Azure Blob Storage	
Azure Data Services	Azure Blobs / Azure File / Azure Queue / Azure Tables / Azure Disks
Azure Storage redundancy	Redundancy in the primary region: ● **Locally redundant storage (LRS)** ● **Zone-redundant storage (ZRS)** ● **Geo-redundant storage (GRS)** ● **Geo-zone-redundant storage (GZRS)**
Access Tiers	**Hot tier** **Cool tier** **Archive tier**
Azure blobs	Azure Storage offers three types of blob storage: **Block Blobs, Append Blobs and page blobs.**
Authorization Methods	**AD,** **Shared key** **Shared access signature** **ADDS**
Encryption	Two basic kinds of encryption available for Azure Storage: Encryption at rest Client-side encryption (done with client libraries) Data in a new storage account is encrypted with Microsoft-managed keys by default. You can use either type of key management: ● ***customer-managed key*** ● ***customer-provided key*** **Azure Storage infrastructure level encryption:** When infrastructure encryption is enabled, data in a storage account is **encrypted twice** — **once at the service level and once at the infrastructure level** — with two different encryption algorithms and two different keys.

URL	`https://myaccount.blob.core.windows.net/mycontainer/myblob`
Types of storage	Standard Premium ● Block blobs ● File shares ● Page Blobs
Data protection overview	**Soft delete for containers** **Soft delete for blobs** **Blob versioning** **Point-in-time restore for block blobs** (soft delete/versioning/change feed should be enabled) **Change Feed**
Data lifecycle	Lifecycle policies
Object replication for block blobs	When you configure object replication, you create a replication policy that specifies the source storage account and the destination account.
Compute	
Virtual Machines	
VM sizes	
VM Power states	Creating → Starting → Running (Stopping → Stopped or Deallocating → Deallocated)
Bringing and creating Linux images in Azure	When bringing your Linux image you have two options: ● **Managed images** for simple VM creation in a development and test environment. ● **Azure Compute Gallery** for creating and sharing images at-scale.
Azure Compute Gallery	An Azure Compute Gallery helps you build structure and organization around your Azure resources, like images and applications. **Scaling:** Compute gallery allows you to specify no replicas to keep. Helps in multi-VM deployment scenarios.

	Replication: can replicate to other Azure regions automatically. **Sharing:** When you use Azure Compute Gallery multiple resource types are created: ● **Image definitions:** logical grouping of versions of images. ● **Image Versions**: actual image ● **Image Source:**
Azure dedicated hosts	
Azure Spot VM	
Azure Reservations	Reserved Instances On-demand Capacity Reservation
Azure virtual machine extensions and features	Extensions are small applications that provide post-deployment configuration and automation on Azure VMs. ● **Azure disk encryption** ● **Key vault VM extension** ● **Custom script extension** ● **VM snapshot extension** ● **Antimalware extension Windows**
Availability and scale	● **Availability sets:** An availability set is a **logical grouping of VMs** that allows Azure to understand how your application is built to provide for redundancy and availability. 99.95% Azure SLA. Each virtual machine in your availability set is assigned an **update domain and a fault domain** by the underlying Azure platform. Each availability set can be configured with up to **three fault domains and twenty update domains**. **Update domains(20)** indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time**. Only one update domain is rebooted at a time.** **Fault domains(3)** define the group of virtual machines **that share a common power source and network switch.**
Disks	Standard HDD

	Standard SSD Premium SSD Premium SSD v2 Ultra disk Redundancy options for managed disk: LRS and ZRS
Overview of managed disk encryption options: Inside your vm or VM host or at storage level at rest.	**Server side encryption:** encrypts your data at rest. **Azure disk encryption:** encryption happens inside your VM, with dm-crypt or bit-locker. **Encryption at host:** end-to-end encryption which starts at VM host itself. **Double encryption at rest:** When infrastructure encryption is enabled, data in a storage account is encrypted twice — once at the service level and once at the infrastructure level — with two different encryption algorithms and two different keys. Service-level encryption supports the use of either Microsoft-managed keys or customer-managed keys with Azure Key Vault. Infrastructure-level encryption relies on Microsoft-managed keys and always uses a separate key.
Encryption key management	Platform-managed keys: Customer-managed keys
Disk Encryption Sets	**Disk encryption set** is introduced for simplifying the key management for managed disk. - Create a disk encryption set, while doing so specify key vault and key. - With a disk encryption set **system assigned, managed identity** is created. - User associates disk encryption set with encrypted disk - Disk uses managed id of disk encryption set to use key vault keys
Backup and data protection	
Managed identities	Why managed identities: - No need to manage credentials - Authenticate to any resource using Azure AD authentication\ There are two types of managed identities: ● **System-assigned:** created/deleted with resource, can’t be shared ● **User-assigned:** can be shared

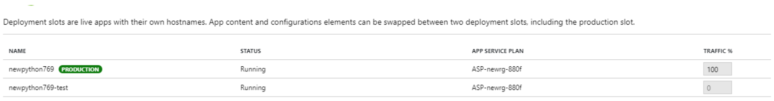
Updates and maintenance overview	Automatic OS upgrades: Once configured, the latest OS image published by image publishers is automatically applied to the scale set without user intervention. **Automatic VM guest patching:** Enabling automatic VM guest patching for your Azure VMs helps ease update management by safely and automatically patching virtual machines to maintain security compliance. **Patch orchestration modes:** ● **AutomaticByPlatform (Azure-orchestrated patching):** ● **AutomaticByOS (for windows)** ● **Manual** ● **ImageDefault** Update management center: new service to manage updates Maintenance control
Backup and Recovery	Azure Backup: VMSnapshot extension is installed for backup. Azure Site Recovery: You can configure Azure Site Recovery for your VMs so that your applications are recoverable in a matter of minutes with a single click. You can replicate to an Azure region of your choice. Managed snapshots: Snapshot consistency: ● **Application consistent:** captures memory consistent and pending i/o operations. ● **File-system consistent:** taking a snapshot of all files at same time. ● **Crash consistent backup:** vm is shut down at the time of backup.

User data	User data is a new version of custom data.offers following benefits
	● Data can be retrieved after provisioning
	● Data can be updated/added without stopping or rebooting vm
	Update/get data:
	`GET`
	`"/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/virtualMachines/{VMName}?$expand=userData"`
	`PUT`
	`"/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/ virtualMachines/{VMName}`
	`PATCH`
	`"/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/ virtualMachines/{VMName}`

Virtual machine scale set	
Virtual machine scale set	Orchestration modes for Virtual Machine Scale Sets in Azure ● **Uniform orchestration** ● **Flexible orchestration** **Types of Autoscaling:** ● **Dynamic autoscale** ● **Scheduled Autoscale** ● **Predictive Autoscale** **Custom scale-in policy:** ● **Default (highest instance id)** ● **Newest VM** ● **OldestVM** Types of instance protection: ● **Protect from scale-in action** ● **Protect from scale set action** **Overprovisioning:** With overprovisioning turned on, the scale set actually spins up more VMs than you asked for, then deletes the extra VMs once the requested number of VMs are successfully provisioned. Upgrade policy: ● **Automatic** ● **Rolling** ● **Manual** **Automatic OS upgrade:** will do the upgrade in batches taking health extensions in account.
Azure Functions	
Triggers	Types of trigger: **Timer** (execute function at set interval) **HTTP** **Blob** (Execute function when file uploaded) **Queue** (Execute function when message is added)

	Azure Cosmos DB (when document changes) **EventHub** (event hub receives a new event)
Bindings	Types of bindings: ● Input ● Output Binding properties: Name: Type: (table/queue trigger) Direction: (in/out) Connection: connection strings
Hosting plans	● Consumption plan: fully serverless hosting option ● Premium plan: functions are kept initialized ● Dedicated plan:
Choose best service to automate	Design first: ● Logic Apps (developers) ● Microsoft Power Automate (users) Code first: ● WebJobs (existing webapp) ● Azure Functions
Execution Time	By default, functions have a **timeout of five (5) minutes.** This timeout is configurable to a **maximum of 10 minutes.** **Durable function without any timeouts.**
Durable functions	Function types:
Azure Functions Core Tools	
App service	
Azure App service	

	Create a webapp
App service plans	
Deploy to App Service	
App Service networking features	
Configure application settings	In App service, app settings are variables passed as environment variables.
General settings	General settings Stack settings Platform settings Debugging: (Enable remote debugging)
Path mappings	
Diagnostic logging	**Web server logging (win)** **Detailed Error logging (win)** **Failed request logging (win)** **Application logging (linux and win):** application logs messages **Deployment logging (linux and win):** why deployment failed
Autoscaling	Scale up to S1 or P level Standard or premium
Deployment slots	**Auto Swap:** As soon as an application is deployed to a slot it automatically swaps into a target slot. This is not the same as deploying directly to the target because the application gets a warm start, and the previous release of the target slot is preserved if a rollback is required. **Swap:** The most basic swap type that requires you to manually trigger the swap operation. **Swap with preview:** This type is similar to a regular swap but allows you to preview the swap before completing it. Because each slot maintains its own configuration and application settings, the web app may not behave exactly as it did in the originating slot, and that is a good thing.
Route production traffic	Specify % in traffic column

<table>
<tr><td></td><td>
Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot.
<table><tr><th>NAME</th><th>STATUS</th><th>APP SERVICE PLAN</th><th>TRAFFIC %</th></tr><tr><td>newpython769 PRODUCTION</td><td>Running</td><td>ASP-newrg-880f</td><td>100</td></tr><tr><td>newpython769-test</td><td>Running</td><td>ASP-newrg-880f</td><td>0</td></tr></table></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

Networking

<table>
<tr><th colspan="2">Virtual network</th></tr>
<tr><td>Routes</td><td>Default routes:

<b>System routes</b>
- Route for virtual network
- Route for internet
- Drop traffic for 10.0.0.0/8, 172.16, 192.168./

<b>Optional default routes:</b>
- Vnet peering
- Virtual network gateway
- Virtual network service endpoint

Custom routes:

Next hop types:
● Virtual network
● Internet
● Virtual appliance
● Virtual network gateway
● None

<b>Service tags:</b> is a group of IP address prefixes from a given Azure service. E.g Storage, Storage.AustraliaEast</td></tr>
<tr><td>Private Endpoint vs Service Endpoint</td><td>Private endpoint: allow connection privately. DNS changes are required. No need for public IP.</td></tr>
</table>

	Service endpoint: allow connection from specific VNET, public IP still required. One service point for the entire service.
Application Security groups	Allow you to group virtual machines and define network security based on those groups.
Load balancer	
Load balancer	Operates at Layer 4
SKU	**Basic** – not zone redundant **Standard** **Gateway load balancer** -
Components	Components of Load balancer: ● **Frontend IP configuration** ● **Backend pool** ● **Health probes** ● **Load balancer rules** ● **Inbound nat rules** ● **Outbound rules** **HA port:** protocol - all port -0 all protocols all ports rule. Internal standard LB **Load balancing algorithm** 1. Hash based 2. Session persistence a. Session Persistence: Client IP b. Session Persistence: Client IP and Protocol A Load Balancer can either be **zone redundant, zonal, or non-zonal**. **zone redundant(zones= [1,2,3])** **zonal(zone=[1] or [2])** **non-zonal(zone=[ ])**
Cross-region load balancer	The backend pool of cross-region load balancers contains one or more regional load balancers. Azure cross-region load balancer uses a geo-proximity load-balancing algorithm for the routing decision.
Gateway Load Balancer	Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party **Network Virtual Appliances**

	(NVAs). With the capabilities of Gateway Load Balancer, you can easily deploy, scale, and manage NVAs. NVA - filter application traffic
Load Balancer TCP Reset and Idle Timeout	
Azure's outbound connectivity methods	1. Use frontend IP of load balancer via outbound rules 2. NAT gateway to the subnet 3. Assign public IP to VM 4. Default outbound access use
Floating IP	To configure floating IP you need to add load balancer IP address in VM as a loopback IP.

Azure Application Gateway

Azure application gateway	Works at OSI layer 7 URL based / path based routing SKUs: ● Standard ● WAF ● Standard V2 ● WAF V2 V2 enhancement: **Auto scaling** **Zone redundancy** Static VIP mTLS Key vault integration Private link Performance enhancement Faster deployment and update time
Application gateway components	● **Frontend IP address** ● **Listeners (basic / multisite)** ● **HTTP settings** ○ Cookie based affinity ○ Connection draining (gracefully remove backend)

	● **Backend Pool** ● **Health Probes**
	An application gateway is a dedicated deployment in your virtual network. **Within your virtual network, a dedicated subnet is required** for the application gateway. TLS termination support at gateway, TLS cert is in PFX format End-to-end TLS encryption supported
Diagnostic logs	● **Activity Log** ● **Access log** ● **Performance log** ● **Firewall log**
Traffic Manager	
	Azure Traffic Manager is a **DNS-based traffic load balancer**. Traffic Manager routing methods: 1. **Priority** 2. **Weighted** 3. **Performance** 4. **Geographic** 5. **Multivalue** 6. **Subnet (get more info)** Nested Traffic Manager profiles: ● Minimum child endpoints
Azure Front Door	
	Azure Front Door:

	● Load balances requests across regions, routes the traffic via Microsoft edge network. ● define, manage, and monitor the global routing for your web traffic ● instant global failover for **high availability** CDN: caches content
Azure front door SKUs	● Azure front door: same as above ● Azure front door standard: combines front door and CDN ● Azure front door premium: combines front door, CDN and WAF
Azure front door standard	Define one CDN endpoint , one origin (i.e.) backend and one WAF policy while creating Azure front door standard. Providers below features: ● Global load balancing ● SSL offload ● Static and dynamic content caching/optimization **Origin group:** set of origins **Routes:** map domain and matching URL to origin group.
Azure front door premium	Additional features: ● Private link support ● Integration with Microsoft threat intelligence
Routing methods for backend	● Latency ● Priority ● Weighted ● Session affinity
When to use Azure Front Door	Is your app global? Do you wish to use CDN and WAF with your app?

Azure Firewall

Azure firewall	Fully stateful, built-in high availability
Azure Firewall Standard	**Allow/Deny Traffic on FQDN** **Allow/Deny traffic based on web categories** **Allow/Deny traffic based on FQDN tags (like allow windows updates)** **Outbound SNAT support** **Inbound DNAT support**

Azure Firewall premium	● **TLS inspection** ● **IDPS - A network intrusion detection and prevention system (IDPS)** ● URL filtering not just FQDN ● Web categories

Private Link

Azure private link service	Your own service powered by Azure private link. Service provider: 1. Create application to run behind a standard load balancer 2. Create private link service and attach it to LB 3. Share private link service ID/alias 4. Approve or reject requests. Service consumer: 1. Create a private endpoint by specifying private link service ID. 2. Configure DNS to point to the endpoint. 3. Connection approved/rejected. Alias: Globally unique name. Control service exposure: ● Role based access ● Restricted by subscription ● Anyone with alias

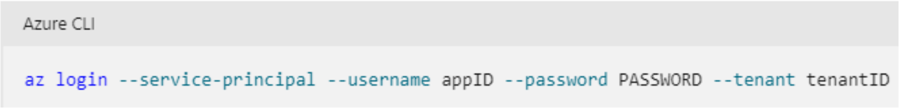
Azure Virtual WAN

Azure virtual wan	Basic: site-to-site VPN only Standard: full mesh connectivity
Azure Virtual WAN hubs	The classic hardware hub allows all network devices plugged into it to communicate directly with each other.

	hubs are automatically interconnected by hub-to-hub links
Azure Network Watcher	
	Verify IP Flow ● Check nsg rule, what is blocking traffic **Next Hop** ● Check if network routing is correctly configured. **Connection Troubleshoot** ● Combines Verify IP flow and next hop ● Specify source and destination VM, it will show nsg rule and routes **Effective security rules** ● What are effective rules at NIC for NSGs **NSG Flow Logs** ● What was allowed and denied at NSG, log it. **Connection Monitor** **Network Topology** **Packet Capture** **VPN Diagnostics**

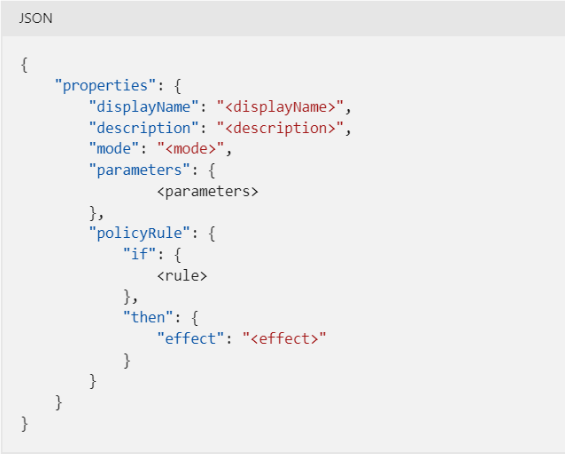
Azure Governance and AD

Azure Active Directory	
What is Azure AD?	An Azure AD tenant is a specific instance of Azure AD containing accounts and groups A Subscription in Azure can be considered as a logical container into which the resources and services can be created, configured, and installed. One tenant can have many subscriptions, but not vice versa.
Azure AD Licenses	Azure AD Free Azure AD Premium P1: dynamic groups Azure AD Premium P2: AD Identity Protection Pay as you go
Group	Types of group: ● Security groups: ● Microsoft 365 groups Membership types: ● **Assigned (static):** ● **Dynamic user** ● **Dynamic device**
Azure AD Connect	Connect your on premises active directory to Azure AD using Azure AD connect.
SSPR	Self service password reset: identify user before allowing password reset. Authentication method: Mobile app notification Mobile app code Email Mobile phone While enabling the SSPR you can select methods for authentication.
Azure AD role	Azure AD role **Global Administrator:** can elevate access by choosing Access management for Azure resources switch in azure portal. **User administrator** **Billing administrator**

Administrative units	Administrative units are containers for users and groups. Use administrative units to delegate roles so that the help desk administrator can reset password in his own region or branch.
Conditional access policy	Using Conditional Access, you can protect your applications by limiting users' **access based on things like groups, device type, location, and role.**
Azure AD Identity Protection	There are two risk policies: **Sign-in risk policy:** suspicious action that comes along with sign-in. (like sign in from unknown location/device **User risk policy:** unusual behavior from users after sign in.
Create and configure identities	Managed Identity 1. System assigned 2. User assigned Service principal: When you register a new application in Azure AD, a service principal is automatically created for the app registration. The service principal is the app's identity in the Azure AD tenant. Access to resources is restricted by the roles assigned to the service principal. There are two types of authentication available for service principals: secret or certificate.  Azure CLI `az login --service-principal --username appID --password PASSWORD --tenant tenantID`
Azure RBAC	
	RBAC control components:

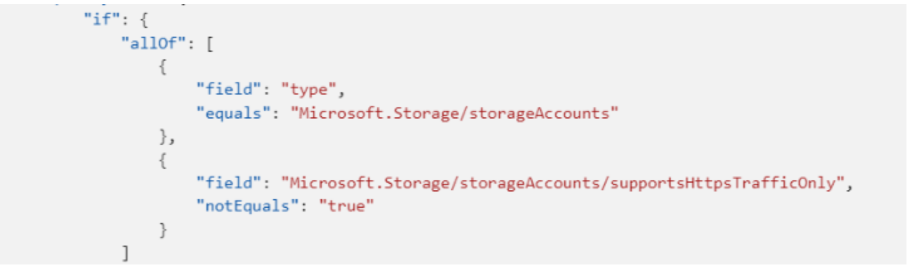
	● Security principal (who): user / group / managed identity / service principal ● Role definition: ○ Name, description, action, not action, data action, data not action, assignable scopes ● Scope: Management group → Subscription → Resource group → Resource

Azure Policy

What is Azure Policy?	Azure policy applies and enforces rules. Rules such as specific resources in specific regions. Azure policy evaluates your resources and highlights resources that aren't compliant or prevent noncompliant resources from being created. **Initiatives:** Group of related policies.
Azure policy in action	Implementing a policy: 1. Create a policy. 2. Policy assignment within a scope. Scope can be a management group, subscription or resource group. 3. Review the evaluation results
Policy definition	

JSON

```json
{
    "properties": {
        "displayName": "<displayName>",
        "description": "<description>",
        "mode": "<mode>",
        "parameters": {
                <parameters>
        },
        "policyRule": {
            "if": {
                <rule>
            },
            "then": {
                "effect": "<effect>"
            }
        }
    }
}
```

<table>
<tr><td></td><td>
<pre>
    "if": {
        "allOf": [
            {
                "field": "type",
                "equals": "Microsoft.Storage/storageAccounts"
            },
            {
                "field": "Microsoft.Storage/storageAccounts/supportsHttpsTrafficOnly",
                "notEquals": "true"
            }
        ]
</pre></td></tr>
<tr><td colspan="2">Azure Blueprint</td></tr>
<tr><td></td><td>Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:<ul><li>Role Assignments</li><li>Policy Assignments</li><li>Azure Resource Manager templates (ARM templates)</li><li>Resource Groups</li></ul></td></tr>
<tr><td></td><td>When the blueprint is assigned it will create a resource group, role assignment, policy assignment and resources through ARM template.

You can specify the name of the resource group, which user is assigned which policy and other variables at the time of assignment.

Main purpose is to build an environment which is within organizational compliance.</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

Messaging

Messaging services	**Storage Queue** **Service Bus**

	Event grid **Event hub**
Which service to choose?	Is it a message or event? **Message:** sending component expects something to be done with the message. **Event:** indicate something happened. No expectation about the action the receiving component takes.
Message: ● Storage queue ● Service bus queue ● Service bus topic	**Queue:** Store the message until the target is ready to receive them. Can use Storage Queue or Service Bus Queue. Service Bus Queue vs Storage Queue: **Service Bus Queue:** ● At-most-once delivery ● FIFO guarantee **Storage queue:** ● Queue will exceed 1TB **Topics:** pub/sub model. Multiple subscriptions for one topic. Can use **Azure Service Bus Topics** for topics.
Event:	Event: **Event grid:** Route event from one service to another. One event at a time. Below services can receive and handle events from event grid: ● Azure functions / webhooks / Azure Logic Apps ● Event hubs ● Service Bus / Storage queues **Event Hub:** (AWS kinesis) streams millions of events.
