Microsoft

Microsoft Azure Arc Webinar Series

Webinar TWO:
Intermediate-Level Practices with Microsoft Azure Arc

© Copyright Microsoft Corporation. All rights reserved.

- Introduction (5 min)
- Recap of Webinar One (5 minutes)
- Advanced Configuration & Management (25 minutes)
- Cost Management (20 minutes)
- Refreshment Break (10 minutes)
- Security Considerations (25 minutes)
- Advanced Azure Arc Features [aka DevOps] (20 minutes)
- Q&A Time (10 minutes)

© Copyright Microsoft Corporation. All rights reserved.

Introduction

(5 minutes)

© Copyright Microsoft Corporation. All rights reserved.

About the Webinar

Elevate your Azure Arc understanding to the next level.

After a quick recap of our introductory webinar, immerse yourself in advanced configuration techniques for managing multiple clusters and ensuring robust policy enforcement

Delve into Azure Arc's potential for cost management, followed by an insightful segment on security considerations.

Experience live demonstrations showcasing the advanced features, particularly focusing on DevOps and Azure Arc-enabled Kubernetes.

We round off this intermediate session with an interactive Q&A session, answering your pressing questions.

Join us for a captivating 2-hour session, followed by a dedicated Q&A segment to address your queries.

© Copyright Microsoft Corporation. All rights reserved.

Recap of Webinar One

(5 minutes)

© Copyright Microsoft Corporation. All rights reserved.

Quick overview of previous webinar content

What is Microsoft Azure Arc?

- An overview of Azure Arc and its concept
- Importance of hybryd cloud environment
- Importance of multi cloud environment

Basics of Installation & Configuration

- Technical requirements
- Licensing Requirements
- Step-by-Step Installation Guide

Overview & Flavors of Azure Arc Services

- Overview of the Services & Infrastructure
- Introduction to Azure JumpStart
- Flavors of Azure JumpStart (Agora, IT-Pros, DevOps, DataOps)

Demo of Basic Use-Case for IT-Pros

- How to manage and organize resources
- Fundamentals of Governance and management

© Copyright Microsoft Corporation. All rights reserved.

SHAc - PUBLIC

Advanced Configuration & Management

(25 minutes)

© Copyright Microsoft Corporation. All rights reserved.

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).

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Validated Providers

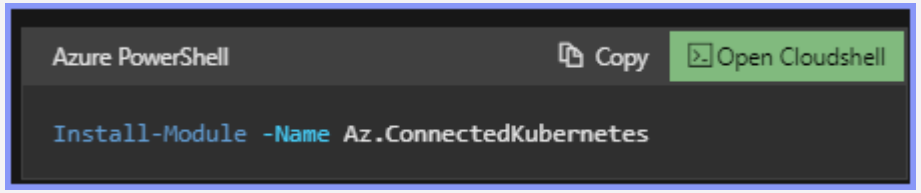
Provider name	Distribution name	Version
RedHat	OpenShift Container Platform	4.9.43, 4.10.23, 4.11.0-rc.6, 4.13.4
VMware	Tanzu Kubernetes Grid	TKGs 2.2; upstream K8s 1.25.7+vmware.3 TKGm 2.3; upstream K8s v1.26.5+vmware.2 TKGm 2.2; upstream K8s v1.25.7+vmware.2 TKGm 2.1.0; upstream K8s v1.24.9+vmware.1
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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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

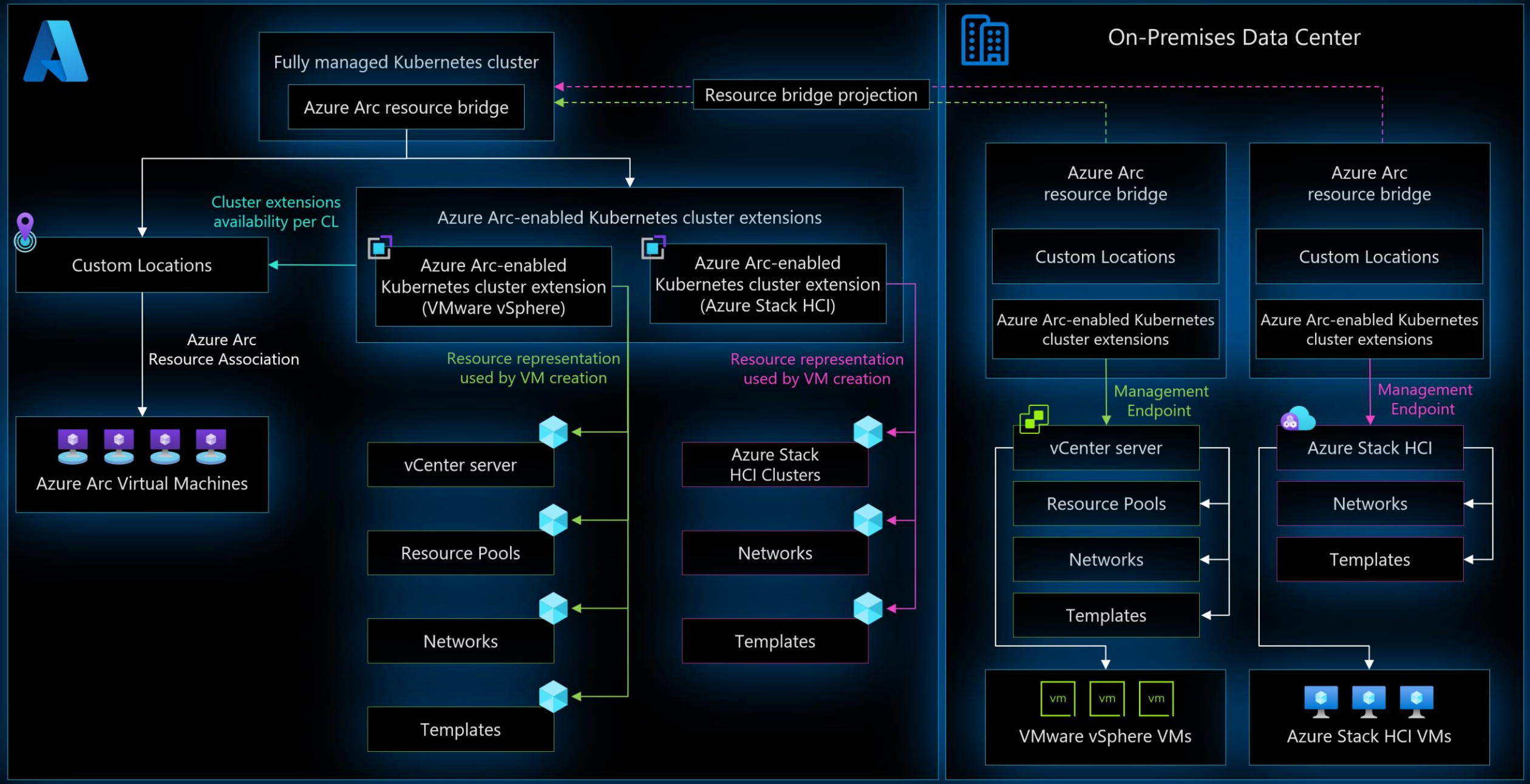
- on-premises environment on Azure Stack HCI
- VMware (Arc-enabled VMware vSphere preview),
- and System Center Virtual Machine Manager (SCVMM) (Arc-enabled SCVMM preview)

Arc resource bridge has the following minimum resource requirements:

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

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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).

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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)

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Policy Assignemnt & 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

© Copyright Microsoft Corporation. All rights reserved.

Policy Assignemnt & 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

© Copyright Microsoft Corporation. All rights reserved.

Rgional Availability ~ Azure Products by Region | Microsoft

	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.

© Copyright Microsoft Corporation. All rights reserved.

Cost Management

(20 minutes)

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Hey Bing:
Create Refreshment Break

Security Considerations

(25 minutes)

© Copyright Microsoft Corporation. All rights reserved.

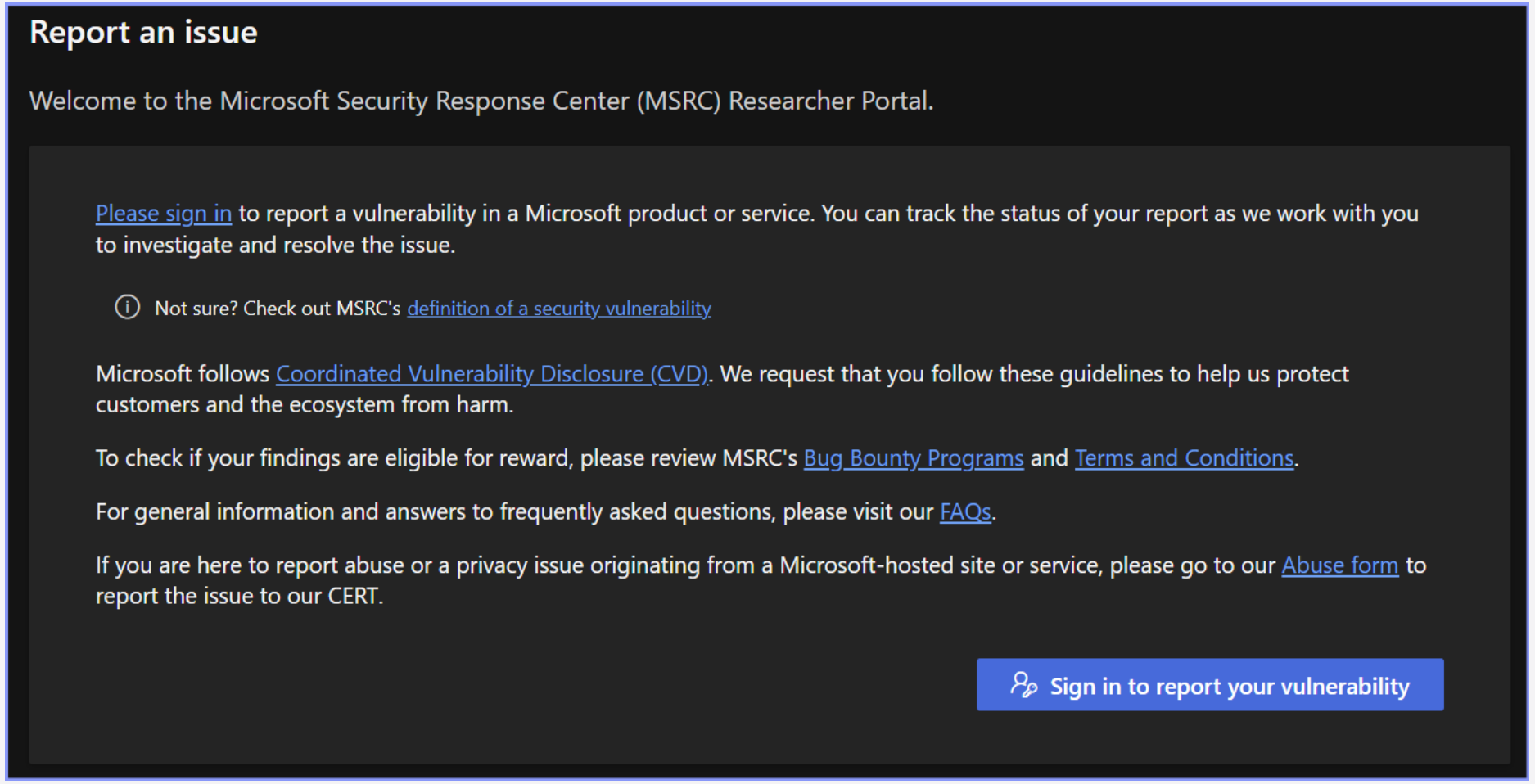
Microsoft Security Approach

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

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security Approach | Report an Issue



© Copyright Microsoft Corporation. All rights reserved.

Identity and access control (1)

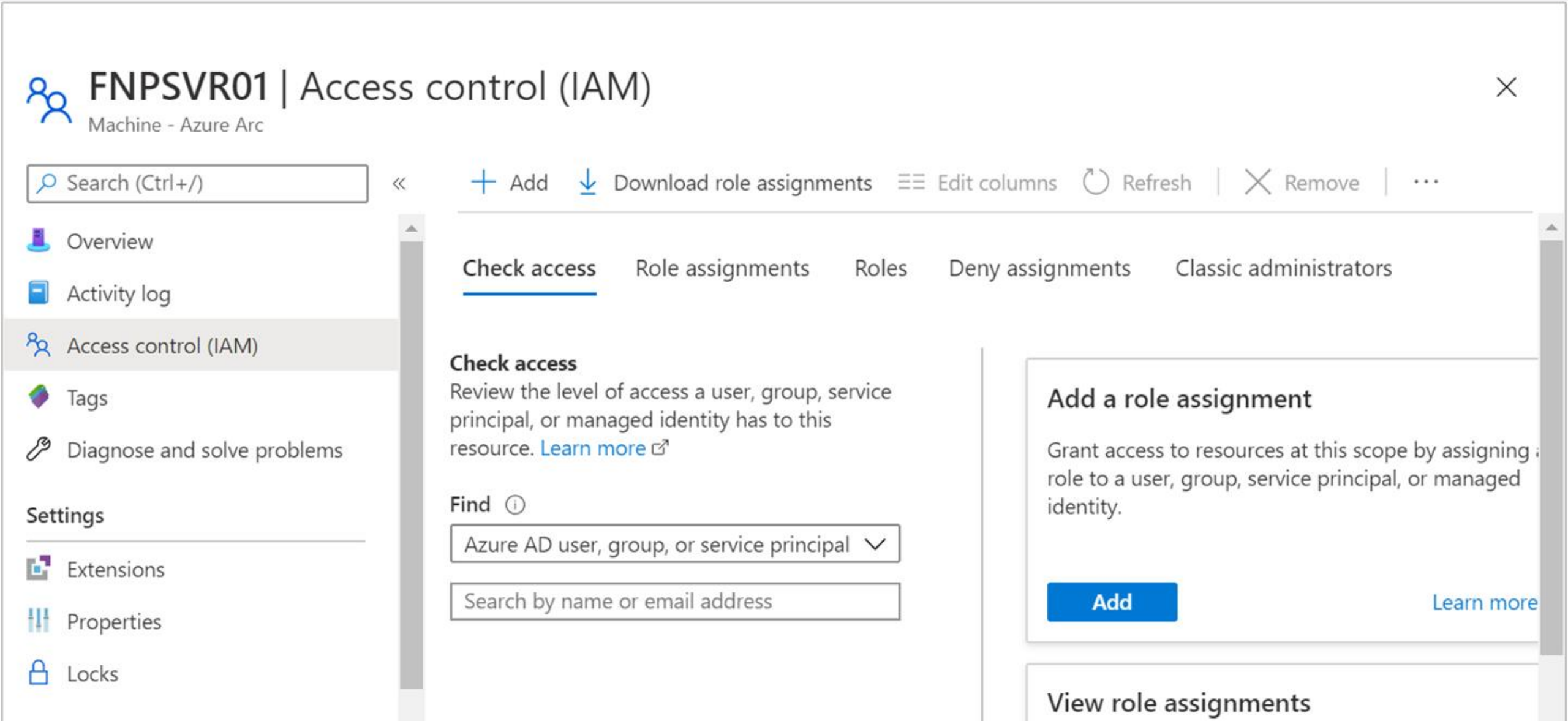
Azure role-based access control is used to control which accounts can see and manage your Azure Arc-enabled server. From the **Access Control (IAM)** page in the Azure portal, you can verify who has access to your Azure Arc-enabled server.

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.

© Copyright Microsoft Corporation. All rights reserved.

SHAc - PUBLIC

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.

© Copyright Microsoft Corporation. All rights reserved.

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).

© Copyright Microsoft Corporation. All rights reserved.

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:

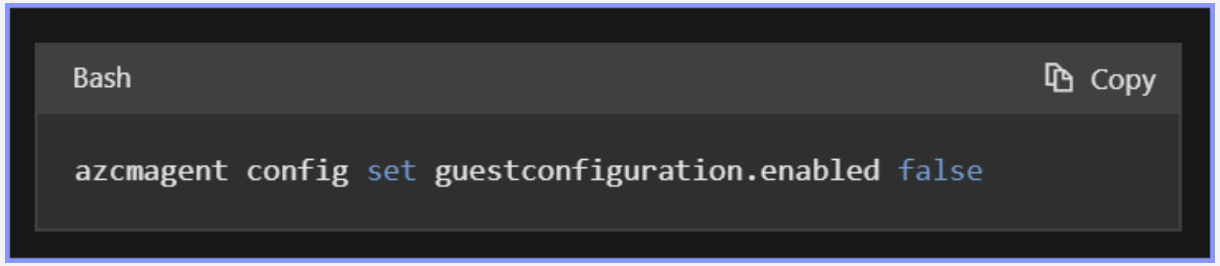
If an extension is already installed on your server before you configure an allowlist or blocklist, **it won't automatically be removed**.
It's your responsibility to delete the extension from Azure to fully remove it from the machine. Delete requests are always accepted to accommodate this scenario.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

© Copyright Microsoft Corporation. All rights reserved.

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.



© Copyright Microsoft Corporation. All rights reserved.

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
```

© Copyright Microsoft Corporation. All rights reserved.

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.*

© Copyright Microsoft Corporation. All rights reserved.

Plan and 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?

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

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

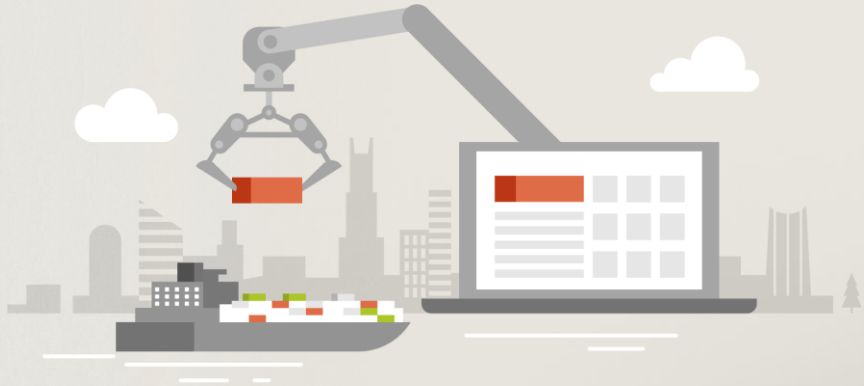
© Copyright Microsoft Corporation. All rights reserved.

Advanced Azure Arc Features

(20 minutes)

© Copyright Microsoft Corporation. All rights reserved.

SHAc - PUBLIC



Azure Kubernetes Service (AKS)

Edge Essentials

© Copyright Microsoft Corporation. All rights reserved.

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

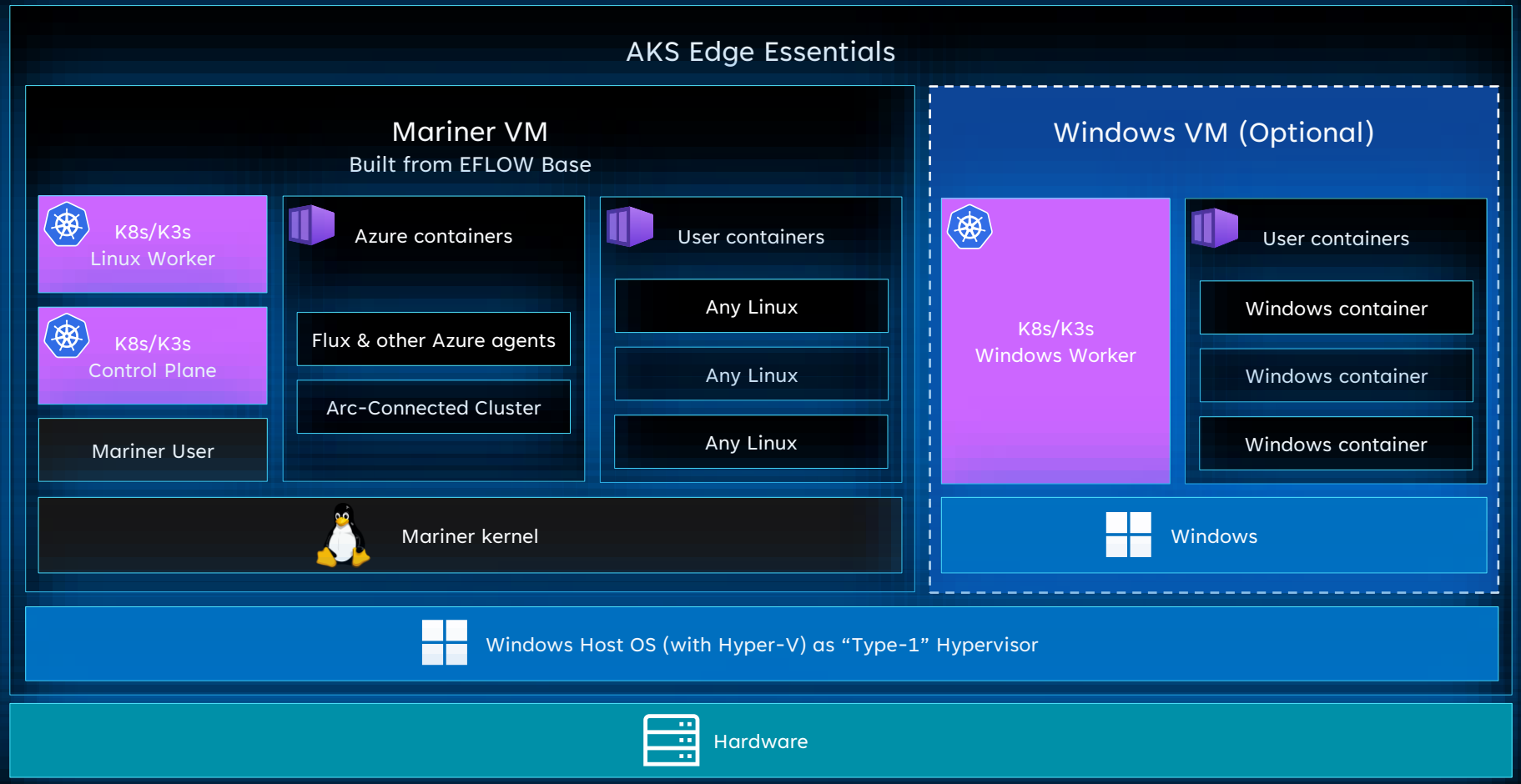
CNCF-conformant Kubernetes platform

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

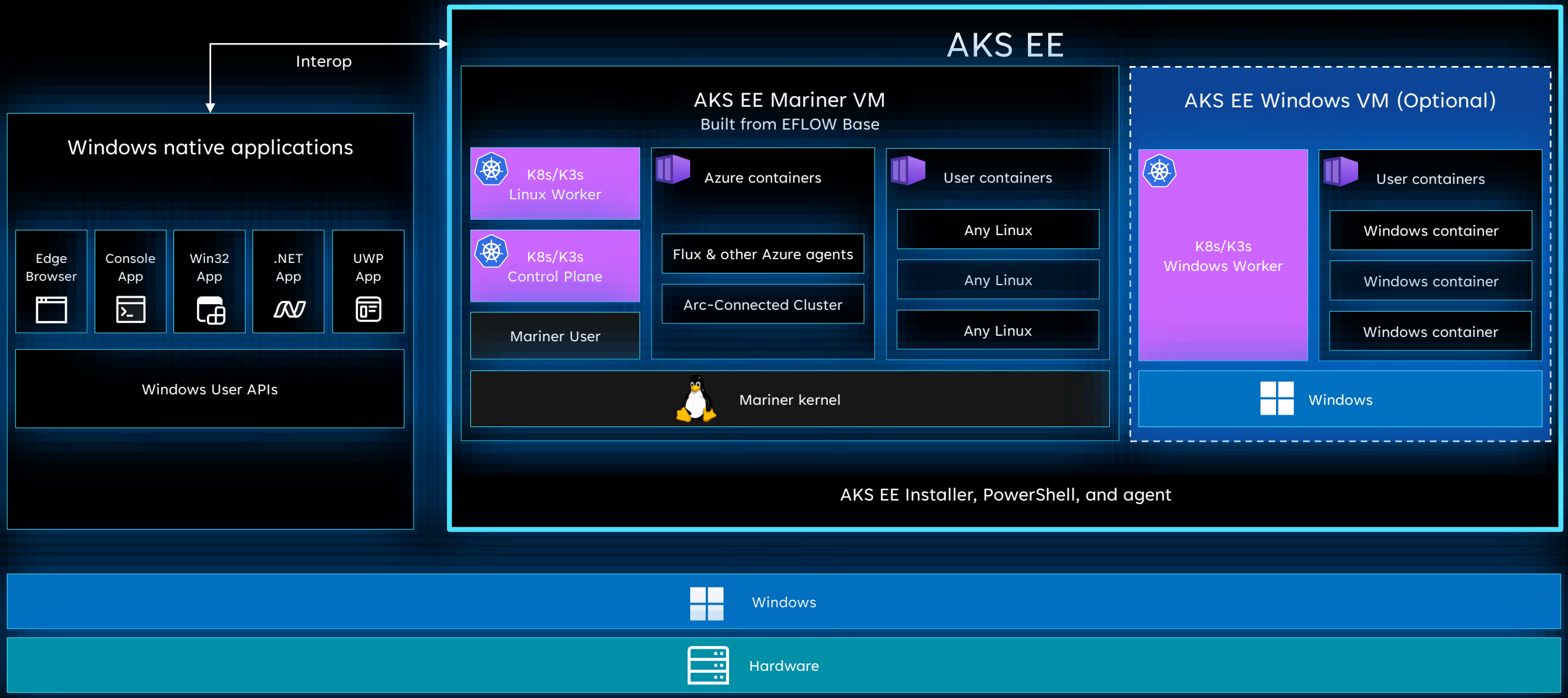
Windows 10/11 (IoT Enterprise / Enterprise / Pro) and Windows Server

Edge computing devices (with 8GB+ RAM)

Azure Kubernetes Service Edge Essentials (AKS EE) architecture

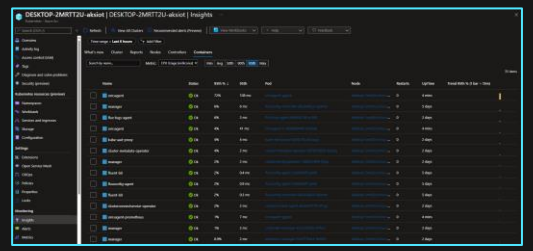


AKS Edge Essentials architecture



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

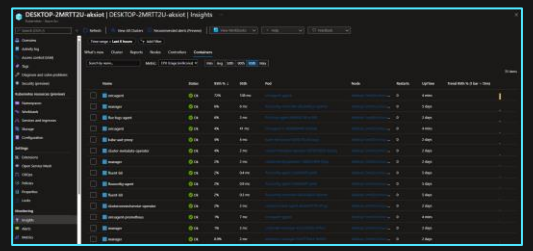
Connected via Azure Arc-enabled servers

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

From cloud to edge and back

Azure Arc

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)

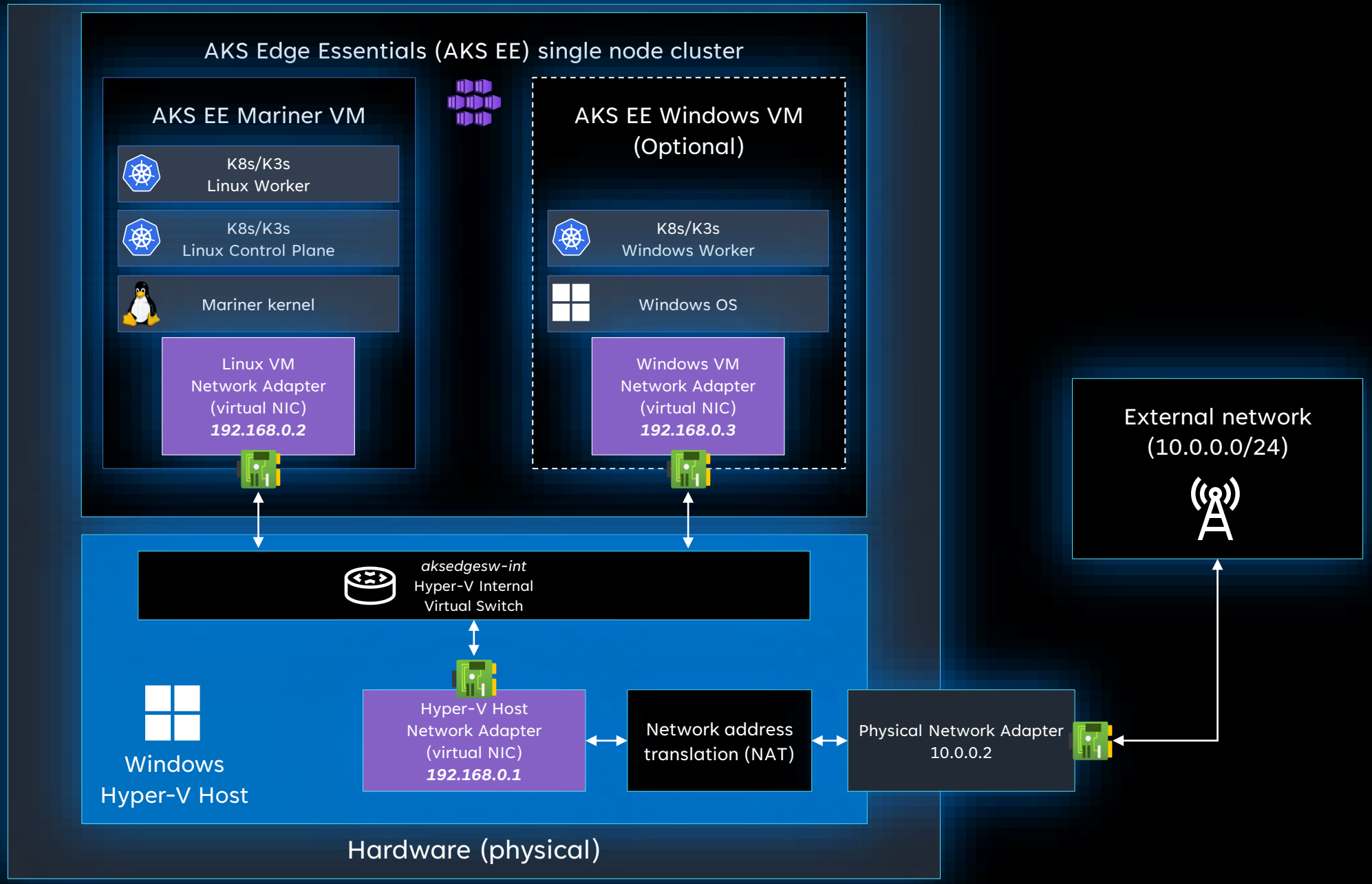
- K8s/K3s Windows Worker
- User containers
  - Windows container
  - Windows container
  - Windows container
- Windows

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

Hardware

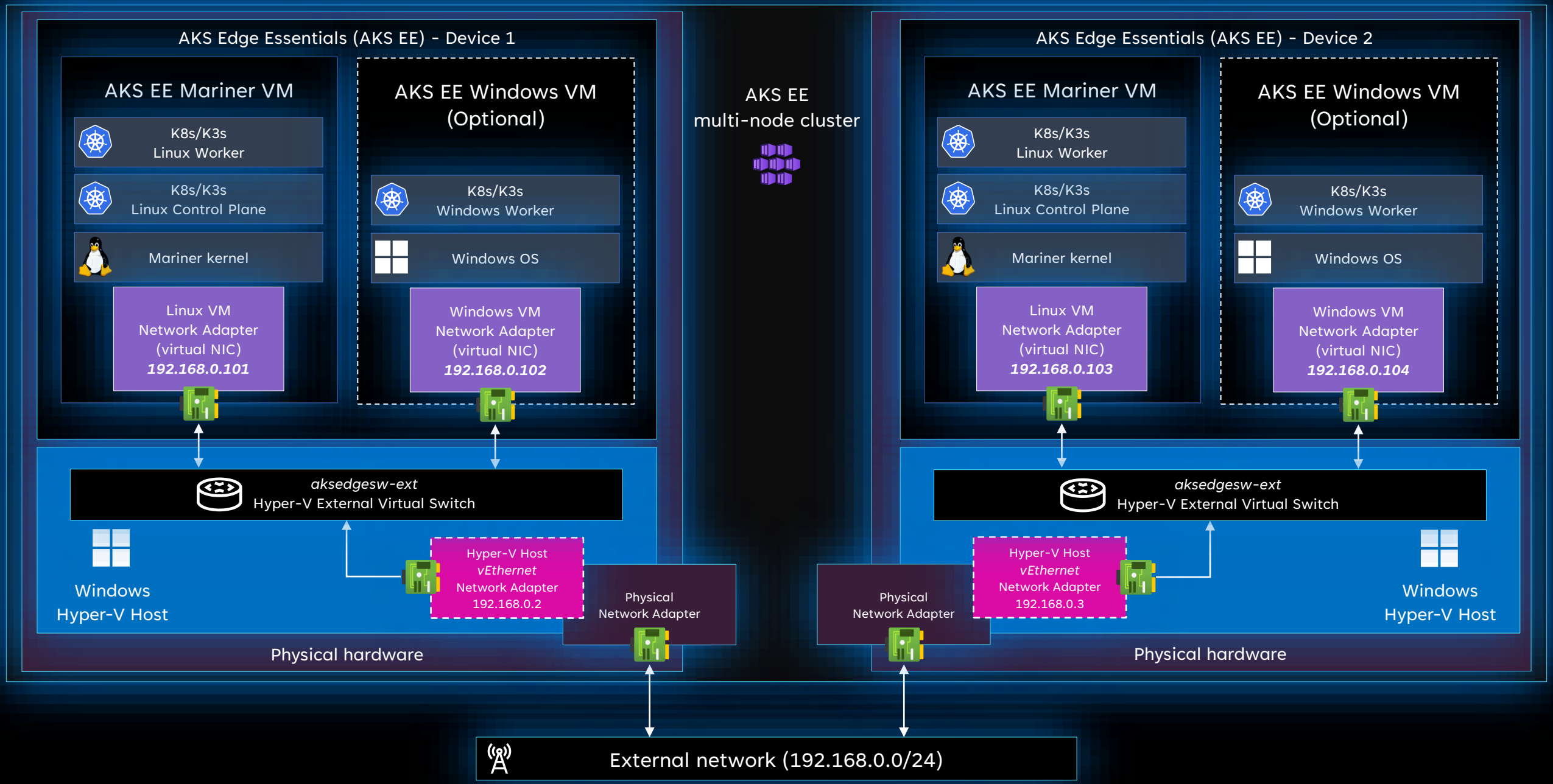
Azure Kubernetes Service Edge Essentials (AKS EE)

Single Node Cluster with Internal Virtual Switch network architecture



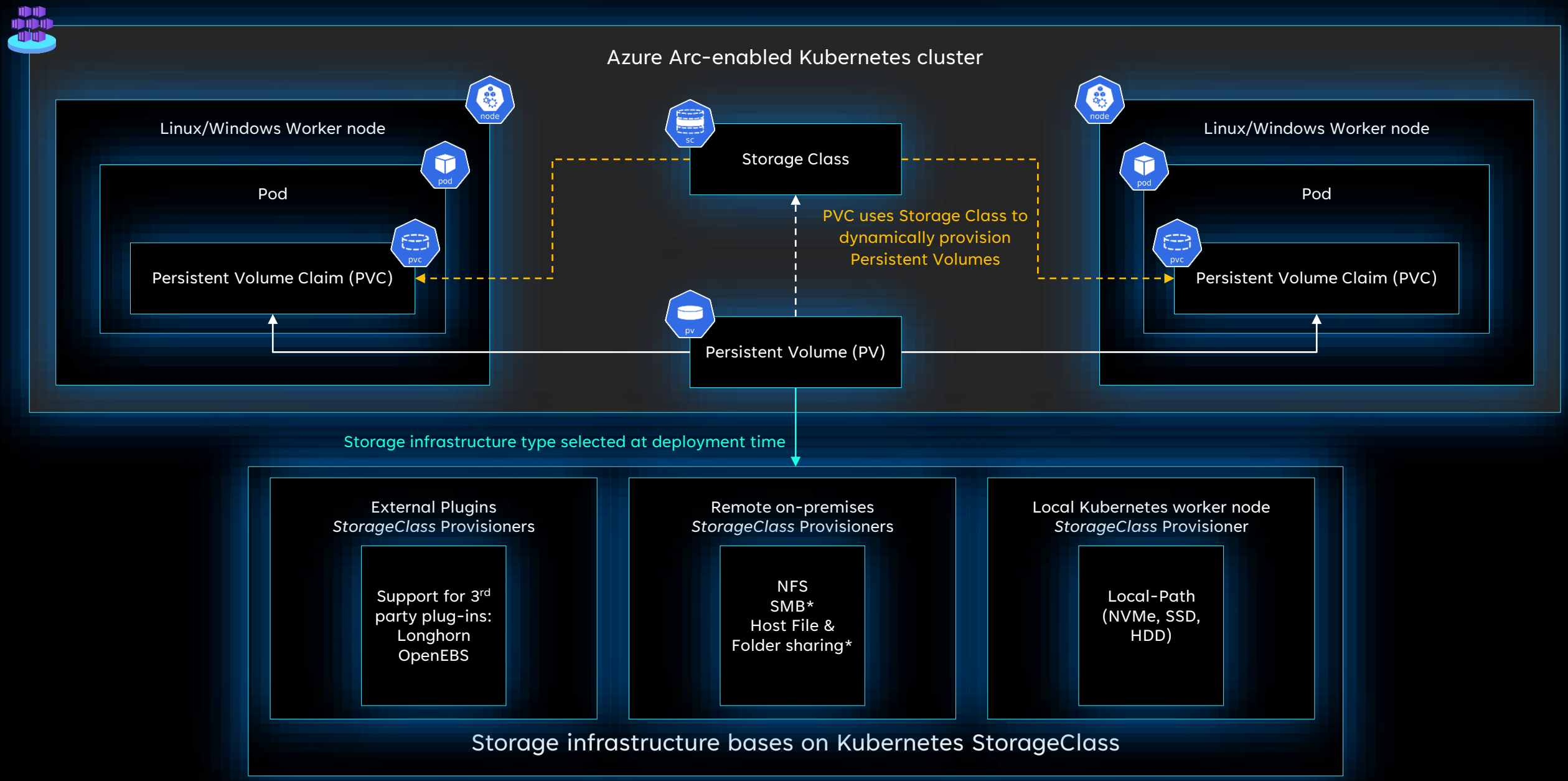
Azure Kubernetes Service Edge Essentials (AKS EE)

Multi-Machine Cluster with External Virtual Switch network architecture



Azure Kubernetes Service Edge Essentials (AKS EE)

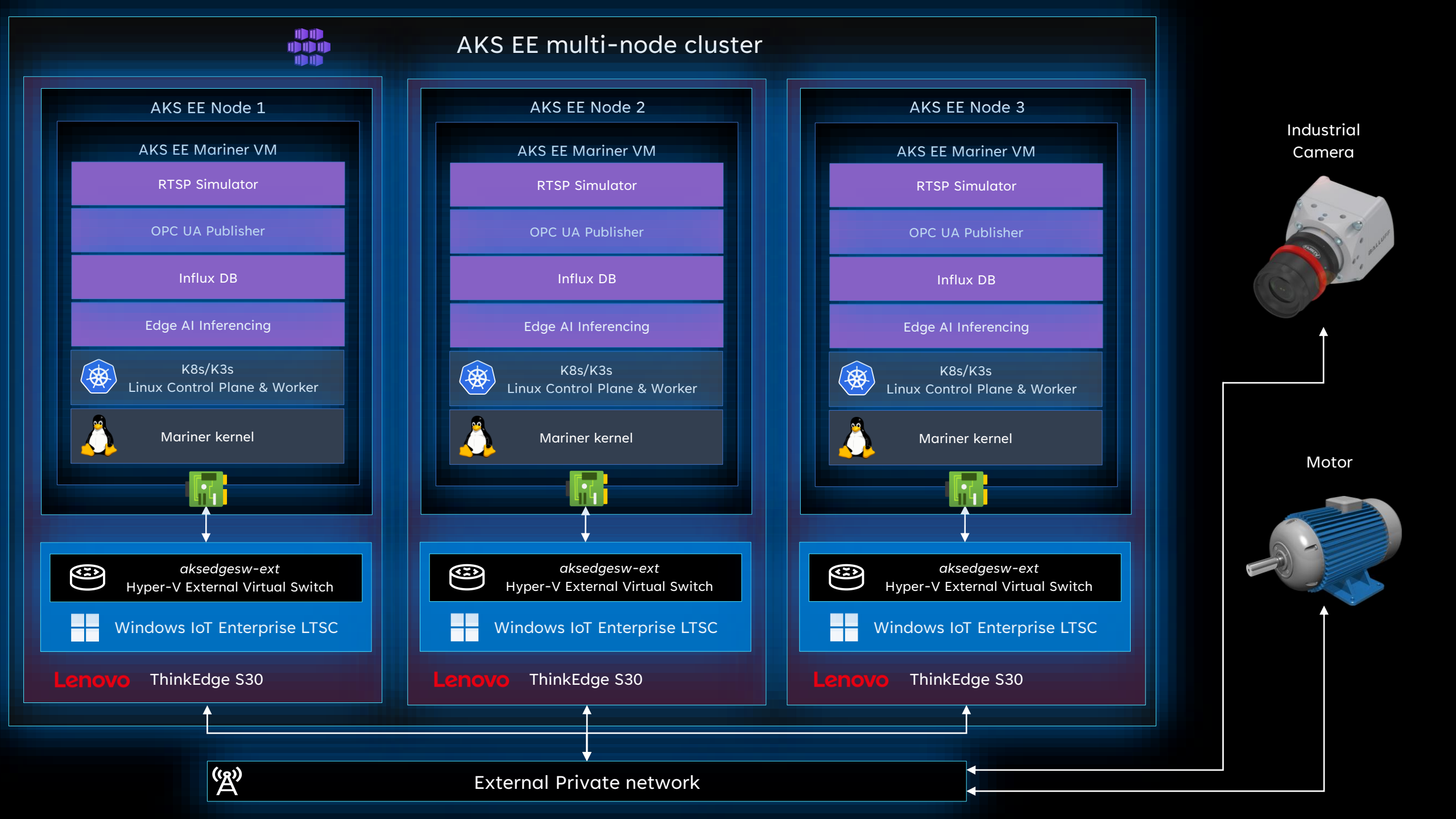
Storage options



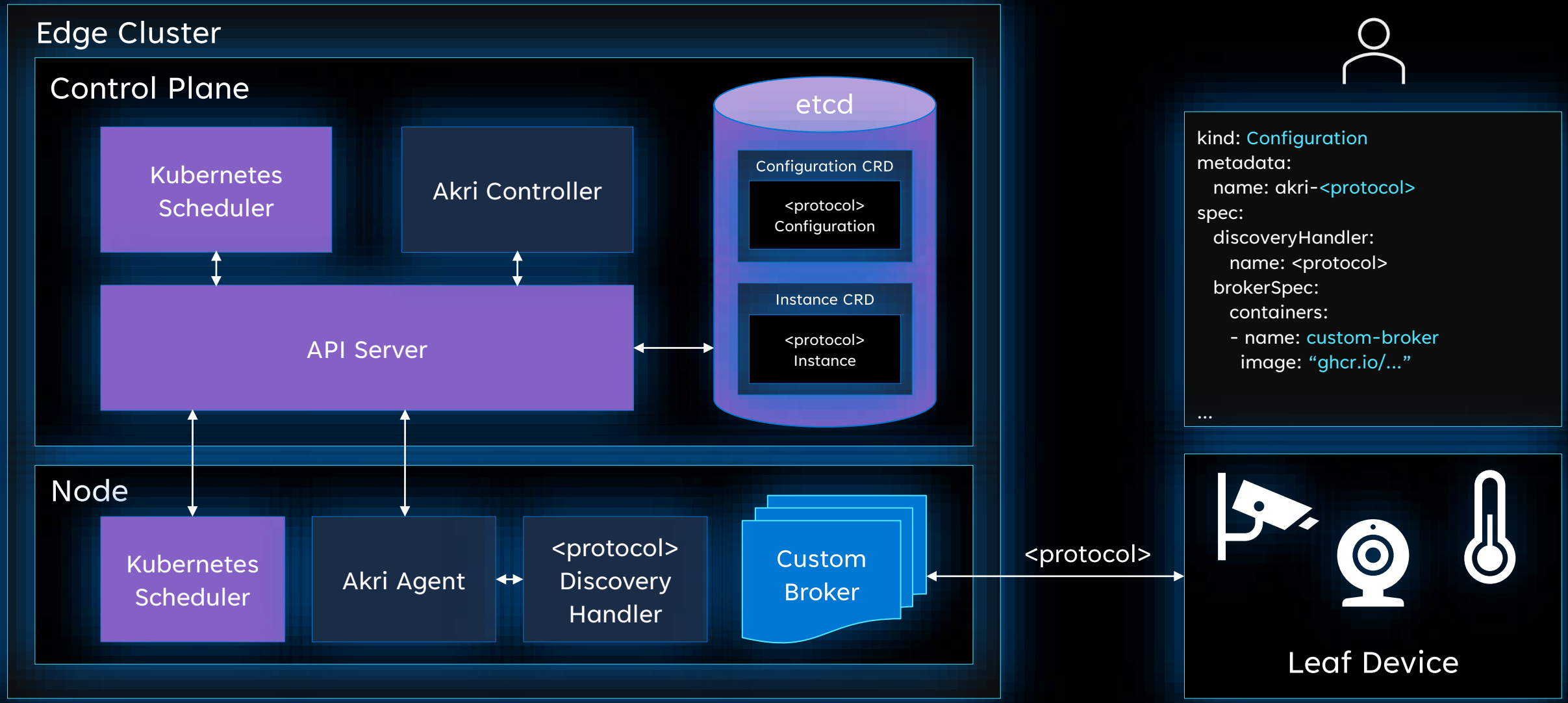
Azure Kubernetes Service Edge Essentials (AKS EE)

Networking – Comparison by deployment type

	Single Machine	Scalable Cluster
Type of Virtual switch	Internal	External
Virtual switch creation	Automatic	Automatic Based on NetAdapterName
IP address assignment	Automatic – Addresses defined	Static IP addresses
Outbound connections	Using NAT	Directly using Physical Net Adapter
Inbound connections	Not reachable	Using Node IP Address
Network Plugin	K8s – Calico K3s – Flannel	K8s – Calico K3s – Flannel
DNS	Configurable – If not provided, use Windows host DNS servers	Configurable – If not provided, use Windows host DNS servers
Proxy	Configurable – *http_proxy*, *https_proxy* & *no_proxy*	Configurable – *http_proxy*, *https_proxy* & *no_proxy*
Offline deployment	Available	Available
Service IP range	If *ServiceIPRangeSize* is defined, will start at *192.168.0.4*	Both *ServiceIPRangeStart* and *ServiceIPRangeSize* can be defined
Static MAC Address	Available	Available
Network MTU	Available	Available


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



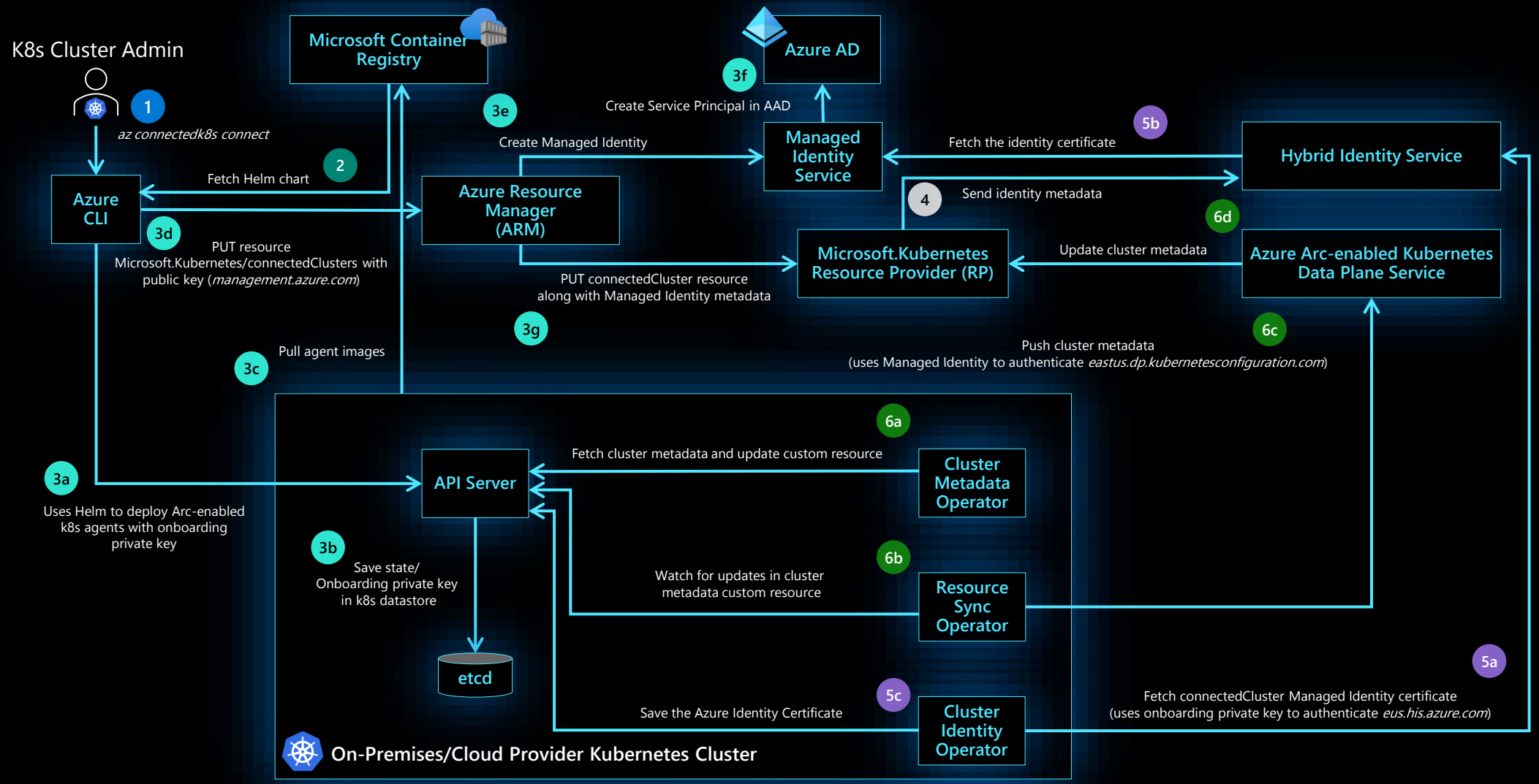
SHAc - PUBLIC

Azure Arc-enabled Kubernetes

© Copyright Microsoft Corporation. All rights reserved.

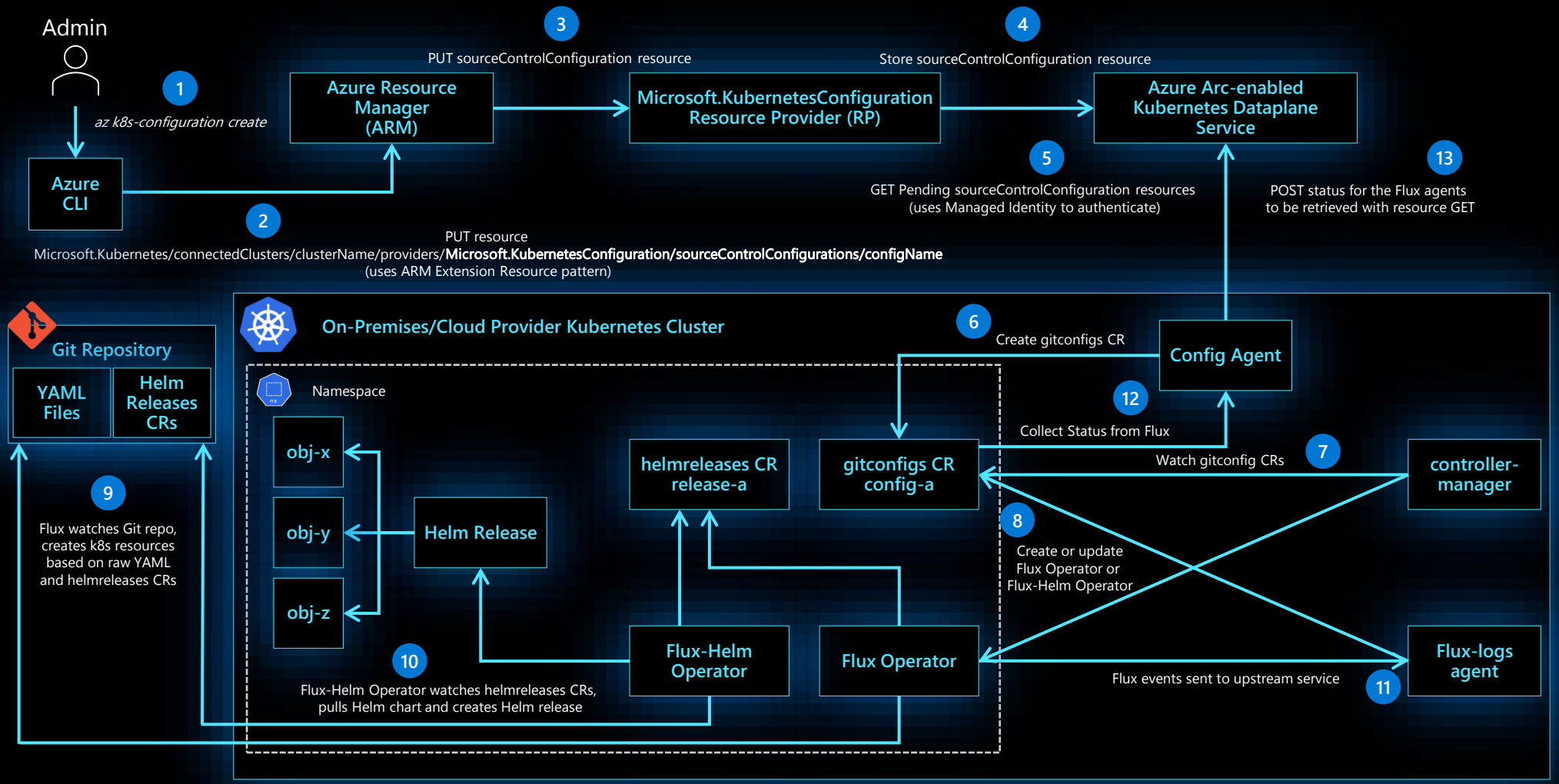
Azure Arc-enabled Kubernetes

Onboarding



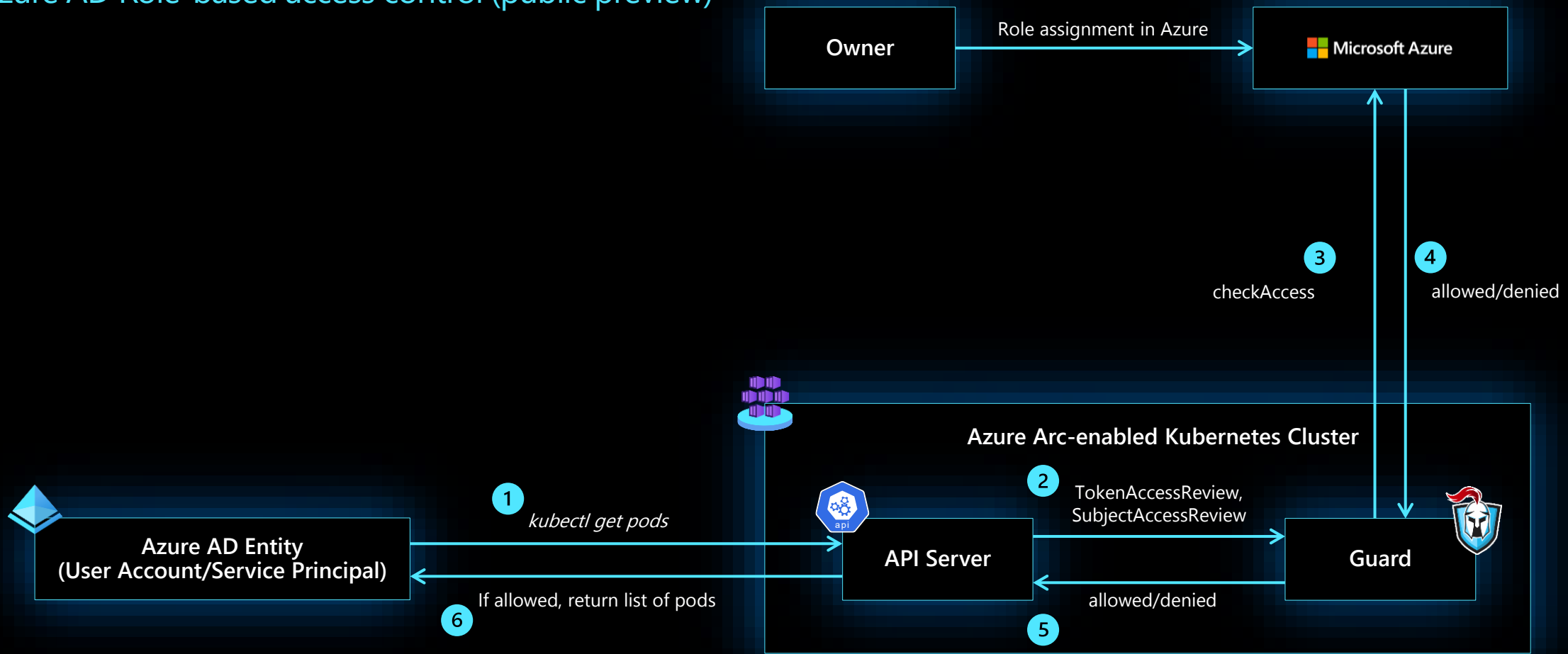
Azure Arc-enabled Kubernetes

GitOps Configuration



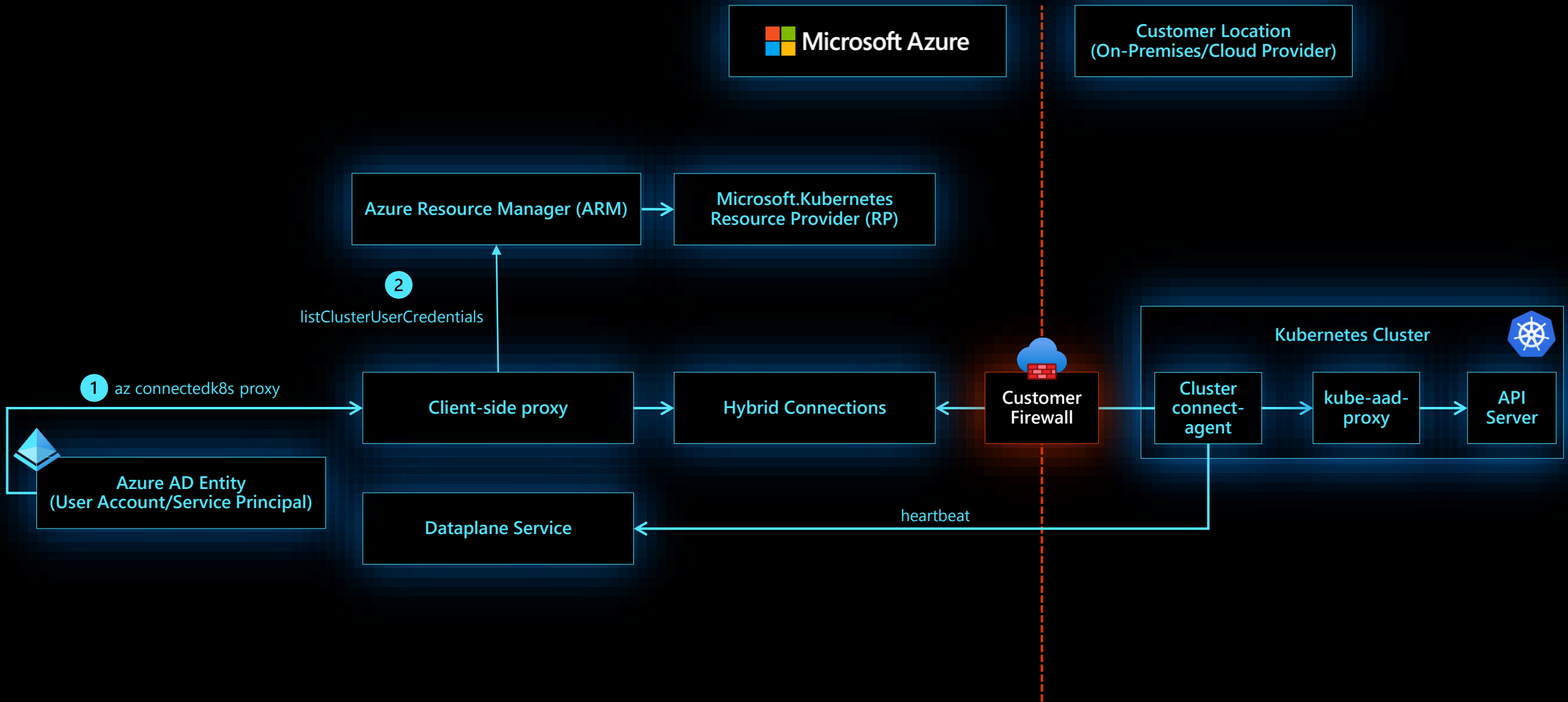
Azure Arc-enabled Kubernetes

Azure AD Role-based access control (public preview)



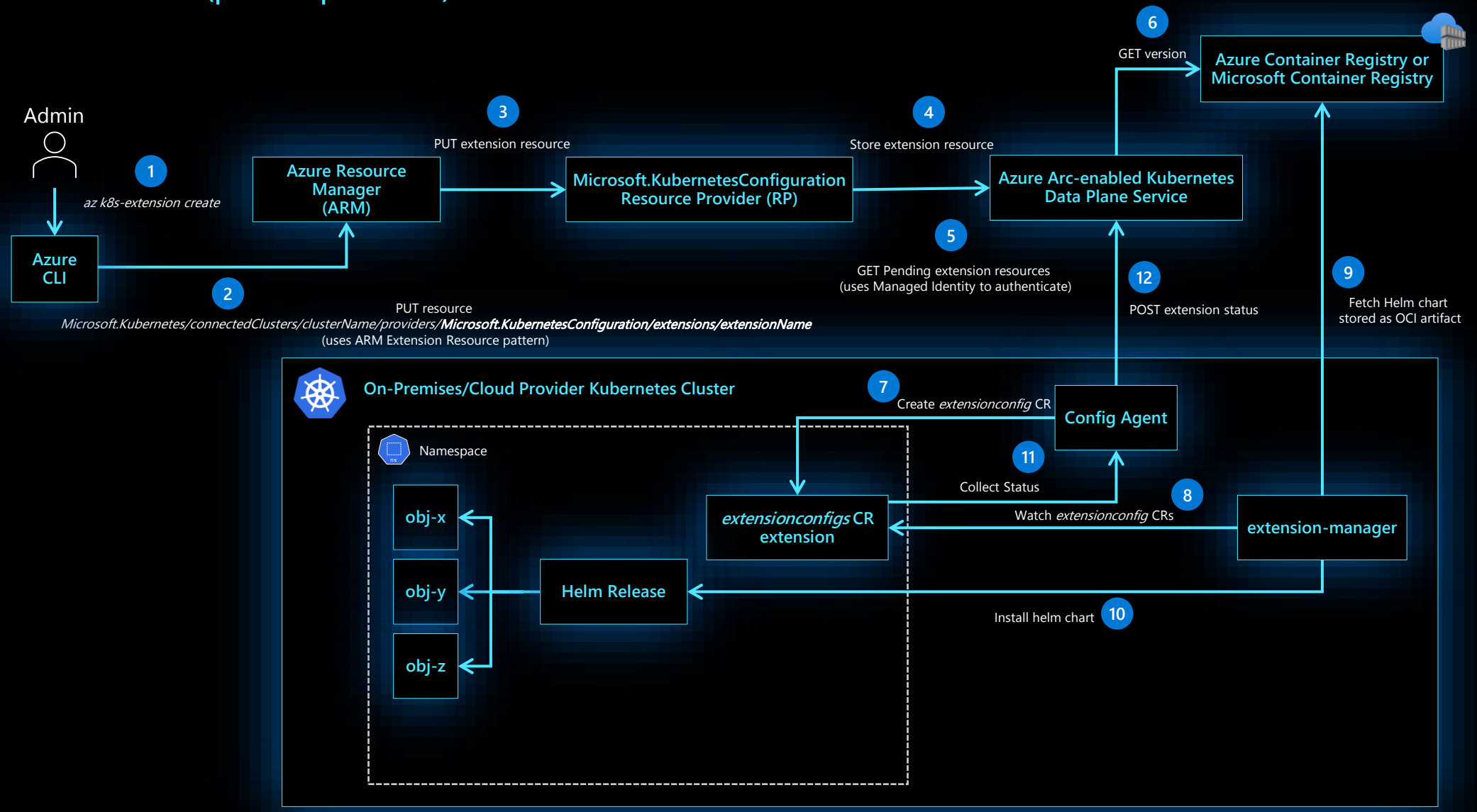
Azure Arc-enabled Kubernetes

Cluster Connect (public preview)



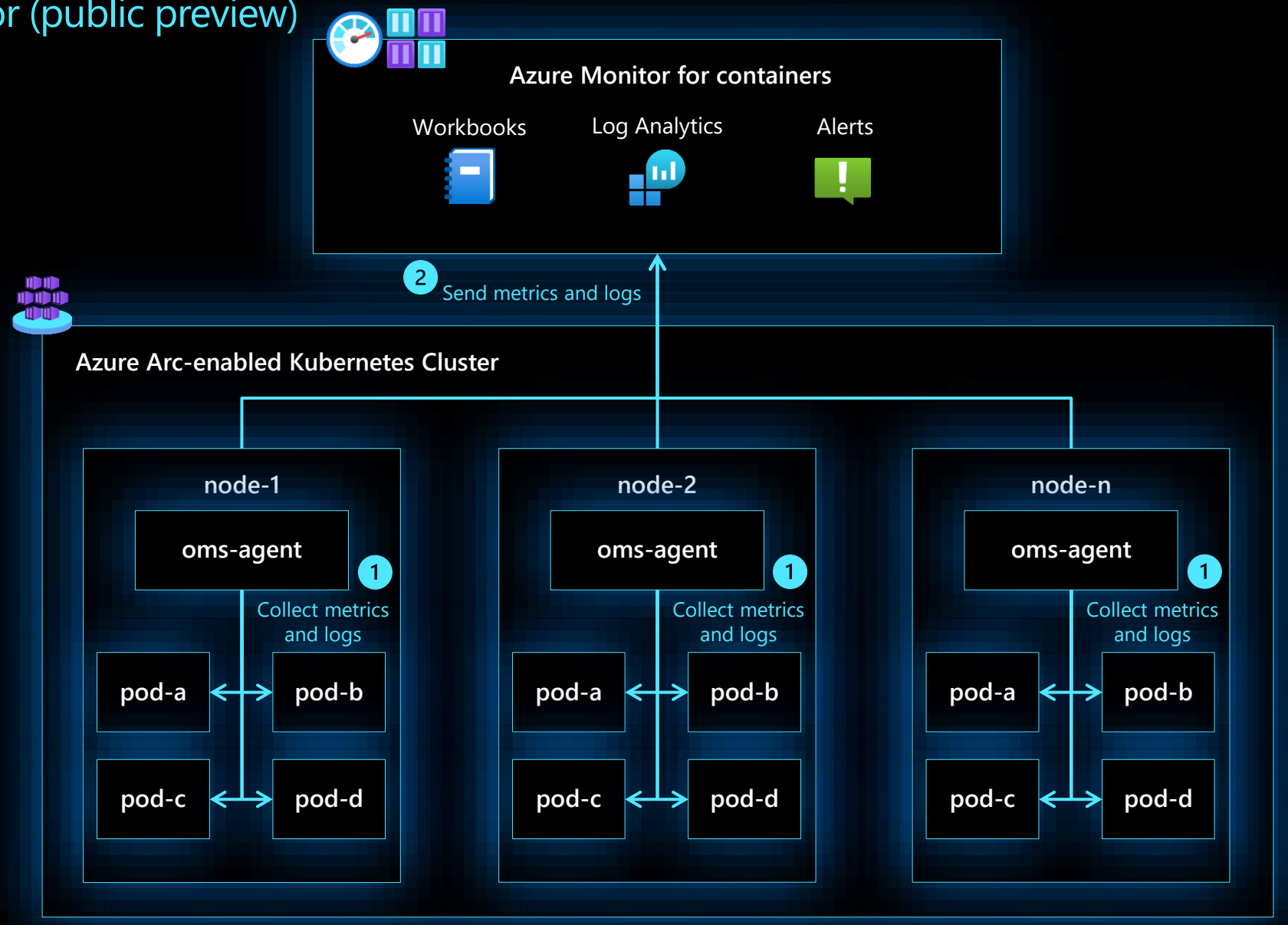
Azure Arc-enabled Kubernetes

Cluster extensions (public preview)



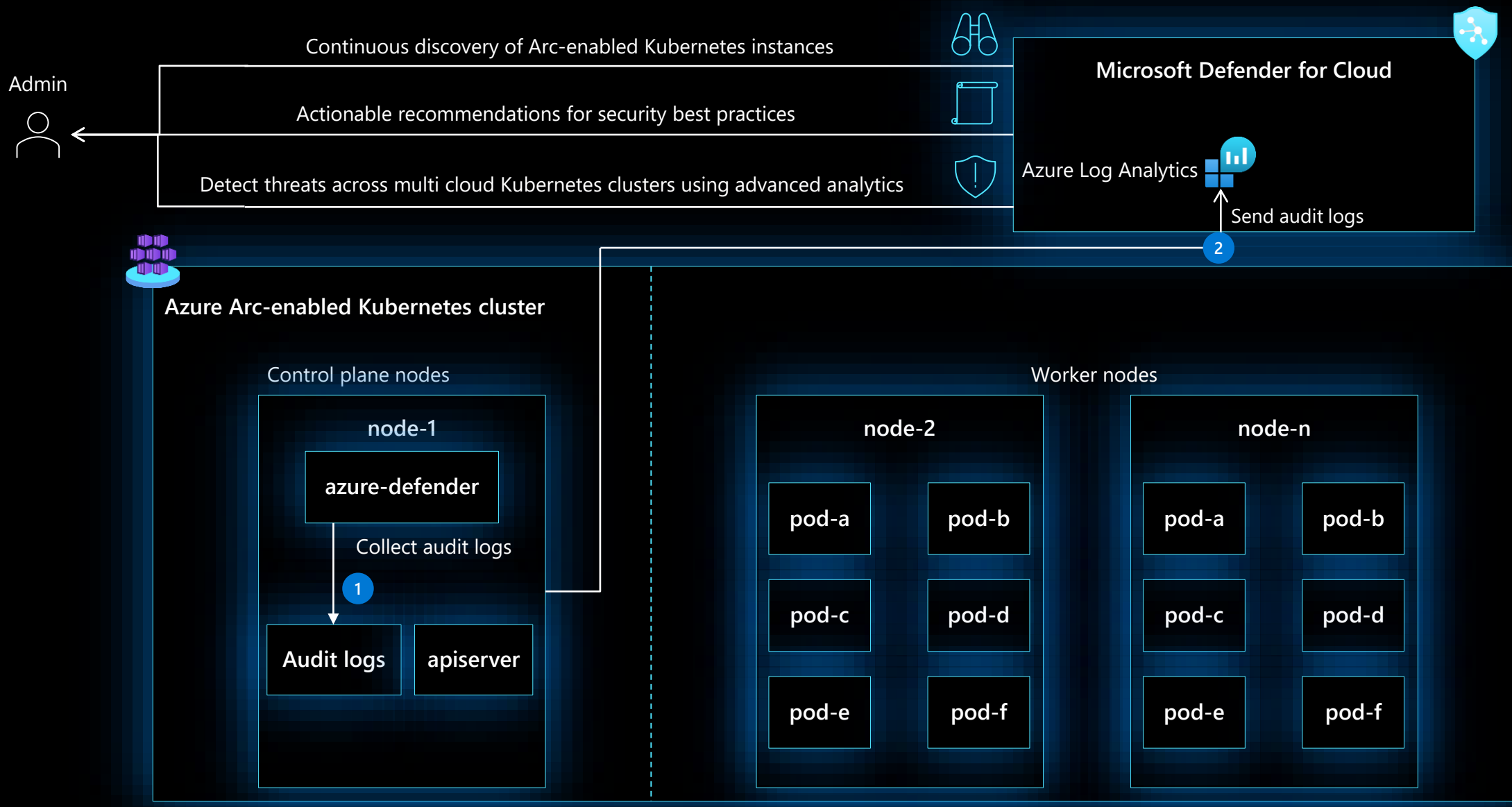
Azure Arc-enabled Kubernetes

Azure Monitor (public preview)



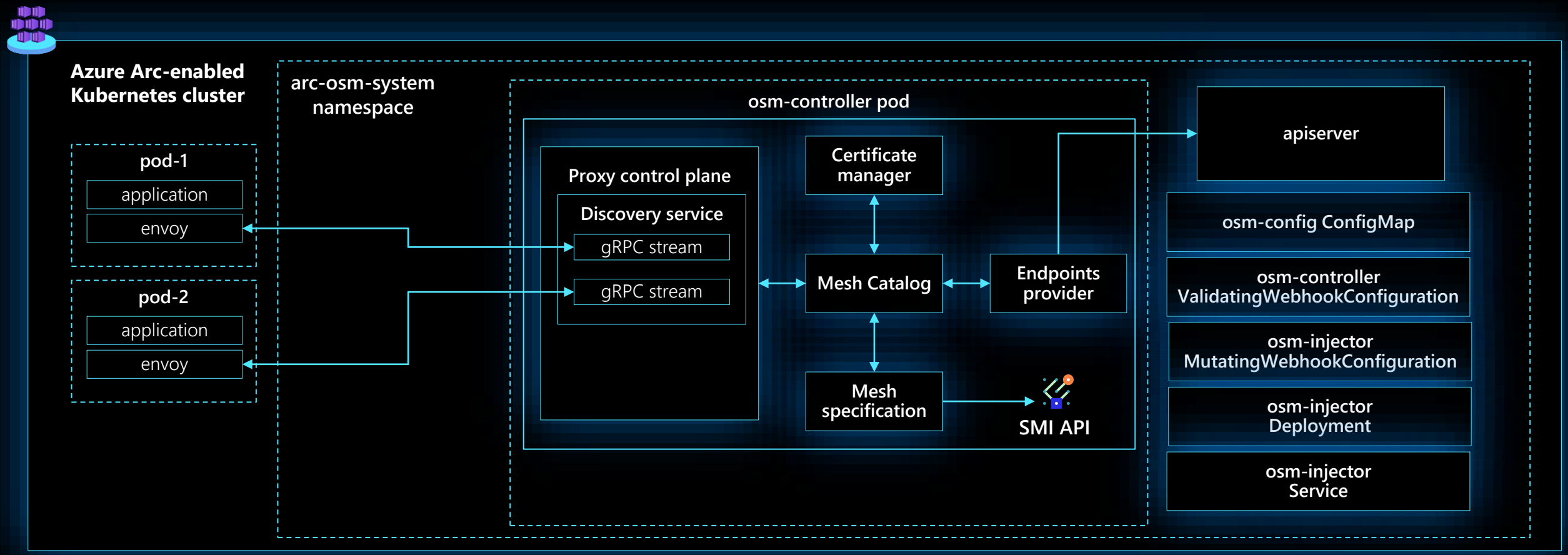
Azure Arc-enabled Kubernetes

Microsoft Defender for Cloud



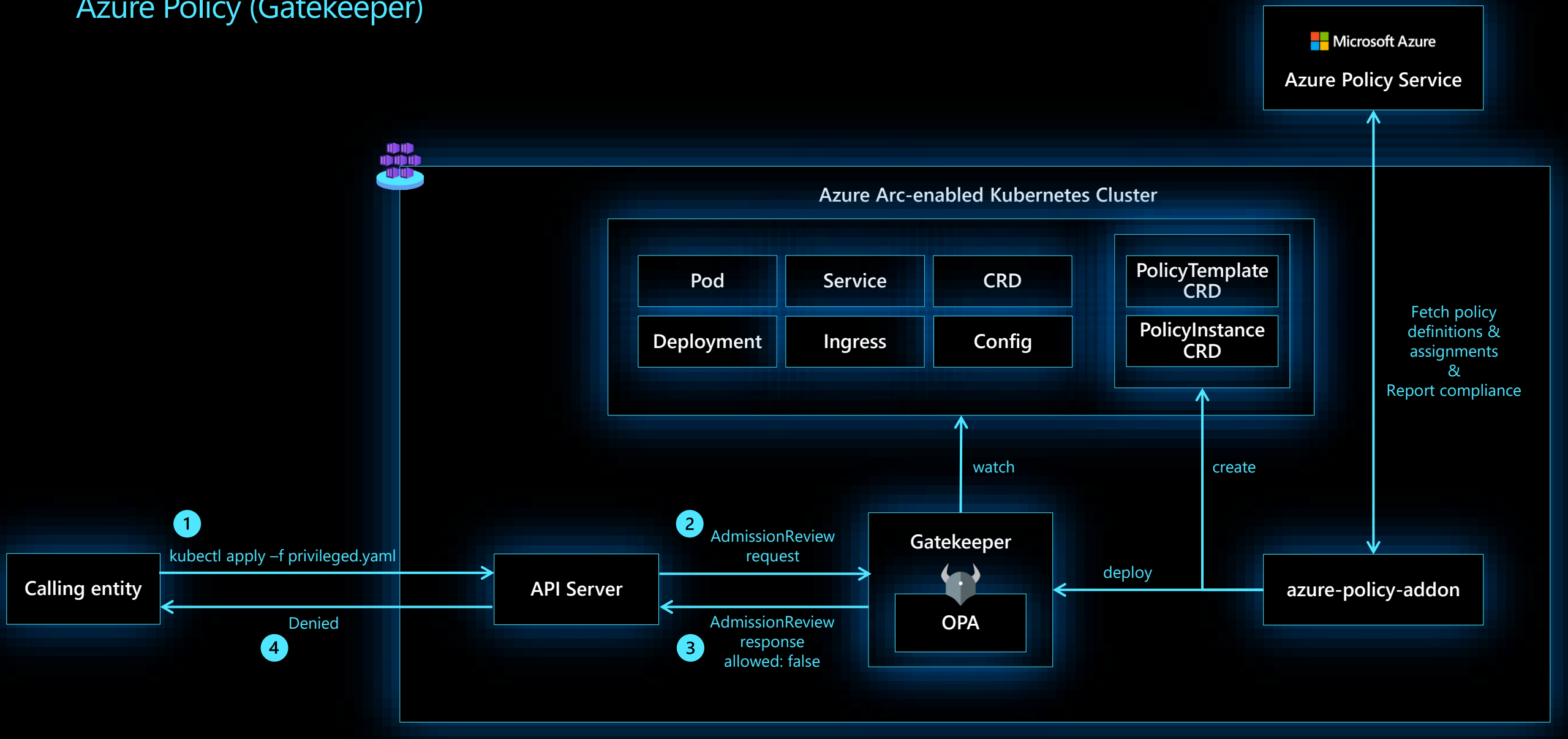
Azure Arc-enabled Kubernetes

Open Service Mesh (Preview)



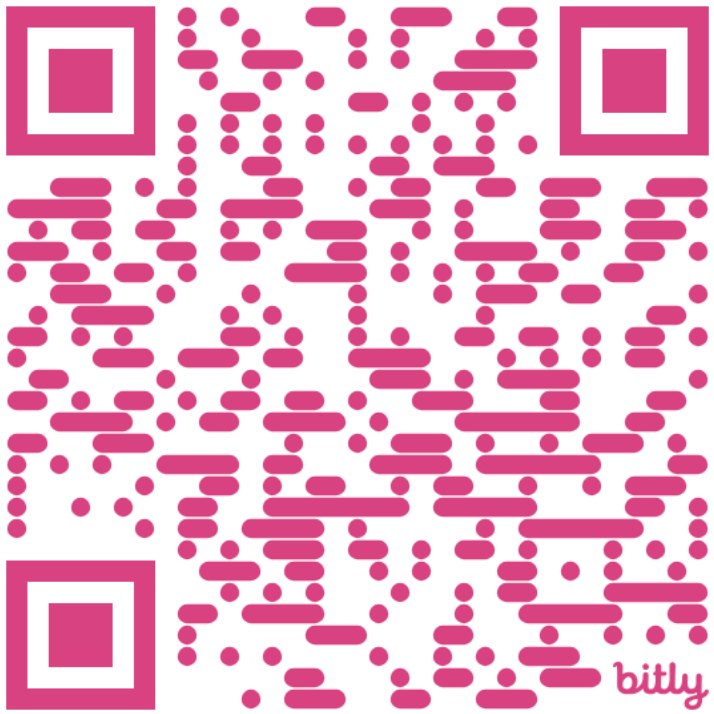
Azure Arc-enabled Kubernetes

Azure Policy (Gatekeeper)



Resources

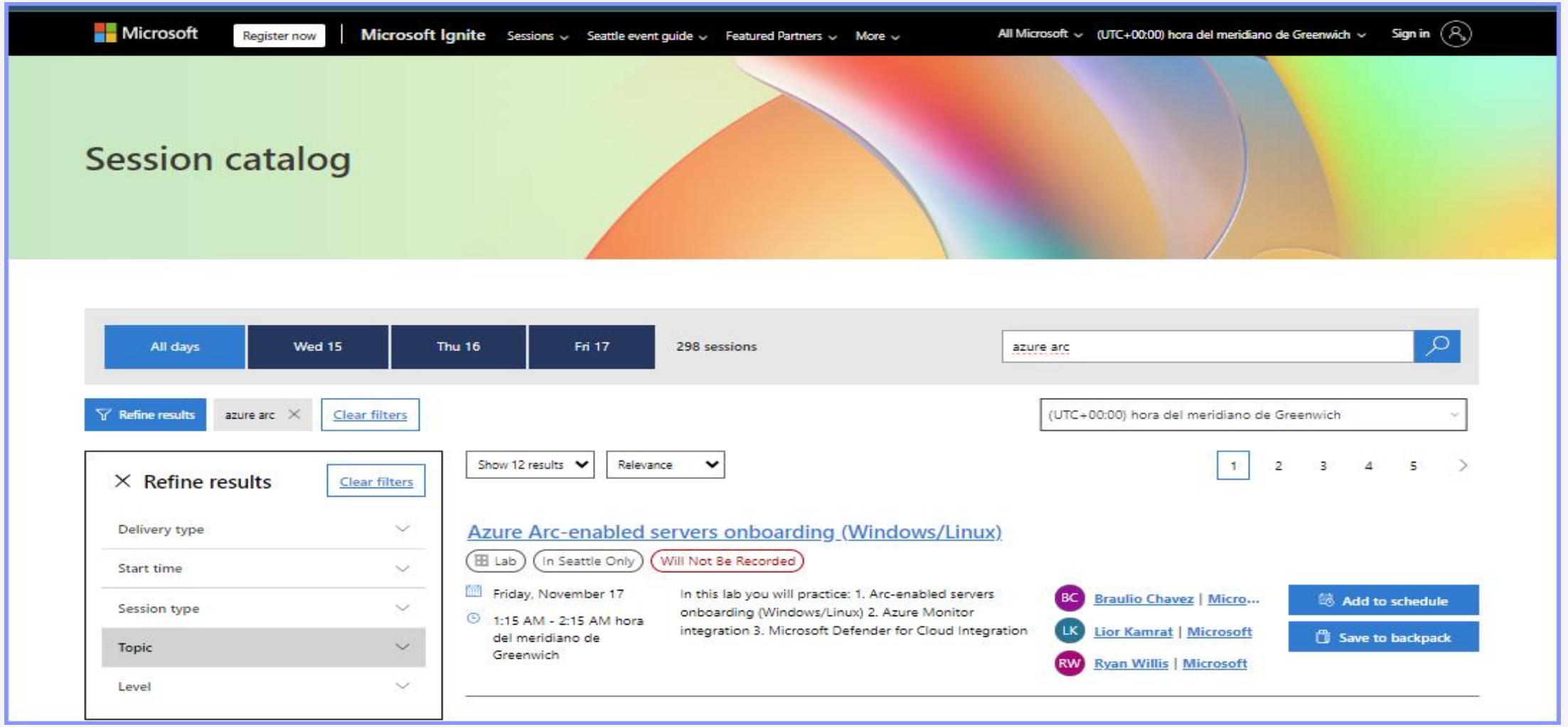
Presentations from all Webinars



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

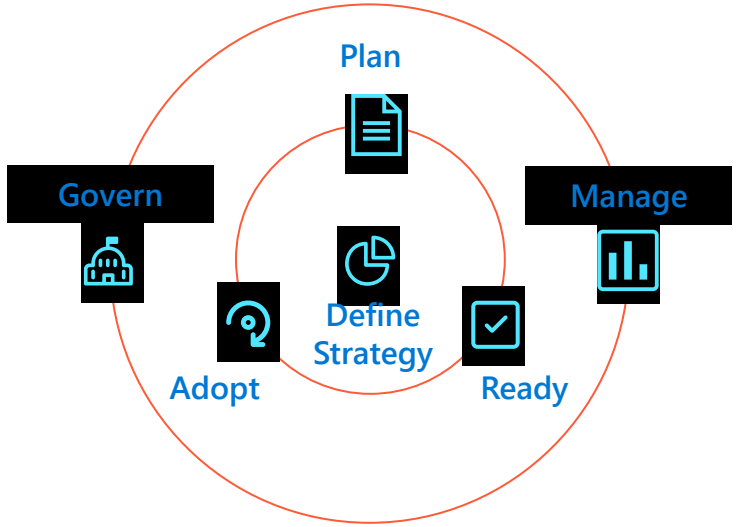
Session catalog (microsoft.com)

Microsoft Azure Arc Jumpstart

Overview | Azure Arc Jumpstart

© Copyright Microsoft Corporation. All rights reserved.

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

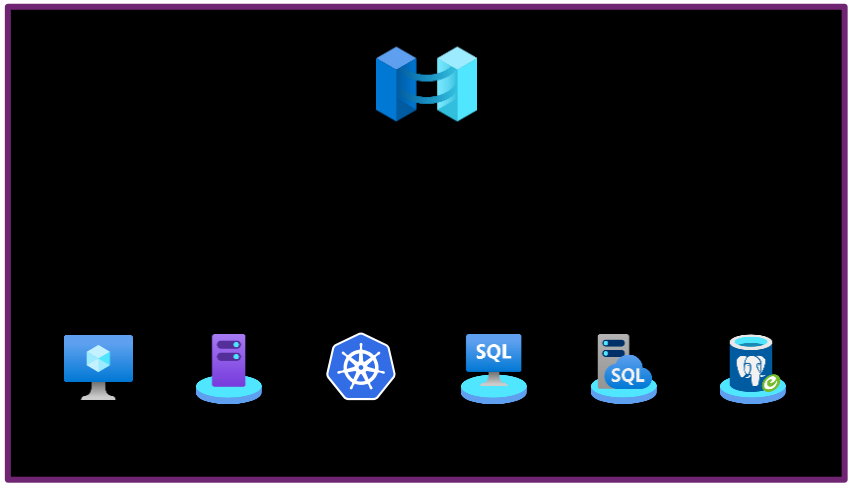
© Copyright Microsoft Corporation. All rights reserved.

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



© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Continue your journey with Azure Arc Webinar Series

Introduction for Microsoft Azure Arc for Beginners

Introduction
Features
Services
Flavors

Intermedate-Level practices with Microsoft Azure Arc

Security
Governance
Best Practices
Cost Management

Mastering Microsoft Azure Arc for Business

Advanced Features
Data Services
Miltiсloud Environmont
Multispace Environment

© Copyright Microsoft Corporation. All rights reserved.

Q & A Time (10 minutes)

© Copyright Microsoft Corporation. All rights reserved.

Let’s look for the questions!

© Copyright Microsoft Corporation. All rights reserved.

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]

© Copyright Microsoft Corporation. All rights reserved.

Microsoft

Thank You for spending time with us!

© Copyright Microsoft Corporation. All rights reserved.