AZ 301 → 304 Solution Architecture Design.

- Compliance
- Identify Requirements:
  - ↳ accessibility — color blindness and other considerations
  - availability — 4 9's options 99.99. → Redundancy sol^{n} is 1st choice.
  - Capacity planning and scalability (dynamic) → Azure Site Recovery Capacity Planner
    - → Azure Migrate
    - → PaaS Manual & automatic scaling
    - → IaaS ← Load Balancers
      - Virtual Machine Scale Sets
    - → Azure Batch.
  - deploy-ability → DEV → TEST → PROD
    - LOW EFFORT
    - — Publish from VS
    - — Azure Pipelines + CI/CD with GitHub & others.
  - configurability
  - governance
  - maintainability
  - security
  - sizing

↳ ability to support app in different configurations in different environments

No hardcoded strings only configs

PaaS → Set app variables inside azure from Web config
- → Deployment slots with own variables
- → Key Vault — Secrets keys and certificates

↳ control mechanisms to ensure only authorized changes are made.

- Azure Policy, RBAC, Azure Pipelines
- Company process to track and approve changes.

↳ ability for an app to be maintained by people other than original developer.

- Diagnostics : Extract log files
- HDInsights, Azure Monitor (Dashboard) similar to Splunk

↳ authentication, authorization, defensive security; preventing attacks etc.

AAD Azure Active Directory → Identity as a service

RBAC, Azure Advisor

↳ predicting how much resources needed to run and optimized over time.

Azure Monitor Cloudyn

Cost center

Azure Advisor Eg: Reserved Instances

Hybrid Benefit for Windows or existing SQL Server license.

Autoscale, Serverless, MS

Az 304

ARM template →

Files downloaded:
- template.json
- parameters.json

} zip

Elements:
- Schema
- Content Version
- api profile
- parameters { },
- variables { },
- functions [ ],
- resources [ ], ⊛
- outputs { }

Template format:

```
JSON
{
"schema"
  :
}
```

Expression is within [ ]

Template section of Azure Portal ← Add to Lib. / Deploy

- Under Portal there is the ARM model which it prepares and executes.

Psw protection

Template.json

adminPassword: { "type": "secureString" }

Parameters.json

value will appear as (null)

resources [ ] array: Each resource represents on this array depicts one resource being deployed in Azure

Eg: VM creates 6 or 7 resources like NIC.

dependencies "dependsOn": [array]

properties of that resources.

⊛ Some imageReference eg. Windows 2016 Datacenter may be hardcoded in template itself not in Parameters.

⊛ During deployment via ARM template Resource Group is not filled because R.G is not part of deployment file because Azure does deployments inside of a resource group so RG pre existing is a required condition.

- We can go back to deployment log of any RG and download template from there.
- If you redeploy same resources with same parameters it is iterative (Redeploy) (no error)

DSC Desired State Configuration. (Configuration Drift: avoidance)

- Update action in Activities
- Automation Account → Runbooks

Azure Express Route

- Layer 3 connectivity (address level) - Point to point any to any network or - virtual cross-connections through Exchange
- Build in redundancy (highly available) Primary & secondary.
- Connectivity to Microsoft cloud services. (Not needed for Office 365) through available.
- Across on-premise connectivity with ExpressRoute Global Reach.
- Dynamic Routing using BGP Border Gateway Protocol.

Models:
- cloud exchange co location
- Point to point Ethernet connection
- Any to any connection.

* Even here DNS queries, certificate revocation list checking and Azure Content Delivery Network requests still sent over the public internet.

Peering Schemes:
1) Microsoft peering
2) Private peering — resources must be located in one or more Azure virtual networks with private IP Addresses.

Steps:
1) Create Express route circuit
2) Send service key to Provider → may take several days to enable
3) Create a peering configuration
4) Connect a virtual network to an expressRoute circuit.

Gateway type → ExpressRoute

* Upto 10 virtual networks can be linked to an ExpressRoute circuit
- these virtual networks must be in the same geopolitical region as ExpressRoute circuit
- Single virtual network can be linked to 4 ExpressRoute circuits.
- 2 connections by default to 2 different Microsoft Edge routers.

ExpressRoute Direct - ultra high-speed dual 100 Gbps connectivity

Fast Path - send network traffic directly to a Virtual Machine (the intended destination) Bypass VN and improve performance.

Azure AD

- Azure AD Domain Services : Domain join, group policy, LDAP, Kerberos/NTLM auth.
  ↳ no need to manage, patch or service domain controller in cloud.

Enterprise State Roaming : Enable AAD > Devices > Enterprise State Roaming

- AAD > Identity Governance > terms of use
  ↳ Entitlement management
  ↳ Access Reviews
  ↳ Privileged Identity Management ← (Read)
- AAD > App registrations
- MFA with conditional Access
- Domain joined used for Azure seamless Single Sign-on
  ↳ on premise Windows Server Active Directory.
- ✱ Pass-through authentication (PTA) and single sign-on
  ↳ use same on-premise password
  ↳ no password hashes stored in the cloud.

✱ Also read difference with Federation (AD FS)

- Password Writeback : to keep on-premise Active Directory passwords in-sync with passwords in the cloud.
- Caching Rule : Configure Azure MFA to set a time period to allow authentication attempts after a user is authenticated.

✱ Check Protocol diagram of MS Identity platform and OAuth 2.0
  ↳ Required: tenant, clientId, response_type, redirect_uri, scope

- Azure Confidential Computing : Encrypt data at rest,
  Trusted Execution Env. enclave
  Stops malicious insiders with admin privileges.
- Secure transfer required setting for storage account <=>

  Set-AzStorageAccount -Name <> -RG <> -
  EnableHttpsTrafficOnly $true.

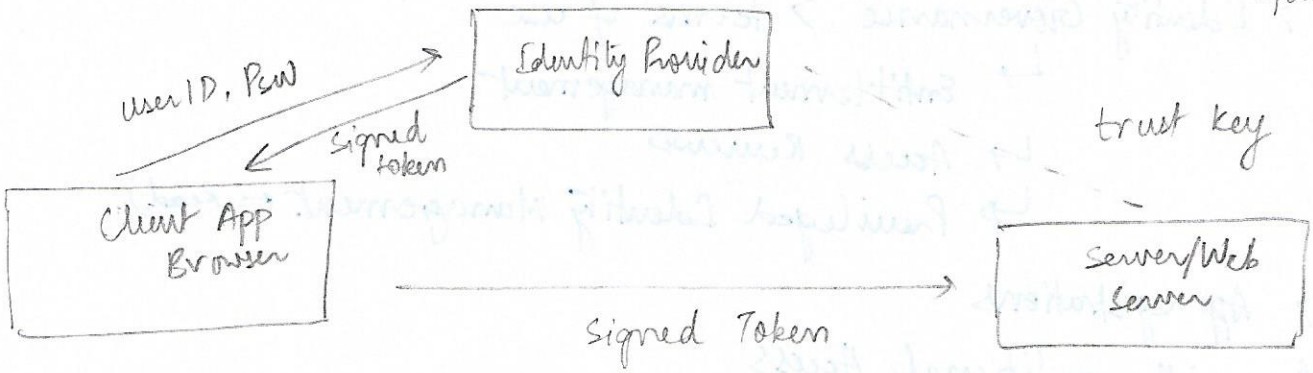
↳ Identity as a service

Azure AD is not the same as Active Directory as it doesn't provides same services as on premise AD

↳ Traditional Active Directory does not work with Internet Protocols.

↳ uses LDAP, Kerberos etc.

↳ SAML, WS Federation, Open ID



- Adding custom domain name → need to verify
- Users → Add roles → RBAC — sign in policies
  ↳ Previlage Identity Management.
- Identity Protection < user risk policy
  sign in risk policy

Self service Password Reset (SSPR)

Conditional Access Vs MFA

Fraud Alerts — allow users to submit fraud alerts
↓
code to report fraud report.
group user or admin & Email Address

- Single sign on — users already logged in can log in seamlessly.
- Pass through authentication — on prem AD always doing the authentication.

Health and anylics is imp to check connection.

Password reset on prem integration.

- Standard SKU Public IP Address
- IP Address range calculations.
- Azure Route tables

CIDR notation. smaller the no. more no. of addresses reserved.

first 4 are reserved by Azure. (5) x.x.x.0 – xxx.3 and last address of subnet.

Invalid IP ranges:

224.0.0.0/4	Multicast
255.255.255.255/32	Broadcast
127.0.0.0/8	Loopback
169.254.0.0/16	Link-local
168.63.129.16/32	Internal DNS

- Smallest supported IPv4 subnet is /29 and Largest is /8
  IPv6 must be /64

⊛ Imp. SLAs

Single VM — 99.90%

2 VM SS — 99.95% VMSS doesn't bound to any SLA as official

Application Gateway — 99.90% for 99.95% get two Gateways.

SQL DB all 3 Basic, Standard and Premium uphold 99.99% SLA

Azure SQL Database Business Critical tier SLA

Configured with Geo replication has a guarantee of

RPO Recovery point objective of 5 sec. for 100% deployed hrs

RTO Recovery time objective of 30 sec. for 100% dep. hrs.

Networking Limits — Azure Resource Manager:

Virtual N/Ws	1000
Subnets / Virtual NW	3000
Vnet peerings / VN	500
VPN Gateways / VN	1
+ ExpressRoute Gateways / VN	1
DNS server / VN	20
Private IP address / VN	65,536

LOAD BALANCERS

	Basic	Standard
Load Balancers	1000	1000
Rules / resource	250	1500
Rules / NIC	300	300
Frontend IP configs	200	600
Backend pool size	300	1000 IP configs single NIC
High availability ports		1 / internal Frontend
Outbound rules / LB		600
TCP idle timeout		4 minutes / 30 minutes

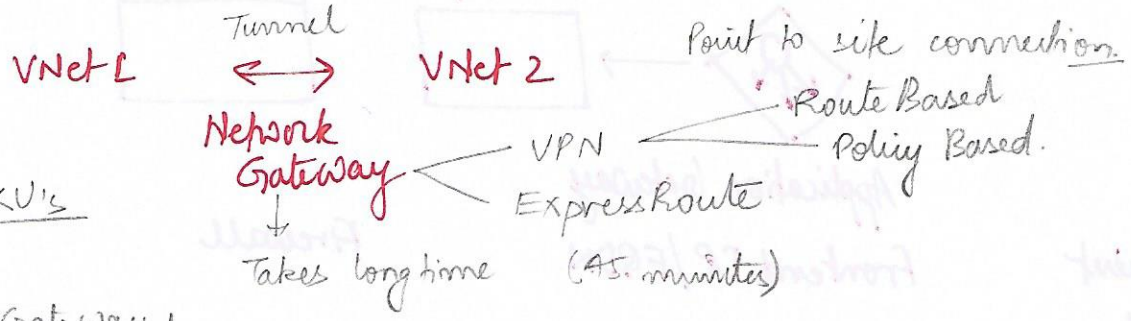
VIRTUAL NETWORK

CIDR notation
IPv4 addresses

- atleast 1 subnet is required in a VN
  10.1.0.0/24 ↓ smaller subset of IP Addresses
  10.1.0.0/25 i.e. half or 10.1.0.0/26 1 quarter

* Any special service such as Bastion Host, DDoS protection or Firewall runs on its own subnet. So you will need a seperate subnet.

* There is no Virtual Network to another Virtual Network connection. So device connected on one VN would not communicate to 2nd VN by default.



1. Create VNet Gateway 1
2. VNet Gateway 2
3. Connect 2 Gateways → Add connection.

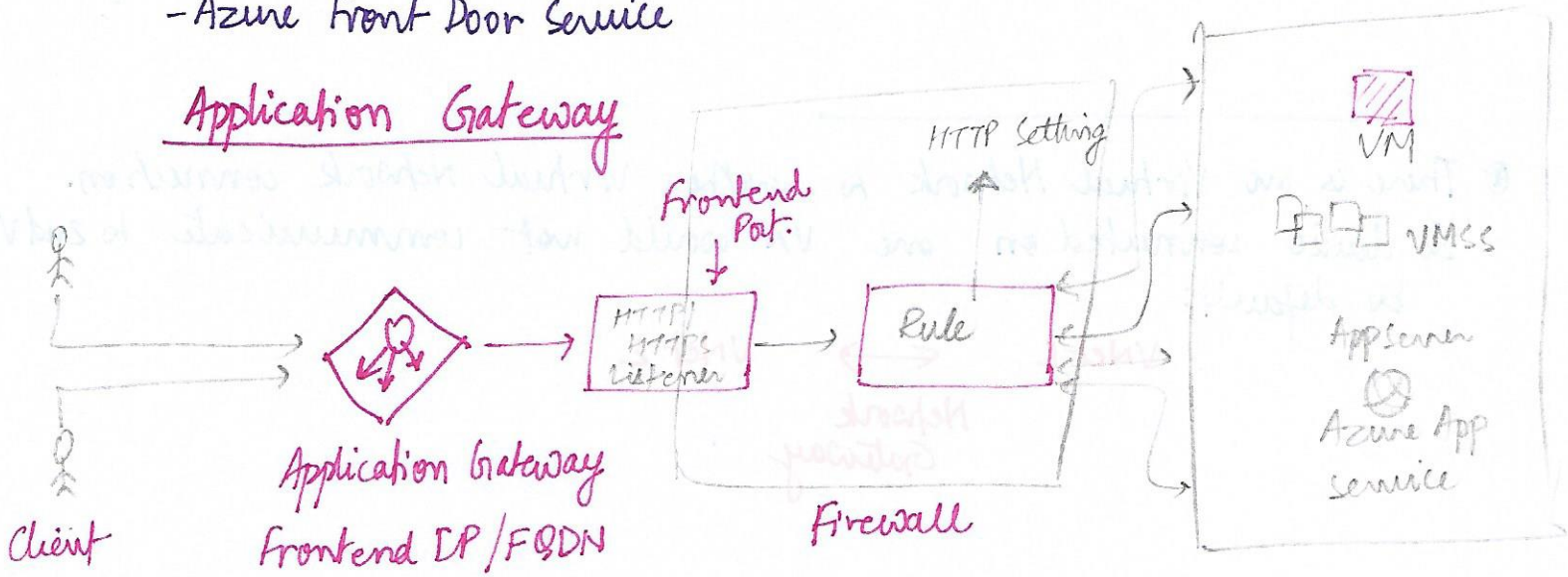
2. Another way is Vnet Peering. → 2 way connection or 1 way connection
   ↳ charged for data transfers
   ↳ Fowarded traffic

Azure Application Gateway:
↳ Backend port settings

Load Balancing

④ things – Load Balancer
– Application Gateway
– ATM Azure Traffic Manager
– Azure Front Door Service

Application Gateway



1) 1st resolve the domain name of App/12 gateway using DNS server. Azure controls DNS entry because all app/12 gateways are in azure.com domain.

2) Azure DNS returns the IP addresses to client which is the formatted IP address of the app/12 gateway.

3) App/12 gateway accepts incoming traffic on one or more listeners. Listener is a logical entity checking for connection requests. Configured with frontend IP address, protocol and port no.

4) If a WAF (Web App/12 Firewall) is used the app/12 gateway checks the request headers and the body if present against WAF rules.
to determine if a request is a valid request or a security threat.

If valid request, it is routed to the backend.

WAF prevention mode blocks requests.

Managed Data Advantages:

- Built-in High availability
- Auto-scaling
- Threat detection
- Auto tuning

OLTP – Relation DB
Lift and shift ↑

Data Strategy

Data Auditing and Caching:

- SQL Database tracks events to an audit-log
- Written to append blobs
- Server level vs database level auditing.
- Azure monitor can inject those logs and alerts.

SQL Server system function.

DTU Database Transaction Unit
↳ A relative measure of performance.

Cosmos Pricing:
Provisioned Throughput ← multiple writes per 100 RUs — Request Units — 0.016/hr
single write / 100 RUs — 0.008/hr

SSD Storage — 0.25 GB/month

Data Retention Strategy

- Automatic geo-redundant backups
- Configure from 7 to 35 days
- Long term retention policy – upto 10 years.
- Restore deleted database / Restore to another region.

Data availability, consistency and Durability
↓
Removing single point of failure. (Replicate copies)

Azure SQL Database SLA

Azure SQL Database Business Critical tier with geo-replication:
- RPO Recovery Point Objective — 5 sec for 100% deployed hours
- RTO Recovery Time Objective — 30 sec for 100% deployed hours.

Data Warehouses ⟶ Azure Analysis, PowerBI, Big Data

- used for analytics
- not used for transactions
- doesn't support updates, deletes

Data Geo-Replication

- Geo-redundant storage (GRS) ⊗ multi-master DB

Data Encryption:

Encrypted at Rest — TDE — Transparent Data Encryption

Data in transit — SSL — Force SSL connections

Always Encrypted: never unencrypted unless arrives on yr machine.
↳ client decrypts

Dynamic Data Masking: credit card no. etc.

Scaling

- Small downtime when server switches
- manual not automatic
- read scale-out

Database sharding

Azure Data Box

Data Box: 100 TB, 70 TB usable capacity after RAID 5 protection
50 Lbs
10 GBps Data transfer interface.

Data Box Heavy: 1 PB raw capacity. 770 TB usable capacity
500 Lbs weight
Cannot be rack mounted
40 Gbps data transfer interface

Components:
1) Data Box Heavy Device
2) Data Box Service
3) Local Web user interface (to connect to local Network)

Data Box Disk: 1-5 Solid state Disks
Each 8 TB encrypted disks SSDs
Configure, connect and unlock disks via the Data Box service in Azure Portal.

- Uses a USB 3.0 connection to move upto 35 TB of data in less than a week in cost effective way.

AES 128 encryption all the time.

Virtual Networks

- You cannot reserve a private IP address for a VM to be created at a later time.

Can you manually assign IP addresses to NIC's within the VM operating system. → YES

Update Management

- consistent control and compliance of a VM with Update Management.
- Requires Log Analytics and Automation Account. (Same region)

Multi Factor Authentication:

* Available only for Azure AD users not for guest users.

Conditional Access:

One time pass — Safe / Secure location 300 sec. window
Fraud Alert — Blocked user list — 90 days block by default
Verification methods. 5 ways
Role Based Conditional Access.

* Custom Roles: Not available on Portal.
  Create using Powershell or CLI — Copy JSON & edit.
  Powershell Samples on GitHub. { Combine different roles and assign.

WebApps using PaaS

Create an App Service Container App
Quick Start, Azure Container Registry, Docker Hub, Private Registry.
- no free App Service Plan in Linux

Deployment — No multiple options for deployment.
Azure DevOps option.

Web Jobs — Run scripts or programs as background process
Background jobs. scheduled cron job. Powershell script or any specified executable.
.cmb .bat .exe .ps1, .sh .php .js .jar

Web App can time out after 20 minutes of inactivity.
Only requests to the actual Web App resets timer
→ enables Always On Web Apps.

Patterns of Autoscaling

1. On and Off
2. Adding resources
3. Unpredictable autoscaling
4. Predictable autoscaling.

Azure Automation.
↳ Import script, edit and run

Azure Migrate

- Host of migration services and estimates about migration
  - Server assessment
  - Server migration
  - Fill out CSV file
    - ↳ Download a VM image (.OVA) to set up application or
    - Download the zip folder (.zip) with Powershell script to run on existing VMware Virtual Machine

Azure Recovery Service Vault.

- Region is important as you should put the recovery service vault in the same region as Resources.

only 2 functions < Backup
Site recovery or Replication — copy so storage is needed.

Soft Delete

↳ Properties > Security Settings > Soft delete enable/disable
Backup is retained for 14 days after delete

Backup can run on on Premise
Policy Backup Freqeuncy. (Daily default) but limit is then