



# Microsoft Azure Arc Webinar Series

Webinar THREE:  
Mastering Microsoft Azure Arc for Business



- 
- ❖ Introduction (5 min)
  - ❖ Recap of Webinar One & Two (5 minutes)
  - ❖ Infrastructure as a Code with Azure Arc (20 minutes)
  - ❖ Monitoring and Analytics (30 minutes)
  - ❖ Refreshment Break (10 minutes)
  - ❖ Disaster Recovery & High Availability (25 minutes)
  - ❖ Future Roadmap and Upcoming Features (15 minutes)
  - ❖ Q&A Time (10 minutes)

# Introduction

(5 minutes)

# About the Webinar

Venture into the advanced realms of Microsoft Azure Arc in this expert-led webinar.

After recapping key takeaways from the initial sessions, delve into Infrastructure as Code with Azure Arc.

Stay updated with Azure Arc's future roadmap and how to get involved more deeply with the platform.

Discover monitoring and analytics capabilities, alongside vital information on ensuring business continuity with Azure Arc.

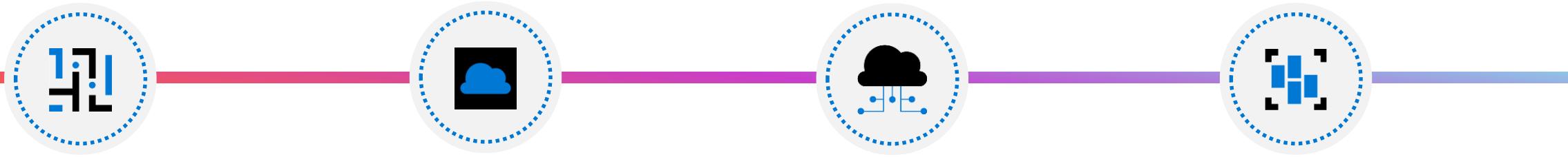
Equipping yourself with the skills to deploy and manage resources seamlessly.

This advanced session is perfect for those ready to master Azure Arc's complexities and potentials, capped with a dedicated Q&A time.

# Recap of Webinars One & Two

(5 minutes)

# Quick overview of previous webinar content [Webinar ONE]



## What is Microsoft Azure Arc?

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

## Basics of Installation & Configuration

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

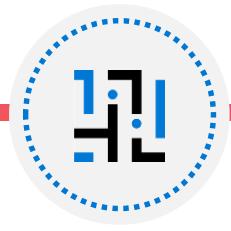
## Overview & Flavors of Azure Arc Services

- 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

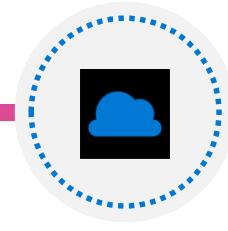
- How to manage and organize resources
- Fundamentals of Governance and management

# Quick overview of previous webinar content [Webinar TWO]



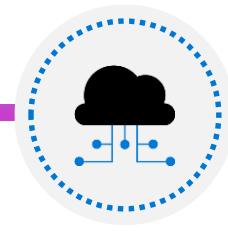
## Advanced configuration and management

- How to manage multiple clusters
- Policy Enforcement
- Governance in complex environments



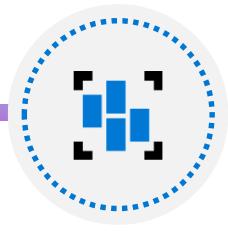
## Cost Management

- Optimisation
- Cost Prediction
- Azure Hybrid Benefits
- Extended Security Updates



## Security Considerations

- Microsoft Security Approach
- Identity & RBAC
- Best Practices
- Building Great Foundation with Planning



## Advanced Azure Arc Features

- Azure Kubernetes Service (AKS) with Edge Essentials
- Azure Arc-enabled Kubernetes Anywhere

# Infrastructure as Code with Azure Arc

(20 minutes)

# 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



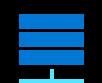
Serverless



Diverse infrastructure



Datacenters



Hosters



Branch offices



OEM hardware



IoT devices



Edge

Hybrid & Multi-Cloud

**Microsoft Azure****Alibaba Cloud****Google Cloud****vmware®****IBM Cloud**

# Introduction to Infrastructure as Code concepts

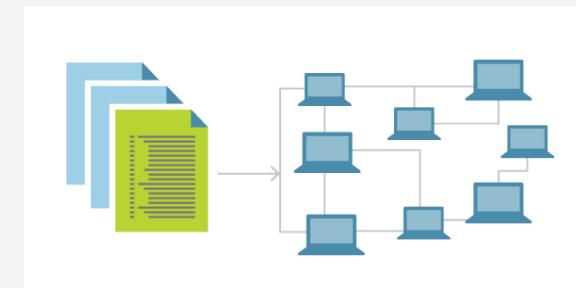
**Infrastructure as code (IaC)** uses **DevOps** methodology and versioning with a descriptive model to define and deploy infrastructure, such as networks, virtual machines, load balancers, and connection topologies. Just as the same source code always generates the same binary, an IaC model generates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

(30 minutes)

# 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

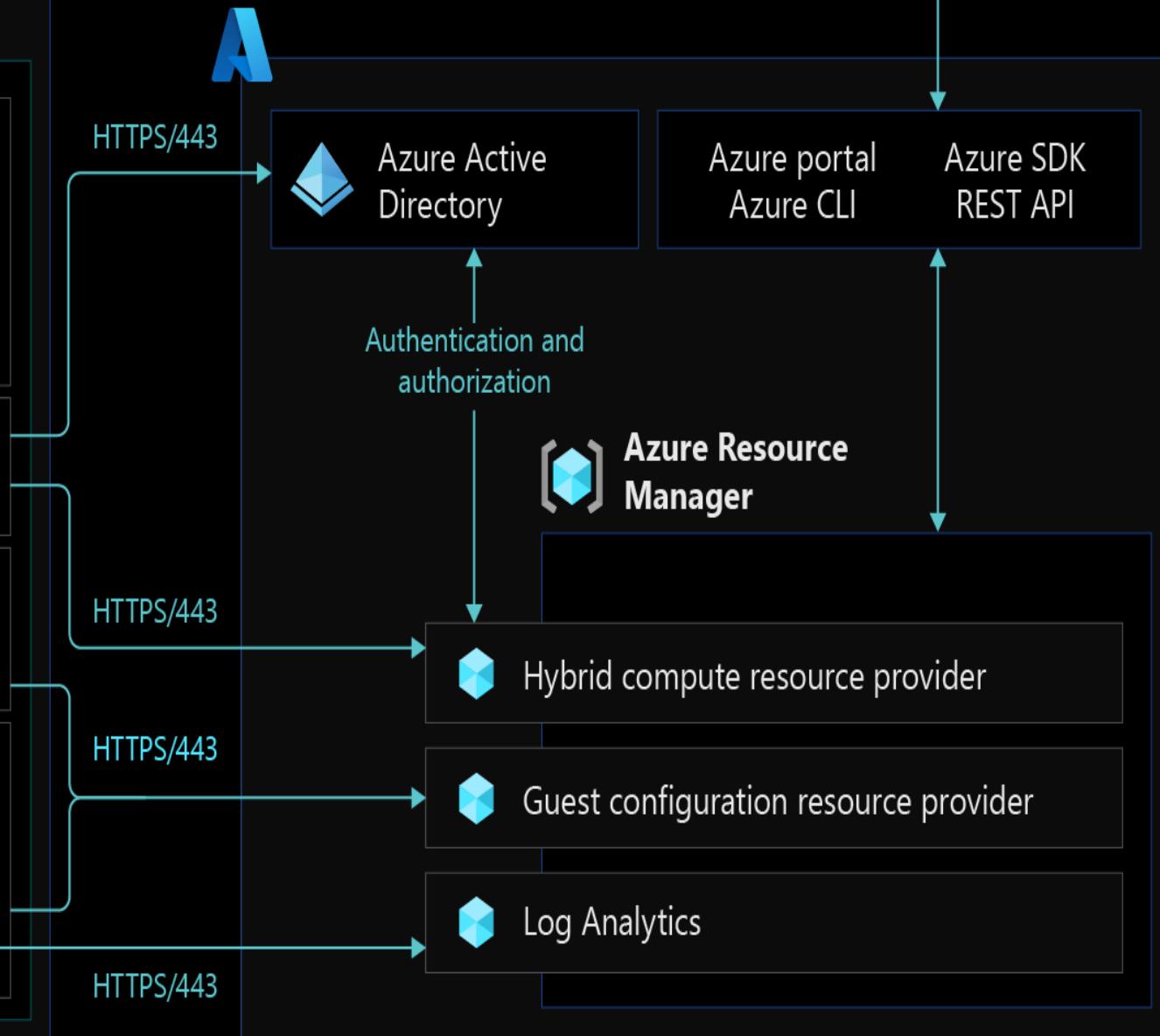
### Extension manager

Manages VM extensions, including install, uninstall, and upgrade

Custom script

ASC

MMA/AMA



# 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



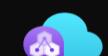
Azure Arc-enabled servers onboarding

Multicloud and On-premises servers



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

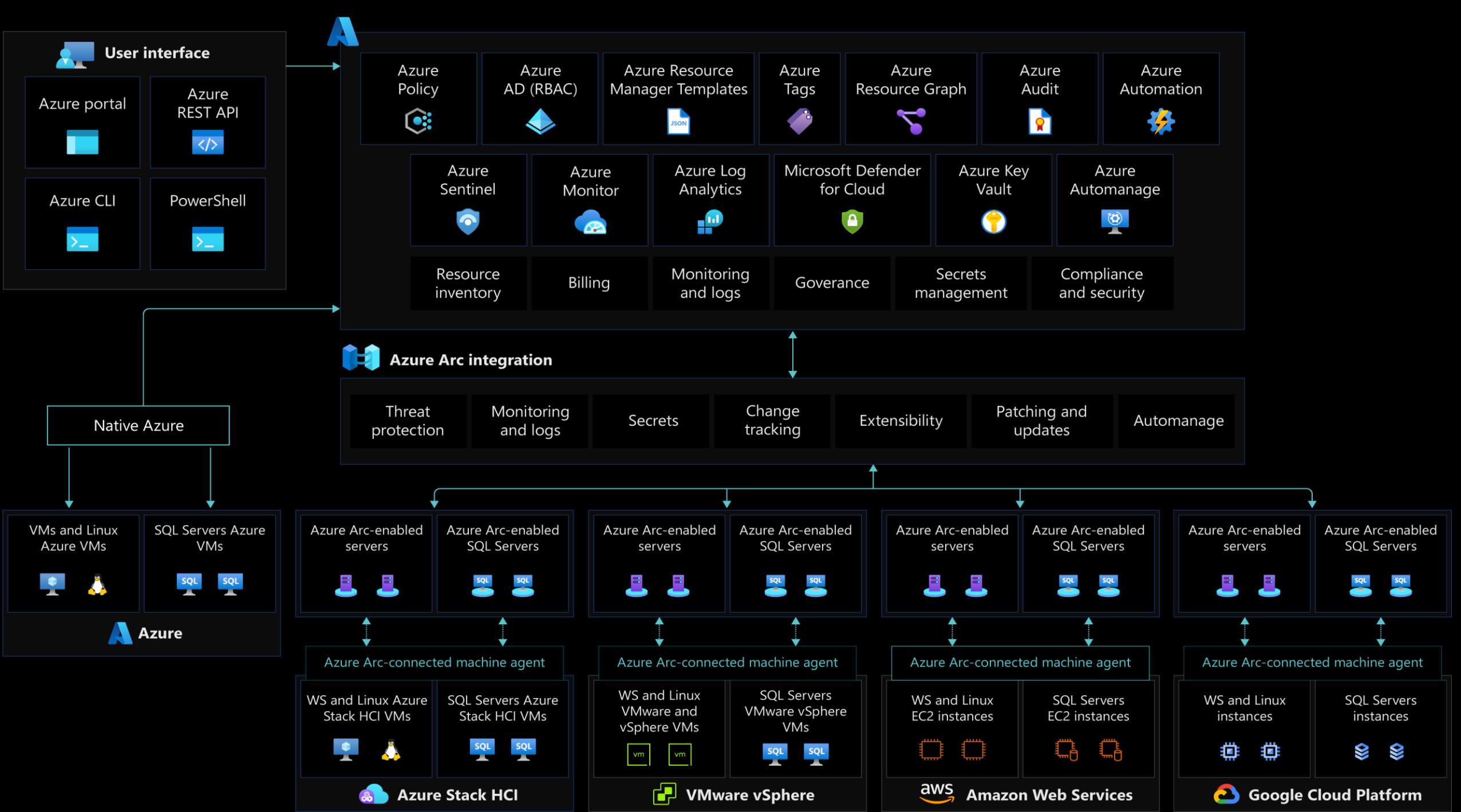
One of your first tasks will be to onboard your fleet of servers and virtual machines to Azure. After [generating an installation script](#), if you only have a few servers, you can opt to run the script directly from your [Windows](#) or [Linux](#) machines. For larger fleets of servers, there are several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

We recommend 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



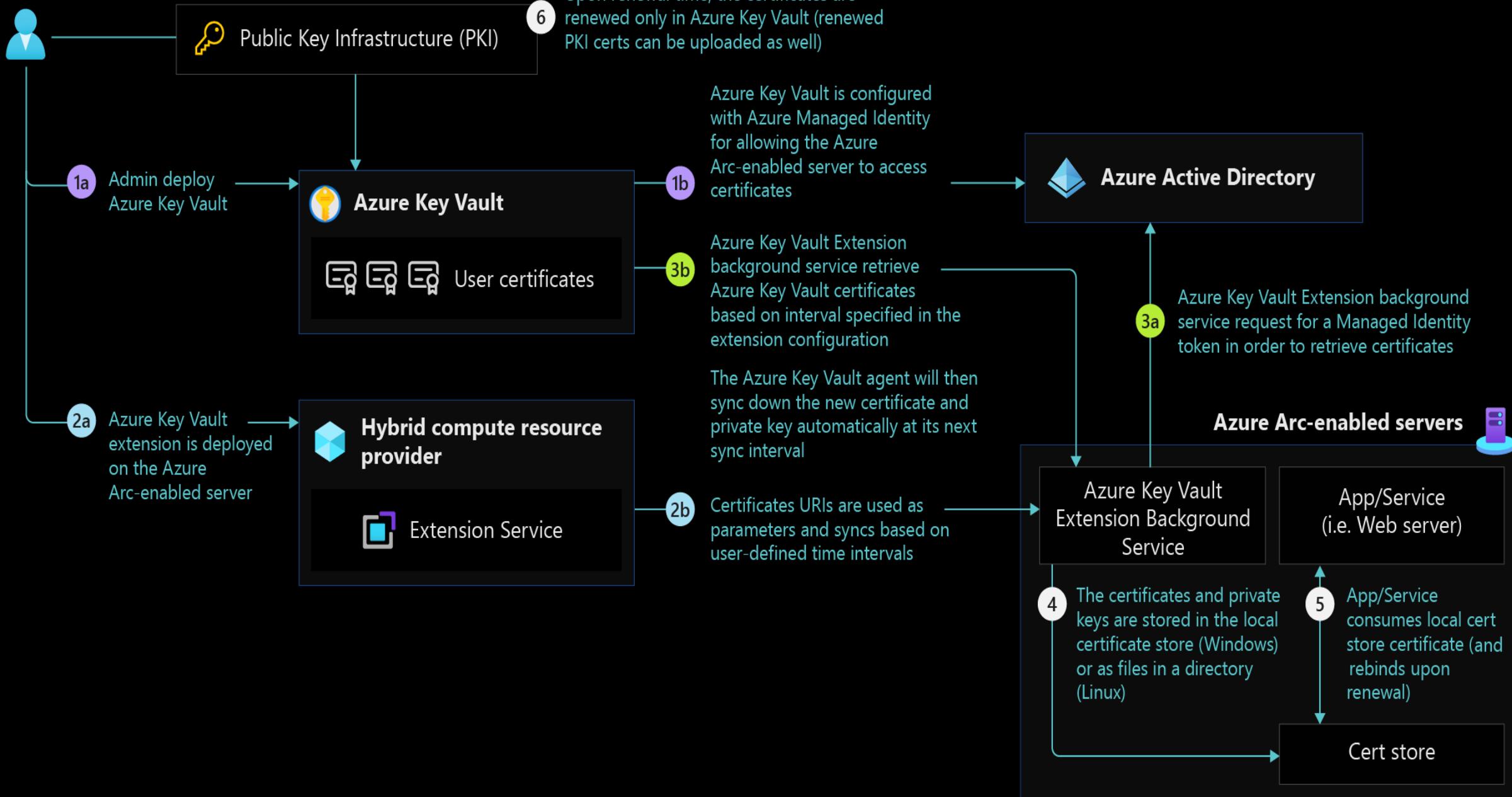
# Azure Arc | Security Discipline // considerations

## 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



# 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.

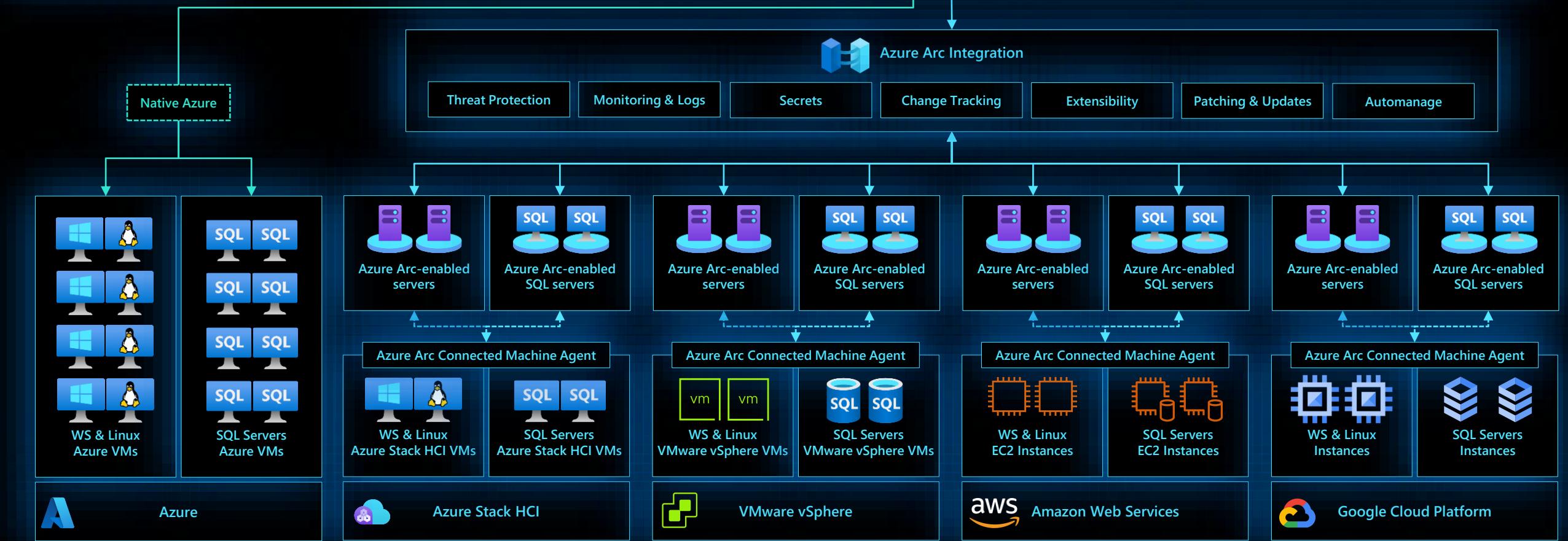
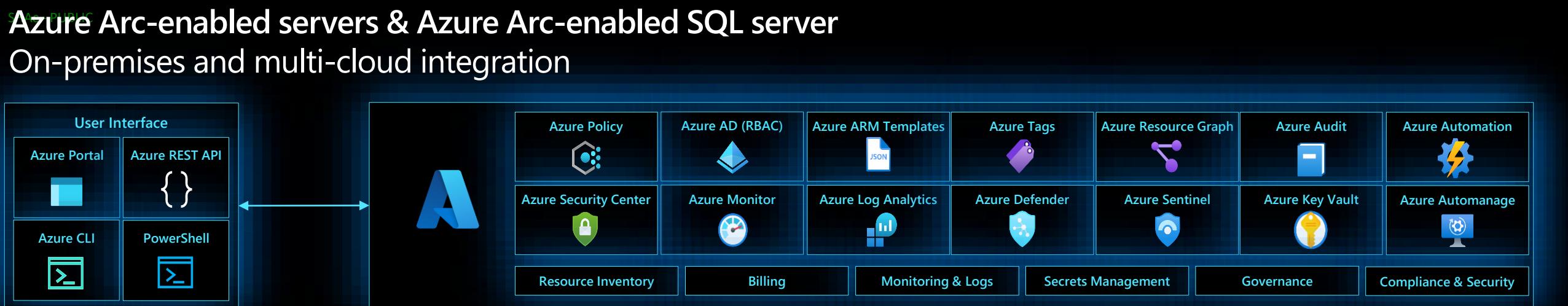
However, the cloud has introduced a new approach to IT governance with automated guardrails and checks. [Azure Policy](#) and [Microsoft Defender for Cloud](#) are cloud-native tools that allow the implementation of these controls, reports, and remediation tasks in an automated fashion.

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



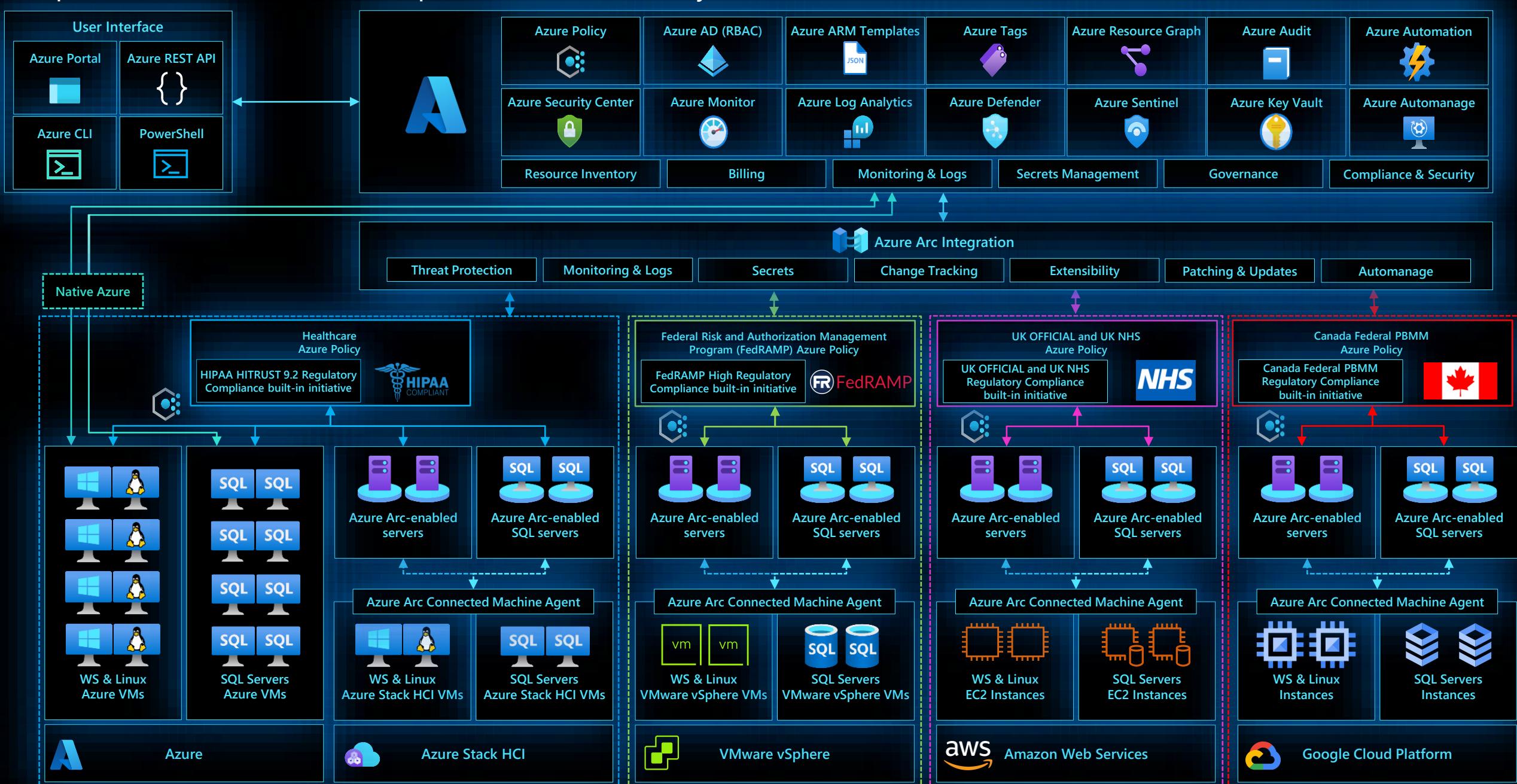
Hey Bing:  
Create Refreshment Break





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

## On-premises and multi-cloud compliance with Azure Policy









# Disaster Recovery, High Availability & Chaos

(25 minutes)

# 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.

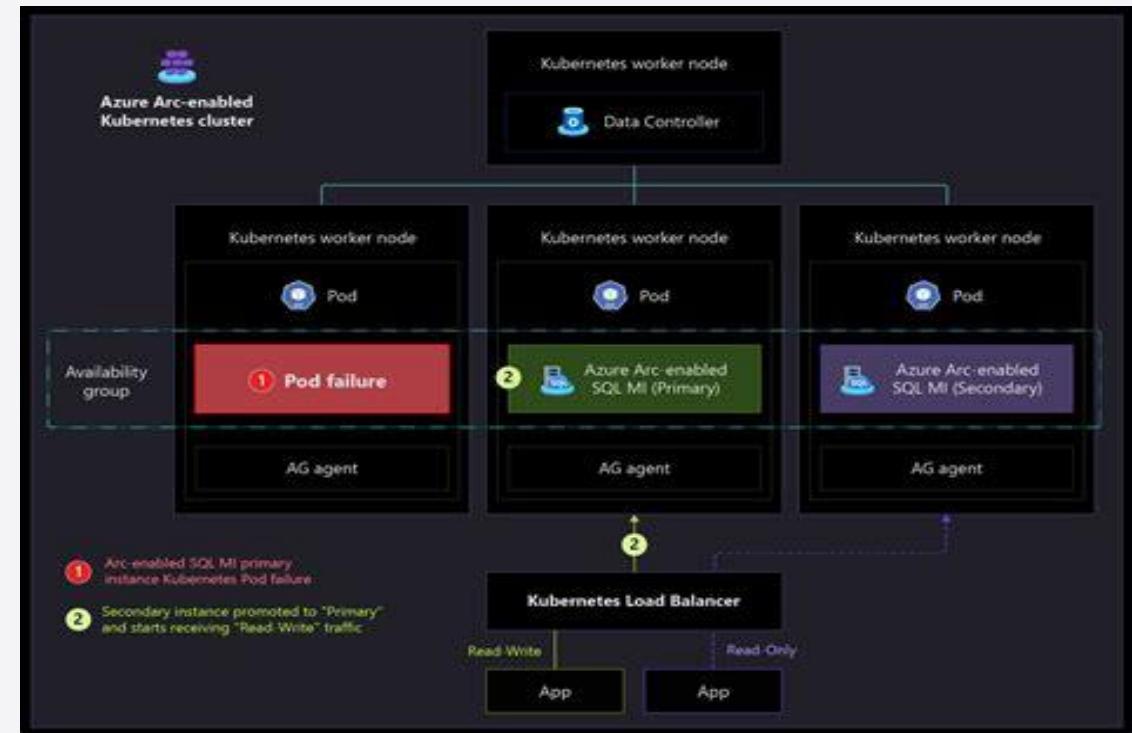
**Disaster Recovery:** You can configure disaster recovery by setting up another Azure Arc-enabled SQL Managed Instance in a geographically separate data center to synchronize data from the primary data center. This scenario is useful for recovering from events when an entire data center is down due 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.

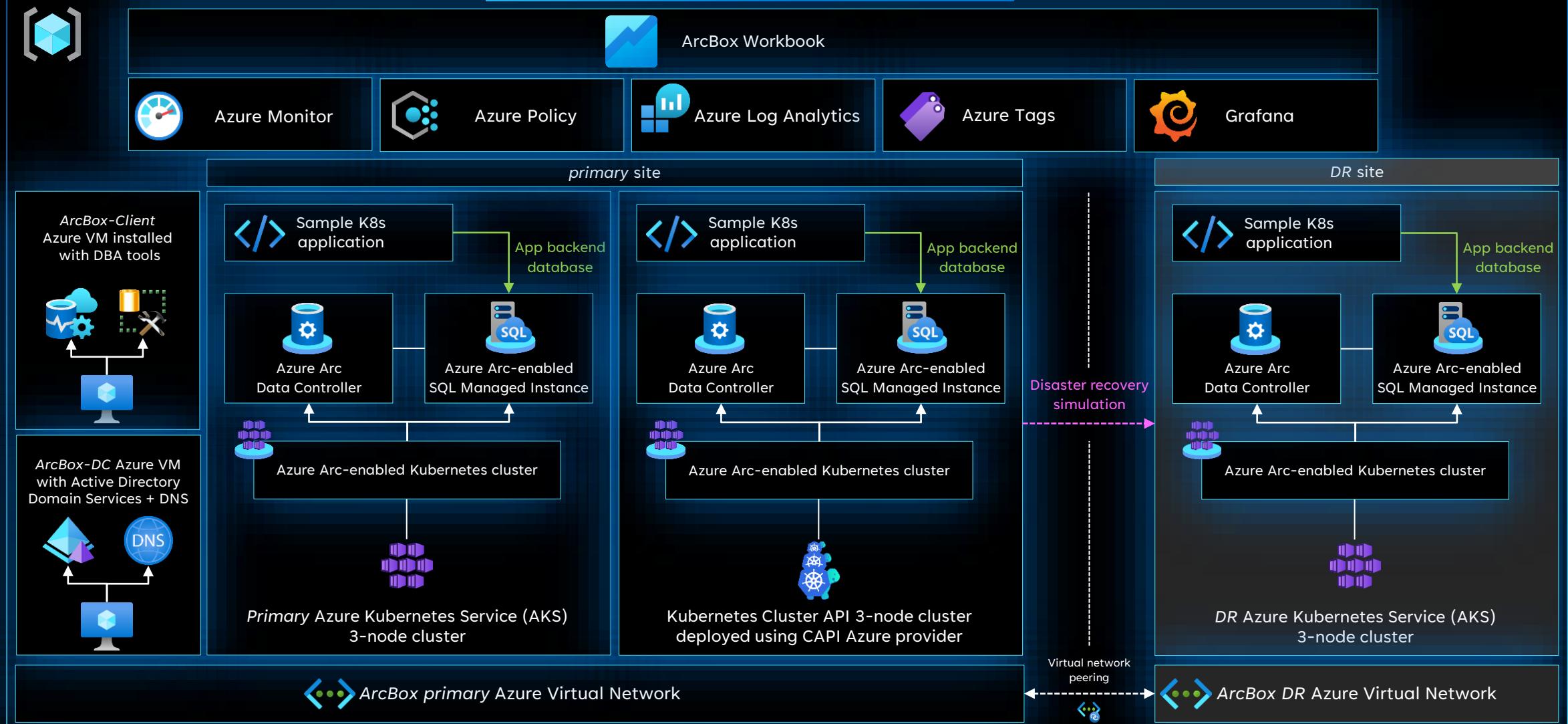
The entire solution is automatically deployed and includes all required Azure integrations, as well as three Kubernetes clusters and the supported Azure infrastructure alongside a sample application so users will have everything they need to get hands-on with the tech.

# DataOps edition

Azure Resource Manager (ARM)  
Azure Bicep  
Hashicorp Terraform



## ArcBox DataOps Azure Resource Group



# Example of Disaster-Ready Approach

# Azure Arc-enabled data services (1 of 5)

## SQL Managed Instance High Availability

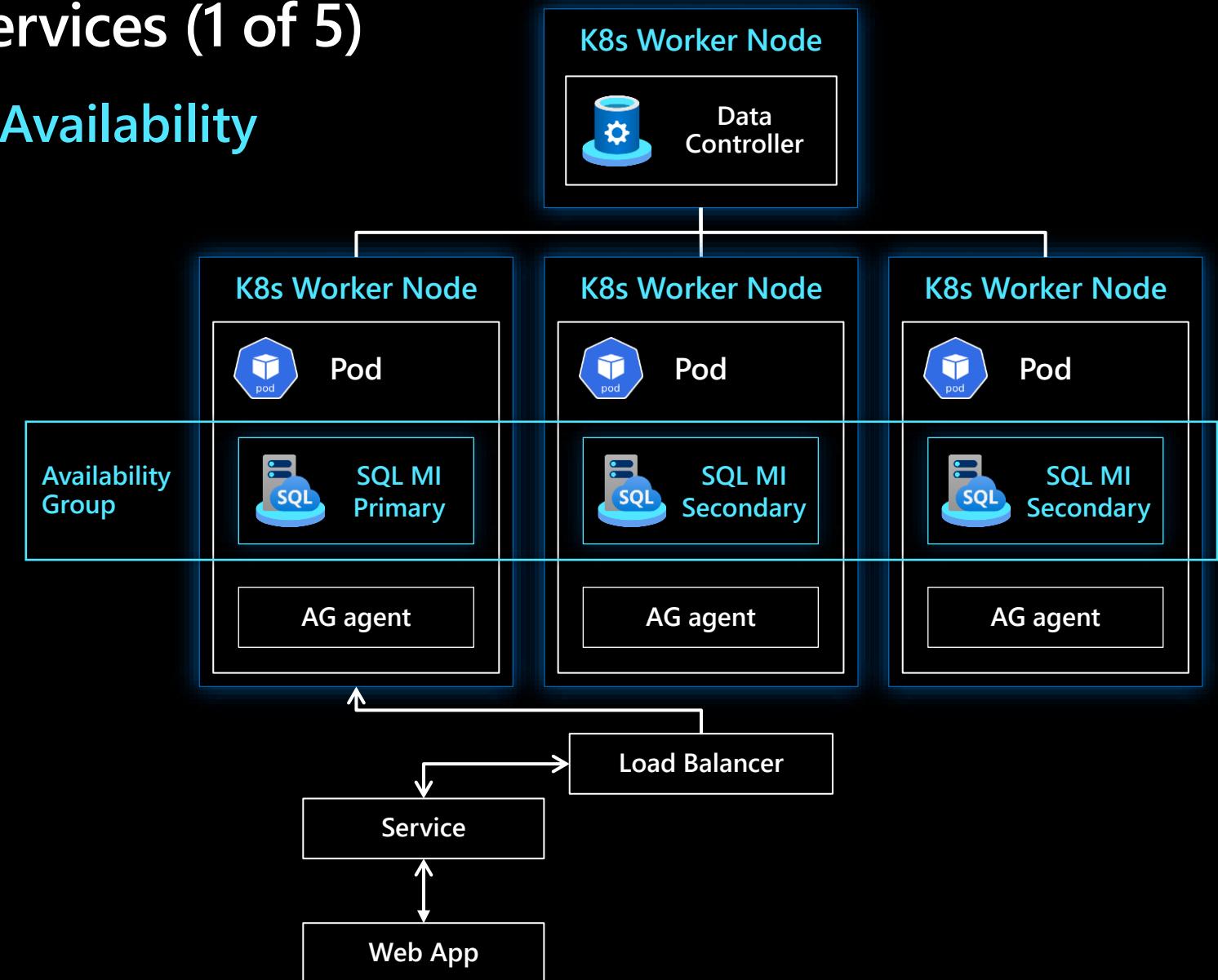
Built-in Setup

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

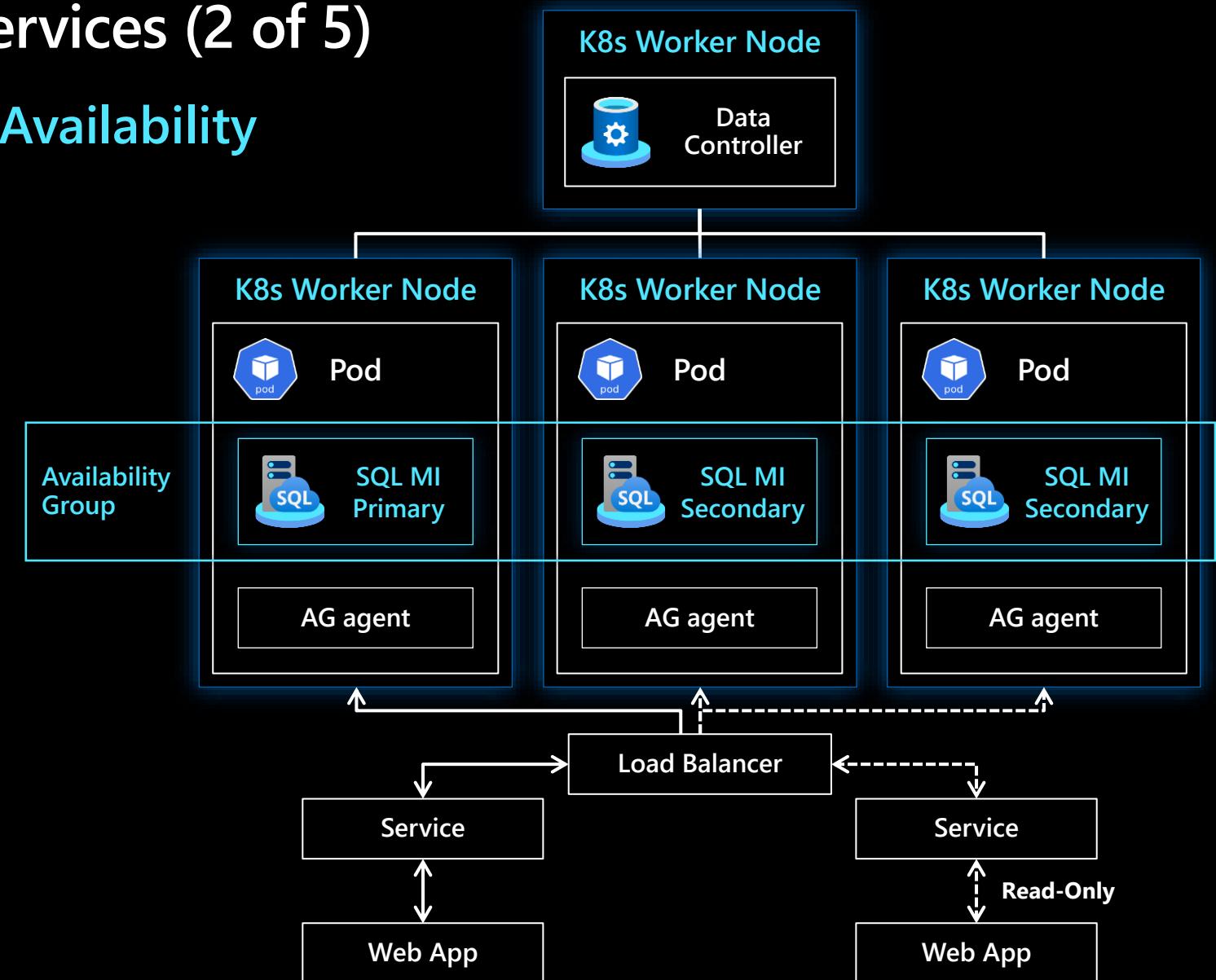
Built-in Setup

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

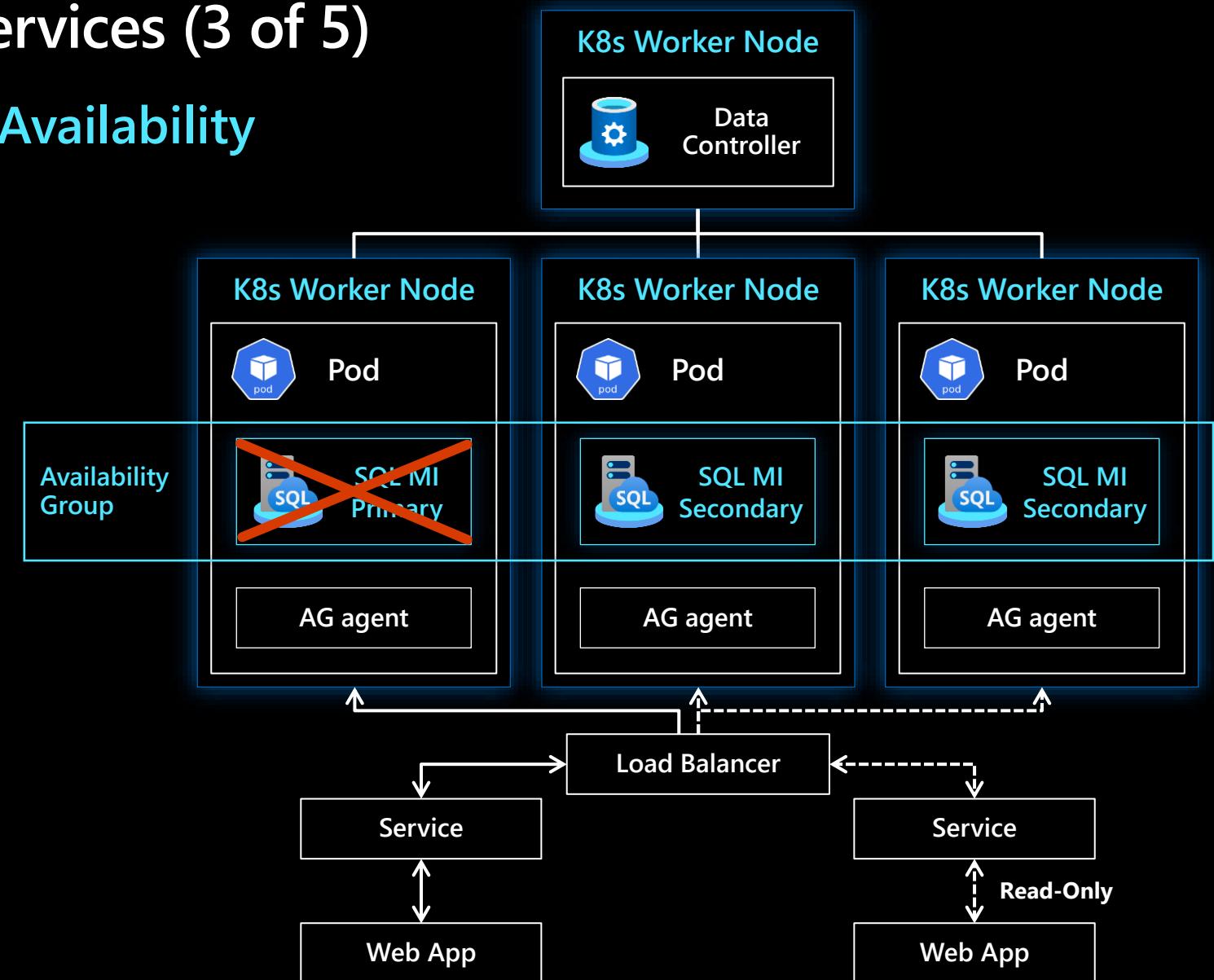
Built-in Setup

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

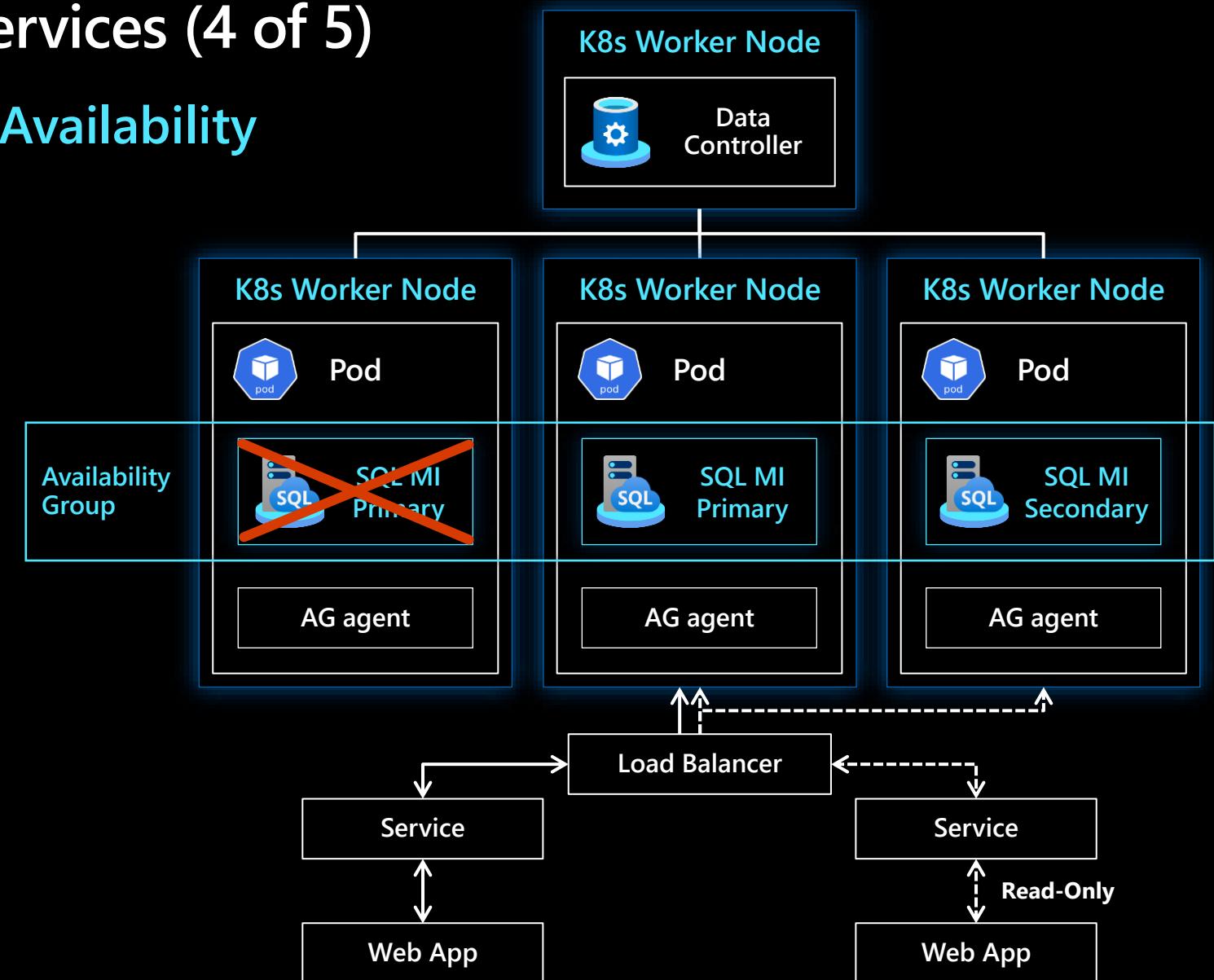
Built-in Setup

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

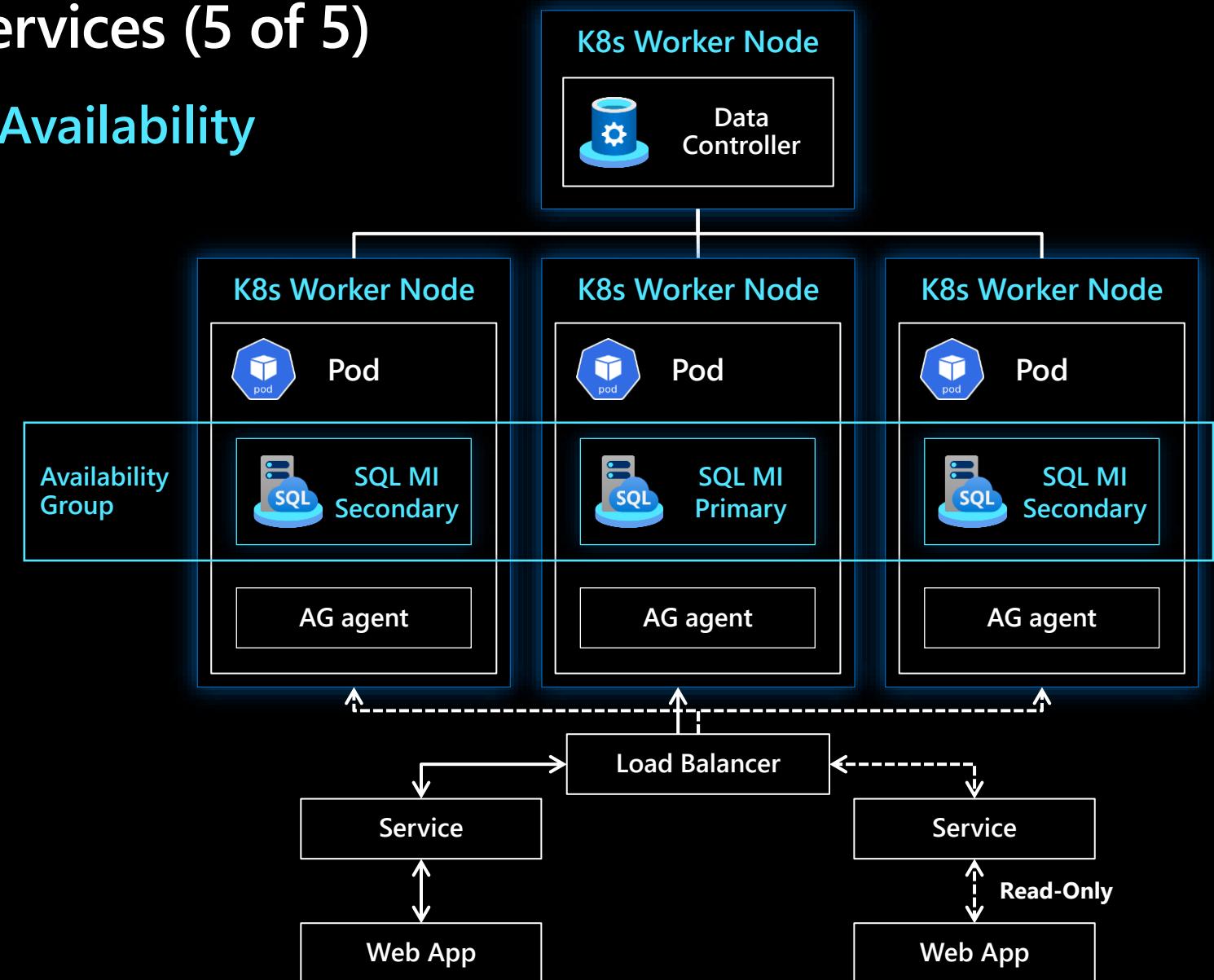
Built-in Setup

No other cluster technologies

Default configuration with  
3 sync replicas

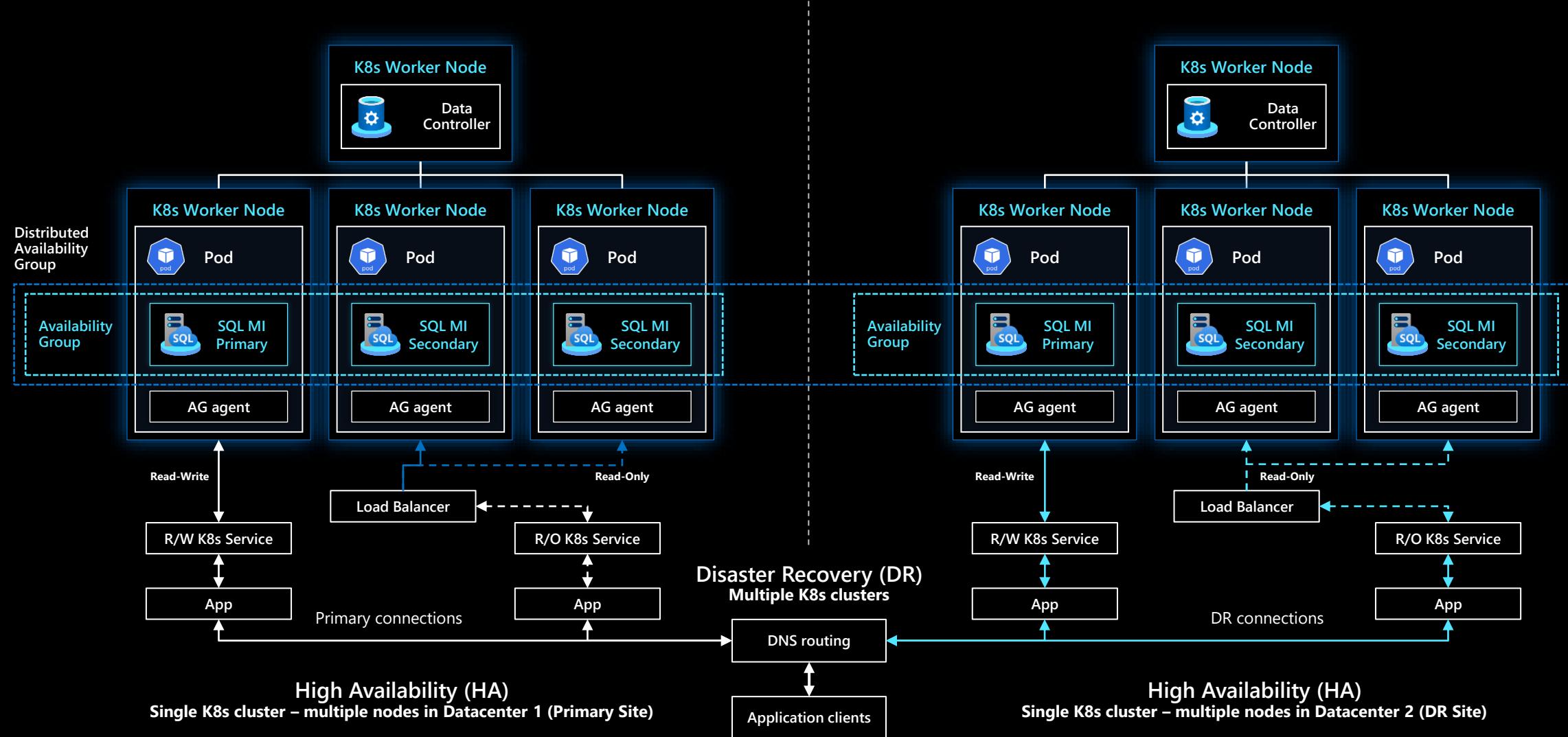
Primary and readable secondary  
endpoints

Automated Failover



# Arc-enabled Azure SQL Managed Instance

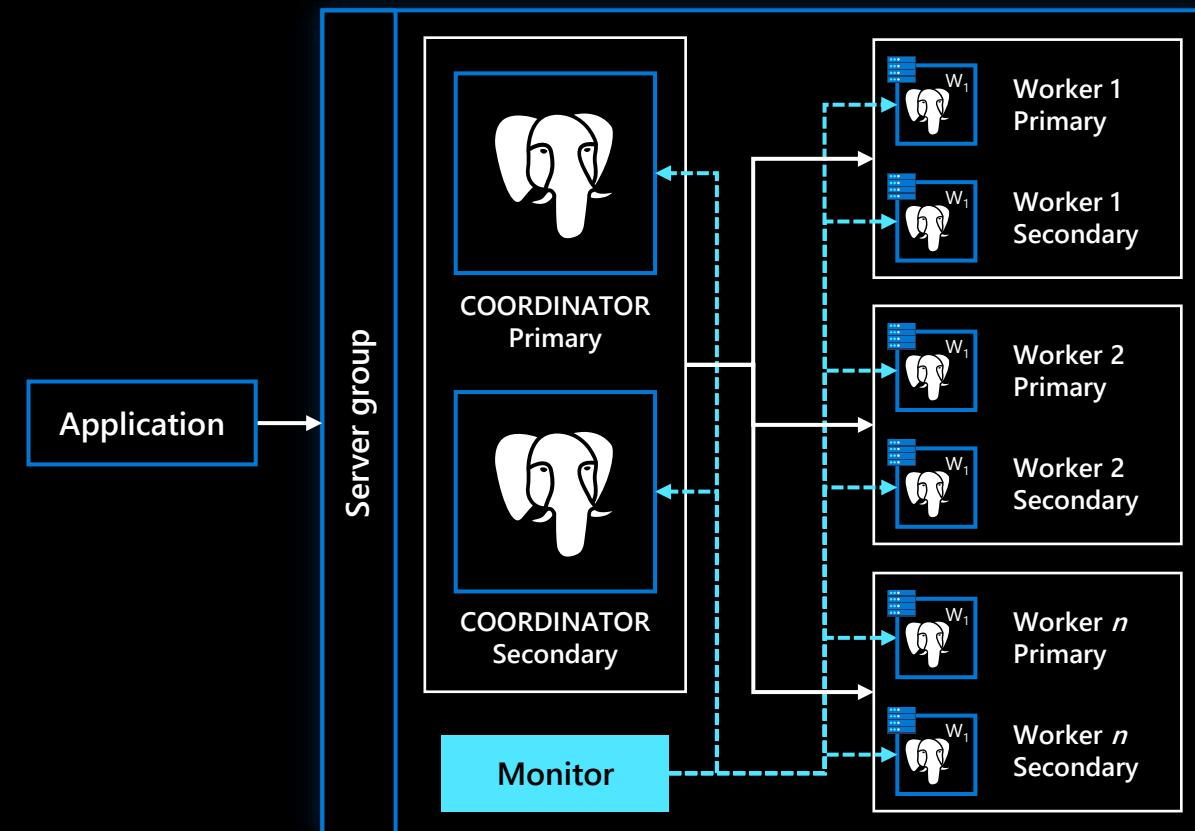
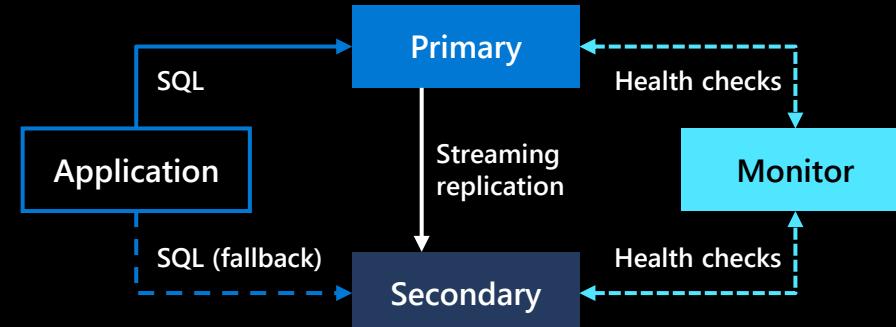
## High Availability and Disaster Recovery using Availability Groups



# 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.

## 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.

## 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.

## 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

(15 minutes)



# 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

The screenshot shows the Microsoft Ignite session catalog interface. At the top, there's a navigation bar with the Microsoft logo, a "Register now" button, and links for "Microsoft Ignite", "Sessions", "Seattle event guide", "Featured Partners", and "More". On the right, it shows "All Microsoft" and "(UTC+00:00) hora del meridiano de Greenwich" along with a "Sign in" link and a user icon.

The main area is titled "Session catalog" and features a large, colorful abstract graphic in the background. Below the title, there are date filters: "All days", "Wed 15", "Thu 16", and "Fri 17", followed by "298 sessions". A search bar contains the text "azure arc" with a magnifying glass icon.

Below the search bar, there are additional filters: "Refine results" (which is active), "azure arc" (highlighted in blue), and "Clear filters". There are also dropdowns for "Show 12 results" and "Relevance".

The main content area displays a single session card for "Azure Arc-enabled servers onboarding\_(Windows/Linux)". The card includes the following details:

- Delivery type:** Lab, In Seattle Only, Will Not Be Recorded
- Date and Time:** Friday, November 17, 1:15 AM - 2:15 AM hora del meridiano de Greenwich
- Description:** In this lab you will practice: 1. Arc-enabled servers onboarding (Windows/Linux) 2. Azure Monitor integration 3. Microsoft Defender for Cloud Integration
- Speakers:** Braulio Chavez (BC), Lior Kamrat (LK), Ryan Willis (RW)
- Actions:** Add to schedule, Save to backpack

# Resources



**Microsoft Learn / Docs**

[Azure Arc | Microsoft Learn](#)

**Microsoft Learn / Intro to Azure Arc**

<https://bit.ly/AzureArcIntroMSLearn>

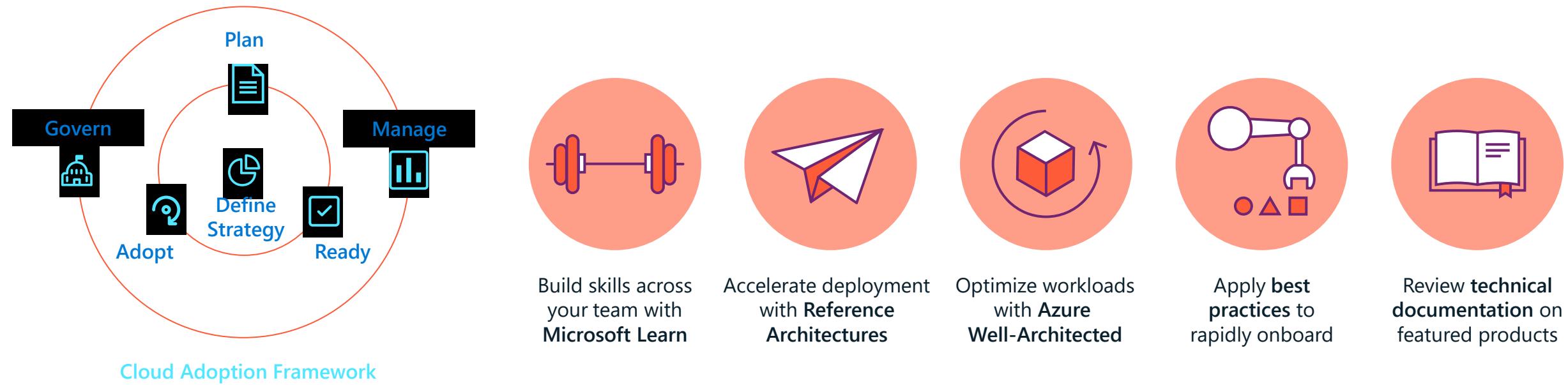
**Microsoft Ignite Conference**

[Session catalog \(microsoft.com\)](#)

**Microsoft Azure Arc Jumpstart**

[Overview | Azure Arc Jumpstart](#)

# Complete guidance for hybrid and multicloud approach



# 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>

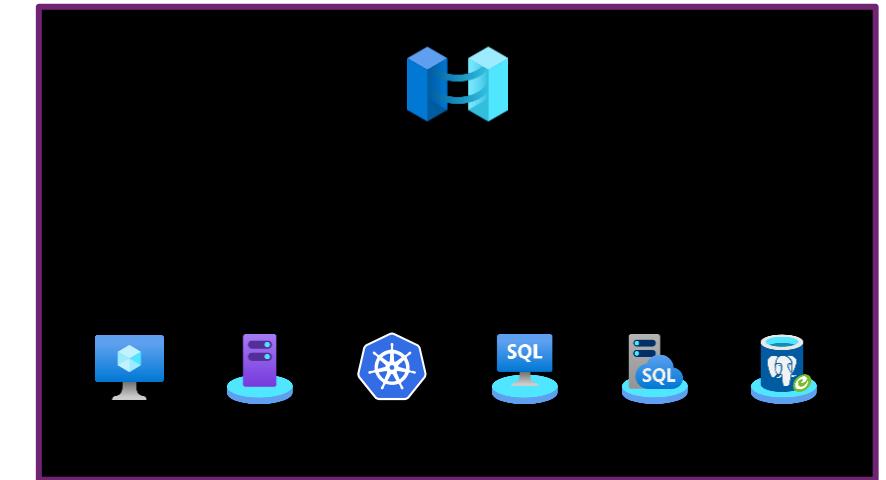
Try Azure Arc-enabled data services: <https://aka.ms/hybrid-data-services>

## 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

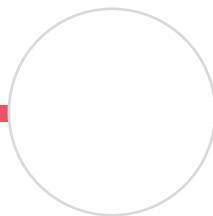
### [aka.ms/arc-ignite-video](#)

Ignite 2021: Innovate across hybrid and multicloud with Azure Arc

### [aka.ms/arc-datadocs](#)

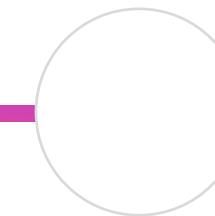
Documentation for Azure Arc-enabled data services

# Continue your journey with Azure Arc Webinar Series



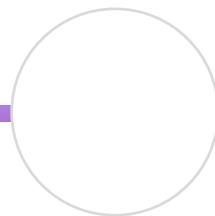
## Introduction for Microsoft Azure Arc for Beginners

- Introduction
- Features
- Services
- Flavors



## Intermediate-Level practices with Microsoft Azure Arc

- Security
- Governance
- Best Practices
- Cost Management



## Mastering Microsoft Azure Arc for Business

- Advanced Features
- Data Services
- Milticloud Environment
- Multispace Environment

# Q & A Time (10 minutes)

# Let's look for the questions!

# Webinar build on:

Materials from Azure Jumpstart Team

Almost all black/blue/colour slides

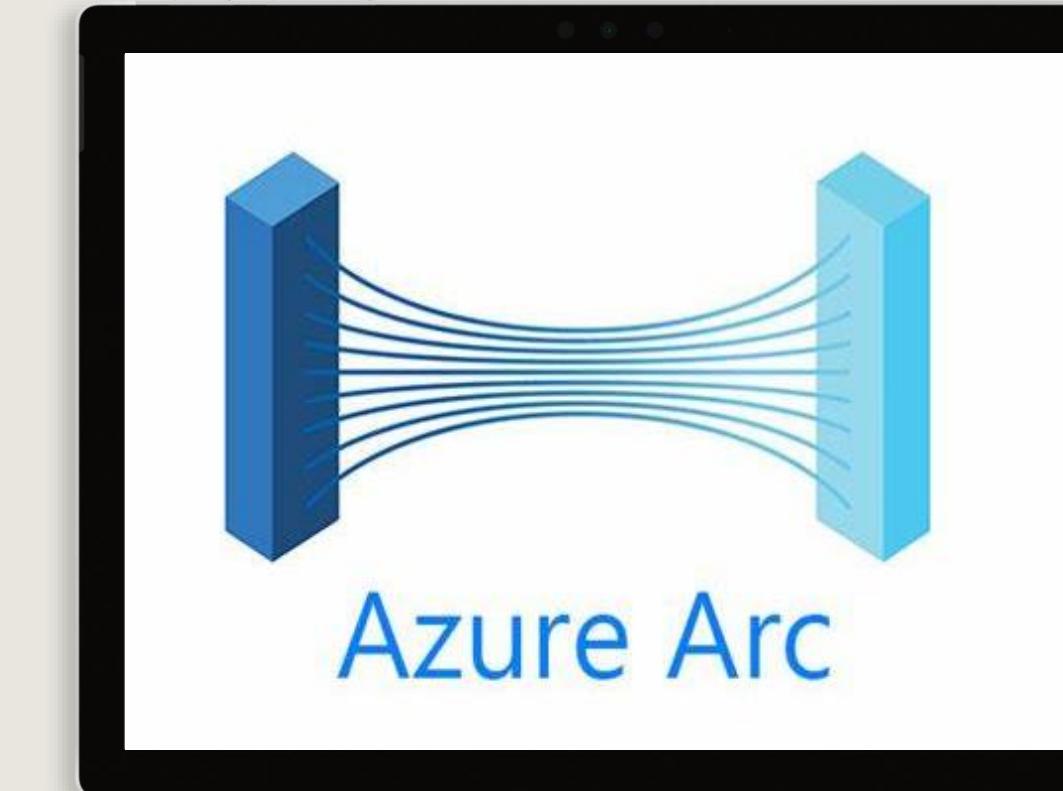
Big Thanks for Lior & Jan

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)
- | **ISC<sup>2</sup>** (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]





Thank You for spending  
time with us!

