Azure Arc-Enabled Kubernetes and Servers

Extending Hyperscale Cloud Management to Your Datacenter

—

Steve Buchanan
John Joyner

Foreword by Thomas Maurer, Sr. Cloud Advocate, Microsoft

Apress®

Azure Arc-Enabled Kubernetes and Servers

Extending Hyperscale Cloud Management to Your Datacenter

Steve Buchanan
John Joyner

Foreword by Thomas Maurer, Sr. Cloud Advocate, Microsoft

Apress®

Azure Arc-Enabled Kubernetes and Servers: Extending Hyperscale Cloud Management to Your Datacenter

Steve Buchanan
Minneapolis, MN, USA

John Joyner
Little Rock, AR, USA

ISBN-13 (pbk): 978-1-4842-7767-6
ISBN-13 (electronic): 978-1-4842-7768-3
https://doi.org/10.1007/978-1-4842-7768-3

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Joan Murray
Development Editor: Laura Berendson
Coordinating Editor: Jill Balzano

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media LLC, 1 New York Plaza, Suite 4600, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484277676. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

I would like to dedicate this book to my Mom and Dad for always supporting me and encouraging me to pursue all my dreams and aspirations.

—Steve Buchanan

Dedicated to the true greatest accomplishment of my life, my daughter Ava.

—John Joyner

Table of Contents

About the Authors

Steve Buchanan is a Director, Azure Platform Lead, and Containers Services Lead on a Cloud Transformation team with a large consulting firm. He is a ten-time Microsoft MVP, a Pluralsight author, and the author of eight technical books. He has presented at tech events, including DevOpsDays, Open Source North, Midwest Management Summit (MMS), Microsoft Ignite, BITCon, Experts Live Europe, OSCON, Inside Azure management, and user groups. He stays active in the technical community and enjoys blogging about his adventures in the world of IT at www.buchatech.com.

John Joyner is Senior Director, Technology, at AccountabilIT, a managed services provider of 24x7 Network Operations and Security Operations Center (NOC and SOC) services. As an Azure Solutions Architect Expert, he designs and builds modern management and security solutions based on Azure Lighthouse, Azure Arc, Azure Monitor Logs, Microsoft Sentinel, and Microsoft Defender for Cloud. John is also an authority on System Center products in private cloud and hybrid cloud environments and has been awarded Microsoft MVP 14 times. John is a retired US Navy Lt. Cmdr., where he was a computer scientist, worked for NATO in Europe, and served aboard an aircraft carrier in the Pacific. He is a veteran of the Persian Gulf War.

About the Contributor

Fred Limmer is the Cloud Architecture Group Manager with a large Microsoft-focused consulting firm. He is a regular contributor to local and regional events focusing on the organizational journey to the cloud and a frequent speaker and SME at Microsoft-sponsored events and other engagements.

Fred's primary focus is fueling enterprise growth through cloud adoption and transformation via a well-architected Microsoft Azure cloud platform implementation.

About the Technical Reviewer

Adnan Hendricks, Creative Director Cloud Solutions at Microspecialist Consulting, is a leading Azure infrastructure consultant, a Microsoft MVP, and trainer and is actively involved in Microsoft TAP programs.

His day-to-day job is implementing and architecting solutions with a focus on cloud, public/hybrid infrastructure, and the modern workspace.

As an international speaker and trainer, he often spends his time flying around the globe, consulting, teaching, and speaking at IT community events.

Acknowledgments

First and foremost, thanks to God for continued blessings and opportunities like this in my life and career. Thank you to my wife, Ayasha, for being patient with me and supporting me as I pursue opportunities like this. Thank you to my sons (Malcolm, Jalen, Sean, and Isaac) for being one of the reasons I stay motivated and want all of you to succeed in life.

A huge shout-out and thank you to my coauthor John Joyner. I know you did not plan on writing another book. Thanks for taking up this opportunity. As someone whom I respect and have looked up to in the Microsoft and MVP community, it means a lot to collaborate with you on a project like this.

A big thanks to Fred Limmer for jumping in and contributing to this book.

I would also like to thank the team at Apress, Joan Murray and Jill Balzano, for being great and easy to work with.

Finally, thanks to Chris Sanders, Lior Kamrat, Thomas Maurer, and the rest of the Arc team at Microsoft for bringing this exciting technology to the market.

—Steve Buchanan

Thank you, Steve Buchanan, for inviting me to coauthor the book; it has been a pleasure and an honor to collaborate with you to bring this content to our shared community.

Probably, Steve and I might not be in a position to author this book without the resources and opportunities afforded to recipients of the Microsoft MVP award. I know we are both grateful and appreciative for the MVP program's existence and our continued participation.

Much appreciation also to my employer AccountabilIT LLC, which graciously provides me the space to keep learning and writing and also supports a private cloud lab environment that is key for my research and development.

—John Joyner

Foreword

Today, hybrid and multicloud scenarios are critical for many organizations. There is a lot of momentum for building and implementing a hybrid and multicloud strategy. Based on studies, 90% of enterprises depend on hybrid and 93% have a multicloud strategy.

Microsoft Azure is an open, flexible, enterprise-grade cloud computing platform that provides all the services and features required to help you build and operate your technology solutions in the cloud. However, we understand that there are several reasons and motivations that drive the necessity of using multiple private and/or public clouds. Avoiding single cloud provider lock-in, addressing regulatory and data sovereignty requirements, improving business continuity, and maximizing performance by running applications close to user locations to avoid latency are all common business drivers to architect and build hybrid and multicloud environments. That is why Microsoft Azure is built from the ground up to support hybrid environments.

To quote our Azure Engineering lead and Executive Vice President Jason Zander at Microsoft: "Hybrid is not just an in-between state until everything is moved to the cloud, it will be an end state for many of our customers."

Running in hybrid, multicloud, and edge environments not only adds more complexity, but also often leads to an increase in operating costs and challenges when it comes to governance and compliance. With the Azure Resource Manager and additional Azure management services, Microsoft offers a strong management solution for resources and services deployed in Microsoft Azure. With Azure Arc, we are extending the management capabilities, and a number of the services to environments outside of the Azure cloud, to address these challenges. Now you can use Azure as a single control plane for your hybrid and multicloud environments.

With Azure Arc we offer two high level pillars: Azure Arc enabled infrastructure and Azure Arc enabled services. Azure Arc enabled infrastructure allows you to connect existing infrastructure, such as Windows and Linux servers, as well as Kubernetes clusters running outside of Azure to the Azure control plane to get visibility, and to organize and manage these resources. Azure Arc enabled services allow you to deploy

Azure services such as Azure data or Azure application services anywhere. This allows you to build consistent hybrid and multicloud architectures, as well as using the cloud-native tooling for your IT operations, DevOps, and developer processes.

This book, by two industry leading Azure experts, introduces you to the fundamentals of hybrid, multicloud, and edge computing. I have known Steve Buchanan and John Joyner for more than a decade now as valued members in the Microsoft MVP program and personally as friends. Their book provides you insights into Azure Native Management tooling for managing servers and Kubernetes clusters, running both on-premises and other cloud providers. They teach you how to leverage the Azure control plane to get visibility and management capabilities with Azure Arc, which are extremely useful to strengthen your security and governance posture. They also show how to leverage Azure Arc to seamlessly deliver Azure Monitor and/or Azure Sentinel, and achieve regulatory compliance with industry standards using Azure Arc, delivering Azure Policy from Microsoft Defender for Cloud.

An added bonus—their book also provides context on how to set up GitOps using Azure Arc in a hybrid and multicloud environment to empower your DevOps teams to perform tasks that typically fall under IT operations, and much more. In short, if you and your organization are running workloads in a hybrid or multicloud environment, this is the book for you.

—Thomas Maurer
Senior Cloud Advocate
Microsoft
October 2021

Introduction

This book is a practical guide to Microsoft's Azure Arc service. The goal of this book is to take you from 0 to 100 using Microsoft's new multicloud management tool, bringing Azure Management features to your servers and Kubernetes clusters, no matter where they are.

This practical guide on Azure Arc scales back on theory content, giving just enough to grasp important concepts while focusing on practical straight to the point knowledge that can be used to go spin up and start utilizing Azure Arc in no time.

In this book, you will learn about Azure Resource Manager, Git, GitHub, GitOps, Azure Management, and using Azure Arc to extend the Microsoft control plane for management of Kubernetes clusters and Servers in other environments and multiple clouds.

CHAPTER 1

Azure Arc As an Extension of the Azure Control Plane

Welcome to the first chapter in this *Azure Arc-Enabled Kubernetes and Servers* book. This book overall is going to take you on a journey into the world of both Azure Arc-enabled Kubernetes and Azure Arc-enabled servers. Azure Arc has many offerings, and we wanted to focus in this book on Azure Arc's Kubernetes and Server offerings to give you the most value we can on two focused topics.

Before we dive into Azure Arc offerings themselves, it is important to understand how Azure Arc fits as an Extension of the Azure Control Plane. This is what we are going to explore in this chapter. This will help to build foundational knowledge for the remaining chapters in this book.

Hybrid, Multicloud, and Edge

Hybrid cloud, Multicloud, and Edge cloud computing are areas that are all growing at a fast rate. Let's briefly define what each of these are:

Hybrid Cloud

Hybrid cloud combines on-premises data center (private cloud) with a public cloud to create a single cloud environment for an organization. Hybrid cloud gives you workload portability between public cloud and on-premises, a.k.a. private cloud. Hybrid cloud allows an enterprise to choose the optimal computing location for each workload as needed.

S. Buchanan and J. Joyner, *Azure Arc-Enabled Kubernetes and Servers*,
https://doi.org/10.1007/978-1-4842-7768-3_1

Multicloud

Multicloud is when an enterprise combines the use of two or more public clouds from different cloud providers. Multicloud is not something that is provided by a single cloud provider. Multicloud is often a mix of a couple or more of these major cloud providers: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft (Azure), Alibaba, and IBM.

Edge Cloud Computing

Edge cloud computing is extending cloud services, computing, and data storage to or near the source of data. Edge cloud computing saves bandwidth and is ideal for workloads with latency concerns. IoT and data-intensive workloads are common use cases for edge cloud computing.

It is important to look at some stats for these areas to understand the growth. A great resource that is published yearly is the Flexera State of the Cloud Report. This report breaks down all things cloud and gives some hard stats on what is happening in the cloud space with enterprises. Let's take a look at some stats from the Flexera 2021 State of the Cloud Report.

1. **Enterprises are embracing hybrid-cloud**

   87% of enterprises that responded to the Flexera 2021 State of the Cloud Report reported adopting a hybrid cloud strategy.

2. **Enterprises are embracing multicloud**

   93% of enterprises that responded to the Flexera 2021 State of the Cloud Report reported having a multicloud strategy. They also reported combining public and private clouds in their strategy.

3. **Enterprises are embracing edge cloud computing**

   49% of enterprises that responded to the Flexera 2021 State of the Cloud Report are experimenting with or plan to use edge services.

To sum this up, most enterprises have adopted Hybrid as their cloud model, which includes multicloud. The following image from the Flexera 2021 State of the Cloud Report shows this.

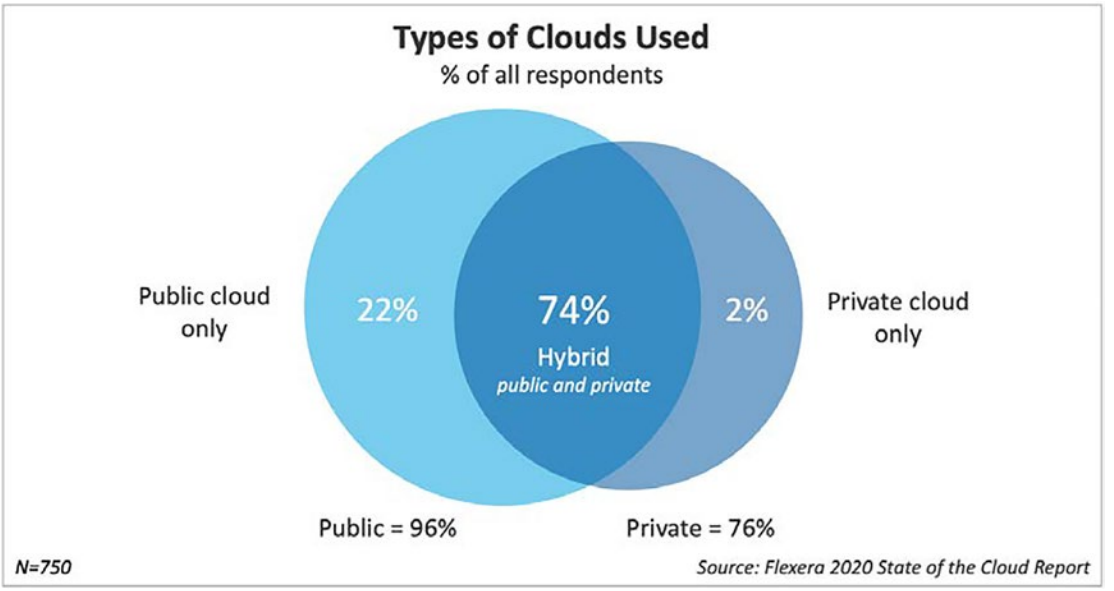

Figure 1-1. *Types of clouds used chart from the Flexera 2021 State of the Cloud Report*

This demonstrates that the growth in cloud is in hybrid, multicloud, and edge cloud computing.

Overview of Azure Arc

As we saw from the previous section, there is a growing demand for hybrid cloud, multicloud, and edge cloud computing in the world of tech today. With running workloads across hybrid cloud, multicloud, and edge cloud computing environments, the complexity to manage them is also increasing.

In 2019, at Microsoft's large technical conference, Microsoft Ignite announced Azure Arc. Azure Arc extends Azure capabilities to environments outside of Azure such as on-premises data centers and other private and public clouds. Azure Arc sets out to simplify complex and distributed environments by bringing the Azure Resource Manager (ARM) and its management tools to environments regardless of what cloud they are on. Azure Arc gives technical teams the power to deploy workloads and manage resources, regardless of where they exist.

Arc is a response to the increasing complexities that on-premises and multicloud management needs enterprises have. Azure Arc enables you to create and manage resources as well as workloads on

- On-premises
- Non-Azure clouds (i.e., GCP, AWS, Alibaba, etc.)
- Private clouds
- Microsoft Hybrid (Azure Stack Hub, Azure Stack HCI, Azure Stack Edge)

Arc all up consists of multiple offerings to help meet an organization's various multienvironment needs. Here are three key areas where Azure Arc provides value:

Consistency

Arc gives you consistent governance, inventory, and management of resources and workloads.

Zero-touch compliance and configuration

With Arc, you can gain zero-touch compliance and configuration across resources and workloads such as servers, Kubernetes, and more.

Unified experience

Azure Arc gives you a unified experience for a single pane and single control plane across environments and resources/workloads running on them. The same tooling is used regardless of where the workloads and resources are running through management with the Azure portal, Azure CLI, Azure PowerShell, or Azure REST API.

Now, Azure Arc extends Azure services to resources and workloads running outside of Azure. The services that are extended will differ based on the Azure Arc offering. Here is a list of many of the Azure services that can be extended via Azure Arc:

- Management Groups
- Subscriptions
- Resource Groups
- Role-Based Access Control
- Tagging

- Security Center/Azure Defender
- Azure Sentinel
- Azure Key Vault
- Azure Policy/Azure Policy Guest Configuration
- Azure Backup
- Update Management, Change Tracking, and Inventory
- Azure Monitor
- Azure Automation
- Viewing and Access in the Azure portal
- Azure SDK
- ARM Templates
- And more

Currently, Azure Arc is offered at no additional cost when managing Azure Arc-enabled servers and Azure Arc-enabled Kubernetes. Azure Arc control plane functionality is offered for free. The services that are considered as a part of the Azure Arc Control plane are

- Attaching servers and Kubernetes clusters to Azure
- Resource organization through Azure management groups and Tagging
- Searching and indexing through Resource Graph
- Access and security through Azure RBAC and Azure subscriptions
- Patch management through Update Management
- Environments and automation through ARM templates and Azure extensions

Azure Arc Offerings

When Azure Arc was launched, it had a few offerings available, the first being Azure Arc-enabled servers. Since its launch, Microsoft has been quickly adding additional offerings to Arc and extending the functionality of the current offerings. Azure Arc offerings break down into two categories. Infrastructure is your infrastructure to run workloads. Services are Azure services being extended out of Azure through Arc. The first category is infrastructure, and the second category is services. Azure Arc offerings and the resource types it is able to manage include the following:

Infrastructure

- **Servers:** Supports Linux and Windows, supports bare-metal servers, on-premises servers, AWS EC2 virtual machines, GCP computer engine virtual machines, VMWare virtual machines, and Hyper-V virtual machines
- **Azure Arc-enabled SQL Server:** Manages instances of SQL Server from Azure, extending Azure services to SQL Server instances hosted outside of Azure
- **Kubernetes:** On-premises Kubernetes clusters, Rancher K3s, AWS EKS clusters, GCP GKE clusters
- **Azure Arc IoT:** Via Azure Arc-enabled Kubernetes, centrally manages and deploys IoT workloads at the edge

Services

- **Data services:** Run Azure data services outside of Azure including SQL Managed Instance and PostgreSQL.
- **Azure Arc with Lighthouse:** The combination of Azure Arc and Azure Lighthouse for expanded Lighthouse management capabilities to non-Azure environments.
- **Azure application services with Azure Arc:** Azure Application PaaS services (App service, Functions, Logic Apps, Event Grid, API Management) and other PaaS services can run on any Kubernetes cluster via Arc.

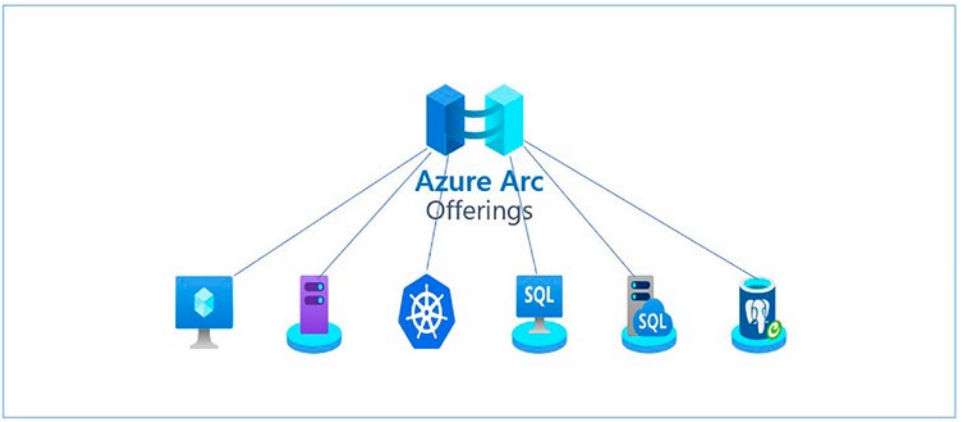

Figure 1-2. *Azure Arc offerings*

Why Would I Want to Use Azure Arc for My Organization?

Multicloud architectures are often more complex and more of a challenge to manage. From the Flexera 2021 State of the Cloud Report, 68% of enterprises that responded to the report are not utilizing multicloud management tools currently. Only 32% are utilizing multicloud management tools. The report goes on to cover multicloud governance, security, and cost management tool stats. The percentages in these other areas have low adoption as well. This means there is a tremendous opportunity of growth in multicloud management tooling. Microsoft set out to fill this gap with Azure Arc.

Use Cases

Here are some use cases that make sense for using Azure Arc:

Legal Jurisdiction

Some workloads are legally required to process and retain data within a specific region, country, etc., requiring infrastructure across multiple data centers and cloud providers.

Latency

Some workloads have latency requirements that have to be met by locating the workload in a specific geography.

Legacy Infrastructure

Some legacy infrastructure is old and is challenging and sometimes can't be moved to the cloud. Arc can extend the cloud to that on-premises legacy infrastructure.

Availability

The ability to run the same services across multiple cloud providers and even on-premises for greater availability in the event of cloud provider or on-premises outages.

Developer Options

The ability to provide a choice to developers to run workloads on any environment that best fits their needs.

Edge Compute Needs (local)

As organizations continue to expand their edge and local footprint for running workloads, i.e., stores, warehouses, factories, in the field, etc., extending cloud and centralizing management can reduce complexity in managing across edge locations.

Hybrid Cloud Scenario

There are many scenarios for organizations when it comes to utilizing Azure Arc. Let's walk through one of these scenarios. In this example, the organization is running a container-based web application that has components spread across Azure cloud and their on-premises data center.

In this specific scenario, the organization needs to have low latency for users that will utilize the web app from on-premises, and they want public traffic to come into the web app; running on Azure as cloud can better handle the external traffic load.

This organization is utilizing Azure Arc to manage both the on-premises Kubernetes cluster and the cloud-based Azure Kubernetes Service (AKS) cluster. They are also utilizing GitOps to ensure the on-premises Kubernetes cluster and the cloud-based AKS cluster configuration and application deployment match at all times. Also, they are utilizing Azure Container Instance (ACI) for very fast burstable capacity as needed on the AKS cluster. The following image visualizes the architecture for this hybrid-based application.

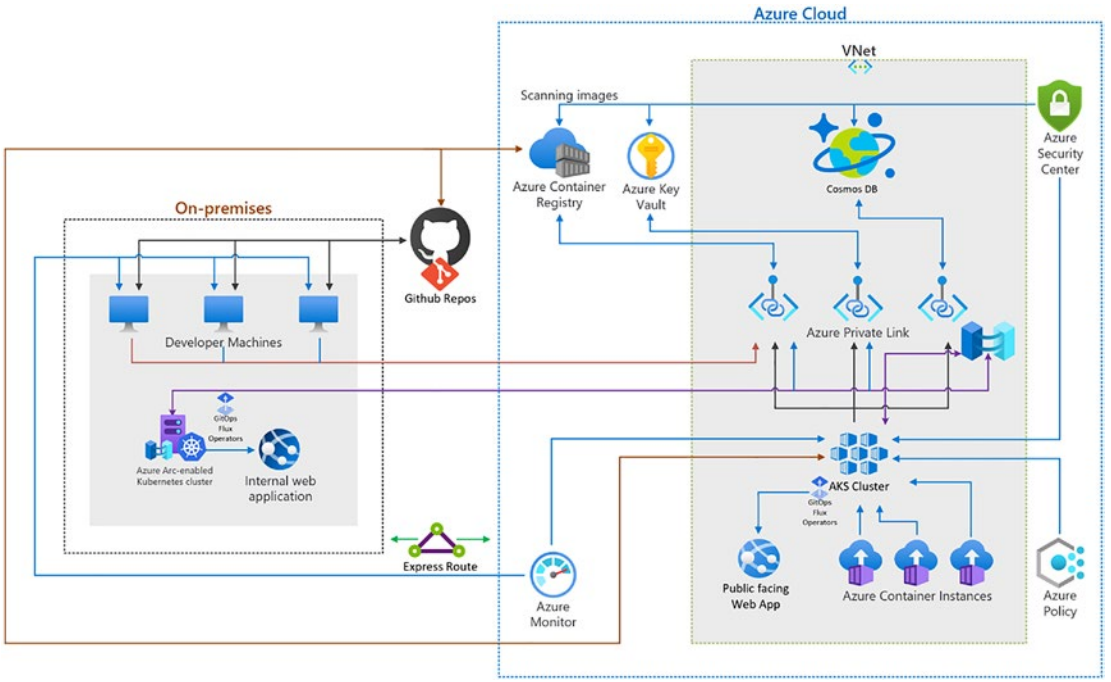

Figure 1-3. *Container-based web app running in hybrid cloud model*

Summary

This brings us to a close of the first chapter. In this chapter, we took time to understand hybrid, multicloud, and edge areas and the challenges that come with managing them. We worked through an overview of Azure Arc. We dove into Azure Arc's offerings to give an understanding of what Azure Arc is made up of. We finally explored why your organization might adopt Azure Arc. This all is to set you up with a solid foundation of knowledge of Azure Arc to help as you further embark on the remaining chapters in this book, moving deeper into the world of hybrid, multicloud, and edge and Azure Arc.

CHAPTER 2

Azure Resource Manager Insights

Introduction

In this section, we'll be examining the Azure Resource Manager or "ARM" platform management layer in Microsoft Azure. We'll talk about what it is, how it works, what you can do with it, and tips and tricks for how to use it effectively in your Azure ARC deployment and other implementation projects in Azure.

What Is Azure Resource Manager?

ARM, at its core, is the deployment and management service for Azure. It allows for the creation, configuration, and management of resources, such as virtual machines or virtual networks, and Platform as a Service, or "PaaS," offerings such as Azure App Service, ARC, and Azure SQL.

In Azure's infancy, a system of management and structure referred to as the Azure Service Manager, or "ASM," was implemented to manage the platform. This immature system quickly exposed its limitations regarding governance, security controls, resource organization, structure, and environment management.

ASM was eventually supplanted with a more flexible and capable management layer called Azure Resource Manager or "ARM." ASM, however, still exists in the Azure environment, and ASM-based resources are labeled as "Classic."

S. Buchanan and J. Joyner, *Azure Arc-Enabled Kubernetes and Servers*,
https://doi.org/10.1007/978-1-4842-7768-3_2

The ARM management layer essentially executes tasks like creating resources and managing them with identity and access controls (IAM), organizing and grouping with tags, or adding locks to prevent unauthorized changes.

Think of ARM as the interpreter between you and Azure. You tell it WHAT you want to do, and it figures out HOW to do it.

ARM enables you to perform a host of tasks inside of the Azure platform. It allows for the management of infrastructure through declarative means rather than static scripts or other actions. This means that you can deploy, manage, configure, and monitor resources as a group rather than attempting to manage them separately. For example, you can apply a defined Access Control design to a group of resources rather than having to configure each one individually, saving time and reducing potential for human error.

This approach not only allows for a simpler management approach to a scope of resources, but it allows you to easily redeploy that same group of resources as part of another separate deployment. This comes in quite handy when you need to deploy resources for a solution using a life cycle approach where you might start initially with a Development environment and then move to a Testing or QA environment before eventually reaching Production.

When determining your Azure deployment strategy, there are a number of different considerations that you need to take into account.

Firstly, once you start down a path, it can sometimes be very difficult to change course. For example, if you decide that you want to deploy resources with PowerShell scripts but later decide that you want to switch to using another deployment method like Terraform, that change can be very difficult and might require a significant amount of effort. Take the time to review the options and decide on the best path for you.

Consider the technological investment. What will you need to buy to take this path? Do you need to build and host servers? Will you need to purchase software licensing? Will you require a third-party service? Will you need to train your team? What are the costs and what is the value?

Additionally, what are the future cloud adoption plans for the organization? What is the plan for Azure? Do you have a road map to follow? What external situations exist that might drive additional Azure adoption or consumption? Does the company need to plan a data center exit in the near future or close a key location?

Your people will also be key to the success of your program. Who on your team has the knowledge necessary to make use of the tools, services, or applications? Is there a skill gap? How will you close it? How will you manage the knowledge documentation and transfer to new or junior resources in the future?

Keep in mind that your choice here will not only affect the team(s) using ARM to deploy infrastructure resources but will potentially affect how your application development or data and analytics teams will function when they are deploying solutions to the Azure environment as well. Be sure to get everyone engaged as early as possible so every perspective is considered, and the best choice made.

These are all key areas that will require organization-wide thought, discussion, and group decisions before charting your course.

Secondly, planning what you actually want to do with Azure up front is key to success. You shouldn't build anything in Azure until you have at least defined basic requirements, a list of resources, and a road map.

Will you only be using Azure for a web application, or will you be using it solely for data analytics? Will you extend your data center into the environment and use Azure to operate and manage your core infrastructure across the organization?

Each of these varying scenarios will drive you down a diverging path and will require vastly different resources to accomplish.

Understanding ARM

ARM is structured in a standard hierarchy with five levels of scope with each level inheriting the settings from the level above.

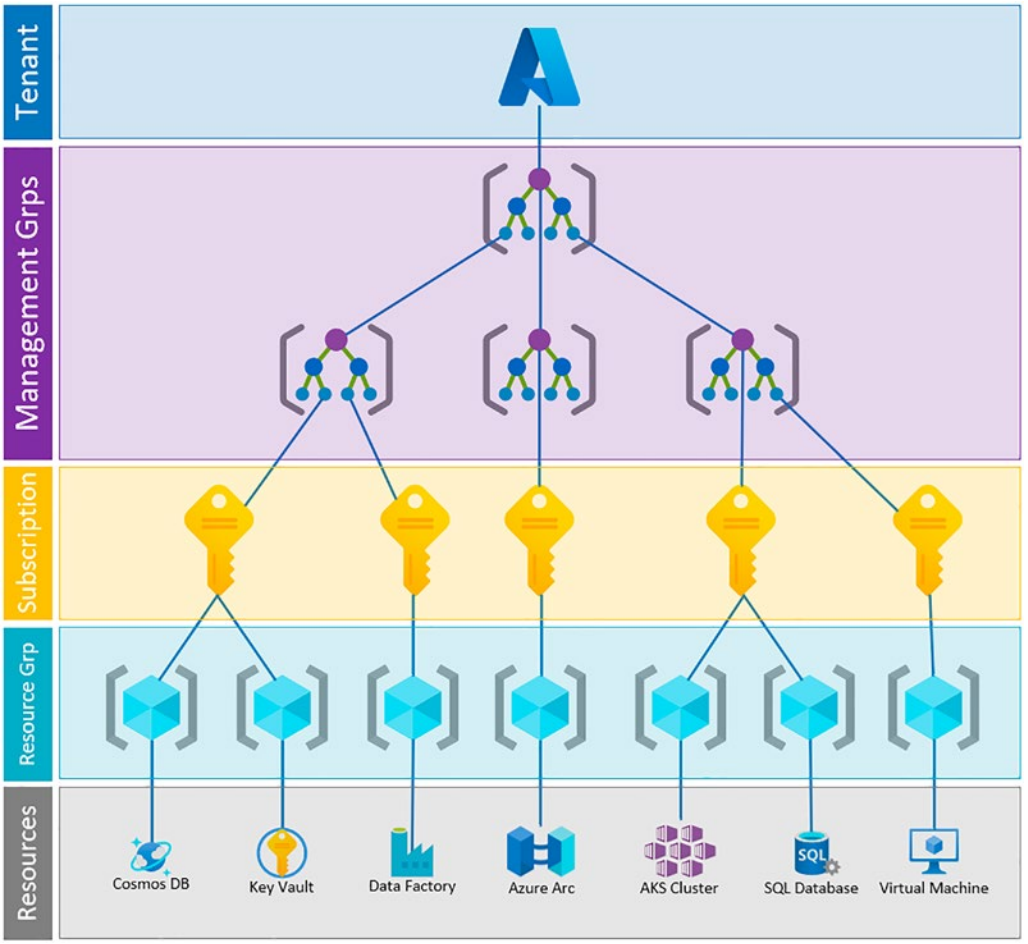

Figure 2-1. *Azure management scopes*

At the top of the hierarchy is the Azure Tenant. This is also often referred to as the "Enrollment" or the "Directory." From the perspective of our organization discussion, the name doesn't really matter. It's simply the highest level of the hierarchy.

The first scope level commonly utilized for structure, administration, policy, or other broader administration is the Management Group. This level of the hierarchy generally contains Subscriptions but can also have multiple tiers of Management Groups in scenarios where you may have different policies for different geopolitical regions such as North America vs. Europe, or Asia Pacific.

Settings can be applied at any level in the hierarchy, but access controls, permissions, and policies for governance and/or security will often be created in a Management Group so that they are inherited by the Subscriptions and everything below them in the structure.