Azure

Architecture :
- Data Security (Secure)
- Scale UP | Down (Efficient)
- Failures & DRs (Reliable) (out / In) (Resilient)

Scale-UP : Increase size of Current VM
Scale-OUT : " No. of VMs.

On-prem AD ← Azure AD Connect → Azure AD

Azure AD Can provide Conditional Access Policy (CAP) by group, location, device.

Azure AD B2C – An identity Mgmt Service.
Can connect to google, Facebook, LinkedIn.

RBAC → Secures resource access Mgmt
Users ← Roles → Resources

Azure AD PIM (privileged ID Mgmt): Manage, Monitor, & Control important resources.

Application Gateway :
Layer 7 LB + Web App Firewall (WAF)

NSG : controlls communication between VMs.

Azure Security Center : Free Service.
Works with App. Gateway & WAF.
Analyze logs realtime & Alerts.

Polyglot Persistence : Use different Storages (logs in blobs, Products & reviews in NoSQL, and User profiles in SQL DB)

Subscriptions & Resource Groups to logically Group / organize Resources.
Tags Can play when Resource relationship spans the boundaries of Subscriptions / RGs.

Load Balance Technologies
- Azure Traffic Mgr: DNS Load Balancing
- " App. Gateway: Layer-7 " " Ex: URL path routing
- " Load Balancer: Layer-4 LB. Between HTTP servers.

Solution / Application Architect :
- Deliver Business Value through Functional requirements of an Application
- Planning, design, implement, & ongoing improvements of a technology system.

Azure AD App Application Proxy: Extend legacy Apps available to access from cloud.
Two Components :
- Connector Agent on a Windows Server inside the Corp. network
- An External End point

Azure Storage Service Encryption (SSE)
- for data @ rest. 256 AES encryption
- for Managed Disks, Blob storage, Queues, Tables.

Azure Disk Encryption (ADE)
- for VM disk encryption
- BitLocker for Windows, DM-crypt for Linux

Transparent Data Encryption (TDE)
- for Azure SQL DB, Azure Data Warehouse

Azure Key Vault → for Secrets.

Azure Serverless :
- Functions
- Container : AKS & ACI
- Logic Apps – Microsoft Workflows

Azure App Insights → by installing small instrumentations Package in your App.

Azure log Analytics : Log ingestion & Iaas Monitoring

Activity Logs → Logs Activities & Changes.
Azure App. insights → Install an instrumentation on your app to collect & Track the performance

Azure DevTest Labs → Provides Automation Capabilities.

Azure Site Recovery : East to West replication of VMs in Case of DR.

Azure Backup Server / Agent → (Backup to) Recovery Vault

Function App.
- Code or Docker Container
- Runtime Stack: .NET, Node, Python, Java, PowerShell
- OS: Linux or Windows
- SKU & Size: Dev/Test, Prod, Isolated.

App. Service – Pricing Tiers
Dev/Test: F1, B1, B2, B3 (No Autoscale)
Production: P1V2, P2V2, P3V2

Azure Advisor → for optimization Recomm.
VMs, ExpressRoutes, Gateways, Unused Public IPs, Managed Disks Data Factory Pipelines.

Pricing Calculator: Estimate for Group of Resources.

TCO (Total Cost of Ownership) Calculator:
- Cost compare between onprem Vs cloud for resources.
- Can be used to evaluate cost of Azure before migrating to Azure.

✓ # Organizing Resources:
- Resource Hierarchy: Subscription (Billing & Mgmt) → R. Groups (Workload separation) → Resources
- Tagging: Cost Mgmt, Resource Mgmt, Automation
- Some Resources spread Across R. Groups & Subscriptions.

Azure Service Trust Portal: Audit reports for
- PCI/DSS
- SOC (Service org. controls)
- ISO 27001
- FedRAMP
- GDPR
- NIST

Compliance Manager: for Risk Assessments

Log Analytics VM Extension or Agent
- Sends data to Log Analytics WorkSpace
- Activity logs, Status logs, etc
-

Azure Advisor
- High Availability
- Security
- Performance
- Operational Excellence
- Cost.

Azure Cost Management
- Cost Analysis / Expenditure Analysis
- Budget Estimates, Alerts

Monitoring
- Monitor Metrics
- Query & Analyze Logs
- Setup Alerts & Actions (Respond & Route)

Audit & Compliance
- Legal & org. requirements

Monitoring:
- App. Insights: App. map, Smart Detection, Availability, Usage.
- Network Insights: Topology, Network Performance, VPN troubleshoot, Traffic Analytics.
- Integrate with Event Hub, Logic Apps, APIs, Webhook, ITSM, Automation Runbook
- Store Logs: Event Hub → to Storage Account

✓ # Azure Policy:
- Audit Environment.
- Enforce rules: Ex: Tags, naming, VMI
- Prevent resource creation
- Policy Assignment: To Sub → R.G. → Res. @ Any level.
- Compliance: Shows any resource that is not compliant.
- Initiative Defn: One or more policies

Identity Mgmt, Access Controls

Users, systems ↑ MFA, Delegation ↑

User → AC → Resources (VMs, Files, etc)

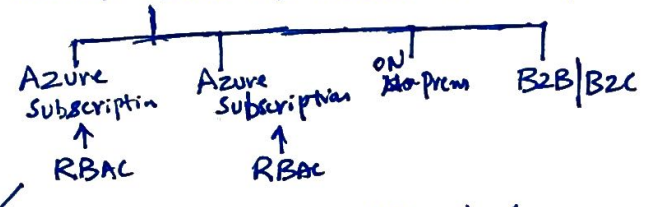
Azure AD Domain Service (DS)

- Managed AD domain.
- Integrates with on-prem AD
- Limitations: LDAP writes, Not all objects are Synchronized.

Management Groups. (New Azure Tool)

- Helps RBAC rules setup across multiple Subscriptions

* Microsoft Azure AD Tenant → Roles & Admins



* Azure AD Roles are different from Azure Subscription RBAC.
[like Authentication & Authorization]

* Azure AD Identity Protection

- Risky user
- " Sign-ins
- Risk Events → unfamiliar locations, Anonymous IPs, infected devices, etc
- Vulnerabilities

Azure AD Licensing

- Free: 500K objects, SSO for 10 apps
- Premium P2: PIM & AD Conditional Access
- " P1: AD Conditional Access; No PIM

Azure AD

- Authen. & Author.
- SSO - Device Mgmt - Self service
- B-2-B - B2C - ID protections
  (B2C: FaceBook, etc)
- Seperate B2B, B2C AD Tenant. + Link B2B or B2C AD Tenant to your Azure Subscription (or AD)

Resource Locks → Prevents Accidental Deletes

@ Subscription or RGs or Resources

* ① Can Not Delete ② Read-only

Managed Identities (Managed Services Identities - MSI)

- Assign identity on the Resource (ex: VM)
- Not all resources can be assigned or support AD Authentication.

Key Vault

- Secret Mgmt, Key Mgmt, Cert Mgmt
- Compliance with Fed Info. Processing Stans (FIPS)
- Setup Access policy (No RBAC)

Azure AD Conditional Access

- User/Groups - All or Few Apps
- Device State - Location
- Sign-in Risk - Client App (Web, Mobile)

Azure AD PIM (Privileged Identity Mgmt)

- Can do JIT (Just in Time) Access: To a role.
- Time Bound Access - MFA
- Access Reviews - Audit History

Azure AD Monitoring

- Security Reports
- Activity " / logs

Audit logs: 7 days for Free License / 30 days default
Sign in logs: 30 days default for P1, P2.
Not available for Free.

DBs

* Azure SQL: DTU
  - Basic: Backup 7 days, Storage <2GB/Pool 156GB
  - Standard: " 35 days, " <1TB/Pool 4TB
  - Premium: " " " <4TB/Pool 4TB
* Azure SQL: VCore
  - GP : 5GB-4TB, 1 replica
  - Bus. critical : 4TB, 3 replicas
  - Hyperscale : 100TB
* DB Pool: Add DBs to pool
  - Combine low utilized DBs & put them on a pool
* Scaling Considerations: on premium DBs
  - Read Scale Out: Read Replicas to distribute load
  - Sharding: distribute (identical structured data) across many DBs.
* Azure Data Factory (ADF)
  - Workflow driven Solution to Connect & move, transform data. ETL or ELT.
  - Connections & Linked Services → Data Set → Pipelines → Connections & Linked Services.
  - Code can put in GIT

Data Protection:
- Replication, Zone redundancy, Service redundancy (Farms, clusters)

Data Security
- In transit, Rest, In Use.
- DB Server-level Network Security.
  * Firewalls & Vnets (add them explicitly)
  * Private End Points
- RBAC: @ Mgmt Layer / Infrastructure. Not for Data in the DB.
- Azure AD: Extends AD Access to Data in the DB. Run Access SQLs on the DB.
- Dynamic Data Masking @ DB.Table.Field

A2 AD Access	A1 RBAC	A2 DB Data Access
↑ @ Network Layer	↑ @ Mgmt/infra Layer	@ DB Data/Table Layer

* Cosmos DB: Backups: 4 hours & 30 days retention
  - No SQL, Multi-model, Multi-Master, global distribute
    [Key-Value, Column Family, Document, Graph]
  - DB API options: * HMAC tokens for Access.
    SQL (Core), Cassandra, MongoDB, Gremlin
  - Throughput Units: 400 - 1000K RUs
  - Consistency Levels: Strong, Bounded-Staleness, Session, Consistent Prefix, Eventual
  - Replication: 10-20 fault Domains.
* SQL Data Warehouse:
  - Range from 100 DWU - 30K DWU
  - 60 Distributions. RPO: 8 hours. Snapshots: 7-days (Geo RPO: 24 hours)
* Azure Data Lake Storage (ADLS):
  - Bigdata: Petabytes
  - Throughput: Gbps
  - HDFS compatible.
  - Supports HDInsight, Hadoop, Azure Databricks.
* Azure Databricks
  - Tool to Analyze big data. Spark based.
  - Scala, R, Java, SQL support. (Notebook Language)
  - Uses Spark Cluster.
* SQL DB Data Replication / Failover:
  - Active Geo Replication @ DB level
  - Failover Group Geo Replication @ Server level
  - Asynchronous Process
* Azure Data Explorer:
  - Data Storage, Data Ingestion, Data Query/Analy
  - Compute & Storage like Databricks.

* Site Recovery (ASR) - DRaaS
- Primary Site → Secondary Site
  Backup & Recovery @ both
- RPO + RTO + RLO (Recovery level Objective → level of granularity of backups)
- App. Consistancy | Filesys. Consitancy | Crash consistency (5 minutes)
  ↳ on Windows VSS (Volume Shadow Copy Service), Linux pre/post Scripts
- Backup & Recovery of data upto 9999 recovery points
- Agents: MARS Agent
  MABS (Microsoft Azure Backup Server)
  VM Backup ~~Agent~~ Extension
  DPM (Data Protection Mgr) → On-Prem.

* High Availability (HA)
- Protecting from Faults & Outages.
- ✓ Scale Sets for VMs
- ✓ Failover for DBs
- ✓ A LB for Public availability or Traffic Mgr.
- Region Pairs (for HA) & AZs
- Fault Domains + update Domains
- Availability Set: 99.95% uptime for VMs
- A.Z. 99.99% Uptime for VMs
- Storage H.A.:
  Locally Redundant Storage (LRS)
  Zone (ZRS), Geo (GRS),
  Geo Zone (GZRS)
- ZRS is Sync replica

Recovery Services Vault (RSV)
- For Azure VMs (App, Web, DB)
- App. Consistent Snapshot Frequency: 1-12 hours
- RPO: 0-72 hours Retension
- Recovery plan: RTO for DB, App, Web
  Replication Group → Group DB, App, Web for an Application.
  Test Failover: Great tool to test.

Data Archiving: Blob - Life cycle Rule.

Frequently used Active Data	Less Frequent Inactive	Rarely used Archive Data
SSD	HD	Tap
Hot	Cold	Unused
Desktop	Shelf	Garage | Storage
Less Data	Mid Volume	More Volume
Speed Access 99.99	Mid Speed 99.00	Slow Offline

* HA - Connectivity
- LB: Layer 4 - TCP|UDP like http.
- AGW: " 7. Route URLs .. /images or /web + WAF.
- Traffic Mgr: DNS, Network Level).
  ↳ Geo Routing, Weighted, Priority, Performance, Multi Value, Subnet.

Azure

Azure Deployments

- Manual: Tenant & Subscriptions.
- Tool: Azure Portal (Manual), CLI | PowerShell, SDK, ARM API Rest Intfc.
- Infrastructure as a Code (IaaS) + Configuration Mgmt (Chef, Puppet, etc)

Azure Automation (like AWS CFT)

- Supports both on-prem & cloud (Azure/AWS)
- Runbooks: GUI, Python, PowerShell
- Automates Build of Resources
- DSC (Desired State Config): Force the Config during/after deployment.
  * Always wants Example 'tags', always wants certain plugin installed on VMs.
  * Deploy Compliances items/ softwares on VMs.

* Integration Migrations:
  - Messaging Patterns: Async
  - APIs: Sync

* Azure API Mgmt ~~Gateway~~ Service
  - API Gateway: Accept & route calls
  - Azure Portal: Config APIs, Policies
  - Developer Portal: API Docs, Test APIs

* Storage:
  - Block Level (iSCSI): Hardware level Storage; For OS. 0-4-1.
  - File Level (SMB, NFS): Example OS Filesystems Linux EXT4, Windows NTFS.
  - Object Level (Rest APIs): Unstructured Data Store. Backups & Archiving.

* Azure StorSimple: Hybrid cloud Storage solution.
  - On Prem Storage Device Connects to Azure.
  - Block Level Storage. iSCSI.
  - Similar to SAN

* Azure File Sync: Extends ~~File~~ Azure Files to On-Prem.

ARM Templates.

- JSON Syntax
- 3 Main Sections: Parameter, Variables (Fixed Values), Resources
  - Parameter: Selections/options like LRS, GRS, ZRS for Deployment
- Deployment is Incremental → only resources that are not exist/created will be deployed.
- Deployment Complete: Deletes resources that not in ARM Template.

Azure Migrations.

- Base (current) on Prem Arch. Vs Target solution Arch on Azure.
- Migrate: Data, APP, Config
- Migration Strategies:
  1. Rehost → Lift n Shift
  2. Refactor → Small design changes.
  3. Rearchitect → Major Arch changes
  4. Rebuild → Ground up on cloud.
- Server Migration: Microsoft & 3 party Tools
  * Assessment Tools: Cloudamize, Corent Tech, Device42, Unifycloud, etc
  * Migration Tools: → Carbonite, Corent Tech
- [redacted] DB Migration:
  * Assessment Tool: Unify cloud
  * No Migration Tools other than Microsoft.
  * Azure DB Migration Service: SQL Server
    - Schema only
    - Off-line Data
    - Online Data
    - Create Project only
- On Prem to Azure DB Replication then Migration
- Azure Import | Export: Using External Hard Drives.

Compute:

- HPC (High Performance Compute): Break complex job into small efficient processing units.
  Ex: Weather Prediction, Cancer Research, etc.
  Parallel Tasks & Tightly Coupled Tasks.
- Design Considerations:
  1. Minimize data Transfer.
  2. Efficient Memory Utilization.
  3. Parallel Task Execution.
  4. Use Cluster networking (e.g. InfiniBand, Single Route Input/output Virtualization ← SR-IOV)
  5. Storage like Parallel File Systems (HDFS, PVFS)
- Just in time Access for VMs
- ✓ Azure Batch (Similar to EMR!
  * Tasks & Worker Nodes.
- VM Series:
  HB → High Memory. Weather Modeling, Fluid dynamics
  HC → High Compute. Molecular dynamics, element Analysis
  N → Graphics, AI
- Placement Groups are new in Azure.

Network Infrastrure Design Considerations

- Route Presidence:
  * User Define Then Express|BGP Then Default.
  * VNet ① → Route Table → Sub Net
    Route Table ② → Sub Net
    → Sub Net

SubNet ← NSG ③ → Inbound Rules + Priority
SubNet ← → Outbound Rules + v
NIC

Order for Inbound: SubNet then NIC
Order for outbound: NIC then Subnet

- Service End Points:
  Vnet/Subnet to Managed Services or Storage
  Connection bypass Public Internet & Use Microsoft Backbone.

Compute Hosting Models

- VMs
- App. Services
- Containers

Compute options

- Monolithic
- Microservices (App. Service)
- Event-Driven (Azure Functions)
- Full fledged Orchestration (Kubernetes, ServiceFabric)

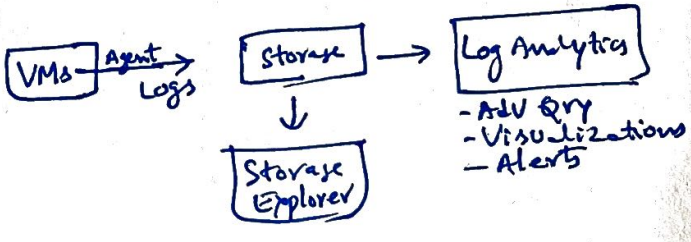
App. Services:

- 99.9

Azure Functions: Serverless. Ideal for APIs

- C#, Java, JS, F#, Python
- Default: Cold Start. Option for "always-On"

- Default No Vnet: for Containers, App Service as they are managed Services.



Azure Monitoring

VMs

- Three Agents
  1. Azure Diagnostic Ext : Events, Sys, Perf, Trace → Sends to Storage, Az Monitor, Event Hub
  2. Log Analytics Agent : Events, Sys, Perf
  3. Dependency Agent → Network Connects

  (2 & 3 Sends to → Az Monitor)

Containers:

- Log Analytics Agent on Container OS.

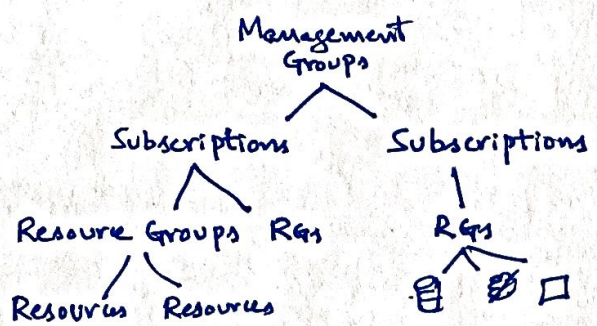
DBs:

- Azure SQL : No Agents.
  Azure SQL Analytics tool.
- SQL Server : Microsoft Monitoring Agent (MMA)
- Cosmos DB : No Agents. Azure Monitor.

Custom Apps:

- Instrument Using Az Applications Insights

Organize your Azure Resources:



- Mangmt Groups → Access, Policy, Compliance for multiple Subscription
- Subscriptions → Manage Costs

Azure Blueprints → Cloud Architects to define a repeatable set of Az Resources. Patterns.

Azure Policy → Enforce rules on Az Resources.

Az Security Center → Unified View of Security across Az workloads, Provides Actionable items.

Manage Access:

	Reader	Contributor	Owner
Subscription	Observer	Use Resource / Manage	Admin
R.G.	Observer	Use / Manage Resource	Admin
Resource			

CICD pipeline → with Azure DevOps Projects

Az Migrate: Assessment & Migration

Az Site Recovery: DR & Migration

Az Database Migration Service: Many DBs to Az data platform

Data Migration Assistant: Helps in upgrade DB. It detects Compatibility issues

SQL Server Migration Assistant: Automate DB migration from DB2/Oracle/MySQL to SQL Server

Database Experimentation Assistant: New A/B solution for SQL Server upgrades.

Cosmos DB Data Migration Tool: JSON, CSV, SQL, MongoDB, Az Table Storage, AWS DynamoDB to Cosmos DB.
