# To Search for particular term, use the following steps

**Azure Roles :** Azure built-in roles->Azure roles, Microsoft Entra roles, and classic subscription administrator roles - > Ref -> Bulit-in

**Entra Roles** : Overview of Microsoft Entra role-based access control (RBAC) -> Ref -> Bulit-in

**Azure Disk Encryption -**> encrypt a Windows virtual machine in Azure

**AzCopy** Tutorial: Migrate on-premises data to Azure Storage with AzCopy -> Get Started.

**ARM** -> Create a Windows VM from a template in Azure -> Quick Start -> Create a Windows VM in the Azure portal - Azure Virtual Machines -> ARM

Use a template to join a Windows VM to Microsoft Entra -> -> Microsoft Entra ID documentation - Microsoft Entra ID -> Domain Services, How TO -> domain join VMs

**SSRP** -> Enable Microsoft Entra self-service password reset -> Authnetcation

**LRS/ZRS** -> learn about types of storage account -> Blob storage=> Availability and disaster recovery -> data reduendacy

**Route table** : virtual network documentation - > manage connectivity -> routing

**Recovery Services vaul**t and migrate vmware viruatl machine from on premise to sub -> “Site Recovery Documentation” -> tutorial -> prepare azure

—-----------------------------------------------------------------------------------------------------------------

# Key Notes:

## Admin & Policy

**custom security attributes** cannot be assigned to Microsoft 365 groups.

in a **free** Microsoft Entra ID tenant, you can only assign licenses to individual users

**Licenses** are only for accessing services and **do not affect dynamic or assigned group** memberships.. e.g., member rule : (user.city -startWith “m”) user.department -notIn [“test”])

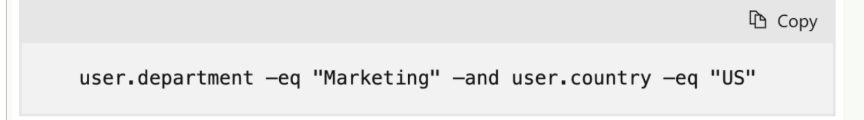
**join** the virtual machine to an **Active Directory domain -> ARM** -> Microsoft.Compute/virtualMachines/extensions ->

**group-based licensing** does not support nested group inheritance.

SSRS -> least the Authentication Policy Administrator role

A **group cannot be deleted** if it has **licenses** directly assigned to it

Azure does not permit the use of security questions for administrators e..g, billing admin, security admi, etc.



enabling **Multi-User Authorization (MAU) in a Recovery Services** vault requires creating a resource guard.

—-----------------------------------------------------------------------------------------------------------------

## Azure Mmontor, DCR, Network Watcher, Log Analytics

| **Tool/Service** | **Purpose** | **When to Use** |
| --- | --- | --- |
| **Azure Virtual Network Watcher** | Provides tools like connection monitor, IP flow verify, NSG diagnostics | Use for diagnosing and monitoring connectivity and flow between resources in your VNets |
| **Azure Monitor Network Insights** | Provides **dashboards** with **visual topology** and **detailed metrics** | Use when you need **network topology visualization** and aggregated metrics (e.g., for ExpressRoute, VNets) |
| **Data Collection Rule (DCR)** | Defines how telemetry (logs/metrics) is collected and sent to destinations | Use when configuring **data ingestion** rules for Log Analytics or custom monitoring |
| **Log Analytics** | Query and analyze logs/metrics collected from Azure resources | Use when you want to **write custom queries** or analyze collected telemetry data |

—-----------------------------------------------------------------------------------------------------------------

## Networking

**Public IP addresses** can be associated with a load balancer or a network interface to enable external communication

**Ports:** Azure File Share (port 445), HTTP (port 80), HTTPS (port 443), RDP for Windows VMs (port 3389), SSH for Linux VMs (port 22), SQL Database (port 1433), Azure Bastion (port 443), Load Balancer health probes (ports vary, often TCP 80/443), App Services (HTTP/HTTPS), ports 53 DNS Server

**DNS record types**: A records map a domain to an IPv4 address, while **AAAA** records map to an IPv6 address. **CNAME** records point a domain alias to another domain name, and **MX records** handle mail exchange for routing emails. **NS** records define the name servers for a DNS zone, essential for domain delegation, and **SOA** records (Start of Authority) hold zone information—automatically managed by Azure. **PTR** records are used for reverse DNS lookups (IP to domain name), **TXT** records store arbitrary text such as SPF data or domain verification details, and **SRV** records help locate services like SIP or LDAP within a domain.

**Azure Firewall** can connect to a virtual network within the same region and resource group

**network interfaces** (NICs) must be created in the same region as the virtual network (VNet) they are associated with

**Azure Bastion** requires a Standard Public IP address for both the Basic and Standard SKUs. Additionally, the IP address must be IPv4, have a Regional tier, and use a Static assignment

**AzureBastionSubnet** for **Azure Bastion** requires a subnet prefix of at **least /26** to function properly

172.16.10.0/25 -> maximiun num is : 32 – 25 = 7 => 2^7 = 128 – (5 preseverd)

**global virtual network** peering allows you to peer virtual networks across different regions and subscriptions,

**private endpoint** connection allows secure access to the container registry over a private network

**Network Security Group**  An NSG can only be applied to subnets in virtual networks located in the same Azure region as the NSG, regardless of the resource group.

| **Command** | **Purpose** |
| --- | --- |
| ✅ New-AzLoadBalancerInboundNatRuleConfig | 🔹 Maps ports for VM access (✅ Correct for this use case) |
| New-AzLoadBalancerProbeConfig | 🔸 Health probes for backend pool (not for RDP or ports) |
| New-AzLoadBalancerRuleConfig | 🔸 For distributing traffic to backend pool (not NAT/RDP-specific) |
| New-AzLoadBalancer | 🔸 Creates a new load balancer object (not a configuration rule) |

—-----------------------------------------------------------------------------------------------------------------

## Backup:

**Azure Backup** requires that the storage account used for diagnostic settings (like **Azure Backup reports**) be in the same region as the Recovery Services vault (Vault1)

Recovery Services vault can only back up resources that are in the same geographic region as the vault itself

* **Recovery Services Vault** supports:
  + VMs via extension
  + File Shares (on Storage Accounts)
  + SQL Server/SAP HANA (on Azure VMs)
* **Backup Vault** (older name) supports:
  + Managed disks
  + Blobs
  + PostgreSQL DBs

**Object replication** supports general-purpose v2 storage & premium block blob storage ( BlobStorage); append blobs and page blobs aren't supported.

to **restore a backup** from the Recovery Services vault to a different virtual machine (in this case, VM2), you need to have the Microsoft Azure Recovery Services (MARS) Agent installed on the destination VM

**exclude specific** files or folders from a backup by creating a \_backup.filter file in the root directory of the app.

**Geo-replication** in **Azure Container Registry** is only supported in the **Premium** SKU

—-----------------------------------------------------------------------------------------------------------------

## Redundancy Storage

| **Redundancy Type** | **Replication Scope** | **Primary Region** | **Secondary Region** | **Durability (per year)** | **Read Access to Secondary?** | **Best For** |
| --- | --- | --- | --- | --- | --- | --- |
| **LRS**  (Locally Redundant Storage) | 3 copies in **1 datacenter** | ✅ | ❌ | **11 nines**  (99.999999999%) | ❌ | Low-cost, non-critical data, data residency limits |
| **ZRS**  (Zone-Redundant Storage) | 3 copies in **3 availability zones** (same region) | ✅ | ❌ | **12 nines**  (99.9999999999%) | ❌ | High availability within region, Azure Files, Data Lake |
| **GRS**  (Geo-Redundant Storage) | LRS in primary + async LRS in secondary | ✅ (LRS) | ✅ (LRS) | **16 nines**  (99.99999999999999%) | ❌ (Unless using **RA-GRS**) | Regional disaster recovery, backup |
| **RA-GRS**  (Read-Access GRS) | Same as GRS | ✅ (LRS) | ✅ (LRS) | **16 nines** | ✅ (Read only) | Readable geo-redundant backup |
| **GZRS**  (Geo-Zone-Redundant Storage) | ZRS in primary + async LRS in secondary | ✅ (ZRS) | ✅ (LRS) | **16 nines** | ❌ (Unless using **RA-GZRS**) | Critical apps needing both zone + region redundancy |
| **RA-GZRS**  (Read-Access GZRS) | Same as GZRS | ✅ (ZRS) | ✅ (LRS) | **16 nines** | ✅ (Read only) | Max durability with read-access geo-redundancy |

—-----------------------------------------------------------------------------------------------------------------

## Network Watcher

| **Feature** | **Description** | **Use Case / Benefit** |
| --- | --- | --- |
| **Monitoring and Diagnostics** | Provides tools to monitor, diagnose, view metrics, and enable logging for resources in a virtual network. | Visibility into network health and traffic flow. |
| **Connection Monitor** | Monitors connectivity between Azure resources, hybrid environments, and internet. | Track reachability, latency, and network performance. |
| **IP Flow Verify** | Checks if a packet is allowed or denied to/from a VM based on NSG rules. | Debug inbound/outbound traffic issues. |
| **NSG Flow Logs** | Logs all traffic that passes through a Network Security Group. | Audit and troubleshoot traffic; analyze patterns. |
| **Topology** | Visualizes the resources in a virtual network. | Understand network architecture and dependencies. |
| **Next Hop** | Shows the next hop for a packet from a VM. | Diagnose routing issues. |
| **Effective Security Rules** | Displays effective NSG rules applied to a VM's NIC or subnet. | Validate NSG configuration. |
| **Packet Capture** | Captures packets sent/received by a VM. | Deep-dive troubleshooting, intrusion detection. |
| **Connection Troubleshoot** | Tests connectivity between Azure resources and external endpoints. | Spot latency or unreachable issues quickly. |
| **VPN Troubleshoot** | Diagnoses common VPN gateway or connection problems. | Isolate VPN configuration issues. |
| **Traffic Analytics** | Uses NSG Flow Logs and Azure Monitor to provide insights. | Visualize traffic trends and potential threats. |

—-----------------------------------------------------------------------------------------------------------------

## Azure Container Apps, Azure Container Instances (ACI) , Azure App Service , VM and resources

| **Feature** | **Azure Container Apps** | **Azure Container Instances (ACI)** | **Azure App Service** |
| --- | --- | --- | --- |
| **Purpose** | Serverless container orchestration for microservices, APIs, background tasks | Run containers without managing servers; good for short tasks or burst workloads | PaaS for hosting web apps, APIs, and mobile backends |
| **Best For** | Microservices, event-driven apps, background jobs | Fast container runs, dev/test, scheduled jobs | Web apps (Node.js, .NET, PHP, Java, Python) |
| **Orchestration** | Built-in with **Kubernetes-like** features (via KEDA, Dapr, Envoy) | None – single container or simple multi-container groups | Built-in load balancing and scaling |
| **Scaling** | Automatic scale to zero, based on events (HTTP, queue, etc.) | Manual or scheduled (no autoscale to zero) | Auto-scale based on HTTP traffic or schedules |
| **Stateful Support** | Yes (via Dapr and volume mounting) | Limited (Ephemeral) | Yes (persistent storage options available) |
| **Ingress/HTTP Routing** | Built-in with revisions and traffic splitting | Manual setup required | Built-in with custom domain, SSL |
| **CI/CD Integration** | GitHub Actions, Azure DevOps, etc. | Limited – requires custom setup | Native support via Azure DevOps, GitHub |
| **Networking Options** | VNet integration, managed identity, custom domains | VNet support, managed identity | Full VNet support and hybrid connections |
| **Pricing Model** | Per second of usage and resource consumption (scale-to-zero saves cost) | Per second of usage (CPU/memory) | App Plan pricing (reserved compute) |
| **Use Case Example** | API with event-driven scale | Run a batch job for 5 mins | Host a business web portal |

| **App Service OS** | |
| --- | --- |
| **Runtime Stack** | **Supported OS** |
| ASP.NET (e.g., 4.8) | **Windows only** |
| .NET (Core, 5–8 LTS) | **Windows or Linux** |
| Node.js, PHP, Python | **Windows or Linux** |
| Java | **Depends on version and container** |

| **Fault and update domain**  **Each availability set can have up to 3 fault domains and 20 update domains** | | |
| --- | --- | --- |
| **Concept** | **Purpose** | **Key Details** |
| **Availability Set** | Logical grouping of VMs to ensure high availability | VMs are spread across **fault and update domains** |
| **Update Domain** | Helps with **planned maintenance** | One update domain is rebooted at a time; each domain has **30 mins to recover** before the next restarts |
| **Fault Domain** | Helps with **unexpected hardware/power/network failures** | VMs in different fault domains **don’t share the same physical hardware**, power source, or switch |
| **Default Limits** | - 5 Update Domains (can be increased)- 3 Fault Domains (Azure default) | After reaching the max, the cycle repeats (e.g., VM6 in same update domain as VM1) |

**Azure Key Vault** supports enableing key rotation policies

All **app serivics support** both windows & linix, except for Azure Container Apps only supports Linux-based.

Even though VM is **deallocated**, its 16 vCPUs still count toward **the regional vCPU quota** because Azure reserves these resources for the VM

Enable **content trust** to push and pull signed images for Azure container registry.

Customer manage key : RSA -> keys of sizes 2048, 3072 and 4096

Resource Group blade in the Azure portal includes an option to view the deployment history and allows you to access the templates used

**container app environment** requires a dedicated **subnet** with a minimum address space of **/23** when connecting to a virtual network.

—-----------------------------------------------------------------------------------------------------------------

## Storage types & Lifecycle

| **Feature** | **Hot Tier** | **Cool Tier** | **Cold Tier** | **Archive Tier** |
| --- | --- | --- | --- | --- |
| **Purpose** | Frequently accessed data | Infrequently accessed data | Rarely accessed, but still online | Rarely accessed, offline |
| **Latency (Time to first byte)** | Milliseconds | Milliseconds | Milliseconds | Hours (rehydration required) |
| **Storage cost** | Highest | Lower | Lower than cool | Lowest |
| **Access/transaction cost** | Lowest | Higher | Higher than cool | Highest |
| **Minimum retention** | None | 30 days | 90 days | 180 days |
| **Availability** | 99.9% | 99% | 99% | 99% |
| **Availability (RA-GRS reads)** | 99.99% | 99.9% | 99.9% | 99.9% |
| **Supported redundancy** | All (LRS, ZRS, GRS, RA-GRS, GZRS, RA-GZRS) | All | All | Only LRS, GRS, RA-GRS |
| **Immediate access** | Yes | Yes | Yes | No (rehydration required) |
| **Modifiable/readable** | Yes | Yes | Yes | No (rehydration needed for read/modify) |
| **Metadata access** | Full access | Full access | Full access | Metadata accessible; content not readable |
| **Snapshots** | Supported | Supported | Supported | Not supported |
| **Early deletion penalty** | None | Yes (before 30 days) | Yes (before 90 days) | Yes (before 180 days) |
| **Best for** | Active apps, frequent data use | Short-term backups, DR, infrequent access | Large datasets, rarely accessed data | Archival, compliance, long-term retention |
| **Rehydration required?** | No | No | No | Yes (to hot, cool, or cold) |
| **Default for new accounts?** | Yes (GPv2 default) | Optional | Optional | Not supported |

**Lifecycle management** policies support: blobk blobs, append blobs, generatlv2, premium block blob, and blob storage account.

—-----------------------------------------------------------------------------------------------------------------

## **Azure Storage type** (Queue, Blob, Table, Files):

| **Service** | **Use Case** | **Access Pattern** | **Key Features** |
| --- | --- | --- | --- |
| **Azure Queue Storage** | Messaging between components in a decoupled architecture (e.g., microservices) | FIFO message queue | Simple, scalable message queuing |
| **Azure Blob Storage** | Store unstructured data like images, videos, backups, logs | Read/write blobs | Hot/cool/archive tiers, large-scale object storage |
| **Azure Table Storage** | Store structured NoSQL key-value data (fast and scalable) | Key-based queries | Low-cost, schema-less, massive scalability |
| **Azure Files** | Lift-and-shift legacy apps needing shared file access (like SMB) | File share over SMB/NFS | Mountable in Windows/Linux, good for shared access |

| **✅ Criteria** | **🧠 Decision Rule** | **💡 Notes** |
| --- | --- | --- |
| **Region Match** | Storage account must be in the **same region** as the resource (e.g., Web App in West US → use West US storage) | Avoids cross-region transfer costs |
| **Kind = StorageV2** | Prefer **StorageV2** for general-purpose, cost-effective support for **Blob, File, Queue, Table**, and backup integration | Most flexible and cost-effective option |
| **Kind = BlobStorage** | Acceptable if only blob backup is needed — still cheaper than BlockBlobStorage | Lower flexibility; not recommended for File-based or mixed backup types |
| **Kind = BlockBlobStorage** | **More expensive** — specialized for performance; **not ideal** when cost is a concern | Avoid unless explicitly required for performance-sensitive scenarios |
| **Kind = FileStorage** | Specialized; only use when **Azure File Share** or SMB protocol is needed | Not usable for general app service backup |
| **Redundancy and Performance** | If mentioned, choose **LRS (Locally-redundant)** and **Hot Tier** to minimize cost | GRS/ZRS and Cool/Archive tiers may incur extra costs or limitations |

**blockBlob** are designed to store large amounts of unstructured data, such as images or backups, **appendBlob** it is generally used for log data where the need is to continuously append new data. **page** **blobs** are typically used for storing virtual hard disks (VHDs) for Azure virtual machines

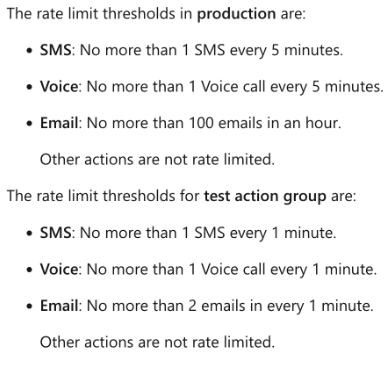
—-----------------------------------------------------------------------------------------------------------------

## IAM, Access Keys, Shared Access Signature

| **Method** | **When to Use** | **Scope** | **Security Level** |
| --- | --- | --- | --- |
| **Access Control (IAM)** | When assigning role-based access (RBAC) to Azure resources securely. | Fine-grained (user/group/app) | High (centralized control) |
| **Access Keys** | When you need full access to a storage account programmatically. | Account-wide | Medium-Low (broad access) |
| **Shared Access Signature** | When granting temporary, limited access to resources (e.g., a file, blob). | Resource-level | Medium (time-bound, limited access) |

—-----------------------------------------------------------------------------------------------------------------

## Alert Limit



—-----------------------------------------------------------------------------------------------------------------