Microsoft

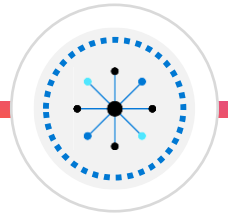
Microsoft Azure Arc In A Day

Microsoft Azure Arc in a Day

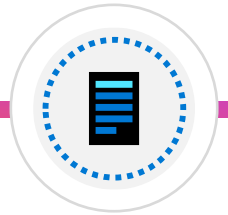
- Introduction
- What is Microsoft Azure Arc
- Installation & Configuration – The Basics
- Microsoft Azure Arc Services
- Demo Time: Your First Use Case [aka IT Pro]
- Advanced Configuration & Management
- Cost Management
- Security Considerations
- Advanced Azure Arc Features [aka DevOps]
- Infrastructure as a Code with Azure Arc
- Monitoring and Analytics
- Disaster Recovery & High Availability
- Future Roadmap and Upcoming Features
- Q&A Time

What is Microsoft Azure Arc?

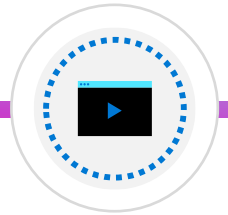
An overview of Azure Arc and its core concepts



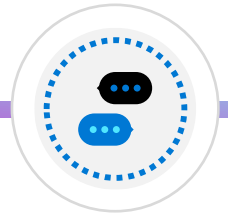
Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.



Develop cloud-native applications with a consistent development, operations, and security model.



Azure Arc runs on both new and existing hardware, virtualization and Kubernetes platforms, IoT devices, and integrated systems.



Do more with less by leveraging your existing investments to modernize with cloud-native solutions.

An overview of Azure Arc and its core concepts

- Consistent development and operation experience to run cloud-native apps anywhere and on any Kubernetes platform.
- Deployment of data services like SQL and PostgreSQL as cloud-native services in your preferred environment for data insights.
- Azure security and governance for applications, data, and infrastructure across diverse environments.
- Flexible infrastructure and connectivity options to meet your regulatory and latency requirements.

Develop cloud-native apps and operate them anywhere

- Build and modernize cloud-native apps on any Kubernetes.
- Integrate Azure monitoring, security, and compliance into your DevOps toolkit.
- Reduce errors and accelerate innovation with GitOps and policy-driven deployment and configuration across environments.
- Get up and running immediately with your existing tools and practices including GitHub, Terraform, and Visual Studio.
- Write to the same application service APIs that can run consistently on premises, across multiple clouds, and in edge environments using any Kubernetes.
- Optimize costs with Azure Hybrid Benefit to run Azure Kubernetes Service on Windows Server and Azure Stack HCI at no additional cost for Windows Server Software Assurance or CSP subscription customers.

Harness data insights from the cloud to the edge

- Create applications faster with an end-to-end solution from local data collection, storage, and real-time analysis.
- Reduce management overhead and risk exposure through integrated security and governance tools for data.
- Improve operational efficiency through consistent data and AI tools, services, and automations.
- Deploy Azure Arc-enabled SQL Managed Instance or PostgreSQL (in preview) on any Kubernetes distribution and on any cloud.
- Get started in minutes with one-click deployment of the managed machine learning add-on, and train models on any Kubernetes cluster with Azure Machine Learning.

Secure and govern applications, data, and infrastructure across diverse environments

- Get Extended Security Updates enabled by Azure Arc to secure and patch your Windows Server 2012/R2 and SQL Server 2012 resources.
- Govern your disparate environments through the Azure portal to simplify multicloud management and drive operational efficiencies.
- Use cloud-based threat detection, response, and analytics with Microsoft Defender for Cloud.
- Centrally manage a wide range of resources including Windows Server on Azure, Linux on Azure, SQL server, Azure Kubernetes Service, and Azure Arc-enabled data services.
- Perform virtual machine (VM) lifecycle management for your Azure Stack HCI and VMware environments from a centralized location.
- Delegate access and manage security policies for resources using role-based access control (RBAC) and Azure Lighthouse.

Meet regulatory and connectivity needs with flexibility

- Meet residency and sovereignty needs with a variety of infrastructure options including Azure Stack HCI.
- Meet governance and compliance standards for apps, infrastructure, and data with Azure Policy.
- Get simplified edge computing infrastructure for low-latency applications.
- Operate with full, intermittent, or no internet connection.

Importance in hybrid cloud environments

- **Best of Both Worlds:** A hybrid cloud refers to a storage and computing infrastructure composed of a mixture of private cloud services, a public cloud, and/or on-premises infrastructure. This setup allows an organization to leverage the advantages of both private and public clouds.
- **Flexibility and Control:** A hybrid cloud platform provides greater flexibility, control, and scalability. It offers more deployment options and global scale.
- **Security and Compliance:** It ensures integrated cross-platform security and unified compliance. It's important to ensure the security of your hybrid cloud environment.
- **Efficiency:** Hybrid clouds improve workload, operational, and cost efficiencies across the enterprise, consistently achieving more value from existing infrastructure.
- **Workload Mobility:** A hybrid cloud environment aids in workload mobility, integration, and management across multiple computing environments.

Importance of multi cloud environment

- **Flexibility and Agility:** Multi-cloud environments allow businesses to choose the best cloud services for their specific needs, not being tied down to the offerings of a single provider.
- **Risk Mitigation:** By distributing operations across multiple cloud platforms, businesses can ensure uninterrupted services, mitigating the risk of downtimes.
- **Cost Efficiency:** Different cloud providers have different pricing models. By strategically distributing workloads across various providers, businesses can optimize costs.
- **Innovation and Speed:** Multi-cloud environments allow businesses to leverage the best features from each cloud provider, leading to faster deployment of services and an overall boost in operational efficiency.
- **Regulatory Compliance:** Multi-cloud strategies allow businesses operating in multiple regions to store data in specific regions to comply with local data protection regulations.

Installation & Configuration Basics

Licensing Requirements

- **Prerequisites:** You need to install the Connected Machine agent to onboard a physical server or virtual machine to Azure Arc-enabled servers. Azure Arc supports various Windows and Linux operating systems.

- **Licensing:** Azure Arc offers its core control plane at no cost to customers, while preserving consistent pricing on all management and services originated from Azure.

However, specific Azure Arc-enabled services like Azure Arc-enabled SQL Server, Azure Arc-enabled SQL Managed Instance, and Azure Arc-enabled PostgreSQL will be charged consistently as in the original Azure services.

Licensing Requirements

- **Extended Security Updates:** Microsoft provides Extended Security Updates enabled by Azure Arc for Windows Server 2012/R2 and SQL Server 2012/R2.

With Azure Arc, organizations can purchase and seamlessly deploy Extended Security Updates in on-premises or multicloud environments, right from the Azure portal.

- **Azure Hybrid Benefit:** If you have Windows Server or SQL Server core licenses with Software Assurance or a subscription to these products, you can use the Azure Hybrid Benefit.

Step-by-step guide to installing Azure Arc | Prerequisites

Step 1 – create Azure Account with an active subscription

Step 2 – prepare accounts with permission of desired machine (root for Linux, local admin for Windows)

Step 3 – register resource providers on your subscription:

- *Microsoft.HybridCompute*
- *Microsoft.GuestConfiguration*
- *Microsoft.HybridConnectivity*
- *Microsoft.AzureArcData*

Step-by-step guide to installing Azure Arc | Prerequisites

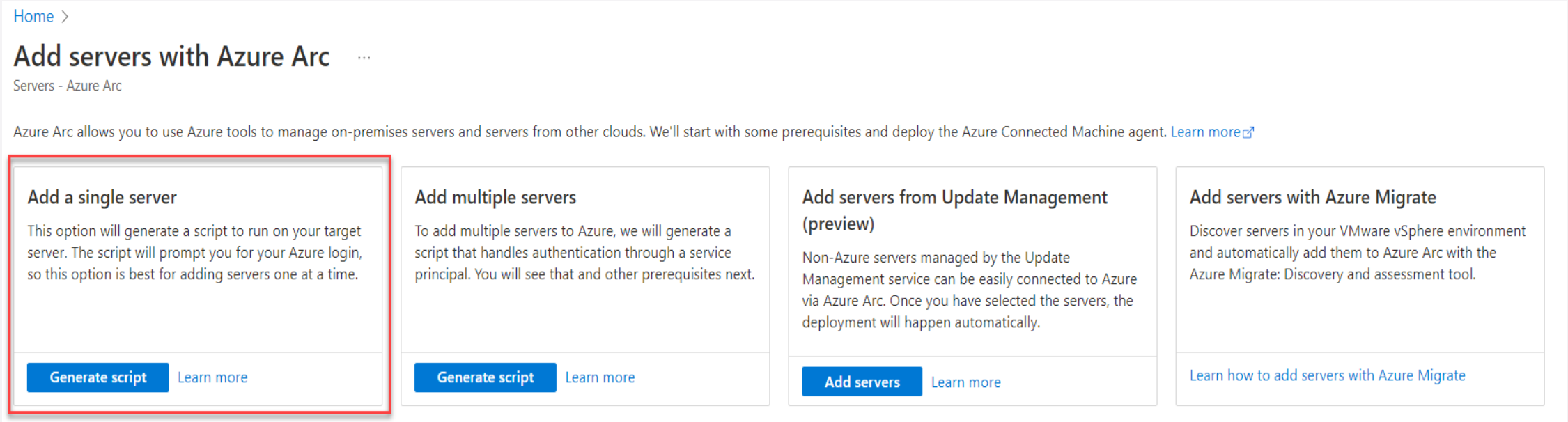
Step 4 – review agent prerequisites:
- supported operating system
- assigned RBAC roles
- location of machine in supported region
- check if hostname (linux) and computer name (windows) do not contain reserved words
- check firewall trafic to appropriate url’s

Step-by-step guide to installing Azure Arc | Installing Agents

From Azure Portal > type Azure Arc (or Arc) > choose single server

--

In later steps you fill data from prerequsites part



Step-by-step guide to installing Azure Arc | Installing Agents (1) | Windows

```
try {
    $env:SUBSCRIPTION_ID = "85528a56-3137-423d-aa23-           ";
    $env:RESOURCE_GROUP = "SHAc-TheArk";
    $env:TENANT_ID = "1a7315f1-279a-447f-a639-           ";
    $env:LOCATION = "canadacentral";
    $env:AUTH_TYPE = "token";
    $env:CORRELATION_ID = "95ab8b6e-2acc-4578-b39f-           ";
    $env:CLOUD = "AzureCloud";


    [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;

    # Download the installation package
    Invoke-WebRequest -UseBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile
"$env:TEMP\install_windows_azcmagent.ps1";
```

Step-by-step guide to installing Azure Arc | Installing Agents (2) | Windows

```
    # Install the hybrid agent
    & "$env:TEMP\install_windows_azcmagent.ps1";
    if ($LASTEXITCODE -ne 0) { exit 1; }

    # Run connect command
    & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group
"$env:RESOURCE_GROUP" --tenant-id "$env:TENANT_ID" --location "$env:LOCATION" --subscription-id
"$env:SUBSCRIPTION_ID" --cloud "$env:CLOUD" --tags
"Datacenter=SHACHQ,City=HUCKNALL,StateOrDistrict=NOTTS,CountryOrRegion=ENGLAND,Location=Brexitland,Project=Azur
eArc" --correlation-id "$env:CORRELATION_ID";
}
catch {
    $logBody =
@{subscriptionId="$env:SUBSCRIPTION_ID";resourceGroup="$env:RESOURCE_GROUP";tenantId="$env:TENANT_ID";location=
"$env:LOCATION";correlationId="$env:CORRELATION_ID";authType="$env:AUTH_TYPE";operation="onboarding";messageTyp
e=$_.FullyQualifiedErrorId;message="$_";};
    Invoke-WebRequest -UseBasicParsing -Uri "https://gbl.his.arc.azure.com/log" -Method "PUT" -Body ($logBody |
ConvertTo-Json) | out-null;
    Write-Host  -ForegroundColor red $_.Exception;
}
```

Step-by-step guide to installing Azure Arc | Installing Agents (2) | Linux

```
export subscriptionId="85528a56-3137-423d-                ";
export resourceGroup="SHAc-TheArk";
export tenantId="1a7315f1-279a-447f-a639-             ";
export location="canadacentral";
export authType="token";
export correlationId="95ab8b6e-2acc-4578-b39f-             ";
export cloud="AzureCloud";
```

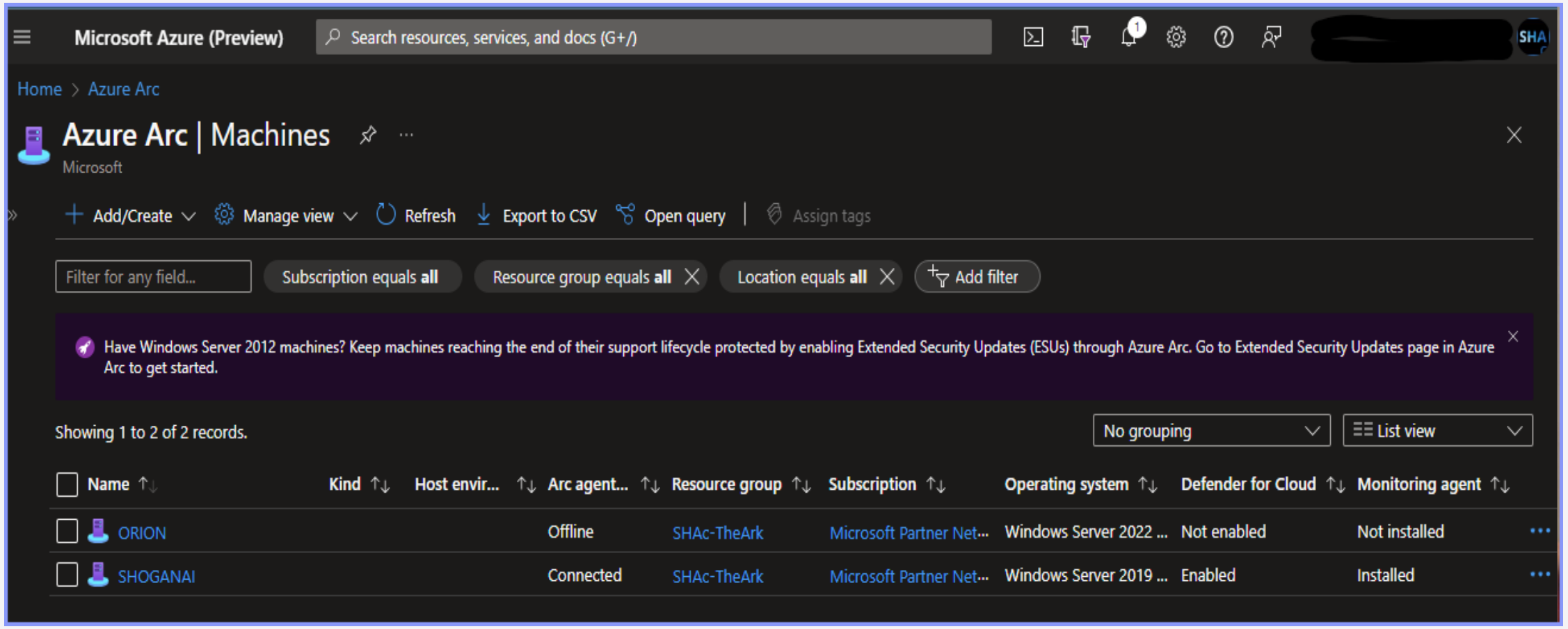
Step-by-step guide to installing Azure Arc | Installing Agents (2) | Linux

```
# Download the installation package
output=$(wget https://aka.ms/azcmagent -O ~/install_linux_azcmagent.sh 2>&1);
if [ $? != 0 ]; then wget -qO- --method=PUT --body-
data="{\"subscriptionId\":\"$subscriptionId\",\"resourceGroup\":\"$resourceGroup\",\"tenantId\":\"$tenantId\",\
"location\":\"$location\",\"correlationId\":\"$correlationId\",\"authType\":\"$authType\",\"operation\":\"onboa
rding\",\"messageType\":\"DownloadScriptFailed\",\"message\":\"$output\"}" "https://gbl.his.arc.azure.com/log"
&> /dev/null || true; fi;
echo "$output";

# Install the hybrid agent
bash ~/install_linux_azcmagent.sh;

# Run connect command
sudo azcmagent connect --resource-group "$resourceGroup" --tenant-id "$tenantId" --location "$location" --
subscription-id "$subscriptionId" --cloud "$cloud" --tags
"Datacenter=SHACHQ,City=HUCKNALL,StateOrDistrict=NOTTS,CountryOrRegion=ENGLAND,Location=Brexitland,Project=Azur
eArc" --correlation-id "$correlationId";
```

Step-by-step guide to installing Azure Arc | Verify Connection



Azure Arc Services

Overview of services that can be managed

Azure Arc-Enables Services

Azure Kubernetes Services

Run AKS on supported customer-managed infrastructures and deploy containerized Windows and Linux applications in datacenters and at the edge.

Create GitOps configurations to keep Kubernetes clusters in sync and automate updates for new and existing deployments. With service mesh, provide capabilities like traffic management, resiliency, policy, security, strong identity, and observability to your workloads.

LINK
https://bit.ly/3tQvS1z

Overview of services that can be managed

Azure Arc-Enables Services

Azure Application Services

Choose from multiple application services including
Azure App Service,
Azure Functions,
Azure Logic Apps,
Azure API Management,
Azure Event Grid,
Azure Container Apps.

LINK
https://bit.ly/3Skz3sy

Overview of services that can be managed

Azure Arc-Enables Services

Azure Data Services

Deploy critical Arc-enabled data services like
Azure SQL Managed Instance and
PostgreSQL (in preview)

on premises, in the multicloud environments, or on any Kubernetes distribution.

LINK
https://bit.ly/3SgL5mU

Overview of services that can be managed

Azure Arc-Enables Services

Azure Machine Learning

With Azure Machine Learning—training (in preview), train machine learning models and get reliability with service-level objectives.

With Azure Machine Learning—inferencing (in preview), deploy trained models using Azure Arc–enabled machine learning.

LINK
https://bit.ly/3FGRFLO

Overview of services that can be managed

Azure Arc-Enables Infrastructure

Servers

Use Linux and Windows virtual machines (VMs), bare-metal servers, and other clouds with the same server management experience across environments.

With built-in Azure policies for servers, you're able to view and search for noncompliant servers.

LINK
https://bit.ly/45ZE64W

Overview of services that can be managed

Azure Arc-Enables Infrastructure

Kubernetes

Use the container platform of your choice to add built-in Kubernetes Gatekeeper policies and inventory, organize, and tag Kubernetes clusters.

Deploy apps and configuration as code using GitOps with out-of-the-box support for most CNCF (Cloud Native Computing Foundation)–certified Kubernetes.

LINK
https://bit.ly/3Mrr6OB

Overview of services that can be managed

Azure Arc-Enables Infrastructure

Azure Stack HCI (Hyper-Converged Infrastructure)

Extend your datacenter to the cloud and deploy compute resources as well as cloud-native apps at your remote locations and manage them in the Azure portal.

Choose from more than 25 hardware-validated partners, or re-use hardware that meets validation requirements.

LINK
https://bit.ly/3Qkpnf5

Overview of services that can be managed

Azure Arc-Enables Infrastructure

VMware (Public Preview)

Perform full lifecycle management on VMware VMs and use Azure RBAC to provision and manage VMs on demand in the Azure portal.

Access governance, monitoring, update management, and security at scale for VMware VMs from your datacenters or using Azure VMware Solution, Kubernetes clusters, and VMware Tanzu Application Service.

LINK
https://bit.ly/3sc6cw7

Overview of services that can be managed

Azure Arc-Enables Infrastructure

System Center Virtual Machine Manager

Configure and manage your datacenter components as a single fabric in Virtual Machine Manager (VMM). Add, provision, and manage Hyper-V and VMware virtualization hosts and clusters.

Discover, classify, provision, allocate, and assign local and remote storage. Use VMM fabric to create and deploy VMs and services on virtualization hosts.

LINK
https://bit.ly/3Snuez0

Azure Arc Jumpstart

Introduction for Azure Arc Jump Start

The Azure Arc Jumpstart is designed to provide a “zero to hero” experience so you can start working with Azure Arc right away!

The Jumpstart provides step-by-step guides for independent Azure Arc scenarios that incorporate as much automation as possible, detailed screenshots and code samples, and a rich and comprehensive experience while getting started with the Azure Arc platform.

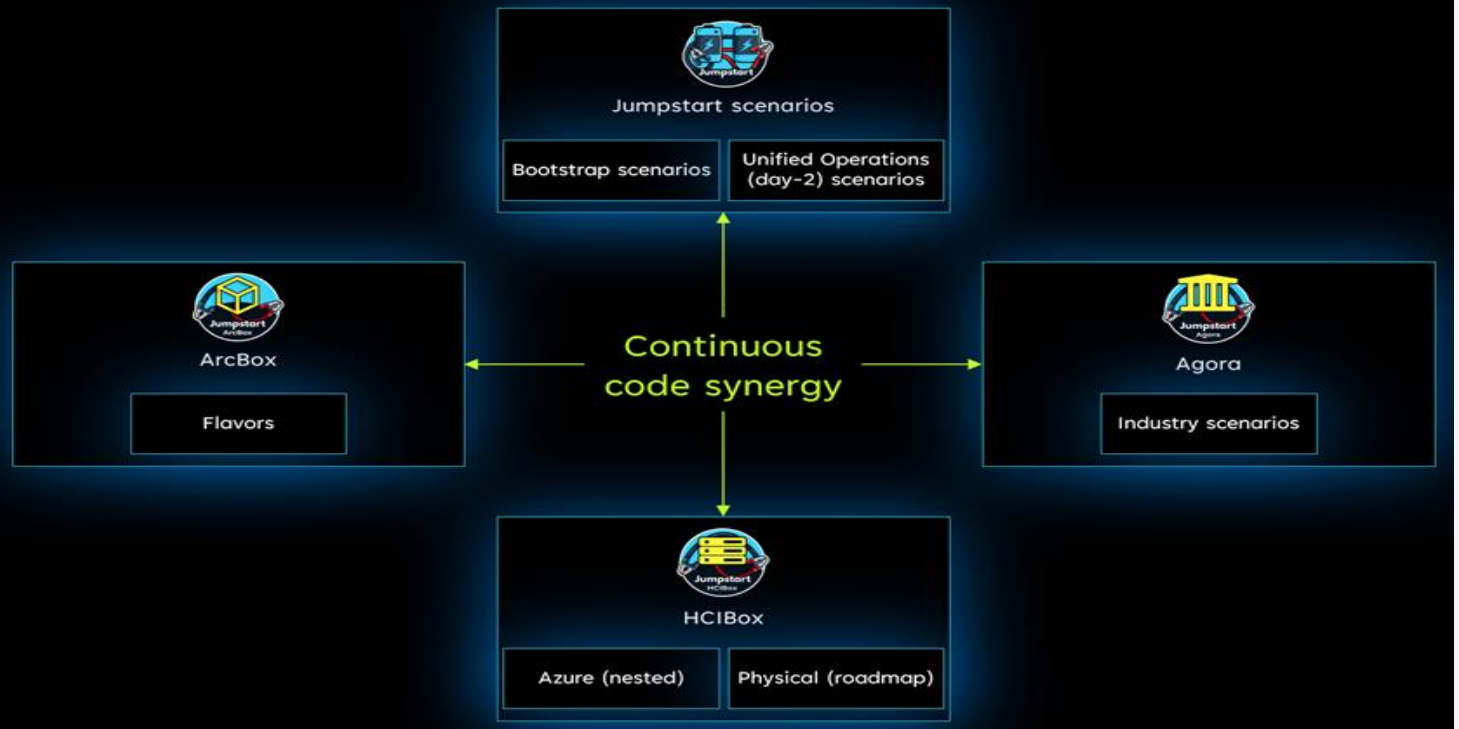
Our goal is for you to have a working Azure Arc environment spin-up in no time so you can focus on the core values of the platform, regardless of where your infrastructure may be, either on-premises or in the cloud.

Discussion on Azure Arc flavours

Azure Arc Jumpstart

Core Design Principals

- "User never fail" mentality
- Minimum dependency between bootstrap and unified operations scenarios
- If it can be automated, it will be automated
- 1-click automation
- Modular automation, Lego-like coding, reusable, comprehensive, repeatable, reliable
- Support as many deployment options as possible
- No detail is too small, no screenshot, note, disclaimer or explanation left behind
- Only public preview and GA services/features



Agora

Jumpstart Agora is a marketplace of various “cloud to edge” industry scenarios, designed to provide an end-to-end user experience.

The word “Agora” comes from the ancient Greek term for a public gathering place or assembly, and it has come to be used more broadly to refer to any place or forum where people come together for discussion or exchange.

Our mission is to create a rich marketplace of applications that can leverage Hybrid Cloud, Internet of Things (IoT), and artificial intelligence (AI) technologies and make those accessible for enablement and educational purposes via the Jumpstart automation mechanisms

Contoso Supermarket

Applications and technology stack

Tooling and operations

Inner loop process
Outer loop process
Dev Containers
IDE
GitHub Actions
GitOps
Dashboards
Cost management
Client interfaces

Contoso Supermarket applications stack

Point of Sale (PoS)

Checkout Queue Monitoring

Freezer Monitoring for Food Safety

Microsoft Defender for Cloud

Azure Log Analytics

Prometheus and Grafana Observability stack (OSS)

Azure Container Registry (ACR)

Azure Monitor

3 x AKS Edge Essentials (as Arc-enabled Kubernetes)

Azure Kubernetes Service

Windows 11 IoT (as Arc-enabled servers)

Azure Automation

Azure Data Explorer (ADX)

Azure IoT Hub

Azure Cosmos DB

Azure Compute, storage and network stack

Azure

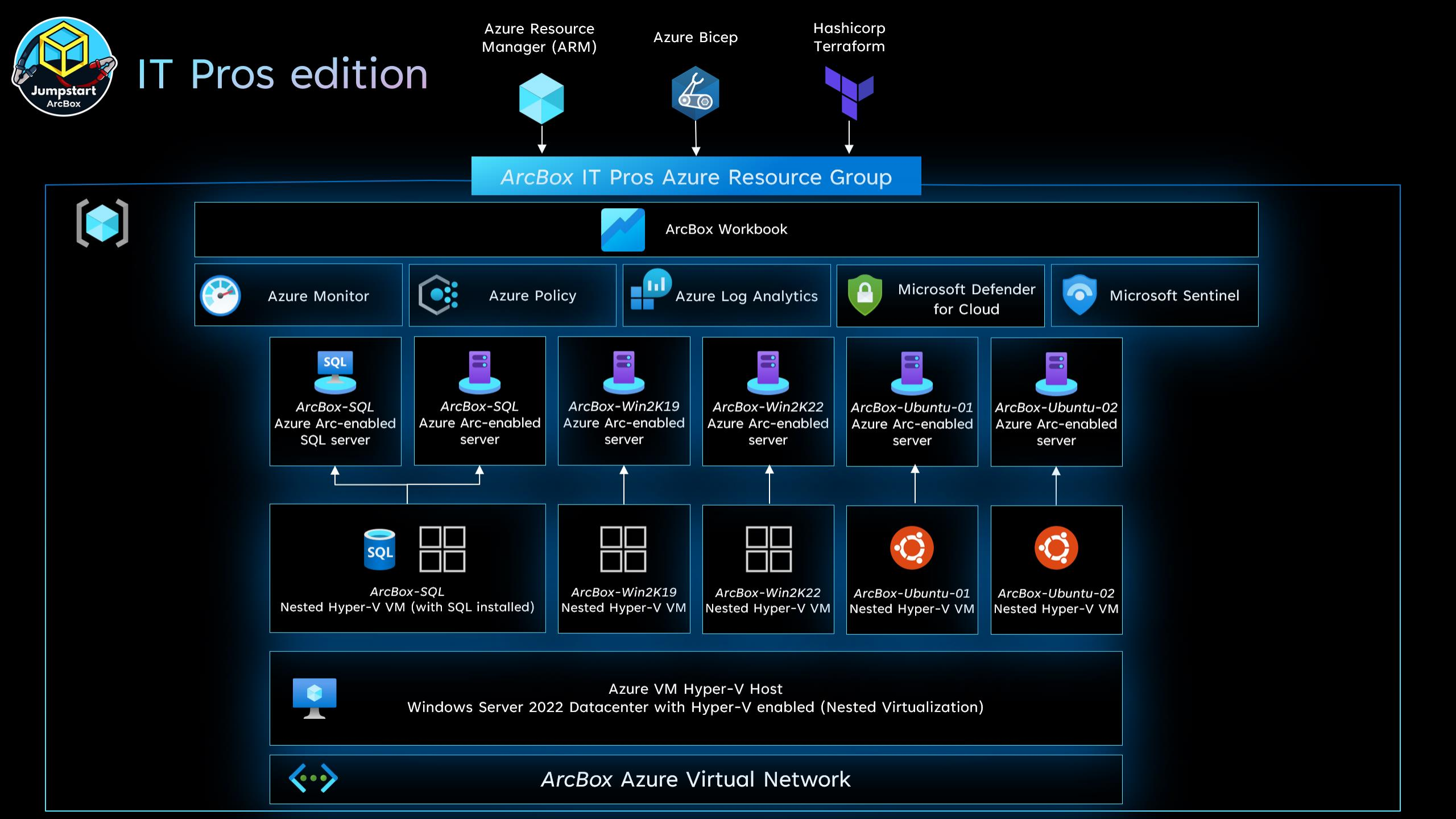
IT Pros (Arc-enabled servers and SQL Server)

ArcBox for IT Pros is a special “flavor” of ArcBox that is intended for users who want to experience Azure Arc-enabled servers capabilities in a sandbox environment.

Use cases

- Sandbox environment for getting hands-on with Azure Arc technologies
- Accelerator for Proof-of-concepts or pilots
- Training tool for Azure Arc skills development
- Demo environment for customer presentations or events
- Rapid integration testing platform
- Infrastructure-as-code and automation template library for building hybrid cloud management solutions

IT Pros edition



Dev Ops (Arc-enabled Kubernetes and DevOps Engineers)

ArcBox for DevOps is a special “flavor” of ArcBox that is intended for users who want to experience Azure Arc-enabled Kubernetes capabilities in a sandbox environment.

Use cases

- Sandbox environment for getting hands-on with Azure Arc technologies and Azure Arc-enabled Kubernetes landing zone accelerator
- Accelerator for Proof-of-concepts or pilots
- Training solution for Azure Arc skills development
- Demo environment for customer presentations or events
- Rapid integration testing platform
- Infrastructure-as-code and automation template library for building hybrid cloud management solutions

DevOps edition

Azure Resource Manager (ARM)

Azure Bicep

Hashicorp Terraform

ArcBox (DevOps) Azure Resource Group

ArcBox Workbook

Azure Monitor

Azure Policy

Azure Log Analytics

Microsoft Defender for Cloud

GitOps configurations

Service observability with Open Service Mesh (OSM)

Secrets management with Azure Key Vault

ArcBox-Client Azure VM

Sample applications

Azure Arc-enabled Kubernetes cluster

Kubernetes Cluster API 3-node cluster deployed using CAPI Azure provider

Sample applications

Azure Arc-enabled Kubernetes cluster

Rancher K3s 1-node Kubernetes cluster

Azure VM Ubuntu server

ArcBox Azure Virtual Network

Data Ops (Arc-enabled SQL Server Managed Instances)

ArcBox for DevOps is a special “flavor” of ArcBox that is intended for users who want to experience Azure Arc-enabled Data Service capabilities in a sandbox environment.

Use cases

- Sandbox environment for getting hands-on with Azure Arc technologies and Azure Arc-enabled Data Platform landing zone accelerator
- Accelerator for Proof-of-concepts or pilots
- Training solution for Azure Arc skills development
- Demo environment for customer presentations or events
- Rapid integration testing platform
- Infrastructure-as-code and automation template library for building hybrid cloud management solutions

DataOps edition

Azure Resource Manager (ARM) | Azure Bicep | Hashicorp Terraform

ArcBox DataOps Azure Resource Group

ArcBox Workbook

Azure Monitor | Azure Policy | Azure Log Analytics | Azure Tags | Grafana

primary site

ArcBox-Client Azure VM installed with DBA tools

ArcBox-DC Azure VM with Active Directory Domain Services + DNS

Sample K8s application

App backend database

Azure Arc Data Controller

Azure Arc-enabled SQL Managed Instance

Azure Arc-enabled Kubernetes cluster

Primary Azure Kubernetes Service (AKS) 3-node cluster

Kubernetes Cluster API 3-node cluster deployed using CAPI Azure provider

Disaster recovery simulation

DR site

DR Azure Kubernetes Service (AKS) 3-node cluster

ArcBox primary Azure Virtual Network

Virtual network peering

ArcBox DR Azure Virtual Network

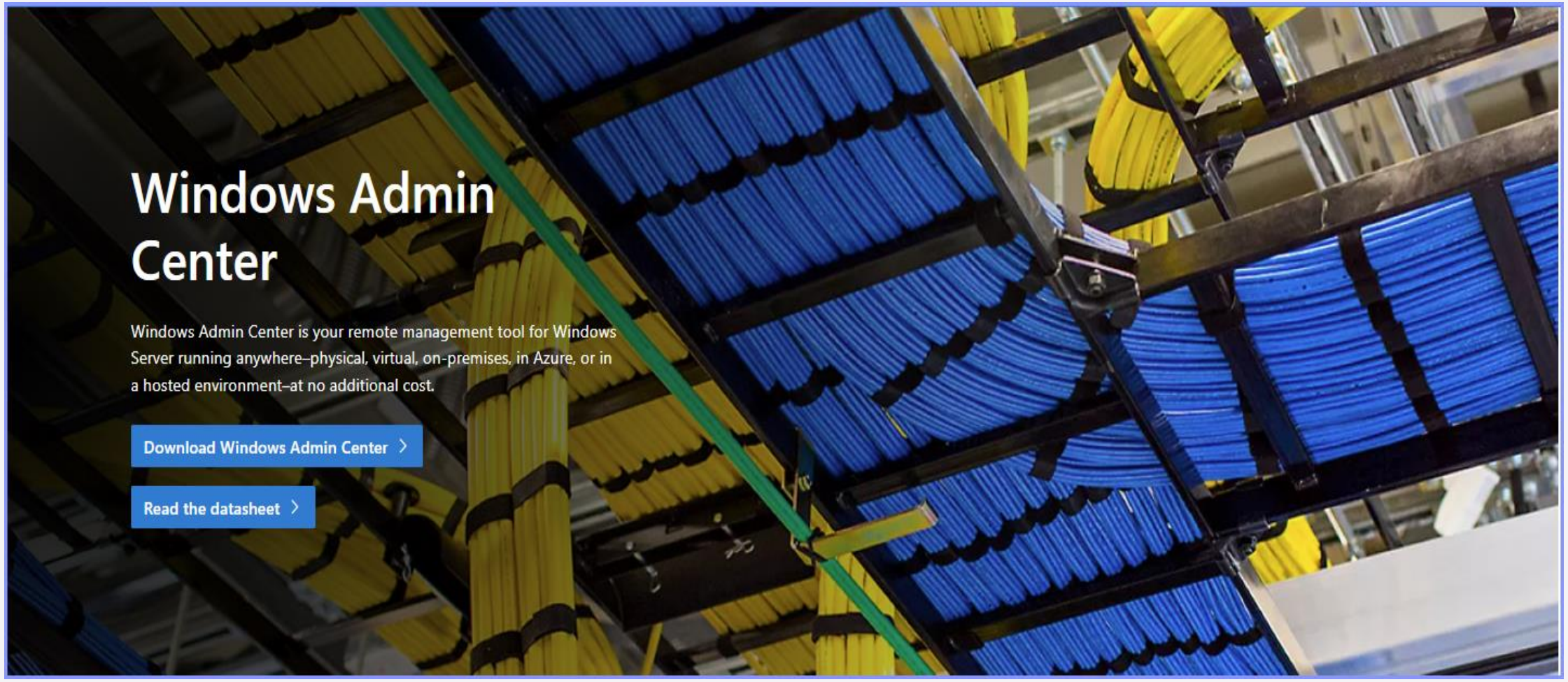
Where to Deploy Azure Arc Box (any flavour)

ArcBox must be deployed to one of the following regions.
Deploying ArcBox outside of these regions may result in unexpected results or deployment errors.

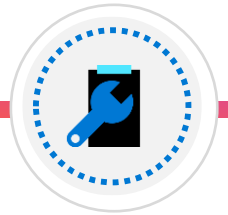
- ❑ East US
- ❑ East US 2
- ❑ Central US
- ❑ West US 2
- ❑ North Europe
- ❑ West Europe
- ❑ France Central
- ❑ UK South
- ❑ Australia East
- ❑ Japan East
- ❑ Korea Central
- ❑ Southeast Asia

Introductory Use-Case

How to manage and organize resources



How to manage and organize resources

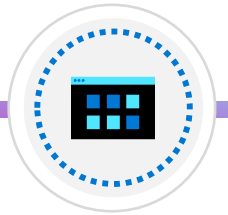


Windows Admin Center in Azure

This new capability allows you to manage the Windows Server OS running on Azure IaaS seamlessly and at a more granular level. Windows Admin Center in the Azure Portal is available to customers running Windows Server 2016, 2019, or 2022 virtual machines.

Hybrid Management In Azure

Integrate your on-premises servers with Azure in just a few clicks. Leverage the power of Azure for monitoring, storage, backup, disaster recovery, and more.



Modern Server Management

Simplify server administration with streamlined server management tools. Configure and troubleshoot your servers and manage Windows Server workloads remotely from a web browser. Use it to manage any version, from 2012 to 2022 and Azure Stack HCI.

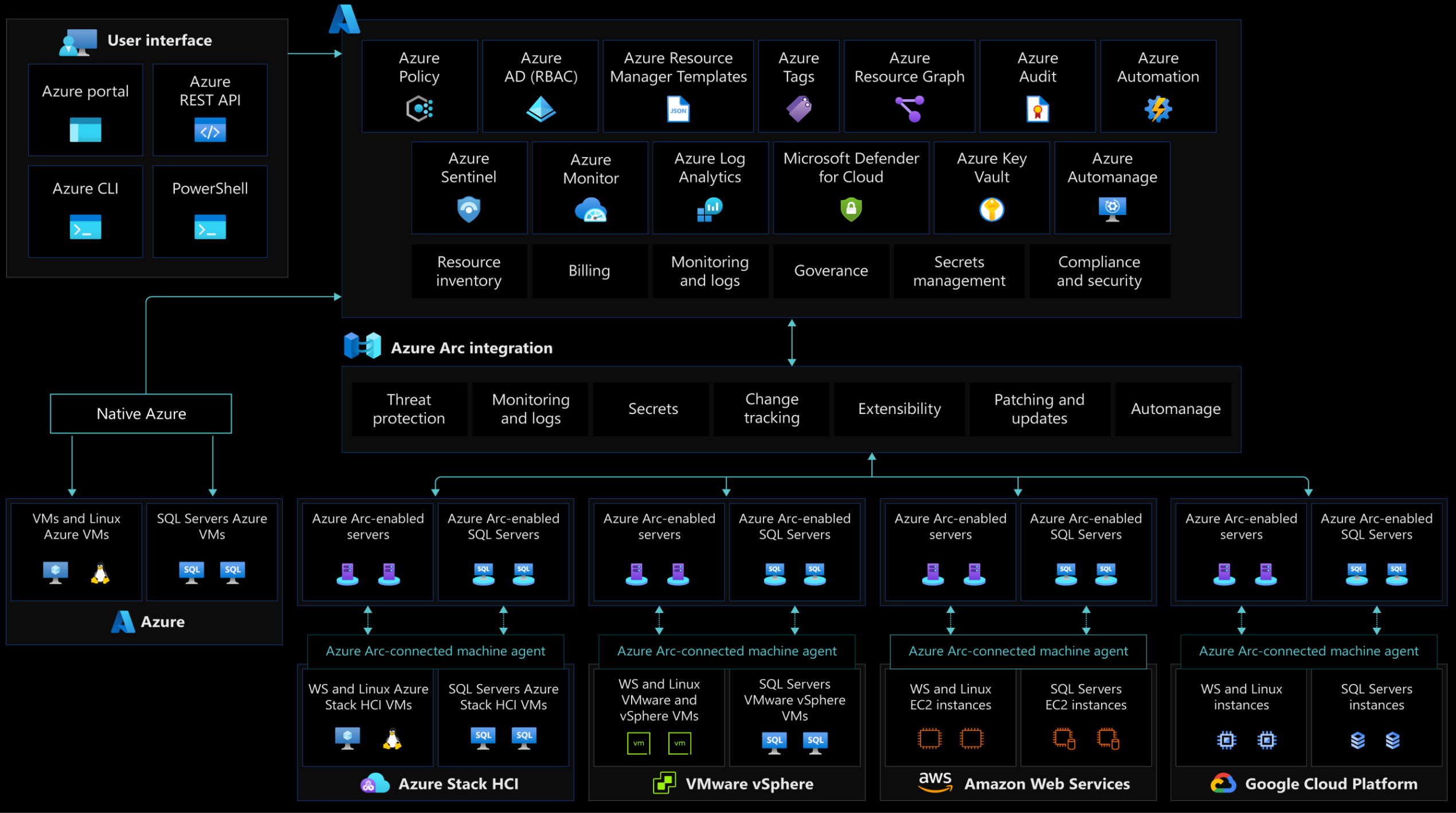
Governance, security, and compliance baseline for Azure Arc-enabled servers

Defining and applying the proper control mechanisms is key in any cloud implementation, as it's the foundational element to stay secured and compliant.

In a traditional environment, these mechanisms usually involve review processes and manual controls. However, the cloud has introduced a new approach to IT governance with automated guardrails and checks.

Azure Policy and **Microsoft Defender for Cloud** are cloud-native tools that allow the implementation of these controls, reports, and remediation tasks in an automated fashion.

By combining them with Azure Arc, you can extend your governance policies and security to any resource in public or private clouds.


User interface
Azure portal
Azure REST API
Azure CLI
PowerShell
Azure Policy
Azure AD (RBAC)
Azure Resource Manager Templates
Azure Tags
Azure Resource Graph
Azure Audit
Azure Automation
Azure Sentinel
Azure Monitor
Azure Log Analytics
Microsoft Defender for Cloud
Azure Key Vault
Azure Automanage
Resource inventory
Billing
Monitoring and logs
Goverance
Secrets management
Compliance and security
Azure Arc integration
Threat protection
Monitoring and logs
Secrets
Change tracking
Extensibility
Patching and updates
Automanage
Native Azure
VMs and Linux Azure VMs
SQL Servers Azure VMs
Azure
Azure Arc-enabled servers
Azure Arc-enabled SQL Servers
Azure Arc-connected machine agent
WS and Linux Azure Stack HCI VMs
SQL Servers Azure Stack HCI VMs
Azure Stack HCI
WS and Linux VMware and vSphere VMs
SQL Servers VMware vSphere VMs
VMware vSphere
WS and Linux EC2 instances
SQL Servers EC2 instances
Amazon Web Services
WS and Linux instances
SQL Servers instances
Google Cloud Platform

Advanced Configuration & Management

How to manage multiple clusters | Kubernetes

Azure Arc-enabled Kubernetes allows you to attach Kubernetes clusters running anywhere so that you can manage and configure them in Azure. By managing all of your Kubernetes resources in a single control plane, you can enable a more consistent development and operation experience to run cloud-native apps anywhere and on any Kubernetes platform.

Once clusters are connected to Azure, they're represented as their own resources in Azure Resource Manager, and they can be organized using resource groups and tagging.

Azure Arc-enabled Kubernetes works with any Cloud Native Computing Foundation (CNCF) certified Kubernetes clusters. This includes clusters running on other public cloud providers (such as GCP or AWS) and clusters running on your on-premises data center (such as VMware vSphere or Azure Stack HCI).

Azure Arc Validate Partners

The Azure Arc team works with key industry Kubernetes offering providers to validate Azure Arc-enabled Kubernetes with their Kubernetes distributions. Future major and minor versions of Kubernetes distributions released by these providers will be validated for compatibility with Azure Arc-enabled Kubernetes.

Important

Azure Arc-enabled Kubernetes works with any Kubernetes clusters that are certified by the Cloud Native Computing Foundation (CNCF), even if they haven't been validated through conformance tests and are not listed on this page.

Validated Distributions

Distribution and infrastructure provider	Version
Cluster API Provider on Azure	Release version: 0.4.12; Kubernetes version: 1.18.2
AKS on Azure Stack HCI	Release version: December 2020 Update; Kubernetes version: 1.18.8
K8s on Azure Stack Edge	Release version: Azure Stack Edge 2207 (2.2.2037.5375); Kubernetes version: 1.22.6
AKS Edge Essentials	Release version 1.0.406.0; Kubernetes version 1.24.3

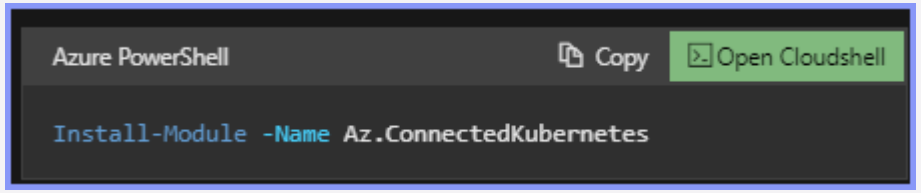
Validated Providers

Provider name	Distribution name	Version
RedHat	OpenShift Container Platform	4.9.43, 4.10.23, 4.11.0-rc.6, 4.13.4
VMware	Tanzu Kubernetes Grid	TKGs 2.2; upstream K8s 1.25.7+vmware.3 TKGm 2.3; upstream K8s v1.26.5+vmware.2 TKGm 2.2; upstream K8s v1.25.7+vmware.2 TKGm 2.1.0; upstream K8s v1.24.9+vmware.1
Canonical	Charmed Kubernetes	1.24, 1.28
SUSE Rancher	Rancher Kubernetes Engine	RKE CLI version: v1.3.13; Kubernetes versions: 1.24.2, 1.23.8
SUSE Rancher	K3s	v1.27.4+k3s1, v1.26.7+k3s1, v1.25.12+k3s1
Nutanix	Nutanix Kubernetes Engine	Version 2.5; upstream K8s v1.23.11
Kublr	Kublr Managed K8s Distribution	Kublr 1.26.0; Upstream K8s Versions: 1.21.3, 1.22.10, 1.22.17, 1.23.17, 1.24.13, 1.25.6, 1.26.4
Mirantis	Mirantis Kubernetes Engine	MKE Version 3.6.0 MKE Version 3.5.5 MKE Version 3.4.7
Wind River	Wind River Cloud Platform	Wind River Cloud Platform 22.12; Upstream K8s version: 1.24.4 Wind River Cloud Platform 22.06; Upstream K8s version: 1.23.1 Wind River Cloud Platform 21.12; Upstream K8s version: 1.21.8 Wind River Cloud Platform 21.05; Upstream K8s version: 1.18.1

Azure Arc-enabled Kubernetes [quickstart]

Get started with Azure Arc-enabled Kubernetes by using **Azure CLI** or **Azure PowerShell** to connect an existing Kubernetes cluster to Azure Arc.

Requirements:
- Azure Subscription
- Identity (user or service principal)
- Azure Powershell min 6.6.0
- Running Kubernetes cluster
    - or Kubernetes in Docker (KIND)
    - or Kubernetes in Docker for Mac or Windows
    - or self-managed Kubernetes with Cluster API
- kubeconfigfile
- network access (next slide)



Requirements for Agent:
- min 850 mb free space
- be ready for about 7% of utilisation of single CPU

Azure Arc-enabled Kubernetes [quickstart] Network Req

Azue Arc agents require the following outbound URLs on https://:443 to function. For *.servicebus.windows.net, websockets need to be enabled for outbound access on firewall and proxy.

Endpoint (DNS)	Description
https://management.azure.com	Required for the agent to connect to Azure and register the cluster.
https://<region>.dp.kubernetesconfiguration.azure.com	Data plane endpoint for the agent to push status and fetch configuration information.
https://login.microsoftonline.com https://<region>.login.microsoft.com login.windows.net	Required to fetch and update Azure Resource Manager tokens.
https://mcr.microsoft.com https://*.data.mcr.microsoft.com	Required to pull container images for Azure Arc agents.
https://gbl.his.arc.azure.com	Required to get the regional endpoint for pulling system-assigned Managed Identity certificates.
https://*.his.arc.azure.com	Required to pull system-assigned Managed Identity certificates.
https://k8connecthelm.azureedge.net	az connectedk8s connect uses Helm 3 to deploy Azure Arc agents on the Kubernetes cluster. This endpoint is needed for Helm client download to facilitate deployment of the agent helm chart.
guestnotificationservice.azure.com *.guestnotificationservice.azure.com sts.windows.net https://k8sconnectcsp.azureedge.net	For Cluster Connect and for Custom Location based scenarios.
*.servicebus.windows.net	For Cluster Connect and for Custom Location based scenarios.
https://graph.microsoft.com/	Required when Azure RBAC is configured.
*.arc.azure.net	Required to manage connected clusters in Azure portal.
https://<region>.obo.arc.azure.com:8084/	Required when Cluster Connect is configured.
dl.k8s.io	Required when automatic agent upgrade is enabled.

What is Azure Arc Resource Bridge (Preview)

Azure Arc resource bridge (preview) is a Microsoft managed product that is part of the core Azure Arc platform. It is designed to host other Azure Arc services.

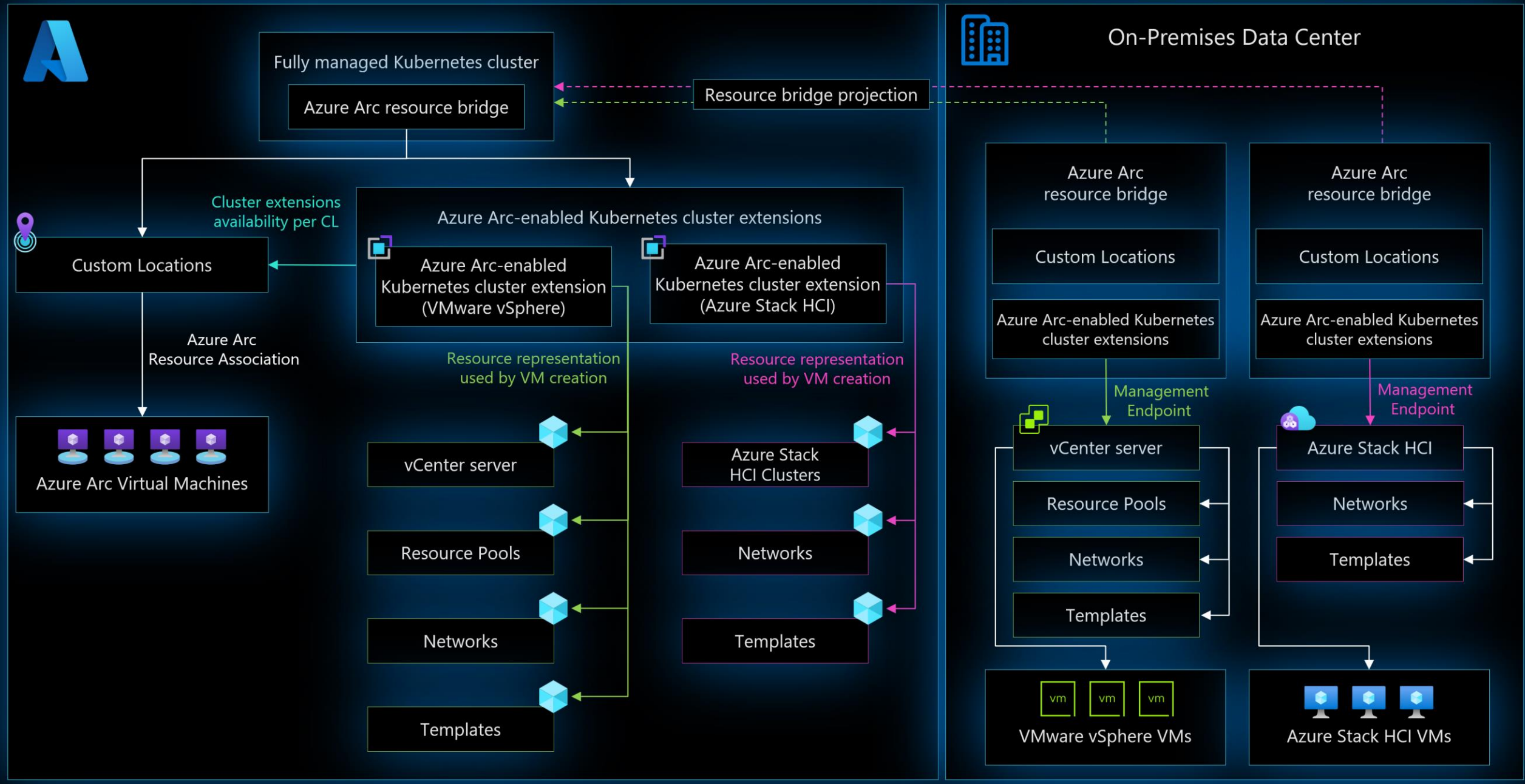
In this release, the resource bridge supports VM self-servicing and management from Azure, for virtualized Windows and Linux virtual machines hosted in an

- on-premises environment on Azure Stack HCI
- VMware (Arc-enabled VMware vSphere preview),
- and System Center Virtual Machine Manager (SCVMM) (Arc-enabled SCVMM preview)

Arc resource bridge has the following minimum resource requirements:

- ❑ 50 GB disk space
- ❑ 4 vCPUs
- ❑ 8 GB memory

Azure Arc Resource Bridge architecture



Azure Arc Resource Bridge | Two main concepts

Cluster Extention

The Azure service deployed to run on-premises. For the preview release, it supports three services:

- Azure Arc-enabled VMware
- Azure Arc VM management on Azure Stack HCI
- Azure Arc-enabled System Center Virtual Machine Manager (SCVMM)

Custom Location

A deployment target where you can create Azure resources. It maps to different resource for different Azure services. For example, for Arc-enabled VMware, the custom locations resource maps to an instance of vCenter, and for Azure Arc VM management on Azure Stack HCI, it maps to an HCI cluster instance.

Azure Arc Resource Bridge | general benefits

Arc resource bridge delivers the following benefits:

- Enables VM self-servicing from Azure without having to create and manage a Kubernetes cluster.
- Fully supported by Microsoft, including updates to core components.
- Supports deployment to any private cloud hosted on Hyper-V or VMware from the Azure portal or using the Azure Command-Line Interface (CLI).

Azure Arc resource bridge (preview) hosts other components such as custom locations, cluster extensions, and other Azure Arc agents in order to deliver the level of functionality with the private cloud infrastructures it supports. This complex system is composed of three layers:

- The base layer that represents the resource bridge and the Arc agents.
- The platform layer that includes the custom location and cluster extension.
- The solution layer for each service supported by Arc resource bridge (that is, the different type of VMs).

Azure Arc Resource Bridge | benefits for VMware

By registering resource pools, networks, and VM templates, you can represent a subset of your vCenter resources in Azure to enable self-service.

Integration with Azure allows you to manage access to your vCenter resources in Azure to maintain a secure environment. You can also perform various operations on the VMware virtual machines that are enabled by Arc-enabled VMware vSphere:

- Start, stop, and restart a virtual machine
- Control access and add Azure tags
- Add, remove, and update network interfaces
- Add, remove, and update disks and update VM size (CPU cores and memory)
- Enable guest management
- Install extensions

Azure Arc Resource Bridge | benefits for SCVMM

You can connect an SCVMM management server to Azure by deploying Azure Arc resource bridge (preview) in the VMM environment.

Azure Arc resource bridge (preview) enables you to represent the SCVMM resources (clouds, VMs, templates etc.) in Azure and perform various operations on them:

- Start, stop, and restart a virtual machine
- Control access and add Azure tags
- Add, remove, and update network interfaces
- Add, remove, and update disks and update VM size (CPU cores and memory)

Policy enforcement and governance in complex environments

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

Specifically, some useful governance actions you can enforce with Azure Policy include:

- ❑ Ensuring your team deploys Azure resources only to allowed regions
- ❑ Enforcing the consistent application of taxonomic tags
- ❑ Requiring resources to send diagnostic logs to a Log Analytics workspace

It's important to recognize that with the introduction of **Azure Arc**, you can extend your policy-based governance across different cloud providers and even to your local datacenters.

Policy Assignement & non-compliant resources (1)

The first step in understanding compliance in Azure is to identify the status of your resources. Azure Policy supports auditing the state of your Azure Arc-enabled server with guest configuration policies. Azure Policy's guest configuration definitions can audit or apply settings inside the machine.

The process of creating and assigning a policy in order to identify which of your Azure Arc-enabled servers don't have the Log Analytics agent for Windows or Linux installed. These machines are considered *non-compliant* with the policy assignment.

Policy Assignment & non-compliant resources (2)

Required steps:

- Go to *Policy* in Portal
- Select *Assignment*
- Choose *Scope* (Management Group/Subscription/Resource Group
- Choose *Exclusion* (if needed)
- Select *Policy Definition* (they could include below)
  - Enforce tag and its value
  - Apply tag and its value
  - Inherit a tag from the resource group if missing

Policy Assignmnt & non-compliant resources (3)

Regulatory Assessments

Australian Government ISM PROTECTED
Canada Federal PBMM
CMMC Level 3
FedRAMP High
FedRAMP Moderate
HIPAA HITRUST 9.2
IRS 1075 September 2016
New Zealand ISM Restricted
New Zealand ISM Restricted 3.5
RBI ITF Banks v2016
RBI ITF NBFC v2017
RMIT Malaysia
SWIFT CSP-CSCF v2021

Industry Assessments

CIS Microsoft Azure Foundations Benchmark 1.1.0
CIS Microsoft Azure Foundations Benchmark 1.3.0
CIS Microsoft Azure Foundations Benchmark 1.4.0
CIS Microsoft Azure Foundations Benchmark 2.0.0
ISO 27001:2013
Microsoft cloud security benchmark
NL BIO Cloud Theme
PCI DSS 3.2.1
PCI DSS 4.0
UK OFFICIAL and UK NHS

Regional Availability ~ Azure Products by Region |

	UNITED KINGDOM		UNITED STATES							
Products	UK South	UK West	Central US	East US	East US 2	North Central US	South Central US	West Central US	West US	West US 2
Azure Arc										
Azure Arc enabled servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Arc enabled Kubernetes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Arc-enabled PostgreSQL Hyperscale	■		■	■	■	◕				■
Azure Arc-enabled SQL Managed Instance	✓		✓	✓	✓	✓	✓	✓	✓	✓
SQL Server – Azure Arc	✓		✓	✓	✓		✓	✓		✓
Azure Arc enabled VMware vSphere	■			■	■		■			■
Azure Arc-enabled System Center VMM				□						

Release dates, features and requirements are subject to change prior to final commercial release of the products/features/software described herein. This page is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION ON THIS PAGE. To see which regions Microsoft Azure Offers may be eligible, see Find Azure credit offers in your region.

Cost Management

How Azure Arc can help in cost management and optimization

OPTIMIZATON: Extend Azure management and services anywhere

Azure Arc extends management and services from Azure to any infrastructure. As an extension of Azure, it offers the below core control plane at no cost to customers, while preserving consistent pricing on all management and services originated from Azure.

- ❑ Resource inventory and organisations through Azure resource groups and tags
- ❑ Indexing and searching through Azure Resource Graph
- ❑ Access and security through RBAC and subscriptions
- ❑ Environments and automation through templates and extensions

How Azure Arc can help in cost management and optimization

OPTIMIZATON: Extend Azure management and services anywhere

Below Azure Arc-enabled services will be charged consistently as in the original Azure services, excluding any customer-provided infrastructure costs.

- ❑ Azure Arc-enabled SQL Server
- ❑ Azure Arc-enabled SQL Managed Instance
- ❑ Azure Arc-enabled PostgreSQL (Preview)
- ❑ Other arc-enabled services that become available

How Azure Arc can help in cost management and optimization

COST:

Azure Arc is offered at no additional cost for managing Azure Arc–enabled servers and Azure Arc–enabled Kubernetes, though there are charges for add-on Azure management services.
Azure Arc–enabled SQL Managed Instance is generally available for an additional cost. Additional data and application services are in preview and currently offered at no additional cost.

Pricing – Azure Arc | Microsoft Azure

How Azure Arc can help in cost management and optimization

Azure Arc-enabled servers

The following Azure Arc control plane functionality is offered at no extra cost:

- Resource organization through Azure management groups and tags
- Searching and indexing through Azure Resource Graph
- Access and security through Azure Role-based access control (RBAC)
- Environments and automation through templates and extensions

Any Azure service that is used on Azure Arc-enabled servers, such as Microsoft Defender for Cloud or Azure Monitor, will be charged as per the pricing for that service.

For information, see the Azure pricing page.

How Azure Arc can help in cost management and optimization

Azure Arc-enabled Kubernetes
Any Azure service that is used on Azure Arc-enabled Kubernetes, such as Microsoft Defender for Cloud or Azure Monitor, will be charged as per the pricing for that service.

For more information on pricing for configurations on top of Azure Arc-enabled Kubernetes, see the Azure pricing page.

Azure Arc-enabled data services
For information, see the Azure pricing page.

Azure Hybrid Benefits in Azure Arc

Windows Server VMs on Azure

The license for Windows Server is covered by Azure Hybrid Benefit, so you only need to pay for the base compute rate of the VM.

The base compute rate is equal to the Linux rate for VMs.

Azure Stack HCI

The Azure Stack HCI host fee and Windows Server subscription fee are waived with Azure Hybrid Benefit.

That is, unlimited virtualization rights are provided at no extra cost. You still pay other costs associated with Azure Stack HCI (for example, customer-managed hardware, Azure services, and workloads).

Software Assurance must be active to use this benefit.

Azure Kubernetes Services

Run AKS on Windows Server and Azure Stack HCI at no extra cost.

You still pay for the underlying host infrastructure and any licenses for Windows containers unless you're also eligible for Azure Hybrid Benefit for Azure Stack HCI.

With Azure Hybrid Benefit for Azure Stack HCI, you can waive fees for the Azure Stack HCI host and Windows Server subscription.

Extended Security Updates in Azure Arc

Additional year of extended security updates, only on Azure, for Windows Server and SQL Server
As SQL Server and Windows Server releases end support, many customers are taking advantage of Azure's commitment to security and compliance and have moved to Azure to protect their workloads with free Extended Security Updates.

For those customers who need some more time to upgrade and modernize their SQL Server and Windows Server on Azure, we will now provide one additional year of free extended security updates, only on Azure. This includes other Azure products such as Azure Dedicated Host, Azure VMWare Solution, Azure Nutanix Solution, and Azure Stack (Hub, Edge, and HCI).

What dates do I need to keep in mind?

July 12, 2022

SQL Server 2008 and 2008 R2 Extended Security Updates end. SQL Server 2012 end of support.

Jan 10, 2023

Windows Server 2008 and 2008 R2 Extended Security Updates come to an end.

Oct 10, 2023

The end of support for Windows Server 2012 and 2012 R2.

Jan 09, 2024

Windows Server 2008 and 2008 R2 Extended Security Updates on Azure come to an end.

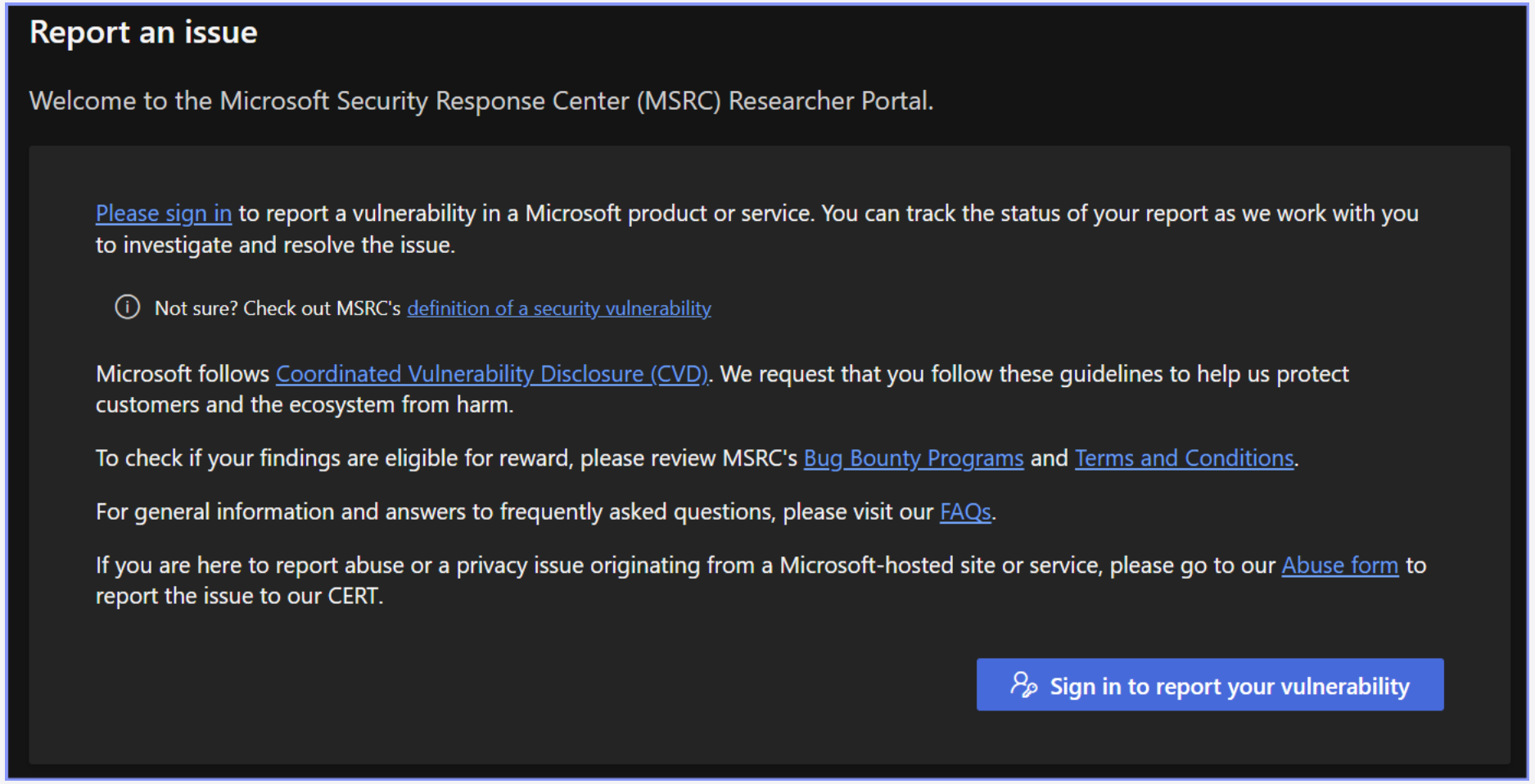
Security Considerations

Microsoft Security Approach

Microsoft takes the security of our software products and services seriously, which includes all source code repositories managed through our GitHub organizations, which include Microsoft, Azure, DotNet, AspNet, Xamarin, and our GitHub organizations.

If you believe you have found a security vulnerability in any Microsoft-owned repository that meets Microsoft's definition of a security vulnerability, please report it to us

Microsoft Security Approach | Report an Issue

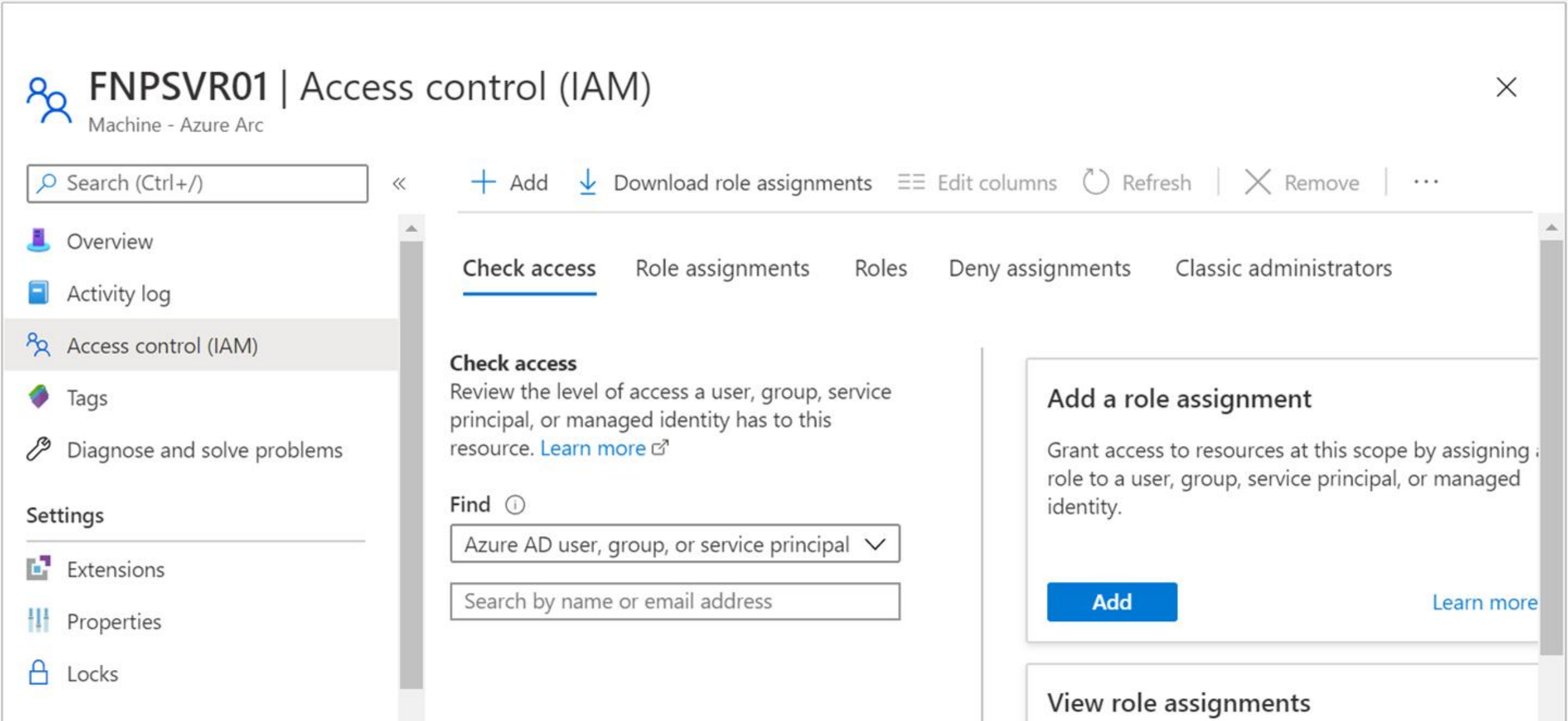


Identity and access control (1)

Azure role-based access control is used to control which accounts can see and manage your Azure Arc-enabled server. From the **Access Control (IAM)** page in the Azure portal, you can verify who has access to your Azure Arc-enabled server.

Users and applications granted contributor or administrator role access to the resource can make changes to the resource, including deploying or deleting extensions on the machine. Extensions can include arbitrary scripts that run in a privileged context, so consider any contributor on the Azure resource to be an indirect administrator of the server.

Identity and access control (2)



Identity and access control (3)

To manage the Azure Connected Machine agent (azcmagent) on Windows, your user account needs to be a member of the local Administrators group. On Linux, you must have root access permissions.

The Azure Connected Machine agent is composed of three services, which run on your machine.

- **The Hybrid Instance Metadata Service (himds)** service is responsible for all core functionality of Arc. This includes sending heartbeats to Azure, exposing a local instance metadata service for other apps to learn about the machine's Azure resource ID, and retrieve Microsoft Entra tokens to authenticate to other Azure services. This service runs as an unprivileged virtual service account (NT SERVICE\himds) on Windows, and as the **himds** user on Linux. The virtual service account requires the Log on as a Service right on Windows.
- **The Guest Configuration service (GCService)** is responsible for evaluating Azure Policy on the machine.
- **The Guest Configuration Extension service (ExtensionService)** is responsible for installing, upgrading, and deleting extensions (agents, scripts, or other software) on the machine.

The guest configuration and extension services run as **Local System** on Windows, and as **root** on Linux.

Local agent security controls

Starting with agent version 1.16, you can optionally limit the extensions that can be installed on your server and disable Guest Configuration. These controls can be useful when connecting servers to Azure for a single purpose, such as collecting event logs, without allowing other management capabilities to be used on the server.

These security controls can only be configured by running a command on the server itself and cannot be modified from Azure. This approach preserves the server admin's intent when enabling remote management scenarios with Azure Arc, but also means that changing the setting is more difficult if you later decide to change them. This feature is intended for sensitive servers (for example, Active Directory Domain Controllers, servers that handle payment data, and servers subject to strict change control measures).

Extension allowlists and blocklists

To limit which extensions can be installed on your server, you can configure lists of the extensions you wish to allow and block on the server. The extension manager evaluates all requests to install, update, or upgrade extensions against the allowlist and blocklist to determine if the extension can be installed on the server. Delete requests are always allowed.

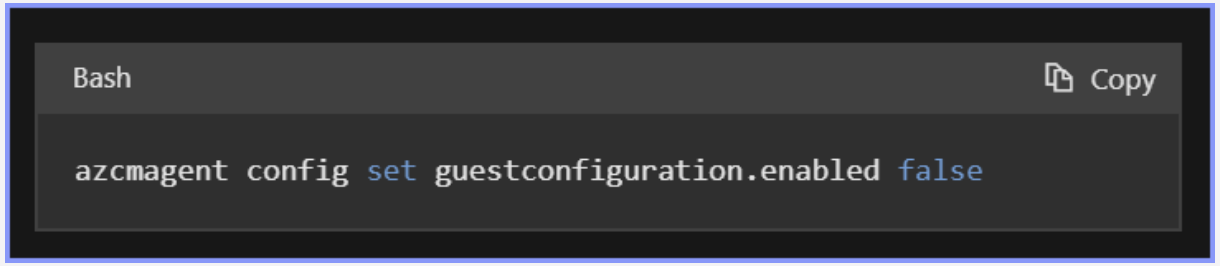
The most secure option is to explicitly allow the extensions you expect to be installed. Any extension not in the allowlist is automatically blocked. To configure the Azure Connected Machine agent to allow only the Azure Monitor Agent for Linux, run the following command on each server:

If an extension is already installed on your server before you configure an allowlist or blocklist, **it won't automatically be removed**.
It's your responsibility to delete the extension from Azure to fully remove it from the machine. Delete requests are always accepted to accommodate this scenario. Once deleted, the allowlist and blocklist determine whether or not to allow future install attempts.

Enable or disable Guest Configuration

Azure Policy's Guest Configuration feature enables you to audit and configure settings on your server from Azure. You can disable Guest Configuration from running on your server if you don't want to allow this functionality.

When Guest Configuration is disabled, any Guest Configuration policies assigned to the machine in Azure show as noncompliant. Consider creating an exemption for these machines or changing the scope of your policy assignments if you don't want to see these machines reported as noncompliant.



Enable or disable the extension manager

The extension manager is responsible for installing, updating, and removing VM Extensions on your server. You can disable the extension manager to prevent managing any extensions on your server, but we recommend using the allow and blocklists instead for more granular control.

Disabling the extension manager won't remove any extensions already installed on your server. Extensions that are hosted in their own Windows or Linux services, such as the Log Analytics Agent, might continue to run even if the extension manager is disabled.

Other extensions that are hosted by the extension manager itself, like the Azure Monitor Agent, don't run if the extension manger is disabled. You should remove any extensions before disabling the extension manager to ensure no extensions continue to run on the server.

```bash
azcmagent config set extensions.enabled false
```

Locked down machine best practices

When configuring the Azure Connected Machine agent with a reduced set of capabilities, it's important to consider the mechanisms that someone could use to remove those restrictions and implement appropriate controls. Anybody capable of running commands as an administrator or root user on the server can change the Azure Connected Machine agent configuration.

Extensions and guest configuration policies execute in privileged contexts on your server, and as such might be able to change the agent configuration. If you apply local agent security controls to lock down the agent, Microsoft recommends the following best practices to ensure only local server admins can update the agent configuration:

- *Use allowlists for extensions instead of blocklists whenever possible.*
- *Don't include the Custom Script Extension in the extension allowlist to prevent execution of arbitrary scripts that could change the agent configuration.*
- *Disable Guest Configuration to prevent the use of custom Guest Configuration policies that could change the agent configuration.*

Plan BEFORE deploy Azure Arc-enabled servers

know your stuff

Deployment of an IT infrastructure service or business application is a challenge for any company. In order to execute it well and avoid any unwelcome surprises and unplanned costs, you need to thoroughly plan for it to ensure that you're as ready as possible. To plan for deploying Azure Arc-enabled servers at any scale, it should cover the design and deployment criteria that needs to be met in order to successfully complete the tasks.

For the deployment to proceed smoothly, your plan should establish a clear understanding of:

- ❑ Roles and responsibilities.
- ❑ Inventory of physical servers or virtual machines to verify they meet network and system requirements.
- ❑ The skill set and training required to enable successful deployment and on-going management.
- ❑ Acceptance criteria and how you track its success.
- ❑ Tools or methods to be used to automate the deployments.
- ❑ Identified risks and mitigation plans to avoid delays, disruptions, etc.
- ❑ How to avoid disruption during deployment.
- ❑ What's the escalation path when a significant issue occurs?

Phase 1 | Build a Foundation

Task	Detail	Estimated duration
Create a resource group	A dedicated resource group to include only Azure Arc-enabled servers and centralize management and monitoring of these resources.	One hour
Apply Tags to help organize machines.	Evaluate and develop an IT-aligned tagging strategy that can help reduce the complexity of managing your Azure Arc-enabled servers and simplify making management decisions.	One day
Design and deploy Azure Monitor Logs	Evaluate design and deployment considerations to determine if your organization should use an existing or implement another Log Analytics workspace to store collected log data from hybrid servers and machines.[1]	One day
Develop an Azure Policy governance plan	Determine how you will implement governance of hybrid servers and machines at the subscription or resource group scope with Azure Policy.	One day
Configure Role based access control (RBAC)	Develop an access plan to control who has access to manage Azure Arc-enabled servers and ability to view their data from other Azure services and solutions.	One day
Identify machines with Log Analytics agent already installed	Run the following log query in Log Analytics to support conversion of existing Log Analytics agent deployments to extension-managed agent: Heartbeat | summarize arg_max(TimeGenerated, OSType, ResourceId, ComputerEnvironment) by Computer | where ComputerEnvironment == "Non-Azure" and isempty(ResourceId) | project Computer, OSType	One hour

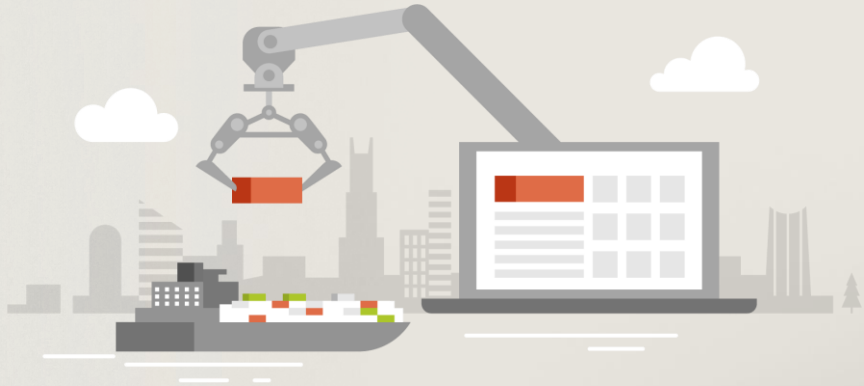
Phase 2 | Deploy

Task	Detail	Estimated duration
Download the pre-defined installation script	•Review and customize the pre-defined installation script for at-scale deployment of the Connected Machine agent to support your automated deployment requirements. Sample at-scale onboarding resources: At-scale basic deployment script •At-scale onboarding VMware vSphere Windows Server VMs •At-scale onboarding VMware vSphere Linux VMs •At-scale onboarding AWS EC2 instances using Ansible	One or more days depending on requirements, organizational processes (for example, Change and Release Management), and automation method used.
Create service principal	Create a service principal to connect machines non-interactively using Azure PowerShell or from the portal.	One hour
Deploy the Connected Machine agent to your target servers and machines	Use your automation tool to deploy the scripts to your servers and connect them to Azure.	One or more days depending on your release plan and if following a phased rollout.

Phase 3 | Manage and operate

Task	Detail	Estimated duration
Create a Resource Health alert	If a server stops sending heartbeats to Azure for longer than 15 minutes, it can mean that it is offline, the network connection has been blocked, or the agent is not running. Develop a plan for how you'll respond and investigate these incidents and use Resource Health alerts to get notified when they start. Specify the following when configuring the alert: **Resource type** = **Azure Arc-enabled servers** **Current resource status** = **Unavailable** **Previous resource status** = **Available**	One hour
Create an Azure Advisor alert	For the best experience and most recent security and bug fixes, we recommend keeping the Azure Connected Machine agent up to date. Out-of-date agents will be identified with an Azure Advisor alert. Specify the following when configuring the alert: **Recommendation type** = **Upgrade to the latest version of the Azure Connected Machine agent**	One hour
Assign Azure policies to your subscription or resource group scope	Assign the **Enable Azure Monitor for VMs** policy (and others that meet your needs) to the subscription or resource group scope. Azure Policy allows you to assign policy definitions that install the required agents for VM insights across your environment.	Varies
Enable Update Management for your Azure Arc-enabled servers	Configure Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines registered with Azure Arc-enabled servers.	15 minutes

Advanced Azure Arc Features



Azure Kubernetes Service (AKS)

Edge Essentials

Azure Kubernetes Service (AKS) hybrid options on Windows

Deploy your Linux and/or Windows containerized workloads

AKS hybrid options on Windows

Azure Arc control plane to manage your cluster in Azure

Standard kubectl to manage your cluster using PowerShell

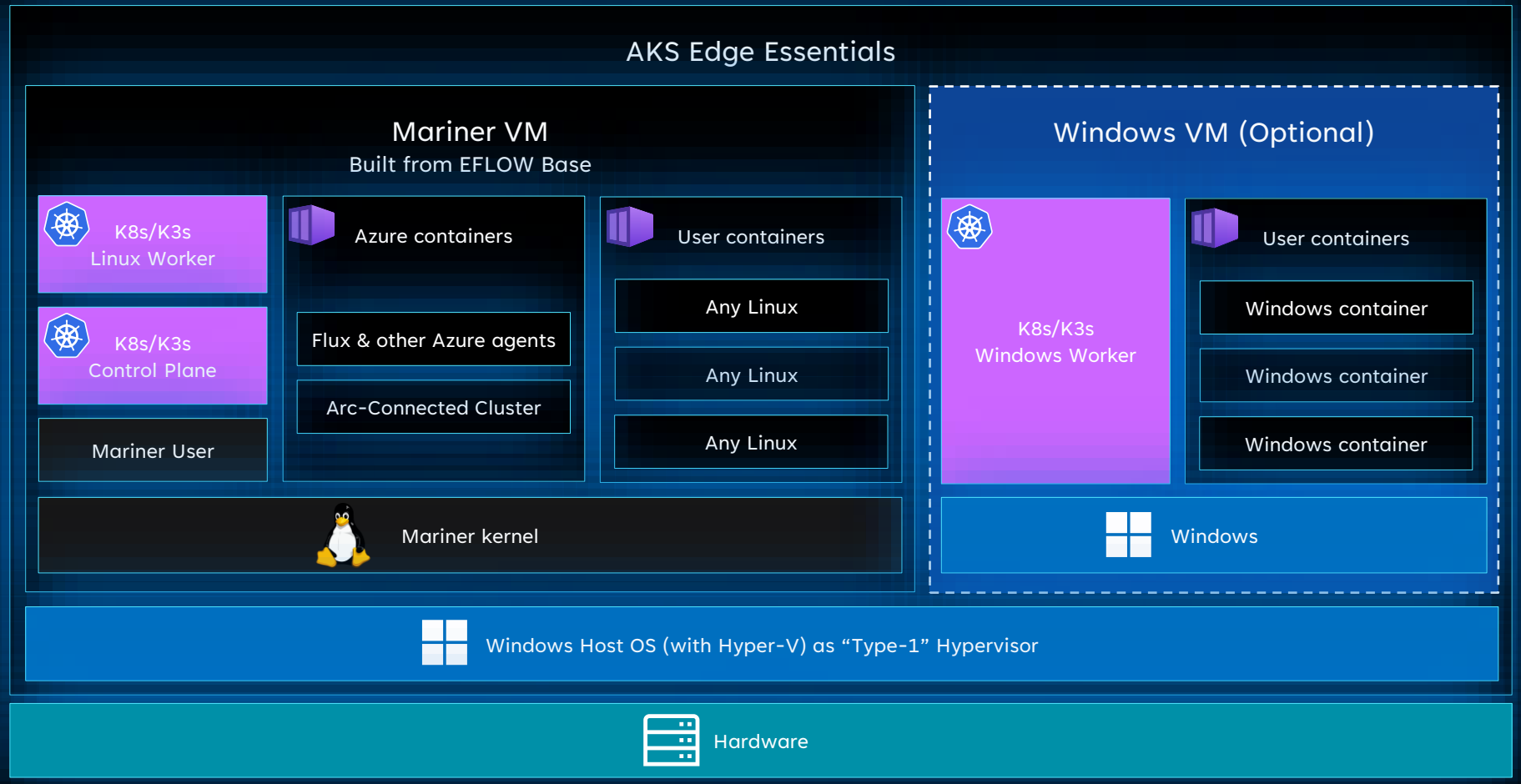
CNCF-conformant Kubernetes platform

PowerShell cmdlets and agents to enable provisioning and control of VMs and infra

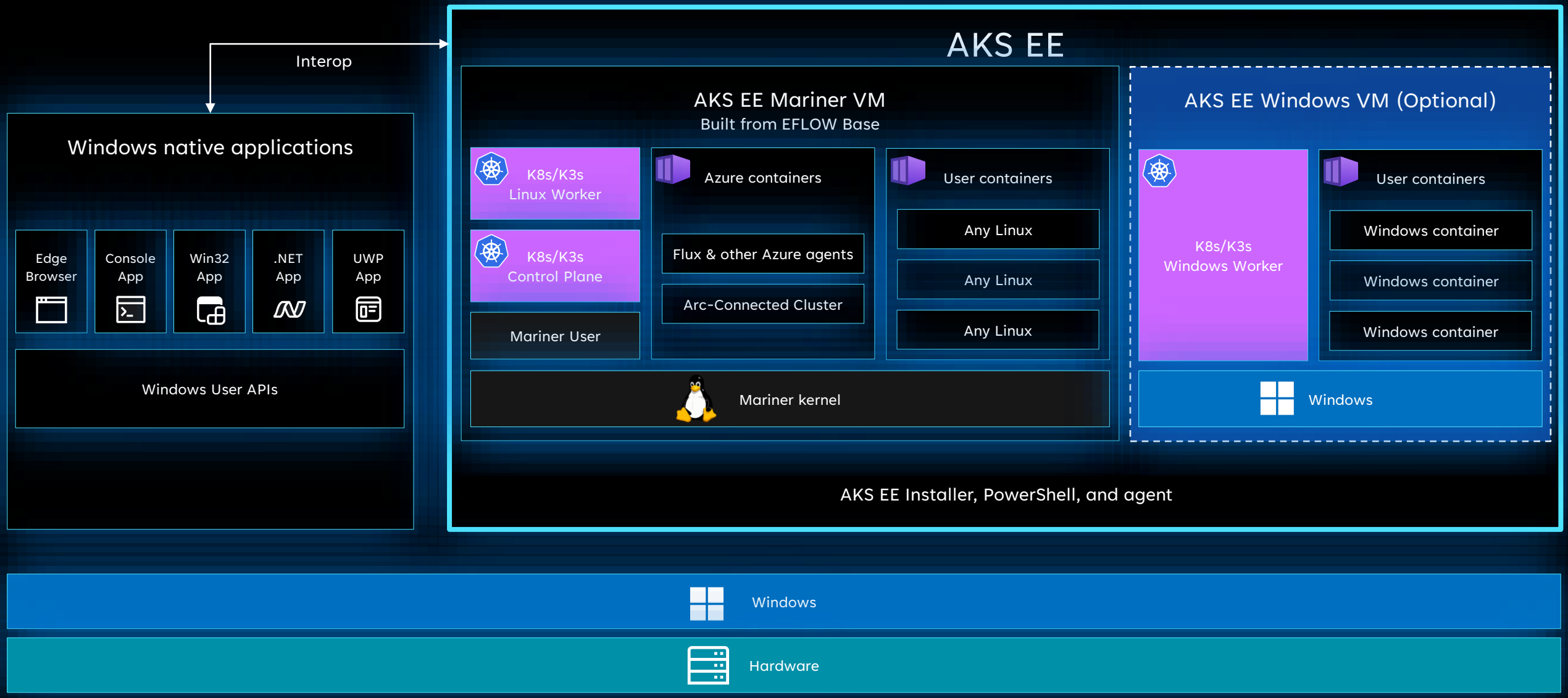
Windows 10/11 (IoT Enterprise / Enterprise / Pro) and Windows Server

Edge computing devices (with 8GB+ RAM)

Azure Kubernetes Service Edge Essentials (AKS EE) architecture

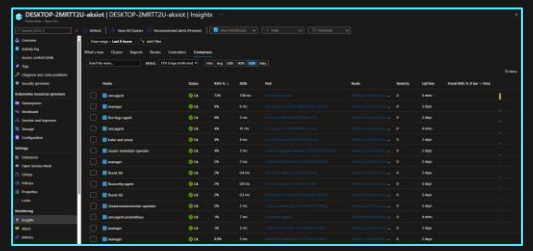


AKS Edge Essentials architecture



Azure Resource Manager

Build and manage cloud deployments directly from the Azure portal



Deploy Cluster extensions

Azure Monitor
Monitor servers in Azure, machines on-premises or at other cloud providers.

Azure Policy
Enforce organizational standards and assess compliance at-scale.

Azure App Service
Quickly build, deploy, and scale web apps and APIs on Kubernetes or Azure.

Deploy your own workloads

PR Pipeline

App repository

GitOps
Manage your desired state Kubernetes cluster configurations with Git

CI Pipeline

CD Pipeline

GitOps repository

Microsoft Artifact Registry
Build, store, and manage container artifacts for your deployments

OS and VM Updates

Windows Update
Get the latest fixes, updates and security improvements

From cloud to edge and back

Azure Arc

Cluster extensions

User workloads

Flux

Containerized workloads

Pull cluster desired state

Deploy AKS-IoT on a device like an application

AKS EE Kubernetes Platform

K8s/K3s

Linux VM

Windows VM (optional)

Connected via Azure Arc-enabled Kubernetes

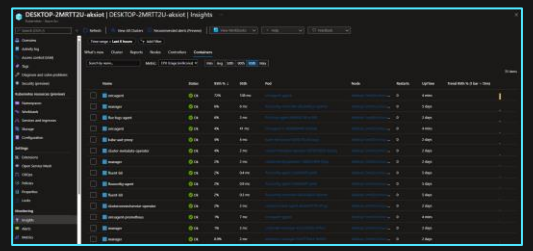
Connected via Azure Arc-enabled servers

Windows Host OS (with Hyper-V)

Hardware

Azure Resource Manager

Build and manage cloud deployments directly from the Azure portal



Deploy Cluster extensions

Azure Monitor
Monitor servers in Azure, machines on-premises or at other cloud providers.

Azure Policy
Enforce organizational standards and assess compliance at-scale.

Azure App Service
Quickly build, deploy, and scale web apps and APIs on Kubernetes or Azure.

Deploy your own workloads

PR Pipeline

App repository

GitOps
Manage your desired state Kubernetes cluster configurations with Git

CI Pipeline

CD Pipeline

GitOps repository

Microsoft Artifact Registry
Build, store, and manage container artifacts for your deployments

OS and VM Updates

Windows Update
Get the latest fixes, updates and security improvements

Azure Arc

From cloud to edge and back

Deploy AKS-IoT on a device like an application

Connected via Azure Arc-enabled Kubernetes

Cluster extensions

User workloads

Flux

Containerized workloads

AKS EE Kubernetes Platform

K8s/K3s

Linux VM

Windows VM (optional)

Windows Host OS (with Hyper-V)

Hardware

Cache containers

Cache updates

On-premises, user-owned private Container Registry

Pull cluster desired state

GitOps repository

Windows Server Update Services (WSUS) enables IT admins to deploy Microsoft updates.

Disconnected on-premises

On a managed VM

With a managed VM you do not need to manage two operating systems

Use **your choice** of world-class Windows management & deployment tools for device config and updates

- Remote Desktop
- Remote PowerShell
- Image building and Reflash
- Endpoint Manager
- Azure Arc-enabled servers
- Ecosystem of MDMs & Tooling

VM Policies
VM config and A/B VM Update packages including Mariner OS + Kubernetes patches

OS Polices
OS Configurations, Updates, and Certificates

Use Azure to manage all your Containers and Kubernetes configs across cloud and on-prem with Arc-enabled Kubernetes

AKS Edge Essentials

Mariner VM
Built from EFLOW Base

- K8s/K3s Linux Worker
- K8s/K3s Control Plane
- Mariner User
- Azure containers
  - Flux & other Azure agents
  - Arc-Connected Cluster
- User containers
  - Any Linux
  - Any Linux
  - Any Linux
- Mariner kernel

Windows VM (Optional)

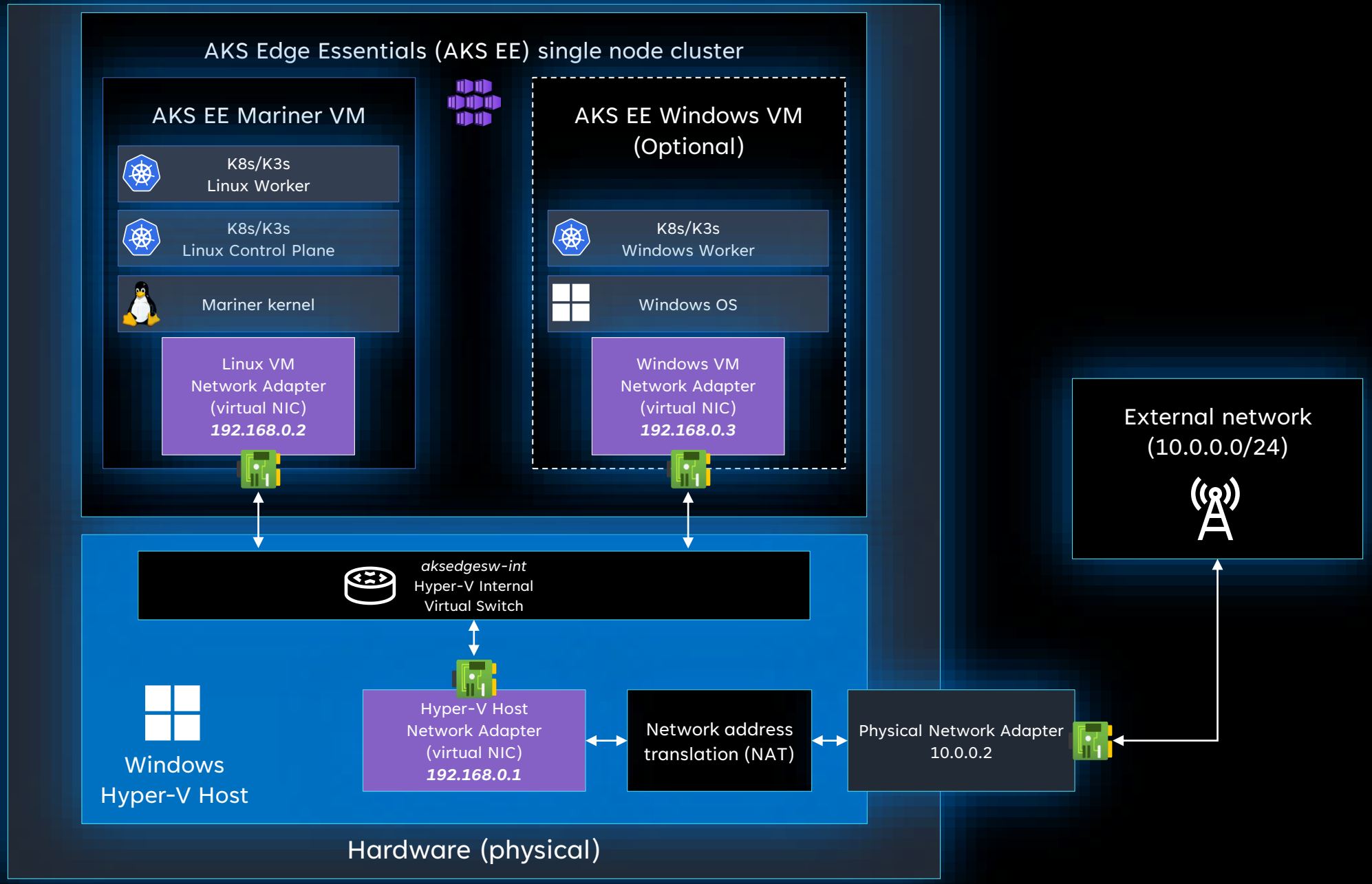
- K8s/K3s Windows Worker
- User containers
  - Windows container
  - Windows container
  - Windows container
- Windows

Windows Host OS (with Hyper-V) as “Type-1” Hypervisor

Hardware

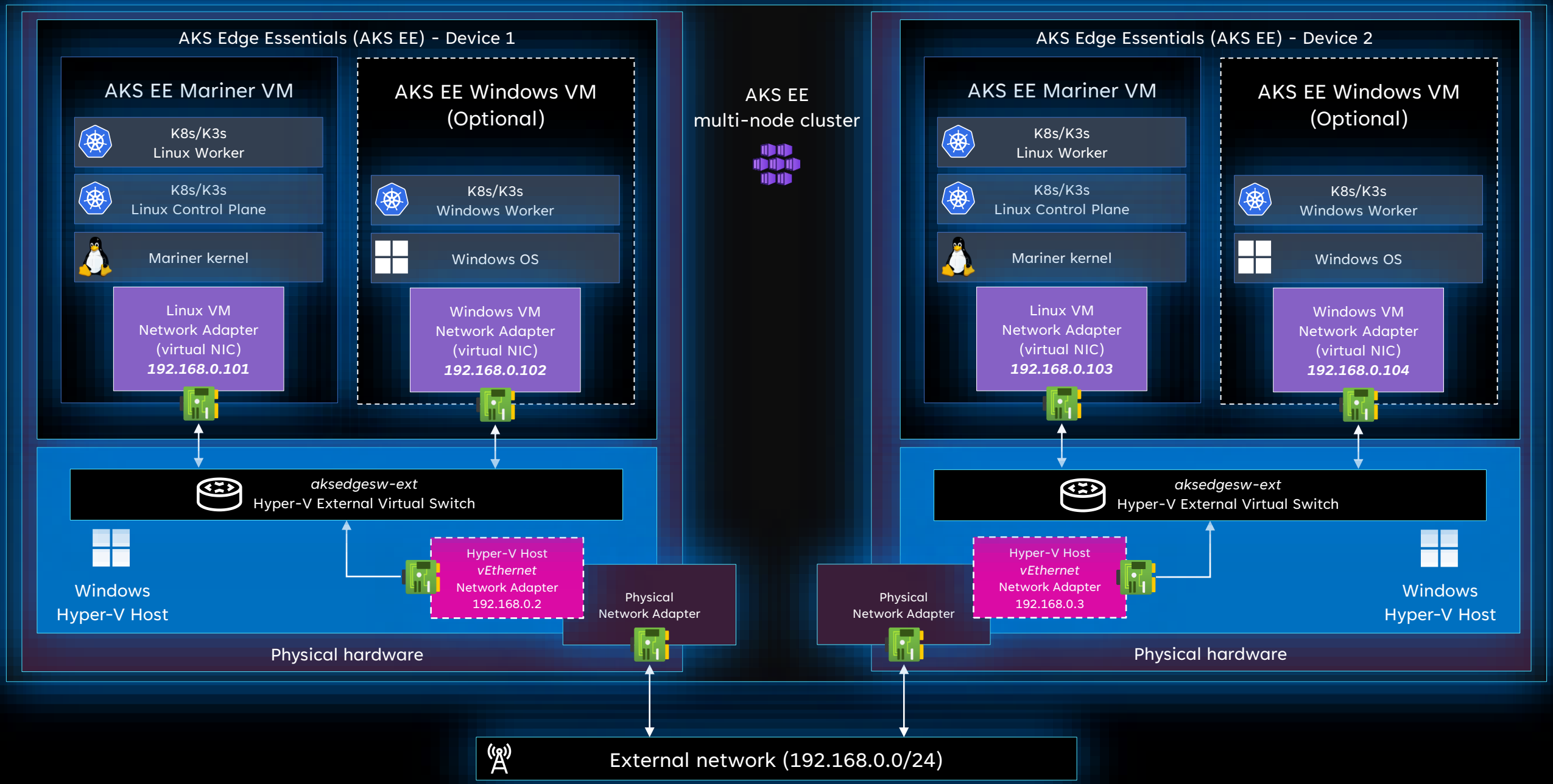
Azure Kubernetes Service Edge Essentials (AKS EE)

Single Node Cluster with Internal Virtual Switch network architecture



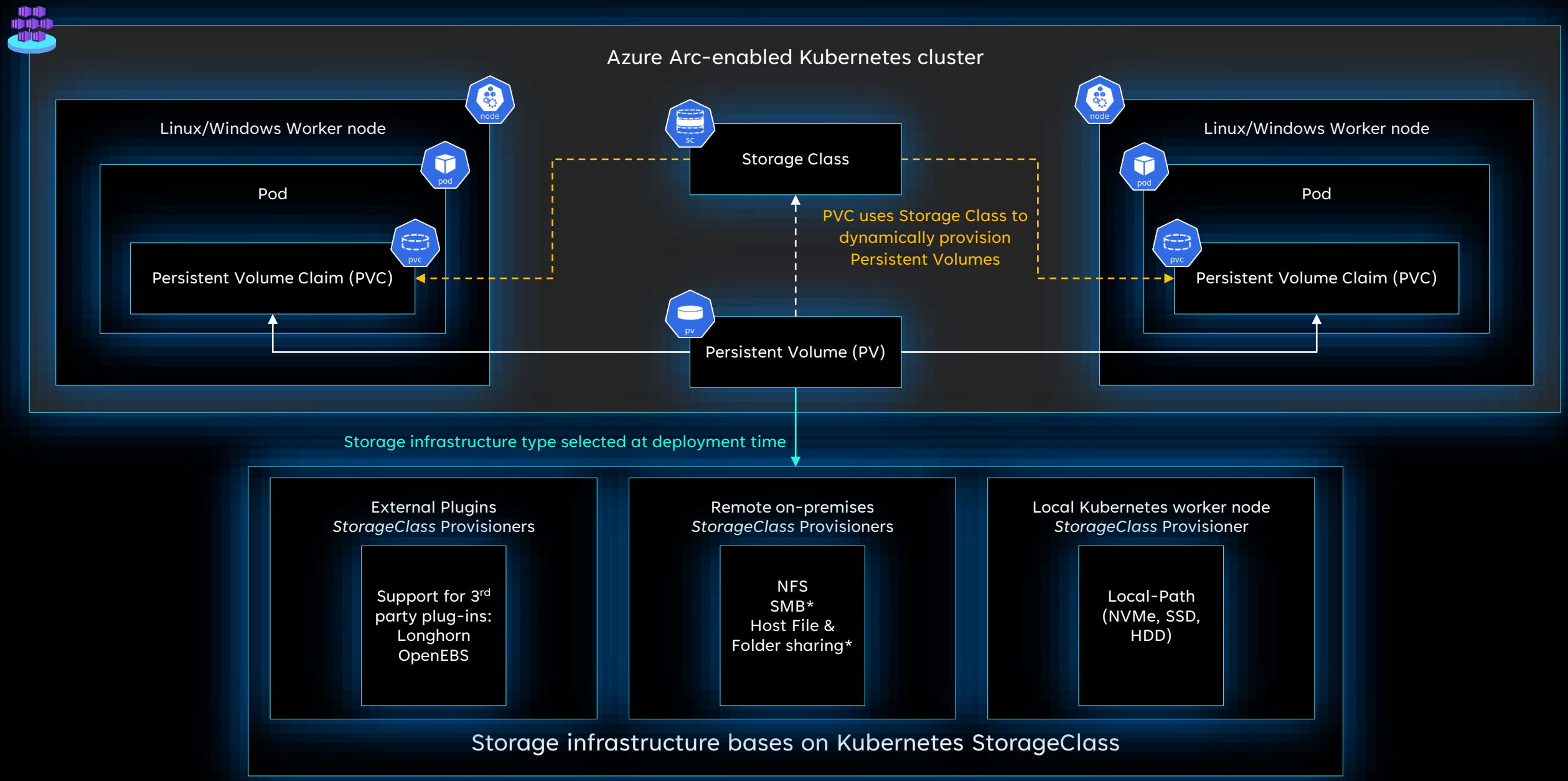
Azure Kubernetes Service Edge Essentials (AKS EE)

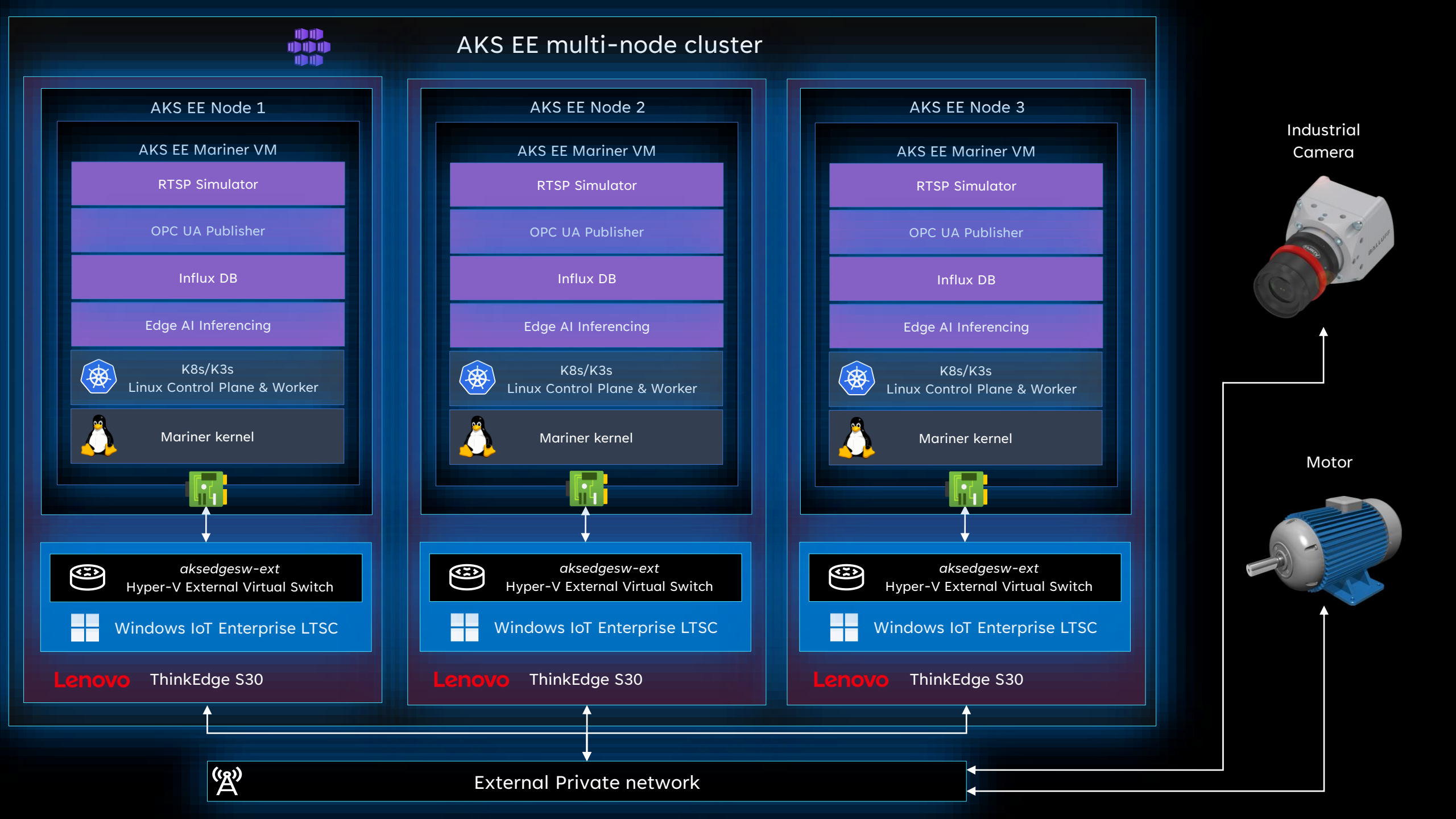
Multi-Machine Cluster with External Virtual Switch network architecture



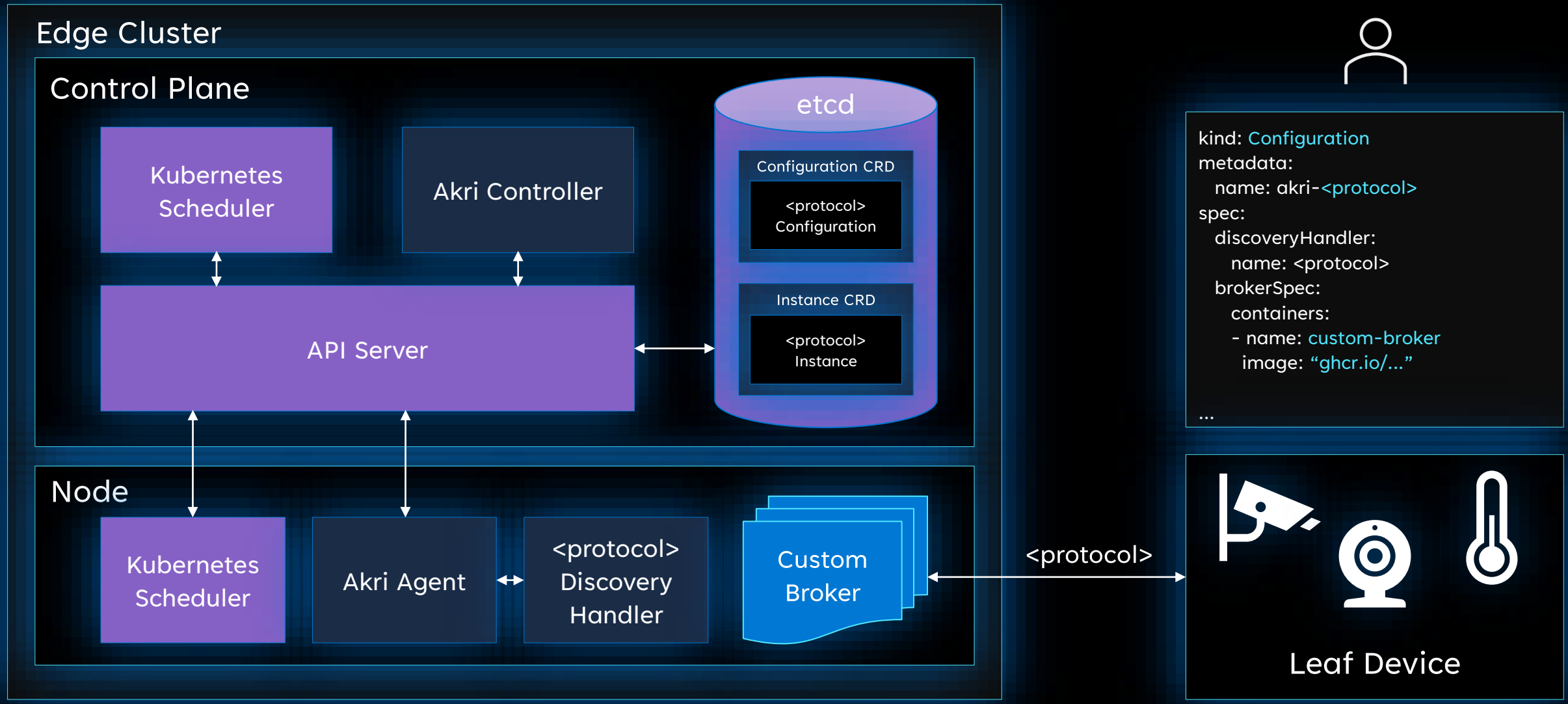
Azure Kubernetes Service Edge Essentials (AKS EE)

Storage options




AKS EE multi-node cluster
AKS EE Node 1
AKS EE Mariner VM
RTSP Simulator
OPC UA Publisher
Influx DB
Edge AI Inferencing
K8s/K3s
Linux Control Plane & Worker
Mariner kernel
aksedgesw-ext
Hyper-V External Virtual Switch
Windows IoT Enterprise LTSC
Lenovo ThinkEdge S30
AKS EE Node 2
AKS EE Mariner VM
RTSP Simulator
OPC UA Publisher
Influx DB
Edge AI Inferencing
K8s/K3s
Linux Control Plane & Worker
Mariner kernel
aksedgesw-ext
Hyper-V External Virtual Switch
Windows IoT Enterprise LTSC
Lenovo ThinkEdge S30
AKS EE Node 3
AKS EE Mariner VM
RTSP Simulator
OPC UA Publisher
Influx DB
Edge AI Inferencing
K8s/K3s
Linux Control Plane & Worker
Mariner kernel
aksedgesw-ext
Hyper-V External Virtual Switch
Windows IoT Enterprise LTSC
Lenovo ThinkEdge S30
External Private network
Industrial Camera
Motor

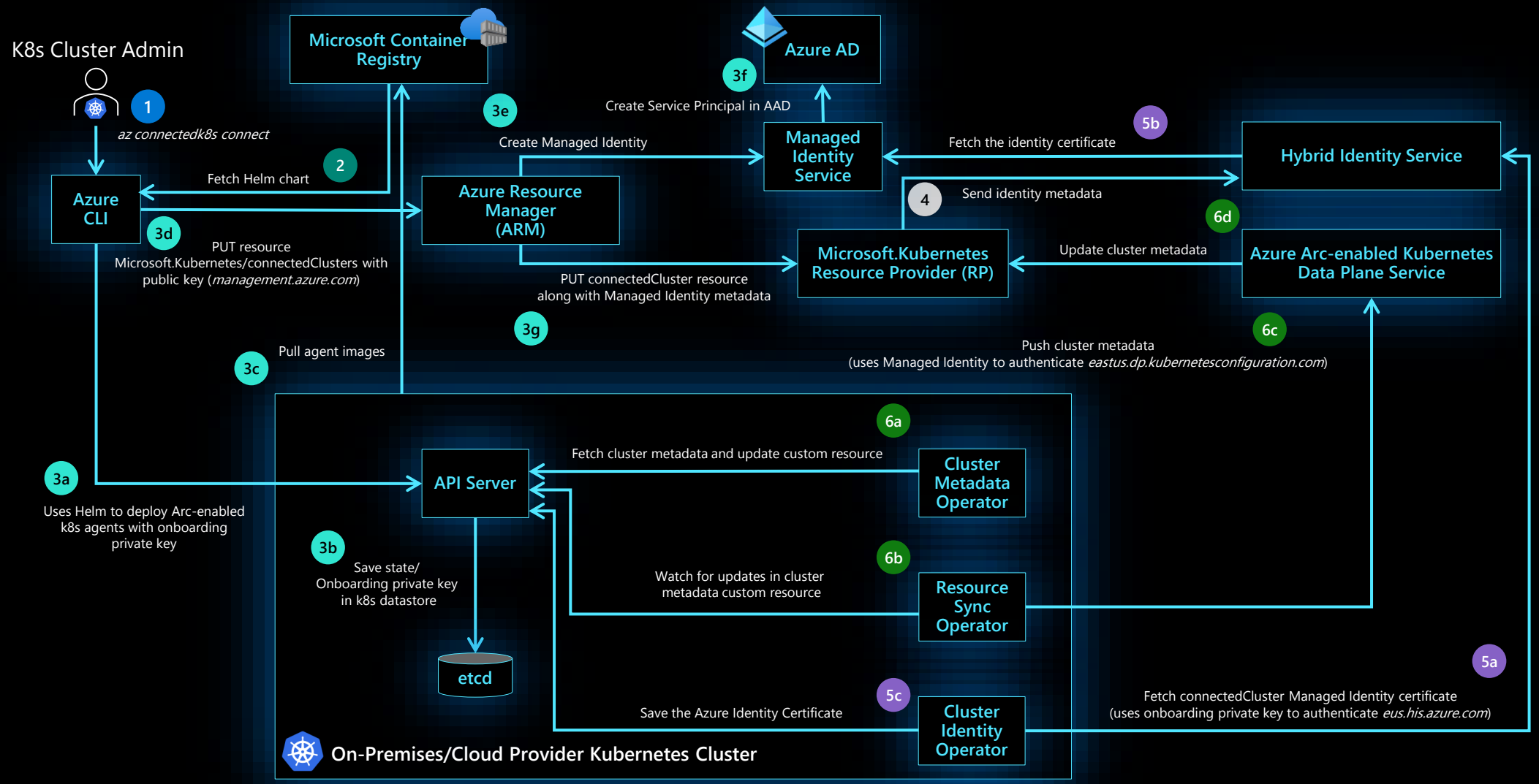
Akri Architecture



Azure Arc-enabled Kubernetes

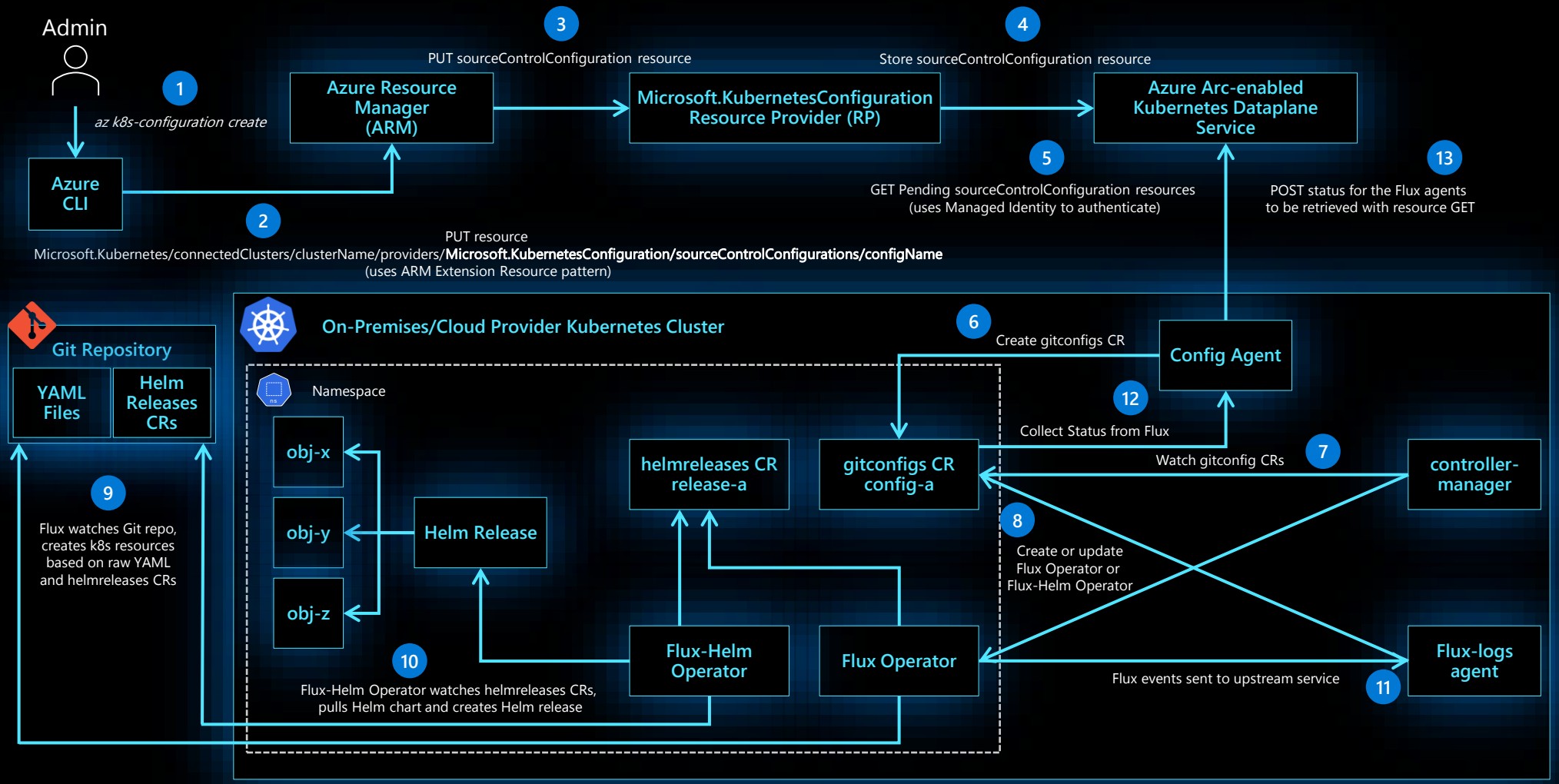
Azure Arc-enabled Kubernetes

Onboarding



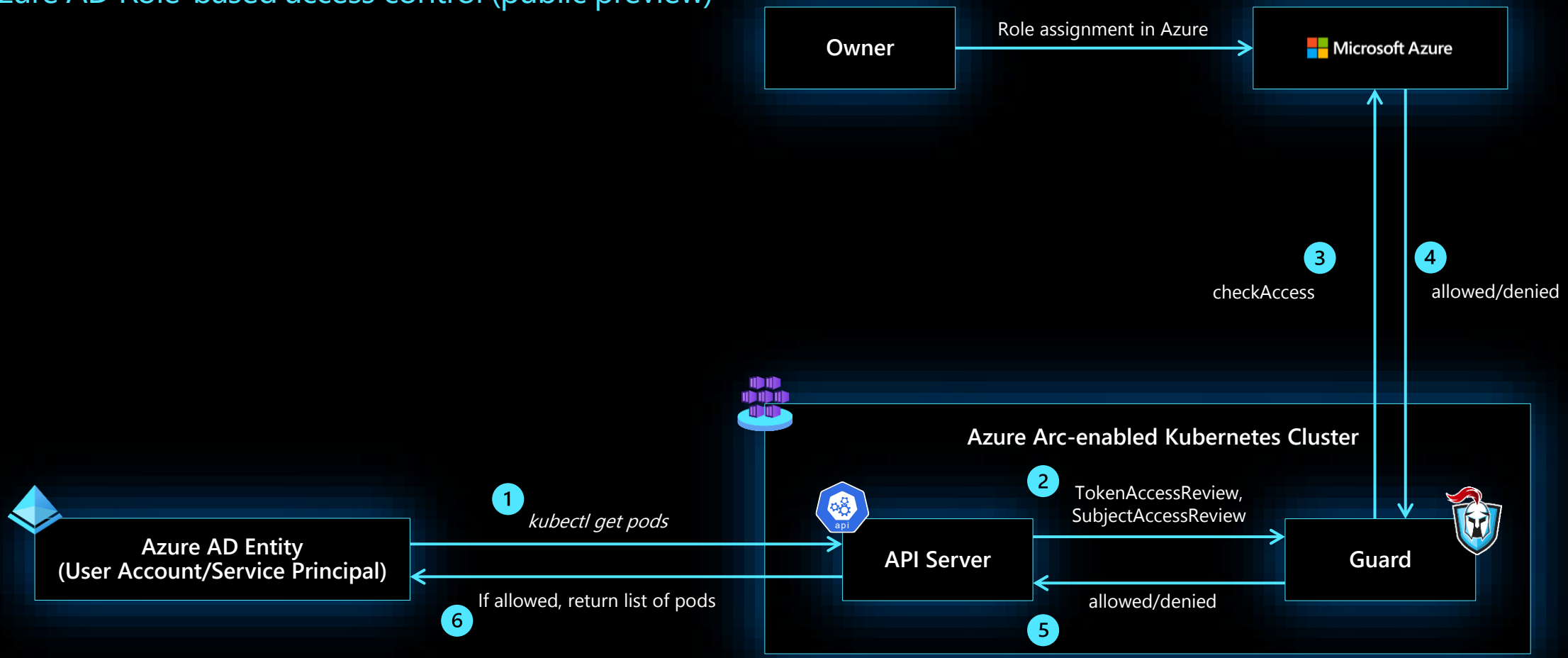
Azure Arc-enabled Kubernetes

GitOps Configuration



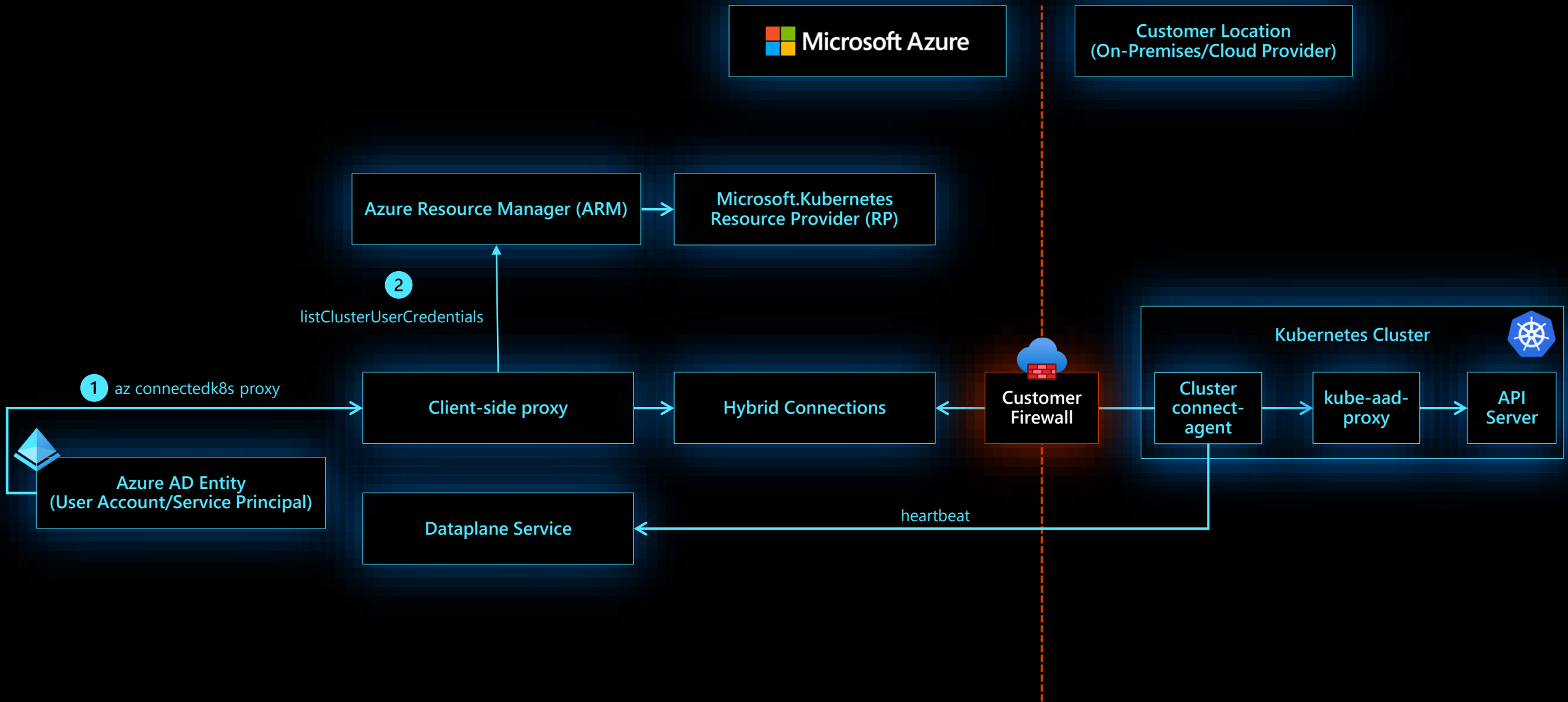
Azure Arc-enabled Kubernetes

Azure AD Role-based access control (public preview)



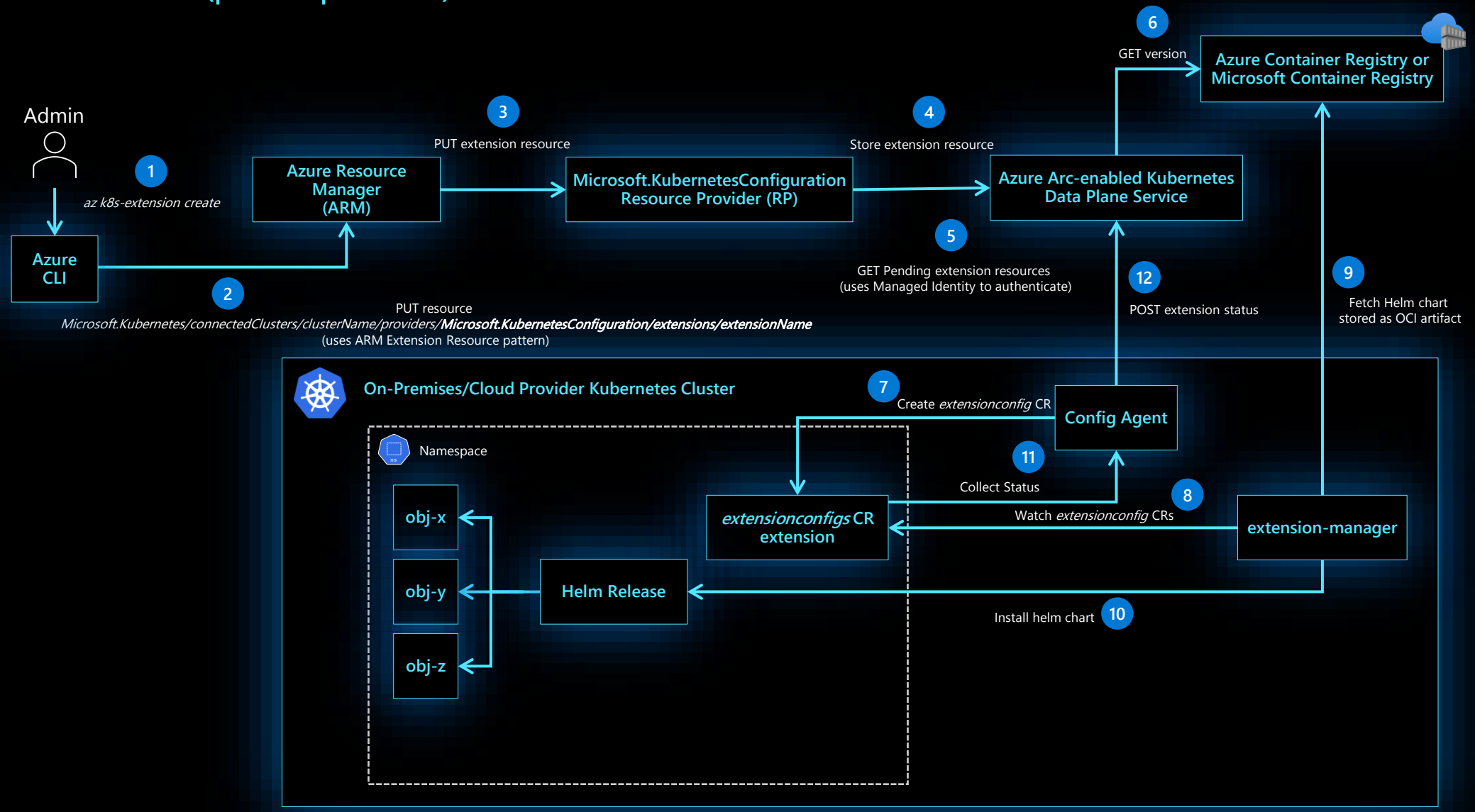
Azure Arc-enabled Kubernetes

Cluster Connect (public preview)



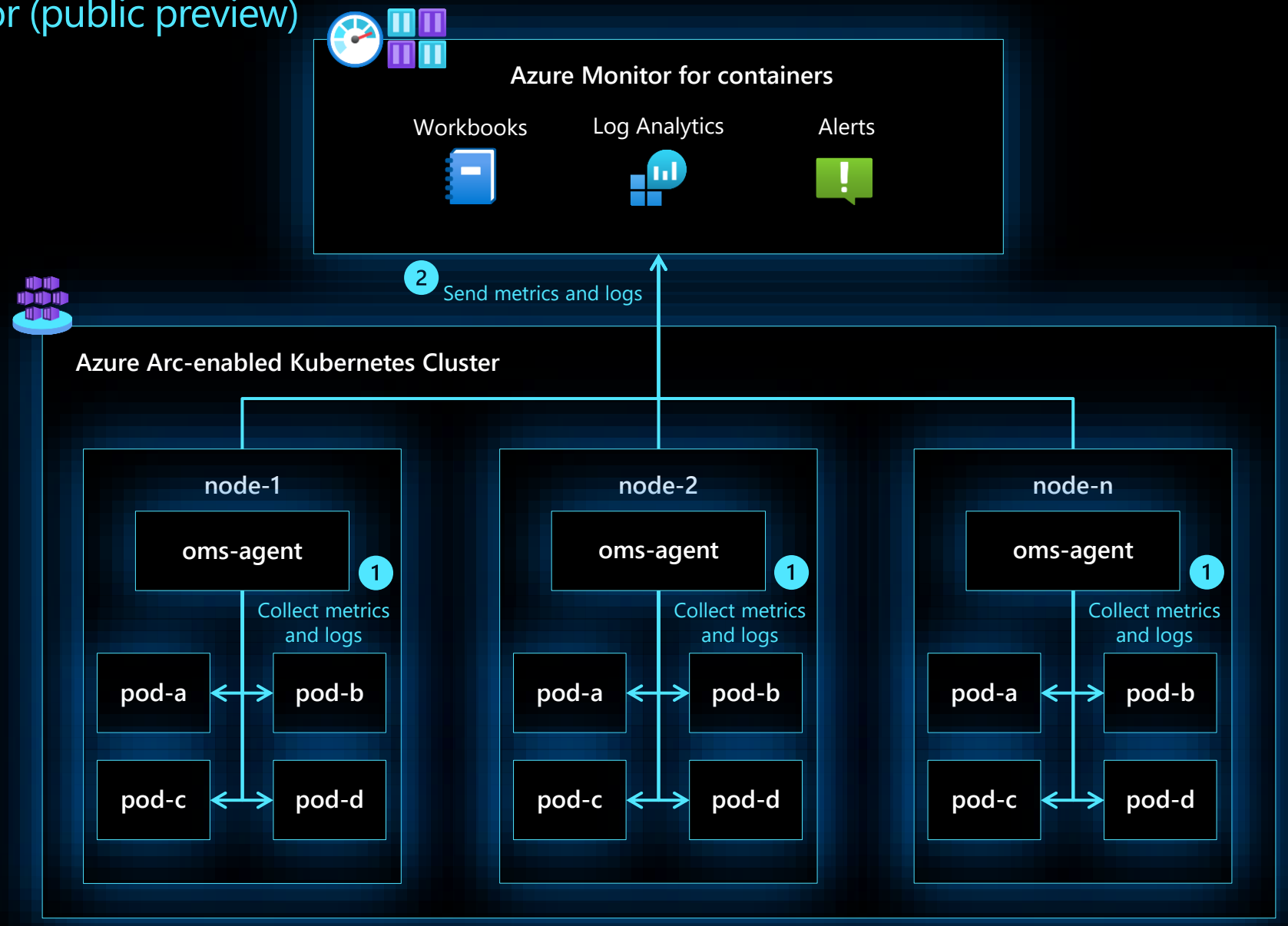
Azure Arc-enabled Kubernetes

Cluster extensions (public preview)



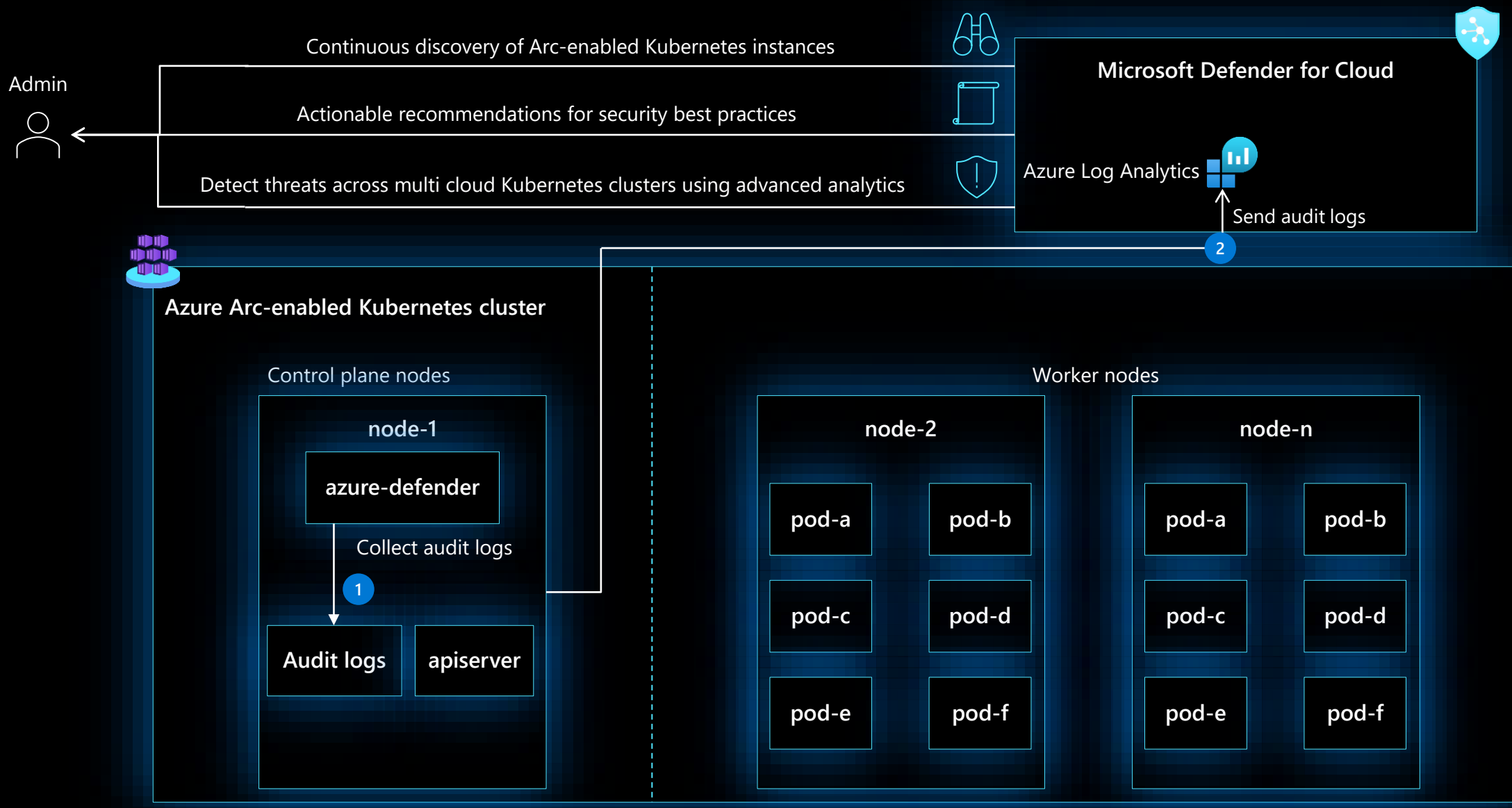
Azure Arc-enabled Kubernetes

Azure Monitor (public preview)



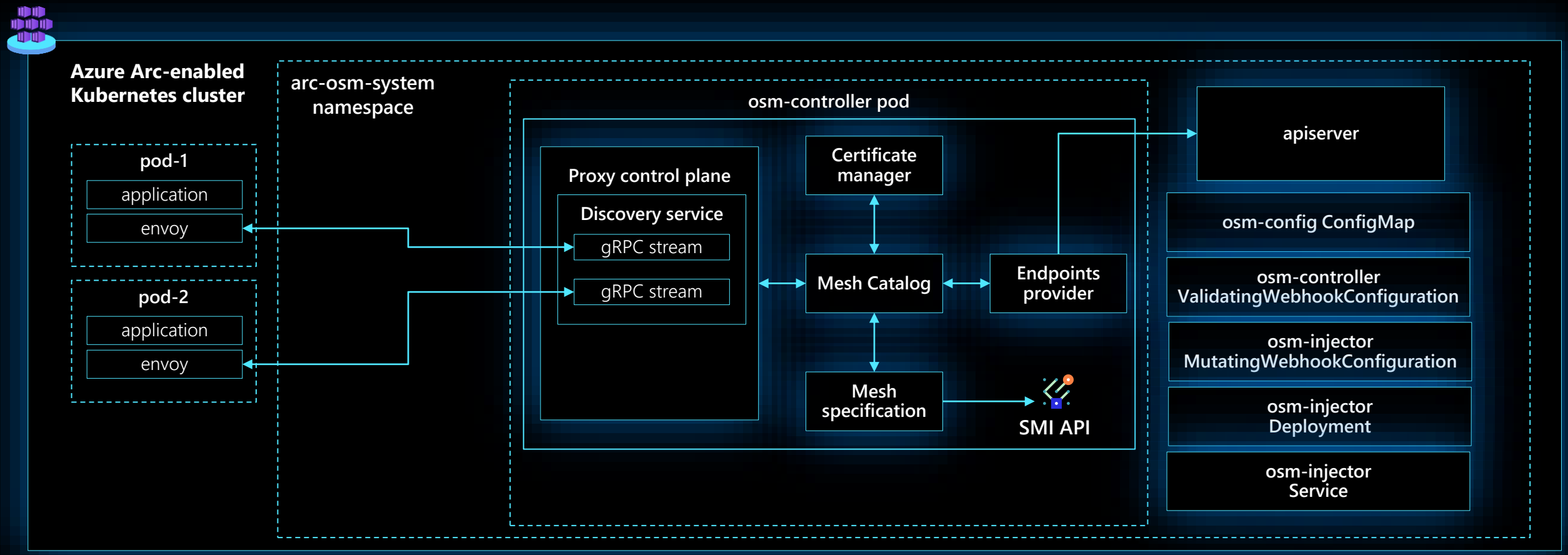
Azure Arc-enabled Kubernetes

Microsoft Defender for Cloud



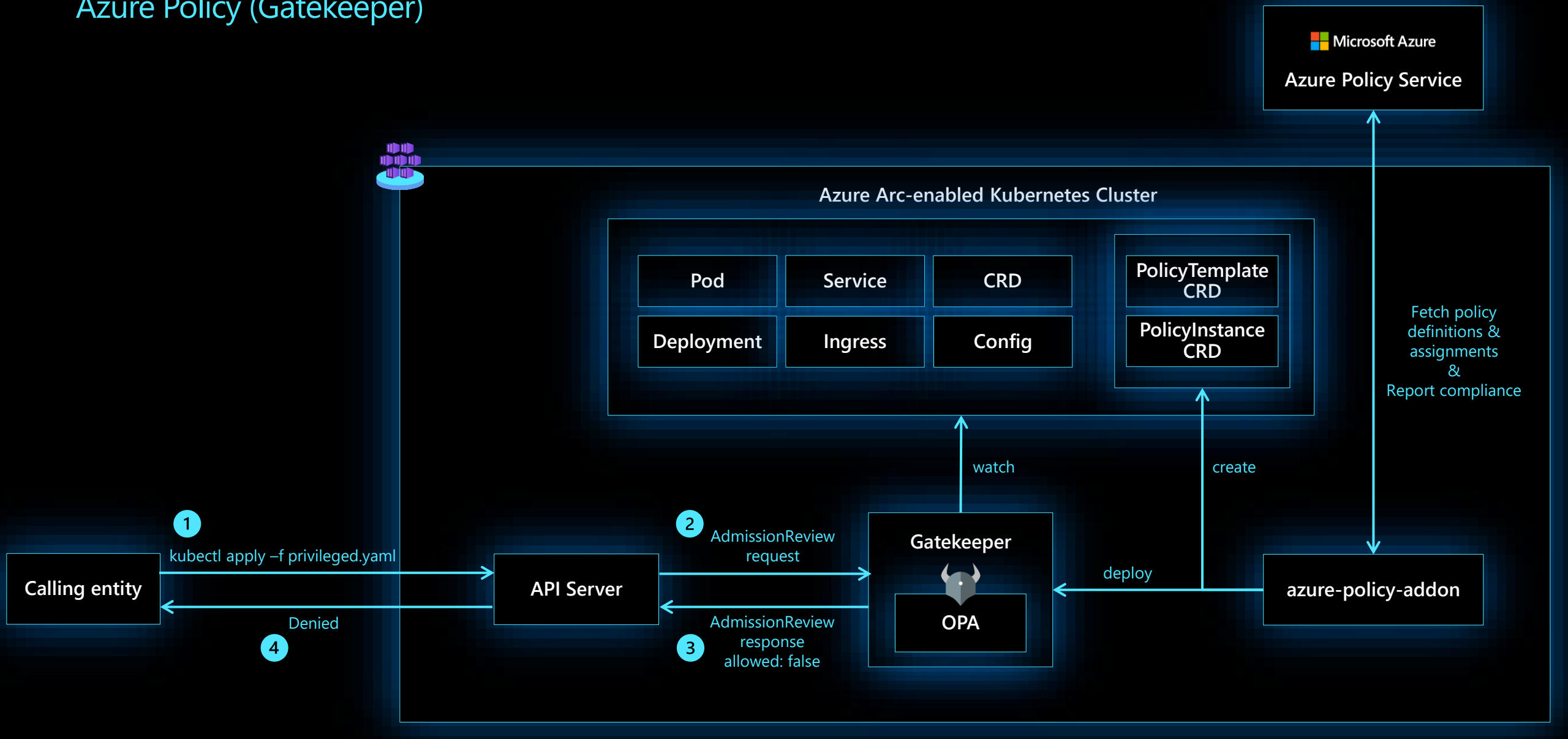
Azure Arc-enabled Kubernetes

Open Service Mesh (Preview)



Azure Arc-enabled Kubernetes

Azure Policy (Gatekeeper)



Infrastructure as Code with Azure Arc

Customer environments and application requirements are evolving

Single control plane with Azure Arc

How to govern and operate across disparate environments?

How to ensure security across the entire organization?

How to best enable innovation and developer agility?

How to meet regulatory requirements and overcome technical hurdles?

100's–1,000's of apps

- VMs
- Databases
- Containers
- Serverless

.NET, JS, Python, Java, GO, php

Diverse infrastructure

- Datacenters
- Hosters
- Branch offices
- OEM hardware
- IoT devices
- Edge

Hybrid & Multi-Cloud

Microsoft Azure

aws

Google Cloud

Alibaba Cloud

vmware

ORACLE

IBM Cloud

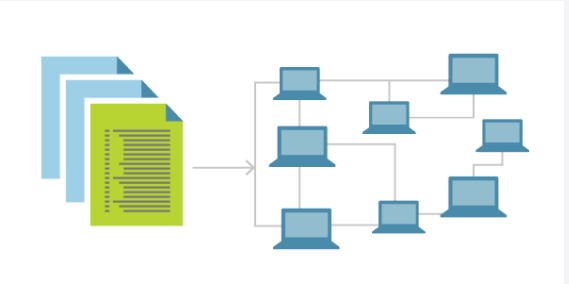
Introduction to Infrastructure as Code concepts

Infrastructure as code (IaC) uses **DevOps** methodology and versioning with a descriptive model to define and deploy infrastructure, such as networks, virtual machines, load balancers, and connection topologies. Just as the same source code always generates the same binary, an IaC model generates the same environment every time it deploys.

IaC is a key DevOps practice and a component of ***continuous delivery***. With IaC, DevOps teams can work together with a unified set of practices and tools to deliver applications and their supporting infrastructure rapidly and reliably at scale.

Infrastructure as Code (IaC) is a key DevOps practice that involves the management of infrastructure, such as networks, compute services, databases, storages, and connection topology, in a descriptive model. IaC allows teams to develop and release changes faster and with greater confidence.
Benefits of IaC include:

- Increased confidence in deployments
- Ability to manage multiple environments
- Improved understanding of the state of infrastructure



Avoid manual configuration to enforce consistency

IaC evolved to solve the problem of *environment drift* in release pipelines. Without IaC, teams must maintain deployment environment settings individually. Over time, each environment becomes a "snowflake," a unique configuration that can't be reproduced automatically. Inconsistency among environments can cause deployment issues. Infrastructure administration and maintenance involve manual processes that are error prone and hard to track.

IaC avoids manual configuration and enforces consistency by representing desired environment states via well-documented code in formats such as JSON. Infrastructure deployments with IaC are repeatable and prevent runtime issues caused by configuration drift or missing dependencies. Release pipelines execute the environment descriptions and version configuration models to configure target environments. To make changes, the team edits the source, not the target.

Deliver stable test environments rapidly at scale

IaC helps DevOps teams test applications in production-like environments early in the development cycle. Teams can provision multiple test environments reliably on demand. The cloud dynamically provisions and tears down environments based on IaC definitions. The infrastructure code itself can be validated and tested to prevent common deployment issues.

Use declarative definition files

IaC should use declarative definition files if possible. A definition file describes the components and configuration that an environment requires, but not necessarily how to achieve that configuration. For example, the file might define a required server version and configuration, but not specify the server installation and configuration process.

This abstraction allows for greater flexibility to use optimized techniques the infrastructure provider supplies. Declarative definitions also help reduce the technical debt of maintaining imperative code, such as deployment scripts, that can accrue over time.

Using Azure Arc for deploying and managing resources through code

There are two approaches you can take when implementing Infrastructure as Code:

- **Imperative Infrastructure as Code** involves writing scripts in languages like Bash or PowerShell. You explicitly state commands that are executed to produce a desired outcome. When you use imperative deployments, it's up to you to manage the sequence of dependencies, error control, and resource updates.

- **Declarative Infrastructure as Code** involves writing a definition that defines how you want your environment to look. In this definition, you specify a desired outcome rather than how you want it to be accomplished. The tooling figures out how to make the outcome happen by inspecting your current state, comparing it to your target state, and then applying the differences.

ARM Templates

ARM stands for Azure Resource Manager. It's an API provisioning engine that is built into Azure and exposed as an API service. ARM enables you to deploy, update, delete, and manage the resources contained in Azure resource group in a single, coordinated operation.

You provide the engine with a JSON-based template that specifies the resources you require and their configuration. ARM automatically orchestrates the deployment in the correct order respecting dependencies.

The engine ensures idempotency. If a desired resource already exists with the same configuration, provisioning will be ignored.

```
"resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "[variables('storageAccountName')]",
      "location": "[parameters('location')]",
      "apiVersion": "2018-07-01",
      "sku": {
        "name": "[parameters('storageAccountType')]"
      },
      "kind": "StorageV2",
      "properties": {}
    }
  ],
```

Bicep

Bicep is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources.

In Bicep files, you define the infrastructure you intend to deploy and its properties.

Compared to ARM templates, Bicep files are easier to read and write for a non-developer audience because they use a concise syntax

```
param location string = resourceGroup().location
param storageAccountName string =
'toylaunch${uniqueString(resourceGroup().id)}'
resource storageAccount
'Microsoft.Storage/storageAccounts@2021-06-01' = {
  name: storageAccountName
  location: location
  sku: {
    name: 'Standard_LRS'
  }
  kind: 'StorageV2'
  properties: {
    accessTier: 'Hot'
  }
}
```

Terraform

Cloud-native applications are often constructed to be cloud agnostic. Being so means the application isn't tightly coupled to a particular cloud vendor and can be deployed to any public cloud.

Terraform is a commercial templating tool that can provision cloud-native applications across all the major cloud players: Azure, Google Cloud Platform, AWS, and AliCloud. Instead of using JSON as the template definition language, it uses the slightly more terse HCL (Hashicorp Configuration Language).

```
provider "azurerm" {
  version = "=1.28.0"
}

resource "azurerm_resource_group" "testrg" {
  name     = "production"
  location = "West US"
}

resource "azurerm_storage_account" "testsa" {
  name                     =
"${var.storageAccountName}"
  resource_group_name      =
"${azurerm_resource_group.testrg.name}"
  location                 = "${var.region}"
  account_tier             = "${var.tier}"
  account_replication_type =
"${var.replicationType}"

}
```

Azure CLI

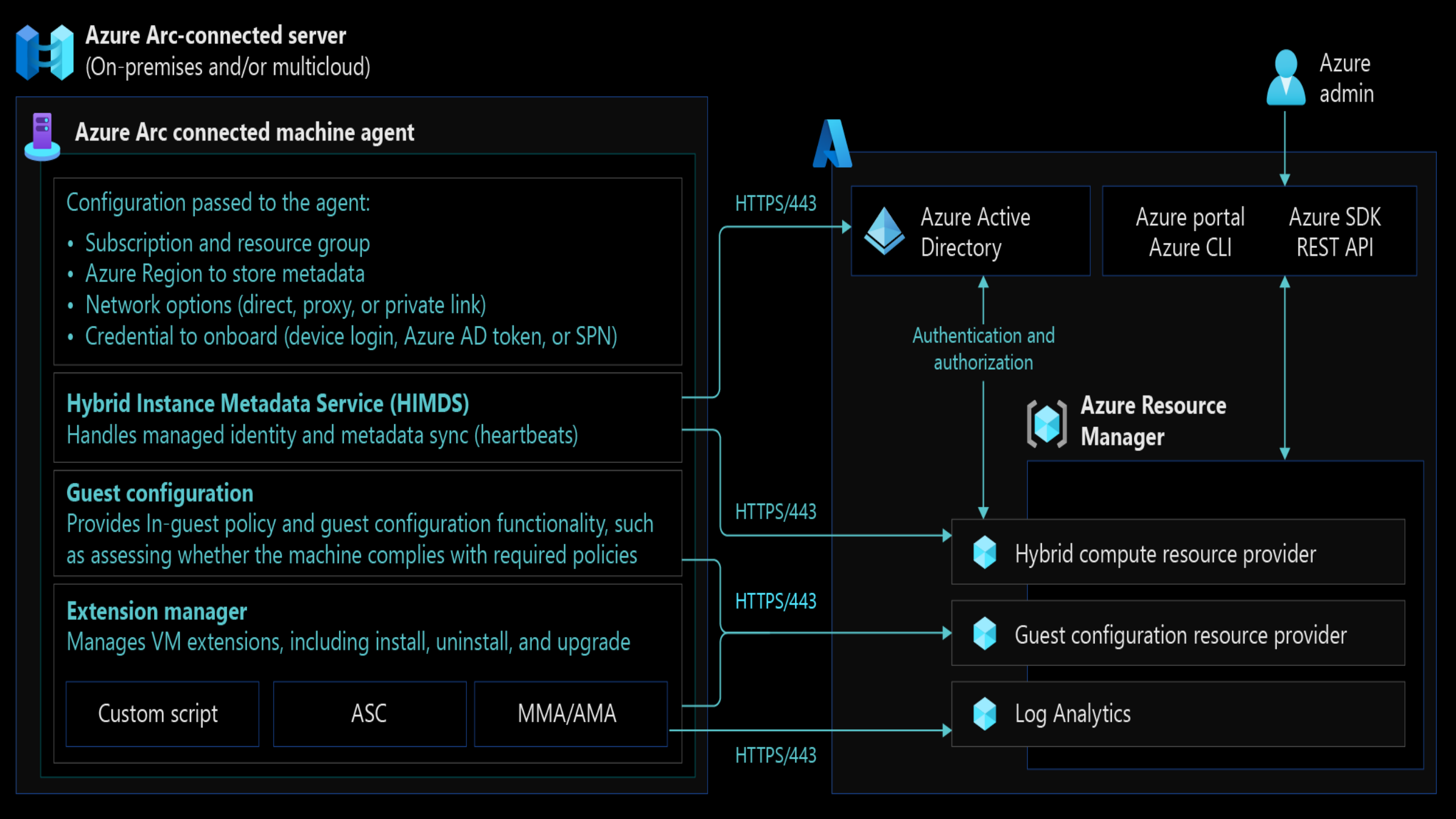
Finally, you can leverage Azure CLI to declaratively script your cloud infrastructure. Azure CLI scripts can be created, found, and shared to provision and configure almost any Azure resource.

The CLI is simple to use with a gentle learning curve. Scripts are executed within either PowerShell or Bash. They're also straightforward to debug, especially when compared with ARM templates.

```
- task: AzureCLI@2
  displayName: Azure CLI
  inputs:
    azureSubscription: <Name of the Azure Resource
Manager service connection>
    scriptType: ps
    scriptLocation: inlineScript
    inlineScript: |
      az --version
      az account show
```

Monitoring & Analytics

Azure Arc // Management Discipline


Azure Arc-connected server
(On-premises and/or multicloud)
Azure Arc connected machine agent
Configuration passed to the agent:
• Subscription and resource group
• Azure Region to store metadata
• Network options (direct, proxy, or private link)
• Credential to onboard (device login, Azure AD token, or SPN)
Hybrid Instance Metadata Service (HIMDS)
Handles managed identity and metadata sync (heartbeats)
Guest configuration
Provides In-guest policy and guest configuration functionality, such as assessing whether the machine complies with required policies
Extension manager
Manages VM extensions, including install, uninstall, and upgrade
Custom script
ASC
MMA/AMA
HTTPS/443
HTTPS/443
HTTPS/443
HTTPS/443
Azure admin
Azure Active Directory
Azure portal
Azure CLI
Azure SDK
REST API
Authentication and authorization
Azure Resource Manager
Hybrid compute resource provider
Guest configuration resource provider
Log Analytics

Azure Arc | Management Discipline // considerations

•**Azure Monitor requirements:** Azure Monitor can collect data directly from your Azure Arc-enabled servers into a Log Analytics workspace for detailed analysis and correlation. This will involve installing monitoring agents like the Log Analytics and dependency agents.

•**Azure Monitor agents deployment:** Review the deployment options for the Azure Monitor agents.

•**Azure Monitor configuration:** Plan your Azure Arc-enabled servers monitoring requirements, including metrics and log collection.
•**Azure connected machine agent management:** The Azure connected machine agent plays a critical role in your hybrid operations. It enables you to manage your Windows and Linux machines hosted outside of Azure, and enforce governance policies. It's important to implement solutions that keep track of unresponsive agents, monitor for new versions, and automate the deployment of upgrades.
•**Update Management for your hybrid resources:** Updates should be automated and installed in a timely manner, to make sure your Azure Arc-enabled servers have the latest operating system and security updates.

Azure Arc | Management Discipline // recommendations 1

Azure Monitor requirements

•Review and understand how the Log Analytics agent operates and collects data before deployment.
•Review the Network connectivity for Azure Arc-enabled servers section of this guide, for network-specific design considerations and recommendations.
•Before onboarding any machine to Azure Monitor, it's important to review the supported list of operating systems and the network requirements of the monitoring agents.

Azure Monitor agents deployment

•The Azure Monitor agents should be automatically deployed to Azure Arc-enabled Windows and Linux servers, through Azure Policy, as part of the enterprise-scale landing zone.
•Logs should be stored centrally on the Log Analytics workspace, a dedicated platform, and control log access with Azure role-based access control (RBAC). If there's a requirement for a separate workspace due to management, data sovereignty, or compliance requirements, using a separate workspace can affect the ability to have a single pane of glass and event correlation, on your Azure Arc-enabled servers across the environment.

Azure Arc | Management Discipline // recommendations 2

Azure Monitor requirements

•Review and understand how the Log Analytics agent operates and collects data before deployment.
•Review the Network connectivity for Azure Arc-enabled servers section of this guide, for network-specific design considerations and recommendations.
•Before onboarding any machine to Azure Monitor, it's important to review the supported list of operating systems and the network requirements of the monitoring agents.

Azure Monitor agents deployment

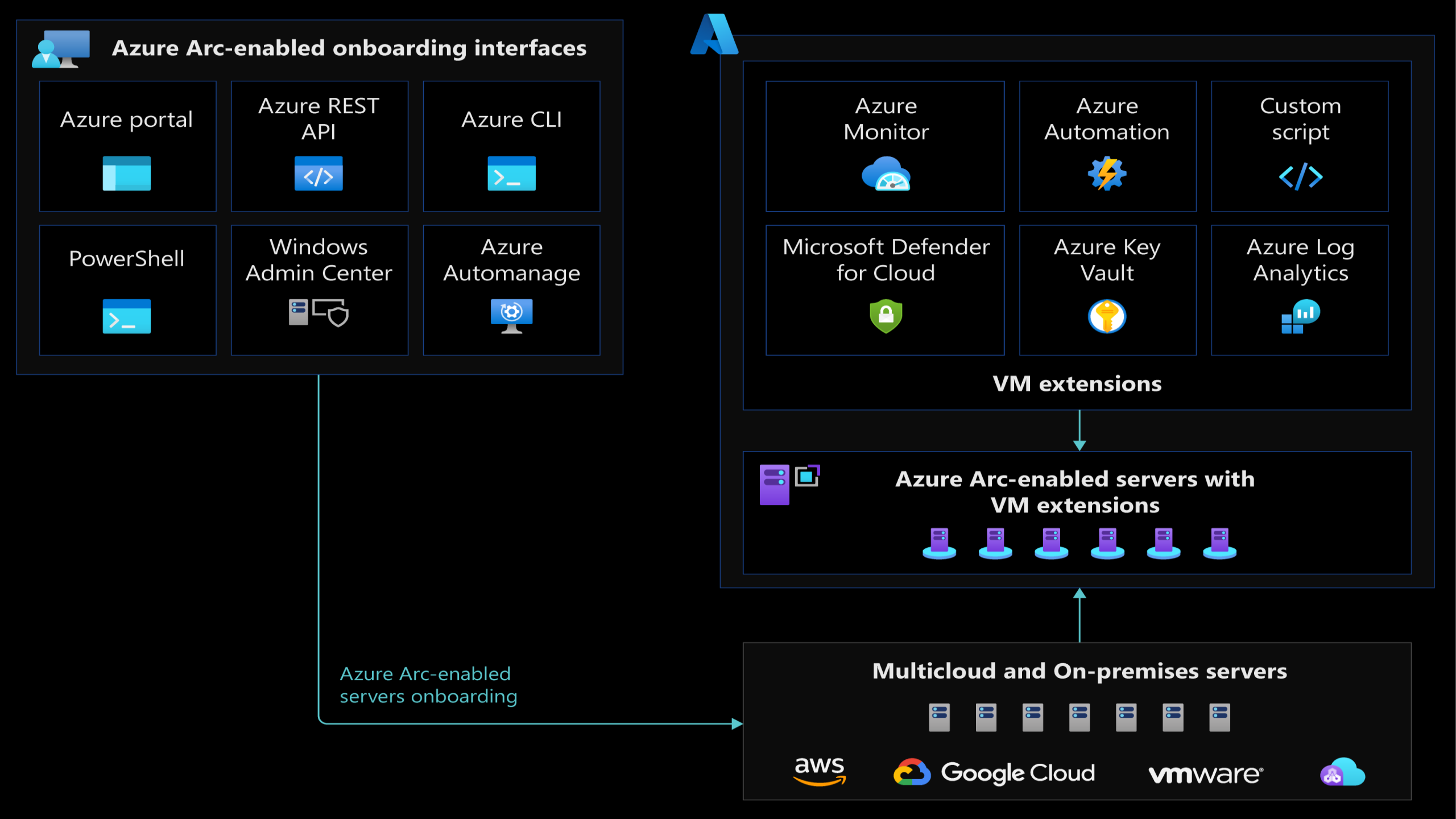
•The Azure Monitor agents should be automatically deployed to Azure Arc-enabled Windows and Linux servers, through Azure Policy, as part of the enterprise-scale landing zone.
•Logs should be stored centrally on the Log Analytics workspace, a dedicated platform, and control log access with Azure role-based access control (RBAC). If there's a requirement for a separate workspace due to management, data sovereignty, or compliance requirements, using a separate workspace can affect the ability to have a single pane of glass and event correlation, on your Azure Arc-enabled servers across the environment.

Azure Arc | Management Discipline // recommendations 3

Azure Monitor configuration

- ✓ Use **VM insights** to analyze the performance of your Azure Arc-enabled Windows and Linux servers. Monitor their processes and dependencies on other resources and external processes.
- ✓ Create **dashboards** or **Azure Monitor workbooks**, to track the relevant metrics and events across your Azure Arc-enabled servers. Samples of Log Analytics queries and VM insights can be found in this here.
- ✓ Configure the needed **performance counters** for the Azure Arc-enabled Windows and Linux servers, on the dedicated Log Analytics workspace.
- ✓ Configure the needed **logs** for the Azure Arc-enabled Windows and Linux servers, on the dedicated Log Analytics workspace.

Azure Arc // Automation Discipline


Azure Arc-enabled onboarding interfaces
Azure portal
Azure REST API
Azure CLI
PowerShell
Windows Admin Center
Azure Automanage
Azure Monitor
Azure Automation
Custom script
Microsoft Defender for Cloud
Azure Key Vault
Azure Log Analytics
VM extensions
Azure Arc-enabled servers with VM extensions
Azure Arc-enabled servers onboarding
Multicloud and On-premises servers
aws
Google Cloud
vmware

Azure Arc | Automation Discipline // considerations

Review requirements

- Your machines run a supported operating system for the Azure connected machine agent.
- Your machines have the required software installed before deploying the Azure connected machine agent.

Network connectivity

Your machines have connectivity from your on-premises network or each of the other third-party cloud providers to Azure - either directly connected, via a proxy server or private endpoint.

Check out the Network connectivity for Azure Arc-enabled servers section of Microsoft Learn guide for design considerations and recommendations.

Azure Arc | Automation Discipline // considerations

Environment preparation

- ✓ To deploy and configure the Azure Arc-enabled servers connected machine agent, an account with administrator or root privileges is required.
- ✓ To onboard machines, you have the required Azure permissions.
- ✓ See the Identity and access management for Azure Arc-enabled servers section of Microsoft Learn guide for more identity and access related content.

Onboard Azure Arc-enabled servers

- ✓ Before onboarding machines, you've registered the Azure resource providers for Azure Arc-enabled servers.
- ✓ Decide how you'll install and configure the Azure connected machine agent across your fleet of servers. Typically, you'll deploy the agent using your organization's standard automation tools.

Azure Arc | Automation Discipline // recommendations

Environment preparation

- ✓ Create a dedicated resource group to include only Azure Arc-enabled servers and centralize management and monitoring of these resources.
- ✓ Evaluate and develop an IT-aligned tagging strategy that can help reduce the complexity of managing your Azure Arc-enabled servers and simplifies the process of making management decisions.
- ✓ Create a service principal to connect machines non-interactively using Azure PowerShell or from the Azure portal.

Azure Arc | Automation Discipline // considerations

Onboard Azure Arc-enabled servers

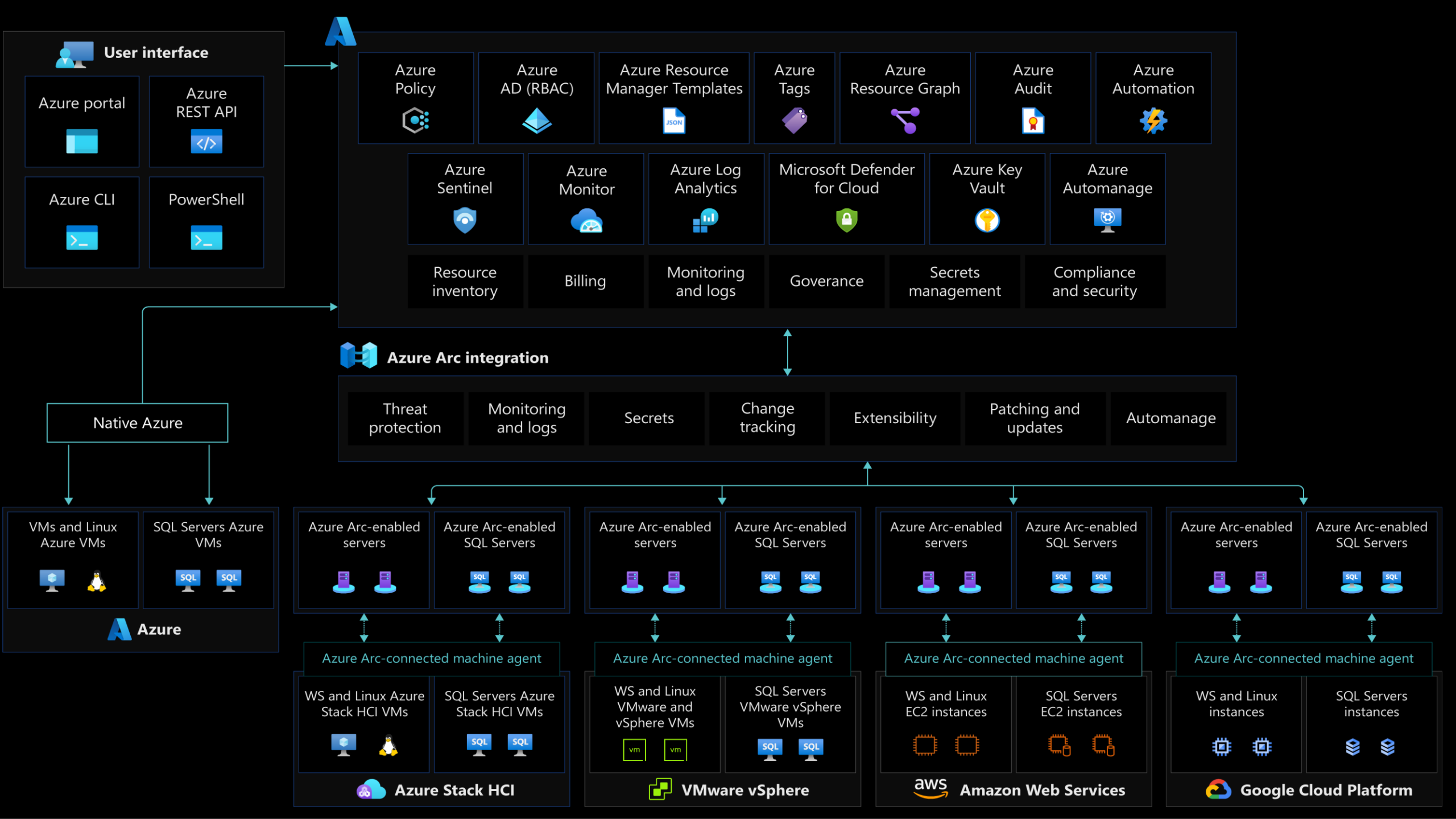
One of your first tasks will be to onboard your fleet of servers and virtual machines to Azure. After generating an installation script if you only have a few servers, you can opt to run the script directly from your Windows or Linux machines. For larger fleets of servers, there are several options available in Azure to automate the onboarding process.

We recommended creating a service principal and apply one of the following methods:

- Review and customize the predefined installation script for at-scale deployment of the connected machine agent to support your automated deployment requirements.
- Generate a PowerShell script using a service principal, and deploy via your organizations existing automation platform
  - Connect machines using automation Update Management
  - Connect machines using PowerShell remoting or PowerShell DSC
  - Connect machines from Windows Admin Center

Afterwards, be sure to verify your connection to Azure Arc.

Azure Arc // Security Discipline


User interface
Azure portal
Azure REST API
Azure CLI
PowerShell
Azure Policy
Azure AD (RBAC)
Azure Resource Manager Templates
Azure Tags
Azure Resource Graph
Azure Audit
Azure Automation
Azure Sentinel
Azure Monitor
Azure Log Analytics
Microsoft Defender for Cloud
Azure Key Vault
Azure Automanage
Resource inventory
Billing
Monitoring and logs
Goverance
Secrets management
Compliance and security
Azure Arc integration
Threat protection
Monitoring and logs
Secrets
Change tracking
Extensibility
Patching and updates
Automanage
Native Azure
VMs and Linux Azure VMs
SQL Servers Azure VMs
Azure
Azure Arc-enabled servers
Azure Arc-enabled SQL Servers
Azure Arc-connected machine agent
WS and Linux Azure Stack HCI VMs
SQL Servers Azure Stack HCI VMs
Azure Stack HCI
WS and Linux VMware and vSphere VMs
SQL Servers VMware vSphere VMs
VMware vSphere
WS and Linux EC2 instances
SQL Servers EC2 instances
Amazon Web Services
WS and Linux instances
SQL Servers instances
Google Cloud Platform

Azure Arc | Security Discipline // considerations

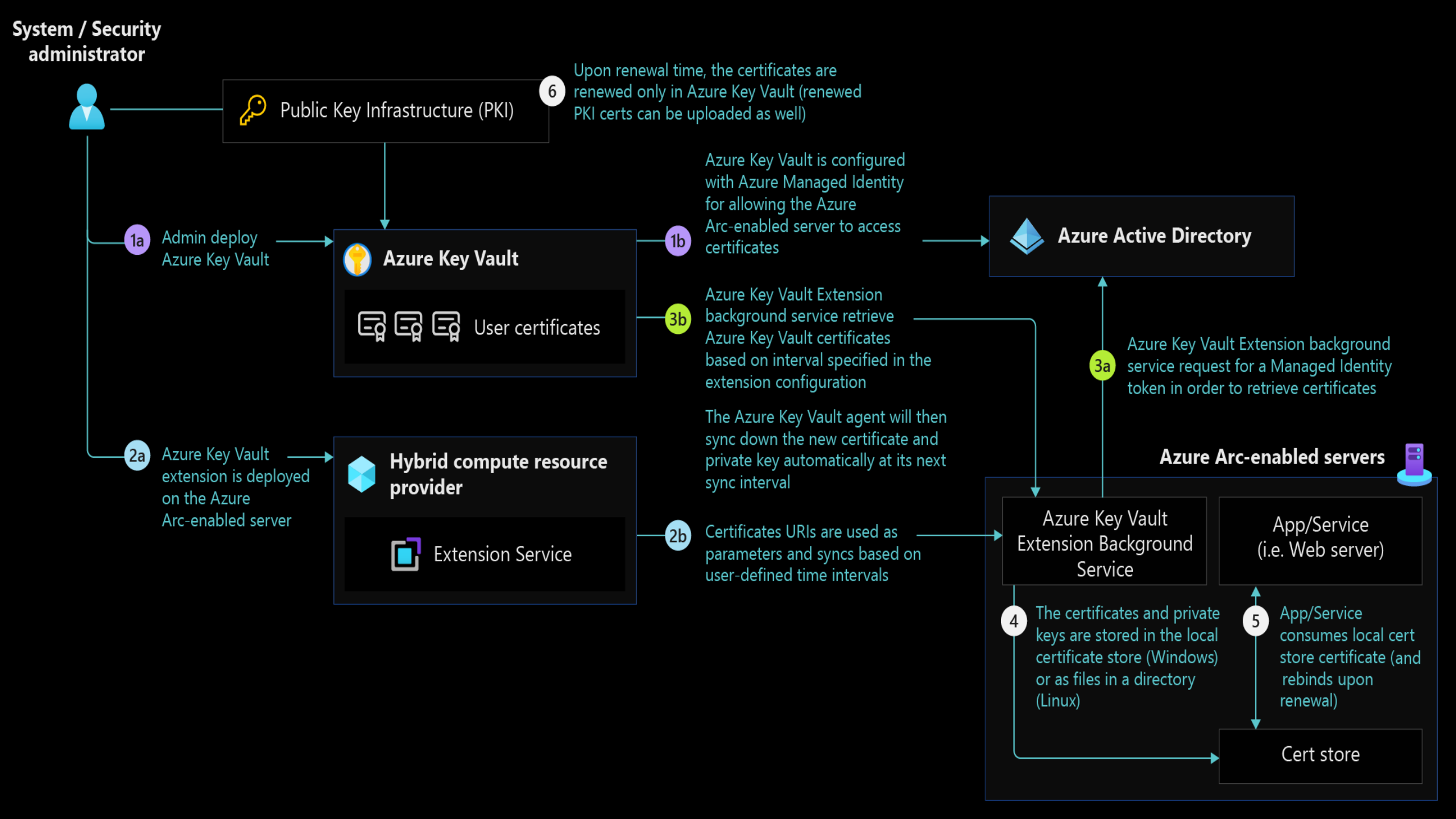
Identity and access management

•**Agent security permissions:** Secure access to the Azure connected machine agent by reviewing users with local administrator privileges on the server.

•**Managed identity:** Use managed identities with Azure Arc-enabled servers. Define a strategy for identifying which applications running on Azure Arc-enabled servers can use a Microsoft Entra token.

•**Azure role-based access control (RBAC):** Define administrative, operations, and engineering roles within the organization. This will help allocate day-to-day operations in the hybrid environment. Mapping each team to actions and responsibilities will determine Azure RBAC roles and configuration.

Consider using a RACI matrix, to support this effort and build controls into the management scope hierarchy you define, while following the resource consistency and inventory management guidance. For more information, review identity and access management for Azure Arc-enabled servers.


System / Security administrator
Public Key Infrastructure (PKI)
6
Upon renewal time, the certificates are renewed only in Azure Key Vault (renewed PKI certs can be uploaded as well)
1a
Admin deploy Azure Key Vault
Azure Key Vault
User certificates
1b
Azure Key Vault is configured with Azure Managed Identity for allowing the Azure Arc-enabled server to access certificates
Azure Active Directory
3b
Azure Key Vault Extension background service retrieve Azure Key Vault certificates based on interval specified in the extension configuration
The Azure Key Vault agent will then sync down the new certificate and private key automatically at its next sync interval
3a
Azure Key Vault Extension background service request for a Managed Identity token in order to retrieve certificates
2a
Azure Key Vault extension is deployed on the Azure Arc-enabled server
Hybrid compute resource provider
Extension Service
2b
Certificates URIs are used as parameters and syncs based on user-defined time intervals
Azure Arc-enabled servers
Azure Key Vault Extension Background Service
App/Service (i.e. Web server)
4
The certificates and private keys are stored in the local certificate store (Windows) or as files in a directory (Linux)
5
App/Service consumes local cert store certificate (and rebinds upon renewal)
Cert store

Azure Arc // Governance Discipline

Azure Arc | Governance Discipline // considerations

Governance disciplines

•**Threat protection and cloud security posture management:** Introduce controls to detect security misconfigurations and track compliance. Also, use Azure's intelligence to protect your hybrid workloads against threats. Enable Microsoft Defender for servers for all subscriptions containing Azure Arc-enabled servers for security baseline monitoring, security posture management, and threat protection.

•**Secret and certificate management:** Enable Azure Key Vault to protect service principal credentials. Consider using Azure Key Vault for certificate management on your Azure Arc-enabled servers.

•**Policy management and reporting:** Define a governance plan for your hybrid servers and machines that translates into Azure policies and remediation tasks.

Azure Arc | Governance Discipline // considerations

Governance disciplines

•**Data residency:** Consider which Azure region you wish your Azure Arc-enabled servers to be provisioned into, and understand the metadata that is collected from these machines.

•**Secure public key:** Secure the Azure connected machine agent public key authentication to communicate with the Azure service.

•**Business continuity and disaster recovery:** Review the business continuity and disaster recovery guidance for enterprise-scale landing zones to determine whether your enterprise requirements are met.

Review the security, governance, and compliance design area of Azure landing zone enterprise-scale, to assess the impact of Azure Arc-enabled servers on your overall security and governance model.

Secure your Azure Arc solutions with Microsoft Defender for Cloud

While the enterprise-scale landing zone documentation covers "Governance" and "Security" as separate topics, for Azure Arc-enabled servers, these critical design areas are consolidated as a single topic.

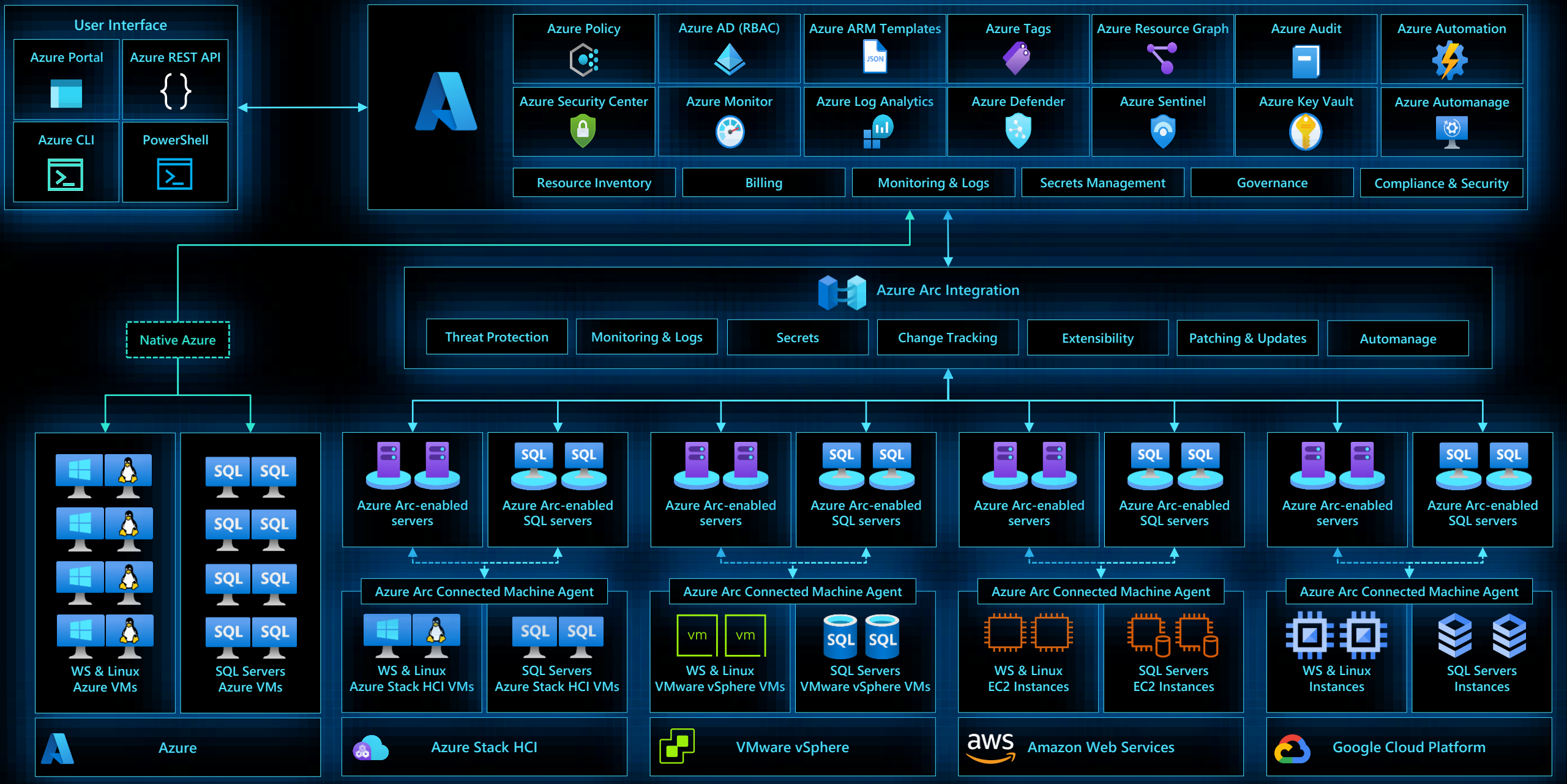
Defining and applying the proper control mechanisms is key in any cloud implementation, as it's the foundational element to stay secured and compliant. In a traditional environment, these mechanisms usually involve review processes and manual controls.

However, the cloud has introduced a new approach to IT governance with automated guardrails and checks. Azure Policy and Microsoft Defender for Cloud are cloud-native tools that allow the implementation of these controls, reports, and remediation tasks in an automated fashion.

By combining them with Azure Arc, you can extend your governance policies and security to any resource in public or private clouds.

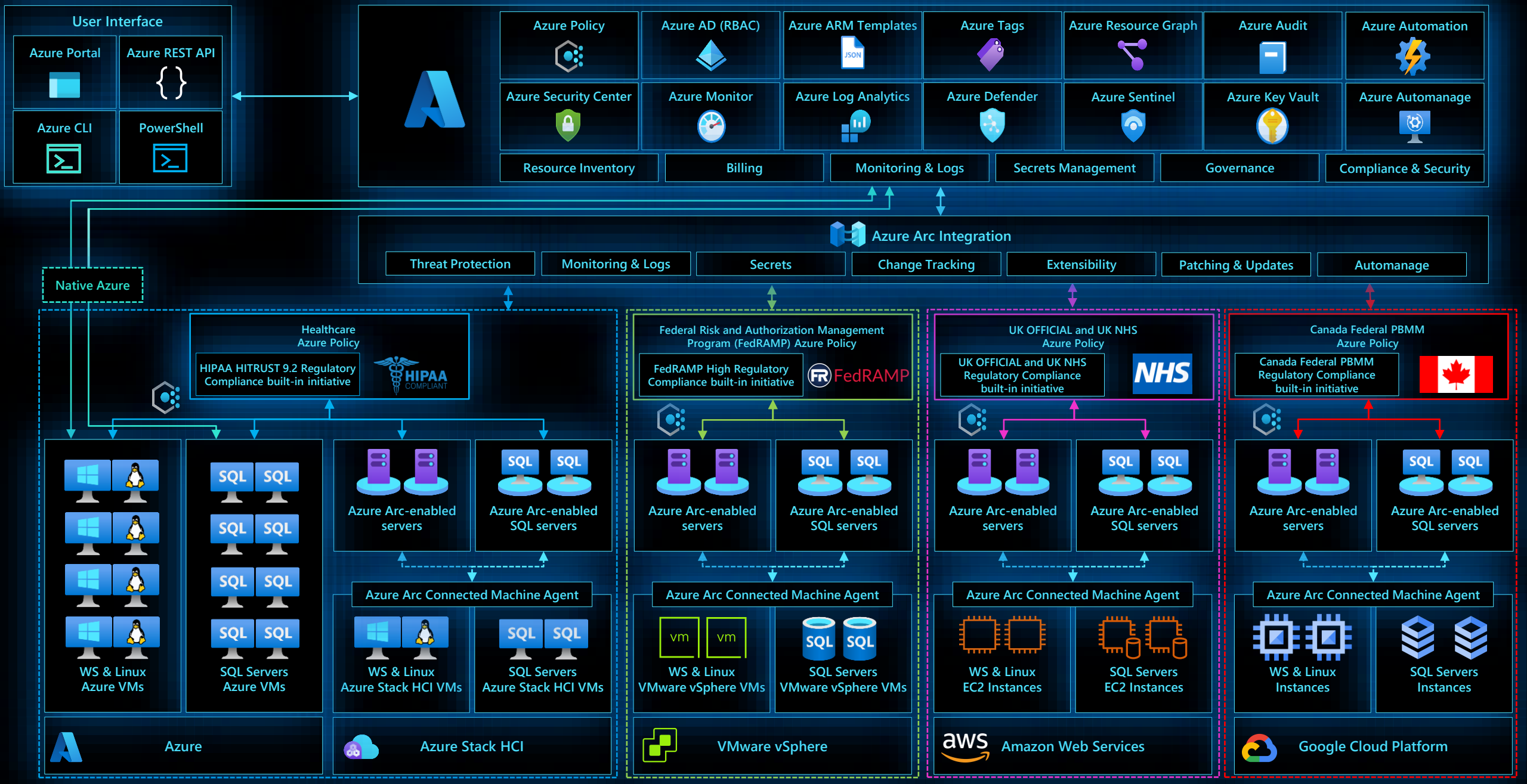
Azure Arc-enabled servers & Azure Arc-enabled SQL server

On-premises and multi-cloud integration



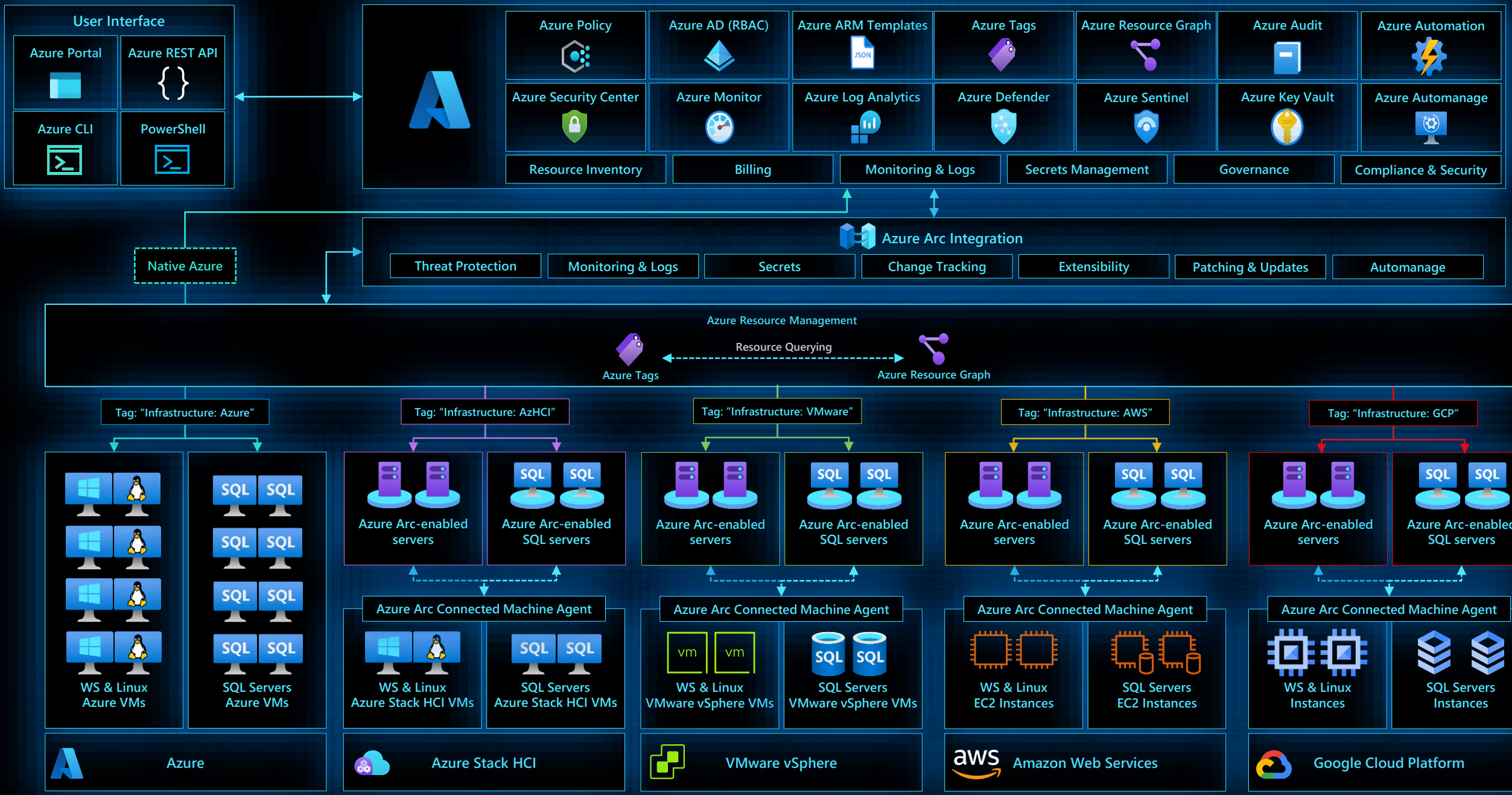
Azure Arc-enabled servers & Azure Arc-enabled SQL server

On-premises and multi-cloud compliance with Azure Policy



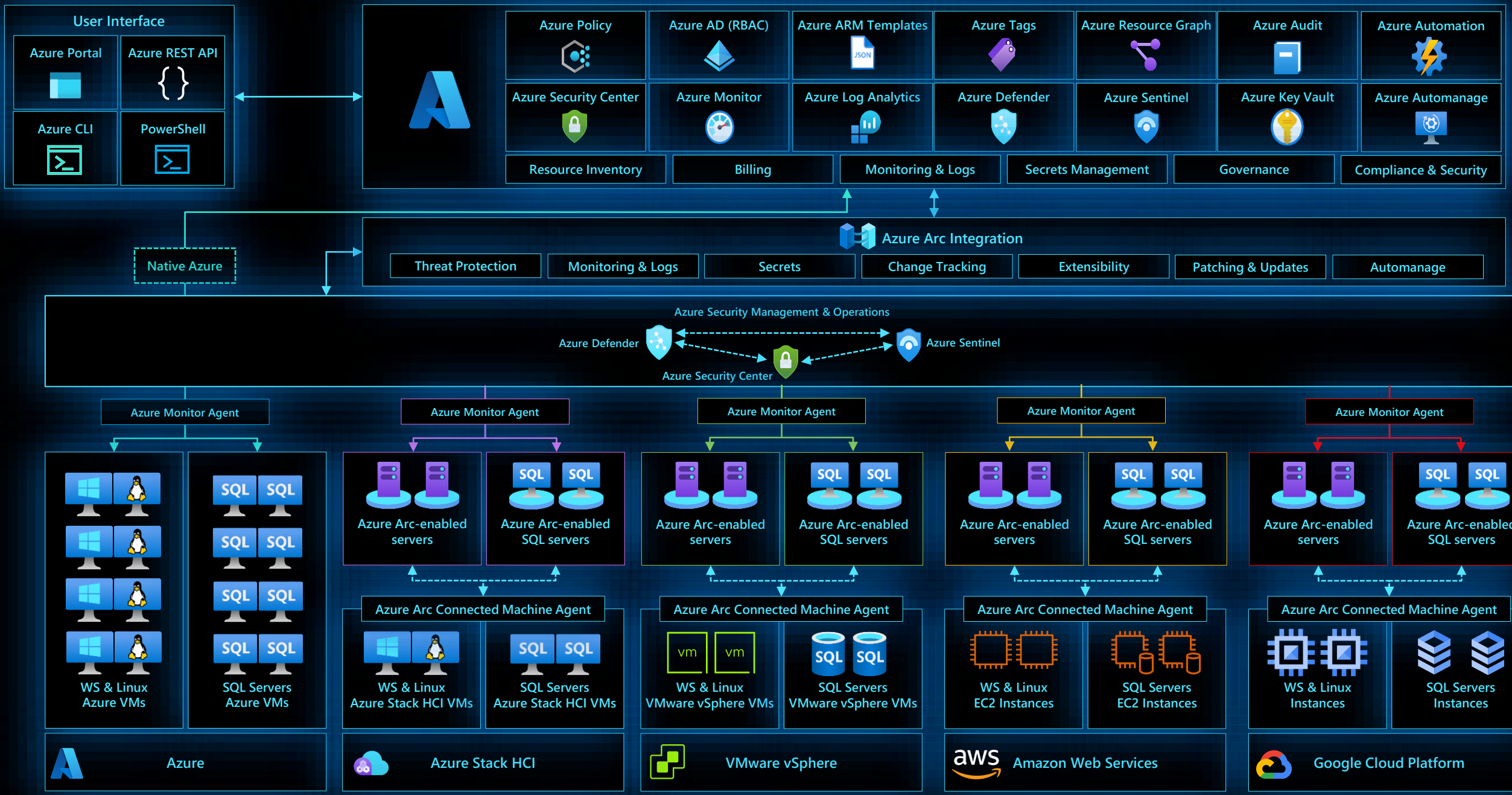
Azure Arc-enabled servers & Azure Arc-enabled SQL server

Resource management with tags



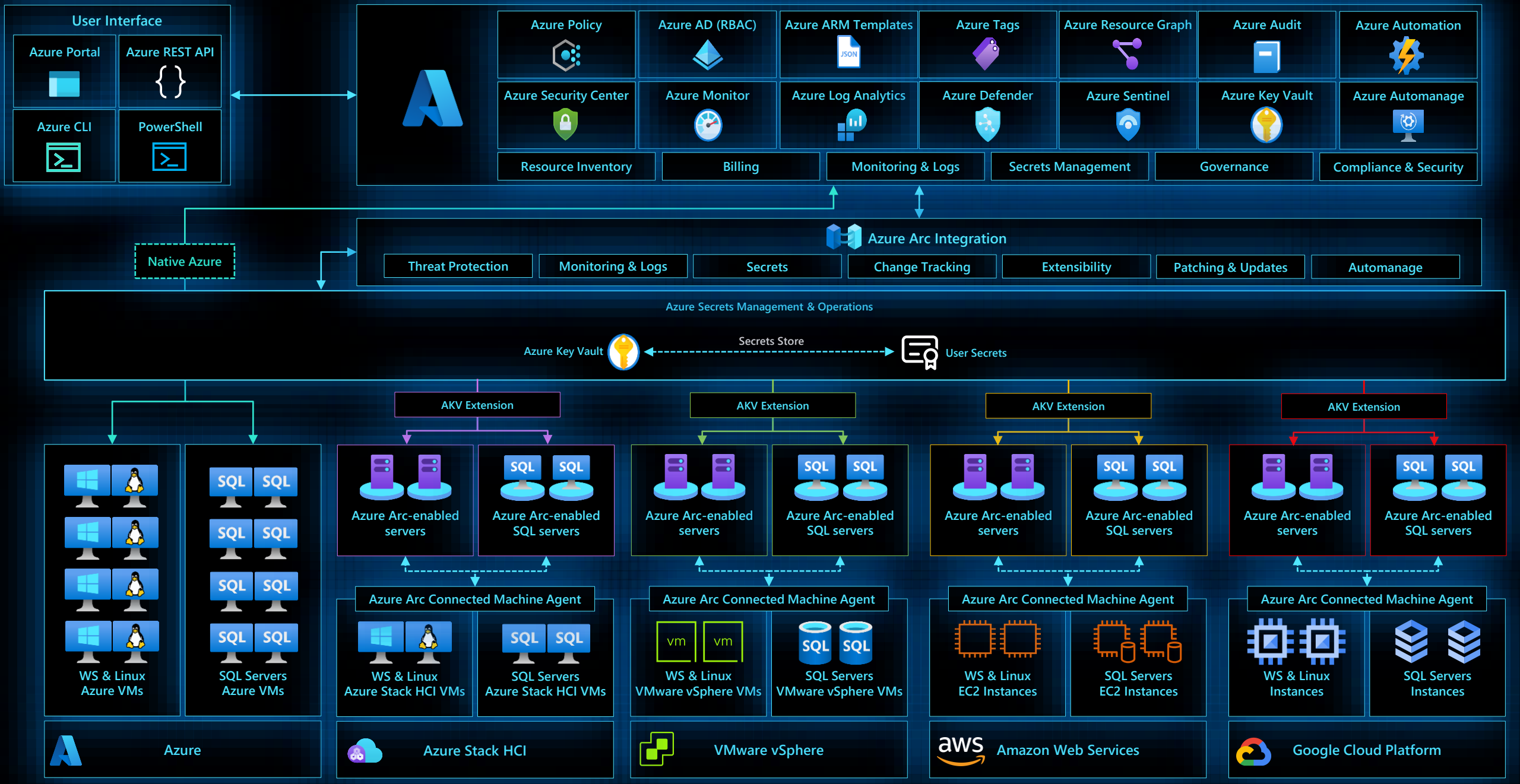
Azure Arc-enabled servers & Azure Arc-enabled SQL server

Security management with ASC, Defender and Sentinel



Azure Arc-enabled servers & Azure Arc-enabled SQL server

Secrets management with Azure Key Vault



Disaster Recovery, High Availability & Chaos

Ensuring business continuity with Azure Arc

Here are some of the features that come built-in with Azure Arc-enabled SQL Managed Instance:

Point in Time Restore (PITR): This feature allows you to recover from situations such as data corruptions caused by human errors. It is available in both General Purpose and Business Critical service tiers.

High Availability: You can deploy the Azure Arc-enabled SQL Managed Instance in high availability mode to achieve local high availability. This mode automatically recovers from scenarios such as hardware failures, pod/node failures, etc. This feature is only available in the Business Critical service tier.

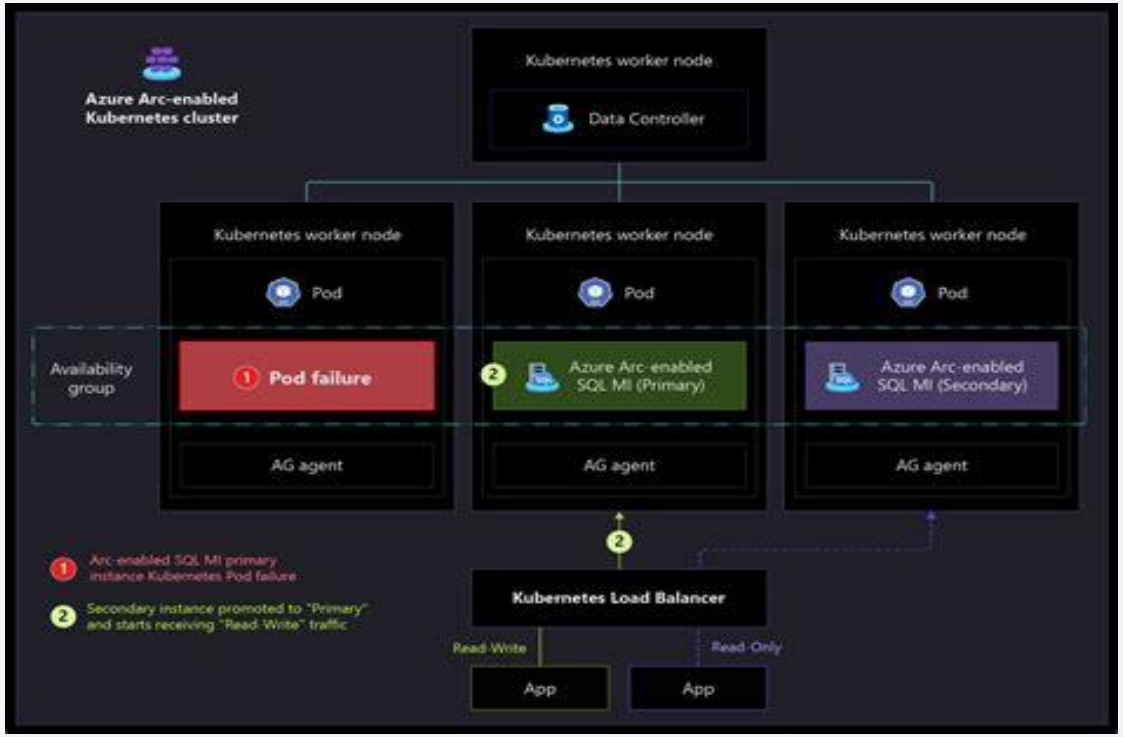
Disaster Recovery: You can configure disaster recovery by setting up another Azure Arc-enabled SQL Managed Instance in a geographically separate data center to synchronize data from the primary data center. This scenario is useful for recovering from events when an entire data center is down due to disruptions such as power outages or other events. It is available in both General Purpose and Business Critical service tiers.

Ensuring business continuity with Azure Arc

Azure Arc provides a set of capabilities for business continuity, which is a combination of people, processes, and technology that enables businesses to recover and continue operating in the event of disruptions.

In hybrid scenarios, there is a joint responsibility between Microsoft and the customer, such that the customer owns and manages the on-premises infrastructure while the software is provided by Microsoft.

You can learn more about configuring point in time restore, high availability, and setting up and configuring disaster recovery in Azure Arc-enabled SQL Managed



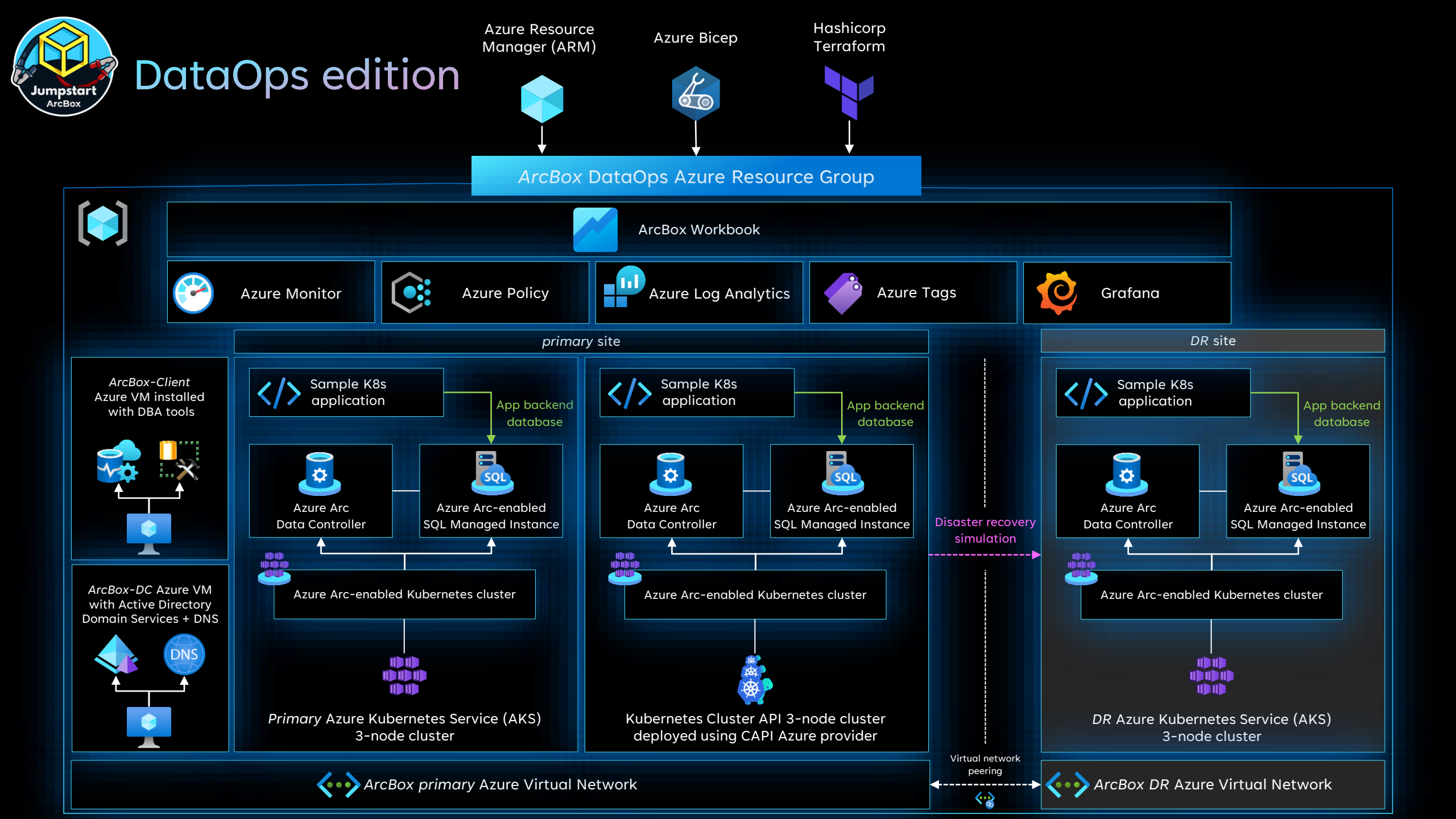
Azure Arc Jumpstart DataOps Flavor

With ArcBox for DataOps, we're bringing the same proven core design principles of the Azure Arc Jumpstart to this new offering. Providing a painless, fully automated deployment for all things Azure Arc is the founding principle of our ArcBox offerings.

We wanted to provide a way for our customers to experience Azure Arc-enabled SQL Managed to its fullest right away, so we baked in multiple Jumpstart scenarios.

ArcBox for DataOps provides users with a rich, fully automated Azure Arc-enabled SQL Managed Instance so they can experience and simulate capabilities like disaster recovery, SQL Backup and Restore, Active Directory integration, and more, all while also having a comprehensive unified operation and management layer that can then be expanded to serve production workload.

The entire solution is automatically deployed and includes all required Azure integrations, as well as three Kubernetes clusters and the supported Azure infrastructure alongside a sample application so users will have everything they need to get hands-on with the tech.

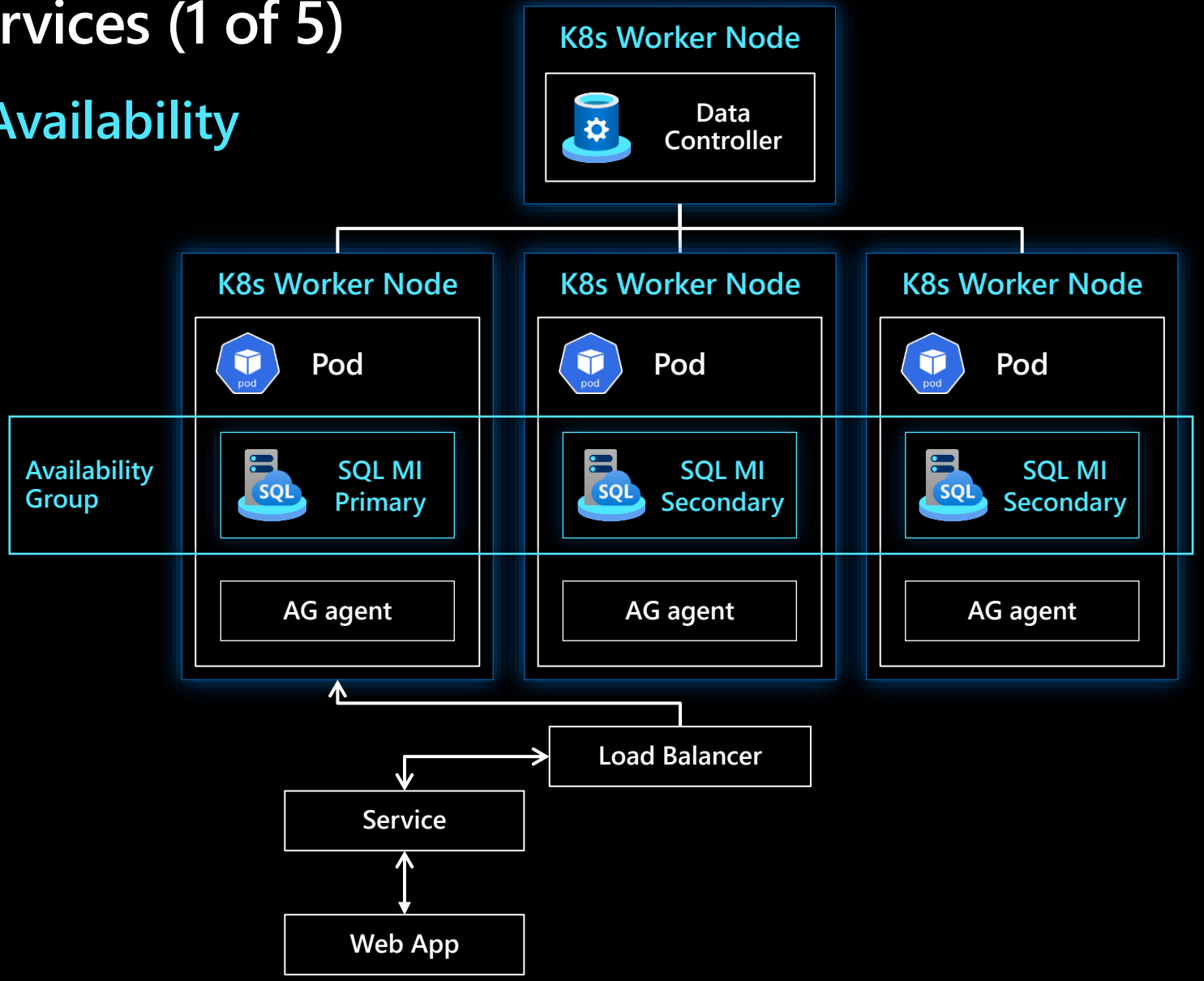

Jumpstart ArcBox
DataOps edition
Azure Resource Manager (ARM)
Azure Bicep
Hashicorp Terraform
ArcBox DataOps Azure Resource Group
ArcBox Workbook
Azure Monitor
Azure Policy
Azure Log Analytics
Azure Tags
Grafana
primary site
DR site
ArcBox-Client
Azure VM installed with DBA tools
ArcBox-DC Azure VM with Active Directory Domain Services + DNS
DNS
Sample K8s application
App backend database
Azure Arc Data Controller
Azure Arc-enabled SQL Managed Instance
SQL
Azure Arc-enabled Kubernetes cluster
Primary Azure Kubernetes Service (AKS) 3-node cluster
Kubernetes Cluster API 3-node cluster deployed using CAPI Azure provider
Disaster recovery simulation
DR Azure Kubernetes Service (AKS) 3-node cluster
Virtual network peering
ArcBox primary Azure Virtual Network
ArcBox DR Azure Virtual Network

Example of Disaster-Ready Approach

Azure Arc-enabled data services (1 of 5)

SQL Managed Instance High Availability

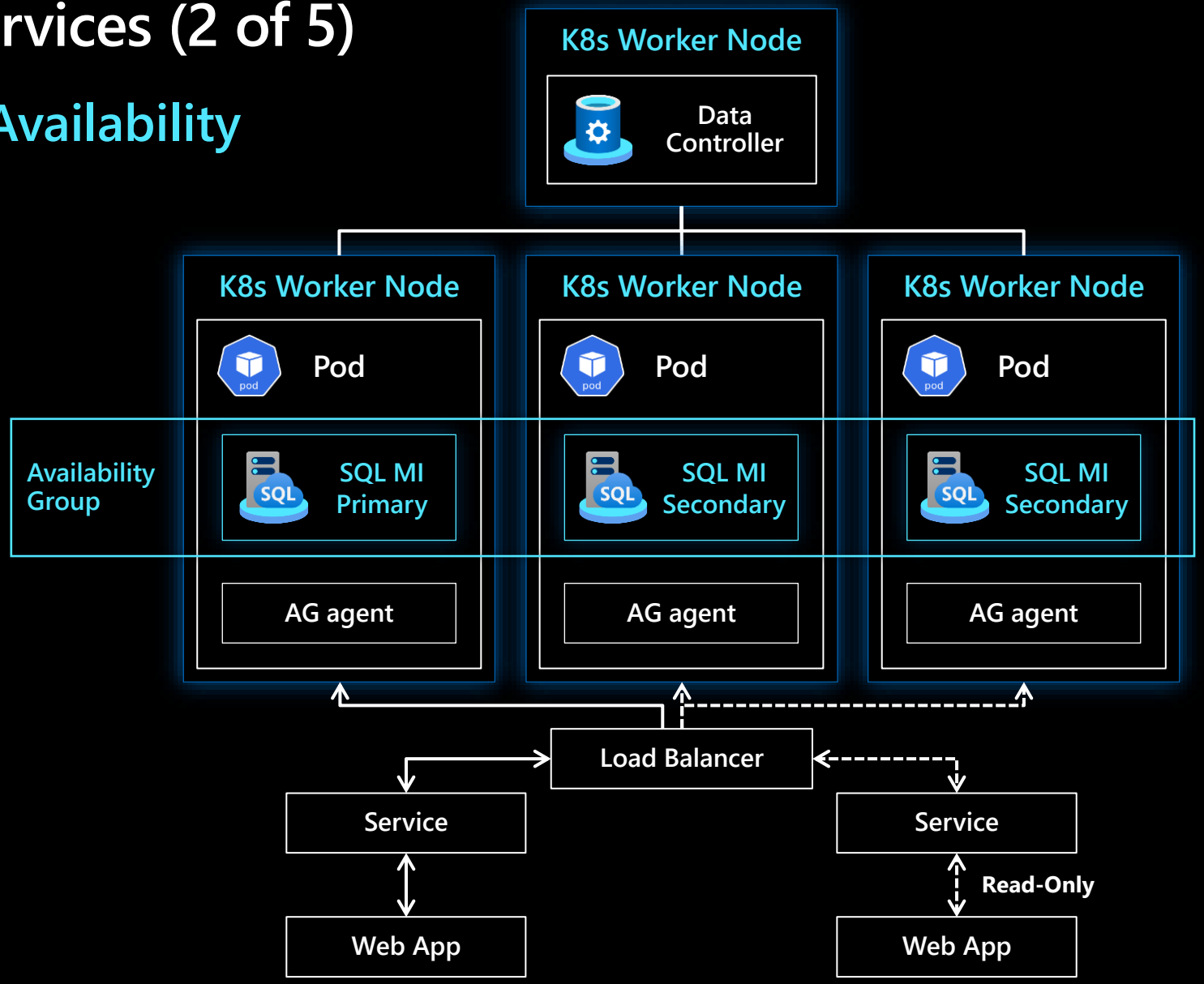
- Built-in Setup
- No other cluster technologies
- Default configuration with 3 sync replicas
- Primary and readable secondary endpoints
- Automated Failover



Azure Arc-enabled data services (2 of 5)

SQL Managed Instance High Availability

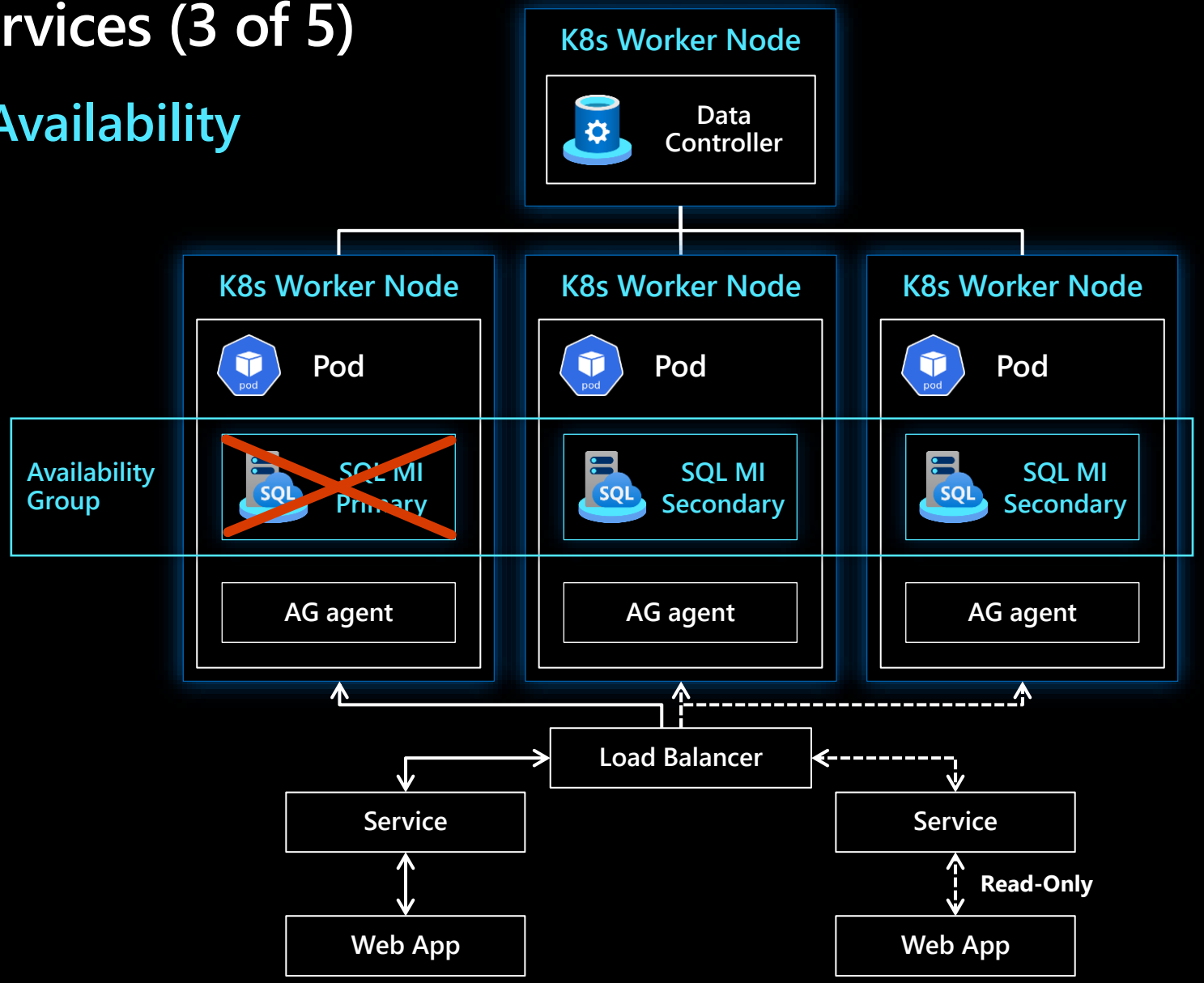
- Built-in Setup
- No other cluster technologies
- Default configuration with 3 sync replicas
- Primary and readable secondary endpoints
- Automated Failover



Azure Arc-enabled data services (3 of 5)

SQL Managed Instance High Availability

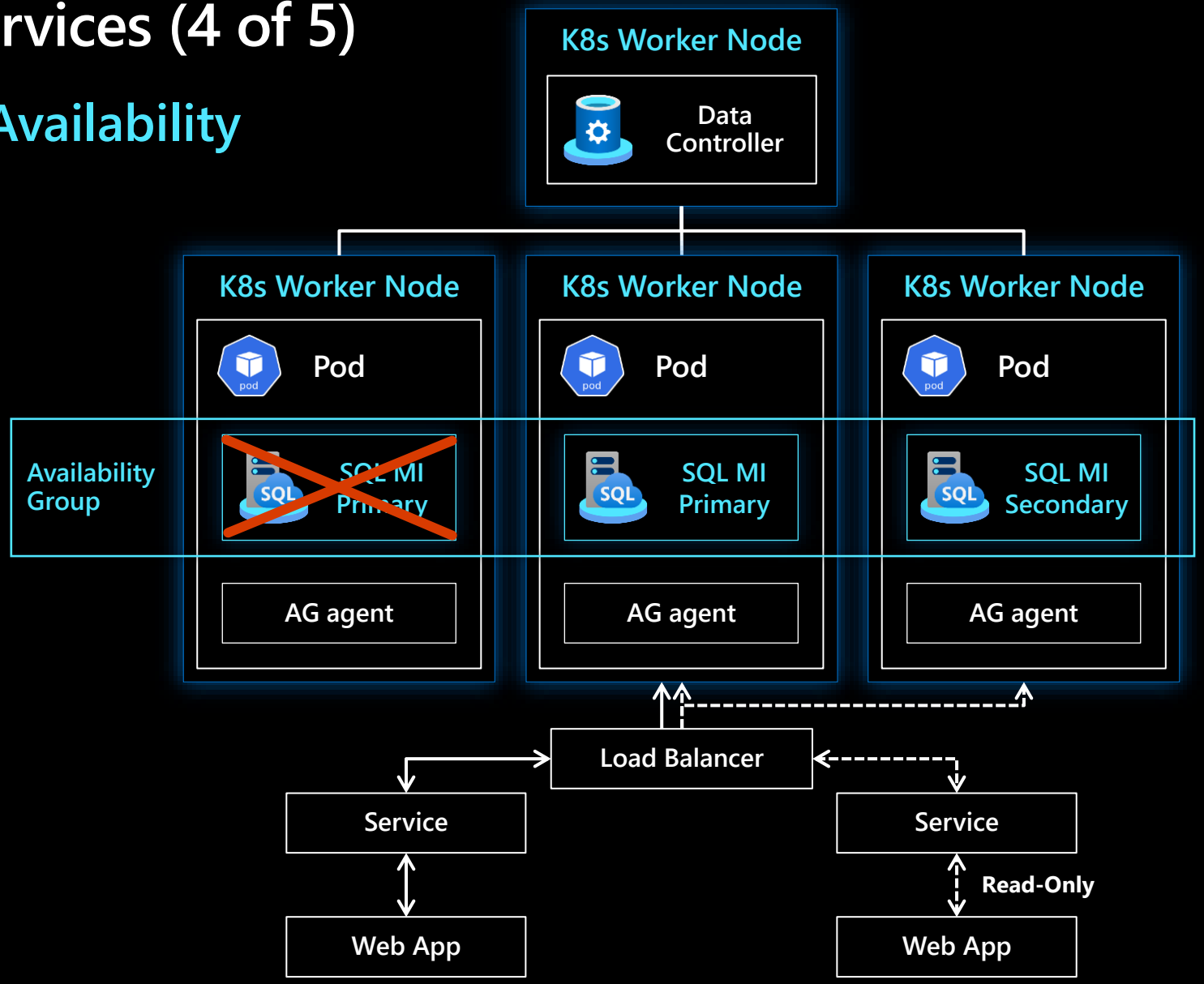
- Built-in Setup
- No other cluster technologies
- Default configuration with 3 sync replicas
- Primary and readable secondary endpoints
- Automated Failover



Azure Arc-enabled data services (4 of 5)

SQL Managed Instance High Availability

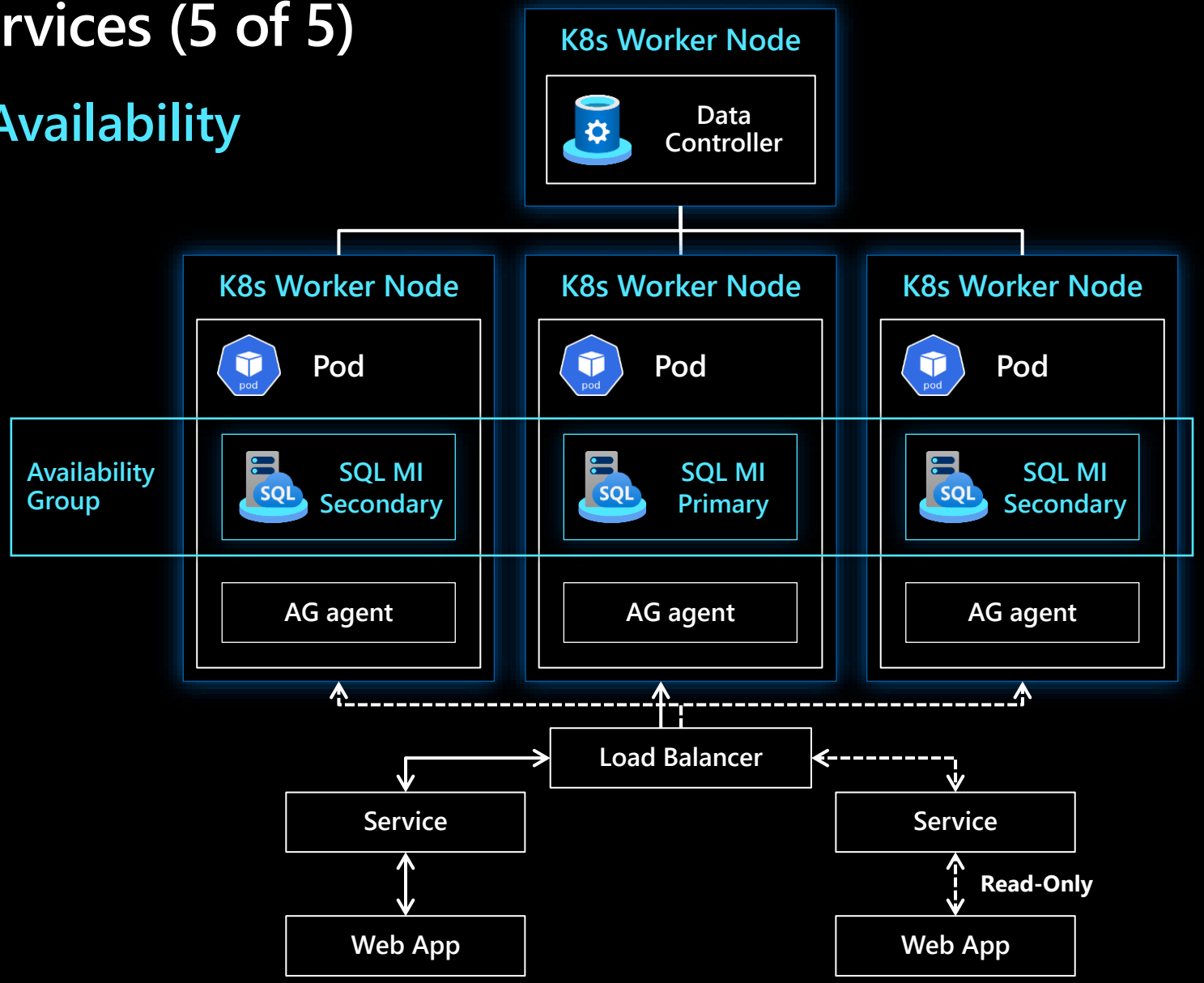
- Built-in Setup
- No other cluster technologies
- Default configuration with 3 sync replicas
- Primary and readable secondary endpoints
- Automated Failover



Azure Arc-enabled data services (5 of 5)

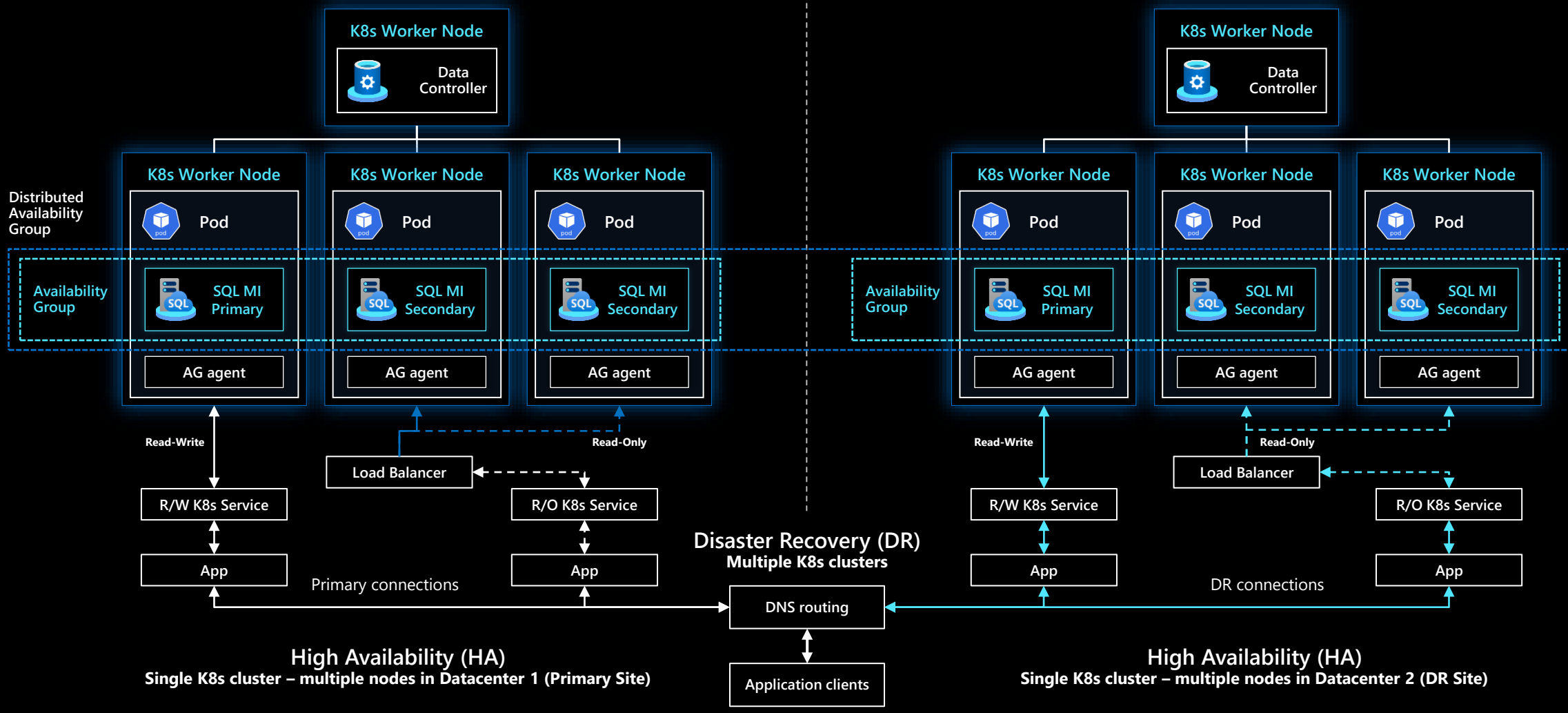
SQL Managed Instance High Availability

- Built-in Setup
- No other cluster technologies
- Default configuration with 3 sync replicas
- Primary and readable secondary endpoints
- Automated Failover



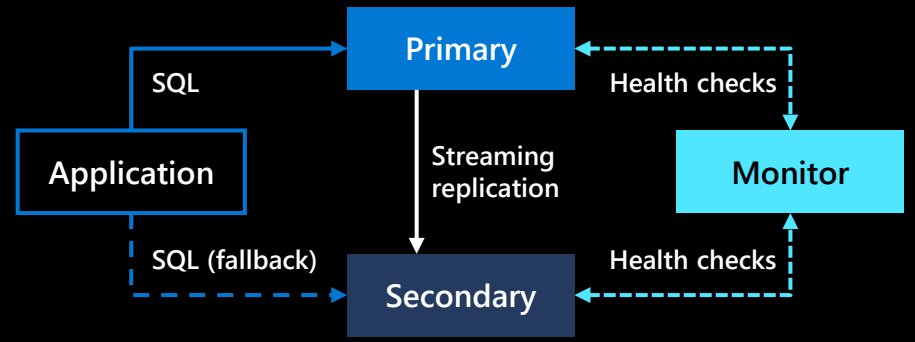
Arc-enabled Azure SQL Managed Instance

High Availability and Disaster Recovery using Availability Groups

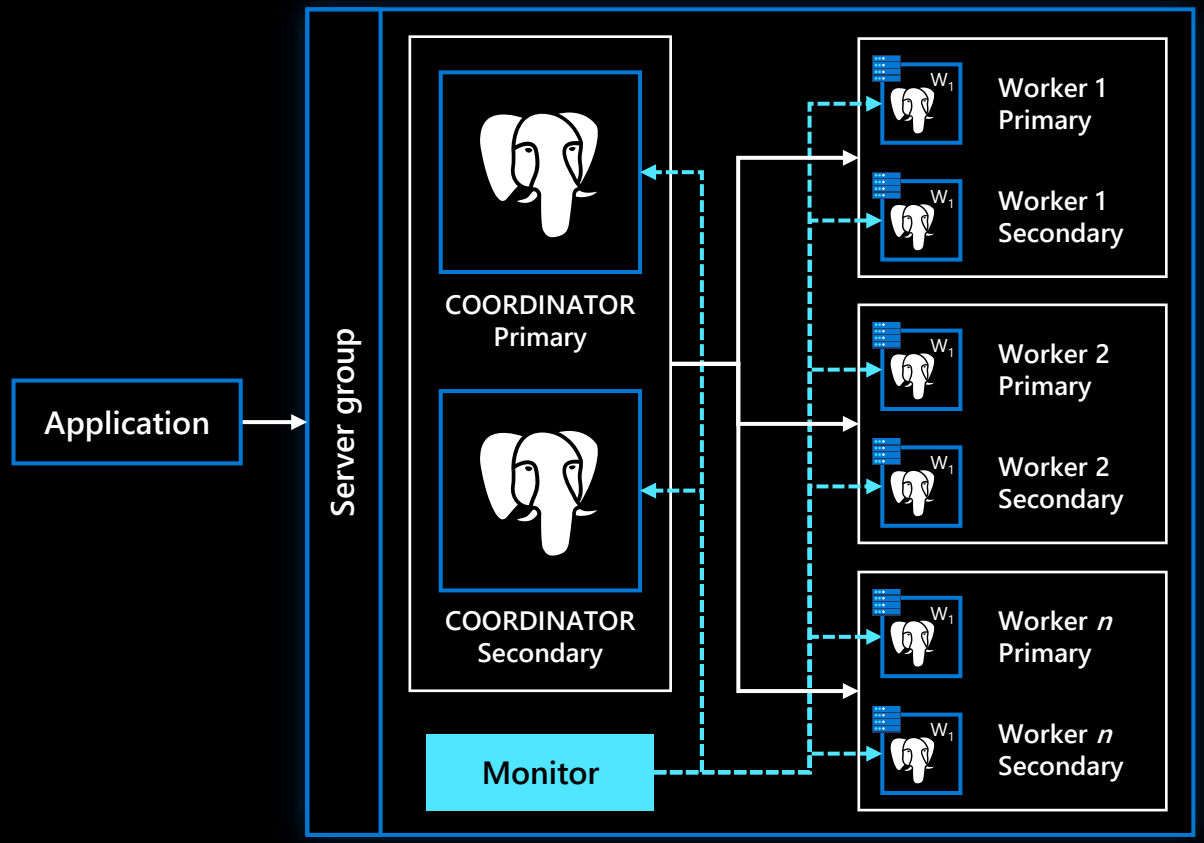


High availability for Arc-enabled PostgreSQL

PREVIEW



- Based on pg_auto_failover extension
- Supports multiple secondaries
- Failover at the Postgres coordinator/worker level



Introduction to Azure Chaos Studio

An experimentation platform for improving app resiliency

Improve application resilience with chaos testing by deliberately introducing faults that simulate real-world outages. Azure Chaos Studio Preview is a fully managed chaos engineering experimentation platform for accelerating discovery of hard-to-find problems, from late-stage development through production. ***Disrupt your apps intentionally*** to identify gaps and plan mitigations before your customers are impacted by a problem.

Benefits of Azure Chaos Studio

: Subject your Azure applications to real or simulated faults
: Observe how your applications respond to real-world disruptions
: Integrate chaos experiments into any phase of quality validation
: Use the same tools as Microsoft engineers to build resilience of cloud services

How to use Azure Chaos Studio [Preview]

Improve the reliability of your Azure applications

Experiment by subjecting your Azure apps to real or simulated faults in a controlled manner to better understand application resiliency. Observe how your apps will respond to real-world disruptions such as network latency, an unexpected storage outage, expiring secrets, or even a full datacenter outage.

Experiment on your own terms

Validate product quality where and when it makes sense for your organization. Use the continuously expanding library of faults, which includes CPU pressure, network latency, blocked resource access, and even infrastructure outages. Drive application resilience by performing ad-hoc drills, integrate with your CI/CD pipeline, or do both to monitor production quality through continuous validation.

Gain insights without the chaos of getting started

Avoid the need to manage tools and scripts while spending more time learning about your application's resilience. Get started quickly with experiment templates and an expanding library of faults—including agent-based faults that disrupt within resources and service-based faults that disrupt resources at the control plane.

Go beyond fault injection with reliability validation

Improve application reliability by implementing a cohesive strategy to make informed decisions before, during, and after chaos experiments. Integrate load testing into your chaos experiments to simulate real-world customer traffic. Disrupt your apps intentionally to identify gaps and plan mitigations before your customers are impacted by a problem.

Future Roadmap and Upcoming Features


SQL

What is on the horizon for Azure Arc

Overview

Once a month, the various Azure Arc Edge and Platform product groups at Microsoft will hold a call to showcase new features, talk through important topics and engage in a Q&A regarding Azure Arc.

The foundational goals of the call are highlighted below:

- Provide the Azure Arc community with product updates
- Host a short talk and/or demo on Azure Arc Edge and Platform technologies and products technologies
- Collect feedback from the community on issues, blockers, use cases, and questions related to Azure Hybrid Cloud technologies and products
- 5-10 minutes: “Ask us anything” and feedback discussion

What is on the horizon for Azure Arc

Who is the "community"? 💬

If you are a customer, partner, Microsoft employee, or just someone who loves tech, for us, you are part of our community. The content presented in our calls is **not under a non-disclosure agreement (NDA)** and is public because our mission is just to spread the ❤ for Azure Arc Edge and Platform solutions and technologies.

Meetup agenda 📃

Each monthly meetup will be 1 hour, don't be late, we have a lot to cover

- 2 minutes: Welcome
- 45-50 minutes: Product updates
- 5-10 minutes: “Ask us anything” and feedback discussion

How to be involve and learn more about Azure Arc

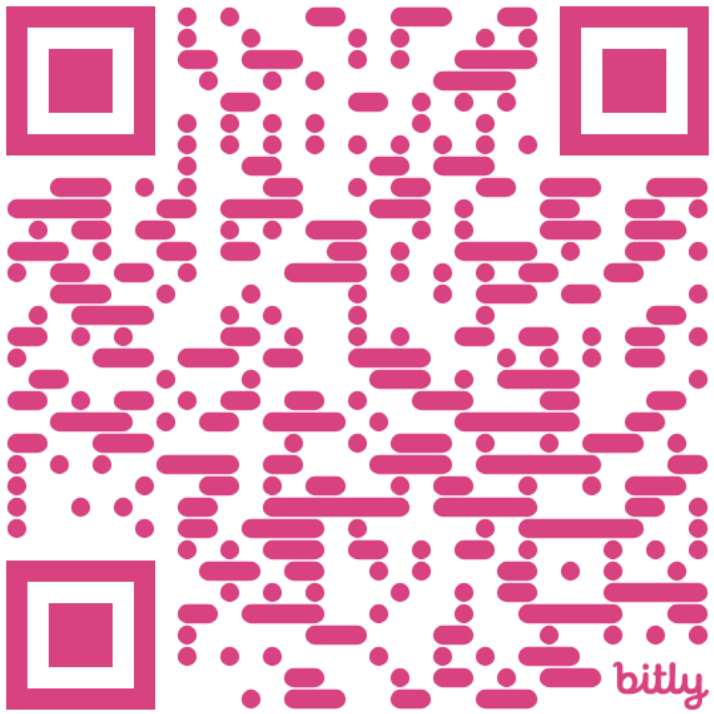
[Azure Arc - Microsoft Community Hub]
Take a part in discussion

[Azure Arc Blog - Microsoft Community Hub]
Read, Share, Propose, Contribute in building Knowledge Hub on Microsoft Azure Arc Blog

[microsoft/azure_arc_community: Public repository for hosting the Azure Arc Community content (github.com)]
Support, Share, Contribute in Azure Arc Community on GitHUb

Resources

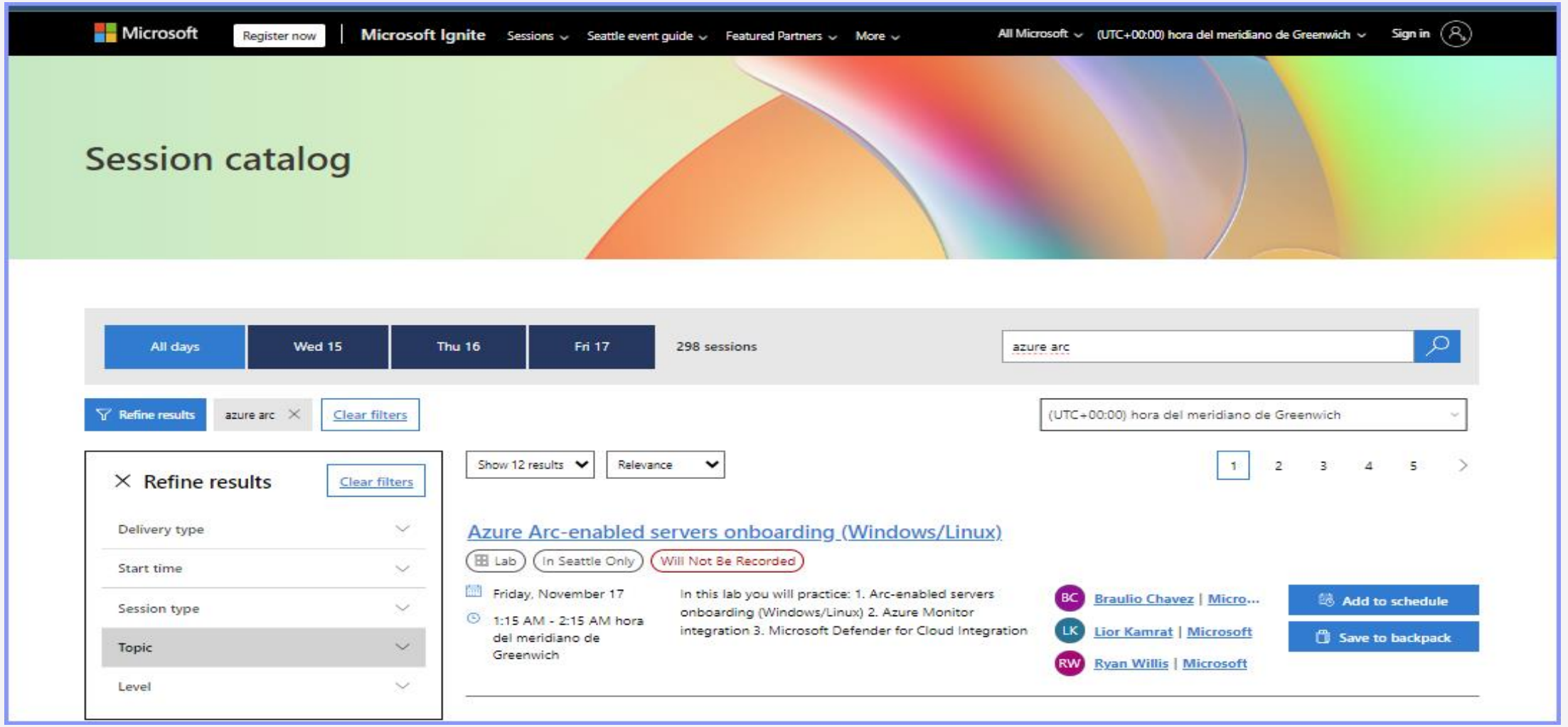
Presentations from all Webinars



GitHub - KoprowskiT/AzureArcWithQA:
Content from all events about Azure Arc delivered with QA

https://bit.ly/AzureArcWithQA

Observe the Future



Resources

Microsoft Learn / Docs

Azure Arc | Microsoft Learn

Microsoft Learn / Intro to Azure Arc

https://bit.ly/AzureArcIntroMSLearn

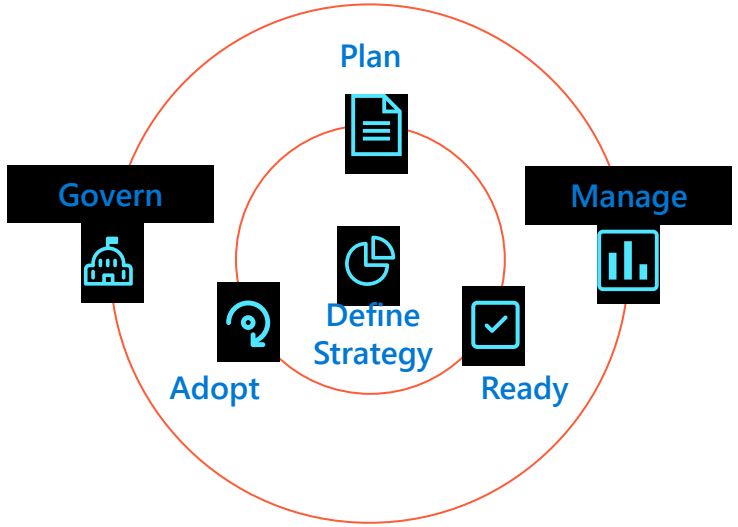
Microsoft Ignite Conference

Session catalog (microsoft.com)

Microsoft Azure Arc Jumpstart

Overview | Azure Arc Jumpstart

Complete guidance for hybrid and multicloud approach



Cloud Adoption Framework

Build skills across your team with **Microsoft Learn**

Accelerate deployment with **Reference Architectures**

Optimize workloads with **Azure Well-Architected**

Apply **best practices** to rapidly onboard

Review **technical documentation** on featured products

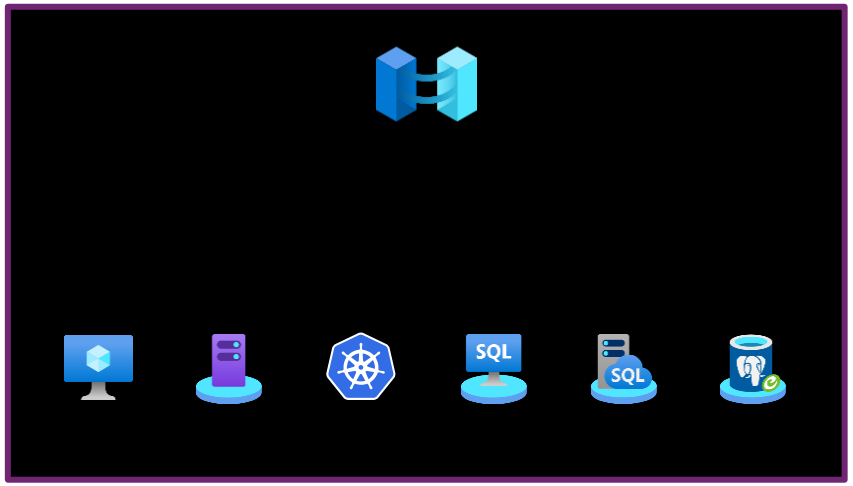
https://aka.ms/adopt/hybrid

Get started

Azure Arc-enabled servers generally available, get started today: https://aka.ms/Azure-Arc
Azure Arc-enabled Kubernetes generally available, get started today: https://aka.ms/Azure-Arc-Kubernetes
Try Azure Arc-enabled data services: https://aka.ms/hybrid-data-services

Learn more

Azure Arc Jumpstart: https://aka.ms/AzureArcJumpstart
Technical documentation: https://aka.ms/AzureArcDocs
Azure Arc Learning Path: https://aka.ms/AzureArcLearn



Resources

Azure Arc complete overview

aka.ms/arc-introvideo

Introducing Azure Arc

aka.ms/arc-compete

Azure Arc compete deck

aka.ms/azurearcpricing
Azure Arc pricing page

aka.ms/arc-techcommunity

Deep dives on Azure Arc, best practices and more

aka.ms/arc-customerstories

Learn how customers are implementing Azure Arc

https://aka.ms/arc-feedback

Public Q&A forum

aka.ms/AzureArcJumpstart

Azure Arc Jumpstart

aka.ms/AzureArcJumpstartDemos

Azure Arc Jumpstart demos

Azure Arc-enabled Kubernetes & servers

aka.ms/arc-blog
Azure Arc: Extending Azure management to any infrastructure

aka.ms/arc-k8svideo

Kubernetes—Managing K8 clusters outside of Azure with Azure Arc

aka.ms/arc-serversvideo

Server management—Organize all your servers outside of Azure with Azure Arc

aka.ms/arc-serversdocs

Documentation for Azure Arc enabled servers

aka.ms/arc-k8sdocs

Documentation for Azure Arc enabled Kubernetes

Azure Arc-enabled data services

aka.ms/arc-datablog

Run Azure data services on-premises, at the edge, and multi-cloud with Azure Arc

aka.ms/arc-data-mechanicsvideo

Azure Arc-enabled data services demos including SQL and PostgreSQL Hyperscale

aka.ms/arc-ignite-video

Ignite 2021: Innovate across hybrid and multicloud with Azure Arc

aka.ms/arc-datadocs

Documentation for Azure Arc-enabled data services

Q & A Time

Let’s look for the questions!

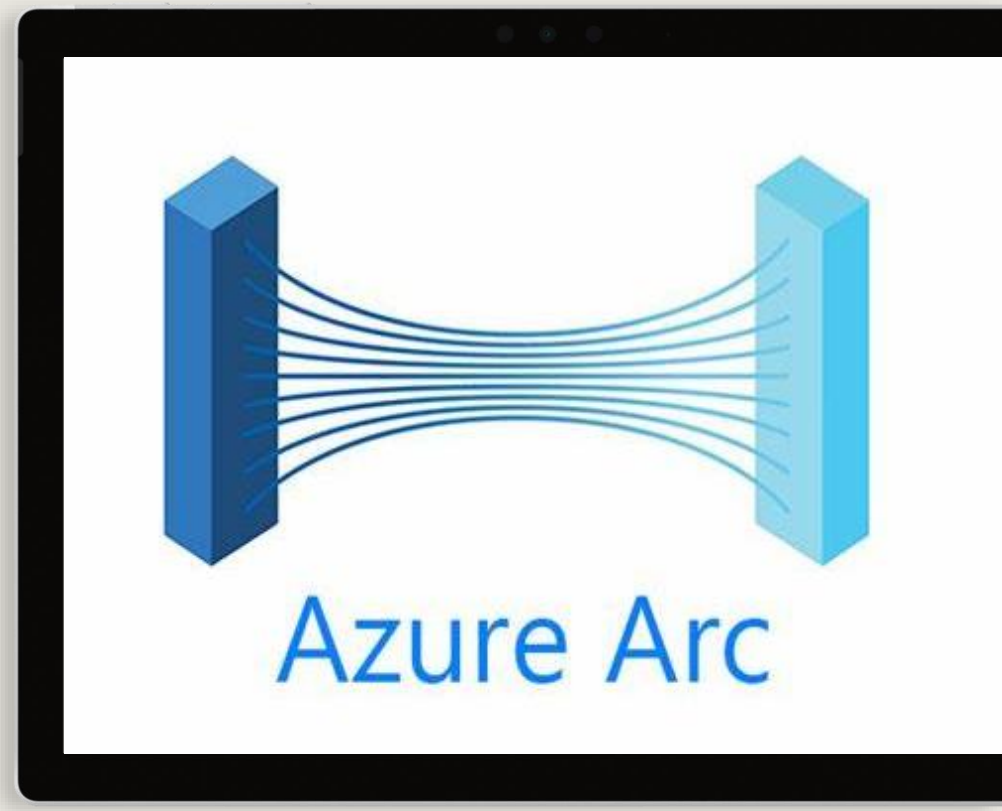
Webinar build on:

Materials from Azure Jumpstart Team

Almost all black/blue/colour slides
Big Thanks for Lior & Jan

Materials from Microsoft Learn

Microsoft Learn
Microsoft Docs
Azure Portal Docs



Webinar delivered by:

Tobias Koprowski

Bachelor in: Banking
Higher national diplomas in: European Law & Corporate Governance
Three years in personal and home insurance
Five years in consumer & corporate banking
Ten years in physical Data Center
Microsoft Certified Trainer (MCT) & Educator (MCE)
CertNexus Authorized Instructor (CAI)

Member of:
| **BCS** (The Chartered Institute of IT
| **IAPP** (International Association of Privacy Professionals)
| **ISSA** (Information Security System Association)
| **ISACA** (Information Systems Auditing & Control Association)
| **ISC²** (International Information System Security Certification Consortium)
| **CSA** (Cloud Security Alliance) – AI Usage Policy Working Group

STEM Ambassador | Royal Voluntary Service

Social Media: KoprowskiT @ [TW|LI|BS|FB]

Microsoft

Thank You for spending time with us!