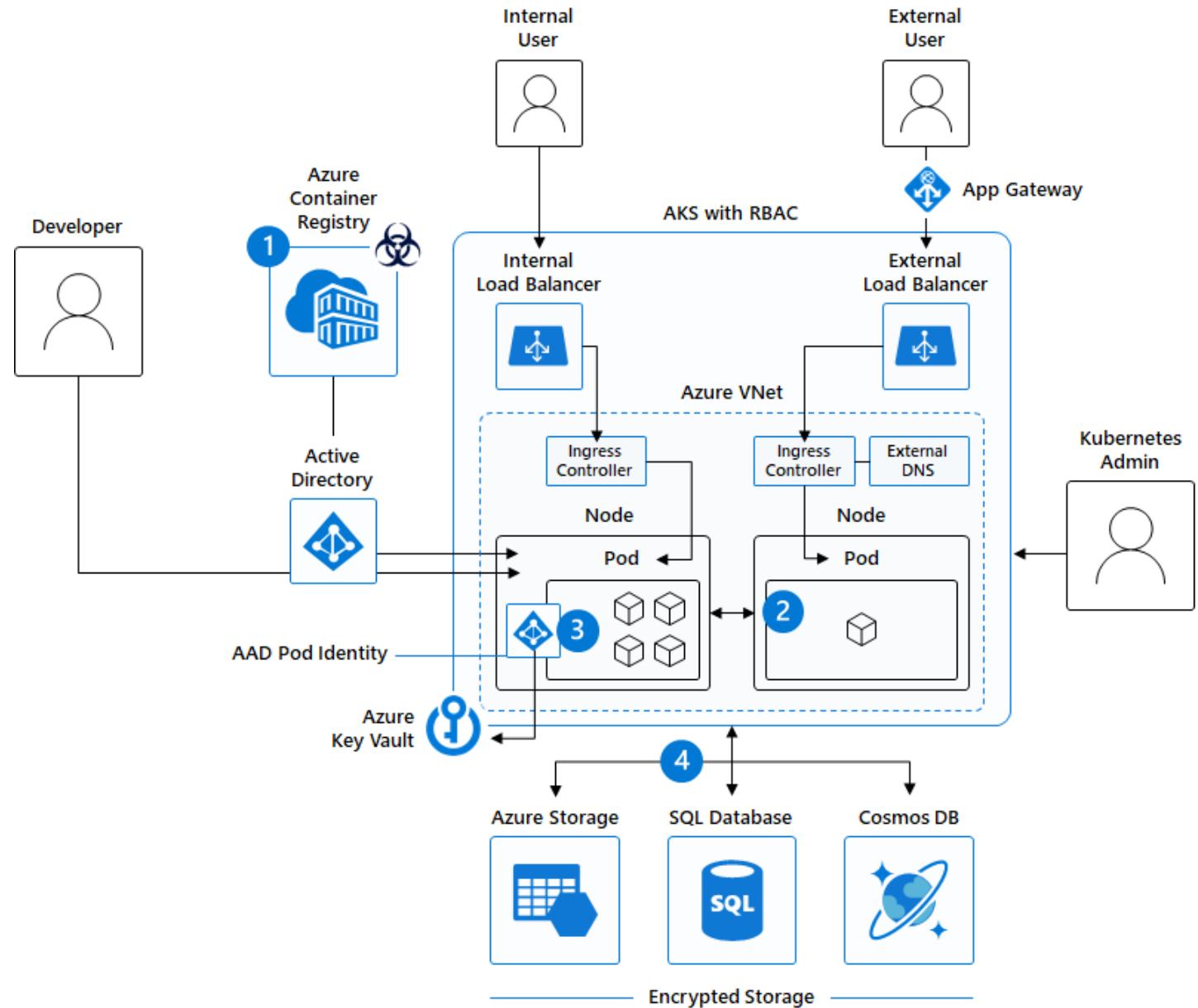
Kubernetes Security Overview

Microsoft Services



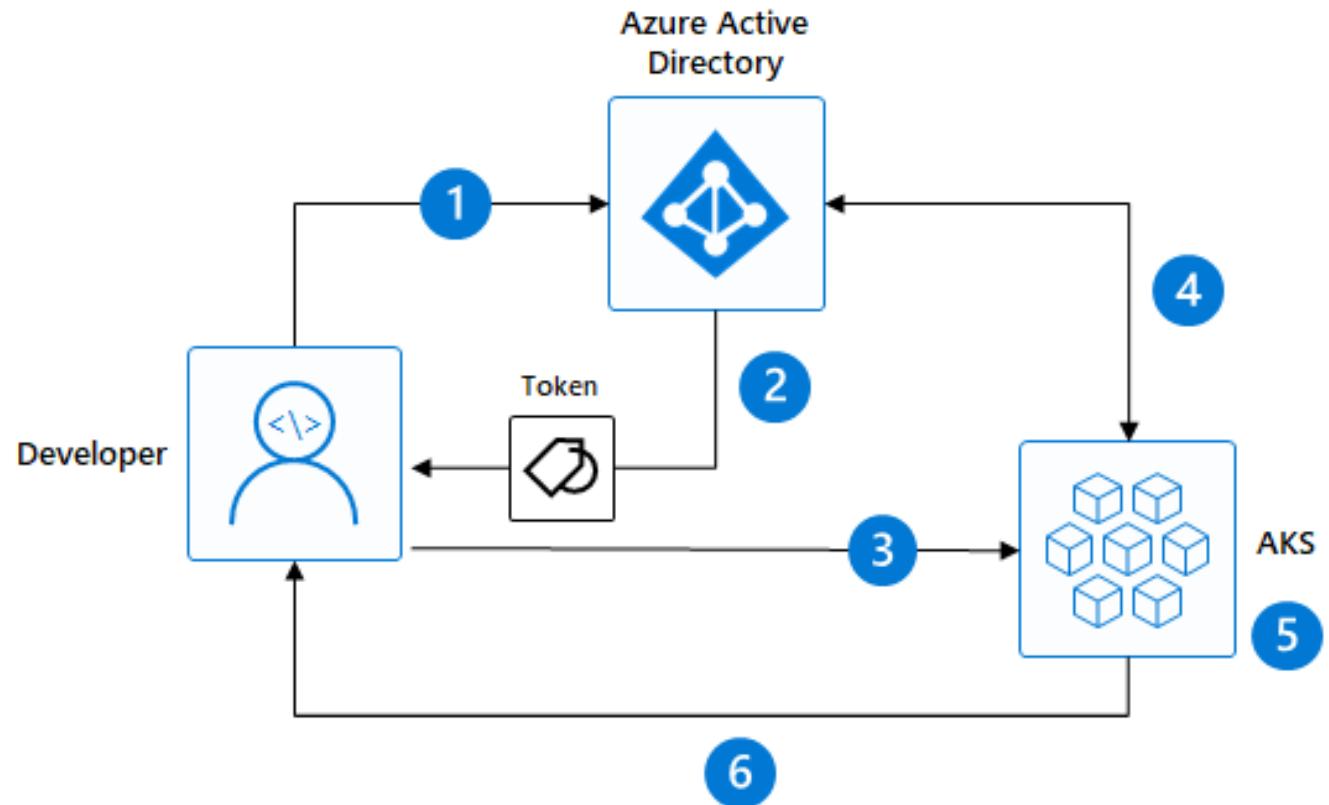
Security overview

1. Image and container level security
2. Node and cluster level security
3. Pod level security
4. Workload level security



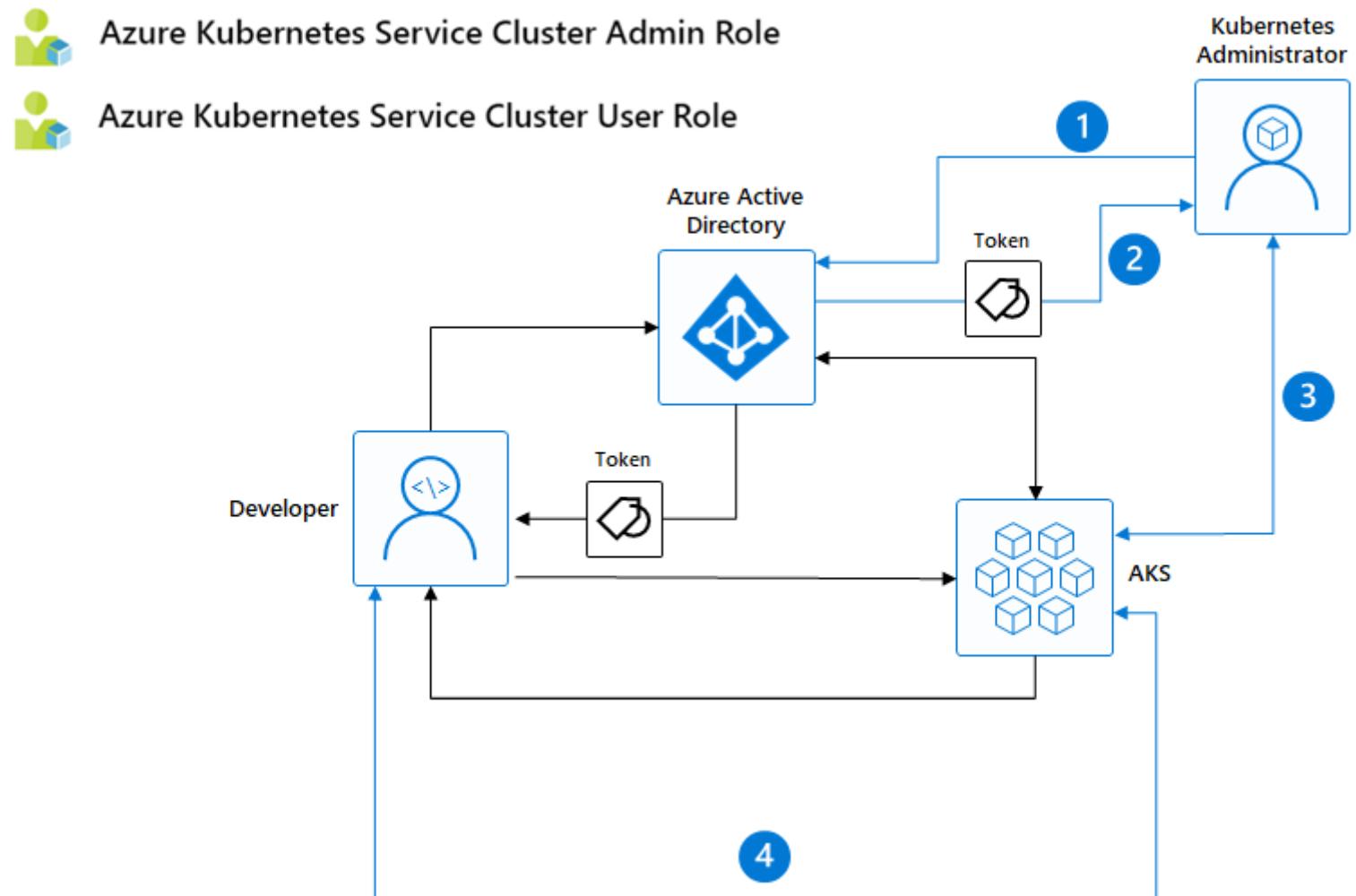
Cluster Level – RBAC and Azure AD integration

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



Azure Level - Kubernetes RBAC and Azure RBAC Roles

1. Kubernetes Administrator authenticates with AAD
2. The AAD token issuance endpoint issues the access token
3. Administrator fetches the admin kubeconfig and configures RBAC roles and bindings
4. Kubernetes Developer fetches the user kubeconfig



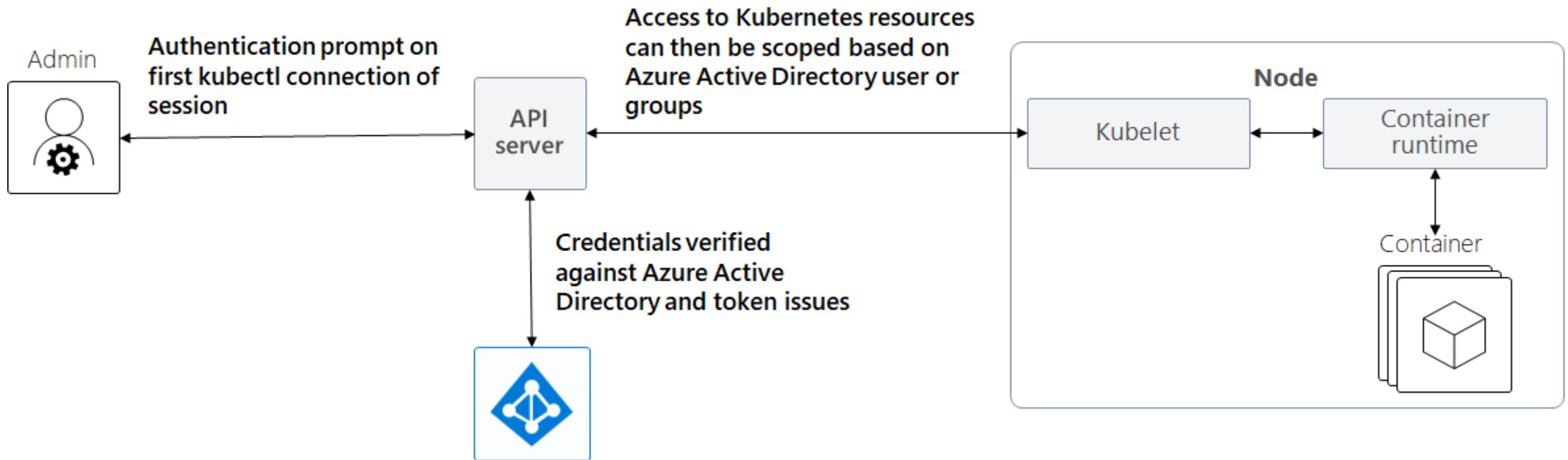
Service Principals

- Cluster Service Principal
 - To allow an AKS cluster to interact with other Azure resources, an Azure Active Directory service principal is used.
- AD Integration Objects
 - When configuring Azure AD for AKS authentication, 2 Azure AD application are configured.
 - Server Application - used to get a user's Azure AD group membership
 - Client Application - used when logging in with the Kubernetes CLI (kubectl)
- You can Rotate/Update their credentials with:

```
az aks update-credentials  
--resource-group myResourceGroup  
--name myAKScluster --reset-service-principal  
--service-principal $SP_ID --client-secret $SP_SECRET
```

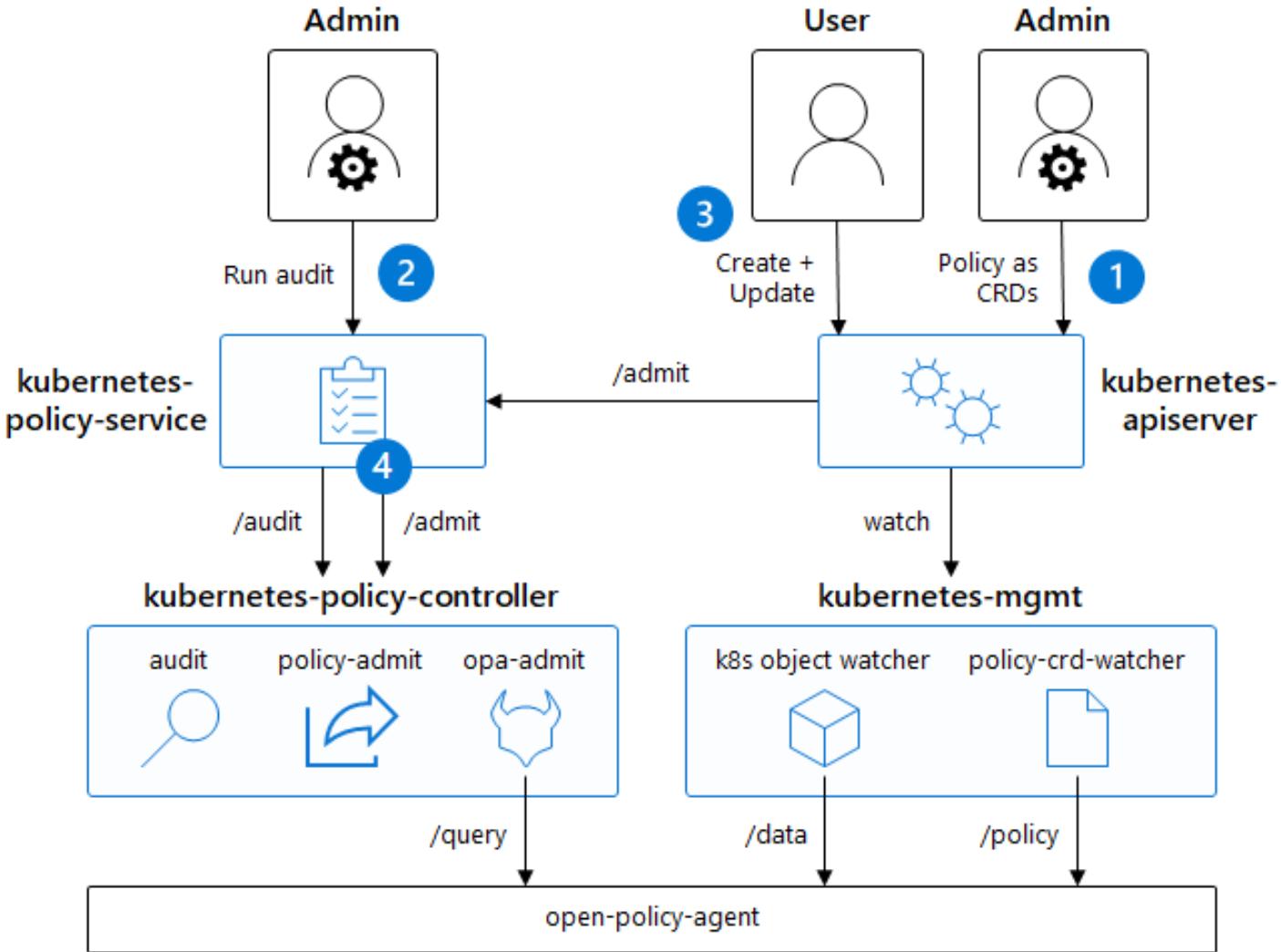
Cluster Level Security

- Securing endpoints for API server and cluster nodes
 - Integrate Kubernetes role-based access control (RBAC) with Azure Active Directory to control access to the API server. These controls let you secure AKS the same way that you secure access to your Azure subscriptions.



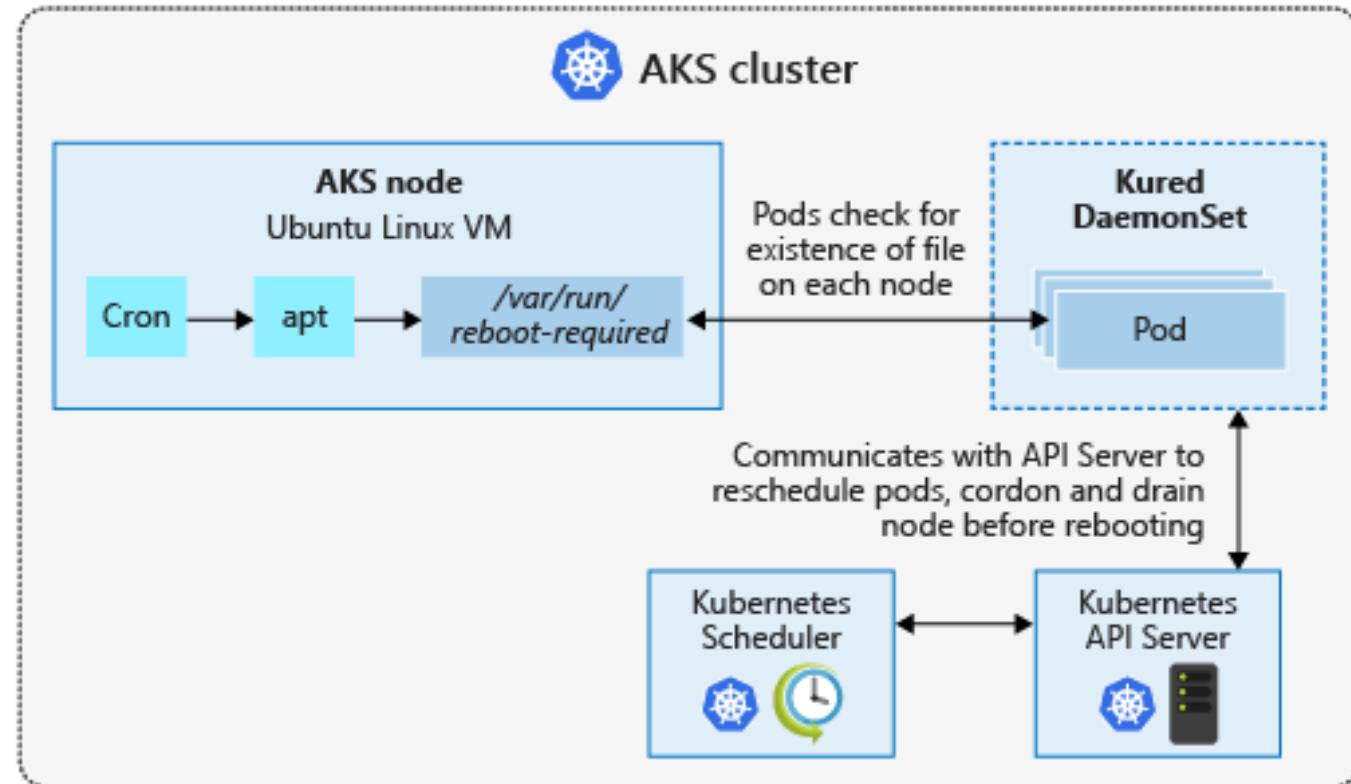
Policy controller

1. Admin adds policy for the cluster
2. Admin audits compliance of the cluster using /audit endpoint
3. User uses standard Kubernetes API to operate the cluster and the create actions are guarded by policy
4. Kubernetes-policy-controller provides an admission controller webhook that performs evaluations by calling open-policy-agent (OPA) service



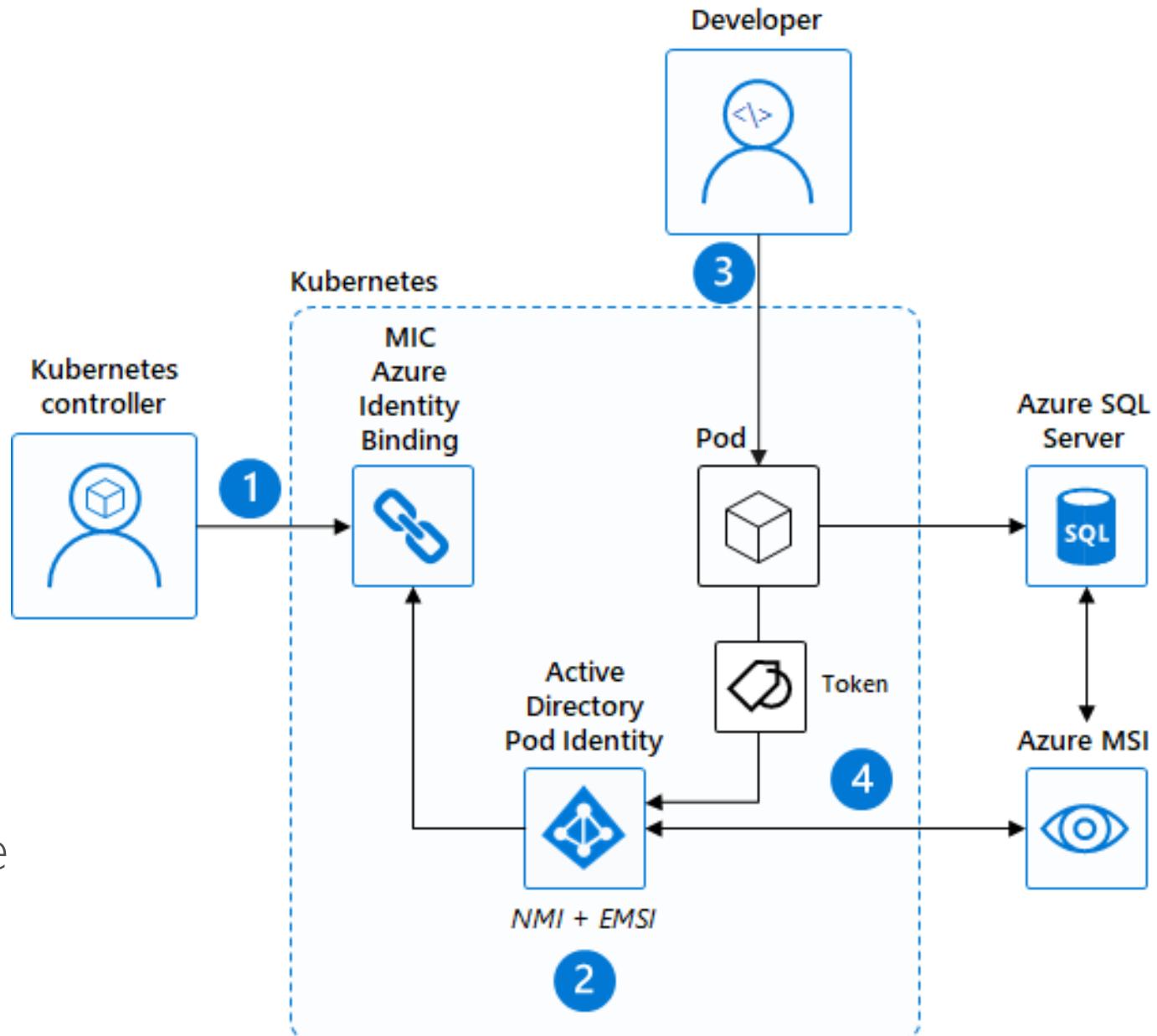
Process Node OS update

- AKS automatically applies security patches to the nodes on a nightly schedule
- You're responsible to reboot as required
- Regular maintenance recommended
 - Monthly ideal, 3 months minimum
- Use Kured DaemonSet to watch for nodes requiring a reboot and handle the reschedule of the pods and reboot of the nodes.



Securing Workloads - 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 Identity (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



Pod Security Policies

- Pod Security Policies (or PSPs) are objects that control security-sensitive aspects of pod specification (like root privileges)
- If a pod does not meet the conditions specified in the PSP, Kubernetes will not allow it to start
- You can assign PSPs at the cluster or project level
- PSPs work through inheritance
- Workloads that are already running in a cluster or project before a PSP is assigned will not be checked

