The Shared Responsibility Model

X AS A SERVICE…

Pizza as a Service

Traditional On-Premises (On Prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Dining Table	Dining Table	Dining Table	Dining Table
Soda	Soda	Soda	Soda
Electric / Gas	Electric / Gas	Electric / Gas	Electric / Gas
Oven	Oven	Oven	Oven
Fire	Fire	Fire	Fire
Pizza Dough	Pizza Dough	Pizza Dough	Pizza Dough
Tomato Sauce	Tomato Sauce	Tomato Sauce	Tomato Sauce
Toppings	Toppings	Toppings	Toppings
Cheese	Cheese	Cheese	Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

■ You Manage　■ Vendor Manages

CLOUD SERVICE MODELS

Traditional

You manage
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Infrastructure
(as a Service)

You manage
- Applications
- Data
- Runtime
- Middleware
- O/S

Managed by vendor
- Virtualization
- Servers
- Storage
- Networking

Platform
(as a Service)

You manage
- Applications
- Data

Managed by vendor
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software
(as a Service)

Managed by vendor
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

TYPICAL ON-PREMISES **CAPEX COSTS**

Server Costs

Backup and Archive Costs

Storage Costs

Datacenter Costs (including DR)

Network Costs

INFRASTRUCTURE AS A SERVICE (IAAS)

Build pay-as-you-go IT infrastructure by renting servers, virtual machines, storage, networks, and operating systems from a cloud provider.
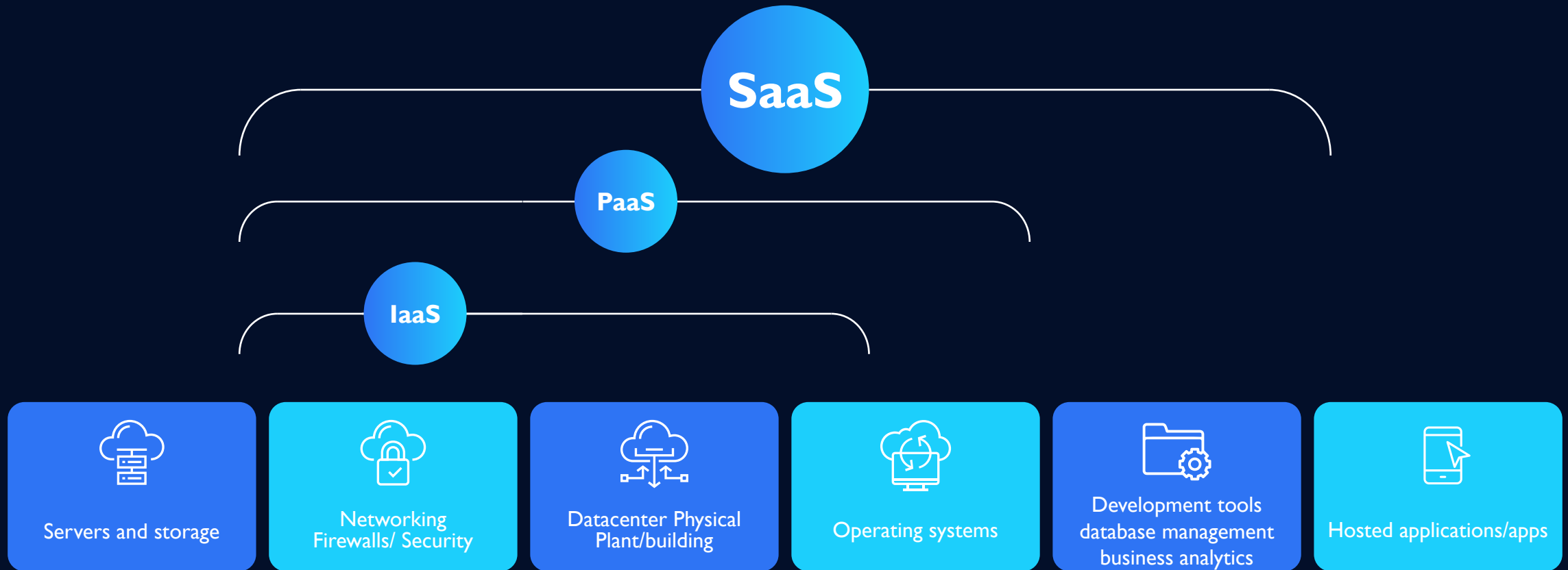
IaaS

Servers and storage

Networking
Firewalls/ Security

Datacenter Physical
Plant/building

PLATFORM AS A SERVICE (PAAS)

Provides environment for building, testing, and deploying software applications; without focusing on managing underlying infrastructure.

PaaS

IaaS

| Servers and storage | Networking Firewalls/ Security | Datacenter Physical Plant/building | Operating systems | Development tools database management business analytics |
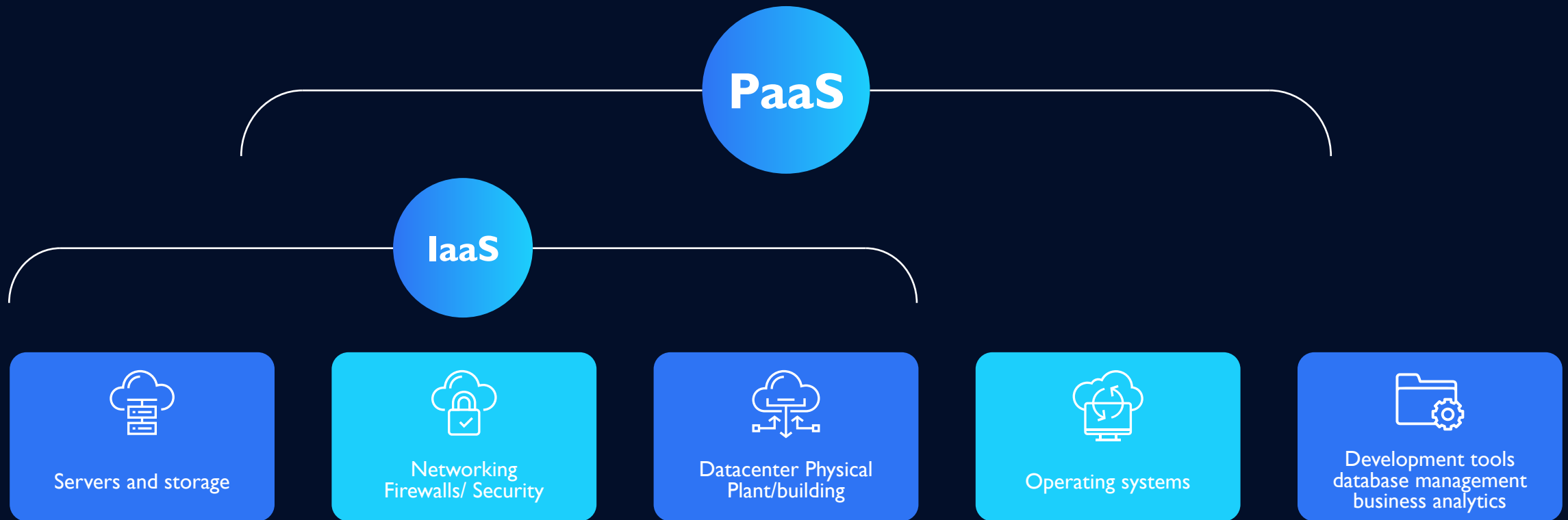
SOFTWARE AS A SERVICE (SAAS)

Users connect to and use cloud-based apps over the internet: for example, Microsoft Office 365, email, and calendars.

SaaS

PaaS

IaaS

| Servers and storage | Networking Firewalls/ Security | Datacenter Physical Plant/building | Operating systems | Development tools database management business analytics | Hosted applications/apps |

CLOUD SERVICE **COMPARISON**

IaaS

- The most flexible cloud service.
- You configure and manage the hardware for your application.

PaaS

- Focus on application development.
- Platform management is handled by the cloud provider.

SaaS

- Pay-as-you-go pricing model.
- Users pay for the software they use on a subscription model.

Define Cloud Computing

Cloud Computing Overview
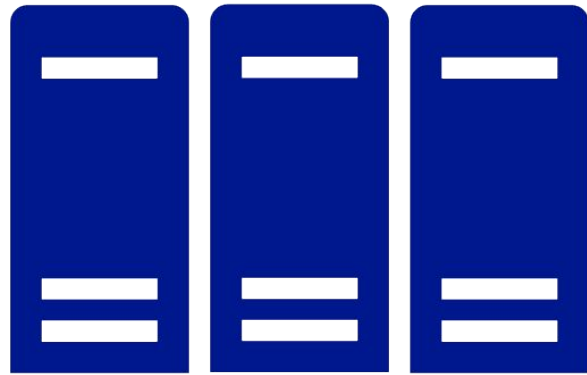
Traditional Datacenter
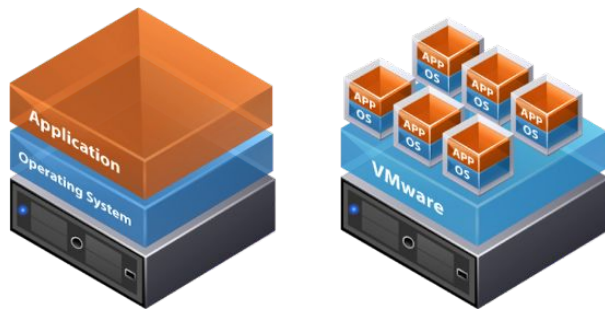
What is cloud computing?

Cloud Computing is the delivery of computing services over the internet, enabling faster innovation, flexible resources, and economies of scale.
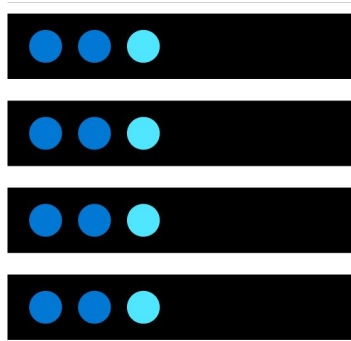
Compute
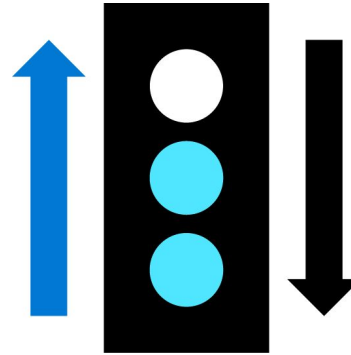
Networking
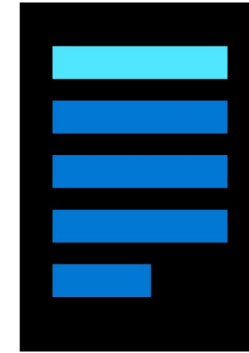
Storage

What is Cloud Computing?

- Cloud computing is about **"renting"** resources vs purchasing hardware
- Pay for what you use
- Run your applications in someone else's datacenter
- Cloud provider is responsible for the physical hardware and facilities necessary to execute your work
- Cloud provider responsible for keeping the services **they** provide up-to-date

The Shared Responsibility Model

SKYLINES
ACADEMY

Shared responsibility model

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Microsoft	Shared	Customer	Customer
	Network controls	Microsoft	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Legend: ■ Microsoft ■ Customer ◪ Shared

Public Cloud

- Common Deployment Model
- Azure, AWS, GCP are examples of Public Cloud providers
- Everything runs on your cloud providers hardware

Public Cloud

Advantages

- High scalability/agility
- Pay-as-you-go pricing – you pay only for what you use, no CapEx costs
- You're not responsible for maintenance or updates of the hardware
- *Minimal* technical knowledge required to get started

Disadvantages

- There may be specific security requirements that cannot be met by using public cloud
- There may be government policies, industry standards, or legal requirements which public clouds cannot meet
- You don't own the hardware
- Unique business requirements

Private Cloud

- You create a cloud like environment in your own datacenter
- You are responsible for the hardware and software services you provide
- Characteristics include:
  - Self Service
  - Automation
  - Agility
  - Financial Transparency

Private Cloud

Advantages

- Complete control over all resources and can support legacy scenarios
- Complete security control
- May be able to meet strict compliance requirements Public Cloud cannot

Disadvantages

- Large upfront costs
- High skillset required
- Owning equipment adds a lag into the provisioning process
- Datacenter management

Hybrid Cloud

- Combines Public and Private Clouds
- Allows flexibility to run in the most appropriate location
- Consume Public Cloud services as needed and potentially keep legacy workloads running on-premises

Hybrid Cloud

Advantages

- Flexibility
- Support for Legacy systems while enabling modern application workloads to move to Public Cloud
- Continue to use your own equipment and investments

Disadvantages

- Complicated to maintain and setup
- Can be more expensive than simply selecting one model

Cloud model comparison

Public Cloud
- No capital expenditures to scale up.
- Applications can be quickly provisioned and deprovisioned.
- Organizations pay only for what they use.

Private Cloud
- Hardware must be purchased for start-up and maintenance.
- Organizations have complete control over resources and security.
- Organizations are responsible for hardware maintenance and updates.

Hybrid Cloud
- Provides the most flexibility.
- Organizations determine where to run their applications.
- Organizations control security, compliance, or legal requirements.

Describe Cloud Consumption

SKYLINES
ACADEMY

Economies of Scale

Economies of scale is the ability to do things more efficiently or at a lower-cost per unit when operating at a larger scale.

Cloud Benefits

- Cloud providers can pass on economies of scale to consumers
- Acquire hardware at lower costs
- Local Government deals
- Datacenter efficiencies

Compare CapEx vs. OpEx

Capital Expenditure (CapEx)

· The up-front spending of money on physical infrastructure.

· Costs from CapEx have a value that reduces over time.

Operational Expenditure (OpEx)

· Spend on products and services as needed, pay-as-you-go

· Get billed immediately
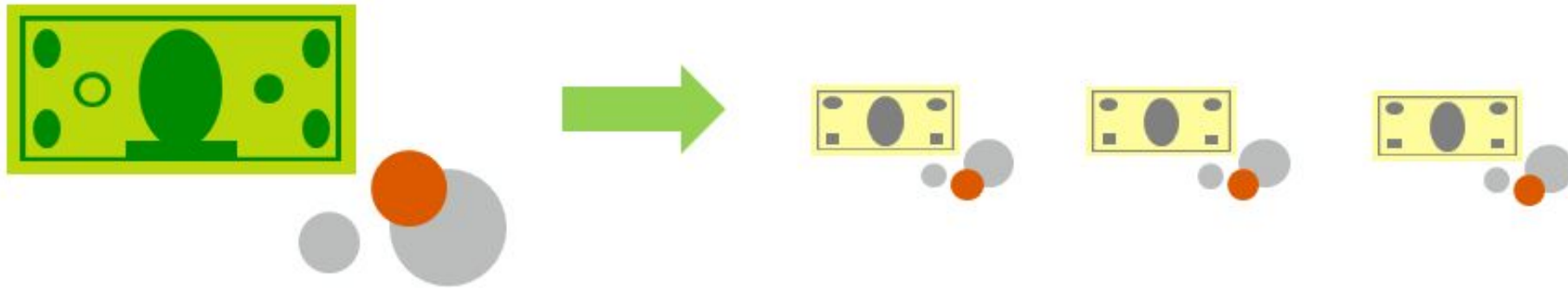
Consumption-based model

- Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use. Whatever they use is what they pay for.

- Better cost prediction

- Prices for individual resources and services are provided

- Billing is based on actual usage
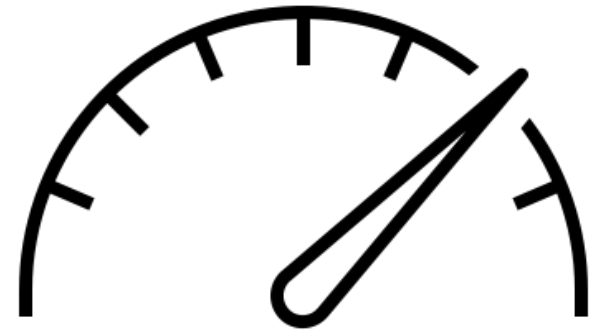
Capex vs Opex

Capital Expenditure (CapEx)

- Spending on infrastructure is completed upfront
- Cost written off over a period of time

Operational Expenditure (OpEx)

- No up-front cost
- Pay for service as you consume it
- Deduct from tax bill in same year as expense occurs

Typical On-Premises CapEx Costs

Server Costs

Storage Costs

Network Costs

Backup and Archive Costs

Datacenter Costs (including DR)

Typical Opex Costs for Cloud Computing

Server Lease Costs

Software and Feature Leases

Usage/Demand Cost Scaling

CapEx vs OpEx Benefits

CapEx Benefits

- Predictability
- Cost effective when you can consume the infrastructure quickly

OpEx Benefits

- Try and buy
- Low initial costs
- Demand fluctuation

Benefits of Cloud Services

Cloud Benefits - Objective Domain

01

Describe the benefits of high availability and scalability in the cloud.

02

Describe the benefits of reliability and predictability in the cloud.

03

Describe the benefits of security and governance in the cloud.

04

Describe the benefits of manageability in the cloud.

High Availability (HA)

What is an SLA?

"A Service Level Agreement (SLA) is an agreement with the business and application teams on the expected performance and availability of a specific service."

General SLA Practices

- Define SLA's for each workload
- Dependency mapping
  - Make sure to include internal/external dependencies
- Identify single points of failure
  - Example – workload requires 99.99% but depends on a service that is only 99.9%

Key Terms

Mean Time To Recovery (MTTR)

- Average time to recover service from an outage

Mean Time Between Failures (MTBF)

- Average time between outages

Recovery Point Objective (RPO)

- Interval of time in which data could be lost during a recovery. E.g. 5 minute RPO means up to 5 minutes of data could be lost.

Recovery Time Objective (RTO)

- Time requirement for recovery to be completed in before there is business impact.

Disaster Recovery and Fault Tolerance

Fault Tolerance

- Redundancy is built into services so that if one component fails, another takes its place.

- Reduces impact when disasters occur.

Disaster Recovery

- Planning for catastrophic failure of workload

- Region to region Failover

- On-Premises to cloud failover

- Automation and Orchestration

HA Examples

Host Outage

- When an underlying host has a catastrophic failure, the virtual machine will automatically be restarted on another host.

- Availability Sets and Zones further increase the availability.

Cross Region Deployment

- An application is deployed in a configuration to be highly available across regions.

- When a service in one region has an outage, traffic can continue to run in the second region.

Elasticity & Scalability

Scalability

- Increase or decrease resources based on workload demand
- Vertical Scaling
  - Also known as scaling up
  - Add additional resources to increase the power of the workload
  - E.g. Add additional CPUs to a Virtual Machine
- Horizontal Scaling
  - Also known as scaling out

Scalability

Vertical Scaling

Horizontal Scaling

Elastic

- Major pattern which benefits from cloud computing
- As your workload changes, resources can be changed to compensate (up or down)
- Example: Seasonal demand for retail web site
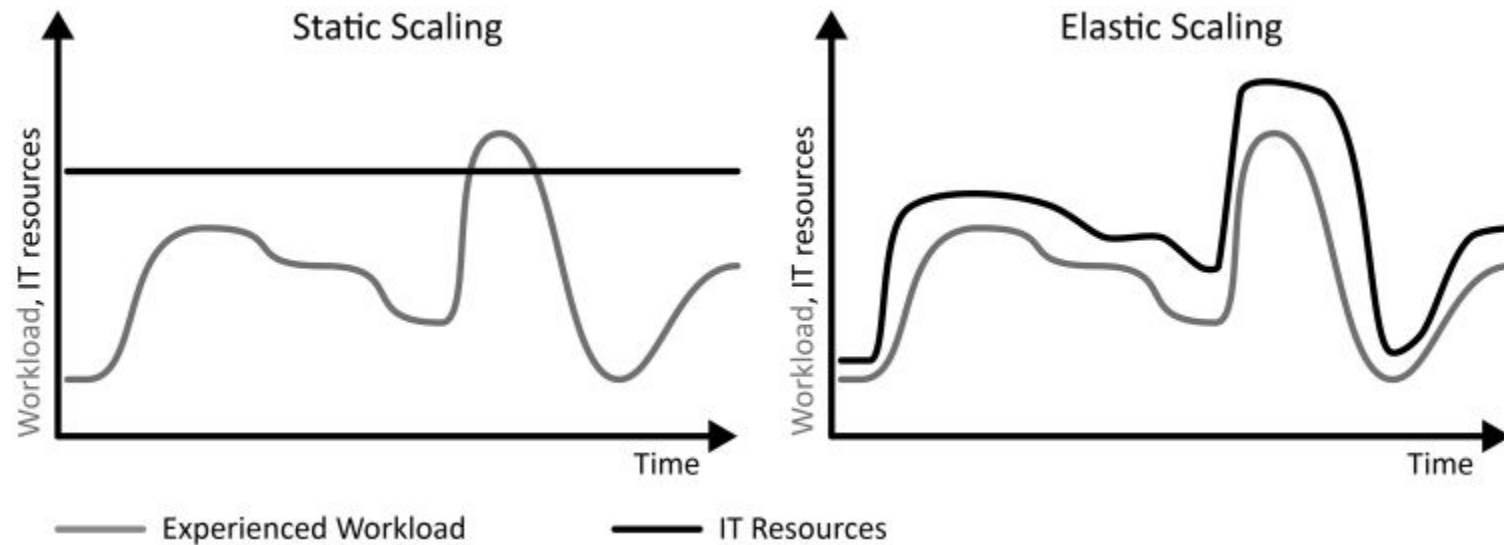
Cloud Deployment Models

SKYLINES
ACADEMY

Understanding Azure Core Services

Platform Services

Security & Management
- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/Marketplace
- VM Image Gallery & VM Depot

Media & CDN
- Media Services
- Media Analytics
- Content Delivery Network

Integration
- API Management
- BizTalk Services
- Logic Apps
- Service Bus

Compute Services
- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Application Platform
- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services
- Visual Studio
- Mobile Engagement
- VS Team Services
- Xamarin
- Application Insights
- HockeyApp

Data
- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence
- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT
- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud
- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute
- Virtual Machines
- Containers

Storage
- Blob
- Queues
- Files
- Disks

Networking
- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure

Regions and Availability Zones

Azure Regions

- Location for your resources
- Area containing at least one datacenter
- Usually need to select a region when deploying a resource
- Examples: East US, West US, Central India, East Asia, Germany Central
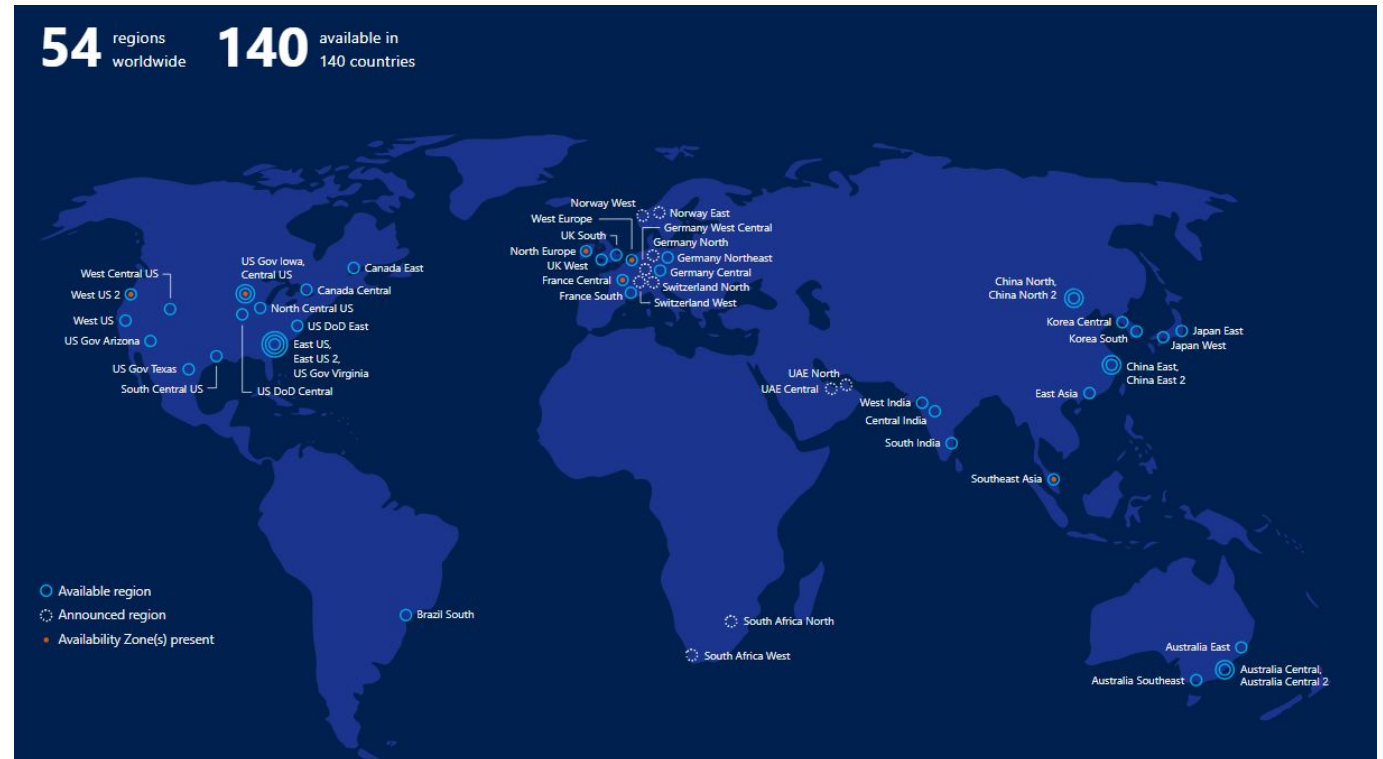
Why Regions Matter?

- More regions = scalable and redundant
- Azure has the most to date
- You might need a specialized region for compliance purposes: E.g. US Gov regions or Chinese regions which are run by 21Vianet due to regulations

Geographies

- Boundaries, often country borders
- Normally 2+ regions for data preservation
- Meets compliance needs
- Data requirements met in boundaries:
- Fault tolerant
- Geographies: Americas, Asia Pacific, Europe, Middle East, Africa
- Each region belongs to a single geography

Region Pairs

Resource Groups

SKYLINES
ACADEMY
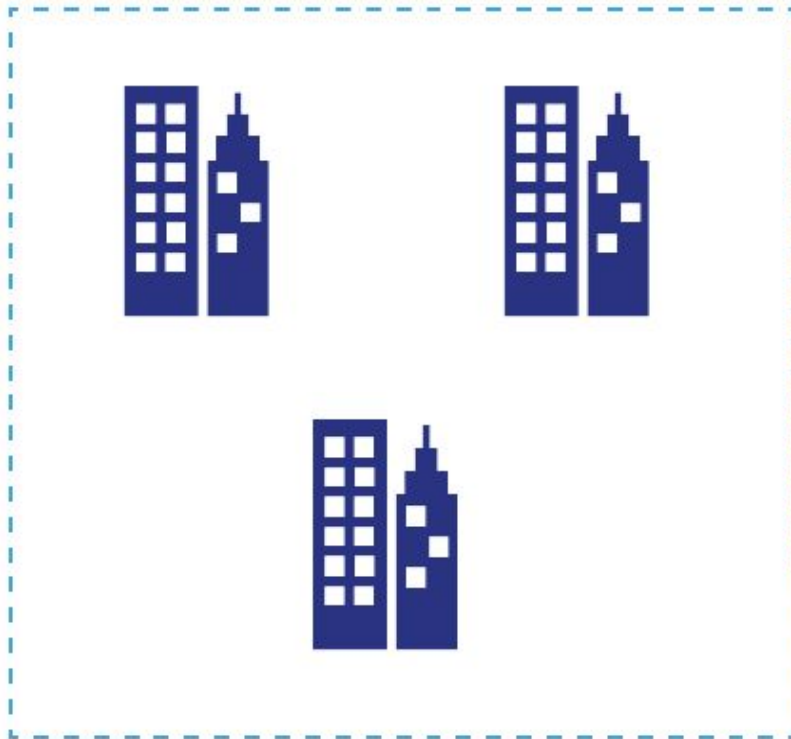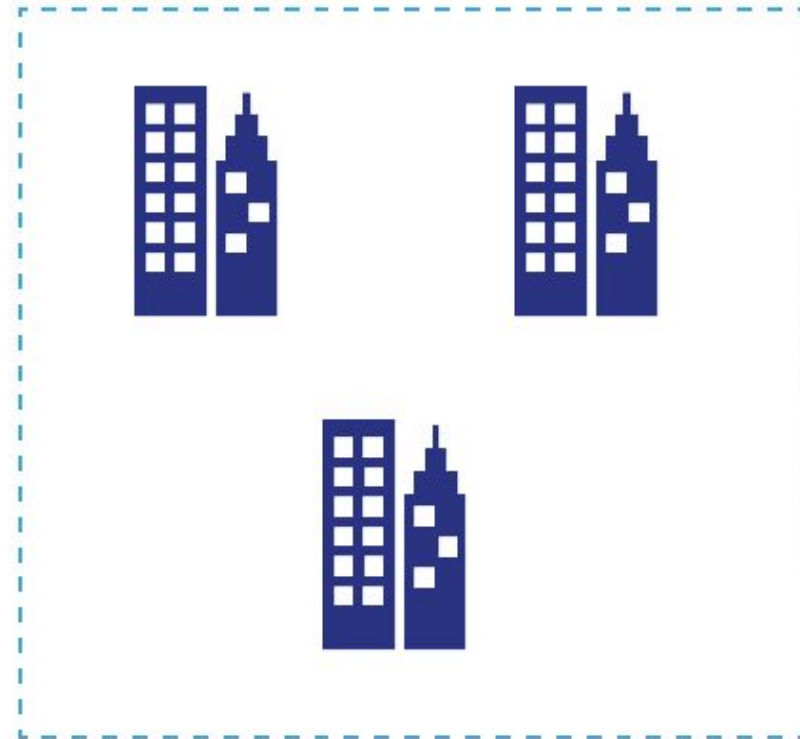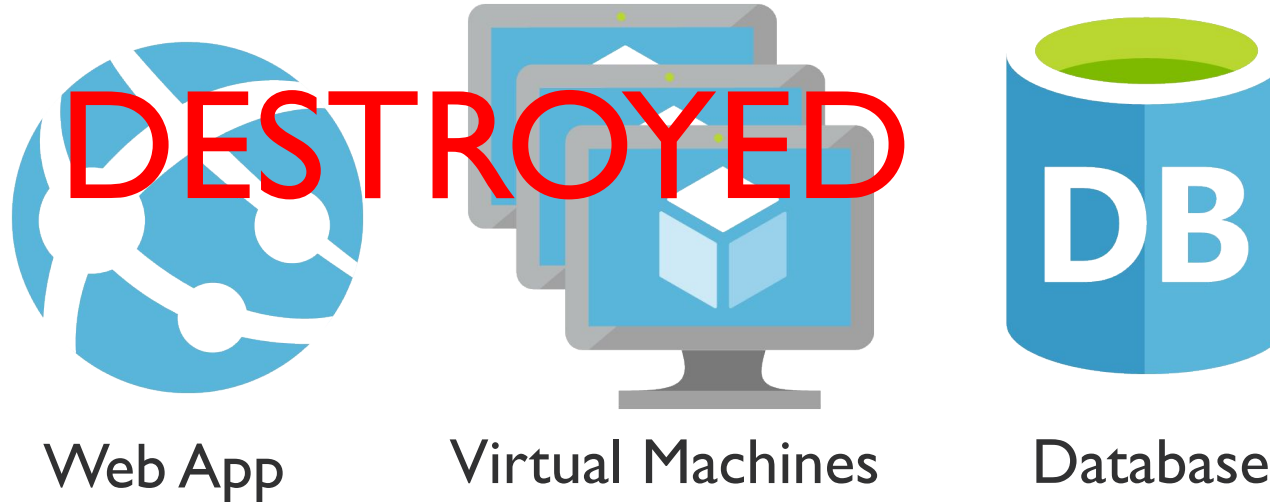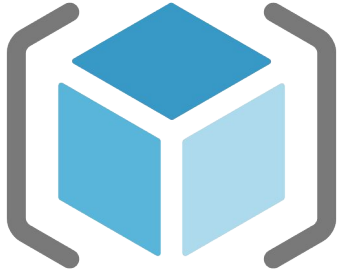
Why Resource Groups?
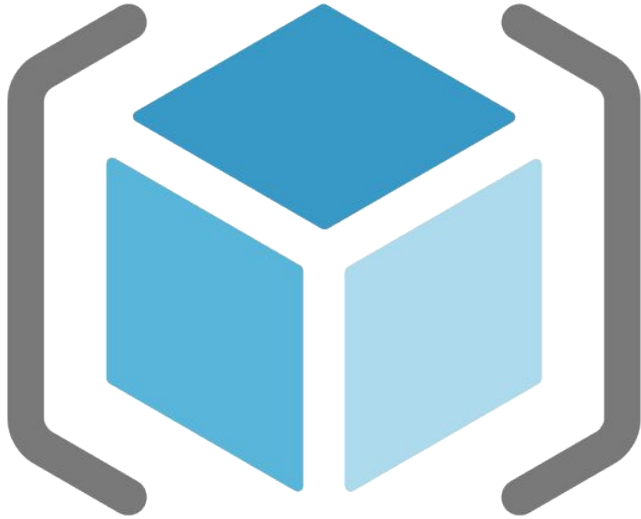
- Organization
- Easy de-provisioning
- Security Boundary
  - RBAC
- Apply Policies

Azure Resource Manager (ARM)

SKYLINES
ACADEMY

Resource Manager Overview

Resource	Resource Group	Resource Provider	ARM Templates

Individual manageable item available to you in Azure

Container where you can house your resources for management

Provider of services you can deploy in Azure e.g. Microsoft.Compute

Files used to define resources you wish to deploy to a resource group

ARM Templates Overview
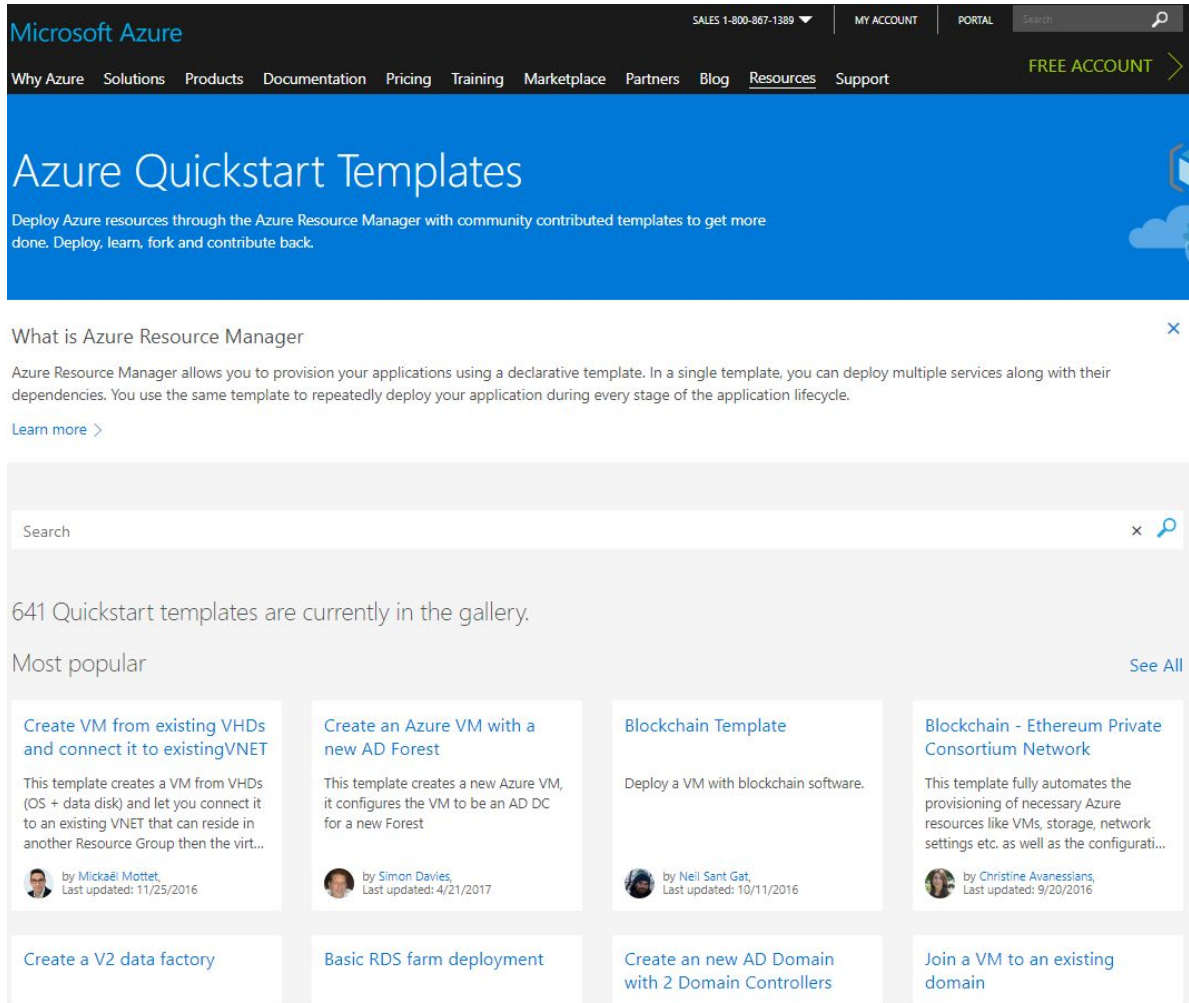
```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
  },
  "variables": {
  },
  "resources": [
    {
      "name": "[concat('storage', uniqueString(resourceGroup().id))]",
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2016-01-01",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "Storage",
      "location": "North Central US",
      "tags": {},
      "properties": {}
    }
  ],
  "outputs": {  }
}
```

**Resource
(E.g. Storage Account)**

- Apply Infrastructure as Code
- Download templates from Azure Portal
- Author new templates
- Use Quickstart templates, provided by Microsoft

Quickstart Templates

https://azure.microsoft.com/en-us/resources/templates/

https://github.com/Azure/azure-quickstart-templates

ARM File Types

ARM Template File	ARM Template Parameter File	Deployment Scripts
Describe the configuration of your infrastructure via a JSON file	Separate your parameters (optional)	E.g. PowerShell for Deployment

ARM Template Constructs

Parameters

Define the inputs you want to pass into the ARM template during deployment.

Variables

Values that you can use throughout your template. Used to simplify your template by creating reuse of values.
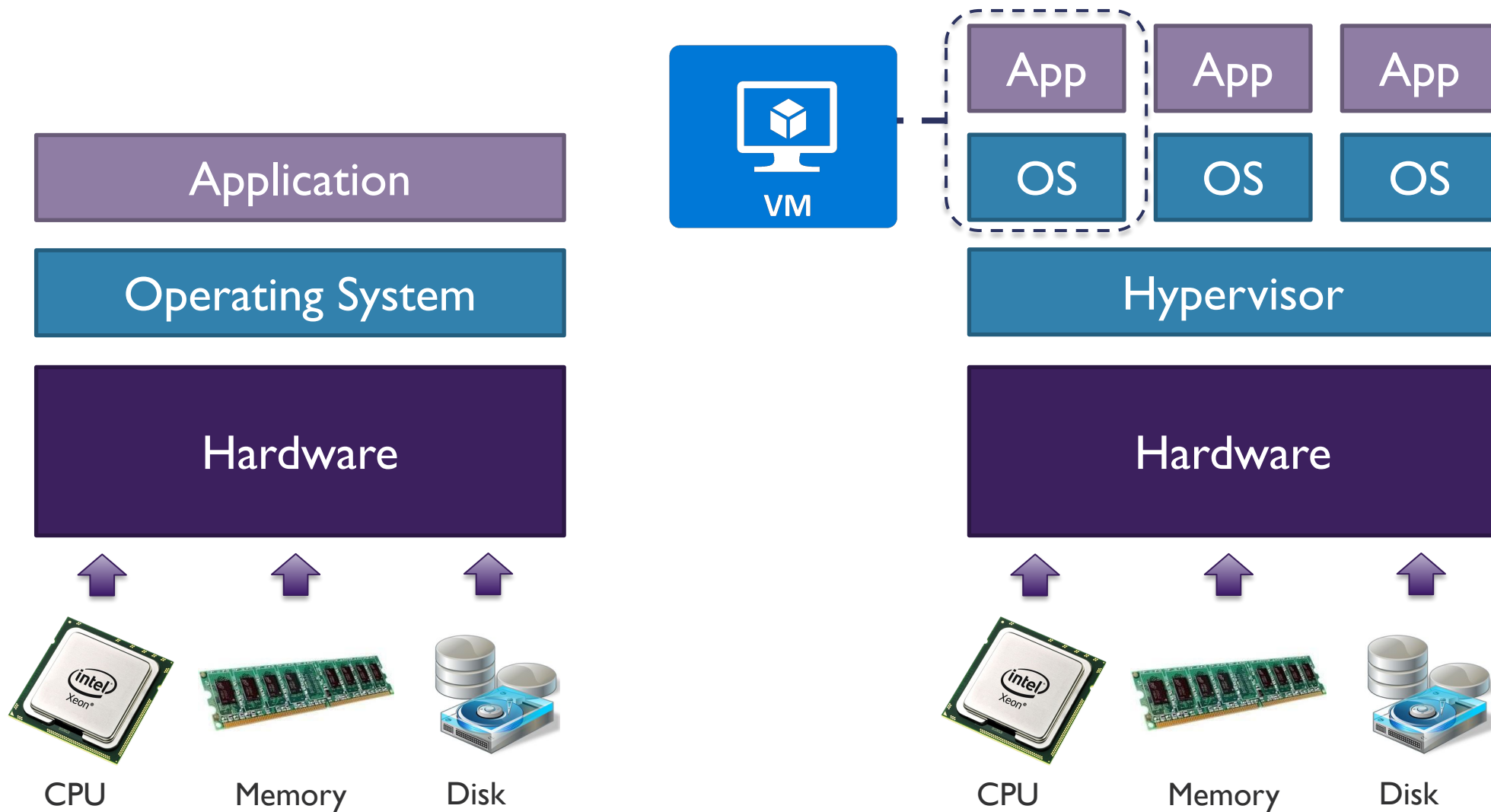
Resources

Define the resources you wish to deploy or update.

Outputs

Specify values that are returned after the ARM deployment is completed.

Azure Virtual Machines

Introduction to Virtual Machines

SKYLINES
ACADEMY

Application

Operating System

Hardware

CPU   Memory   Disk

VM

App   App   App

OS   OS   OS

Hypervisor

Hardware

CPU   Memory   Disk

VM Types

VM

Type	Purpose
A – Basic	Basic version of the A series for testing and development.
A – Standard	General-purpose VMs.
B – Burstable	Burstable instances that can burst to the full capacity of the CPU when needed.
D – General Purpose	Built for enterprise applications. DS instances offer premium storage.
E – Memory Optimized	High memory-to-CPU core ratio. ES instances offer premium storage.
F – CPU Optimized	High CPU core-to-memory ratio. FS instances offer premium storage.
G – Godzilla	Very large instances ideal for large databases and big data use cases.

VM

Type	Purpose
H – High performance compute	High performance compute instances aimed at very high-end computational needs such as molecular modelling and other scientific applications.
L – Storage optimized	Storage optimized instances which offer a higher disk throughput and IO.
M – Large memory	Another large-scale memory option that allows for up to 3.5 TB of RAM.
N – GPU enabled	GPU-enabled instances.
SAP HANA on Azure Certified Instances	Specialized instances purposely built and certified for running SAP HANA.

VM Specializations

VM

S
Premium Storage options available

Example: DSv2

M
Larger memory configuration of instance type

Example: Standard A2m_v2

R
Supports remote direct memory access (RDMA)

Example: H16mr

Module:
VM Availability
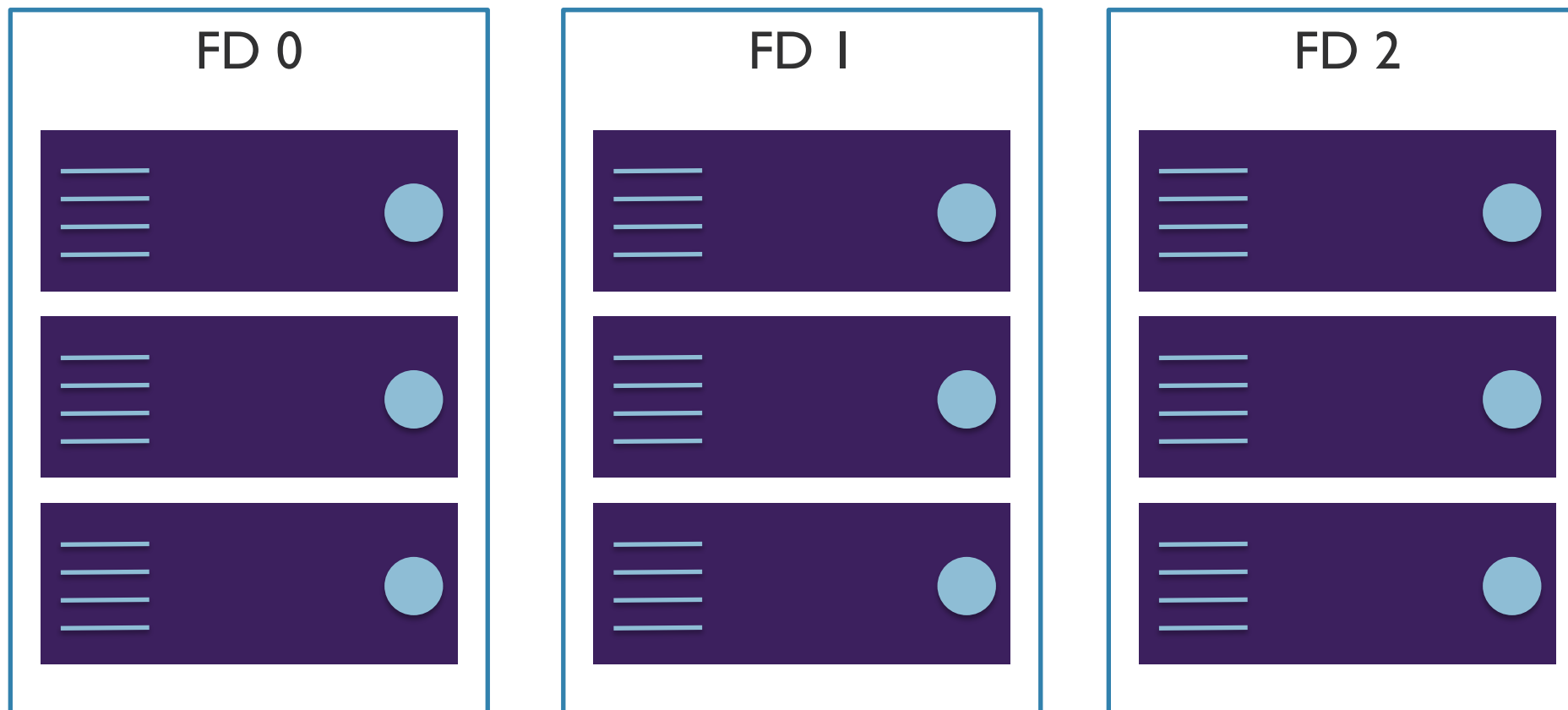
SKYLINES
ACADEMY

Availability Sets

Potential for VM Impact

- Planned maintenance
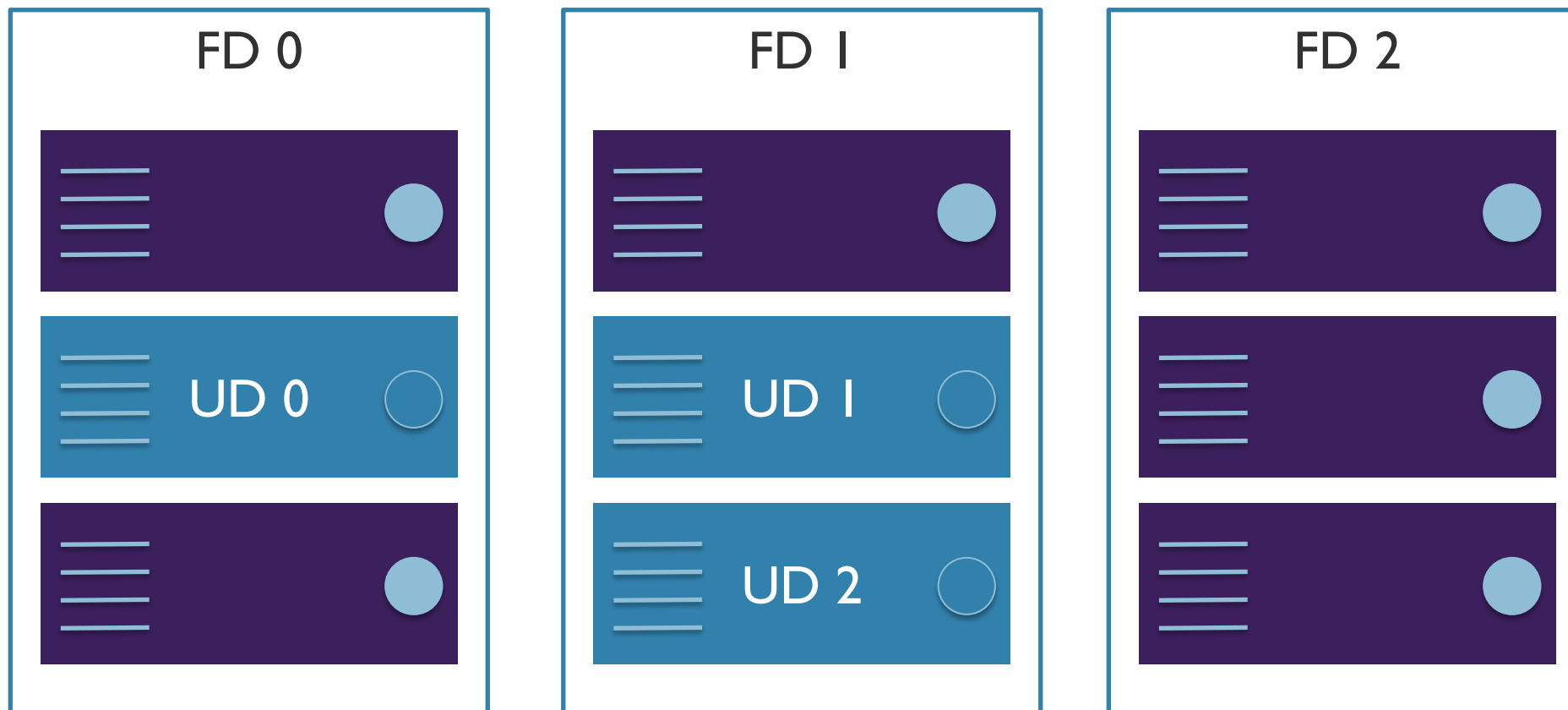- Unplanned hardware maintenance
- Unexpected downtime

Availability Sets

- Group two or more machines in a set
- Separated based on Fault Domains and Update Domains

Fault Domains and Update Domains

Fault Domains and Update Domains

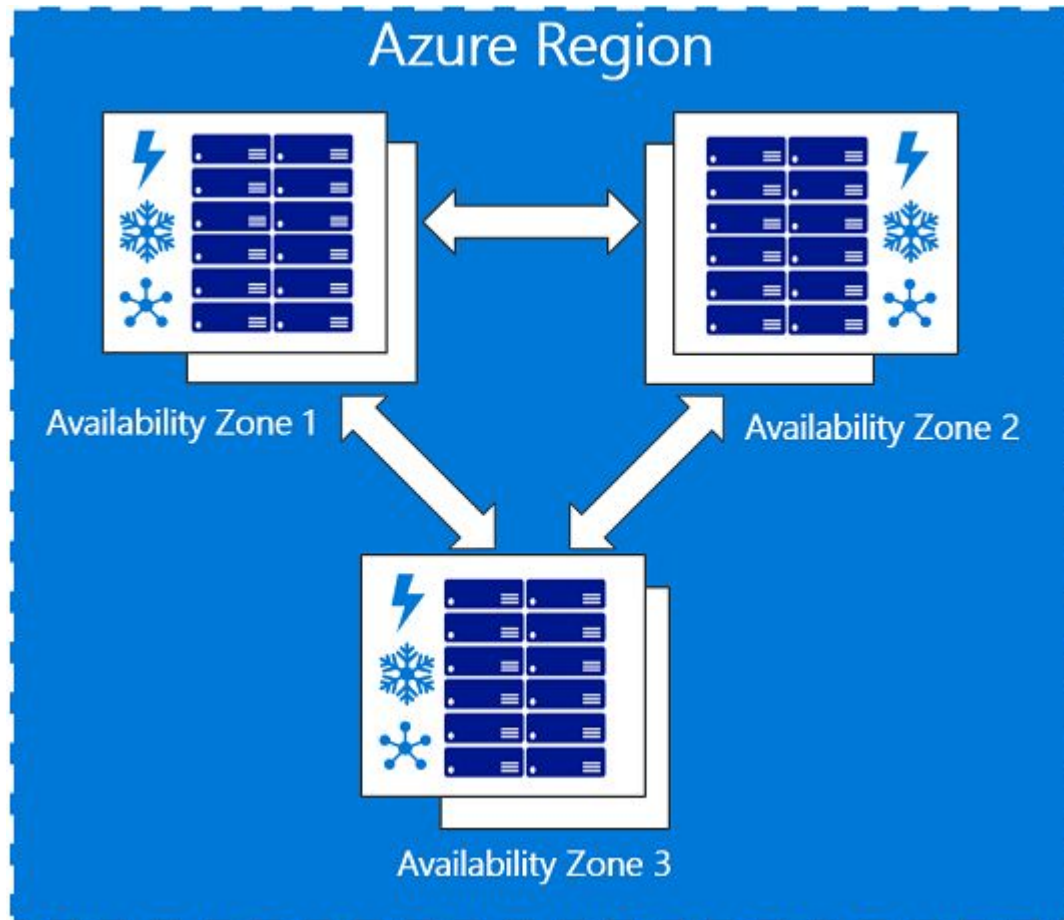# Planning for Availability

Availability Zones

Availability Zones

- Offer 99.99% availability
- Minimize impact of planned and unplanned downtime
- Enforce them like Availability Sets, but now you choose your specific zone in Azure

App Services

Introduction to Web Apps

Azure App Services consist of the following:

| Web Apps | Mobile Apps | Logic Apps | API Apps |

App Service Environments (ASEs)

- Fully isolated environment
- For high-performing apps – high CPU and/or memory
- Individual or multiple service plans
- 2 ways to deploy: *Internal or External*
- Created in a subnet via a VNet, which achieves isolation
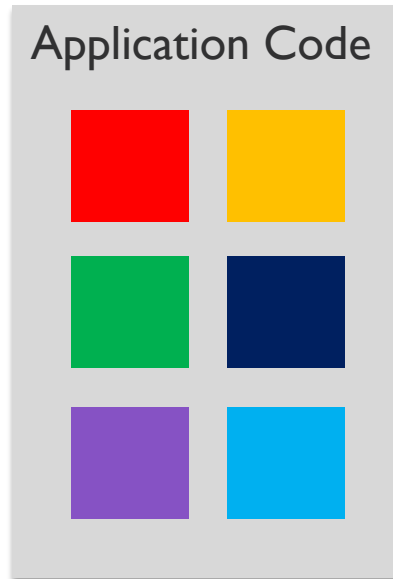- Note: May take a few hours to spin up

Compute Services - Containers

Containers
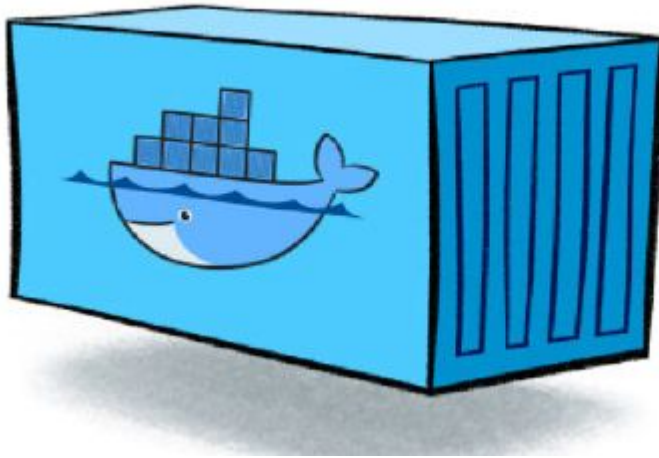
- Standardized packaging for software and dependencies
- A way to isolate apps from each other
- Works with Linux and Windows Servers
- Allows separate apps to share the same OS kernel

Application Modernization

Application Code

Monolithic App Issues:
- Minor code changes required full recompile and testing
- Application becomes a single point of failure
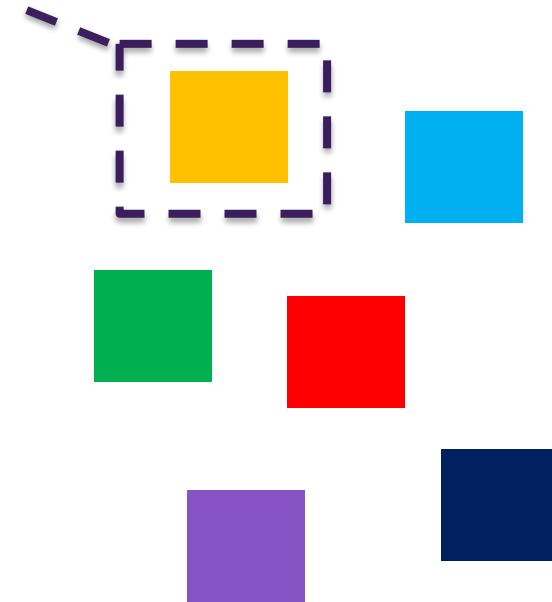- Application is difficult and often expensive to scale

Application Modernization

Microservices:
- Break application out into separate services

12-Factor Apps:
- Make the app independently scalable, stateless, highly availably be design.

Individual service

Comparing Monolithic and Microservices

Monolithic

Microservices

Simple deployments
Inter-module refactoring
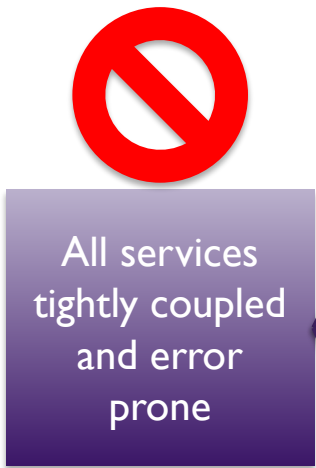Vertical scaling
Technology monoculture

Partial deployments
Strong module boundaries
Horizontal scaling
Technology diversity

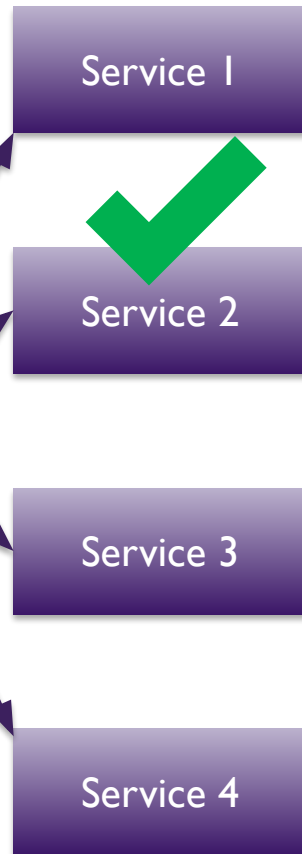# Three Keys to Microservices
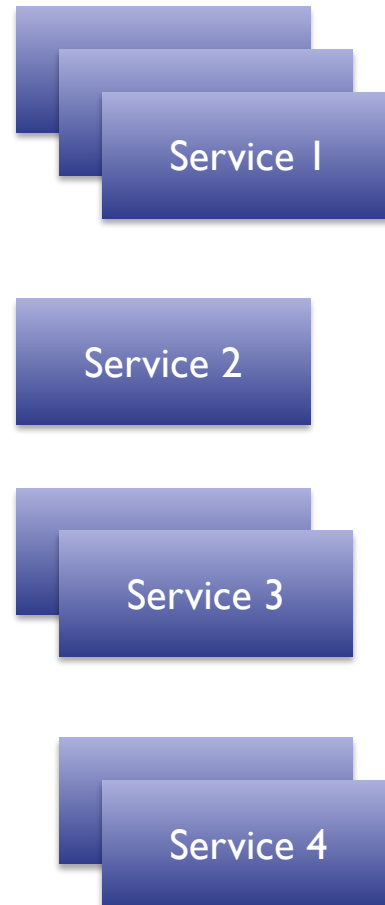
SKYLINES
ACADEMY

1. Functional Decomposition	2. Horizontal Scale	3. Data Decoupling

1. Functional Decomposition

This…   Becomes This

All services tightly coupled and error prone

Service 1

Service 2

Service 3

Service 4

2. Horizontal Scale

Scale what you need to, not what you don't

Service 1

Service 2

Service 3

Service 4

Scaling Options

VM

docker

3. Data Decoupling

Now I can pick the best database for the service

Service 1 → ORACLE

Service 2 → SQL

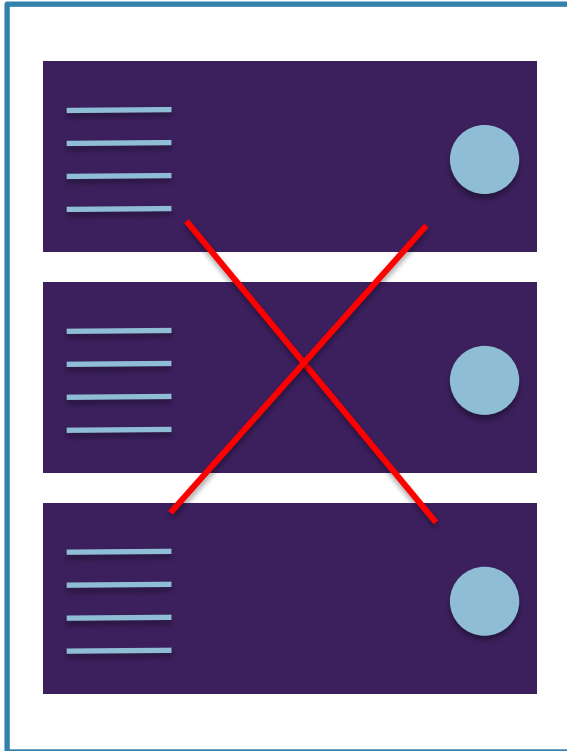Service 3 → redis

Service 4 → SQL
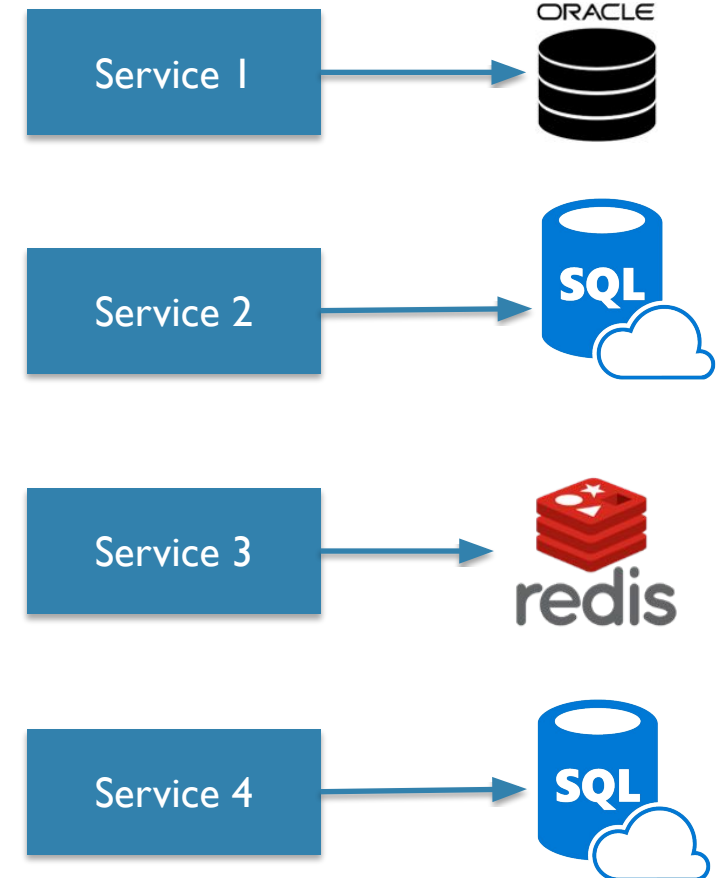
Containers vs. Virtual Machines
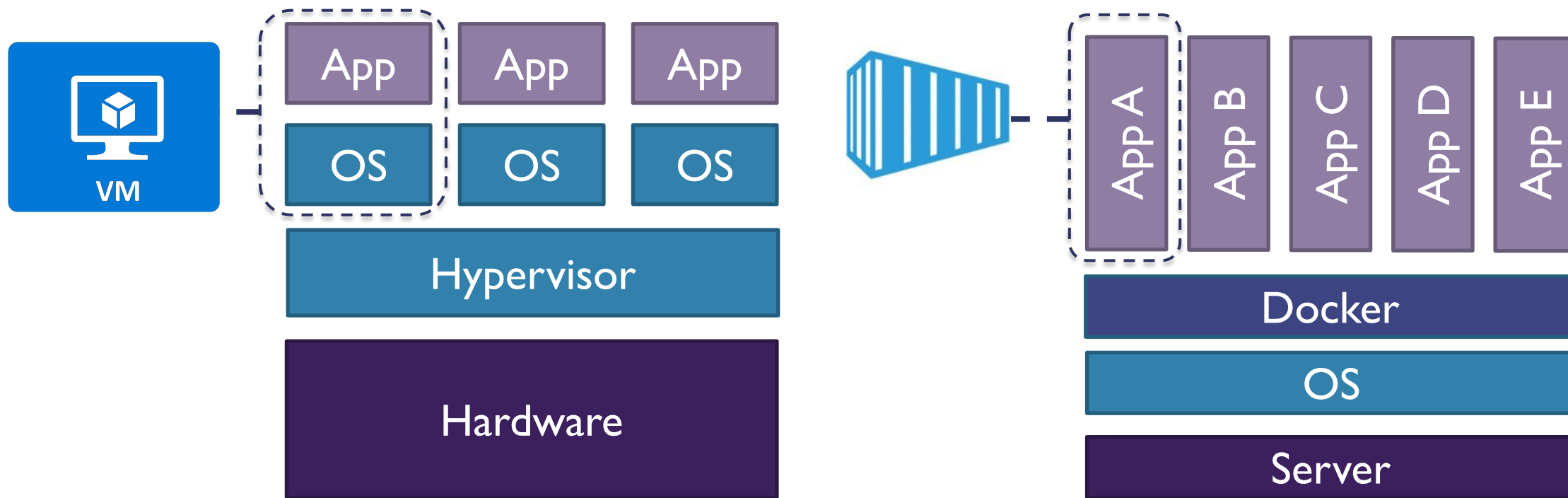
Serverless Computing
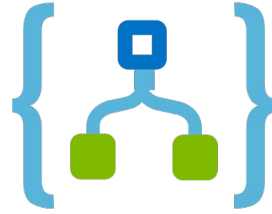
What is Serverless Computing?

- Fully-managed services
- Only pay for what you use
- Flexibility to scale, as needed
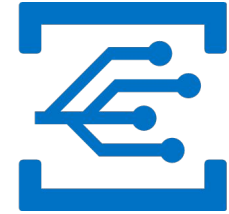- Stitch together applications and services seamlessly

Azure Serverless Computing Services

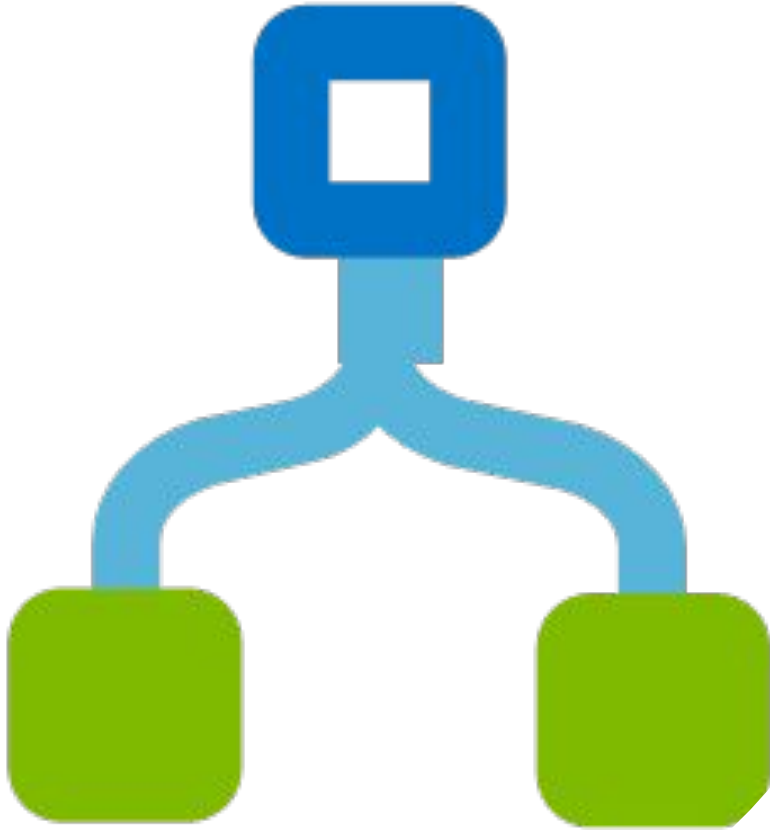Azure Functions

Logic Apps

Event Grid

Azure Functions – Key Features

- Program Languages C#, F#, JavaScript, Java (Preview)
- Pay-per-use Pricing
  - Consumption Plan
  - App Service Plan
    (Run on the same plan as other services)
- Integrated Security with OAUTH providers (Azure AD, Facebook etc.)
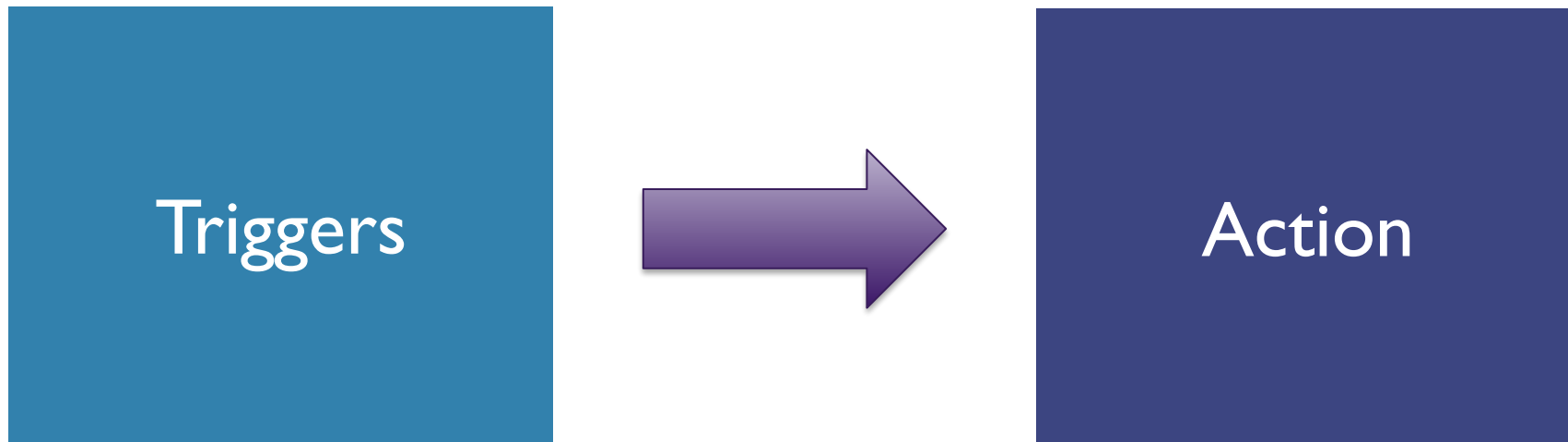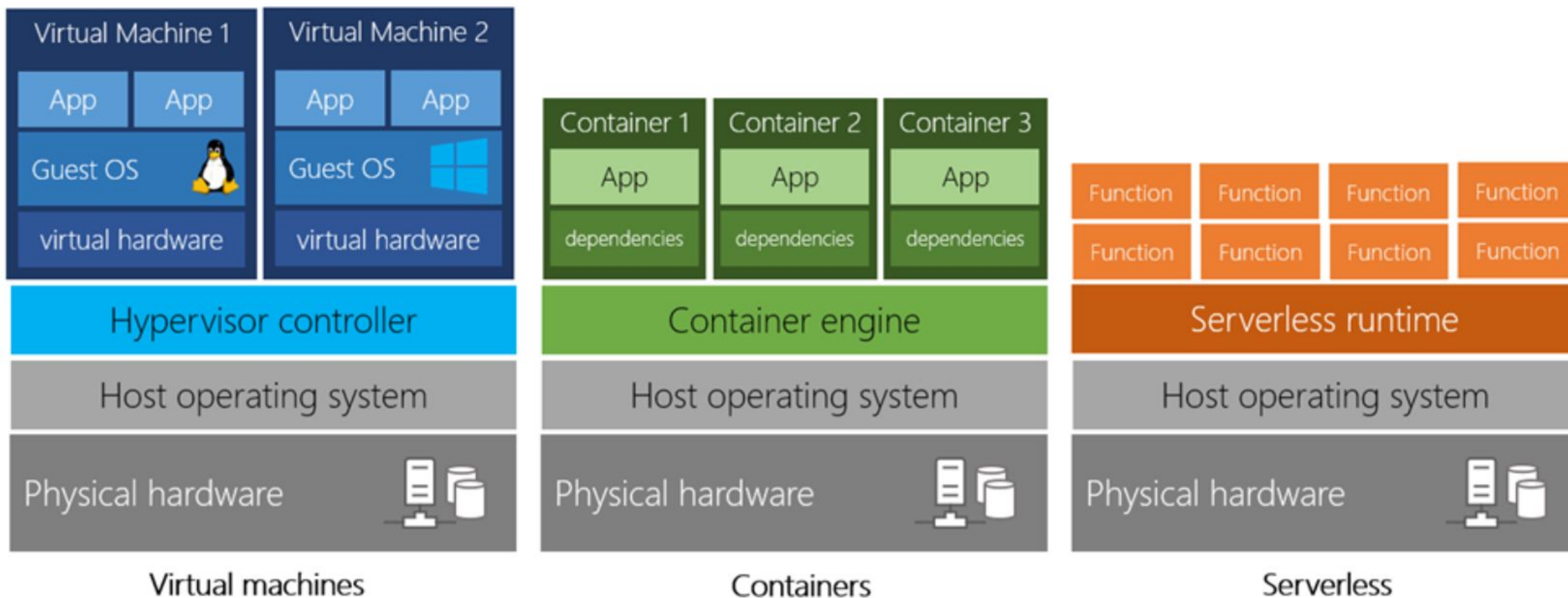- Code in the portal or deploy via DevOps tools

Logic Apps – Key Features

- Workflow Engine
- Used to orchestrate and stitch together functions and services (Just like regular orchestration tools)
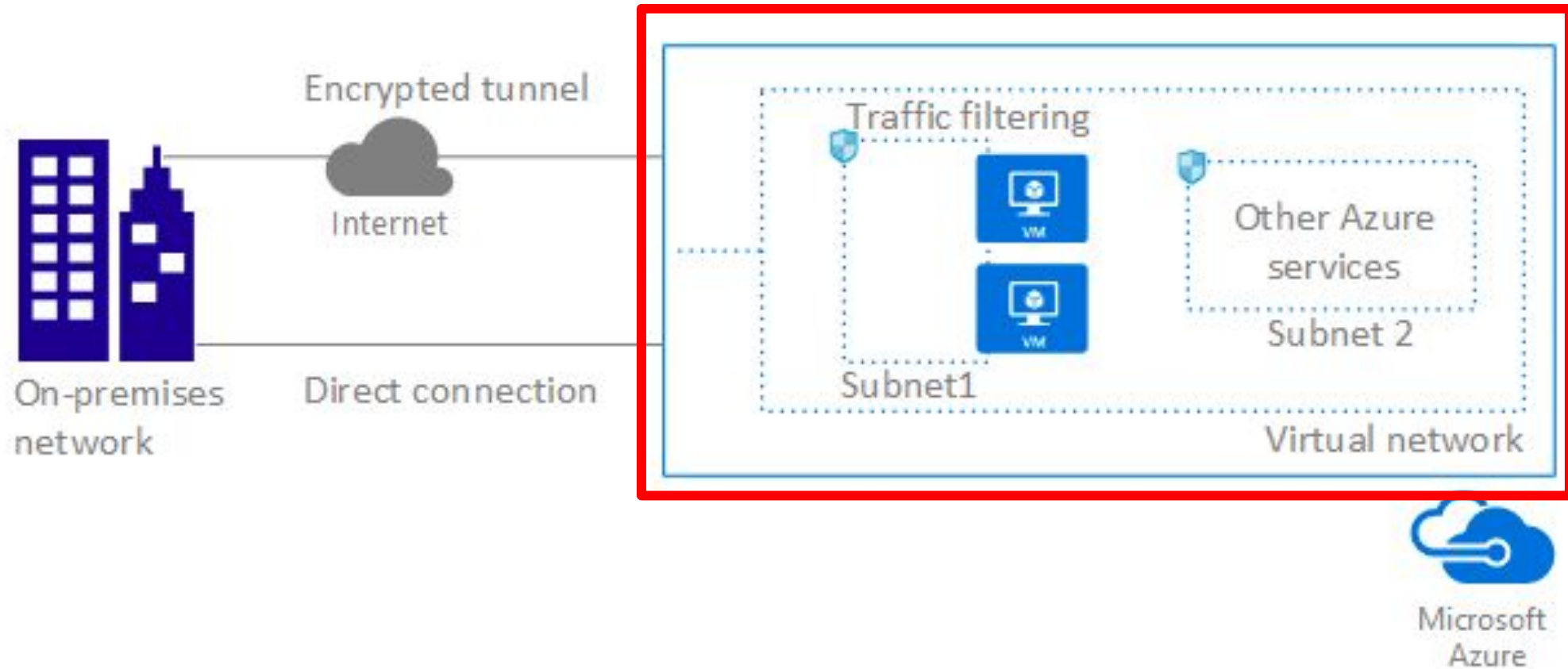- Visualize, Design, Build, Automate

Logic Apps – Key Constructs

Comparing Compute Options

SKYLINES
ACADEMY

Comparing Compute Options

Virtual Machine 1		Virtual Machine 2	
App	App	App	App
Guest OS	🐧	Guest OS	⊞
virtual hardware		virtual hardware	

Hypervisor controller

Host operating system

Physical hardware

Virtual machines

Container 1	Container 2	Container 3
App	App	App
dependencies	dependencies	dependencies

Container engine

Host operating system

Physical hardware

Containers

Function	Function	Function	Function
Function	Function	Function	Function

Serverless runtime

Host operating system

Physical hardware

Serverless

Networking Overview

SKYLINES
ACADEMY

Networking Overview

Source: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Networking Overview (continued)

VNet

Subnet A

NSG   NSG

Subnet B
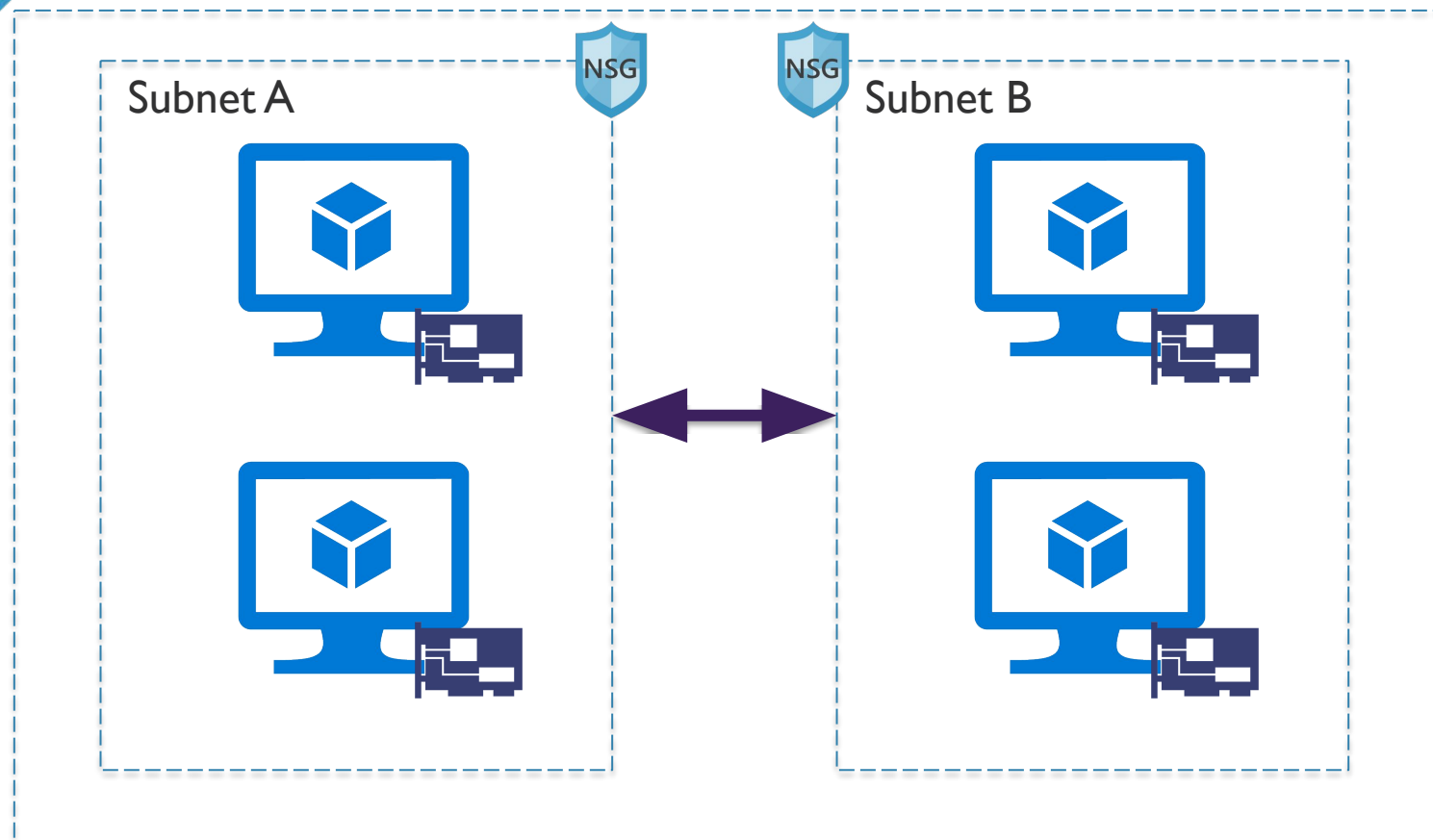
Core VNet Capabilities:

- Isolation
- Internet Access
- Azure Resources (VMs and Cloud Services)
- VNet Connectivity
- On-Premises Connectivity
- Traffic Filter
- Routing

VNets: Key Points

- Primary building block for Azure networking
- Private network in Azure based on an address space prefix
- Create subnets in your VNet with your own IP ranges
- Bring your own DNS or use Azure-provided DNS
- Choose to connect the network to on-premises or the internet
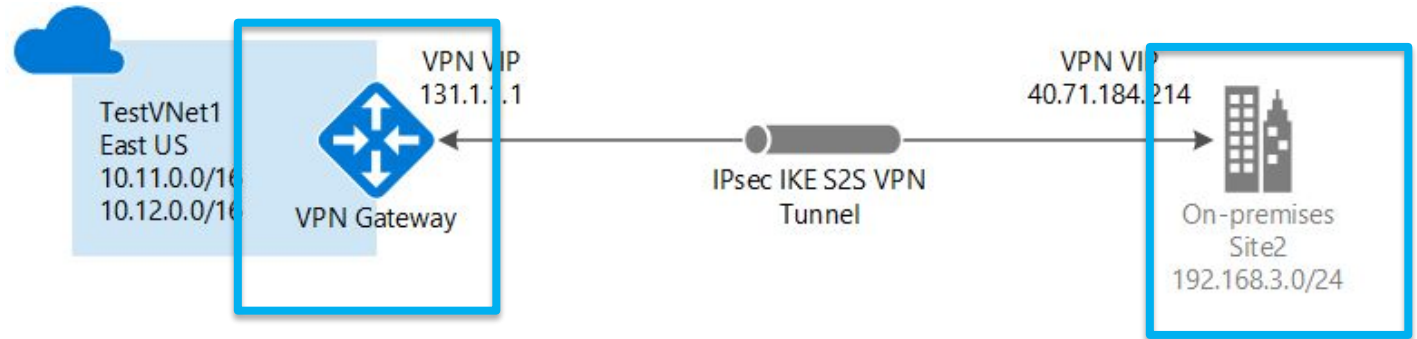
Hybrid Connectivity

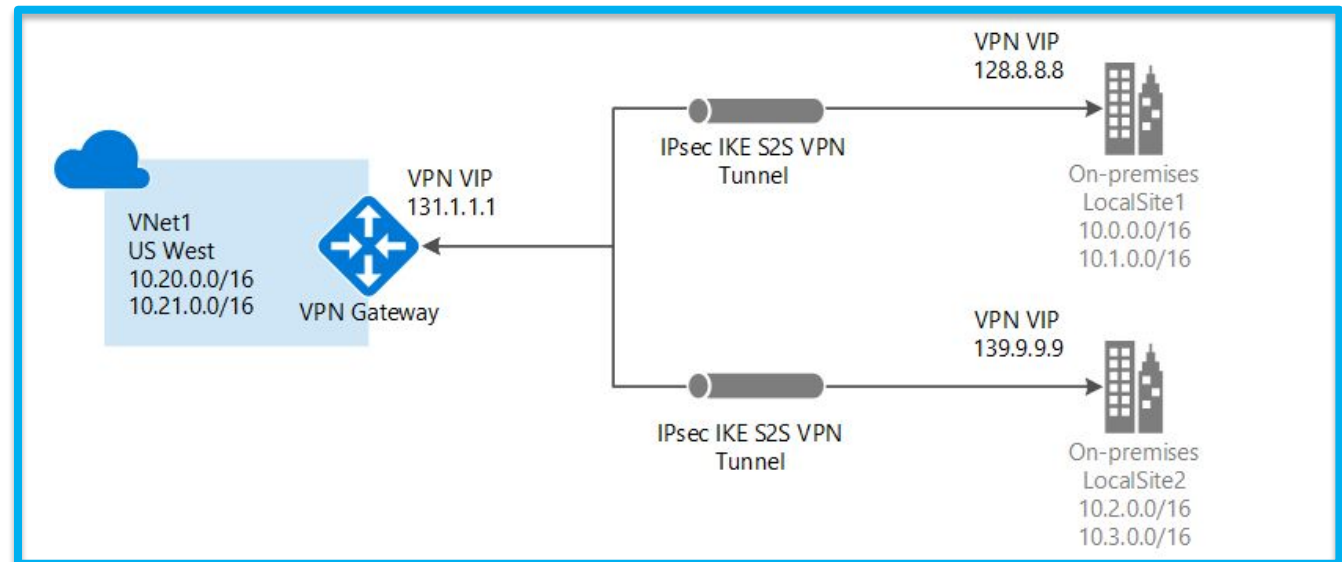# Hybrid Connectivity Options

Site-to-Site (S2S)

ExpressRoute

Point-to-Site (P2S)

S2S

S2S

VPN VIP
131.1.1.1

TestVNet1
East US
10.11.0.0/16
10.12.0.0/16

VPN Gateway

IPsec IKE S2S VPN
Tunnel

VPN VIP
40.71.184.214

On-premises
Site2
192.168.3.0/24

Multi-Site

VNet1
US West
10.20.0.0/16
10.21.0.0/16

VPN Gateway

VPN VIP
131.1.1.1

IPsec IKE S2S VPN
Tunnel

VPN VIP
128.8.8.8

On-premises
LocalSite1
10.0.0.0/16
10.1.0.0/16

IPsec IKE S2S VPN
Tunnel

VPN VIP
139.9.9.9

On-premises
LocalSite2
10.2.0.0/16
10.3.0.0/16

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

- S2S VPN gateway connection is a connection over **IPsec/IKE** (IKEv1 or IKEv2) VPN tunnel
- Requires a VPN device in enterprise datacenter that has a public IP address assigned to it
- Must **not** be located behind a NAT
- S2S connections can be used for cross-premises and hybrid configurations

P2S

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

SKYLINES
ACADEMY
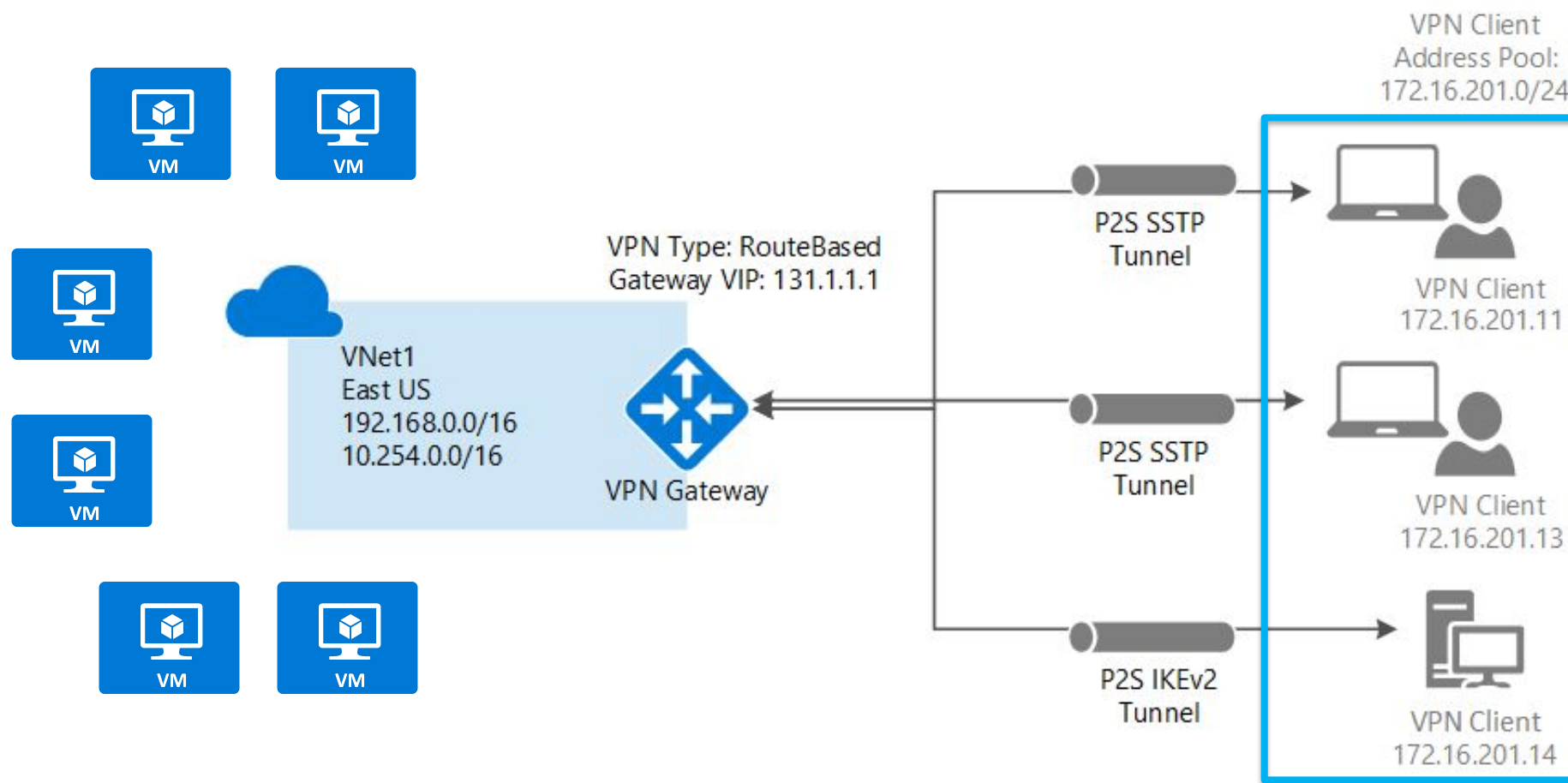
- Secure connection from an individual computer. Great for remote worker situations.

- No need for a VPN device or public IP. Connect wherever user has internet connection.

- OS Support: Windows 7, 8, 8.1 (32 and 64bit), Windows 10, Windows Server 2008 R2, 2012, 2012 R2 64-bit.

- Throughput up to 100 Mbps (unpredictable due to internet).

- Doesn't scale easily, so only useful for a few workstations.

VPN Gateway SKUs

SKU	S2S/VNet-to-VNet Tunnels	P2S Connections	Aggregate Throughput Benchmark
VpnGw1	Max. 30	Max. 128	650 Mbps
VpnGw2	Max. 30	Max. 128	1 Gbps
VpnGw3	Max. 30	Max. 128	1.25 Gbps
Basic	Max. 10	Max. 128	100 Mbps

Gateway Recommendations

Workload	SKUs
Production, critical workloads	VpnGw1, VpnGw2, VpnGw3
Dev-test or proof of concept	Basic

SKU	Features
Basic	**Route-based VPN**: 10 tunnels with P2S; no RADIUS authentication for P2S; no IKEv2 for P2S **Policy-based VPN**: (IKEv1): 1 tunnel; no P2S
VpnGw1, VpnGw2, and VpnGw3	**Route-based VPN**: up to 30 tunnels (*), P2S, BGP, active-active, custom IPsec/IKE policy, ExpressRoute/VPN co-existence

ExpressRoute

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction
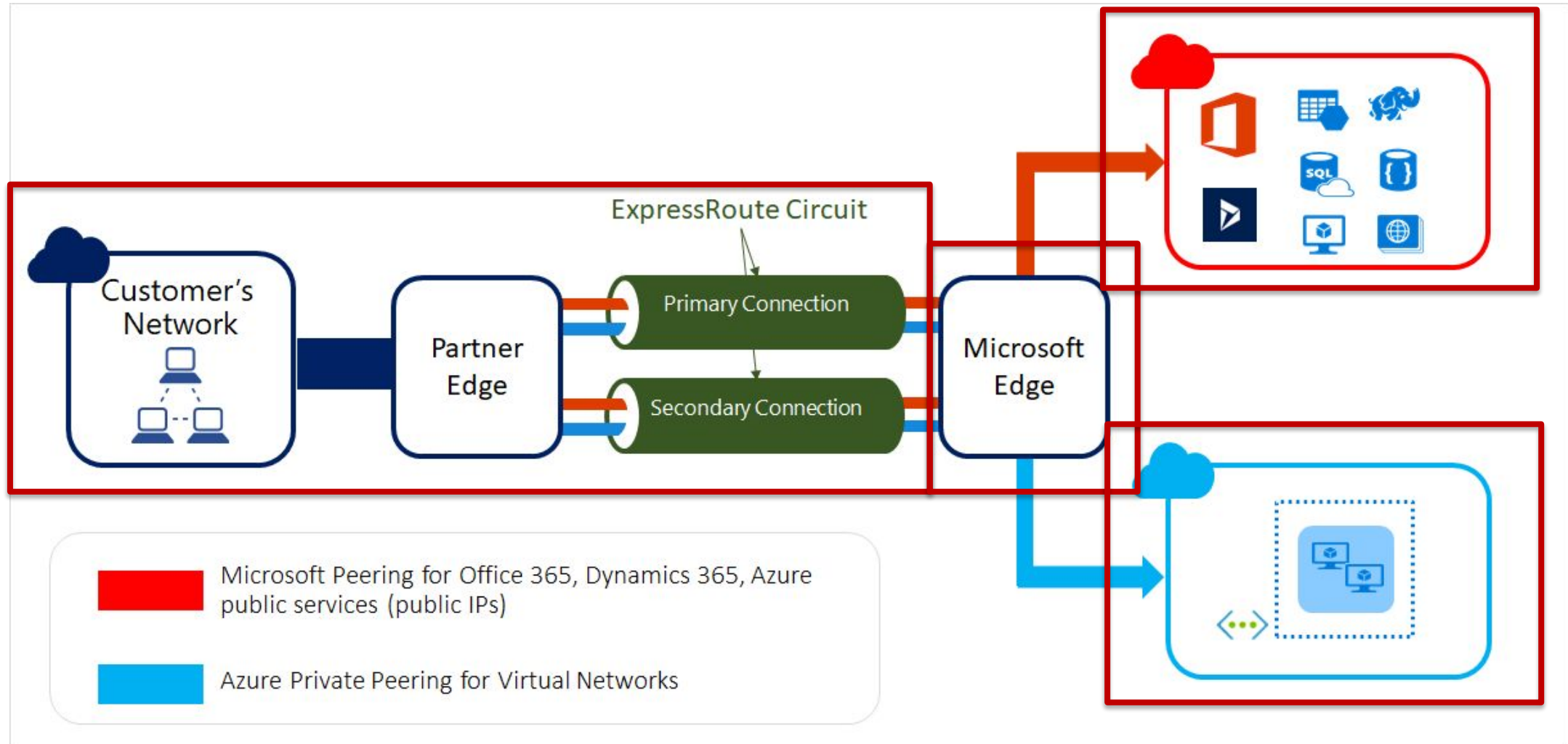
ExpressRoute Key Benefits

Layer 3 Connectivity

Between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.

Connectivity in all Regions

To Microsoft cloud services across all regions in the geopolitical region.

Global Connectivity

To Microsoft services across all regions with ExpressRoute premium add-on.

Dynamic Routing

Between your network and Microsoft over industry standard protocols (BGP).

Built-In Redundancy

In every peering location for higher reliability

ExpressRoute Provisioning

ENSURE THAT PREREQUISITES ARE MET
- Azure subscription created/exists
- Connectivity provider identified and relationship set up
- Physical connectivity with provider set up

ORDER EXPRESS ROUTE CIRCUIT
- Select service provider
- Select peering location
- Select bandwidth
- Select billing model
- Select standard or premium add-on

SERVICE PROVIDER PROVISIONS CONNECTIVITY
- Provide service key (s-key) to connectivity provider
- Provide additional information needed by connectivity provider (VPN ID)
- If provider manages routing, provide details

START USING EXPRESSROUTE CIRCUIT
- Link VNets to Azure private peering
- Connect to Auzre services on public IPs through Azure pubic peering
- Connect to Microsoft cloud Services through Microsoft peering

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-workflows

Peering – Data to Collect

Azure Private Peering

- Peering subnet for path 1 (/30)
- Peering subnet for path 2 (/30)
- VLAN ID for peering
- ASN for peering
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Azure Public Peering

- Peering subnet for path 1 (/30) – must be public IP
- Peering subnet for path 2 (/30) – must be public IP
- VLAN ID for peering
- ASN for peering
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Microsoft Peering

- Peering subnet for path 1 (/30) – must be public IP
- Peering subnet for path 2 (/30) – must be public IP
- VLAN ID for peering
- ASN for peering
- Advertised prefixes – must be public IP prefixes
- Customer ASN (optional if different from peering ASN)
- RIR/IRR for IP and ASN validation
- ExpressRoute ASN = 12076
- MD5 Hash (optional)

Unlimited versus Metered

Unlimited

- Speeds from 50 Mbps to 10 Gbps
- Unlimited Inbound data transfer
- Unlimited Outbound data transfer
- Higher monthly fee

Metered

- Speeds from 50 Mbps to 10 Gbps
- Unlimited Inbound data transfer
- Outbound data transfer charged at a predetermined rate per GB
- Lower monthly fee

ExpressRoute Considerations

Understand the models

- Differences between Unlimited Data and Metered Data
- Understand what model you are using today to accelerate adoption
- Understand the differences in available port speeds, locations and approach
- Understand the limits that drive additional circuits

Understand the providers

- Each offer a different experience based on ecosystem and capabilities
- Some provide complete solutions and management

Understand the costs

- Connection costs can be broken out by the service connection costs (Azure) and the authorized carrier costs (telco partner)
- Unlike other Azure services, look beyond the Azure pricing calculator

Load Balancers

Azure Load Balancing Services

**Load
Balancer**
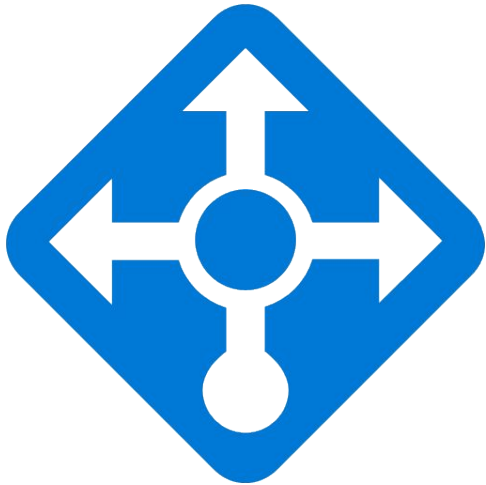
**Application
Gateway**

**Traffic
Manager**
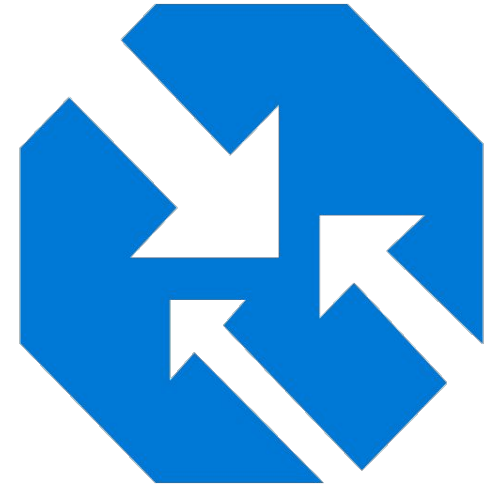
Azure Load Balancer
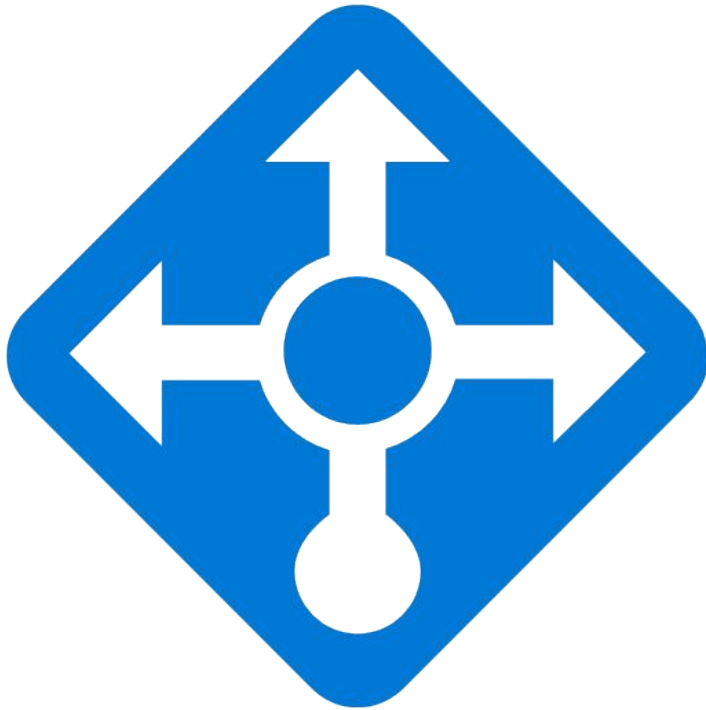
Key Features:

- Layer 4
- Basic and standard (preview) SKUs
- Service monitoring
- Automated reconfiguration
- Hash-based distribution
- Internal and public options

Azure Load Balancer: Internal Example
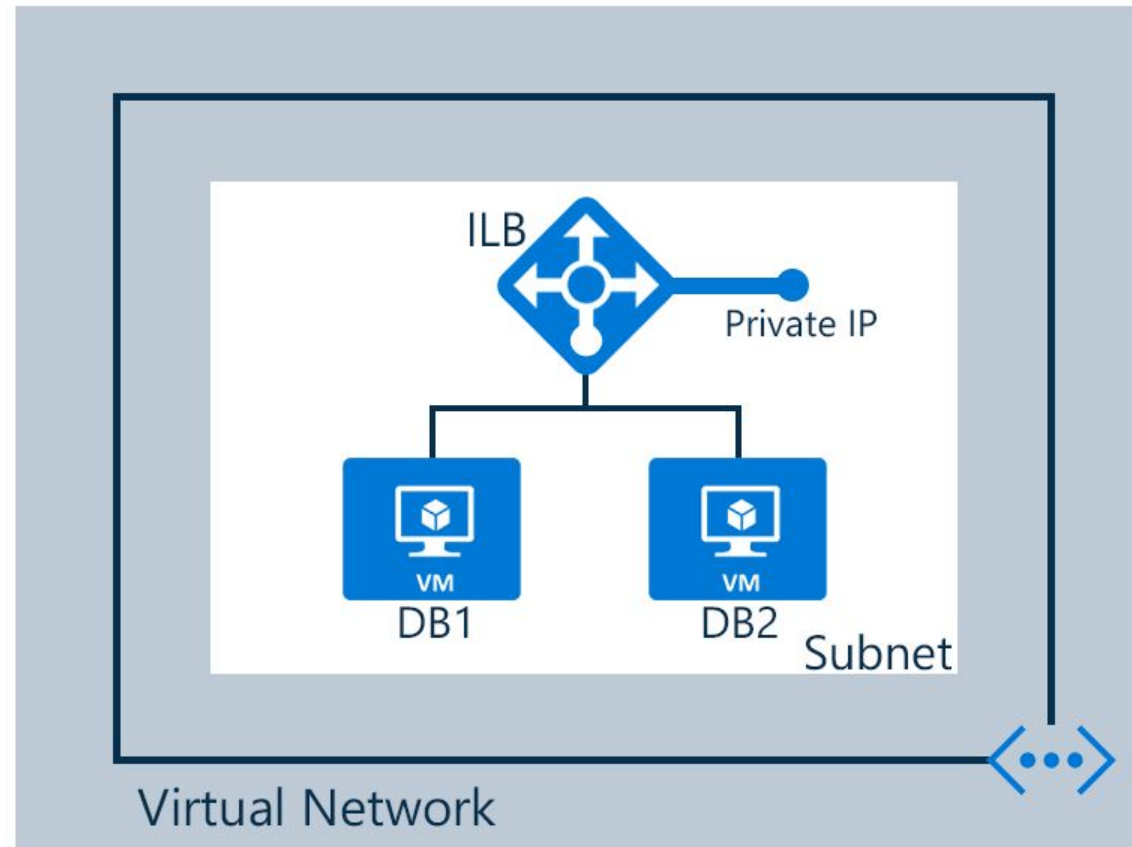
Azure Load Balancer: Public Example
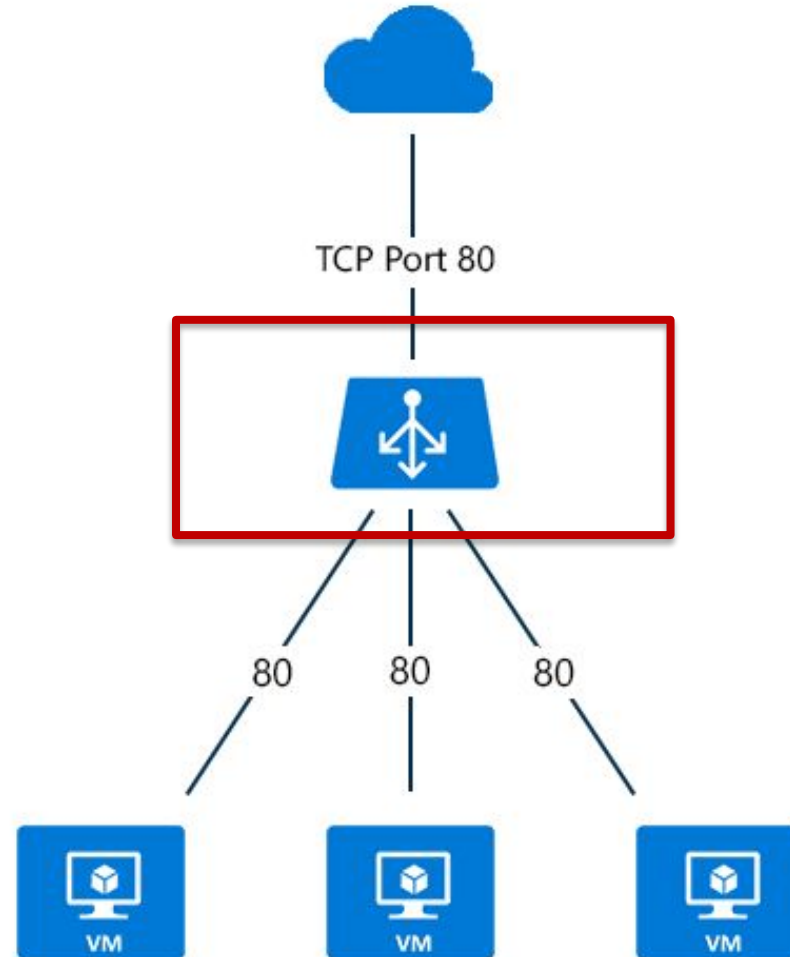
Azure Load Balancer: Multi-Tier Example
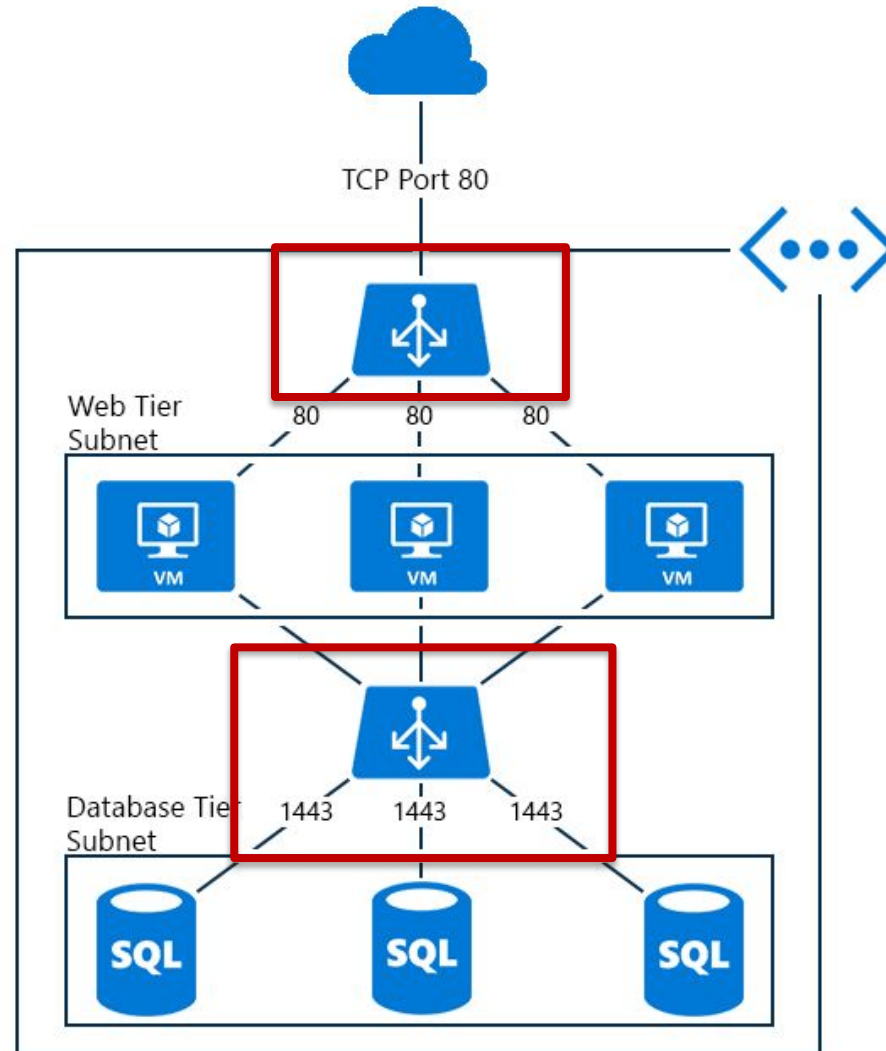
Load Balancing: App Gateway

Key Features:

- Layer 7 application load balancing
- Cookie-based session affinity
- SSL offload
- End-to-end SSL
- Web application firewall
- URL-based content routing
- Requires its own subnet

App Gateway Sizes

Page Response	Small	Medium	Large
6K	7.5 Mbps	13 Mbps	50 Mbps
100K	35 Mbps	100 Mbps	200 Mbp

Load Balancer Comparison

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport level (Layer 4)	Application level (Layer 7)	DNS-level
Application Protocols Supported	Any	HTTP, HTTPS, and WebSockets	Any (An HTTP endpoint is required for endpoint monitoring)
Endpoints	Azure VMs and Cloud Services role instances	Any Azure internal IP address, public internet IP address, Azure VM, or Azure Cloud Service	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
VNet support	Can be used for both Internet- facing and internal (VNet) applications	Can be used for both Internet-facing and internal (VNet) applications	Only supports Internet-facing applications
Endpoint Monitoring	Supported via probes	Supported via probes	Supported via HTTP/HTTPS GET

CDN

CDN

CDN

Theodore

Other Users

Edge
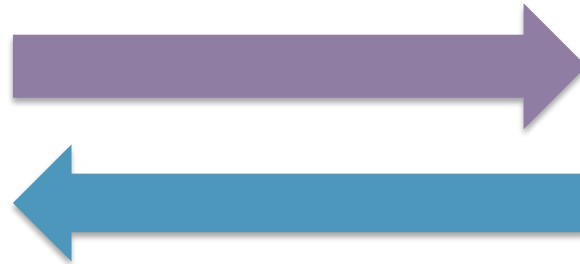
Source
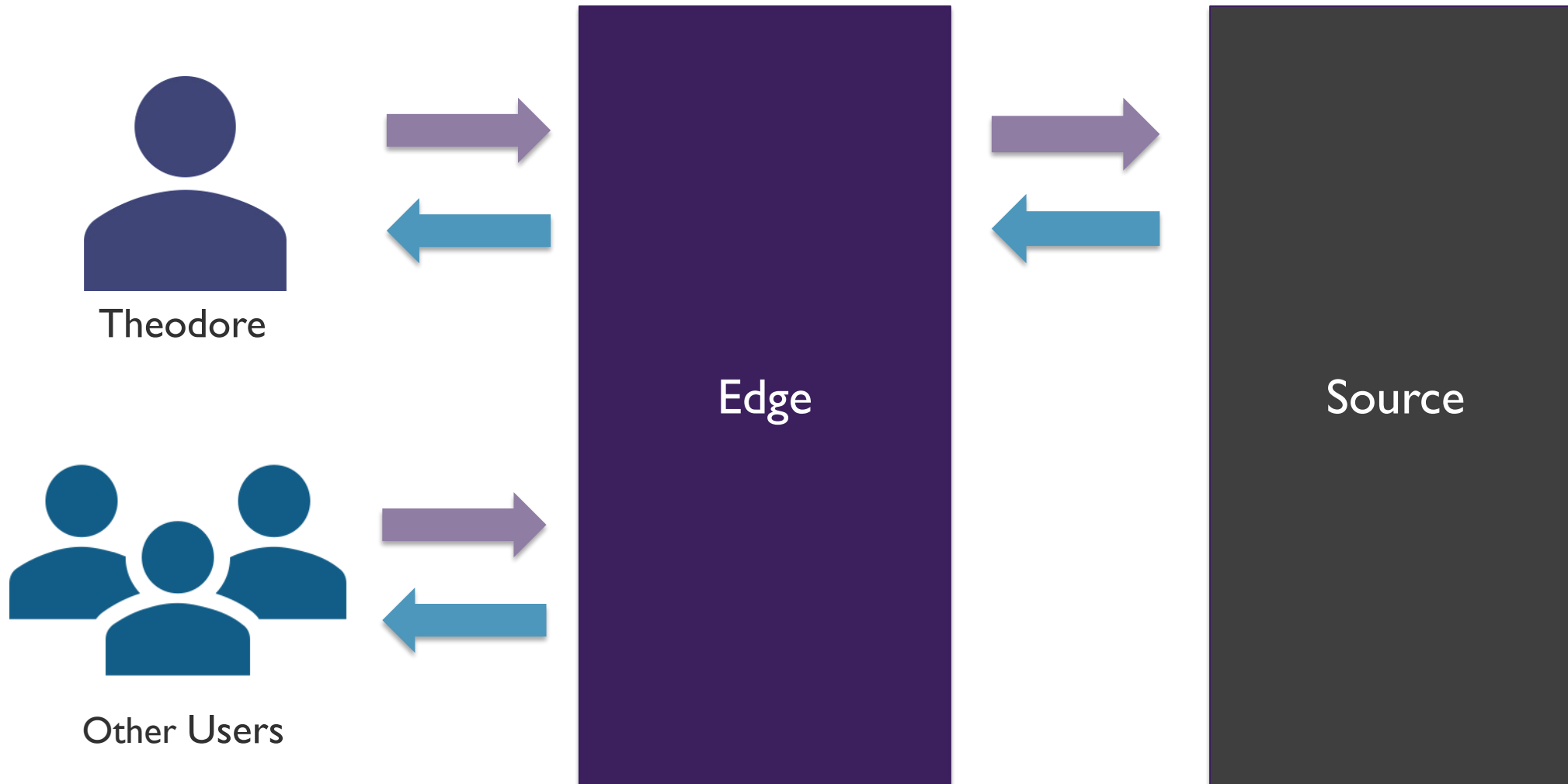
Azure CDN Offerings

Standard Akamai

Standard Verizon

Premium Verizon

https://docs.microsoft.com/en-us/azure/cdn/cdn-overview

Azure CDN Offerings

P1 Premium Verizon
- All standard features
- Token authentication
- Performance analytics
- Realtime analytics
- Mobile device rules
- Custom rules engine
- Cache/Header settings
- URL redirect/rewrite

S1 Standard Verizon
- Endpoint HTTPS
- Custom domain HTTPS
- Content Purge/Load
- Compression
- Geo-filtering
- Core analytics
- Dynamic delivery

S2 Standard Akamai
- Endpoint HTTPS
- Content Purge
- Compression
- Geo-filtering
- Large file optimization
- Media optimization
- Core analytics
- Dynamic delivery

Types of Data

Types of Data

Structured Data

Semi-Structured Data

Unstructured Data

Structured Data
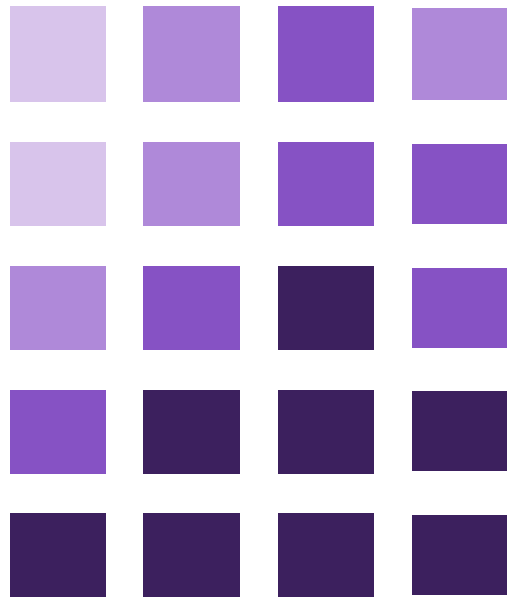
- Adheres to a schema
- All the data has the same field or properties
- Stored in a database table with rows and columns
- Relies on keys to indicate how one row in a table relates to data in another row of another table
- Referred to as "relational data"

Semi-Structured Data

- Doesn't fit neatly into tables, rows and columns.
- Uses tags or keys to organize and provide a hierarchy for the data.
- Often referred to as NoSQL or non-relational data
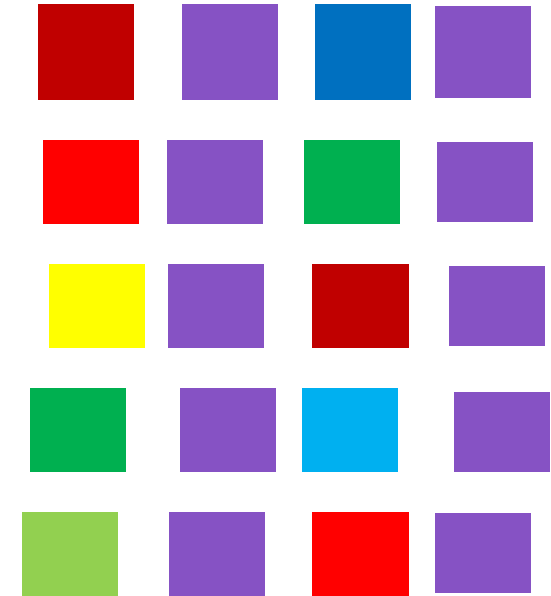
Unstructured Data
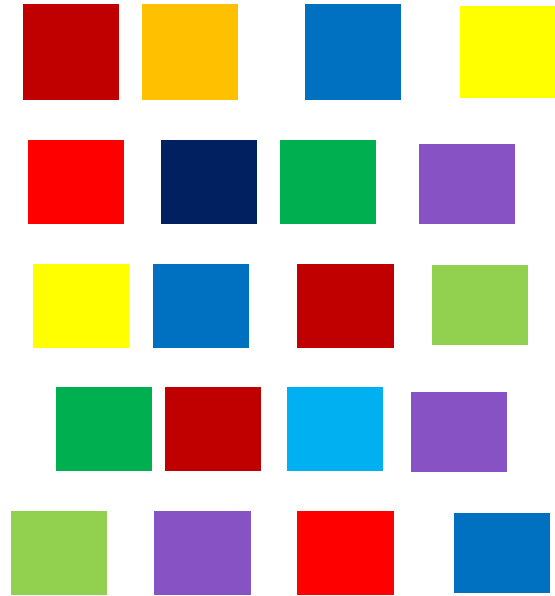
- No designated structure
- No restrictions on the kinds of data it can hold
- Example a blob can hold a PDF, JPEG, JSON, videos etc.
- Enterprises are struggling to manage and tap into the insights from their unstructured data

Azure SQL Services

Azure SQL

- Relational database-as-a-service
- Uses latest stable version of Microsoft SQL
- Create NEW or…
- Migrate Existing databases using the Microsoft Data Migration Assistant

Azure SQL Database – Key Features

Predictable Performance

Measured in database throughput units (DTUs)

High Compatibility

Supporting existing SQL client applications via tubular database stream (TDS) endpoint

Simplified Management

This includes SQL Server-specific Azure tools

Azure SQL Database Tiers

Basic	Standard	Premium
Small database with single concurrent user	**Medium-sized database that must support multiple concurrent connections**	**Large databases that must support a large number of concurrent connections and operations**
• Small dbs • Single active operation • Dev / Test • Small scale apps • 5 DTU	• Good option for cloud apps • Multiple operations • Workgroup or web apps • 10-100 DTU	• High transaction volumes • Large number of users • Multiple operations • Mission critical apps • 100-800 DTU

NEW – Azure SQL Managed Instances

- Managed SQL Servers
- More compatible with legacy workloads

Third-party Databases in Azure – Managed

- Managed database options:
  - Build-in HA at no additional cost
  - Predictable performance
  - Pay-as-you-go
  - Auto-scaling
  - Encryption at-rest and in-transit
  - Automatic backups with point-in-time-restore for up to 35 days
  - Enterprise-grade security and compliance

Third-party Databases in Azure – Non-managed

- Non-managed database options:
  - Windows Azure VMs hosting MySQL installations
  - Linux Azure VMs hosting MySQL installations
  - ClearDB offering managed MySQL instance
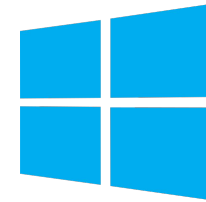
Cosmos DB

Azure Cosmos DB

- Globally Distributed Database Service
- Supports schema-less data
- Used to build highly responsive Always On applications with constantly changing data

Developer frequently updates the catalog

Online course catalog

Azure Cosmos DB database

Global users and training developers

Azure Cosmos DB APIs
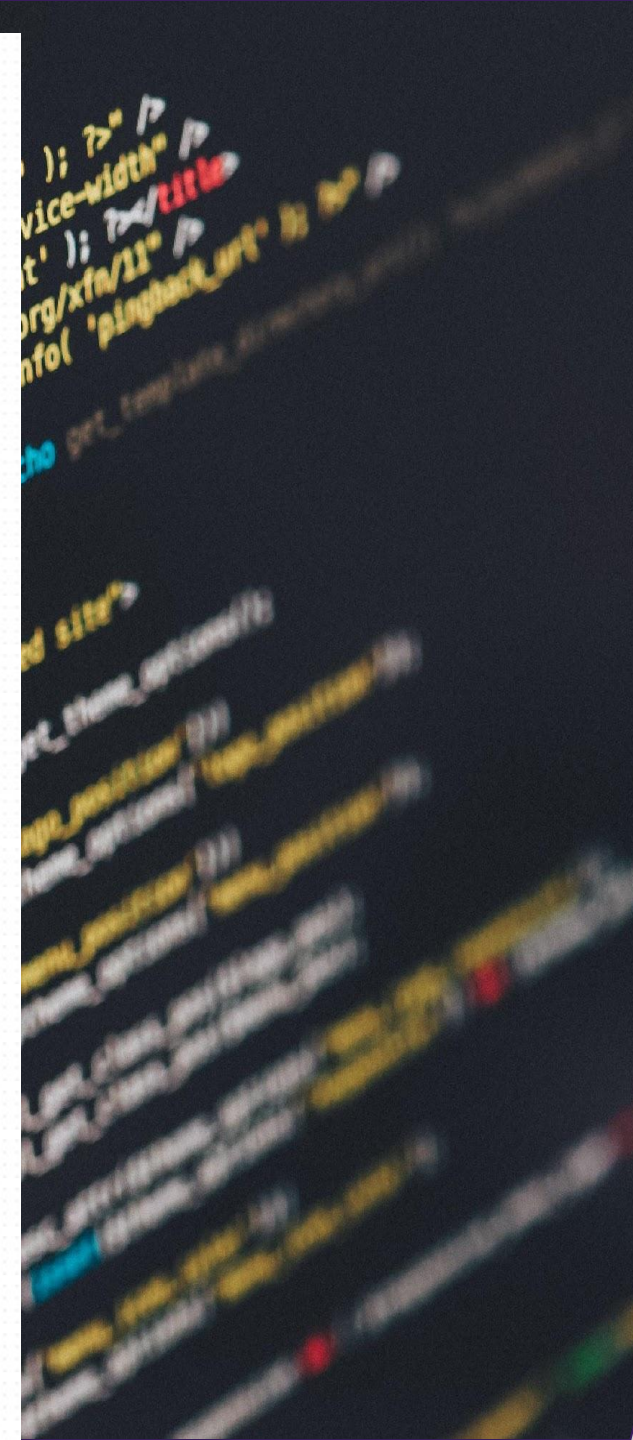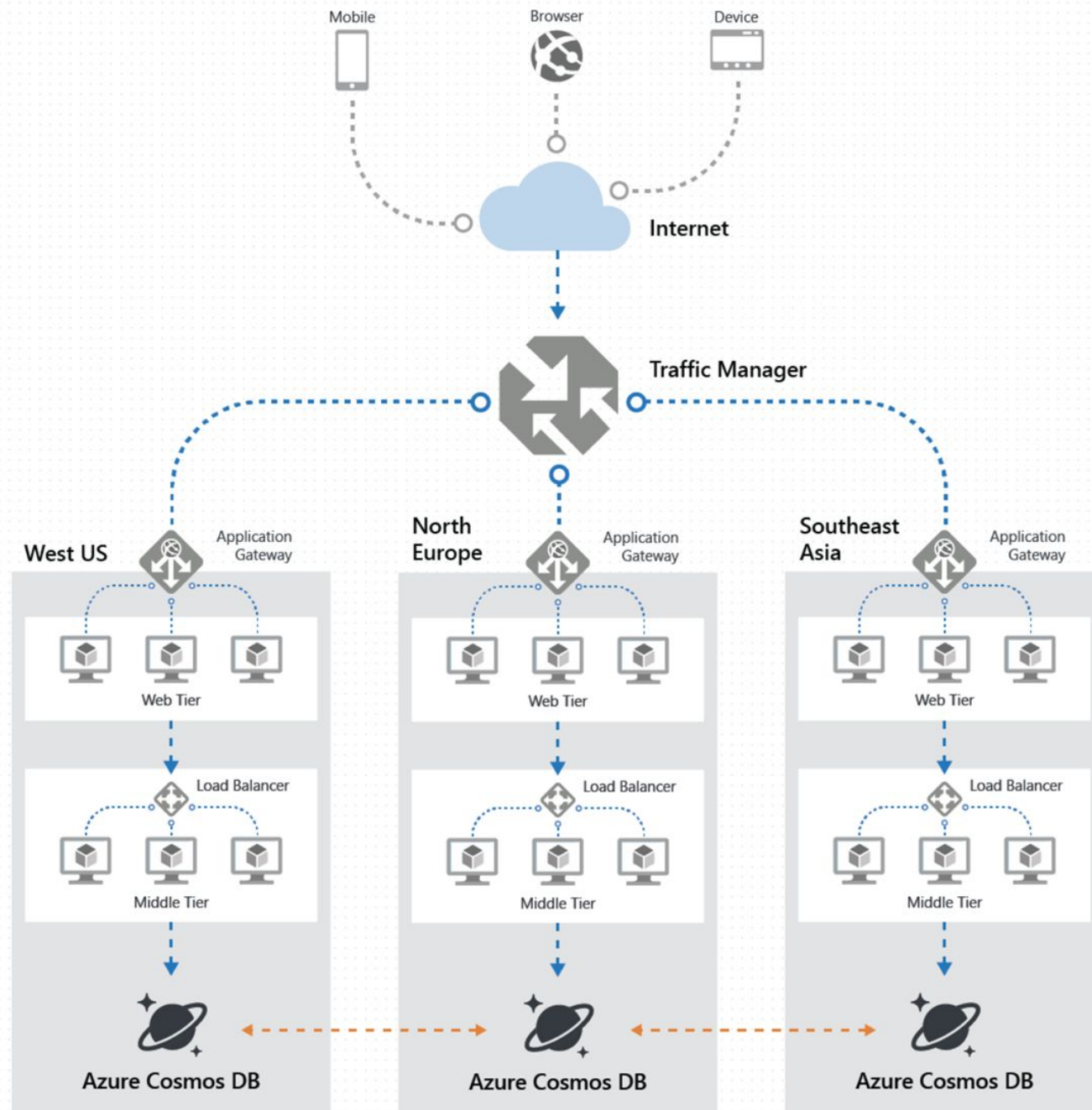
- Accessible via various APIs e.g:
  - Document DB (SQL) API
  - MongoDB API
  - Graph (Gremlin) API
  - Tables (Key/Value) API
- Automatically partitioned for:
  - Performance
  - Storage capacity

Azure Storage

Azure Blob Storage

- Unstructured storage for storing objects
- Store images, video, and files of any type
- Use cases:
  - Streaming video and images direct to user
  - Backup/DR of data
  - Archiving

SMB File Storage – Azure File Services

Benefits

- Easy way to create file shares
- Supports SMB 2.1 (unsecured) and 3.0 (secured)
- Mount on Windows, Linux, or Mac
- Azure File Sync can be utilized to sync file servers on-premises with Azure Files
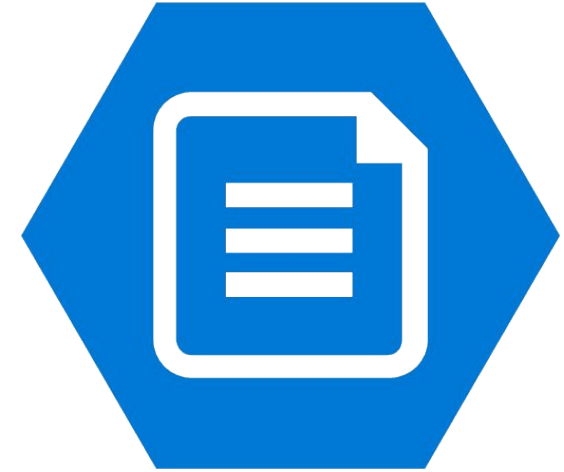
Azure Table Storage

Table Storage

- A NoSQL key-value store
- Schemaless design
- Structured or Unstructured Data
- Access using the Odata protocol and LINQ queries WCF Data Service .NET Libraries
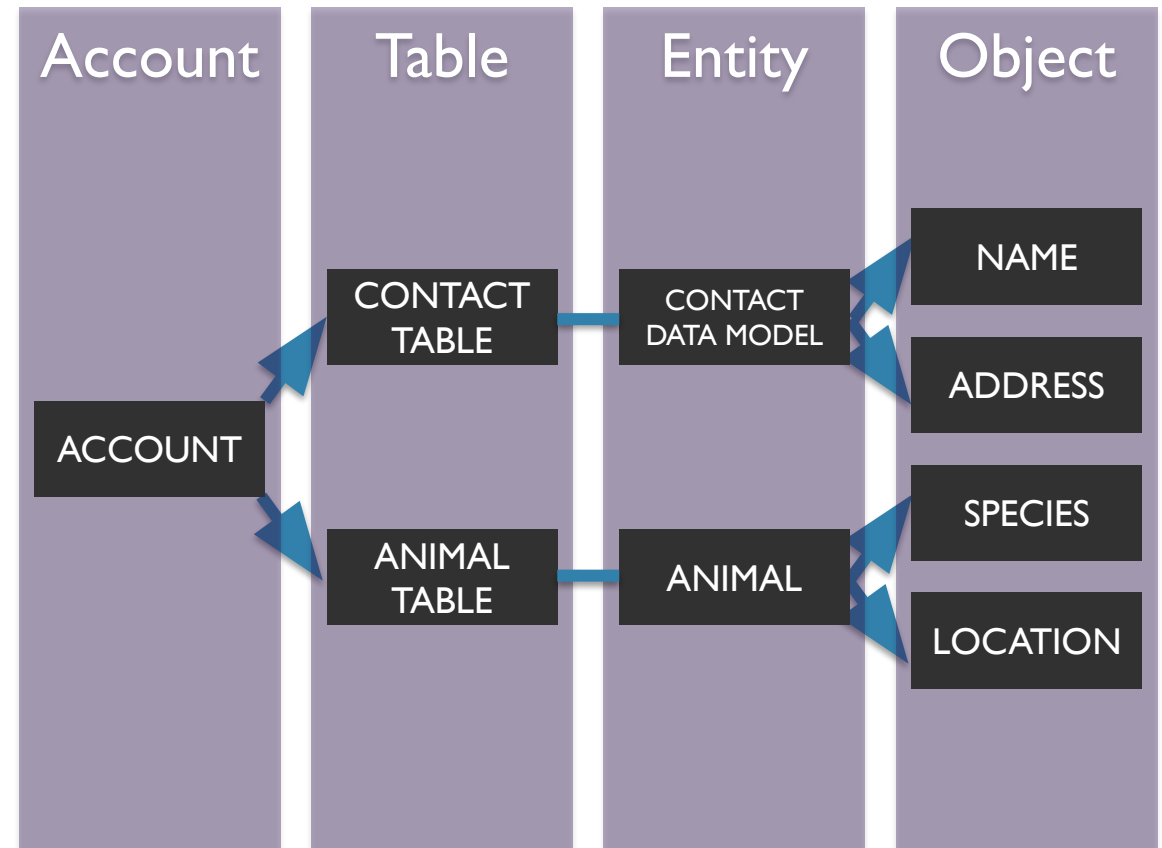
Azure Queue Storage

Queue Storage

- Provides a reliable mechanism for storage and delivering messages for applications
- A single queue message can be up to **64 KB in size**, and a queue can contain millions of messages, up to the total capacity limit of a storage account
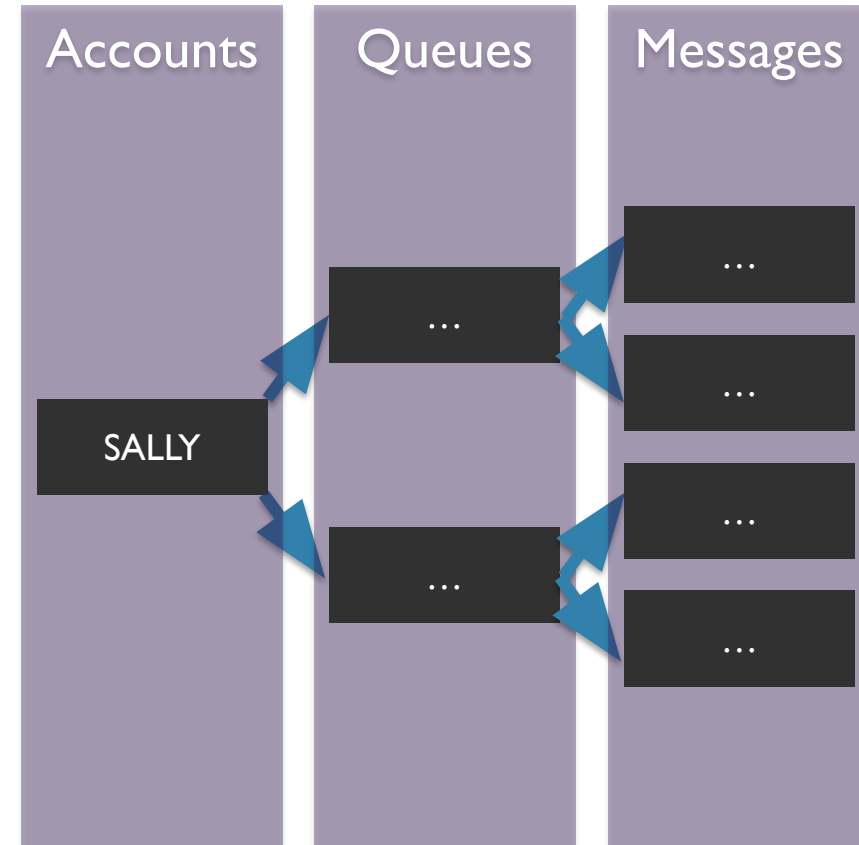
VM Storage

VM Storage Types

Standard HDD

Backed by traditional HDD

Most cost effective

Throughput based on VM

IOPs based on VM

Standard SSD

Backed by SSD drives

Recommended for most workloads

Max throughput – 500MB/S per disk

Max IOPS – 2000 IOPS per disk

Premium Storage

Backed by SSD drives

Higher performance Lowest Latency

Max throughput – 750MB/S per disk

Max IOPS – 7500 IOPS per disk

Managed Disk – Standard Storage Sizes

	S4	S6	S10	S20	S30	S40	S50
Disk size (GB)	32	64	128	512	1024	2048	4095

IOPs and throughput are not provisioned and depend on the performance of the VM.

Standard SSD Storage Sizes

	E4	E6	E10	E15	E20	E30	E40	E50
Disk size (GB)	32	64	128	256	512	1024	2048	4095
Max IOPS	120	240	500	500	500	500	500	500
Max through put	25 MB/s	50 MB/s	60 MB/s	60 MB/s	60 MB/s	60 MB/s	60 MB/s	60 MB/s

Premium SSD Storage Sizes

	P4	P6	P10	P15	P20	P30	P40	P50
Disk size (GB)	32	64	128	256	512	1024	2048	4095
Max IOPS	120	240	500	1100	2300	5000	7500	7500
Max through put	25 MB/s	50 MB/s	100 MB/s	125 MB/s	150 MB/s	200 MB/s	250 MB/s	250 MB/s

Ultra SSD Storage Sizes (Preview)

Disk size (GB)	4	8	16	32	64	128	256	512
Max IOPS	1200	2400	4800	9600	19200	38400	76800	80000
Max throughput MB/s	300	600	1200	2000	2000	2000	2000	2000

1,024 – 65,536 sizes also available increasing in increments of 1TiB.

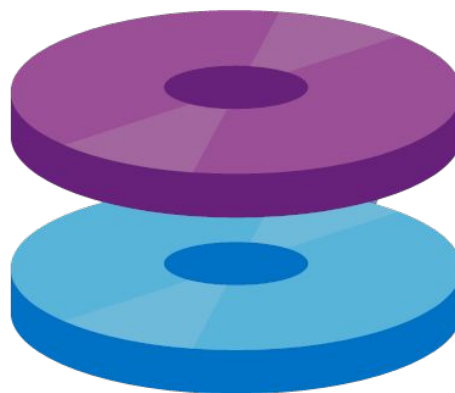IOPs capped at 160,000 and throughput capped at 2,000

Managed vs. Unmanaged Disks

Unmanaged Disks

DIY option

Management overhead
(20000 IOPS per storage
account limit)

Supports all replication
modes
(LRS, ZRS, GRS, RA-GRS)

Managed Disks

Simplest option

Lower management
overhead as Azure manages
the storage accounts

Only LRS replication mode
currently available

Replication Options

| Logically Replicated Storage (LRS)	Zone Replicated Storage (ZRS)	Geographically Replicated Storage (GRS)	Read Only Geographically Replicated Storage (RA-GRS)
Replicated three times within a storage scale unit (collection of racks of storage nodes) hosted in a datacenter in the same region as your storage account was created.	Replicated three times across one or two datacenters in addition to storing three replicas similar to LRS. Data stored in ZRS is durable even in the event that the primary datacenter is unavailable or unrecoverable.	Replicates your data to a second region that is hundreds of miles away from the primary region. Your data is curable even in the event of a complete region outage.	Same replication as per GRS but also provides read access to the data in the other region.

Replication Strategies

Replication Strategy	LRS	ZRS	GRS	RA-GRS
Data is replicated across multiple datacenters?	No	Yes	Yes	Yes
Data can be read from a secondary location *and* the primary location?	No	No	No	Yes
Number of copies of data maintained on separate nodes:	3	3	6	6

Storage Account Overview

SKYLINES
ACADEMY

Azure Blob Storage Overview
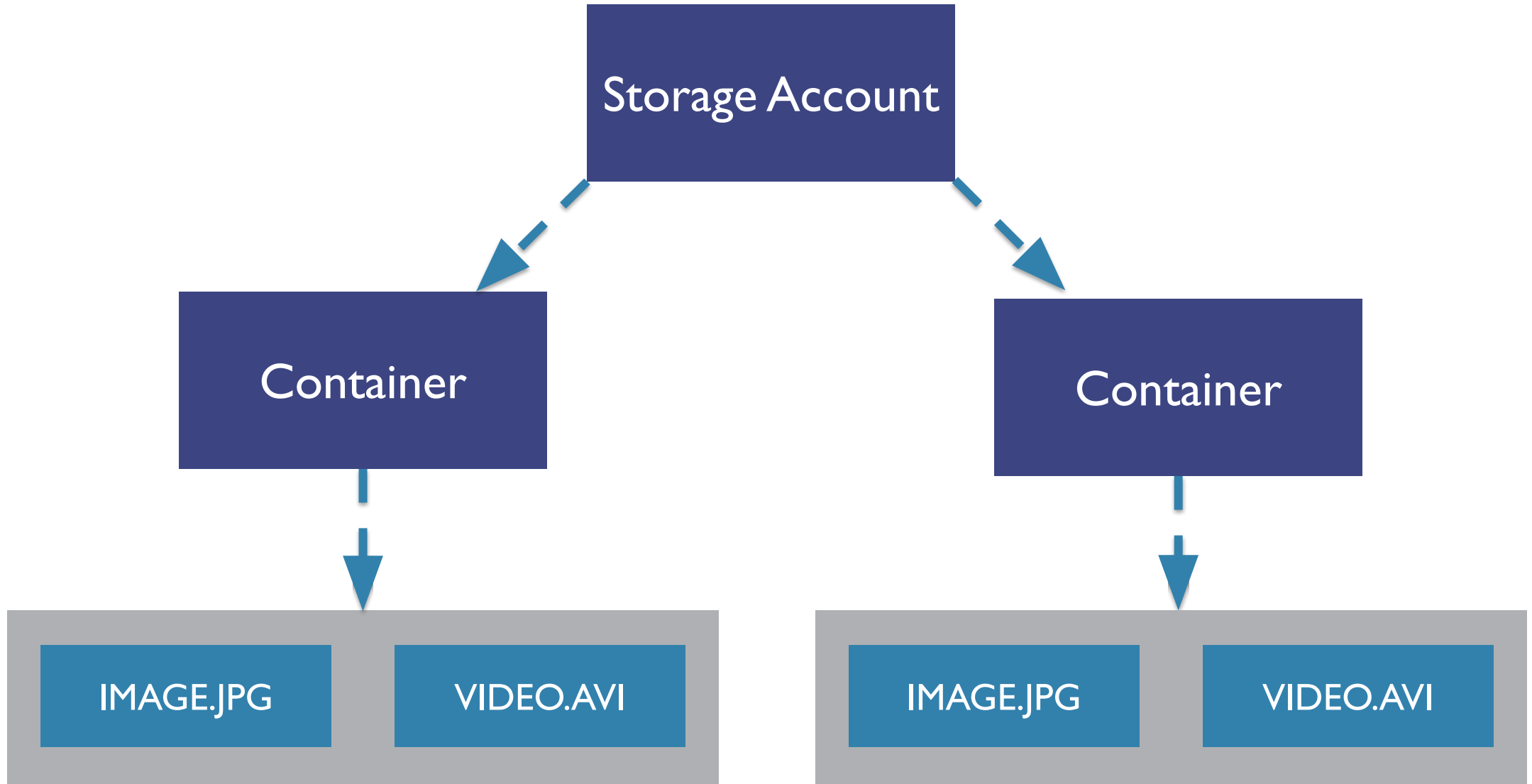
Storage Account Types

General Purpose v1 (GPV1)

Blob Account

General Purpose v2 (GPV2)

Block Blobs vs. Page Blobs

Block Blob

- Ideal for storing text or binary files

- A single block blob can contain up to 50,000 blocks of up to 100 MB each, for a total size of 4.75 TB

- Append blobs are optimized for append operations (e.g. logging)

Page Blob

- Efficient for read/write operations

- Used by Azure VMs

- Up to 8 TB in size

Storage Tiers

Hot

- Higher storage costs
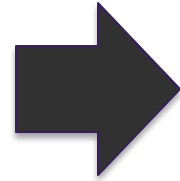- Lower access costs

Cold

- Lower storage costs
- Higher access costs
- Intended for data that will remain cool for 30 days or more

Archive

- Lowest storage costs
- Highest retrieval costs
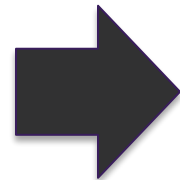- When a blob is in archive storage it is offline and cannot be read
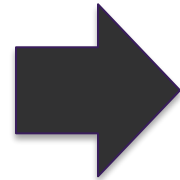
Choosing Between Blobs, Files, and Disks

Blobs

→
- Access application data from anywhere
- Large amount of objects to store, images, videos etc.
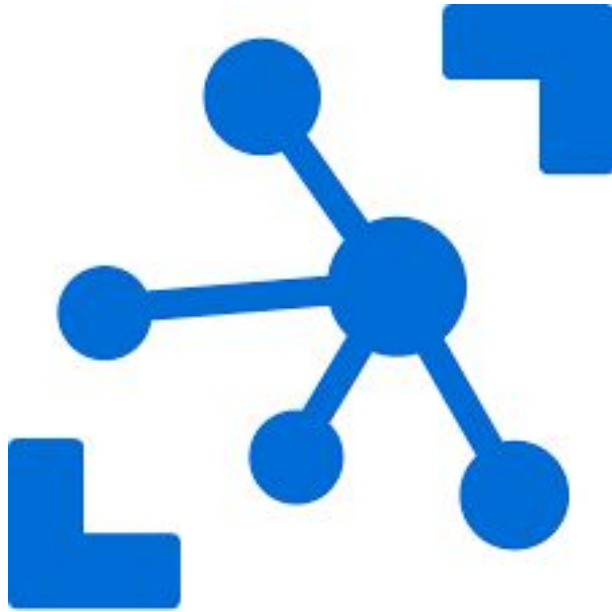
Files

→
- Access files across multiple machines
- Jumpbox scenarios for shared development scenarios

Disks

→
- Do not need to access the data outside of the VM
- Lift-and-shift of machines from on-premises
- Disk expansion for application installations

IoT Services

Azure IoT

- Collection of Microsoft managed cloud services focused on connecting, monitoring and controlling IoT assets

- IoT solutions are made up of 1 or more IoT devices and 1 or more back end services running in the cloud.

IoT Device Examples

- Water sensors for farming
- Pressure sensors on a remote oil pump
- Temperature and humidity sensors in an air-conditioning unit

IoT Services in Azure

IoT Central

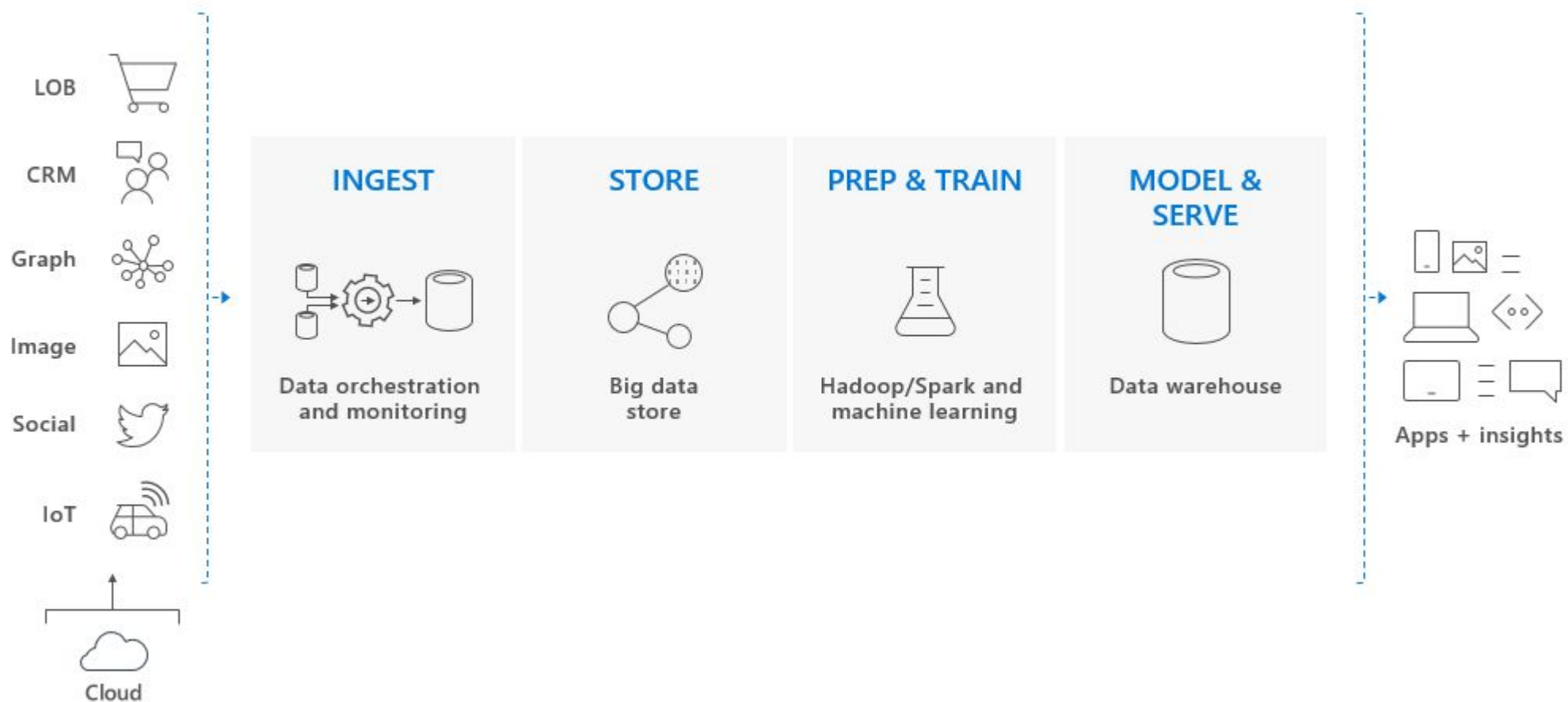SaaS solution to help you connect and manage your devices

IoT Hub

Underlying service needed to facilitate messages between your IoT application and devices

IoT Solution Accelerators

Complete ready to deploy solutions that implement common IoT scenarios

Big Data Services
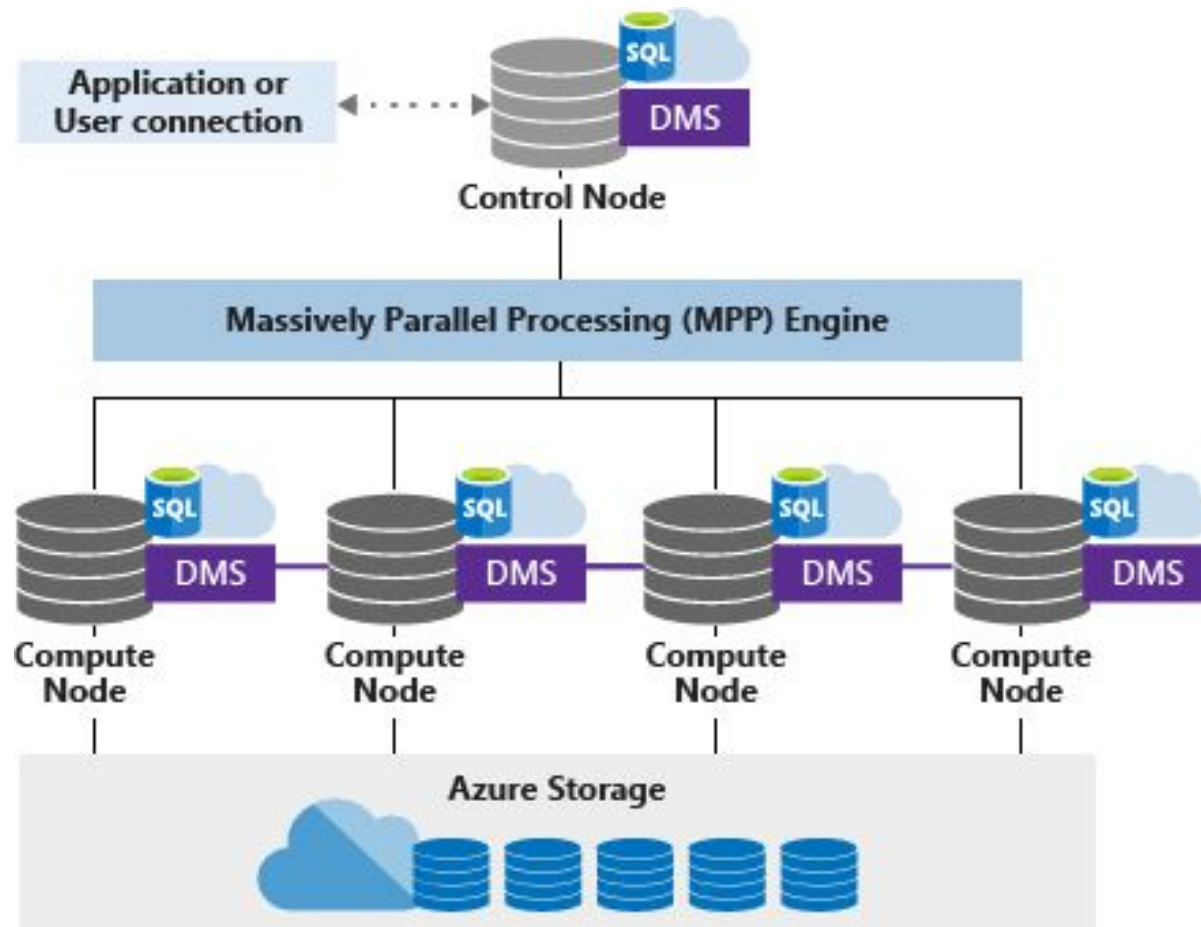
Big Data Solution

SQL Data Warehouse

- Key component of a Big Data solution
- Cloud based Enterprise Data Warehouse (EDW) that uses Massive Parallel Processing (MPP) to run complex queries across petabytes of data.
- Stores data in relational tables reducing storage costs and improves performance

SQL DW Architecture

HD Insight

HDInsight

- Fully managed open-source analytics service for enterprises
- Use the most popular frameworks like Hadoop, Spark, Hive etc.
- Scenarios:
  – Batch Processing (ETL)
  – Data Warehousing

Data Lake Analytics

- On-Demand job service that simplifies big data
- Pay only for your job when it is running
- You write queries to transform your data and extract insights

Which service?

SKYLINES
ACADEMY

| IF YOU WANT...	USE THIS
A fully managed, elastic data warehouse with security at every level of scale at no extra cost	SQL Data Warehouse
A fully managed, fast, easy and collaborative Apache® Spark™ based analytics platform optimized for Azure	Azure Databricks
A fully managed cloud Hadoop and Spark service backed by 99.9% SLA for your enterprise	HDInsight
A data integration service to orchestrate and automate data movement and transformation	Data Factory
Open and elastic AI development spanning the cloud and the edge	Machine Learning
Real-time data stream processing from millions of IoT devices	Azure Stream Analytics
A fully managed on-demand pay-per-job analytics service with enterprise-grade security, auditing, and support	Data Lake Analytics
Enterprise grade analytics engine as a service	Azure Analysis Services
A hyper-scale telemetry ingestion service that collects, transforms, and stores millions of events	Event Hubs
Fast and highly scalable data exploration service	Azure Data Explorer

Machine Learning

Azure Machine Learning

- Machine learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes, and trends. By using machine learning, computers learn without being explicitly programmed.

- Azure Machine Learning service provides a cloud-based environment you can use to prep data, train, test, deploy, manage, and track machine learning models.

- Automated ML and DevOps capabilities
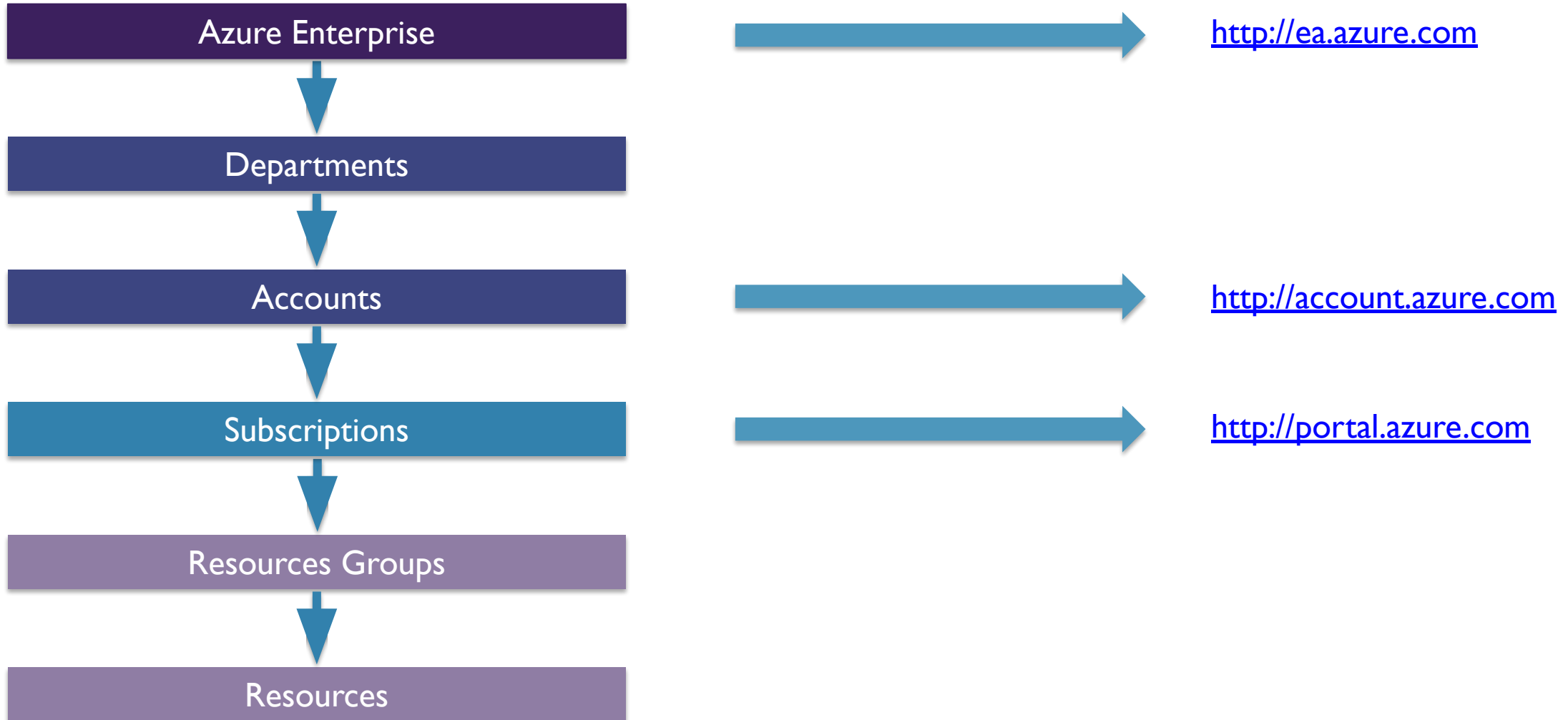
Machine Learning Studio
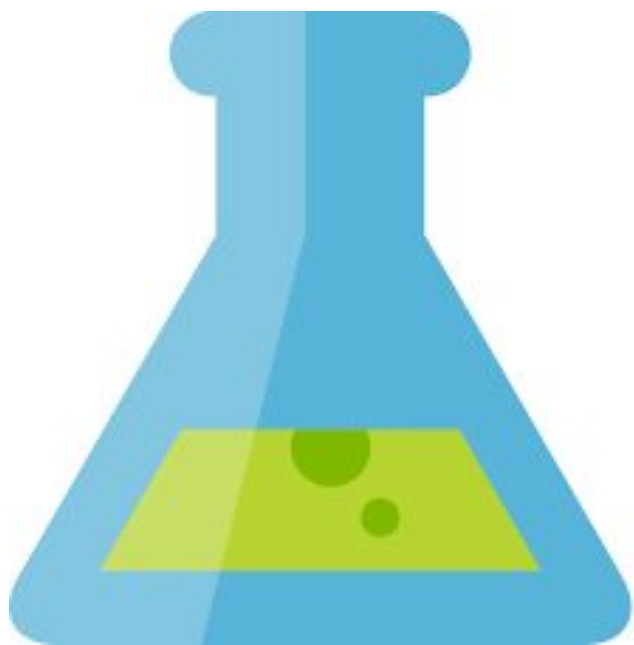
- Collaborative, drag-and-drop visual workspace where you can build, test, and deploy machine learning solutions without needing to write code.

- Uses prebuilt and preconfigured machine learning algorithms and data-handling modules as well as a proprietary compute platform

Azure Account Hierarchy

Azure Enterprise → http://ea.azure.com

Departments

Accounts → http://account.azure.com

Subscriptions → http://portal.azure.com

Resources Groups

Resources

SKYLINES
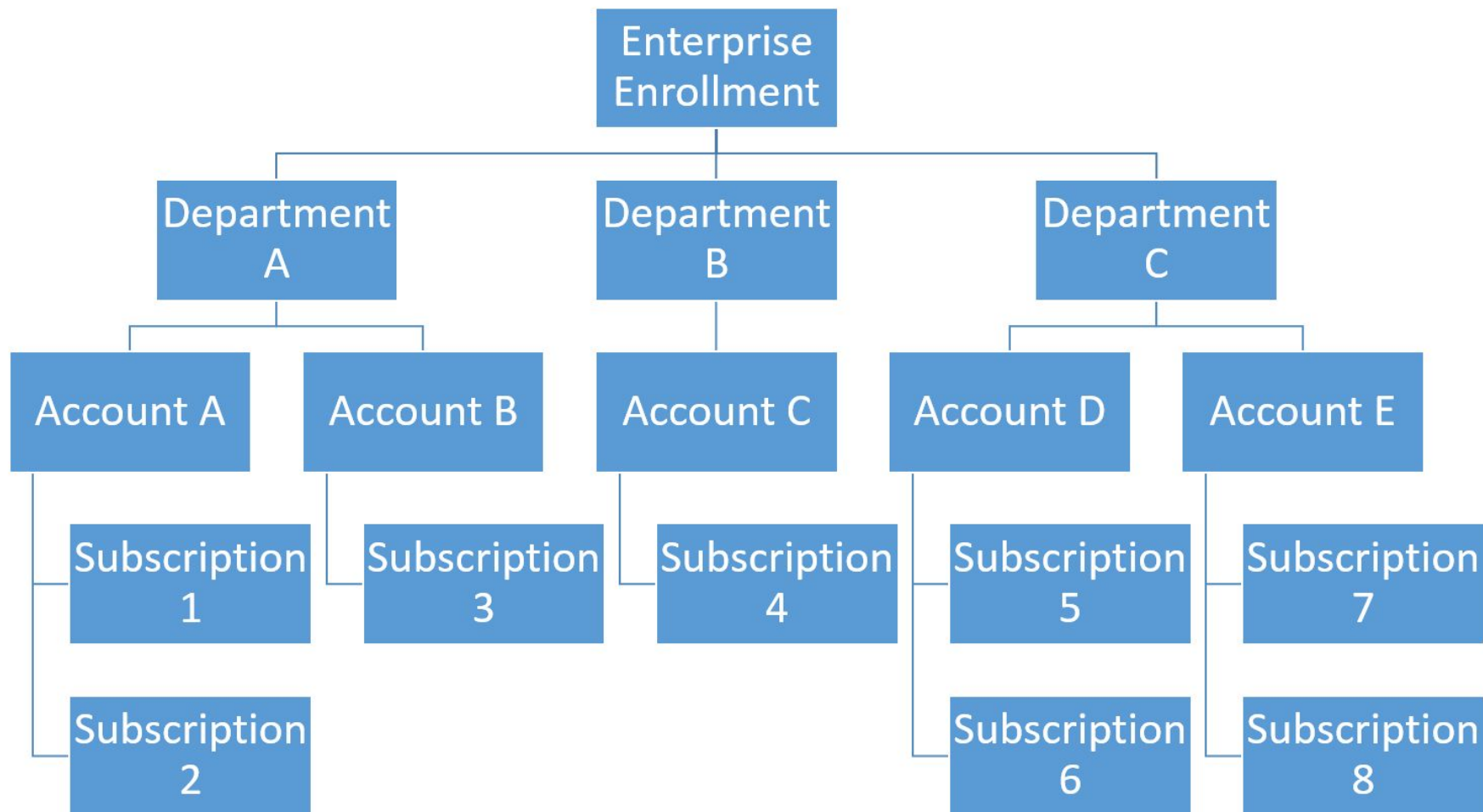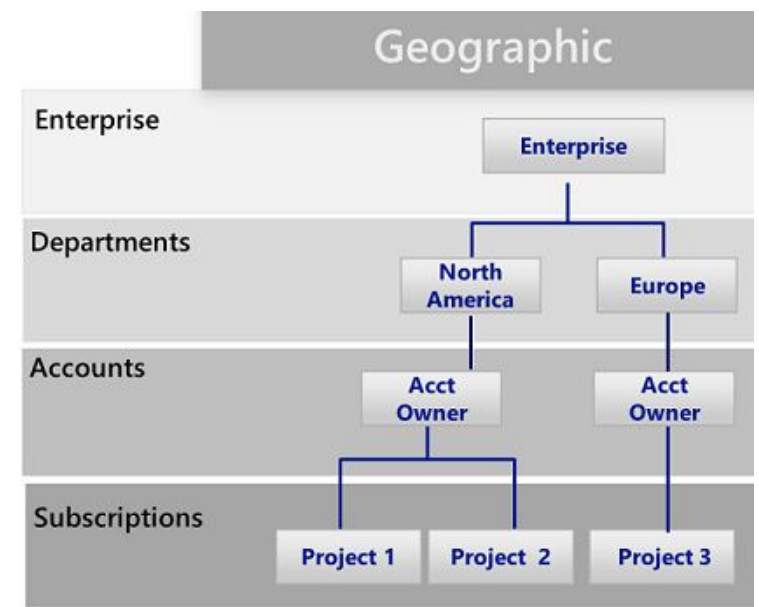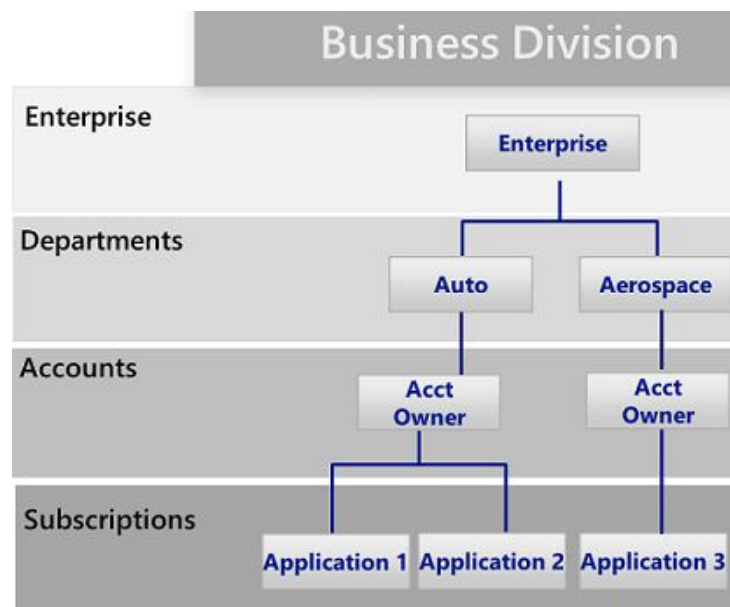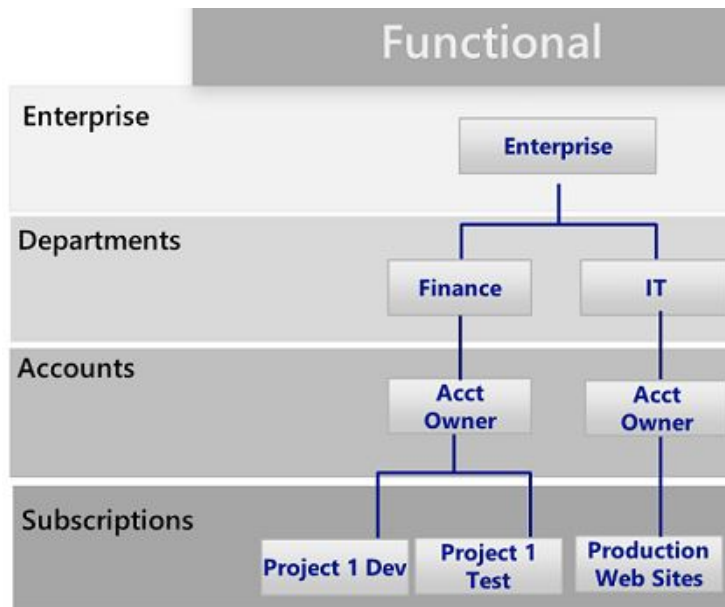ACADEMY

Account to Subscription Relationships

Enterprise Hierarchy Example

Common Scenarios

EA Breakdown

	Enterprise Admin	Department Admin	Account Owner	Service Admin
Add other admins	Enterprise Admins, Department Admins, and Account Owners	Account Owners	Add Service Admins	No
Departments	Add/Edit Departments	Edit Department	X	X
Add or associate accounts to the enrollment	Yes	Yes – to the department	No	No
Add Subscriptions	No – but can add themselves as AO	No	Yes	No
View usage and charges data	Across all Accounts and Subscriptions	Across Department	Across Account	No
View remaining balances	Yes	No	No	No

Domain Services

Domain Services Overview

Azure AD
(AAD)

Active Directory
Domain Services
(ADDS)

Azure Active
Directory
Domain Services
(AADDS)

Azure Active Directory

AAD

- Modern AD service built directly for the cloud

- Often the same as O365 directory service

- Can sync with On-premises directory service

Active Directory Domain Services

ADDS

- Legacy Active Directory since Windows 2000

- Traditional Kerberos and LDAP functionality

- Deployed on Windows OS usually on VMs
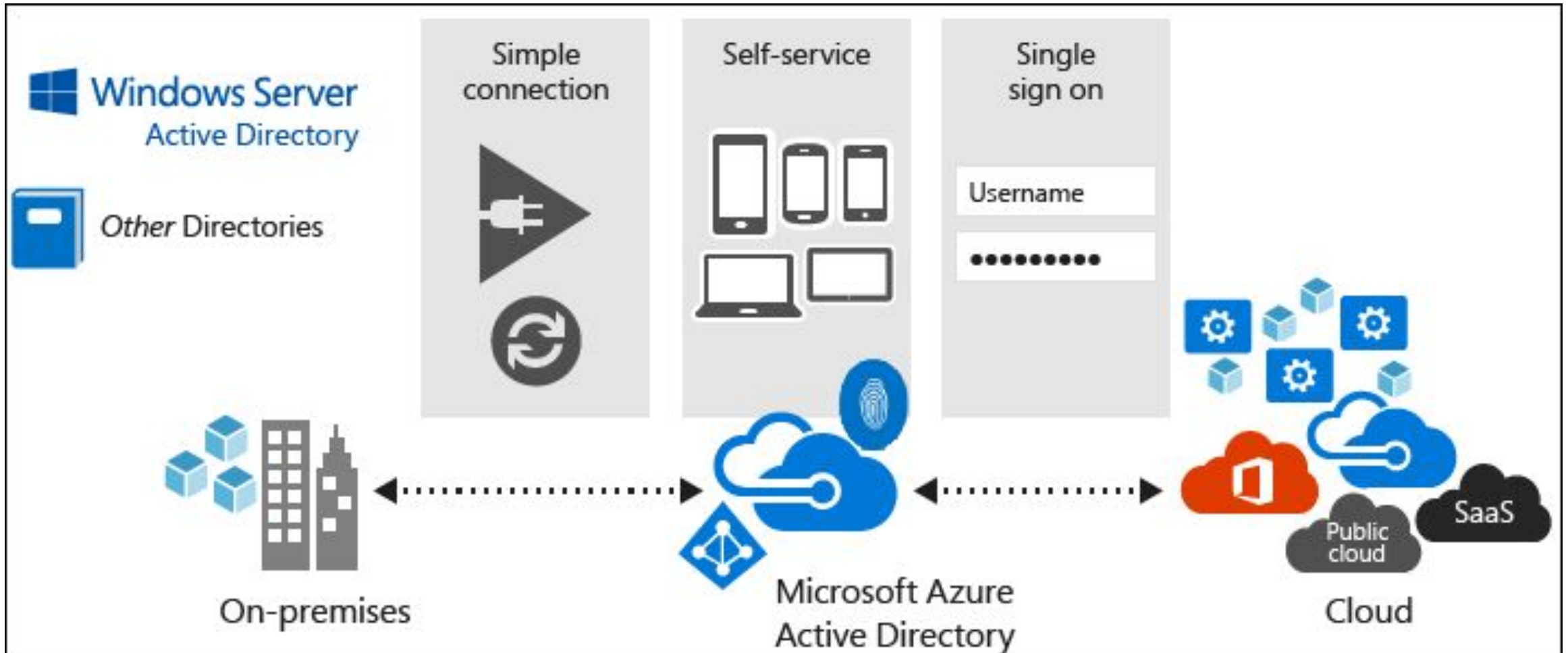
Azure Active Directory Domain Services

AADDS

- Provides managed domain services
- Allows you to consume domain services without the need to patch and maintain domain controllers on IaaS
- Domain Join, Group Policy, LDAP, Kerberos, NTLM; all supported

Azure AD

Azure AD Overview

Azure AD Features

Enterprise Identity Solution

Create a single identity for users and keep them in sync across the enterprise.

Single Sign-On

Provide single sign-on access to applications and infrastructure services.

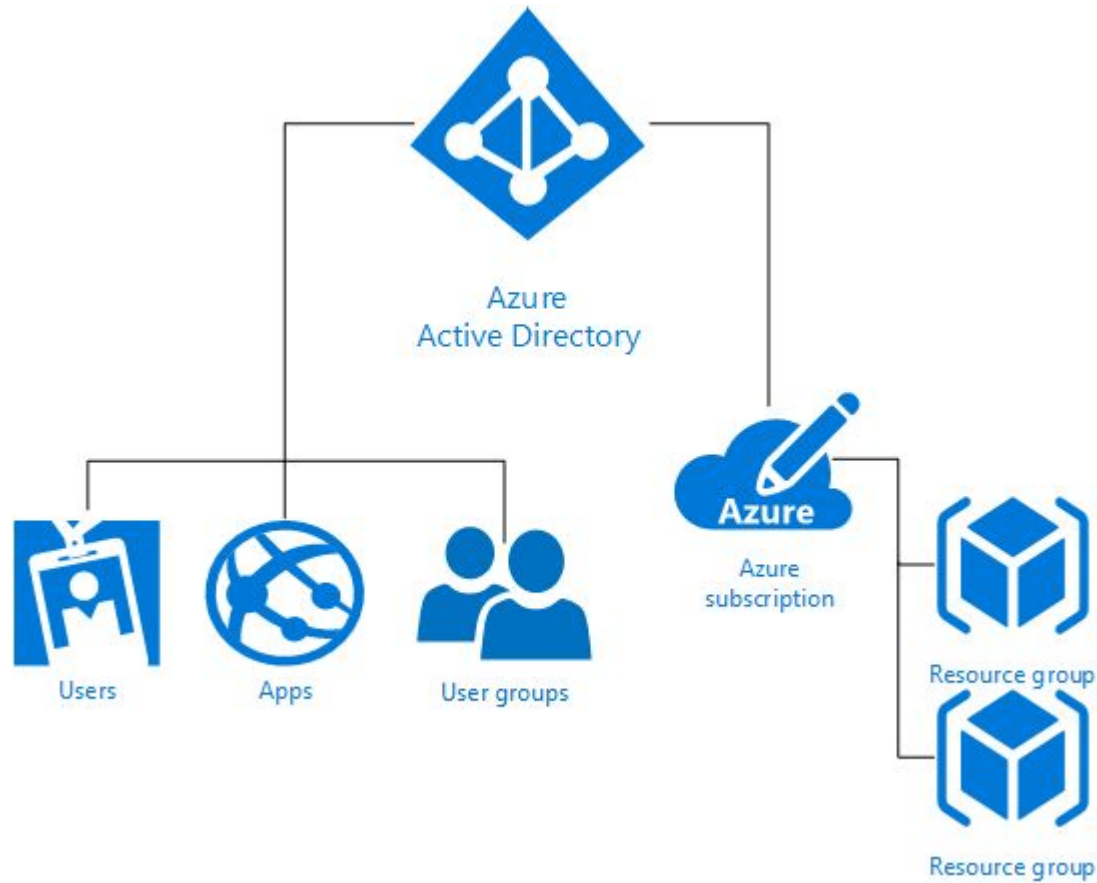## Multifactor Authentication (MFA)

Enhance security with additional factors of authentication.

Self Service

Empower your users to complete password resets themselves, as well as request access to specific apps and services.

Role-based Access Control (RBAC)

RBAC Overview

- Create Users, Apps, Groups
- Assign them to objects in Azure with a specific Role

Azure RBAC Built-in Roles

Owner	Contributor	Reader	Other Roles

Full access to all resources, including the right to delegate access to others

Can create and manage all types of Azure resources, but cannot grant access to others

Can view existing Azure resources, but cannot perform any other actions against them

https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles

Azure RBAC Built-in Roles (continued)

Role Name	Description
API Management Service Contributor	Can manage API Management service and the APIs
API Management Service Operator Role	Can manage API Management service, but not the APIs themselves
API Management Service Reader Role	Read-only access to API Management service and APIs
Application Insights Component Contributor	Can manage Application Insights components
Automation Operator	Able to start, stop, suspend, and resume jobs
Backup Contributor	Can manage backup in Recovery Services vault
Backup Operator	Can manage backup except moving backup in Recovery Services vault
Backup Reader	Can view all backup management services

https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles
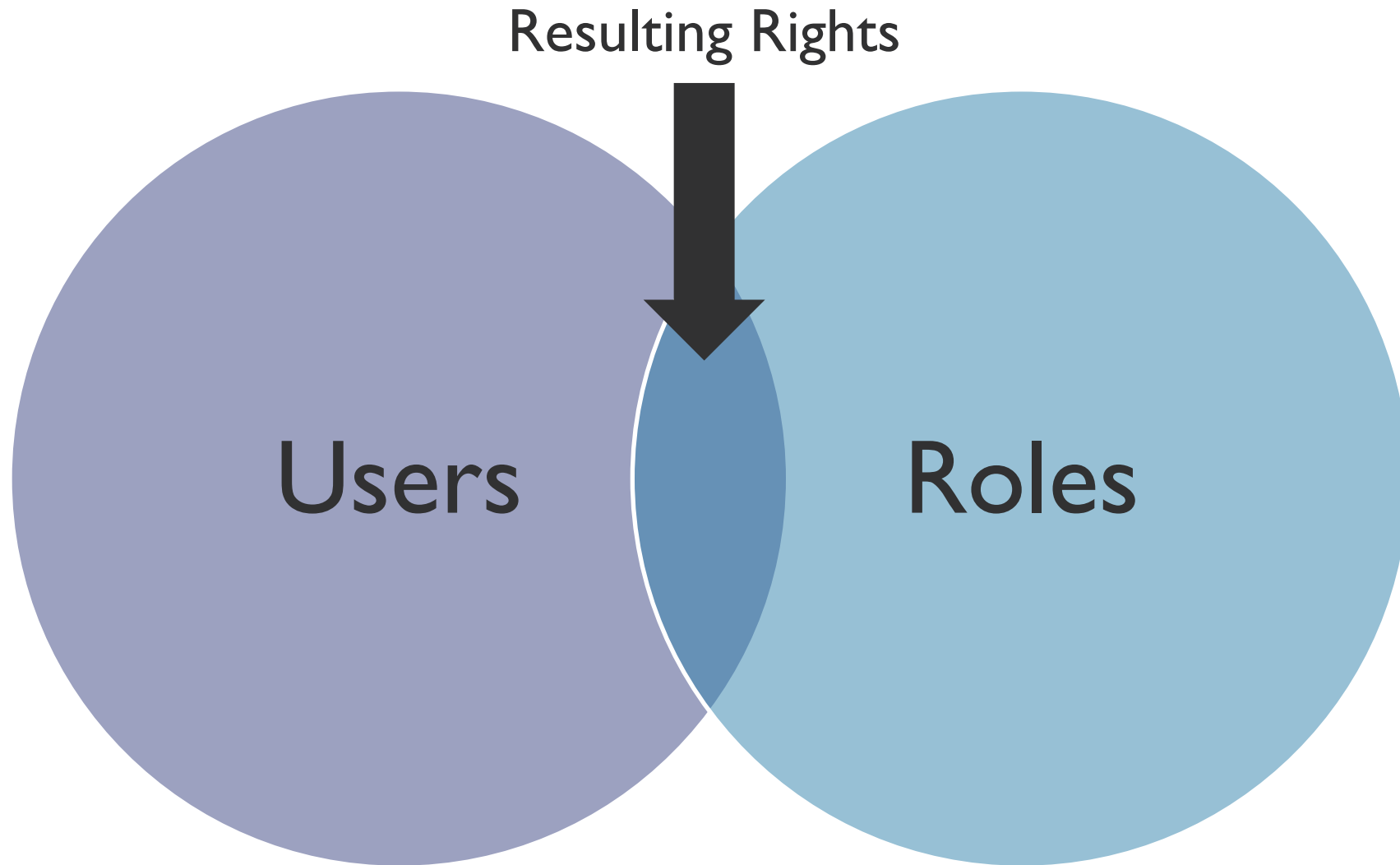
Azure RBAC Built-in Roles (continued)

- Roles include various actions
- Action defines what type of operations you can perform on a given resource type
  - Write enables you to perform PUT, POST, PATCH, and DELETE operations
  - Read enables you to perform GET operations
- Use PowerShell to get latest roles

Get latest roles	Get-AzureRMRoleDefinition

User Rights

RBAC Custom Roles

Create if none of the built-in roles work for you

Each tenant can have to 2000 roles

Use "Actions" and "NotActions"

Assignable scopes:
- Subscriptions
- Resource Groups
- Individual Resources

Azure Policy

SKYLINES
ACADEMY

Azure Policies

Enforce Governance

Built-in or Custom Code

Assigned to Subscriptions or Resource Groups

Create > Assign

Resource Locks

Azure Resource Locks

- Mechanism for locking down resources you want to ensure have an extra layer of protection before they can be deleted

- 2 options available:
  - **CanNotDelete:** Authorized users can read and modify but not delete the resource
  - **ReadOnly:** Authorized users can read the resource but cannot update or delete

Compliance and Security Requirements

SKYLINES
ACADEMY

Shared Responsibility Model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer ■ Cloud Provider

- Security is a joint responsibility

- Cloud computing clearly provides many benefits over on-premises

- As you move from IaaS > PaaS > SaaS you can offload more of the controls to Microsoft

You are always responsible for…

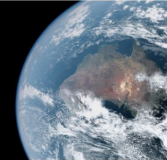| Data | Endpoints | Account | Access Management |

https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91

Microsoft Trust Center

https://servicetrust.microsoft.com/

- In-depth information Access to FedRAMP, ISO, SOC audit reports, data protection white papers, security assessment reports, and more

- Centralized resources around security, compliance, and privacy for all Microsoft Cloud services

- Powerful assessment tools

Compliance Manager

- Manage compliance from a central location

- Proactive risk assessment

- Insights and recommended actions

- Prepare compliance reports for audits
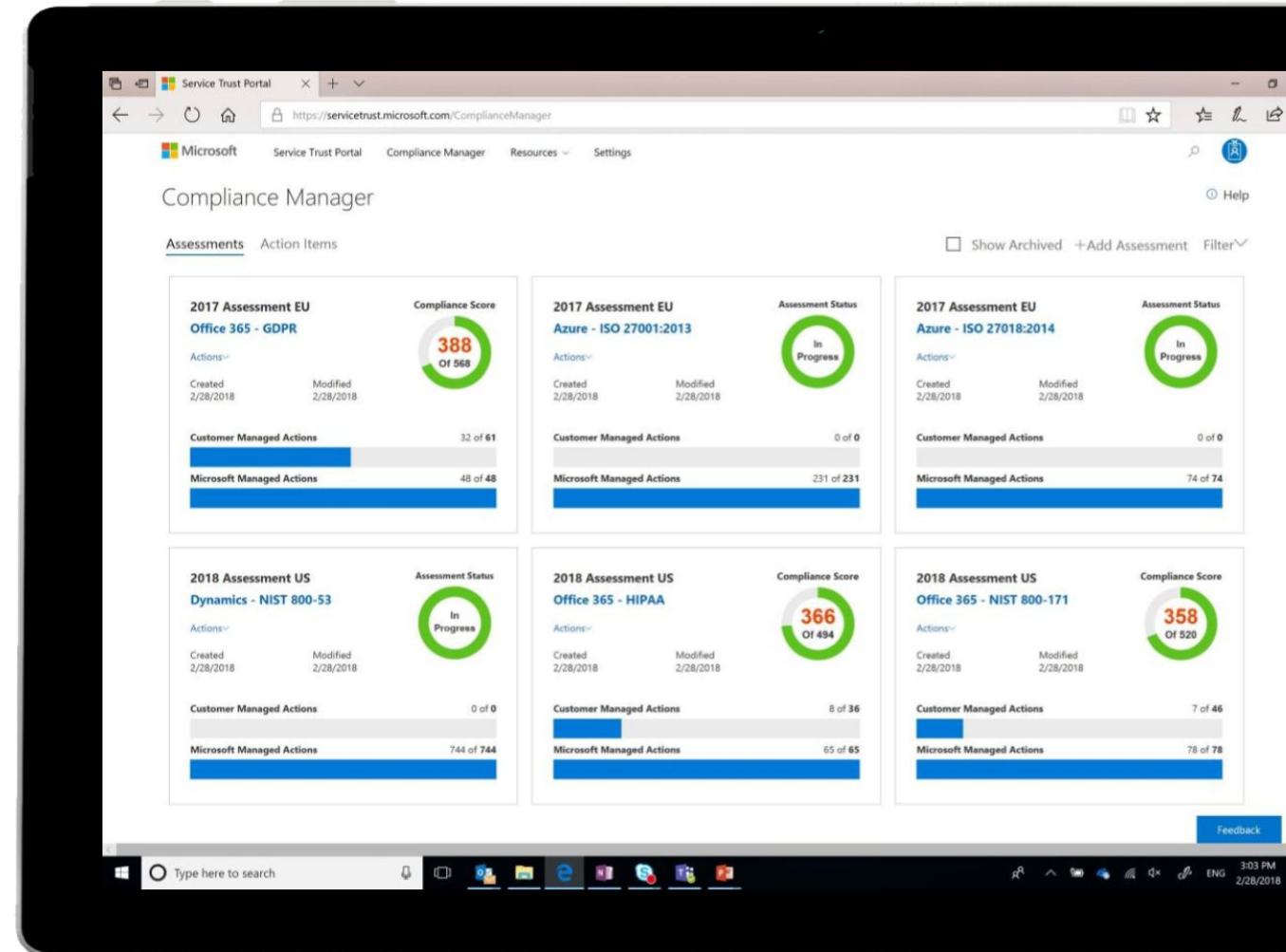
Azure Security Center Overview

Centralized Policy Management

Continuous Security Assessment

Actionable Recommendations

Advanced Cloud Defenses

Prioritized Alerts and Incidents

Integrated Security Solutions

Security Center Pricing Tiers

Free (Azure Resources Only)

- Security assessment
- Security recommendations
- Basic security policy
- Connected partner solutions

Standard

- All features in free tier plus
- Just in time VM access
- Network threat detection
- VM threat detection