AZ-900 Revision Notes

Contents

[Describe Cloud Computing 2](#_Toc148103492)

[What is the shared responsibility model? 2](#_Toc148103493)

[Cloud Models 2](#_Toc148103494)

[Consumption based model 2](#_Toc148103495)

[Cloud Service Types 3](#_Toc148103496)

[Responsibility of cloud service types 3](#_Toc148103497)

[Describe the benefits of using cloud services 3](#_Toc148103498)

[Describe Azure Compute and Networking Services 4](#_Toc148103499)

[Azure Virtual Machines (VM) 4](#_Toc148103500)

[Scaling VMs in Azure 4](#_Toc148103501)

[VMs Use Cases 4](#_Toc148103502)

[VM Resources 4](#_Toc148103503)

[Azure Virtual Desktop 5](#_Toc148103504)

[Describer Azure Containers 5](#_Toc148103505)

[Compare VM with Container 5](#_Toc148103506)

[Azure Container Instances (ACI) 5](#_Toc148103507)

[Azure Kubernates Services (AKS) 5](#_Toc148103508)

[Describe Azure Functions 5](#_Toc148103509)

[Examples 6](#_Toc148103510)

[Describe Application Hosting Options 6](#_Toc148103511)

[Azure App Service 6](#_Toc148103512)

[Azure Dedicated Host 6](#_Toc148103513)

[Azure Virtual Networking 6](#_Toc148103514)

[Azure Express Route 7](#_Toc148103515)

[Azure Storage Services 7](#_Toc148103516)

[Storage Services 7](#_Toc148103517)

[Benefits of Azure Storage 8](#_Toc148103518)

[Blob Storage 8](#_Toc148103519)

[Azure Files 8](#_Toc148103520)

[Azure Queue Storage 8](#_Toc148103521)

[Disk Storage 8](#_Toc148103522)

[Azure Data Migration 8](#_Toc148103523)

[Azure File Movement options 8](#_Toc148103524)

[Security 9](#_Toc148103525)

[Azure Active Directory (AD) 9](#_Toc148103526)

[Azure AD 9](#_Toc148103527)

[Microsoft Entra 9](#_Toc148103528)

[Connecting on-premises AD with Azure AD 9](#_Toc148103529)

[Azure Active Directory 9](#_Toc148103530)

[Azure key Vault 9](#_Toc148103531)

[Azure Authentication Methods 10](#_Toc148103532)

[Single Sign On (SSO) 10](#_Toc148103533)

[Mutli-factor Authentication (MFA) 10](#_Toc148103534)

[Passwordless Authentication 10](#_Toc148103535)

[Azure External Identities 10](#_Toc148103536)

[Azure Conditional Access 11](#_Toc148103537)

[Azure Role Based Access Control (RBAC) 11](#_Toc148103538)

[Zero Trust Model 11](#_Toc148103539)

[Defence in Depth 11](#_Toc148103540)

[Microsoft Defender for Cloud 11](#_Toc148103541)

[MS Sentinel 12](#_Toc148103542)

[Describe Features and Tools for Governance and Compliance 12](#_Toc148103543)

[Azure Blueprints 12](#_Toc148103544)

[Azure policy 12](#_Toc148103545)

[Resource Groups 12](#_Toc148103546)

[Subscriptions 12](#_Toc148103547)

[Resource Locks 13](#_Toc148103548)

[Delete or change a locked resource 13](#_Toc148103549)

[Service Trust Portal 13](#_Toc148103550)

[Features and tools for managing and deploying Azure Resources 13](#_Toc148103551)

[Azure Portal 13](#_Toc148103552)

[Cloud Shell 13](#_Toc148103553)

[Azure ARC 14](#_Toc148103554)

[Azure Resource Manager (ARM) and Azure ARM templates 14](#_Toc148103555)

[Azure Blueprints 14](#_Toc148103556)

[Monitoring Tools 14](#_Toc148103557)

[Azure Advisor 14](#_Toc148103558)

[Azure Service Health 14](#_Toc148103559)

[Azure Monitor 15](#_Toc148103560)

[Azure Log Analytics 15](#_Toc148103561)

[Alert Rules 15](#_Toc148103562)

[Application Insights 15](#_Toc148103563)

[Cost Management in Azure 15](#_Toc148103564)

[Compare pricing and total cost of ownership (TCO) 16](#_Toc148103565)

[Tags 16](#_Toc148103566)

[Azure Advisor 16](#_Toc148103567)

[Regions and Availability Zones 16](#_Toc148103568)

[IoT Services 16](#_Toc148103569)

[AI Services 17](#_Toc148103570)

[Trust Centre 17](#_Toc148103571)

# Describe Cloud Computing

Cloud computing is the delivery of computing services over the internet. This can include Virtual Machine (VM), storage, databases, networking. May also include Internet of Things (IoT), Machine Learning (ML), Artificial Intelligence (AI).

The main benefit is you pay for what you use – cpu/memory/storage, but don’t manage the hardware, security, and infrastructure.

## What is the shared responsibility model?

The customer looks after information and data in the cloud, the accounts and identifies of people, services and devices that connect to the cloud.

The cloud provider looks after the physical data centre, network and hosts.

### Cloud Models

#### Private cloud

Use own hardware, in own datacentre or a 3rd parties. Organisation has complete control and will manage software, hardware and infrastructure as well as licencing, security updates, replacement.

CapEx capital expenditure – upfront cost, less flexible

#### Public cloud

Ideal for variable loads, infrequent use. Rapid application provisioning, scaling and decommissioning. You pay for what is used and management is accessible via internet or a VPN. The organisation doesn’t have complete control of resources and security.

OpEx operational expenditure.

#### Hybrid cloud

Both private and public cloud – mix of resources. Most flexible, organisation determines where applications are run, controls security, compliance and legal requirements.

May use Azure ARC – multi cloud/hybrid cloud management solution

Useful with legacy or systems unsupported by cloud provider

Multi-cloud: use multiple public cloud providers

Azure VM solution: run VMWare workloads in Azure with seamless integration

## Consumption based model

CapEx - one time, upfront expenditure, pays for physical hardware, building, cooling, networking and licences (on-prem infrastructure). Can be restrictive with a need to plan, can’t react to demand

OpEx – spending money on services or products over time – use and pay for what is needed, vms, scalable, stop paying when no-longer required.

Cloud compute is OpEx or pay as you go. Allows for planning and managing costs, running infrastructure more efficiently and scale as needs change.

## Cloud Service Types

IaaS is Infrastructure as a service: a cloud provider is responsible for maintaining hardware, network and physical security, power and connectivity. Customer is responsible for everything else such as OS, configuration, maintenance, network configuration, storage configuration, patching updates, security and backup.

Common scenarios include adding to, or replacing an on-premises datacentre.

PaaS is Planform as a service: everything that IssS does and in addition, the provider maintains the OS, middleware, development tools, business intelligence. They also manage licensing and patching of OS and databases.

Depending on configuration, the provider or customer may be responsible for network settings and connectivity with the Cloud environment, network and application security.

SaaS is Software as a service: is the most complete model. Most aspects are managed by the cloud provider. Essentially the customer rents a fully developed application.

Examples include Office365

### Responsibility of cloud service types

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | On Premises | IaaS | PaaS | SaaS |
| Data | Customer | Customer | Customer | Provider |
| Application |
| Runtime | Provider |
| OS |
| Hardware | Provider |
| Compute |
| Network |
| Storage |

# Describe the benefits of using cloud services

* High availability with Service Level Agreement (SLA). Availability or uptime is measured in %.  
  For example 99.9% is up to 43.2 min/month downtime, 99% is 432 min/month
* Scalability – adjust resources to meet demand ensures you are paying for what you are use.
  + Vertical scaling – increase or decrease resources such as CPU or memory
  + Horizontal scaling – scale deployed resources automatically or manually to meet demand such as by adding more vms or containers
* Reliability – the ability to recover from failures. Multi region resources increaser ability to recover
* Predictability
  + Performance such as auto scaling, load balancing
  + Cost – forecast spend and track resources in real-time
* Security and governance – templates ensure resources meet corporate, regulatory, government requirements. Software patches are automatically applied depending on the operational model. Better equipped to deal with DDos
* Manageability
  + Management of the cloud scale resources, preconfigured templates, monitored resources
  + Management in the cloud how you manage cloud and resources via a web portal, Command Line Interface (CLI), API or PowerShell.

# Describe Azure Compute and Networking Services

## Azure Virtual Machines (VM)

Similar to physical machines where you can customise all the software that runs on the machine. The ideal choice when full control is needed as it can run custom software and hosting configurations. Customer will need to configure, update and maintain the software that runs on the VM. There is no need to buy the physical hardware. Customer can create and provision VM when using configured templates.

### Scaling VMs in Azure

* Run single instance or group of VMs together to provide high availability, scalability, and redundancy. Manage groups of VM with scale sets and availability sets in Azure.
* VM Scale Sets (VMSS) let you create and manage a group of identical load balanced VMs. Azure automates the synchronisation of config and set of routing parameters. It can monitor virtualisation for increasing/decreasing the number of VMs based on demand.
* VM Availability Sets allow for staggering of updates across VMs and have varied power and network connectivity for resilience.
  + Update Domain – allows for a group of machines to be rebooted while the groups remain online
  + Fault Domain – grouping VMs so not all VMs are not using the same physical power and network switch.

### VMs Use Cases

* During development and test phase – rapid provisioning and decommissioning
* Disaster recovery – configure VMs to run datacentre when primary is offline.
* Extending on-prem data centre with demand.
* Migrating to cloud from physical server – create and configure image to host in cloud.

### VM Resources

* User can pick resources associated by VM using SKU (Stock Keeping Unit). Choose appropriate VM with CPU, memory, storage disc (hdd or solid state).
* Choose size for work done

## Azure Virtual Desktop

* A remove desktop system using virtual machines
* Removes need to run full desktop machine
* Secure: all a user needs is a secure network. User doesn’t need company machine to access.
* Accessible through many devices. Device is separate from VM. No data stored on the user’s device.

# Describer Azure Containers

* Contains are virtualization environment. Lightweight, scalable. Can be stopped dynamically
* Can run multiple containers on a single host
* Don’t manage OS on container (VM you do mange OS).
* Kubernates is an example of a container.
* Azure Dedicated host allows for VMs to be on a host without other tenants
* Isolated VM: VM is so big that only one VM can run on a host.

### Compare VM with Container

* VM: admin is control, manages OS, Software, run one OS at one time.
* VM is emulating a physical computer. Slow to restart or to take a snapshot
* Container deployed as unit to container host
* Container only has what it needs, is lightweight, quicker to launch, smaller in size
* Containers virtualise the OS. VM virtualises the hardware
* VM offers complete control.

### Azure Container Instances (ACI)

* ACI are a PaaS.
* Containers are use to create solutions in micro service architecture.
* For example: one container for frontend, another for backend, another for storage. This allows them to be maintained, scaled or updated independently.
* Quick to start and provision

### Azure Kubernates Services (AKS)

* Creates a Virtual Machines Scale set (VMSS)
* Fully managed
* Uses HELM Charts/YAML/GitOps

# Describe Azure Functions

* These are event driven, sever less compute option. Doesn’t require maintaining VMs or a containers.
* If using VM or container, these need to be running to be in use, with Azure Functions, an event watches the function so resources don’t need to be provisioned when there are no event.
* Benefits: no infrastructure management. No need to mange OS and Software. Just deploy code and it runs with high availability.
* Scalable: increase resources on demand without config.
* Pay for what you use – charged for CPU time used
* Performs work in response to event (often by REST request), timer or message from another Azure service.
* Stateless or stateful: stateless behaves as if restarted when done. Stateful (also durable functions) a context is passed to the function to track prior activity.

## Examples

* LogApps: no or low code. Used by ‘citizen developers’. Designer tool is graphical block based designer, has templates and connectors for using well known services.
* Serverless: consumption based, pay for what is used. Event driven, for example when something is written to a storage account.

# Describe Application Hosting Options

## Azure App Service

* Enables you to build and host web apps, background jobs, mobile back ends and RESTful APIs in programming language of choice, without managing infrastructure.
* Offers automatic scaling and high availability
* Supports Windows, Linux. Enables automated deployments from GitHub, Azure DevOps, or any git repo to enable continuous deployment
* Supports multiple languages .NET, .NET Core, Ruby, Java, Node.js, PHP
* Types of AppService: Web, API, WebJobs, Mobile Apps
* App Service handles most of infrastructure decisions such as deployment and management, endpoint security, scaling and load balancing.

## Azure Dedicated Host

* Typically a host may be multi-tenant. If required, client can create their own host with own VM
* A host is a physical server, client can specify a maintenance window

## Azure Virtual Networking

* Azure Virtual networks and virtual subnets enable Azure networks, VM, WebApps, DBs ot communicate with each other on the Internet and On Prem computers
* Considered an extension of on-prem network.
* Supports both public and private endpoints
  + Public has public IP address and accessible from anywhere
  + Private exist in the virtual network and have private IP addresses
  + Network traffic between peered networks is private and travels on the Microsoft Backbone network, never entering the public internet.
* Private network uses IPV4 RFC 1918 IP ranges. 10/8, 172.16/12, 192.168/16  
  Can’t route over internet
* Can choose unique IP range so it doesn’t conflict with on-premises or other networks
* IP ranges, scope to region.
* Can peer with another private network.

## Azure Express Route

* Used to extend on-premises network into MS Cloud over a private connection. Allows connection offices, data centres or other facilities to the MS Cloud
* Connections: from any-to-any (IP VPN) network, point to point Ethernet network or virtual cross-connection through connectivity provider at a co-location facility.
* Features and benefits of Express Route
  + Connection between Azure and On-premises networks
  + Connects to MS Clouse services across all regions in the Geopolitical region
  + Global connectivity to MS Services across al regions with Express Route Global reach.
  + Dynamic route between your network and MS via Border Gateway Protocol (BGP)
  + Built in redundancy
* Express Route enables direct access to Office 365, Dynamics 365, Azure compute (such as Azure VM), Azure Cloud Services (such as Azure Cosmos DB and storage in all regions.
* Data does not travel over public internet. Even with express route, DNS queries, certificate revocation list checking and Azure CDN requests are still sent over the public internet.
* Provides 100Gbps or 10Gbps which supports Active/Active connectivity at scale
* Network Security Group (NSG) limited to subnets and controls and flow of traffic (allow/deny actions).

## Azure Storage Services

Storage Account Redundancy Options

* Locally Redundant Storage (LRS) – replaces data 3 times in a single data centre in a primary region
* Geo-redundant Storage (GRS) 3 copies in each data centre across 2 regions
* Read access geo redundant storage (RA GRS)
* Zone Redundant Storage (ZRS) replicate data synchronously across three Azure availability zones in the primary region. 1 copy each zone.
* Geo-zone Redundant Storage (GZRS)
* Read-access Geo-zone Redundant Storage (RA GZRS)

Recovery Point Objective (RPO) – the time take to write to secondary region. Typically less than 15 minutes, but there is no SLA for replicating data.

### Storage Services

* Azure Blobs – for text and binary data. Also supports for ‘big data’ analytics through Data Lake Storage Gen2
* Azure files – manage file share on cloud, or on premises.
* Azure query – messaging store for reliable messaging between applications
* Azure Desk – block level storage volumes for Azure VM

### Benefits of Azure Storage

* Durable and highly available
* Secure
* Scalable
* Managed – hardware maintenance, update, critical issues are managed
* Accessible – accessible from anywhere in the world. Microsoft provides client libraries for different software development languages

### Blob Storage

Ideal for infrastructure storage with no restrictions of what is stored.

Tiers include

* Hot access – for frequently accessed data such as images for website
* Cold access – infrequently accessed data. Stored for at least 30 days such as invoices for customers
* Archive access – data rarely accessed. Stored for at least 180 days such as long term backups. Data is stored offline, has lowest storage cost, but highest cost to rehydrate and access.

### Azure Files

* Manage file shares in the cloud. Accessibly by Service Message Block (SMB) or Network File System (NFS). Protocols are industry standard. Can be mounted concurrently by cloud or on-premises deployments. Accessible from Windows, MacOS and Linux. SMB Azure File Shares can be cached.

### Azure Queue Storage

* Service for storing large number of messages. Once stored, can be accessed anywhere in the world via authenticated calls using http or https.

### Disk Storage

* Block level storage volumes that can be used by Azure VMs. Conceptually the same as physical disk, but virtualised.

### Azure Data Migration

* Azure Migrate helps migrate from on-premises data centre to Azure. Migrates servers, on-premises infrastructure, SQL, VM Ware.
* DataBox helps move offline data to azure. It is a secure physical unit where data is loaded onto the device and is sent from on-premises to Azure or Azure to on-premises.

### Azure File Movement options

* AzCopy
* Azure Storage Explorer
* Azure File Sync

# Security

## Azure Active Directory (AD)

Used by

* IT Admin to control access to applications and resources.
* App Developers to provide standards based approaches for adding functionality such as enabling the app to work with user’s existing credentials
* Users to manage identity and to take self-service actions
* Online service subscriptions such as staff using Office 365, Azure, MS Dynamics, CRM.

## Azure AD

Provides services such as

* Authentication to verify identity to access applications and resources
* Single sign on
* Application management
* Device management – devices can be registered and managed through tools such as MS Intune. Also allows for device based conditional access.

## Microsoft Entra

Separate to Azure Portal. Includes

* Azure AD
* Verified ID
  + Verified credential issues by organisation. Used to verify ID and is a ‘trust system’
* Permissions management
* Workload identities
* Identify governance
  + Entitlement management, access reviews
  + (Privileged Identify Management) PIM, lifecycle workflows of users

### Connecting on-premises AD with Azure AD

Connect the two using Azure AD Connect ot synchronise user identities and changes of the same. You can use it for SSO, multifactor authentication and self-service password reset.

### Azure Active Directory

Provides managed domain services such as domain join, group policy, lightweight Directory Access Protocol (LDAP) and Kerberos/NTLM authentication.

An Azure AD DS managed domain lets you run legacy apps in the cloud that can’t use modern authentication.

### Azure key Vault

Securely stores secrets, keys, and certificates. Secured, and access controlled, by policy and Role Based Access Control (RBAC).

## Azure Authentication Methods

Authentication is the process of establishing identity of a person, service or device which they are expected to provide a credential.

Azure supports multiple methods including standard passwords, SSO, multifactor authentication (MFA) and password less authentication.

### Single Sign On (SSO)

Enables a user to sign in once and use that credential to access multiple resources and applications from different provides. For this to work, different applications must trust the initial authentication credential. SSO is only as secure as the initial authentication.

### Mutli-factor Authentication (MFA)

Is the process of prompting a user for an extra form or factor of identification. During the sign-in process, MFA protects against a password compromise where a password was compromised, but the second factor wasn’t/.

Examples:

* something the user knows – might be a challenge question
* something the user has – code sent to a phone or device using trusted platform chip
* something the user is – typically biometric such as a face or finger print

Better than single factor authentication (SFA) whereby with SFA, username and password only needs to be known.

### Passwordless Authentication

Password is removed and replaced with something you have, plus something you are or something you know.

Once registered or enrolled, Azure know that it is associated with you. Now that the computer is known, once you provide something you know or are (Pin or finger print) you can be authenticated without a password.

Three passwordless authentication methods that integrate with Azure Active Directory (Azure AD)

* MS Hello for Business – biometric and pin credentials directly tied to user’s PC
* Microsoft authenticator app – on employees phone
* FIDO2 Security Keys (Fast Identity Online) alliance promotes open authentication standards. FIDO2 is the latest standard that incorporates Web Authentication (WebAuthN) standard.  
  FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Uses a hardware device such as USB devices, or Bluetooth or NFC.

### Azure External Identities

* Business to business B2B collaboration – allows external users to sign in using their preferred identity to access Microsoft Apps or applications. Such users are represented as guest in the directory B2B Direct Connect. Establishes a mutual two-way trust with another.
* Azure AD organisation for seamless collaboration. Can access resources through Teams
* Azure AD Business to Customer B2C – use Azure AD B2C for identity management when publishing modern SaaS apps or non-MS Apps to consumers and customers.

### Azure Conditional Access

Conditional Access is a tool that Azure Active Directory uses to allow or deny access to resources based on identity signals – signals include who the user is, where they are and their device.

Users may be challenged for additional authentication depending on where they are. May restrict or block the user based on the ‘signals’.

### Azure Role Based Access Control (RBAC)

Controls that access to resources for a user. Can create groups and permissions (like in AD or an authorisation manager).

### Zero Trust Model

Zero trust is a security model that assumes worst case scenario and protects resources with that expectation.

Traditionally, corporate networks were restricted, protected, and assumed safe. Managed computers could join the network, VPN access controlled, personal devices restricted or blocked.

Zero Trust flips the model. It requires everyone to authenticate and grants access based on authentication rather than location.

### Defence in Depth

|  |  |
| --- | --- |
| Physical Security | 1st line of defence – for instance building access |
| Identity and Access | Access controls to infrastructure and change control |
| Perimeter | DDoS protection |
| Network | Limits communication between resources through segmentation and access controls |
| Compute | Secures access to VMs |
| Application | Helps ensure applications are secure and free from vulnerabilities |
| Data | Controls access to business and customer data. |

### 

### Microsoft Defender for Cloud

* Formally Azure Security Centre
* Secures Azure resources
* Secures hybrid and multi-cloud resources
* Secures on premises machines using Azure ARC and Defender for cloud

MS Defender for Cloud…

* Continuously assess - known security posture, identify and track vulnerabilities
* Secure = harden resources with Azure Security Benchmark
* Defend – detect and resolve threats to resources and services. Get security alerts and advanced threat protection.

### MS Sentinel

* Is a Security Information and Event Management (SIEM) tool
* Is a Security Automation and Response (SOAR) tool
* SIEM – investigate incident, detects security threats
* SOAR – automatically responds to threats
* Uses log analytics workspace, use playbooks to detect and respond, scours security logs, signals
* Works on Azure, On Premises, other clouds, identity, network and SaaS.
* Allows you to automatically get alerts, log incidents, investigate and hunt

# Describe Features and Tools for Governance and Compliance

## Azure Blueprints

There are used to standardise cloud subscriptions or environment deployments. Repeatable settings and policies are applied as new subscriptions are created. For example create a new dev/test environment with security and compliance settings already configured.

## Azure policy

Allows the creation, assignment and management of policies that control or audit resources. Helps resource configuration stay complaint with corporate standards

Azure policy initiative groups several policies together. It contains all the policy definitions to help track compliance state for a larger goal

## Resource Groups

* A resource is added to a resource group when it is created. It can contain resources from multiple regions and different resource types – for instance VM, IP, disc, NiC, etc.
* Can have multiple groups in a subscription
* Use for organising resources for resource management, lifecycle, group things together like a service. They will be commissioned together, managed together, decommissioned together.
* RBAC can be assigned to a resource group. Resources in a group will have group’s RBAC applied
* Policy can be applied for resource group and inherited by resources
* Budget (spend limit) can be applied to resource group and inherited by resources.
* Can add tags (not inherited). Use policy to apply tags to resources.

## Subscriptions

* Subscriptions are linked to, or trusts, an Azure AD tenant. Only one at a time.
* Can use RBAC
* Can apply budgets and policy
* Has a billing model and service limits
* It contains one or more resource groups, these inherit RBAC, budget and policy
* May have different subscriptions for environments (test/prod), billing and limits.

## Resource Locks

These prevent recourses from being deleted or updated even when the person with the right level of access attempts to delete or update it. Resource locks can be applied to individual resources, resource groups or entire subscription.

They are also inherited, meaning all resources in a group can have the resource local applied.

Types or resource lock:

* Delete means authorised users can read and modify a resource, but can’t delete it.
* Read-only means authorised users can read the resource, but can’t delete or modify.

### Delete or change a locked resource

To modify a locked resource, first the lock must be removed. After it is removed, then the resource can be delete or modified. Even owners must first remove the resource lock.

## Service Trust Portal

The Portal provides access to content n, tools and resources about Microsoft Security, Privacy and Compliance Practises. Can be accessed after signing in with MS Cloud Services account.

# Features and tools for managing and deploying Azure Resources

## Azure Portal

* Used to create, configure, and control Azure resources and subscriptions.
* For example
  + Mange settings, policy, backup.
  + Start/stop services
  + Scale resources
  + Track cost, analyse performance, create reports

## Cloud Shell

* Browser based shell allows you to create, configure and manage Azure resources using a shell. Supports Azure PowerShell and Azure Command Line Interface (CLI) which is a Bash shell.
* Azure PowerShell/AZ PowerShell – commands call Azure REST API to perform management tasks in Azure. Azure PowerShell can be installed on Windows, Linux and MacOS.
* AZ CLI – cross platform, useful for Bash users.

## Azure ARC

* Mange resources outside Azure via Azure Portal - such as on-prem or Kubernetes.
* ARC extends Azure compliance and monitoring to hybrid and multi-cloud configurations.
* Azure ARC provides centralised way to
  + Manage entire environment by projecting non-azure resources into Azure Resource Manager (ARM).
  + Manage multi-cloud and hybrid virtual machines, Kubernetes clusters and databases as it they are running in Azure.
  + Use Azure Services and management capabilities regardless of where they live
  + Continue using ITOps while introducing DevOps practices

## Azure Resource Manager (ARM) and Azure ARM templates

* ARM is a deployment and management service for Azure. Provides manages layer to enable you to create, update and delete resources in Azure account.
* ARM Templates allows you to describe infrastructure as lines of code. Using ARM templates you describe resources in declarative JSON format. Deployment code is verified before it is run. The template orchestrates the creation of resources in parallel.
* Store in a git repo and a pipeline can deploy it. An update to template, will update the instance if already provisioned.

## Azure Blueprints

* Collection of Recourse groups, ARM Templates, RBAC, policy.
* Can be versioned and assigned to a subscription.
* Permissions: don’t lock (can modify), don’t delete, read only.

## Monitoring Tools

### Azure Advisor

Evaluates Azure resources and makes recommendations to improve reliability, security and performance, and cost.

### Azure Service Health

Combines three services

* Azure Status – global Azure status such as outages and is a good reference for incidents with wide-spread impact
* Service Health – narrower view of Azure Services and regions. Focuses on Services and regions in use. Authenticated Health experience know what is being used and shows targeted information about outages and maintenance
* Resource Health – info about resources in use. Helps to plan additional resources.

### Azure Monitor

Collects data on resources, analysing that data and visualising the information and even acting on the results. It can monitor Azure resources such as VMs hosted by a different provider.

### Azure Log Analytics

A tool in the Azure Portal where you can write and run log queries on data gathered by Azure Monitor.

### Alert Rules

Creates an alert. Action rules act on alert to call an action. For example to send SMS, Email, call logic app.

### Application Insights

Is an Azure Monitor feature. Monitors web applications and is capable of monitoring applicatons running in Azure, on premises and in different cloud environments. To use, install SDK or Application Insights agent.

Use to monitor

* Request rates, response times, and failure rates
* Dependency rates, response times, and failure rates
* Page views and load performance
* AJAX calls from web pages. Includes rates, response times, and failure rates
* User and service counters
* Performance counters from Windows and Linux server machines such as CPU, memory and network.

# Cost Management in Azure

Azure shifts costs from CapEx of building out and maintaining infrastructure and facilities to an OpEx of relenting infrastructure as you need it.

OpEx cost can be impacted by many factors. Such as

* Resource type: type of resource, its settings and azure region will have an impact on the cost. When an Azure resource is provisioned, a metered instance is created. The meter tracks the usage of the resource and is used to calculate the bill. For VMs for instance, the OS, software, processor and number of cores, attached storage, and network interface can affect costs. For Storage, the region, redundancy, storage type can affect cost.
* Consumption: pay as you go is where you pay for what resources you use in a billing cycle. There is the ability to commit to using a set of resources in advance and get discounts.
* Maintenance - adjust resources based on demand.
* Geography – different regions have different costs such as labour, taxes, power and fees can vary. Network traffic can cost different amounts too. It is less expensive to move data within a region that between regions.
* Network traffic: bandwidth refers to moving data in and out of data centres. Some inbound data transfers will be free, outbound data transfers is based on zones.
* Subscription type: some subscription types also include usage allowance which affects cost. For instance, the free trial subscription includes 30 days of credit and some products that are free for 10 months.
* Azure Marketplace: where you can purchase Azure base solutions from 3rd Party Vendors such as a server with software pre-installed and configured. You pay for Azure resources, as well as the service or expertise of the 3rd Party Vendor who can set up their own billing structures.

## Compare pricing and total cost of ownership (TCO)

* Pricing calculator gives an estimated cost for provisioning a resource in Azure. It is information only.
* TCO calculator is designed to help compare cost of running on premises compared to Azure Cloud. With TCO calculator, you enter current infrastructure configuration costs servers, DBs, storage, outbound network traffic. TCO calculator compares anticipated cost for current environment with an Azure setup supporting the same requirements.

## Tags

Are used to tag resources which can help organise usage and cost. Tags provide metadata about your resources such as resource management, cost management, optimisation, operations management, security, governance and regulatory compliance, workload optimisation and automation.

Example tagging structure could include: app name, cost centre, owner, environment, impact.

These can be managed via PowerShell, Azure CLI, Azure resource manager, REST API or Azure Portal.

## Azure Advisor

Guidance on security, reliability, operational performance, cost.

# Regions and Availability Zones

* Region is defined by latency envelope – a 2ms round trip within a region
* A region may contain several availability zones. Not all regions support availability zones.
* An availability zone is physically isolated from another by power, cooling, network. May be on a single site. No distance guarantee between each AZ. Has 2ms latency.
* A region is geographically and may be geopolitically distinct.
* Use of multiple regions for DR parings will have distance. Second site may be backup (active/active)
* Availability zone is high availability

UK has two regions: UK West (Cardiff) and UK South (London)

# IoT Services

* Azure IoT Hub – register IoT devices. Provides SDK to manage and interact with devices, get telemetry, push firmware, get data.
* Azure IoT central provides dashboards
* Azure Sphere – provides security, secure communication, certificate based authentication.

# AI Services

* Azure Machine Learning – platform making predictions. Total control for data scientists, training and evaluation of models, create an API. User creates data, models, test, ALG -> API.
* Azure Cognitive Services – pre-built models. Don’t have to build and train models.
  + Language – natural language input and understanding
  + Speech – convert speech to test. Translation
  + Vision – recognise visual input
  + Decision
* Azure Bot Service – interacting with people, virtual agents
  + Chat
  + Voice interaction
  + Data in a knowledge base.

# Trust Centre

Purpose of trust centre is to provide Azure compliance documentation. Is a hub for compliance, regulatory, industry and security information.

Includes

* MS Privacy statement (personal data that is collected),
* Online service terms (OST) agreement between MS and the customer
* Data protection addendum – data processing, handling, security.