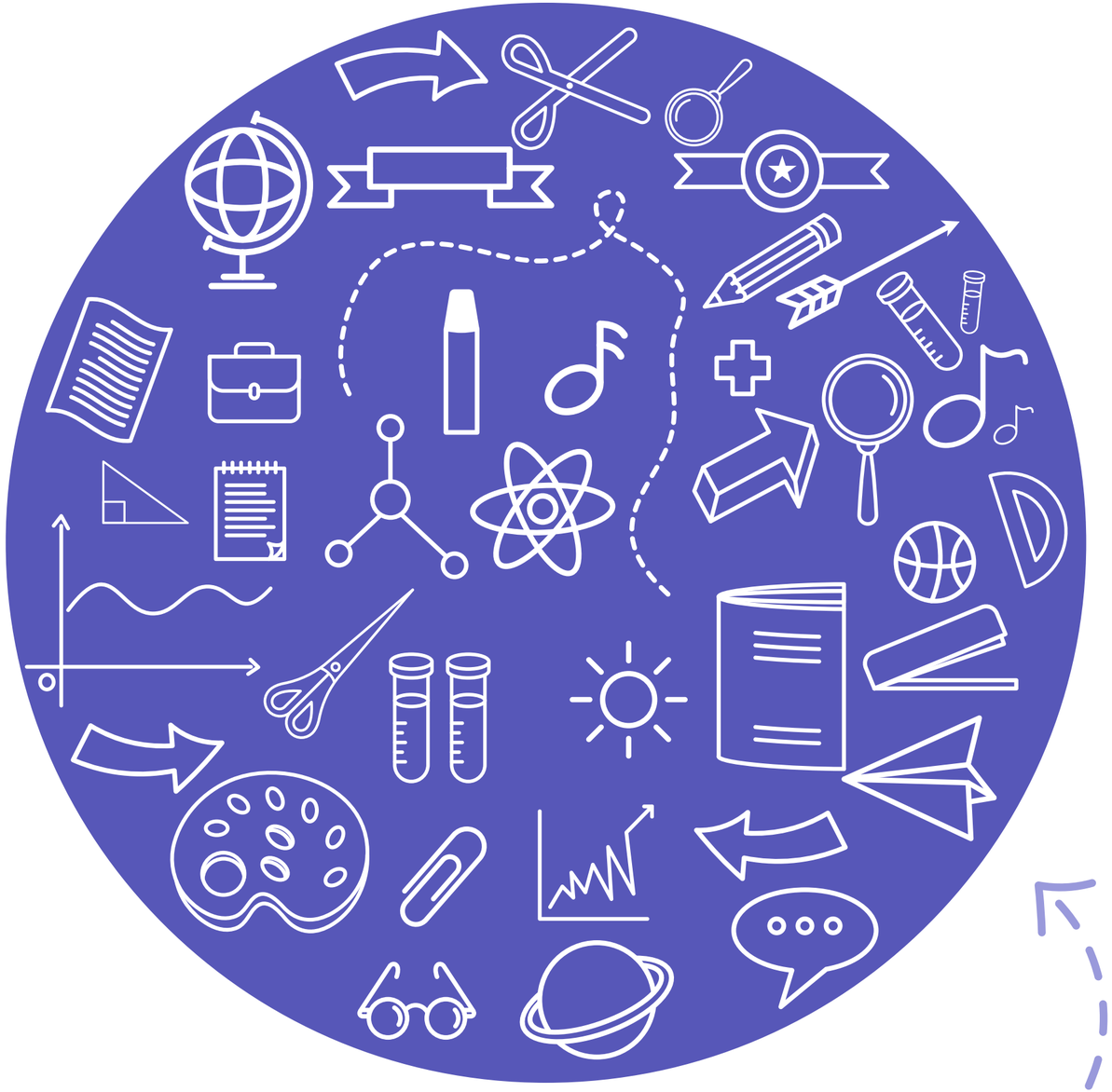
AZ-104 | Microsoft Azure Administrator

Deploy and manage Azure compute

COMPUTE



What is Azure

Microsoft’s cloud platform: compute , storage, networking, databases, AI and more.

Regions

We have datacenters located in different regions across the world. You can decide on the region for your resources.

Build and Deploy

You can build and deploy at scale. You can scale your infrastructure at any point in time.

Cost Benefit

No need of an initial capital investment. The pay-as-you-go model allows you to pay based on usage.

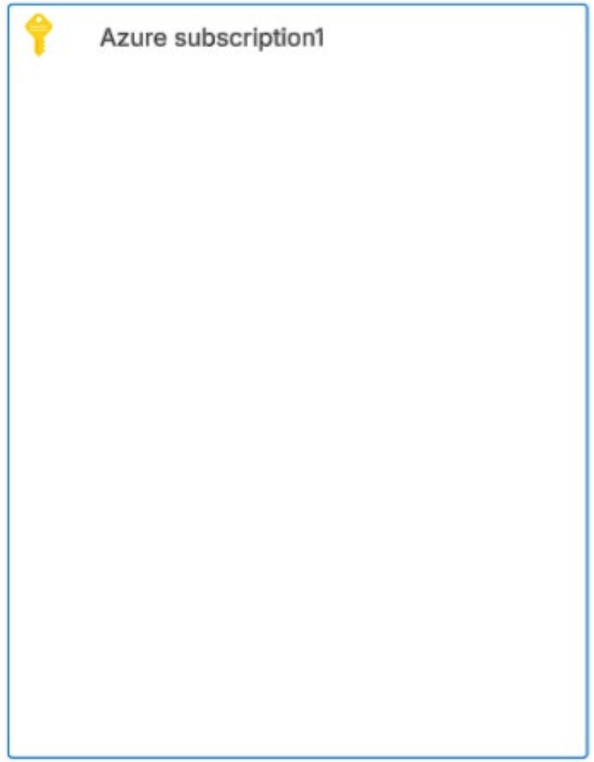
Core benefits

Scalability, Availability, Security and governance.

Azure subscription

Billing and security boundary

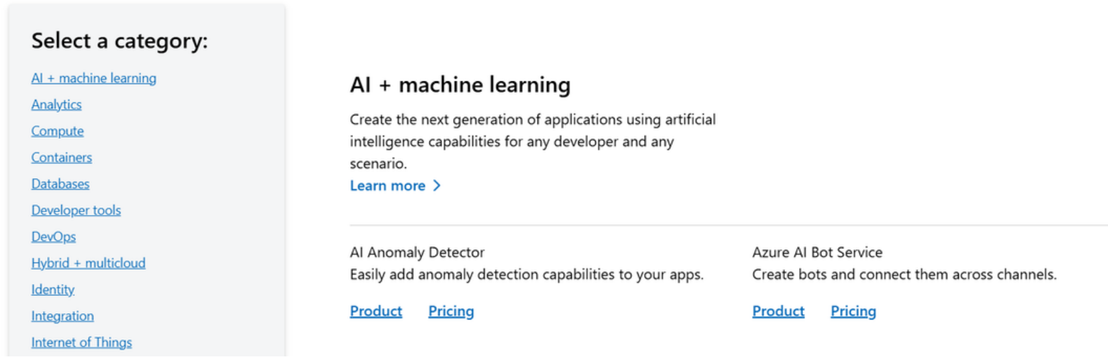
- This is a billing container for your resources.
- You can also apply permissions via RBAC.
- Organizations normally use multiple subscriptions dev/test/prod.
- Every subscription trusts a Microsoft Entra ID tenant.



Azure service

Products

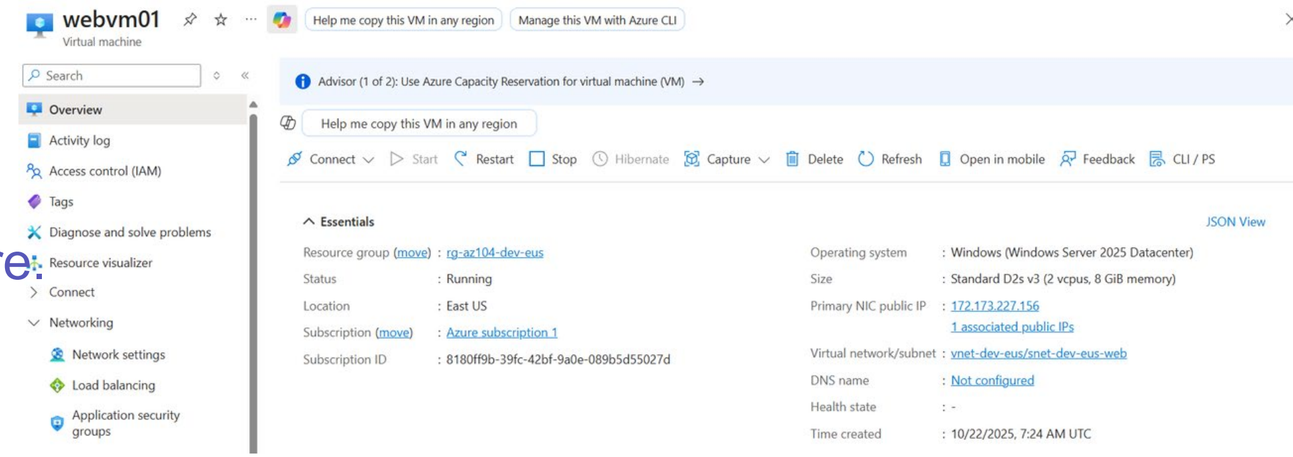
- An Azure service is a product you consume.
- Examples are Azure virtual machines, Azure SQL databases etc.
- Each service provides different SKU’s/tiers.
- You provision resources out of the services.



Azure resource

Item in Azure

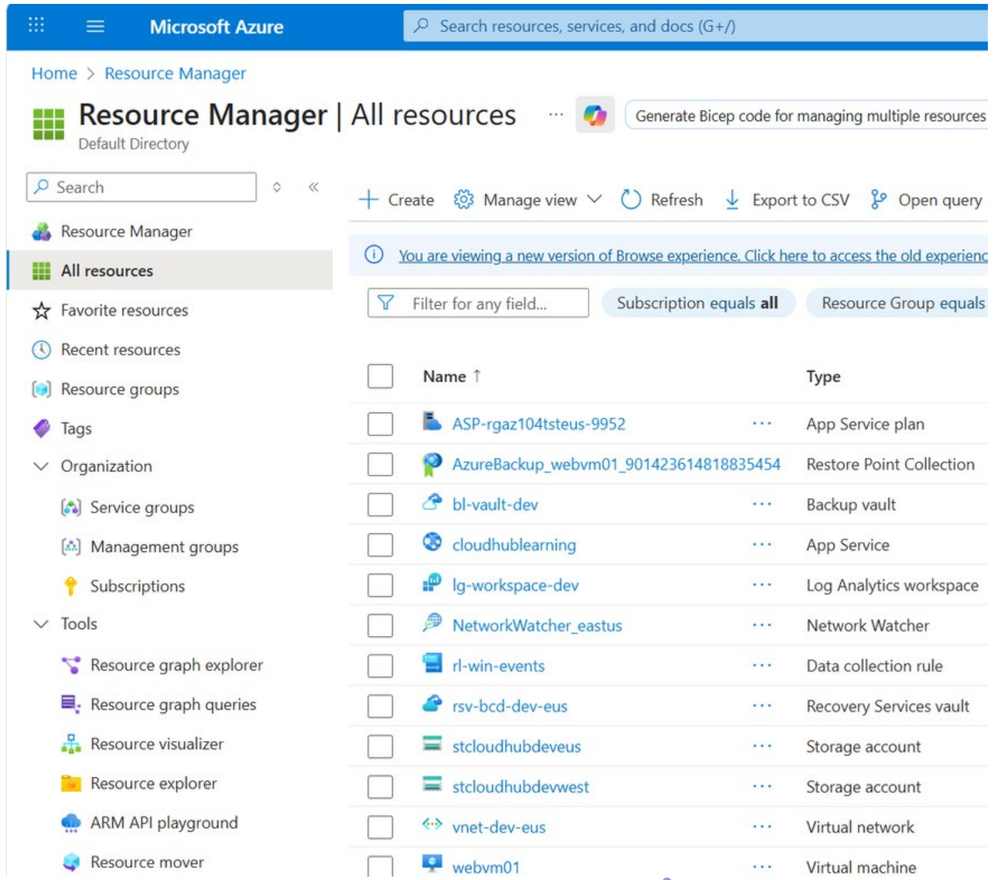
- A resource is an item deployed onto Azure. The resource is based on a service available on Azure.
- Each resource lives inside a resource group.
- Each resource has a resource ID, a location and properties.
- Resources can be governed via RBAC, tags, locks and policies.



Azure portal

Web UI to manage Azure

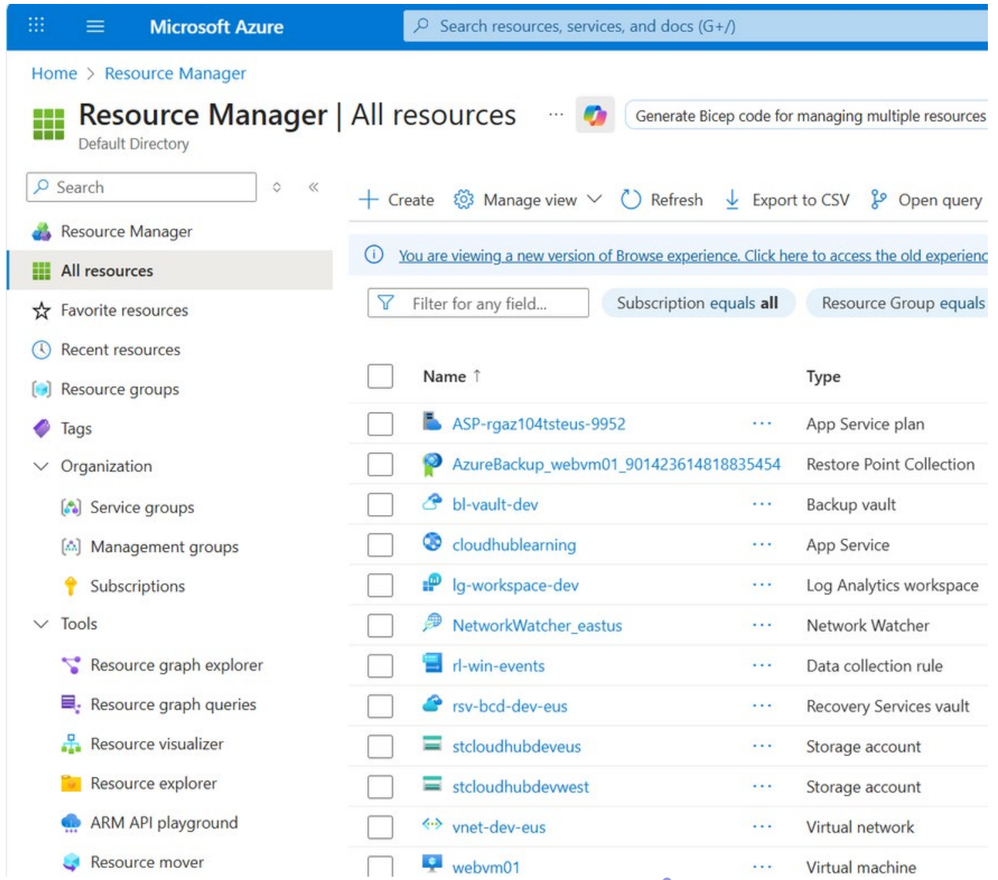
- The Azure Portal allows you to manage resources in Azure.
- You can create, view, update resources.
- It provides a complete UI experience for managing Azure services.



Azure resource group

Logical container for resources

- This is a logical container that holds resources that you want to manage together.
- The resource group can hold resources like virtual machines, disks, SQL databases etc.
- You can apply governance aspects like RBAC, tags and locks onto resource groups.



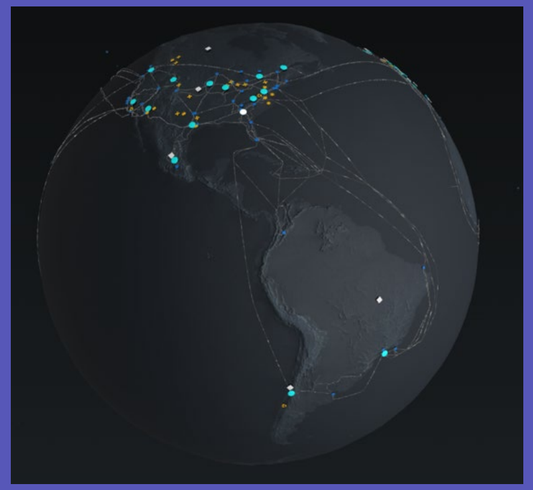
Virtual Machines

- These are on-demand servers in Azure (IaaS- Infrastructure as a service).
- For each machine you decide on the operating system, the size (vCPU/RAM), disks , networking etc.
- Here you pay per second/minute for the compute and disks.
- You can also place the machines in Availability sets of Availability zones for higher infrastructure availability.

Marketplace templates

- When building the virtual machine , we can make use of images in the Azure marketplace.
- The common images for virtual machines - Windows Server 2025, Ubuntu 24.04 LTS.
- There are images that also have pre-hardened application images.

Azure regions



- A specific Azure geography (e.g., East US) with one or more datacenters.
- You choose a region per resource for latency, compliance, pricing.
- Regions also comprise of Availability zones. You can increase the overall redundancy of your infrastructure by spreading the virtual machines across Availability zones.

OS Disk

The operating system disk

NSG

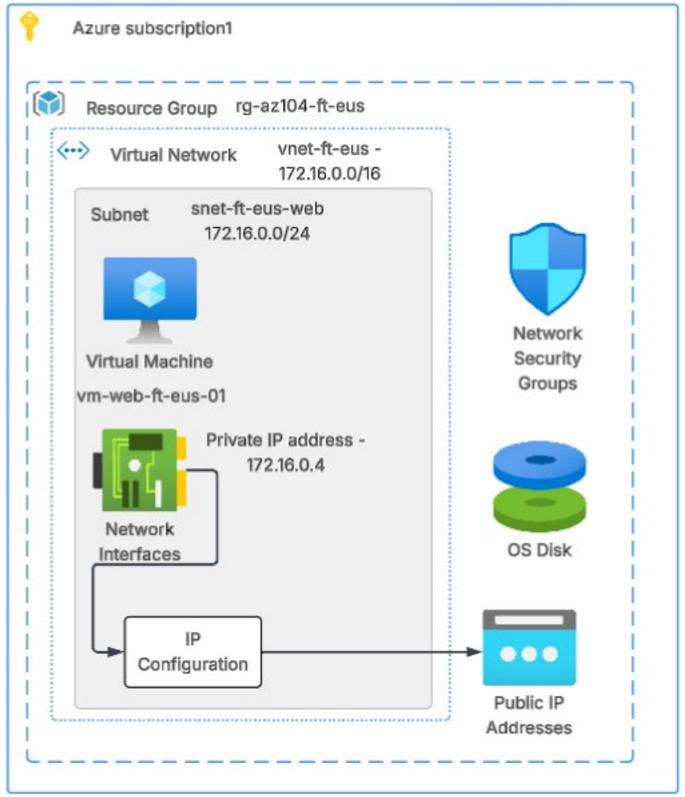
Rules that allow/deny traffic

Virtual Network

This is the private network space for the virtual machines.

Private IP

This is the internal address for the virtual machine inside the VNet



Network Interface

This is the VM's network card that is bound to the subnet.

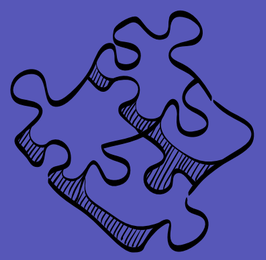
Public IP

This is an IP address that allows Internet resources to interact with the VM.

Building virtual machines

Azure Disk Encryption

- Azure Disk Encryption encrypts the disks inside the VM—BitLocker on Windows and DM-Crypt on Linux.
- The VM uses a data-encryption key (DEK) to encrypt volumes, and a key in Azure Key Vault.
- Azure Disk Encryption can target the OS Disk, then data disks or both.



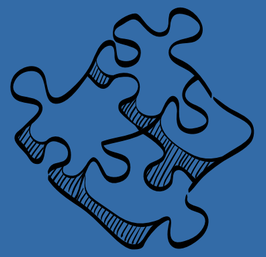
Availability Sets

Goal: Virtual Machines survive rack/ power/ switch failures & planned host updates.

- An Availability Set keeps two or more VMs apart on different fault domains (different racks/power/network) and update domains (host patching).
- If one rack fails or one update domain reboots, at least one VM stays up.
- With two+ VMs in the same availability set, Azure advertises a 99.95% VM SLA.
- You can have a maximum of 3 fault domains and 20 update domains.
- There is no extra cost for the Availability set, you only pay for the virtual machines.

Fault Domain (FD): group sharing power & network; separate VMs to avoid a single rack failure

Update Domain (UD): group that reboots together during planned host updates; only one UD updated at a time


Availability Zones

Goal : Protect against data center level failures.

- Physically separate datacenters inside a region (Zone 1/ 2/ 3).
- Protects from datacenter-level failures (power, cooling, network).
- With two or more VMs across zones, Microsoft advertises 99.99% VM connectivity SLA.
- The zone needs to be assigned to the machine at creation time.
- There is no extra cost for the Availability zone, but there is a data transfer charge across zones.

Virtual Machine Scale Set

- A Virtual Machine Scale Set lets you manage a fleet of VMs as a single unit.
- You set the model (image/size/network), and the set can autoscale based on load.
- Scales out/in automatically on metrics (CPU, requests, queue length).

Virtual Machine Scale Set Orchestration Modes

Uniform

Identical instances; scale set API manages instances.

Supports LB health probe or App Health extension for health.

Great for stateless workloads, simple autoscale, lower variance

Flexible

Manage instances more like regular VMs; mixed sizes/spot/regular possible.

Better for mixed roles, custom availability needs

Azure Web Apps

- Azure Web Apps—part of App Service—is Microsoft's Platform as a Service (PaaS) for hosting web sites and APIs without managing servers.

- You pick a runtime—.NET, Node.js, Python, Java, PHP—or bring your own container, and Azure handles the OS patching, platform updates, and the underlying VM fleet.

- You get first-class features out of the box: custom domains and free TLS, built-in diagnostics and metrics, deployment slots for zero-downtime releases, backups (from supported plan tiers), and authentication integration with Microsoft Entra ID and social providers.

Azure App Service Plans

The App Service Plan is the compute SKU —cores, memory, features, and price

Free/Shared (F1/D1)

Dev/test only; limited CPU; no SLA; no custom SSL; no slots.

Basic (B)

Dedicated VMs, manual scale; limited features; typically no deployment slots/backups.

Standard (S)

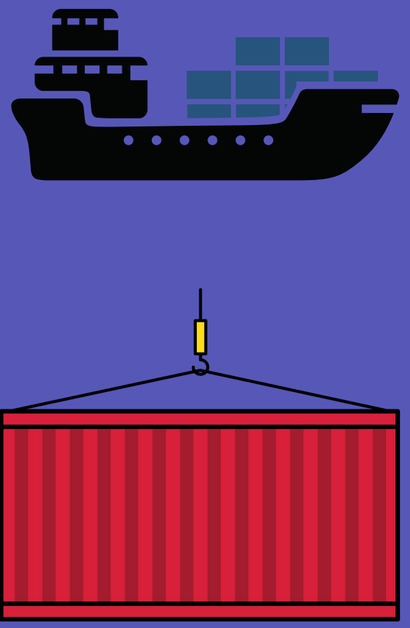
Production entry; autoscale, deployment slots (~5), daily backups, staging; VNet integration (outbound).

Premium v3

Faster compute, more instances, more slots (~20), zone-redundant options, better scale, Private Endpoint for inbound

Azure Web Apps - Custom domain

- Azure Web Apps – The App service plan needs to be a paid one.
- Verify ownership: In App Service → Custom domains → Add → copy the TXT record and create it at your DNS provider.
- Back in Custom domains, Add hostname (it validates the TXT/ CNAME/ A record and attaches it to the app).
- Create/ assign TLS—use App Service Managed Certificate or use your own certificate.



Containers

- Containers package an app and its dependencies into an immutable image that runs as a lightweight, isolated process sharing the host kernel—faster to start and denser than VMs..
- They deliver consistency from dev to prod, portability across environments, and speed for rolling updates and autoscale.
- On Azure, run containers in App Service for Containers, Azure Container Instances, or Container Apps.

Azure Container services

App Service for Containers

Host a single containerized web/API with PaaS conveniences like TLS, slots, and backups

Azure Container Instances

Run a single container or a small group for jobs and quick services —no cluster, pay per second

Azure Container Apps

Serverless microservices with scale to zero, event - driven autoscaling (KEDA), and revisions for blue/green — without running Kubernetes yourself

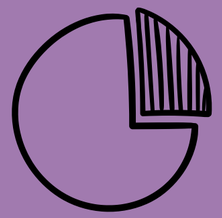
Azure Kubernetes

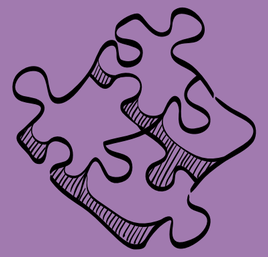
when you do need full Kubernetes control, custom operators, and advanced networking —powerful, but operationally heavier.

Azure Container Instances

Goal: Start simple

- Run containers without managing VMs or Kubernetes.
- Azure Container Instances can use the Docker images stored in Docker Hub or the Azure Container Registry.
- It supports Linux and Windows containers, can expose a public IP for quick APIs, or run privately inside a VNet for internal services.
- Azure File shares can be used for shared state.
- Serverless (no cluster), per-second billing.

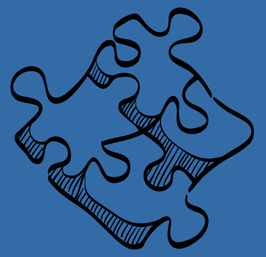




Azure Container Registry

Goal : Private Container Registry

- Azure Container Registry is the private place to store, secure, and replicate container images close to your compute.
- Choose Basic for dev, Standard for most teams, or Premium when you need geo-replication, private endpoints, and higher throughput.
- Azure service like Azure Container Instances, Azure Container Apps, Azure Kubernetes can pull the images from the registry.
- ACR Tasks: build on Git commits, run scheduled builds, and even trigger rebuilds when a base image updates.



Azure Container Apps

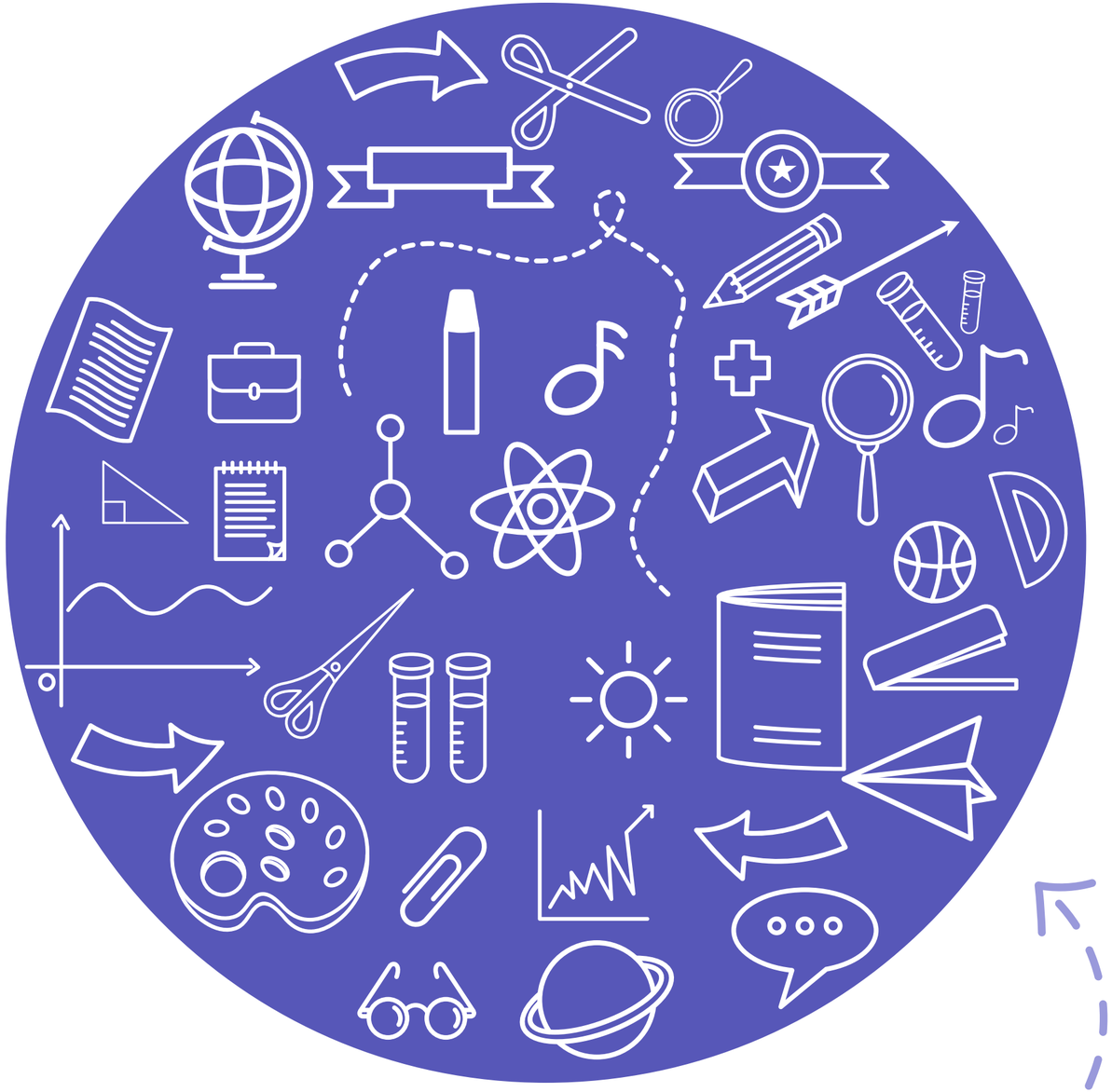
Goal : Serverless Microservices

- Azure Container Apps is a serverless platform for microservices—you get many Kubernetes-like powers without running a cluster.
- You deploy a container image (often from ACR), choose external or internal ingress, and ACA handles autoscale—including scale to zero.
- Every deploy creates a revision; you can direct a percentage of traffic to a new revision for canary tests, then promote to 100%—or roll back instantly by shifting traffic back.
- Currently supports any Linux-based x86-64 (linux/amd64) container image.

AZ-104 | Microsoft Azure Administrator

Configure and manage virtual networking

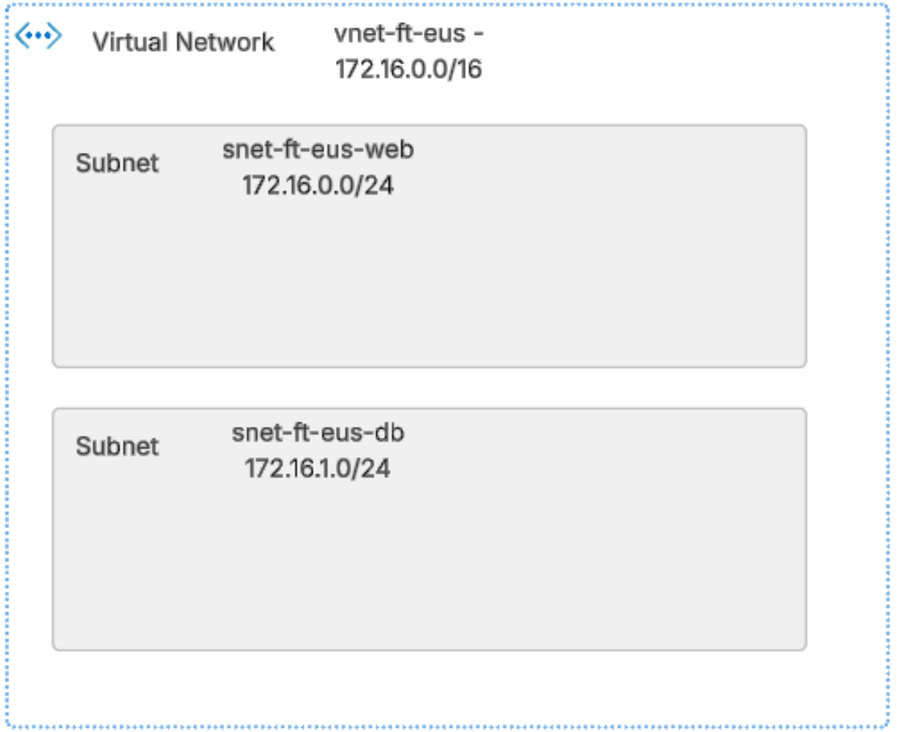
NETWORKING



Azure Virtual Networks

Networking

- An Azure VNet is your private network in the cloud isolated, software-defined, and fully customizable.
- It provides addressing, subnets, routing, and security (NSGs/UDRs) for your workloads.
- Connect VNets (peering) and connect to on-prem (VPN/ExpressRoute.
- Use Private Endpoints for private access to PaaS and NAT Gateway for scalable outbound connectivity.



IP address spaces

- Devices on a network are normally associated with an IP address.
- This allows to identify the device on the network.
- Devices talk to each other by first establishing a connection via their IP addresses.
- With Azure virtual machines, they also receive a Private IP address based on the IP address space assigned to the subnet they are located in..

IP address spaces

- A VNet's address space is defined in CIDR e.g 10.0.0.0/16.
- Classless Inter-Domain Routing (CIDR) is the notation that is normally used to define IP address ranges.
- With an example of 10.0.0.0/16, the first 16 bits of 10.0 represent the network address and the remaining 16 bits can be used to assign to the resources in the network.
- RFC1918 private ranges
  - 10.0.0.0/8 (10.0.0.0 – 10.255.255.255)
  - 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
  - 192.168.0.0/16 (192.168.0.0 – 192.168.255.255)

What are subnets

Partition a VNet into smaller segments for isolation, security, and routing control

Isolation

Subnets divide a VNet for isolation and policy control.

Address prefix

Each subnet has its own address prefix, this is a subset of the address prefix of the virtual network.

Azure reserves 5 IPs per subnet

Security

You can apply Network Security Groups to subnets to control the inbound and outbound traffic flow.

Delegation

Subnets can be delegated to PaaS services (e.g., Azure Container Apps, App Service Environment v3) enabling those services to manage NICs in that subnet.

Private vs Public IP Addresses

IP addresses assigned to resources in your virtual network

Private IPs are routable inside the virtual network.

They are assigned to the NICs in a subnet.

Allocation can be dynamic (DHCP-like from the subnet) or static (you choose an IP from the subnet range, excluding reserved addresses).

Public IPs provide Internet reachability.

They can be assigned to the NIC.

They live as a seperate resource.

Allocation: Public = Static (Standard); Private = Static or Dynamic

Version: IPv4, IPv6 (or both)

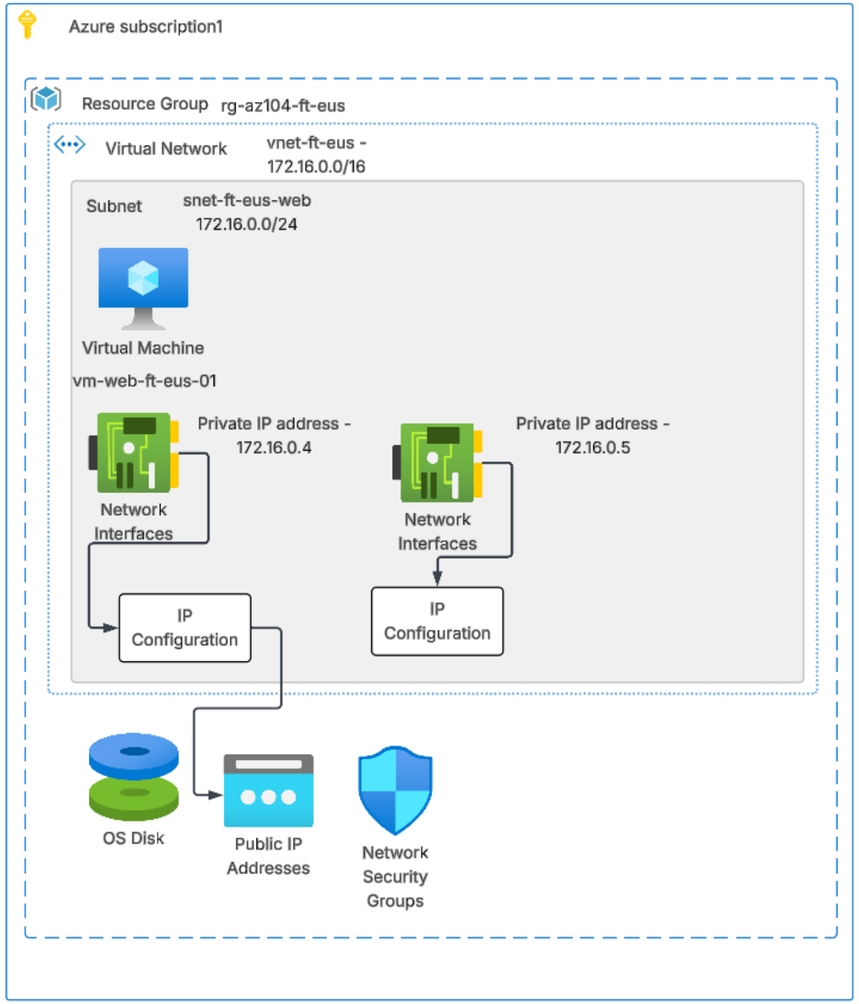
Zone: Zonal / Zone-redundant (Standard only).

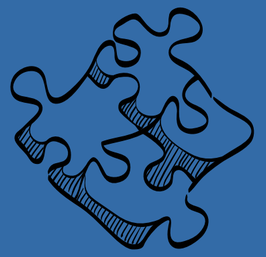
Public IP's are assigned per region.

Azure Virtual Networks

Networking

- If you need to deploy a virtual machine to a virtual network, they need to be in the same region.
- You can slice the virtual network into multiple subnets.
- You can create multiple Network Interfaces and attach it to the virtual machine.
- If you need a Network interface to have a private IP address from a range, deploy the interface in the relevant subnet.





Network Security Groups

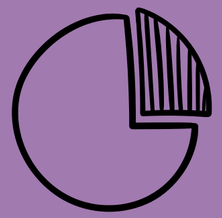
Goal : Filter traffic

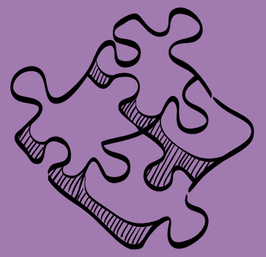
- An NSG is a stateful firewall for Azure VNets that allows or denies traffic using rules defined by source/ destination, port, and protocol.
- You attach NSGs to subnets and/ or NICs; traffic must be allowed at every attached scope.
- Rules are evaluated by priority (100–4096), first-match wins. Use NSGs to implement least-privilege network access around your workloads.
- Every NSG ships with default rules: AllowVNetInBound, AllowAzureLoadBalancerInBound, and DenyAllInBound; and outbound equivalents (AllowVNet, AllowInternet, DenyAll). You can’t delete defaults.

Network Security Groups

Goal : Filter traffic

- Service tags (e.g., Internet, Storage, AzureLoadBalancer) replace huge IP lists with a single token.
- Application Security Groups (ASGs) let you write rules like “web → app” without managing IPs, scaling cleanly across many NICs.
- Combine tags and ASGs for readable, reusable policies.
- Three-tier:
  - allow Internet → web :80/ :443
  - web → app :8080
  - app → db :1433
  - deny the rest





Virtual Network Peering

Goal : Connecting virtual networks

- VNet peering privately connects two Azure VNets over Microsoft's backbone—no VPN gateways or public Internet hops.
- It delivers low-latency, high-bandwidth connectivity while each VNet keeps its own NSGs and route tables.
- Use VNet peering within a region and Global VNet peering across regions.
- Peered VNets must have non-overlapping CIDR ranges. Peering can span subscriptions and tenants but is not transitive.

Azure Bastion

Goal: Connect to virtual machines securely and privately.

- Azure Bastion is a managed jump-host that provides RDP/SSH over TLS 443 directly to VMs' private IPs—no public IPs.
- Sessions can run in the browser or through the native client. This dramatically reduces exposure while keeping remote admin simple.
- Deploy Bastion into a dedicated AzureBastionSubnet. Subnet size must be /26 or larger. The subnet must be in the same virtual network and resource group as the bastion host. The subnet can't contain other resource.
- One Bastion in a hub VNet can serve peered spokes—you don't need a Bastion per VNet.

Azure Network Watcher

Azure Network Watcher is Azure's toolbox for monitoring and diagnosing IaaS networking.

Connection troubleshoot

Runs an on-demand source→destination test and pinpoints the failure stage (DNS, route, NSG/Firewall, port). Shows whether the issue is due to platform or user config

Connection Monitor

Continuously monitors reachability, latency, and loss between monitored sources and endpoints. Supports Azure and non-Azure machines (via agent/extension). Triggers alerts when health degrades.

IP Flow Verify

Simulates a single packet to or from a VM and tells you Allow/Deny with the exact NSG/admin rule responsible. Evaluates effective rules at NIC+subnet

Next Hop

Reveals the route and next hop a VM will use to reach a destination (Internet, VNet, NVA, VPN/ER). Instantly surfaces bad UDRs and blackholes.

Azure Network Watcher

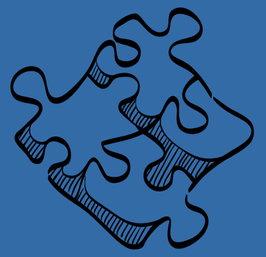
Azure Network Watcher is Azure’s toolbox for monitoring and diagnosing IaaS networking.

NSG Diagnostic

End-to-end rule path analysis for a flow: which NSGs are traversed, which rule matched on each, and the final decision.

NSG Flow Logs

Logs allow/deny decisions per NSG into a Storage account, updated every few minutes. Feed the data to analytics or SIEM for anomaly detection and rule tuning



Azure Load Balancer

Goal : Distribute traffic

- Azure Load Balancer (Standard) is a layer-4 balancer for TCP/ UDP with public and internal modes.
- Standard SKU brings Availability Zone support, larger scale, and advanced features like outbound rules and NAT rule V2, and it’s the recommended SKU for production.
- Use health probes to keep only healthy instances in rotation, and attach frontends (public IPs or private IPs) to distribute traffic to backend pools.

Azure Load Balancer

Inbound NAT Rules

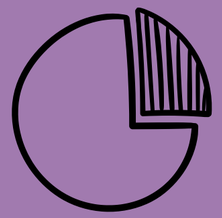
Inbound NAT rules forward a specific LB frontend IP:port to one or more backend instances on a defined port (e.g., 50001→3389).

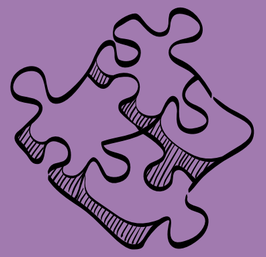
They're ideal for per-VM RDP/SSH access behind a public LB without giving each VM a public IP. Use NAT rules for targeted management

Outbound Connectivity

Outbound rules on a Public Standard LB give you explicit, scalable SNAT so VMs egress to the Internet using the LB's public IP(s).

This simplifies allowlists and avoids scattering public IPs across VMs





Azure DNS and Private DNS

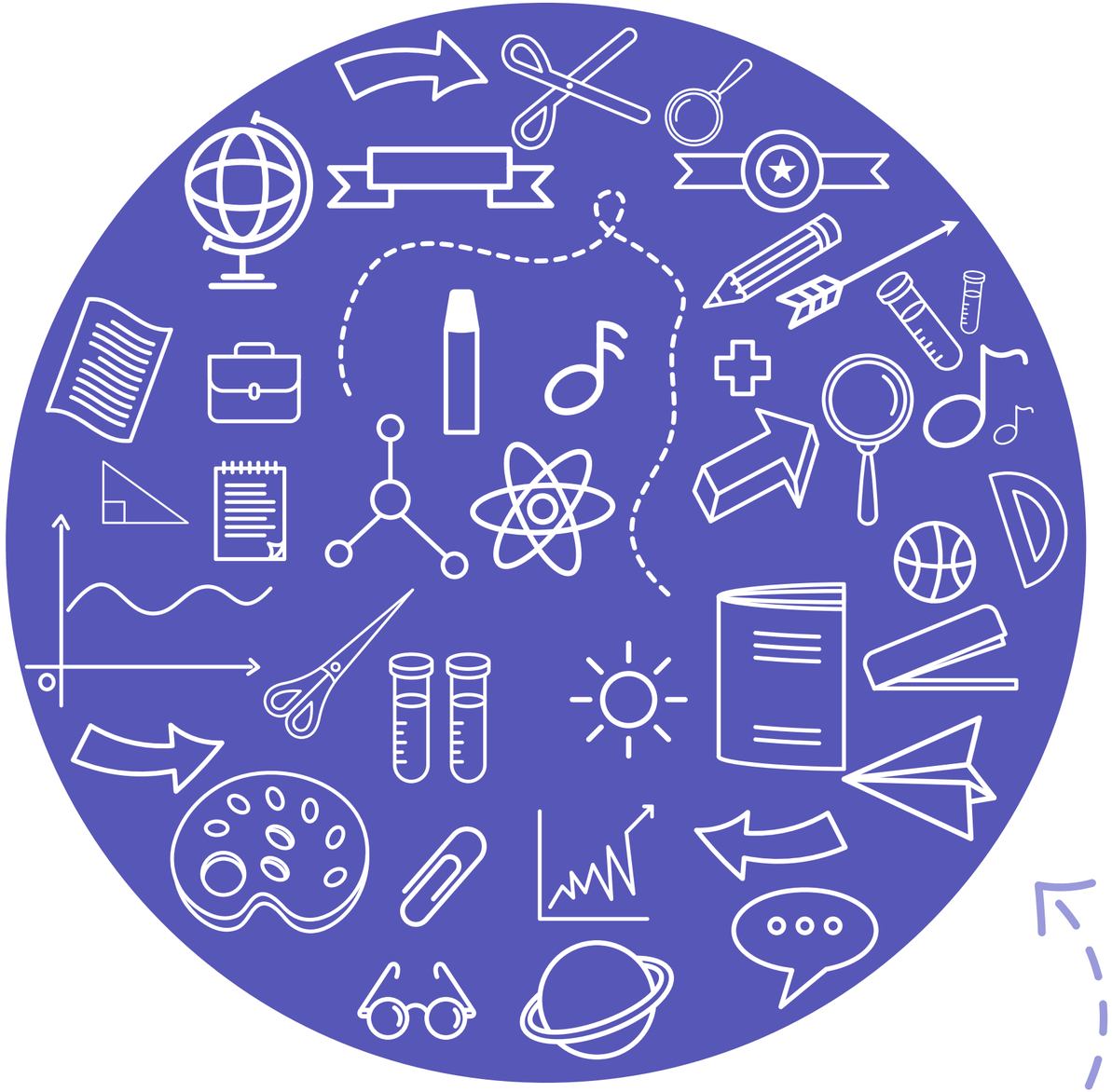
Goal : Domain Names

- Azure DNS hosts public DNS zones on Microsoft's name servers so the Internet can find your apps. You still register the domain with a registrar and delegate it to Azure by updating NS records.
- Azure Private DNS provides private name resolution inside your VNets using private DNS zones. Records in these zones aren't internet-resolvable.
- **VNet Links & Auto-Registration** - Link VNets to a private zone to enable resolution; mark a link as registration-enabled to automatically create and maintain A records for VMs in that VNet .

AZ-104 | Microsoft Azure Administrator

Implement and manage storage

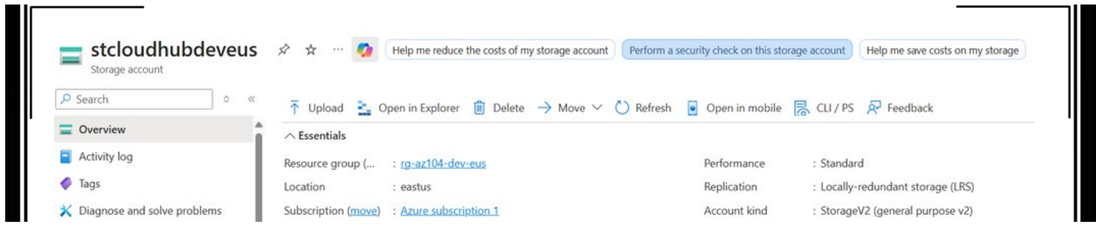
STORAGE

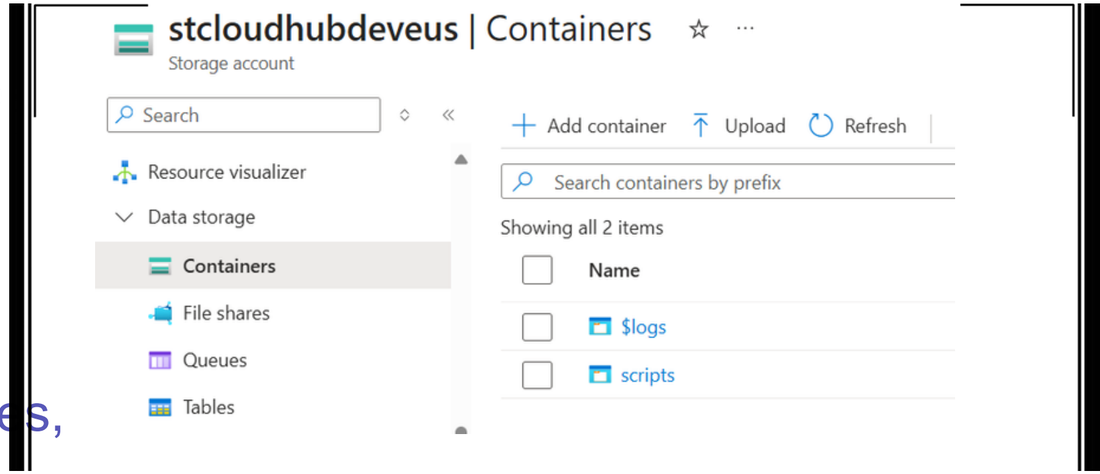


Storage Accounts

Storage

- Azure Storage accounts provide a secure, scalable container for Blob, Files, Queues, and Tables with centralized policies for encryption, networking, and redundancy.
- Use them for app assets, backups, logs, user profiles, and data lakes.
- Choose Standard vs Premium based on latency and throughput needs.





Storage Account types

StorageV2 (GPv2, Standard)

The default for most workloads; supports all four services, blob tiers (Hot/Cool/Cold/Archive), lifecycle management, immutability.

BlockBlobStorage (Premium)

Low-latency object storage for block blobs only; ideal for high-throughput ingestion, media, logs, and artifact stores needing fast commits

FileStorage (Premium)

Low-latency Azure Files with provisioned capacity → predictable IOPS/throughput

Data Lake Storage Gen2

Blob with Hierarchical Namespace turned on. You get directories, file semantics, and POSIX-like ACLs—perfect for analytics pipelines (Spark, Fabric) where folder paths and fine-grained permissions matter

General Purpose V2 storage

The App Service Plan is the compute SKU —cores, memory, features, and price

Blob storage

Blob is Azure’s object store for unstructured data —anything from images, backups, logs, videos, to big analytics datasets.

Azure File shares

Azure Files provides fully managed file shares accessible over SMB and NFS, making it a natural replacement for on - prem file servers. Mount shares directly to Windows, Linux, and macOS.

Queue Storage

Queue Storage is a simple, durable message queue for decoupling producers and consumers

Table Storage

Table Storage is a schemaless NoSQL store for key –value entities —cheap, massively scalable, and ideal for metadata, settings, and simple lookups

Access to Storage

- When you give someone access to an Azure Storage account, you’re choosing how they authenticate and how much power they get.
- Access Keys = the “master keys” to the entire account (all services). Powerful, simple, high risk if leaked.
- SAS (Shared Access Signature) = time-boxed, scope-limited tokens derived from a key or an identity. Designed for least privilege and safe sharing.
- Prefer Microsoft Entra ID + Role-based access control for applications. Use SAS for temporary, delegated access. Keep Access Keys off-limits except for narrow cases.

Access to Storage

- Stored Access Policies (SAPs) let you centrally control SAS permissions and expiry at different levels such as the container level.
- You can later revoke or shorten access by editing/deleting the policy without rotating account keys.
- You can define up to five stored access policies per container.
- If a container-level immutability policy (time -based retention or legal hold) is in effect, the data is WORM (write once, read many): no overwrite or delete is allowed.

Access tiers

What

Access tiers let you trade off storage cost vs. access/ transaction cost and latency for standard (GPv2 / Blob) accounts. You can set a default tier at the account , and you can set/ change the tier per blob at any time

Types

Online tiers are Hot, Cool, Cold; Archive is offline (must be rehydrated before read). Archive also has rehydration priority: Standard (hours) or High (often <1 hour for small objects).

Access tiers

Goal : Save on storage costs.

- **Hot**: Highest storage price, lowest access & transaction cost, lowest latency. Choose for frequently read/ updated data (web assets, active logs, app data).
- **Cool** : Lower storage price, higher read/ operation cost. Good for infrequent access (recent backups, warm archives). 30-day minimum: delete/ overwrite/ move earlier ⇒ early-deletion charge
- **Cold** : Lower storage price than Cool, but higher retrieval/ transaction cost. Good for data you rarely touch but still need online. 90-day minimum with early-deletion charge if violated.
- **Archive** (offline): Lowest storage price, must rehydrate to Hot/ Cool/ Cold before read/ write. 180-day minimum.

Data Redundancy

Why

Azure Storage keeps multiple copies of your data to survive hardware, zonal, or even regional failures.

Choice

You choose where the extra copies live and how they're replicated:

- Within one datacenter
- Across zones in a region
- Across regions

Redundancy options

1 LRS (Locally Redundant Storage)

3 copies within a single datacenter in the chosen region. Dev/test, low -criticality data, or when compliance requires single -region only.

2 ZRS (Zone-Redundant Storage)

Synchronous copies across 3+ availability zones in the same region. Survives a zonal outage with no data loss.

3 GRS (Geo-Redundant Storage)

Writes synchronously like LRS in the primary region, then asynchronously replicates to a paired secondary region. Disaster recovery across regions.

4 RA-GRS (Read-Access GRS)

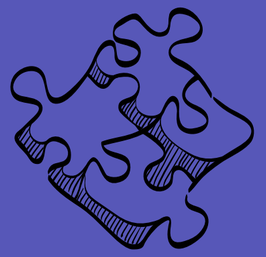
Same as GRS plus read access to secondary endpoints. You want active -read DR—query the secondary for analytics, reduce the pressure on the primary endpoint.

5 GZRS (Geo-Zone-Redundant Storage)

Synchronous ZRS in the primary (across zones) plus asynchronous copy to the paired secondary. You want zonal resilience and regional DR if the whole region fails

6 RA-GZRS (Read-Access GZRS)

GZRS + read access to the secondary endpoints. Zonal resilience, cross -region DR, and readable secondary.


Lifecycle management

Goal: Automate tier transition and deletion.

- Automate Blob tiering (Hot→Cool→Cold→Archive) and retention (delete snapshots/ versions/ base blobs) using rules that key off days since last modified or last accessed.
- Policies run daily and can take up to 24 hours to activate after changes.
- Lifecycle applies to block and append blobs (base, snapshots, versions) in GPv2 and Premium Block Blob/ Blob Storage accounts.
- Enable access time tracking if you want to define rules on the “last accessed” time.

Azure Blob Snapshots

- Blob snapshots are read-only, point-in-time copies of a single blob. They're stored in the same account/container and billed incrementally.
- Snapshots are great when you want an on-demand checkpoint.
- You can't modify a snapshot; you can promote/restore by copying a snapshot over the base blob.
- A snapshot inherits the base blob's metadata and access tier at the time you take it.

Azure Blob Versioning

- Blob versioning automatically keeps previous versions each time a blob is modified or deleted, giving you continuous point-in-time restore without manual snapshots.
- Each change creates a new current version and preserves the prior one with a version ID.
- You can list versions and promote any prior version to become current.
- Lifecycle policies can age off older versions to control cost.

Object Replication

- Object Replication asynchronously copies block blobs from a source container to a destination container —often in another account and/or region.
- It’s policy-based and runs continuously for new and updated blobs after the policy is in place.
- Typical use cases: disaster recovery, neareal-time copy to a reporting account, geo-proximity copies for latency.
- Source storage account- Blob versioning and Change Feed enabled. Destination storage account - Blob versioning enabled.

Azure file share snapshots

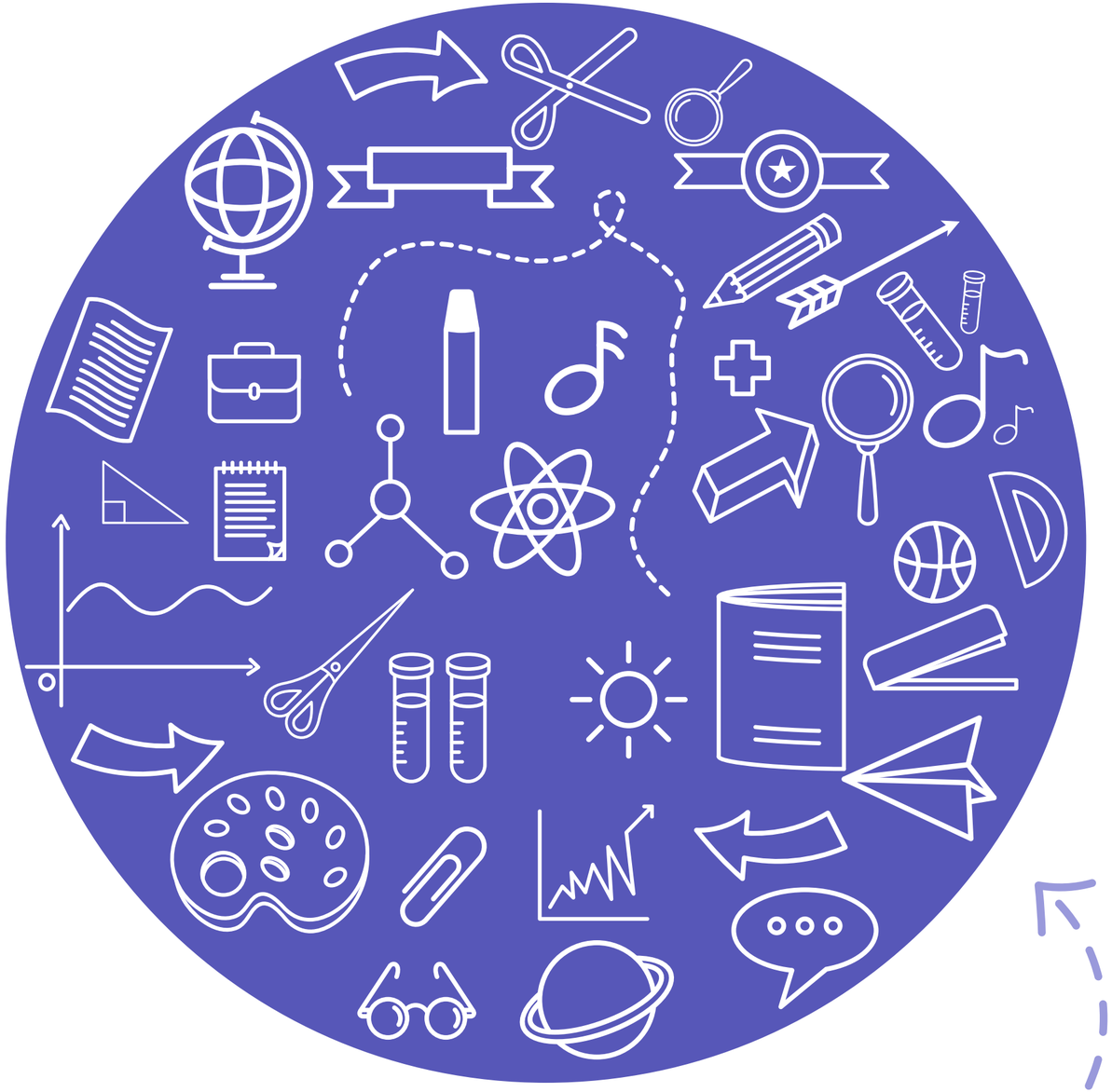
- Azure File share snapshots capture point-in-time states of an entire share.
- They’re incremental—only changed file blocks consume extra capacity.
- You can browse a snapshot in the portal or via SMB and restore either a single file/folder or the entire share.

AzCopy tool

- This is a command-line utility that you can use to copy blobs or files to or from an Azure storage account.
- This tool is supported on Windows, Linux and macOS.
- Authorization is done via Microsoft Entra ID or Shared Access Signatures.

AZ-104 | Microsoft Azure Administrator

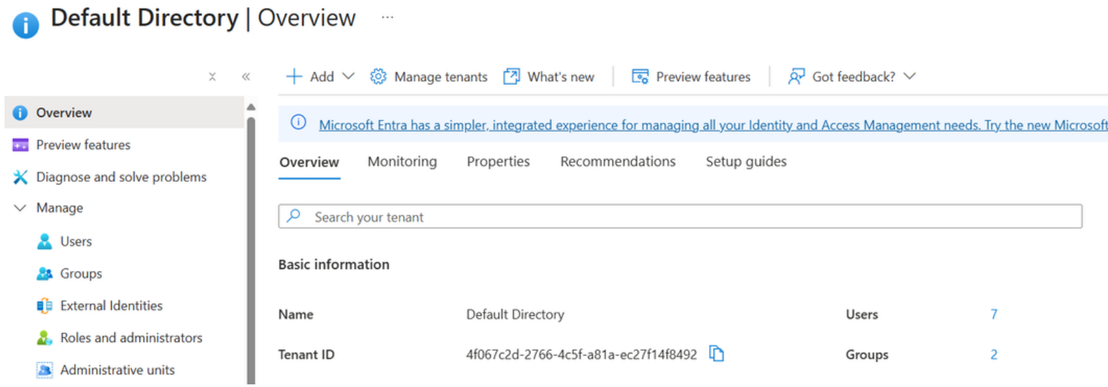
Manage identities and governance



Security

Microsoft Entra ID

Identity



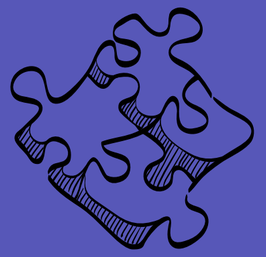
- Microsoft Entra ID is Microsoft's cloud IAM for managing identities and controlling access to apps and Azure resources.
- It authenticates users and issues tokens that services trust.
- Entra ID supports passwords, MFA, and passwordless methods like FIDO2 keys and Windows Hello.

Role-based access control

Goal : Authorization

- Authorization to Azure resources is handled by Azure role-based access control (Azure RBAC). You grant a role assignment to a security principal (user/ group/ service principal/ managed identity) at a scope (management group, subscription, resource group, or resource).

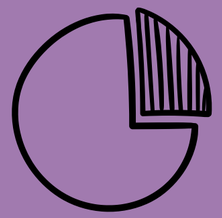
- Where you can assign Azure RBAC:
  - Management group (including the Tenant root group): affects all subscriptions/ resources under it.
  - Subscription: affects all resource groups and resources in that subscription.
  - Resource group: affects all resources in that RG.
  - Resource (and child resources): the narrowest scope—e.g., a single VM, a specific Storage account

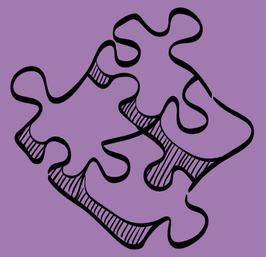




Microsoft Entra ID Roles

Goal: Delegate permissions.

- Microsoft Entra ID roles (formerly “Azure AD admin roles”) control administration of the directory and connected Microsoft cloud services.
- Aspects like managing users, groups, apps (app registrations/enterprise apps), Conditional Access, and security policies.
- They’re separate from Azure RBAC (which controls access to Azure resources like VMs and storage).
- Some common roles.
  - Global Administrator: full control over the tenant and all Microsoft services tied to it.
  - User Administrator: create/ update users, reset passwords, manage user licenses and groups (non-role-assignable groups).
  - Security Administrator: manage security-related settings, alerts, and reports; broad security admin across the tenant.





Microsoft Entra ID Licenses

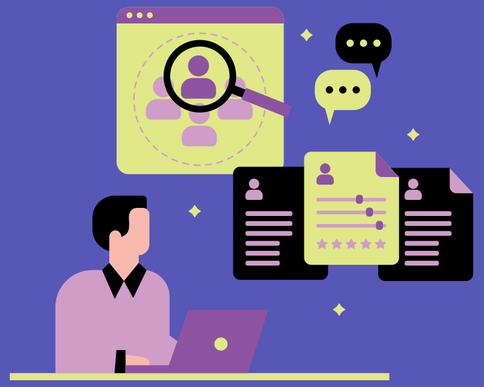
Goal : Additional features

- Entra ID comes with Free Licenses. We also have paid Premium P1 and P2 licenses.
- Entra ID Free: user/ group management, directory sync, basic reports, self-service password change (cloud-only), SSO to Microsoft apps & many SaaS.
- Entra ID P1: adds Conditional Access, dynamic groups, group-based licensing, self-service password reset with write-back (hybrid), and other admin features..
- Entra ID P2: adds Identity Protection (risk-based Conditional Access), Privileged Identity Management (PIM), and access reviews—advanced governance and just-in-time privilege elevation.

Assigning licenses

- Assign per-user in the Admin Center, or at scale with group-based licensing so members inherit entitlements automatically.
- Usage location must be set on each user before assigning a license.
- A user can be in multiple licensed groups—their effective license is the union of enabled service plans across assignments.
- Group-based licensing supports Security Groups and Microsoft 365 Groups with securityEnabled=true.
- It does not support nested groups (no transitive licensing). If you assign to a group that contains groups, only the direct user members get licenses.

Resource tags



- Tags are key-value pairs that add business context to Azure resources for cost, automation, and governance.
- e.g., env=dev,costCenter=CC101, owner=ops.
- Tags defined as a resource group level are not inherited by resources within the resource group.

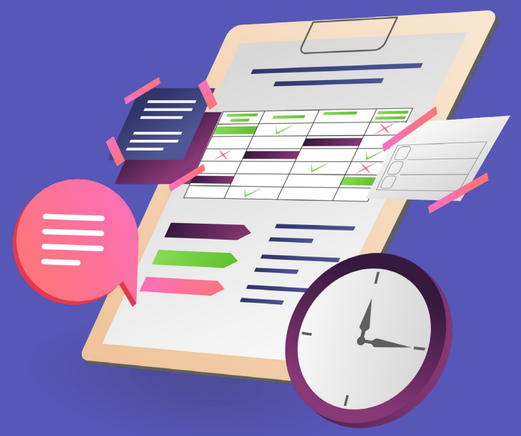
Moving resources

- You can move supported resources to another resource group in the same subscription or to another subscription in the same Entra tenant.
- The platform validates dependencies to ensure resources can be moved.
- Resources don’t change their location when moving to another resource group or subscription.
- When moving resources like virtual machines across subscriptions, you need to move all dependent resources. And all resources need to lie in the same resource group.

Locking resources

- Resource locks protect against accidental change/delete.
- Two types:CanNotDelete (Delete) and ReadOnly.
- Locks can be applied at subscription, resource group, or resource level and inherit downward.

Management Groups



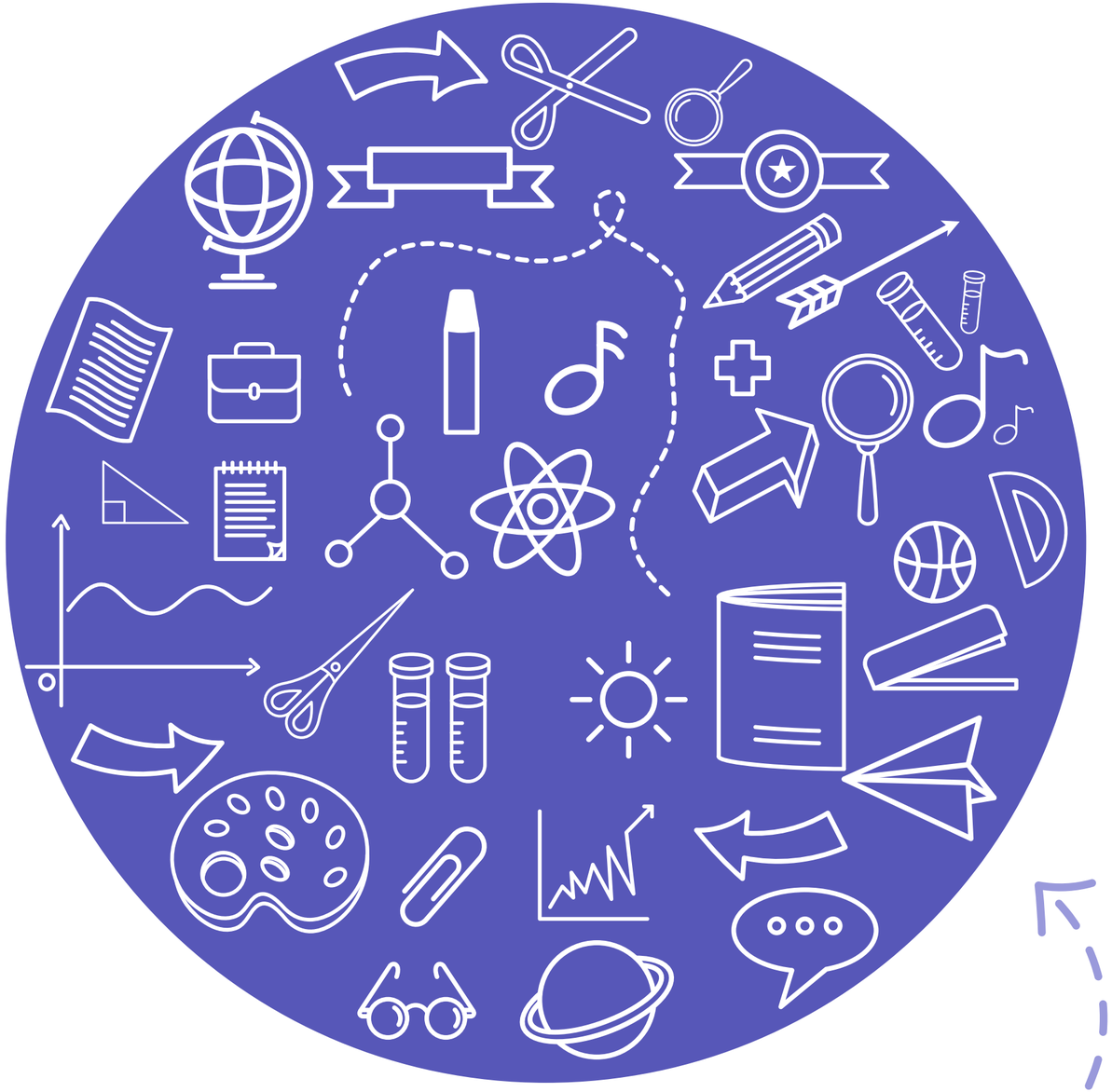
- Management Groups create a governance hierarchy above subscriptions.
- Assign Azure RBAC and Policies at Management Groups to standardize settings across many subscriptions.
- The Tenant Root Group sits at the top; you can nest Management Groups to mirror org structure.

Azure Policy

- Azure Policy evaluates resources/actions against JSON policy definitions and enforces effects (Deny, Audit, Append, DeployIfNotExists/Modify).
- Combine multiple definitions into an Initiative for easier assignment and compliance tracking.
- You can apply policies to the Management Group, to individual subscriptions, to subscriptions, resource groups and certain resource types.

AZ-104 | Microsoft Azure Administrator

Monitor and Maintain Azure resources

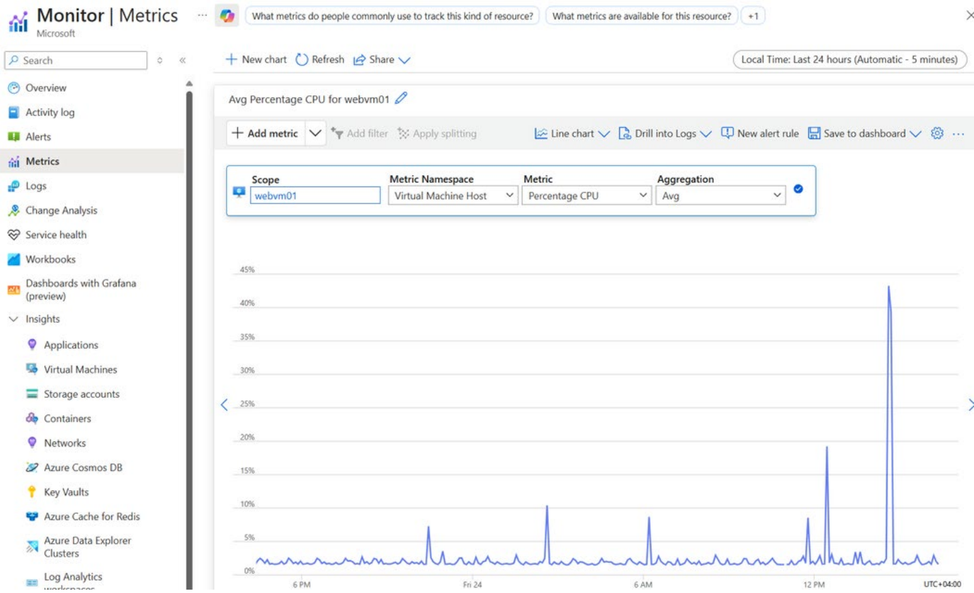


MONITORING

Azure Monitor

Storage

- Azure Monitor is the platform service that collects, stores, analyzes, and acts on telemetry from Azure resources and applications.
- It ingests platform and guest/app signals, stores them (metrics + Log Analytics), and lets you analyze with KQL and visualize with Workbooks.
- You can act using alerts, action groups, and automation.



Activity Log

- The Activity Log records control-plane events in your subscription (create/update/delete operations on Azure resources, service health, policy evaluations).
- Use it to investigate deletions, policy effects, and service health incidents.
- For retention/analytics, export via Diagnostic settings to a Log Analytics workspace, Storage, or Event Hub.

Azure Monitor Alerts

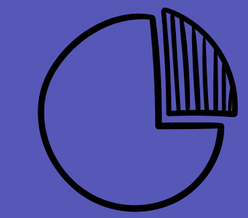
Goal : Get notified when it matters.

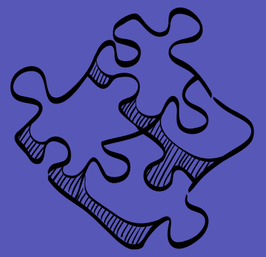
- Alerts turn metrics, logs, and platform events into notifications or automation.
- Signal types
  - Metric alerts: fast, numeric, near real-time (e.g., CPU > 85% for 10 minutes)
  - Activity Log alerts: fire on specific management events (e.g., Delete Virtual Machines).
  - Log alerts (KQL): evaluate a query result on a cadence
- Define scope, condition, frequency, and severity, then attach an Action Group for email/ SMS/ ITSM/ Logic Apps, etc.
- Suppressing Alerts - Use Action Rules to mute alert notifications during maintenance or expected noise, without turning alerts off.

Log Analytics

Goal: Central location/ repository for your logs.

- A Log Analytics workspace is the Azure Monitor data store for logs. Azure resources, servers (Azure +-on-prem/other clouds via Azure Arc), and services send telemetry into tables in this workspace.
- You query it with KQL (Kusto Query Language), visualize with Workbooks, and trigger Log Alerts..
- You pay per ingested GB; set daily caps and retention.
- To make sure your machines can send data to the Log Analytics workspace.
  - Agent: Use the Azure Monitor Agent (AMA) on Windows/ Linux. It's the supported agent for Azure Monitor.
  - Data Collection Rules (DCRs): Define what to collect (Windows Events channels, Syslog facilities, Performance counters, IIS W3C logs, custom logs, etc.) and where to send (a specific workspace).





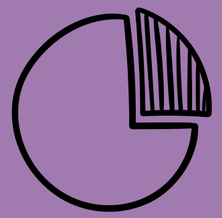
Log Analytics

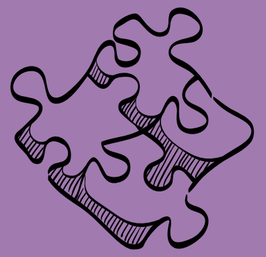
Goal: Central location/ repository for your logs.

- What data can we collect from the machines.
  - Windows Events → Event table: Choose channels (e.g., System, Application, Security). You can filter by event levels (Error, Warning, Information) and by Event IDs.
  - Linux Syslog → Syslog table: Select facilities (auth, daemon, kern, syslog, user, local*) and severities (emerg..debug).
  - Performance counters: CPU, memory, disk, network, process metrics.
  - IIS W3C logs (Windows): Collect HTTP logs into a dedicated table.
  - Custom apps: Use the Logs Ingestion API to push JSON into a custom table you define.

Azure Backup

- Azure Backup is Microsoft’s first-party, cloud-native backup service that protects Azure resources and selected on-prem/other-cloud workloads.
- Recovery Services vault (RSV): Long-standing vault for Azure VMs, SQL/SAP HANA in Azure VMs, Azure Files (snapshot-based) .
- Backup vault: Newer vault for certain modern/“vaulted” scenarios like Azure Disk Backup and Azure Blob Backup.





Recovery Services Vault

Goal : Backup workloads

- A Recovery Services vault stores VM recovery points and policies. Azure Backup snapshots the VM and moves data into the vault.
- Azure Backup enables a backup extension on the VM, takes a snapshot (app-consistent via VSS on Windows when possible), then transfers data to the RSV as a recovery point.
- Instant Restore keeps short-term snapshots to speed up restores.
- Policies: Define schedule (daily/ weekly) and retention (short/ long-term). Older restore points are pruned automatically per policy.
- Microsoft Azure Recovery Services (MARS) agent - backs up Windows files/ folders and system state straight to a Recovery Services vault—simple, agent-based protection where VM-level or app-aware backups aren't needed.

Restore options

- File Restore (Item-level): Mount a recovery point to the source (or another) VM via a downloaded script, copy the needed files, then unmount. Great for accidental deletes or small rollbacks.

- VM / Disk Restore (crash-/app-consistent points):
  - Create new VM (quickest “lift-back”).
  - Restore disks (Managed Disks) to a RG, then attach or deploy from template.
  - Replace existing disks on the original VM. Choose the recovery point, target RG/network, and proceed.

Azure files backup

- Protect Azure file shares by registering the storage account in an RSV and applying a backup policy.
- Azure Backup handles share snapshots (and vaulted backups where supported).
- Restore: entire share or individual files to original/alternate location. Integrates well with File Sync scenarios.

Azure Site Recovery

Goal : Replicate workloads.

- Azure Site Recovery is Microsoft's DRaaS that continuously replicates Azure VMs to another Azure region and lets you fail over and fail back with minimal downtime.

- Key components
  - Recovery Services vault (RSV): Control plane for replication, policies, failover, and recovery plans.
  - ASR/ Mobility service extension on the VM: Installed automatically when you enable replication; tracks disk writes.
  - Cache storage in source region (Standard GPv2): Writes land in a cache storage account first, then stream to target region storage/ managed disks, where recovery points are created.
  - Target resources: ASR prepares/ uses target resource group, VNet/ subnet, managed disks, and (optionally) target availability options. Network mapping links source VNet to target VNet.

- Failover types
  - Test Failover: Proves DR in an isolated network; no impact to prod or replication. Use for drills/ compliance.
  - Planned Failover: For maintenance/ migrations; graceful shutdown