Contents

[1 WordPress (Recommended) Host Requirements: 4](#_Toc46171665)

[2 WordPress on Azure: 4](#_Toc46171666)

[2.1 WordPress and Azure App Service: 4](#_Toc46171667)

[2.2 WordPress and Azure App Service Backup and Restore: 4](#_Toc46171668)

[2.3 WordPress and Azure Backup: 4](#_Toc46171669)

[2.4 WordPress and Azure Storage: 5](#_Toc46171670)

[2.5 WordPress and Azure Database for MySQL server: 5](#_Toc46171671)

[2.6 WordPress and Azure Autoscale: 5](#_Toc46171672)

[2.7 WordPress and Azure Content Delivery Network (CDN): 5](#_Toc46171673)

[2.8 WordPress and Azure Application Insights: 6](#_Toc46171674)

[2.9 WordPress and Azure Key Vault: 6](#_Toc46171675)

[2.10 WordPress and Azure App Service Managed Certificates: 6](#_Toc46171676)

[2.10.1 Azure: App Service Managed Certificates vs. App Service Certificates 7](#_Toc46171677)

[2.11 WordPress and Azure Web App for Containers: 7](#_Toc46171678)

[2.12 WordPress and Azure Kubernetes Service (AKS): 8](#_Toc46171679)

[2.13 WordPress Azure Plugins for in-house development: 8](#_Toc46171680)

[3 Case Study: Highly Scalable and Secure WordPress Website 9](#_Toc46171681)

[3.1 Relevant use cases: 9](#_Toc46171682)

[3.2 Architecture: 9](#_Toc46171683)

[3.3 Components: 10](#_Toc46171684)

[3.4 Alternatives: 10](#_Toc46171685)

[3.5 Considerations: 10](#_Toc46171686)

[4 WordPress VIP: 10](#_Toc46171687)

[4.1 Features of WordPress VIP: 11](#_Toc46171688)

[4.2 Benefits of WordPress VIP: 11](#_Toc46171689)

[5 Magento 2.3 Technology Stack Requirements: 12](#_Toc46171690)

[6 Magento on Azure 12](#_Toc46171691)

[6.1 How Magento Azure Integrations is beneficial for your E-commerce website? 12](#_Toc46171692)

[6.2 Magento and Azure Database for MySQL server: 12](#_Toc46171693)

[6.3 Magento and Azure Resource Manager (ARM) Templates: 13](#_Toc46171694)

[6.4 Magento and Azure Logic Apps: 13](#_Toc46171695)

[6.5 Magento and Azure Web App for Containers: 13](#_Toc46171696)

[6.6 Magento and Azure Kubernetes Service (AKS): 13](#_Toc46171697)

[6.7 Magento and Azure Data Factory: 13](#_Toc46171698)

[6.8 Magento and Azure Synapse 14](#_Toc46171699)

[7 Case Study: An E-commerce Front End on Azure 14](#_Toc46171700)

[7.1 Relevant use cases 15](#_Toc46171701)

[7.2 Architecture 15](#_Toc46171702)

[7.3 Components 16](#_Toc46171703)

[7.4 Alternatives 16](#_Toc46171704)

[8 Azure Security 17](#_Toc46171705)

[8.1 Shared responsibility model for the cloud 17](#_Toc46171706)

[8.2 Security advantages of an Azure PaaS: 18](#_Toc46171707)

[8.3 Security advantages of Azure IaaS 19](#_Toc46171708)

[8.4 Azure Security Technical Capabilities 20](#_Toc46171709)

[9 Azure CI/CD 21](#_Toc46171710)

[9.1 CI/CD for Azure VMs 21](#_Toc46171711)

[9.1.1 Data Flow 21](#_Toc46171712)

[9.1.2 Components 21](#_Toc46171713)

[9.2 CI/CD for Containers 22](#_Toc46171714)

[9.2.1 Data Flow 22](#_Toc46171715)

[9.2.2 Components 22](#_Toc46171716)

[9.3 Container CI/CD using Jenkins and Kubernetes on Azure Kubernetes Service (AKS) 23](#_Toc46171717)

[9.3.1 Data Flow 23](#_Toc46171718)

[9.3.2 Components 23](#_Toc46171719)

[10 WordPress and Azure DevOps 24](#_Toc46171720)

[10.1 WordPress in Azure App Service Containers using Docker 24](#_Toc46171721)

[10.1.1 Components 25](#_Toc46171722)

[10.2 WordPress in Web App Production and Staging Slots 25](#_Toc46171723)

[11 Magento and Azure DevOps 26](#_Toc46171724)

[11.1 Magento in Azure Kubernetes Service (AKS) 26](#_Toc46171725)

[11.2 Components 26](#_Toc46171726)

[12 Azure Dev-Test Labs 27](#_Toc46171727)

[12.1 Dev-Test Deployment for Testing IaaS Solutions 27](#_Toc46171728)

[12.1.1 Components 27](#_Toc46171729)

[12.2 Dev-Test Deployment for Testing PaaS Solutions 28](#_Toc46171730)

[12.2.1 Components 28](#_Toc46171731)

# WordPress (Recommended) Host Requirements:

• PHP version 7.4 or greater

• MySQL version 5.6 or greater OR MariaDB version 10.1 or greater

• HTTPS support

• Apache or Nginx

**Note:**

WordPress is primarily designed to use a MySQL or MySQL-related database server, and officially only supports MySQL or MariaDB, a drop-in replacement for MySQL. [[1]](#footnote-1)

# WordPress on Azure:

## WordPress and Azure App Service:

Azure Web App, available for Linux and Windows, enables developers to easily deploy and scale enterprise grade web applications written in a variety of languages and integrated with a multitude of services without ever worrying about infrastructure management. Azure App Service provides a highly scalable, self-patching web hosting service. Also, you can create, upload, or import a private certificate or a public certificate into App Service. Once the certificate is added to your App Service app or function app, you can secure a custom DNS name with it or use it in your application code including the option to import a certificate from Key Vault. It takes Azure a minute or two to deploy WordPress as an App Service and the Azure portal presents data-rich view of the WordPress App Service.

## WordPress and Azure App Service Backup and Restore:

The Backup and Restore feature in Azure App Service lets you easily create app backups manually or on a schedule. You can configure the backups to be retained up to an indefinite amount of time. You can restore the app to a snapshot of a previous state by overwriting the existing app or restoring to another app. The Azure App Service can back up the following WordPress website elements to an Azure Storage account and container:

• WordPress website's configuration

• File content (posts, pages, media etc.) of the WordPress website

• Database connected to the WordPress website

WordPress often with updates of plugins, themes and/ or core-WP updates may conflict, breaking the website. Being able to go back to the last successful working copy of the website, and then begin step-by-step discovering and eliminating the conflicts from updates, saves a lot of time.

## WordPress and Azure Backup:

Azure Backup is a cloud-based backup solution, part of broad package presented to clients through Azure Recovery Services vault. Though cloud-native, it is also possible to use Azure Backup on-premises as well as in the cloud. Azure Backup is simple to configure and use, offering consistent copies with security features and management controls via the Azure portal. WordPress data remains safe and easy recoverable through Azure Backup. This is even true if you experience data loss due to a breach, hardware failure, or malfunctioning updates.

## WordPress and Azure Storage:

Azure Storage offloads the heavy lifting of datacenter management. Azure Storage consists of the following:

• File - Simple, distributed, cross-platform file system

• Disk - Persistent, high-performance disk storage for every workload

• Blob - Massively-scalable object storage for unstructured data

• Data Lake Storage - Secure, massively scalable data lake storage.

• Archive - Industry leading price point for storing rarely accessed data

• HPC Cache - File caching for high-performance computing

You can fix the image bloat in the WordPress Media Library by using Direct Access to Blob Storage via a hyperlink. Website content such as images & video are delivered by secure read-only https hyperlinks. Images and videos will not be uploaded into the website's wp-content/upload folder. The website is streamlined without embedded images, using only hyperlinks, allowing for easy moving of a website, faster page load times etc. Azure Storage Account Credentials are not exposed on the website's admin pages - even to Administrators. Easily provide SAS/ACCESS to Blob Storage container for other website content contributors via Azure Storage Explorer.

## WordPress and Azure Database for MySQL server:

Azure App Service integrates with Azure Database for MySQL to enable seamless deployment of popular web applications including WordPress. Easily build modern applications using Azure Container Service (AKS) and Azure Database for MySQL.

## WordPress and Azure Autoscale:

Azure provides built-in autoscaling for compute options such as Azure Virtual Machines, Service Fabric, Azure App Service, and Azure Cloud Service using Azure Monitor autoscale, and also provides Azure Functions that automatically allocates compute power, and custom autoscaling solution that uses Azure diagnostics and application-based metrics, along with custom code to monitor and export the application metrics. Setting up Azure autoscale on WordPress enables you to scale up resources to accommodate surges in the demand, and scale out with multiple instances when your server CPU is pegged or on a pre-defined schedule. Azure autoscale provides resources available on a global scale that smaller hosts have a hard time matching, and ensures that your services are maximally available regardless of traffic load.

## WordPress and Azure Content Delivery Network (CDN):

Azure Content Delivery Network (CDN) lets you reduce load times, save bandwidth and speed responsiveness. CDN works seamlessly with Azure services, including Web Apps, Media Services, Storage and Cloud Services. With its distributed, global presence, Content Delivery Network (CDN) easily handles sudden traffic spikes and heavy loads. Azure offers an integrated Content Delivery Network (CDN) that can cache high-bandwidth static content for faster delivery. Azure uses edge servers to speed delivery of dynamic content. The benefits of using Azure Content Delivery Network (CDN) to cache WordPress website assets include:

• Better performance and user experience especially when multiple round-trips are required to load content

• Large scaling to better handle instantaneous high load

• By distributing user requests and serving content from edge servers, less traffic is sent to the origin

• Used in conjunction with Caching, Azure Content Delivery Network (CDN) can considerably speed up the page loading time of WordPress website using Themes that have page-builder functionality, and lots of JS and CSS to load with each page request

**Note:**

You can integrate an Azure Storage account with Azure Content Delivery Network (CDN) by enabling it to cache content from Azure Storage.

## WordPress and Azure Application Insights:

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. You can use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app. It's designed to help you continuously improve performance and usability. You can determine your WordPress web app usage with Application Insights. Application Insights has a range of benefits and uses in relation to monitoring of your application and site, in relation to WordPress.com - benefits of using Application Insights include:

• Usage Analysis: View how users interact with your WordPress.com site

• Profiler: Inspect the execution profiles of sampled requests

• Diagnostic Searching: Search and filter events such as requests, exceptions, dependency calls, log traces, and page views

## WordPress and Azure Key Vault:

Azure Key Vault is a centralized cloud service for storing application secrets such as encryption keys, certificates, and server-side tokens. Key Vault helps you control your applications' secrets by keeping them in a single central location and providing secure access, permissions control, and access logging. There are three primary concepts used in an Azure Key Vault: vaults, keys, and secrets. With these three elements, an Azure Key Vault helps address the following issues:

• Secrets management: Azure Key Vault can securely store (with HSMs) and tightly control access to tokens, passwords, certificates, API keys, and other secrets.

• Key management: Azure Key Vault is a cloud-based key management solution, making it easier to create and control the encryption keys used to encrypt your data. Azure services such as App Service integrate directly with Azure Key Vault and can decrypt secrets without knowledge of the encryption keys.

• Certificate management: Azure Key Vault is also a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with Azure and your internal connected resources. It can also request and renew TLS certificates through partnerships with certificate authorities, providing a robust solution for certificate lifecycle management.

From WordPress, it is possible to retrieve secret stored in Azure Key Vault and also from WordPress installed in Docker Image (Web App for Containers). [[2]](#footnote-2)

## WordPress and Azure App Service Managed Certificates:

 In Azure, to add wildcard certificates for multiple domain and sub-domain Development, QA, and Production Azure-hosted websites, you can use **Let's Encrypt**, the free, automated, and open CA for Azure-hosted websites.

**Note:**

The **Let's Encrypt** certificates expire after 90 days, so a background process using Azure Web Jobs, is necessary to automatically renew and install new certificates. There's **Let's Encrypt Site Extension (Beta)** to do all of the work of requesting, installing and renewing of the Let's Encrypt certificates. Please take note that this Site Extension is beta-software.

**Update:**

Azure now supports free SSL certificates with **App Service Managed Certificates**, which is in preview and currently doesn't support the apex/naked domain. The free Transport Layer Security (TLS) for Azure App Service will let you secure custom domains on your Windows and Linux apps at no additional charge. This provides developers a zero-cost option to work on their Development, QA, and Production sites. The certificate issued will be a standard certificate and not a wildcard certificate. Each certificate will be valid for six months, and about a month before the certificate's expiration date, App Service will renew the certificate.

### Azure: App Service Managed Certificates vs. App Service Certificates

The offering for App Service Certificates will still be available with the launch of App Service Managed Certificates as these two features have their differences and are better suited for different scenarios. Aside from the main difference of pricing, a major difference between the two is that you will not be able to export your App Service Managed Certificates as they are managed by the platform. If you're planning to do a live site migration with TXT record, need support for apex domains, or need a wildcard certificate, then use App Service Certificates or bring your own certificate.

#### Wildcard SSL certificates vs. regular SSL certificates

**Similarities:**

• Regardless of what type of SSL certificate you get, they both provide the same industry-standard encryption strength

• Both come standard with 2048-bit RSA signature keys and facilitate encryption up to 256 bits

**Differences:**

• Regular (standard garden variety single domain) SSL certificates provide encryption for one domain (and technically one sub-domain)

• Wildcards secure websites with multiple sub-domains

**Wildcard certificates drawbacks:**

The drawbacks come from sharing the same private key across all of your subdomains. If your entire site is on one server, that doesn't really matter. But if your subdomains are on different servers, you'll have to move/share your private key. If you are securing multiple public-facing sub-domains, a compromised key would impact the security of all of your subdomains instead of just one. Additionally, there is no Extended Validation (EV) option for Wildcards to activate the green address bar. That's a security decision that will likely never change, so if you want Extended Validation (EV) on your sub-domains it may be better to use an Extended Validation (EV) Multi-Domain certificate.

**Bottom line:**

Choose wildcard SSL certificates if your website has multiple subdomains, despite drawbacks for most sites the pros outweigh the cons.

## WordPress and Azure Web App for Containers:

Web App for Containers provides a flexible way to use Docker images. Azure App Service is a fully managed compute platform that is optimized for hosting websites and web applications. You can use App Service on Linux to host web apps natively on Linux for supported application stacks. App Service on Linux supports a number of Built-in images in order to increase developer productivity. If the runtime your application requires is not supported in the built-in images you can build your own Docker image to deploy to Web App for Containers. Docker makes it to get a WordPress website up and running. There are two different ways of running containers in Azure - first just by using a regular Virtual Machine, and second with Azure Container Instances. Web App for Containers is simply a way of hosting your web application on App Service as a container (Linux or Windows). The advantage of doing this is that App Service offers many features ideally suited to web applications such as configuring custom domains and SSL certificates, slot swapping, CI/CD functionality, auto-scaling, IP address whitelisting, AD authentication and much more. Azure Web App for Containers is an ideal hosting platform for containerized web applications like WordPress. You benefit from many added value web hosting features that App Service has to offer, as well as the cost benefits of being able to host multiple containerized web apps on the same App Service plan.

**Note:**

• Multi-container app (in Web App for Containers) is in preview

• You can enable a TLS endpoint in a sidecar container by creating a container group with an application container and a sidecar container running a TLS/SSL provider, by setting up a container group with a separate TLS endpoint, you enable TLS connections for your application without changing your application code

## WordPress and Azure Kubernetes Service (AKS):

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment and makes it simple to deploy and manage containerized applications in Azure. Your AKS environment is enabled with features such as automated updates, self-healing, and easy scaling. The Kubernetes cluster master is managed by Azure and is free. You manage the agent nodes in the cluster and only pay for the VMs on which your nodes run. Azure Kubernetes Service (AKS) supports the Docker image format that means that you can use any development environment to create a workload, package the workload as a container and deploy the container as a Kubernetes pod. Apart from the standard Kubernetes command-line tools or the Azure CLI, Azure Kubernetes Service (AKS) also supports all the popular development and management tools such as Helm. You can use Helm for setting up WordPress on top of an Azure Kubernetes Service (AKS) cluster, in order to create a highly-available website. In addition to leveraging the intrinsic scalability and high availability aspects of Kubernetes, the setup will help keeping WordPress secure by providing simplified upgrade and rollback workflows via Helm.

**Why host WordPress in Docker and K8s?**

• Fully scripted and source controllable deployment

• Easy to deploy to dev/test/live

• Managed Linux machine on live

• Security - easy to update

• Cost - higher density of applications on VMs

## WordPress Azure Plugins for in-house development:

• WordPress plugin for Azure Storage

• WordPress plugin for Azure Content Delivery Network (CDN)

• WordPress plugin for Azure Application Insights

**Note:**

The existing third party WordPress plugins have fewer active installations, poorly rated/maintained, and are even dumped. For in-house development, Performance, Patching, and Security will have to be considered, and a RACI for DevOps produced. Proagrica has no operational responsibility for the site once it is delivered, therefore it has to be ensured that HomeAgain understands their responsibilities once the site is live.

# Case Study: Highly Scalable and Secure WordPress Website

This example scenario is applicable to a highly scalable and secure installation of WordPress. This scenario is based on a deployment that was used for a large convention and was successfully able to scale to meet the spike traffic that sessions drove to the site.

## Relevant use cases:

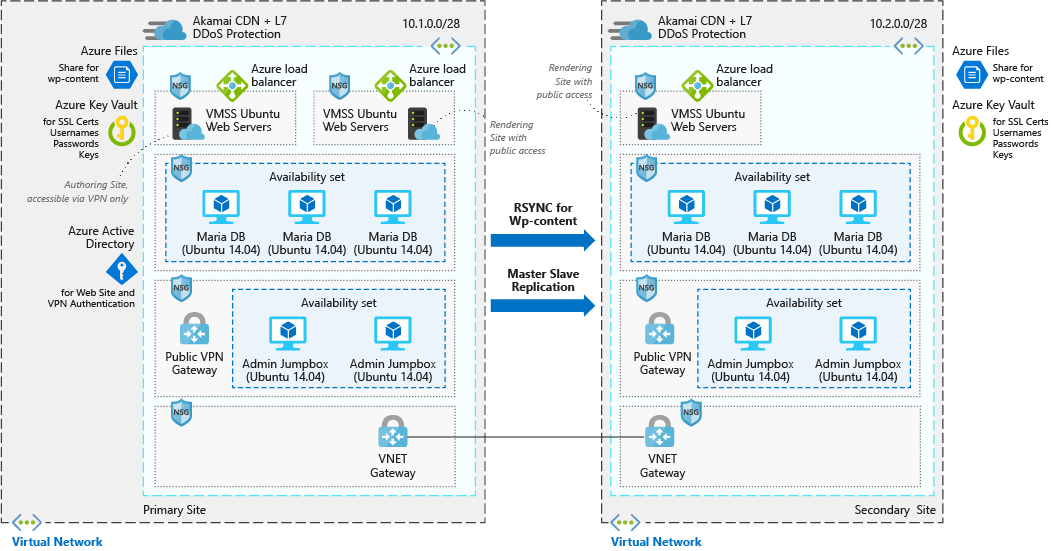
• Media events that cause traffic surges

• Blogs that use WordPress as their content management system

• Business or e-commerce websites that use WordPress

• Web sites built using other content management systems

## Architecture:



This scenario covers a scalable and secure installation of WordPress that uses Ubuntu web servers and MariaDB. There are two distinct data flows in this scenario the first is users access the website:

1. Users access the front-end website through a CDN.

2. The CDN uses an Azure load balancer as the origin, and pulls any data that isn't cached from there.

3. The Azure load balancer distributes requests to the virtual machine scale sets of web servers.

4. The WordPress application pulls any dynamic information out of the Maria DB clusters, all static content is hosted in Azure Files.

5. SSL keys are stored in Azure Key Vault.

The second workflow is how authors contribute new content:

1. Authors connect securely to the public VPN gateway.

2. VPN authentication information is stored in Azure Active Directory.

3. A connection is then established to the Admin jump boxes.

4. From the admin jump box, the author is then able to connect to the Azure load balancer for the authoring cluster.

5. The Azure load balancer distributes traffic to the virtual machine scale sets of web servers that have write access to the Maria DB cluster.

6. New static content is uploaded to Azure files and dynamic content is written into the Maria DB cluster.

7. These changes are then replicated to the alternate region via rsync or primary/secondary replication.

## Components:

• Azure Content Delivery Network (CDN)

• Virtual networks

• Network security

• Load balancers

• Virtual machine scale sets

• Azure Files

• Azure Key Vault

• Azure Active Directory (Azure AD)

## Alternatives:

• Azure database for MySQL can replace the MariaDB data store if you prefer a fully managed solution

• SQL Server for Linux can replace the MariaDB data store

## Considerations:

• Availability: The VM instances in this scenario are deployed across multiple regions, with the data replicated between the two via RSYNC for the WordPress content and primary/secondary replication for the MariaDB clusters.

• Scalability: This scenario uses virtual machine scale sets for the two front-end web server clusters in each region. With scale sets, the number of VM instances that run the front-end application tier can automatically scale in response to customer demand, or based on a defined schedule.

• Security: All the virtual network traffic into the front-end application tier and protected by network security groups. Rules limit the flow of traffic so that only the front-end application tier VM instances can access the back-end database tier. No outbound Internet traffic is allowed from the database tier. To reduce the attack footprint, no direct remote management ports are open.

• Resiliency: In combination with the use of multiple regions, data replication and virtual machine scale sets, this scenario uses Azure load balancers. These networking components distribute traffic to the connected VM instances, and include health probes that ensure traffic is only distributed to healthy VMs. All of these networking components are fronted via a CDN. This makes the networking resources and application resilient to issues that would otherwise disrupt traffic and impact end-user access.

# WordPress VIP:

WordPress VIP is an enterprise fully-managed platform. It allows customers to put away the technical hassle and focus on business. Besides scalability and high-security standards, WP VIP offers 24/7 support, instant bug fixing, domain, cloud hosting, system updates, hourly backups, updates for the core software, and other tech issues that add much to the performance.

## Features of WordPress VIP:

• Security: A custom-built infrastructure protects all the websites. The proactive guard system blocks most types of attacks. All the website traffic is completely encrypted from edge to origin to ensure efficient brute force blockage and other types of attacks. Every piece of custom code undergoes manual review. It adds another security layer to protect websites from potentially vulnerable codes.

• Manual code reviews: It engages the pre-deploy code review process. The staff members check every single line of code manually before deployment. Such strict regulations always result in quality coding and website efficiency, so it takes some time before officially going live, from 10 to 15 working days.

• High optimization: You don't have to worry about code optimization, WordPress VIP plugins, caching, or CDN service. The whole delivery network of 20 data centers worldwide serve the platform. It ensures that users have the best time-to-first byte result, SSL security, latency, and protection against Distributed Denial-of-Service (DDoS) attacks.

## Benefits of WordPress VIP:

1. Fully managed WordPress hosting platform

2. Automatic updates for core software

3. Manual review for third-party plugins and custom codes

4. Automatic scaling to handle massive traffic spikes

5. Automated hourly backups

6. Unlimited storage, bandwidth, CDN, and dedicated support

7. Code pre-deployment

8. Uptime and performance monitoring

9. The fully guided onboarding with step-by-step support

10. Training from the team that is carried out in person or virtually

# Magento 2.3 Technology Stack Requirements: [[3]](#footnote-3)

**Operating systems (Linux x86-64)**

• Linux distributions, such as RedHat Enterprise Linux (RHEL), CentOS, Ubuntu, Debian, and similar.

**Note:**

Magento is not supported on Windows OS and Mac OS.

**Web servers**

• Apache 2.4

• nginx 1.x

**Database**

• MySQL 5.6, 5.7

**PHP**

• ~7.1.3

• ~7.2.0

• ~7.3.0

**SSL**

• A valid security certificate is required for HTTPS.

• Self-signed SSL certificates are not supported.

• Transport Layer Security (TLS) requirement

# Magento on Azure

Azure offers a complete platform so merchants can get everything they need from a single cloud solution. An open and flexible platform supporting any operating system, language, tool, and framework, Azure provides merchants more choice and control to help them move faster, do more, and save money. Azure blends an enterprise-proven, hybrid cloud with one-click setup and easy-to-use monitoring technology to provide Magento merchants a platform with the scalability, flexibility, and reliability.

## How Magento Azure Integrations is beneficial for your E-commerce website?

Magento on Azure with the required APIs, third-party suites, extensions, custom modules can remove data errors and grow sales. It also leads to order fulfillment and helps you gain positive customer reviews. With prop integrations, a 360-degree view of your business is available for your communication channels.

• Empowers the online selling capabilities by offering the customers a smooth user journey.

• Standardizes the business procedure and grows online exposure.

• Identify and integrate the right modules that allow you to track all aspects of your business.

• A properly optimized analytics dashboard is available for each user to get reports and insights in real-time.

• It is simple for you to manage sales and marketing activities like campaigns.

• Integrating social media tools offer better visibility across different channels.

• With Magento + Azure Integrations right modules on your website can save your time and budget.

## Magento and Azure Database for MySQL server:

Azure App Service integrates with Azure Database for MySQL to enable seamless deployment of popular web applications including Magento. Easily build modern applications using Azure Container Service (AKS) and Azure Database for MySQL.

## Magento and Azure Resource Manager (ARM) Templates:

Azure Resource Manager (ARM) Templates are JavaScript Object Notation (JSON) files that define the infrastructure and configuration for your project. Advantages of using templates:

• Declarative syntax: ARM templates allow you to create and deploy an entire Azure infrastructure declaratively.

• Repeatable results: Templates are idempotent, which means you can deploy the same template many times and get the same resource types in the same state.

• Orchestration: Resource Manager orchestrates the deployment of interdependent resources so they're created in the correct order.

You can use an Azure Resource Manager (ARM) Templates to set up Magento. The template contains the source code and shell scripts for setting up a virtual machine on Azure and installing all the prerequisites and Magento on the created virtual machine, and also contains a file that creates a button. Users utilize that button to navigate to Azure in order to deploy the virtual machine and launch the Magento application.

## Magento and Azure Logic Apps:

Azure Logic Apps is a cloud service that automates the execution of your business processes. You use a graphical design tool called the Logic Apps Designer to arrange pre-made components into the sequence you need. The Designer sends a definition of your workflow to the Logic Apps execution engine. The execution engine launches your app when conditions are right and manages the compute resources needed to run it. You can trigger Magento IFTTT Flows in Azure App Service by adding Magento to an IFTTT (if-this-then-that) workflow by using Azure Logic Apps, such as creating a blank logic app, adding a trigger and an action, and then testing your logic app. To produce secure and Swagger-enabled Magento APIs, you can set up the API Server by deploying it on Azure, and use the API Server in a logic app to create process flows around Magento data. The HTTP + Swagger action provides a wizard to define the operations you want to execute to Magento. Then retrieve Magento data in the logic app.

## Magento and Azure Web App for Containers:

Azure Web App for Containers helps to smoothly deploy and run the containerized application on both Windows or Linux based environment. You can at any time scale up or scale down (For Web App for Container) as per your business needs. You can deploy Multi-Container Magento based application on Web App for Container.

## Magento and Azure Kubernetes Service (AKS):

You can deploy Magento into Azure AKS managed Kubernetes cluster for horizontal workload scalability and automatic load balancing in order to respond to outages, peak or incidental traffic. And also set up CI/CD pipelines, so you will be able to utilize the best DevOps practices for the development, testing, and deployment.

## Magento and Azure Data Factory:

Azure Data Factory is a data ingestion and transformation service that allows you to load raw data from over different on-premises or cloud sources. The ingested data can be cleaned, transformed, restructured, and loaded back into a data warehouse. After the data is in the data warehouse, it's ready to use for several analytical purposes. In other words, Azure Data Factory is a cloud-based ETL and data integration service that allows you to create data-driven workflows for orchestrating data movement and transforming data at scale. Using Azure Data Factory, you can create and schedule data-driven workflows (called pipelines) that can ingest data from disparate data stores. The Magento connector is supported for the following activities:

• Copy activity: In Azure Data Factory, you can use the Copy activity to copy data among data stores located on-premises and in the cloud. After you copy the data, you can use other activities to further transform and analyze it. You can also use the Copy activity to publish transformation and analysis results for business intelligence (BI) and application consumption. You can copy data from Magento using Azure Data Factory.

• Lookup activity: Lookup activity can retrieve a dataset from any of the Azure Data Factory-supported data sources. You can use it to dynamically determine which objects to operate on in a subsequent activity, instead of hard coding the object name. Some object examples are files and tables. Lookup activity reads and returns the content of a configuration file or table. It also returns the result of executing a query or stored procedure. The output from Lookup activity can be used in a subsequent copy or transformation activity if it's a singleton value. The output can be used in a ForEach activity if it's an array of attributes.

You can copy data from Magento to any supported sink data store. Azure Data Factory provides a built-in driver to enable connectivity, therefore you don't need to manually install any driver using this connector.

**Note:**

The Magento connector is currently in preview.

## Magento and Azure Synapse

Azure Synapse (formerly Azure SQL Data Warehouse) is a cloud-based petabyte-scale columnar database service with controls to manage compute and storage resources independently. It offers encryption of data at rest and dynamic data masking to mask sensitive data on the fly, and it integrates with Azure Active Directory. It can replicate to read-only databases in different geographic regions for load balancing and fault tolerance. You can extract data from Magento and load it into Azure Synapse. You can use the Magento API to extract information. Magento offers both REST and SOAP versions of its API. You can also pull data directly from the underlying database. Azure Synapse provides a multi-step process for loading data. After extracting the data from its source, you can move it to Azure Blob storage or Azure Data Lake Store. You can then use one of three utilities to load the data:

• AZCopy uses the public internet

• Azure ExpressRoute routes the data through a dedicated private connection to Azure, bypassing the public internet by using a VPN or point-to-point Ethernet network

• The Azure Data Factory (ADF) cloud service has a gateway that you can install on your local server, then use to create a pipeline to move data to Azure Storage

From Azure Storage you can load the data into Azure Synapse staging tables by using Microsoft's PolyBase technology. You can run any transformations you need while the data is in staging, then insert it into production tables.

You can set up a cron job to get new data as it appears in Magento.

# Case Study: An E-commerce Front End on Azure

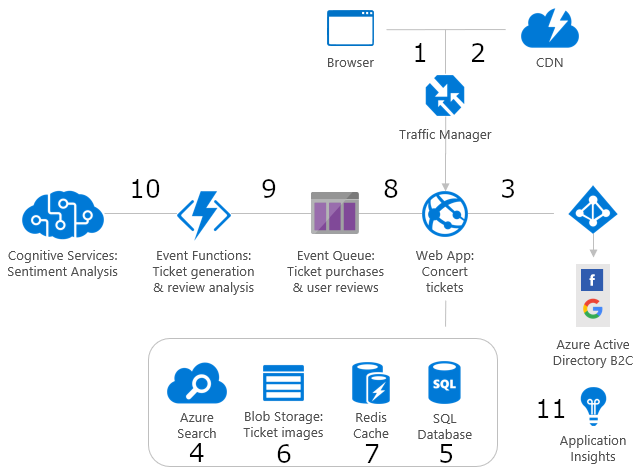
This example scenario walks you through an implementation of an e-commerce front end using Azure platform as a service (PaaS) tools. Many e-commerce websites face seasonality and traffic variability over time. When demand for your products or services takes off, whether predictably or unpredictably, using PaaS tools will allow you to handle more customers and more transactions automatically. Additionally, this scenario takes advantage of cloud economics by paying only for the capacity you use.

## Relevant use cases

• Building an application that needs elastic scale to handle bursts of users at different times.

• Building an application that is designed to operate at high availability in different Azure regions around the world.

## Architecture



This scenario covers purchasing tickets from an e-commerce site, the data flows through the scenario as follows:

1. Azure Traffic Manager routes a user's request to the e-commerce site hosted in Azure App Service.

2. Azure CDN serves static images and content to the user.

3. User signs in to the application through an Azure Active Directory B2C tenant.

4. User searches for concerts using Azure Search.

5. Web site pulls concert details from Azure SQL Database.

6. Web site refers to purchased ticket images in Blob Storage.

7. Database query results are cached in Azure Cache for Redis to improve performance.

8. User submits ticket orders and concert reviews, which are placed in the queue.

9. Azure Functions processes order payment and concert reviews.

10. Cognitive Services provides an analysis of the concert review to determine the sentiment (positive or negative).

11. Application Insights provides performance metrics for monitoring the health of the web application.

## Components

• Azure CDN

• Azure Traffic Manager

• App Services - Web Apps

• Azure Active Directory - B2C

• Storage Queues

• Cognitive Services

• Azure Search

• Storage Blobs

• Azure Cache for Redis

• SQL Database

• Application Insights

## Alternatives

• Service Fabric - A platform focused around building distributed components that benefit from being deployed and run across a cluster with a high degree of control. Service Fabric can also be used to host containers.

• Azure Kubernetes Service - A platform for building and deploying container-based solutions that can be used as one implementation of a microservices architecture. This allows for agility of different components of the application to be able to scale independently on demand.

• Azure Container Instances - A way of quickly deploying and running containers with a short lifecycle. Containers here are deployed to run a quick processing job such as processing a message or performing a calculation and then deprovisioned as soon as they are complete.

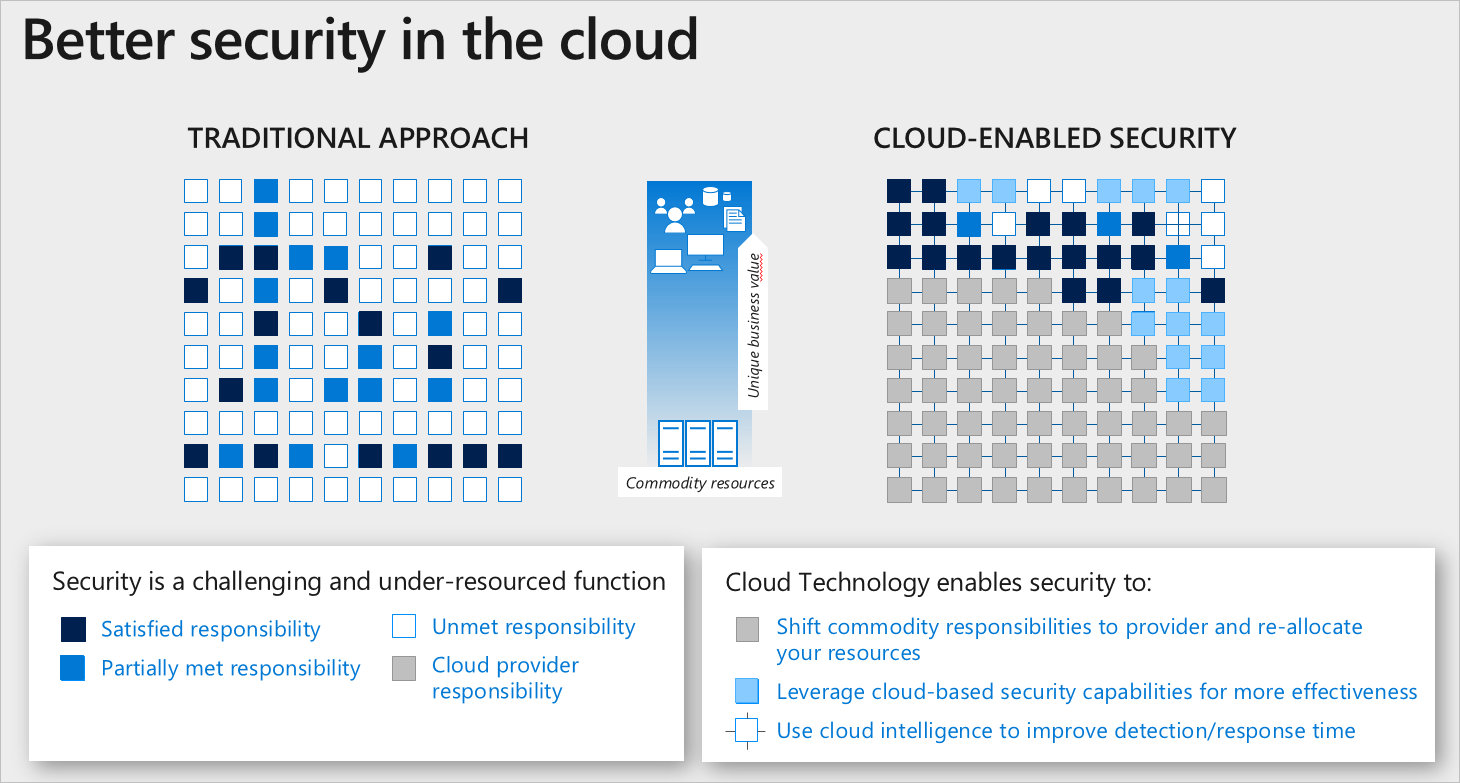
• Service Bus could be used in place of a Storage Queue.

Other options for the data tier include:

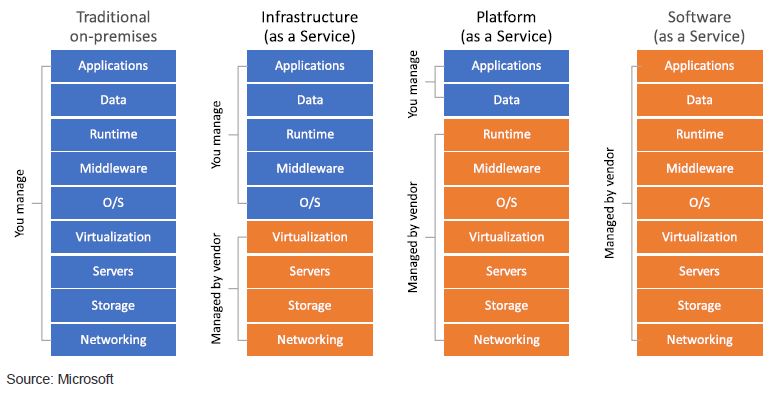
• Cosmos DB: Microsoft's globally distributed, multi-model database. This service provides a platform to run other data models such as Mongo DB, Cassandra, Graph data, or simple table storage.

# Azure Security

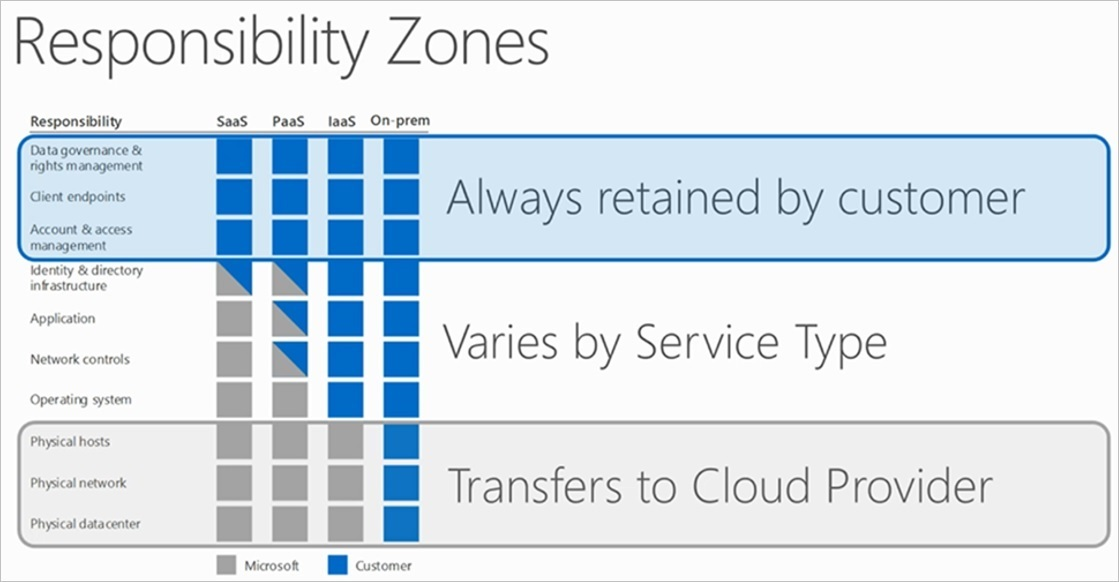
Azure is uniquely positioned to help organizations with the challenges such as securing their datacenters, using many security tools, and keeping pace with the volume and complexity of threats. Azure helps protect business assets while reducing security costs and complexity. Built-in security controls and intelligence help admins easily identify and respond to threats and security gaps, so organizations can rapidly improve their security posture. By shifting responsibilities to Azure, organizations can get more security coverage - which enables them to move security resources and budget to other business priorities.



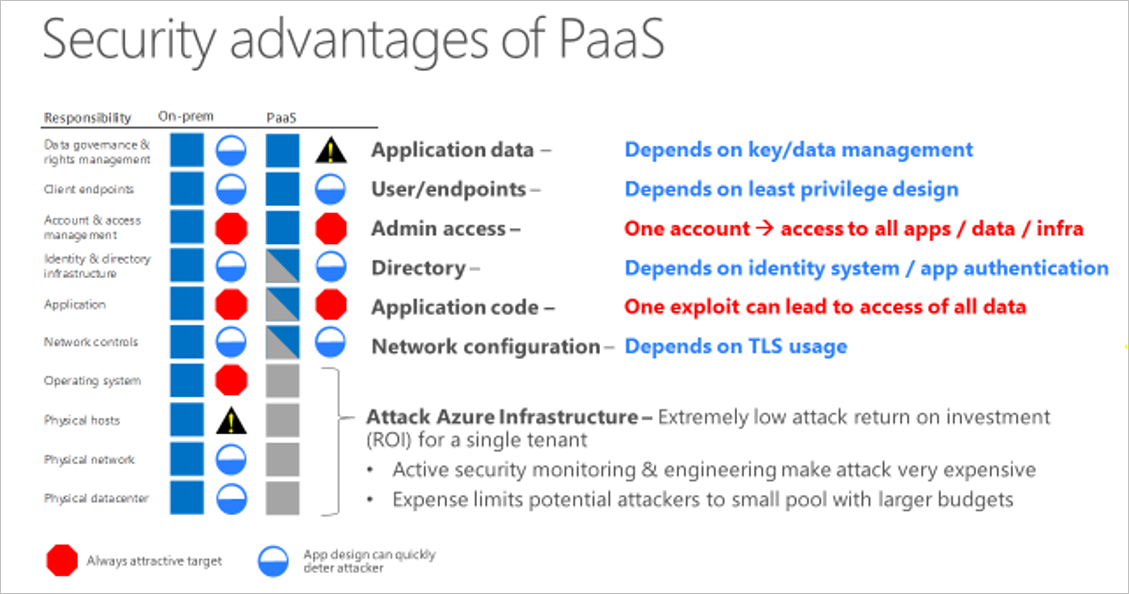
## Shared responsibility model for the cloud



Here's the division of responsibility between you and Microsoft. On-premises, you own the whole stack. But as you move to the cloud, some responsibilities transfer to Microsoft. Microsoft provides a secure foundation across physical, infrastructure, and operational security. Physical security refers to how Microsoft takes a multilayered approach to protect its datacenters. Network infrastructure, firmware and hardware, and continuous testing and monitoring make up the Azure infrastructure. Operational security consists of different security teams at Microsoft that work to mitigate risks across the security landscape. The following figure shows the areas of the stack on-premises and in a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) deployment that you and Microsoft are responsible for.



## Security advantages of an Azure PaaS:



Starting at the bottom of the stack, the physical infrastructure, Microsoft mitigates common risks and responsibilities. Because the Microsoft cloud is continually monitored by Microsoft, it is hard to attack. It doesn't make sense for an attacker to pursue the Microsoft cloud as a target. Unless the attacker has lots of money and resources, the attacker is likely to move on to another target. In the middle of the stack, there is no difference between a PaaS deployment and on-premises. At the application layer and the account and access management layer, you have similar risks. At the top of the stack, data governance and rights management, you take on one risk that can be mitigated by key management. While key management is an additional responsibility, you have areas in a PaaS deployment that you no longer have to manage so you can shift resources to key management. The Azure platform also provides you strong Distributed Denial-of-Service (DDoS) protection by using various network-based technologies. However, all types of network-based Distributed Denial-of-Service (DDoS) protection methods have their limits on a per-link and per-datacenter basis. To help avoid the impact of large Distributed Denial-of-Service (DDoS) attacks, you can take advantage of Azure's core cloud capability of enabling you to quickly and automatically scale out to defend against Distributed Denial-of-Service (DDoS) attacks. We'll go into more detail on how you can do this in the recommended practices articles.

## Security advantages of Azure IaaS

• Improves business continuity and disaster recovery: Achieving high availability, business continuity, and disaster recovery is expensive, since it requires a significant amount of technology and staff. But with the right service level agreement (SLA) in place, IaaS can reduce this cost and access applications and data as usual during a disaster or outage.

• Increase stability, reliability, and supportability: With IaaS there's no need to maintain and upgrade software and hardware or troubleshoot equipment problems. With the appropriate agreement in place, the service provider assures that your infrastructure is reliable and meets SLAs.

• Better security: With the appropriate service agreement, a cloud service provider can provide security for your applications and data that may be better than what you can attain in-house.

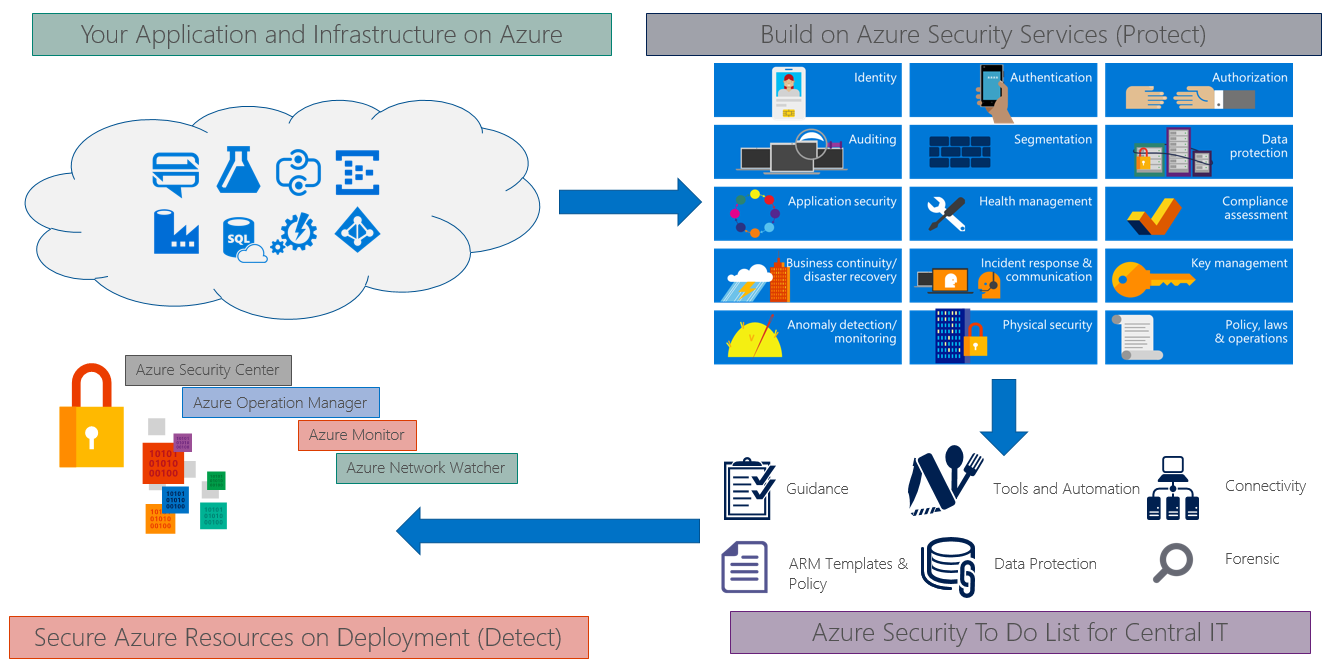
• Azure Virtual Network: An Azure virtual network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure network fabric dedicated to your subscription. You can fully control the IP address blocks, DNS settings, security policies, and route tables within this network. You can segment your VNet into subnets and place Azure IaaS virtual machines (VMs) on Azure Virtual Networks.

• Antimalware & Antivirus: With Azure IaaS, you can use antimalware software from security vendors to protect your virtual machines from malicious files, adware, and other threats. Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a protection capability that helps identify and remove viruses, spyware, and other malicious software. Microsoft Antimalware provides configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems. Microsoft Antimalware can also be deployed using Azure Security Center.

• VM Disk Encryption: Azure Disk Encryption is a new capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. It applies the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your Key Vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in your Azure storage.

## Azure Security Technical Capabilities

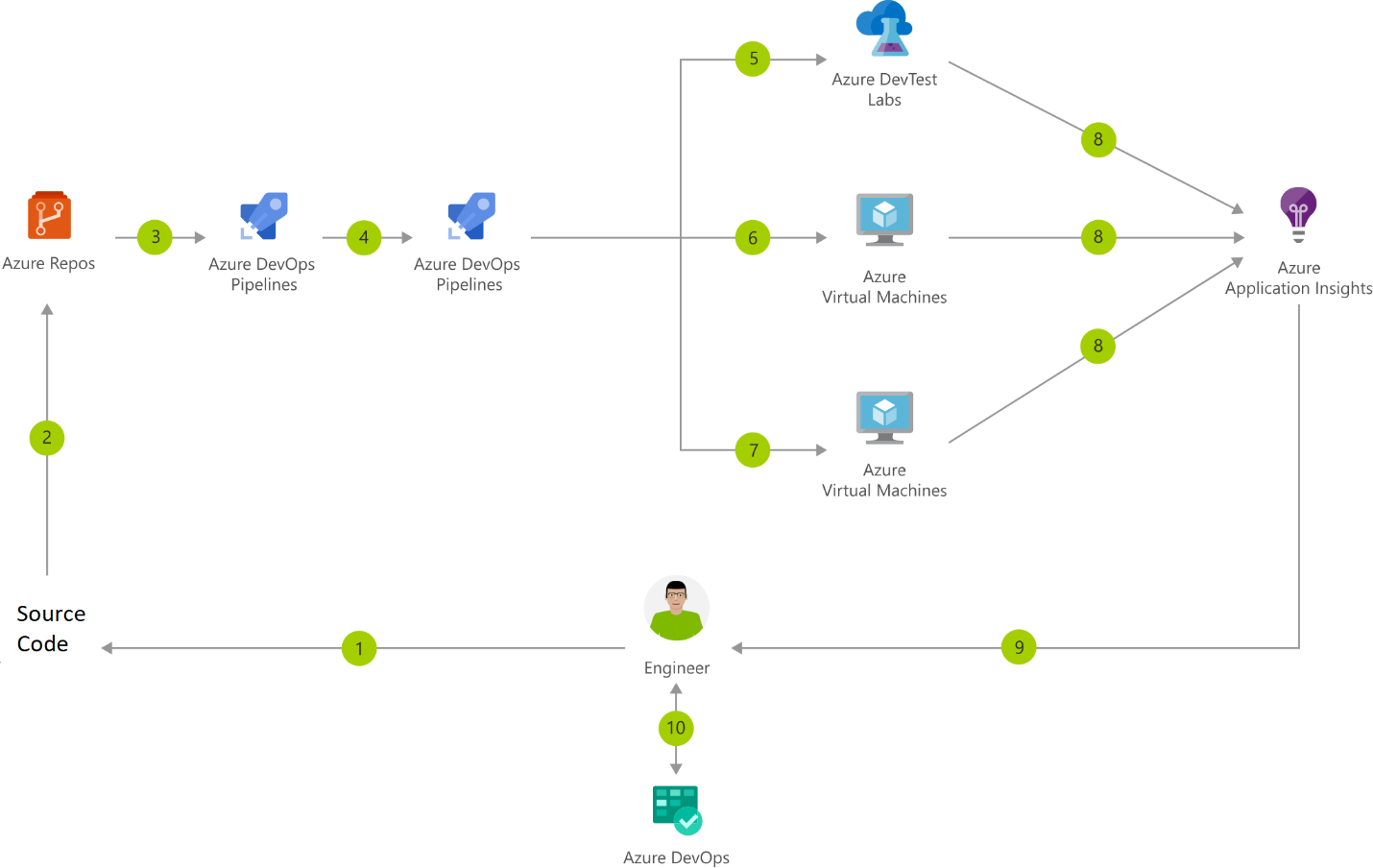
Microsoft Azure provides services that help you meet your security, privacy, and compliance needs. The following picture helps explain various Azure services available for you to build a secure and compliant application infrastructure based on industry standards.



# Azure CI/CD

Azure DevOps provides the CI/CD pipeline, starting with a Git repository for managing your application source code and infrastructure code (ARM templates), a Build system for producing packages and other build artifacts, and a Release Management system for setting up a pipeline to deploy your changes through dev, test, and production environments. The pipeline uses ARM templates to provision or update your infrastructure as necessary in each environment, and then deploys the updated build. You can also use Azure DevTest Labs to automatically tear down test resources that are not in use.

## CI/CD for Azure VMs



### Data Flow

1. Change application source code

2. Commit Application Code and Azure Resource Manager (ARM) Template

3. Continuous integration triggers application build and unit tests

4. Continuous deployment trigger orchestrates deployment of application artifacts with environment-specific parameters

5. Deployment to QA environment

6. Deployment to staging environment

7. Deployment to production environment

8. Application Insights collects and analyses health, performance, and usage data

9. Review health, performance and usage information

10. Update backlog item

### Components

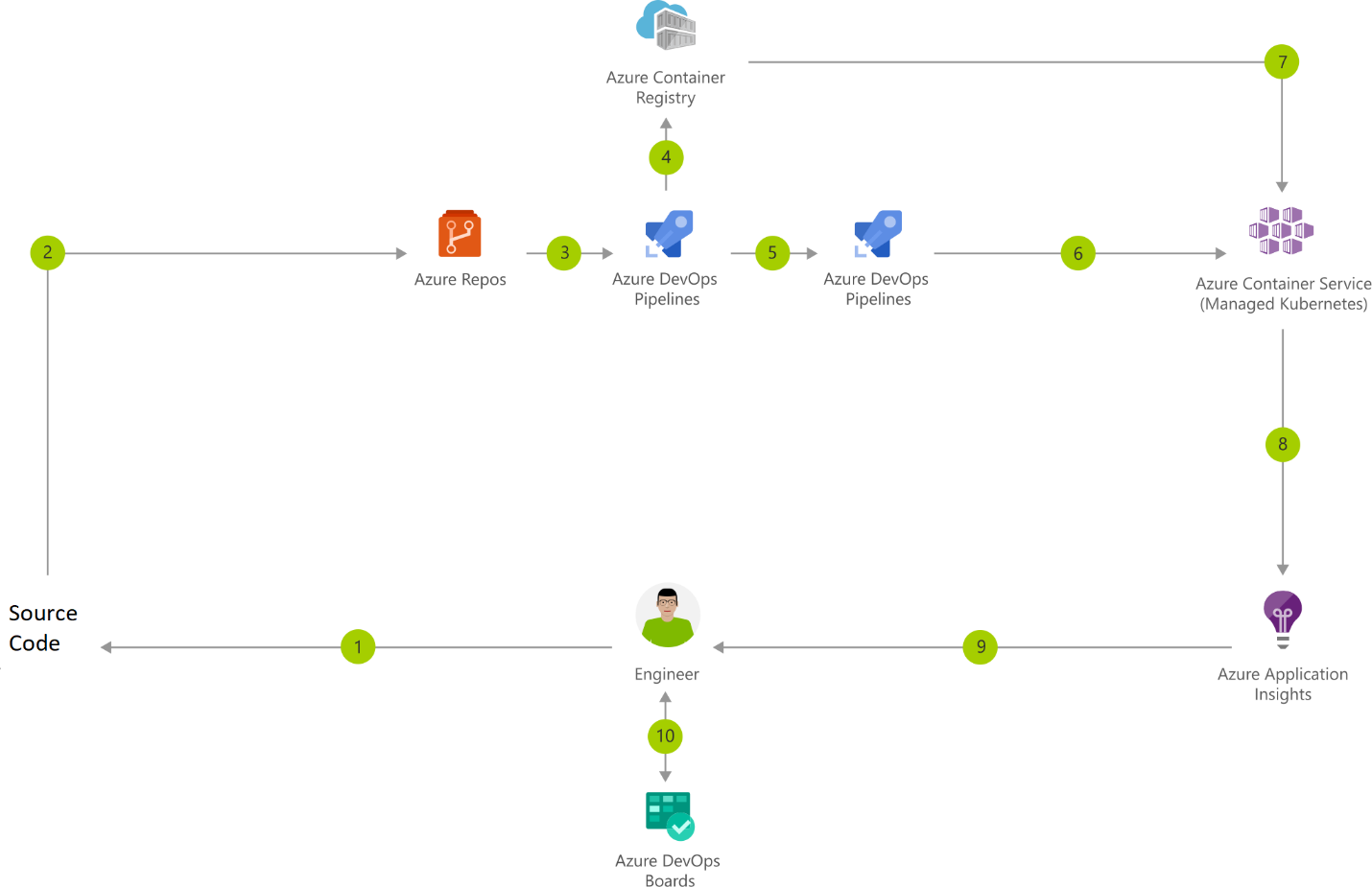
• Virtual Machines: Provision Windows and Linux virtual machines in seconds

• Azure DevTest Labs: Quickly create environments using reusable templates and artifacts

• Application Insights: Detect, triage, and diagnose issues in your web apps and services.

• Azure DevOps: Build and deploy multi-platform apps to get the most from Azure services

## CI/CD for Containers



### Data Flow

1. Change application source code

2. Commit Application Code

3. Continuous integration triggers application build, container image build and unit tests

4. Container image pushed to Azure Container Registry

5. Continuous deployment trigger orchestrates deployment of application artifacts with environment-specific parameters

6. Deployment to Azure Kubernetes Service (AKS)

7. Container is launched using Container Image from Azure Container Registry

8. Application Insights collects and analyses health, performance, and usage data

9. Review health, performance and usage information

10. Update backlog item

### Components

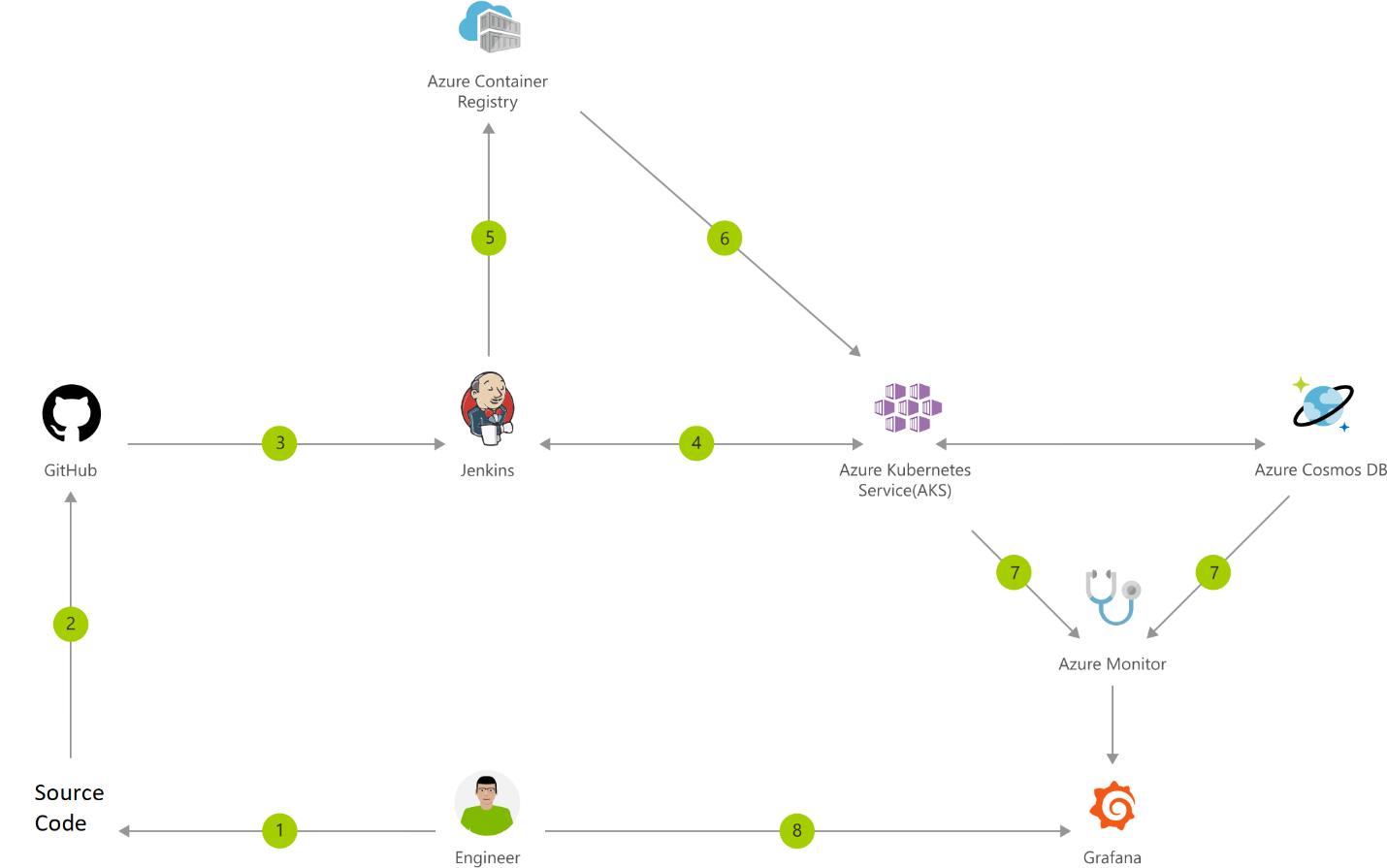
• Container Registry: Store and manage container images across all types of Azure deployments

• Azure Kubernetes Service (AKS): Simplify the deployment, management, and operations of Kubernetes

• Application Insights: Detect, triage, and diagnose issues in your web apps and services

• Azure DevOps: Build and deploy multi-platform apps to get the most from Azure services

## Container CI/CD using Jenkins and Kubernetes on Azure Kubernetes Service (AKS)



### Data Flow

1. Change application source code.

2. Commit code to GitHub.

3. Continuous Integration Trigger to Jenkins.

4. Jenkins triggers a build job using Azure Kubernetes Service (AKS) for a dynamic build agent.

5. Jenkins builds and pushes Docker container to Azure Container Registry.

6. Jenkins deploys your new containerized app to Kubernetes on Azure.

7. Container Service (AKS), backed by Azure Cosmos DB.

8. Grafana displays visualization of infrastructure and application metrics via Azure Monitor.

9. Monitor application and make improvements.

### Components

• Azure Kubernetes Service (AKS): Simplify the deployment, management, and operations of Kubernetes.

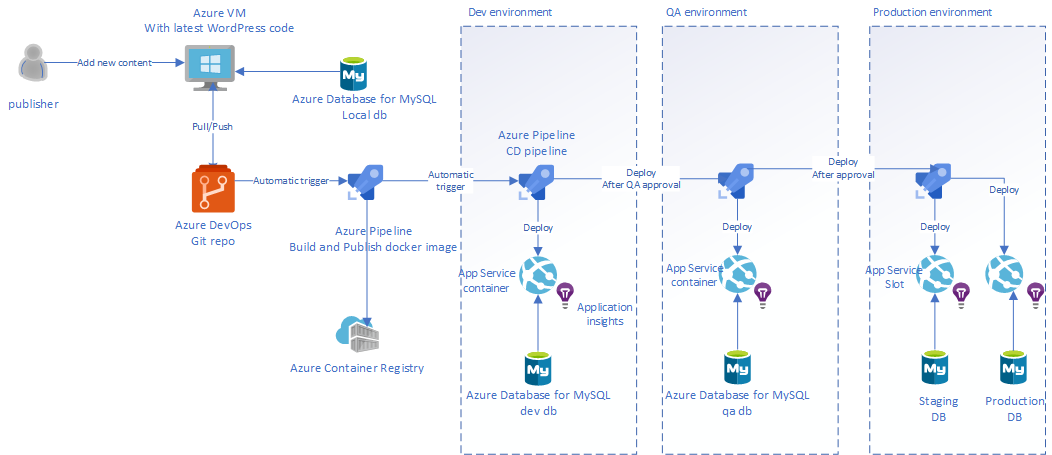
• Container Registry: Store and manage container images across all types of Azure deployments.

• Azure Cosmos DB: Globally distributed, multi-model database for any scale.

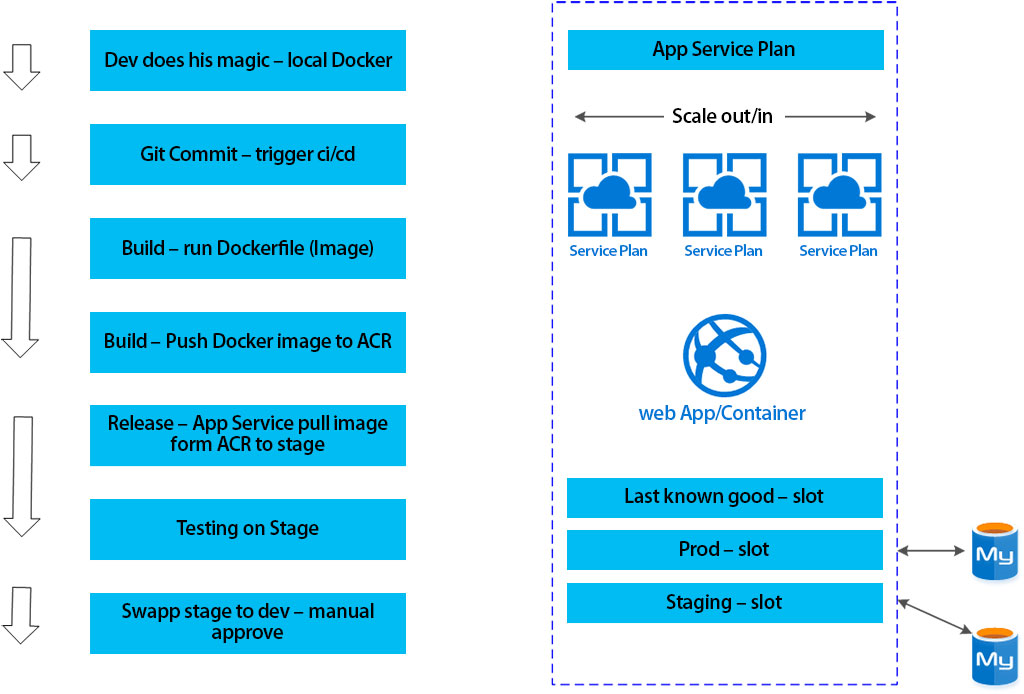
• Azure Monitor: Highly granular and real-time monitoring data for any Azure resource.

# WordPress and Azure DevOps

## WordPress in Azure App Service Containers using Docker



Environments: Development, QA, and Production. The Development environment is for the developer to run the Docker images locally, commit the required changes, and push the code to the Azure DevOps Git repo. The push action will initiate a CI process, which will build and push a new Docker image to the Azure Container Registry. Then WordPress Docker image is built on the basis of a Dockerfile. Azure Database for MySQL is the WordPress database and each environment will have a separate database that will be synced with one another by performing database export from one environment to another. Azure Application Insights is used for logging and monitoring purposes.



### Components

• WordPress Docker image built on the basis of a Dockerfile

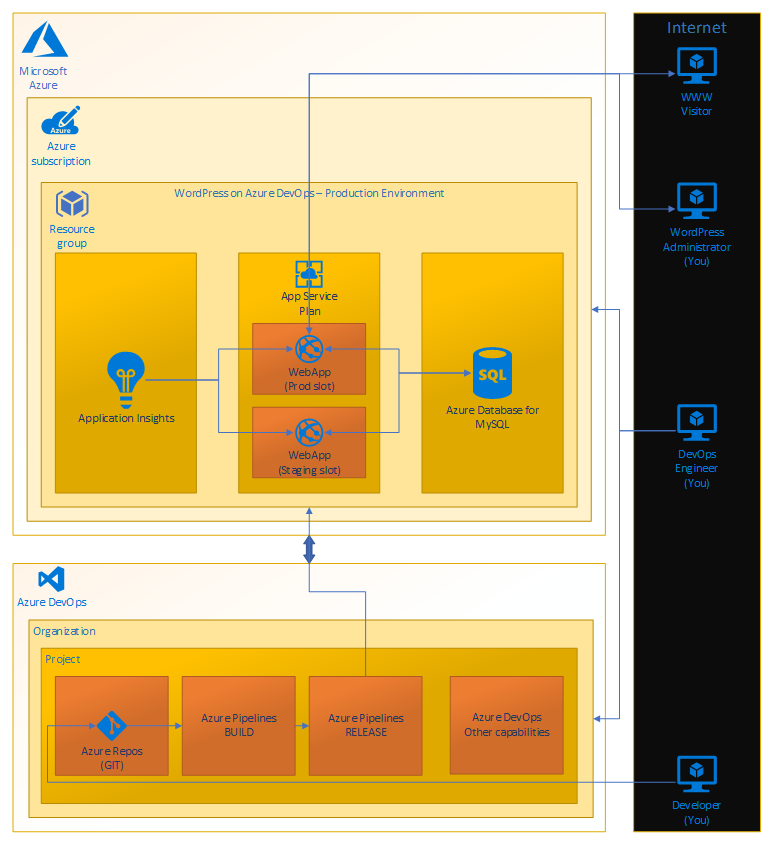
• Azure Repos - Docker WordPress project and WordPress development project

• Developer station with Docker Containers and Git installed on it - Git clone from Azure DevOps Git repo for local development (or work directly with Azure App Service)

• Azure Container Registry (ACR) for Private Registry - Link Azure Container Registry (ACR) with Azure App Service which hosts the site

• Azure DevOps - Execute the pipeline

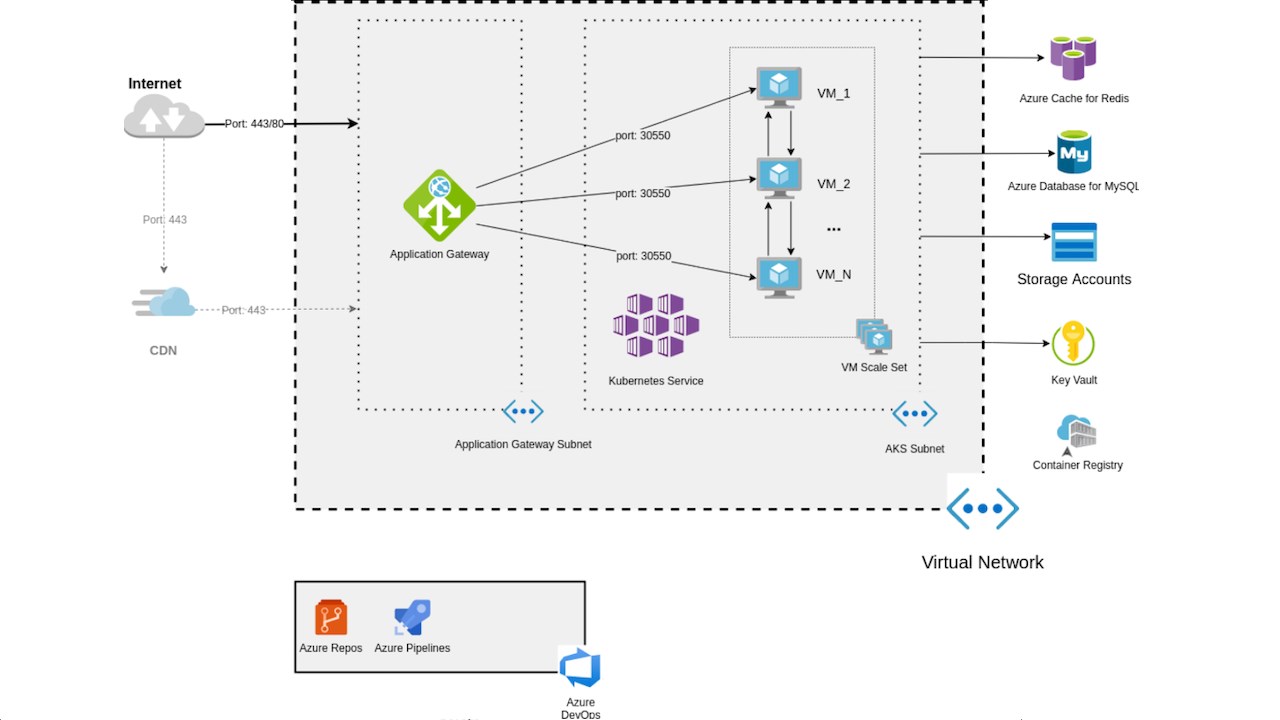
## WordPress in Web App Production and Staging Slots



The main part of the WordPress application is in the Web App Production slot. This is basically both front-end and back-end in one. MySQL database is running on extra server, where the WordPress articles are stored. On the left side there is Application Insights which monitors the Web App performance. Besides the Web App Production slot, there is a Web App Staging slot. It is utilized during application deployment process and ensures there is no Production outage. It provides an easy roll-back option as well. These infrastructure components lie within Microsoft Azure. Below the Microsoft Azure there is Azure DevOps. Azure Repos holds the WordPress source code. This is input for the build pipeline which composes the application into an installation package. The last step is release pipeline which takes the package and deploys it into our Production environment.

# Magento and Azure DevOps

## Magento in Azure Kubernetes Service (AKS)



## Components

• Magento application components deployed into Azure Kubernetes Service (AKS) managed Kubernetes cluster for horizontal workload scalability and load balancing in order to respond to outages, peak or incidental traffic

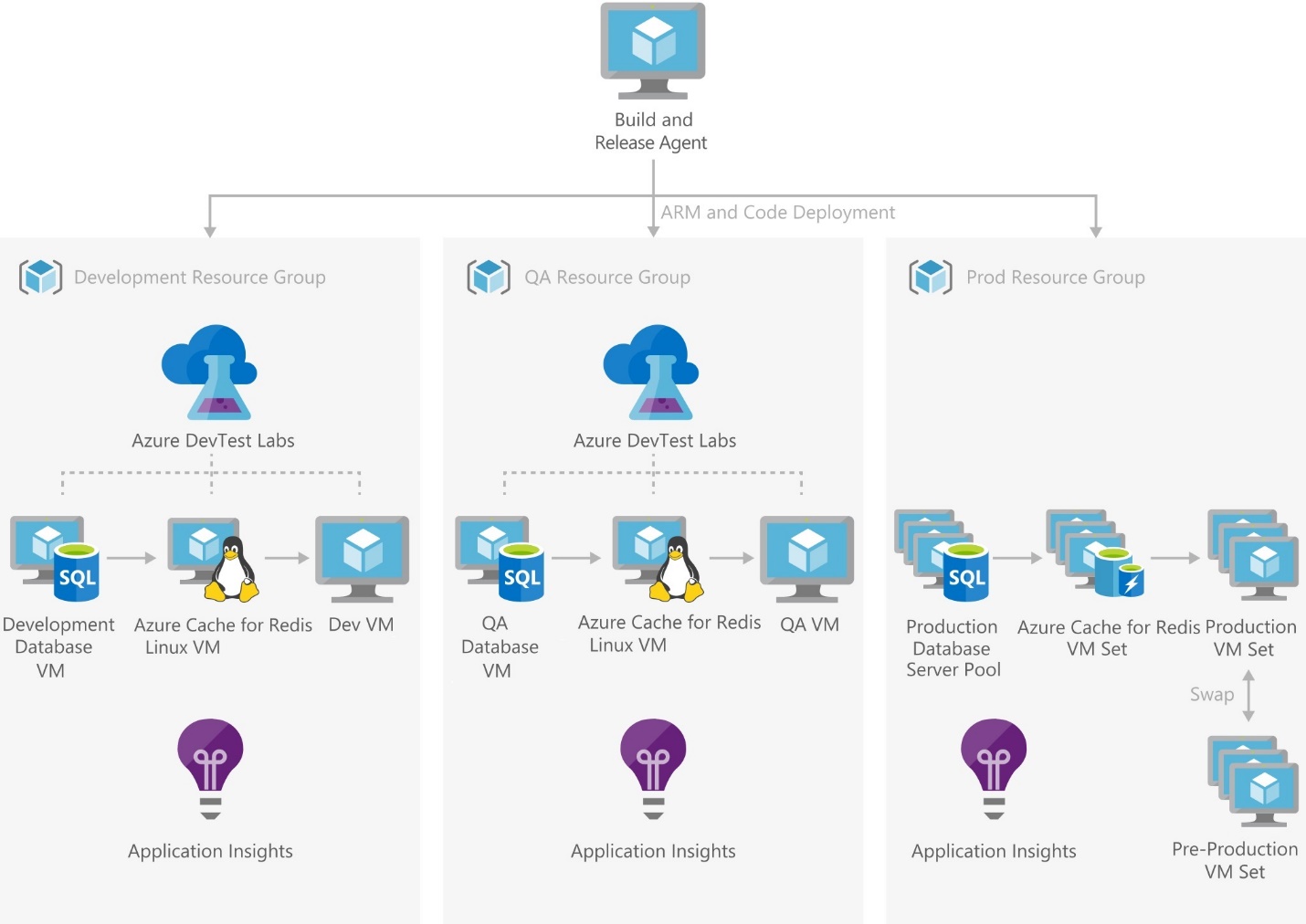
• Azure Kubernetes orchestration using Azure Kubernetes Service (AKS)

• Azure CI/CD pipelines for Development, QA, and Production environments in Kubernetes cluster

# Azure Dev-Test Labs

Azure Dev-Test helps configure your infrastructure for development and testing of a standard system, built on the Azure managed services that run in a high-availability environment, patched, and supported, allowing you to focus on your solution instead of the environment they run in.

## Dev-Test Deployment for Testing IaaS Solutions



### Components

• Azure DevOps manages the development process.

• The Microsoft Release Management build and release agents deploy the Azure Resource Manager template and associated code to the various environments.

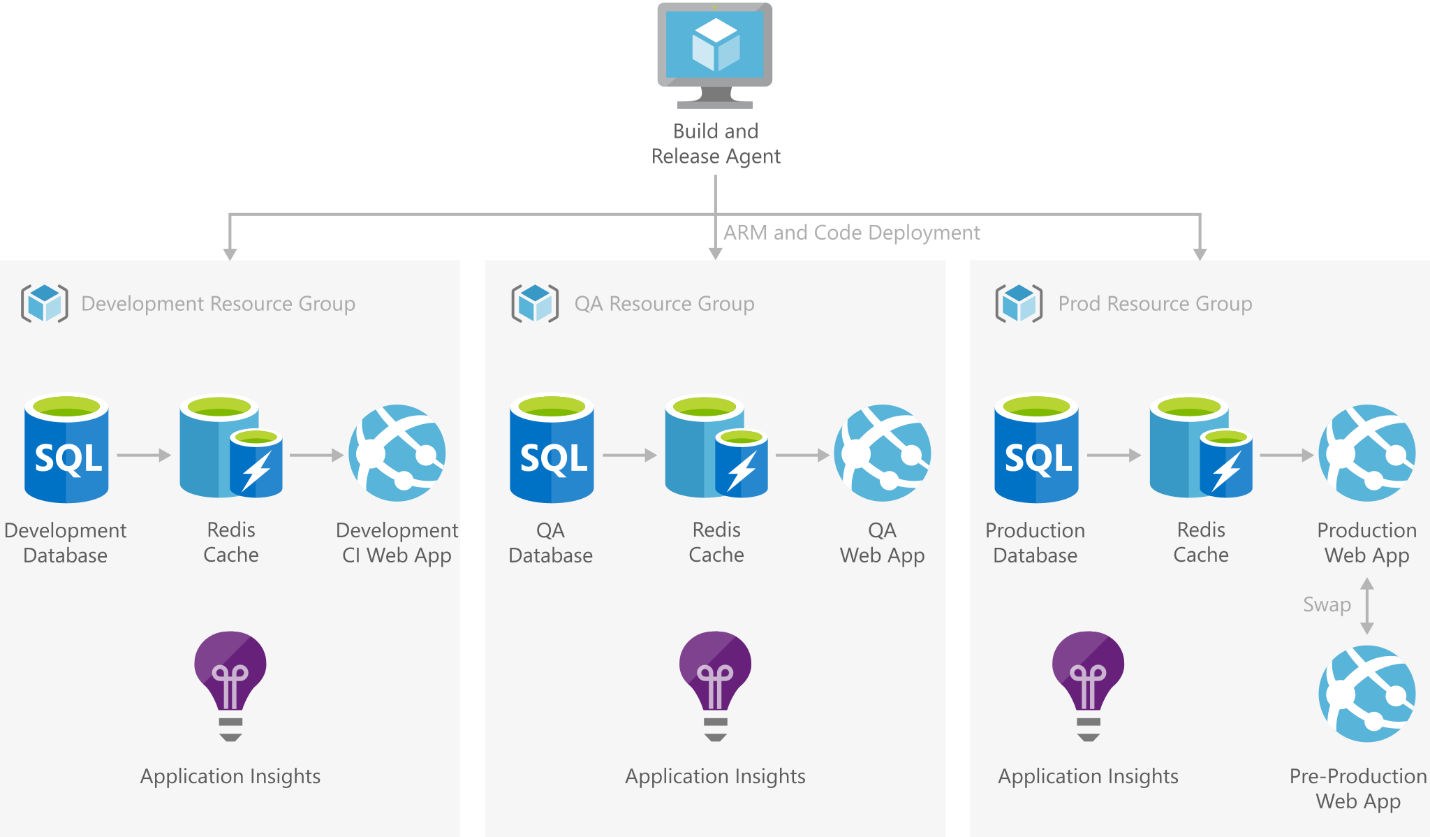
• Azure DevOps resource groups are used to define all the services required to deploy the solution into a dev-test or production environment.

• Azure DevTest Labs: Azure Dev-Test Labs manages all of the virtual machines used in the development and test environments.

• Virtual Machines: Virtual machines are used to deploy all of the products used in the solution. Staging slots swap pre-production and production versions.

• Application Insights: Application Insights monitors the web application during development and test runs, and then monitors the full production system when it’s released.

## Dev-Test Deployment for Testing PaaS Solutions



### Components

• Azure DevOps manage the development process.

• The Microsoft Release Management build and release agents deploy the Azure Resource Manager template and associated code to the various environments.

• Resource Groups: AzureDevOps resource groups are used to define all the services required to deploy the solution into a dev-test or production environment.

• Web Apps: A web app runs the website and is deployed to all environments. Staging slots are used to swap pre-production and production versions.

• Azure SQL Database maintains data for the website. Copies are deployed in the dev, test, and production environments.

• Azure Cache for Redis is used in each environment to improve performance of the website.

• Application Insights: Application Insights monitors the web application during development and test runs, and then monitors the full production system when it's released.

1. <https://wordpress.org/about/requirements/> [↑](#footnote-ref-1)
2. https://social.msdn.microsoft.com/Forums/azure/en-US/ee13d2f8-4d88-47bf-a9f8-3daa837f5f3f/keyvault-references-in-app-services?forum=WindowsAzureAD [↑](#footnote-ref-2)
3. <https://devdocs.magento.com/guides/v2.3/install-gde/system-requirements-tech.html> [↑](#footnote-ref-3)