**70-534 Architecting Microsoft Azure – Udemy**

Check latest exam requirement objectives consistently.

**Study Plan:**

How many hours am I going to give to this each week? GMAT/School/CCNA. Don’t start and have a break. Keep going. Don’t cram.

Create a study plan, $165.00 per exam. Exam can be proctored from home. 2 and a ½ hours with 40 questions. Look at latest test changes. Changes frequently. 1 month of dedicated studying. Official book from library and study test were not the best. One week of extra buffer.

Scenario questions. Different question types. Focused around hybrid solutions. Some vague questions. Fair test.

**ASM (Azure Services Model) – classic portal vs Azure Resource Model (ARM)** – newer portal with deployment model. Some things you can not do and some things are not easier in either portal. Default will be the new portal. Slowly migrating off the old portal

ARM templates/ARM backups were recently added. UDR (User Define Roots, Application Gateway, Azure Storage encryption, Azure Disk Encryption, SQL database TDE, Azure Scheduler,

**Network Services – Objective 1:**

**GFS (Global Foundation Services) called MCIO (Microsoft Cloud Infrastructure and Operations) Datacenters:**

Azure is all over the globe. Products are a ton.

**HA** – architected to stay up and running. 99.999% availability uptime. Two or more VM’s in a set are 99.95% availability. 10% credit or <99% is 25% credit.

Datacenters support all of Microsoft’s online businesses. Large as 3 cruise ships. Over 100 datacenters in 30 regions and 11 geos. NA, EU, AS, SA

Geo is a country but larger than a country. China region is special as a china company runs the datacenter. Needs a separate Azure subscription.

Region are paired with other region. NA/SA for example. DC’s are updated only one pair at a time. Regions don’t support all resources. Australia DC is only available to them. Same for India. Keeping data in region. 300 miles between DC.

**Triple Redundant storage** – 3 times replicated in that region. Or can elect up to 6-times and across geos. Brazil is paired with US in one instance. Pairs are in same geo for data protection laws.

**Racks** – servers are arranged in groups. Two blades per 1U. Height total of 52U. 96 servers on a single rack which would be 48U. JBOD (Just a Bunch of Disks (up to 60GB). 20 racks make up a cluster.

All pre-wired. Clusters have the same hardware. Cluster can have close to 1,000 servers.

**ITPAC** – container of servers, built as one unit and shipped to a Microsoft datacenter for plug and play

Water, power, electricity

**Active Directory:**

Identity, Roles, and Permission, Company directory, Password Policies

**AD DS** – Domain Services, employees log into windows

**AD LDS** – light weight domain services

**AD CS** – Certificate Services, PKI (Public key Infrastructure)

**AD FS** – Federation Services with SSO

**AD RMS** – Rights Management Services, protect documents

Not a replacement for on-prem AD. Azure

Azure AD is there to extend AD from on-prem AD to cloud. Identity management centered, no hierarchical object model. Basic Service. Dynamic or Static IP’s

No private IP to VPN. CNAME records can be used to point your DNS to the Azure domain. A record for DNS model. 4096 private IP per VNET, 60 public dynamic IP’s, 20 public static IP’s first 5 are free and .004/hr. 500 VM per VNET. 50 VNET

ACL’s are for endpoints not vnet/subnets. NSG (Network Security Groups), powerful than ACL. Blacklist IP’s with ACL. You can have up to 50 ACL per endpoint. Ordered rule by priority. Packets get filtered before reaching the VM. Doesn’t take CPU cycles

NSG contain ACL rules. Can be associated with vnets, subnets, or VM’s. NSG ACL applie to the VM inside the subnet. Can only be applied in region. Have priorities

**Resource Groups:**

PaaS started here. Added IaaS later.

Operate groups of VM’s at once. Can’t nest groups, resource can be part of one group

No limits to resources. Can’t rename.

**IP addresses/User Groups:**

Routing tables can be created. VPN through S2S VPN. Or blackhole loops.

These have to be defined and not automatically done.

**Azure Compute:**

Web, worker, VM role.

App Service:

* web apps (shared/dedicated) managed. Any language, powershell, etc. continuous integration
* connect to other platforms, HA, security, application templates, Streamlined visual studio
* mobile apps (IOS, Android, HTML5). SSO. Azure AD FS. Build offline ready apps, push notifications, autoscale, staging environments, continuous integration
* api apps (migration of existing API). CORS (easy consumption, protocol to talk to each other over domains). Access controls, integration with logic apps, integration into visual studio.
* logic apps (build workflow logic). If this, then that. Zapier, IFTTT, can be designed in browser, templates

A0-A4 (extra small to extra large)

A5-A7 – Larger databases memory intensive

A8-A9 – network optimized (messaging)

A10-A11 – compute intensive.

D Series: SSD

* D1-D4 – websites
* D11-D14 – memory intensive

Dv2 Series:

* SSD
* D1\_v2- everyday applications
* D11\_v2-D15\_v2 – large database

Cloud service – PaaS. You can install other things on this VM. Remote in.

* Web role – public endpoint, IIS, HTTP & HTTPS
* Worker Role – No IIS, No public endpoints, computation/data management. Background jobs.
* Perform tasks. Communicate between messaging queues. Configuration set up with instances.
* Don’t create VM. VM is created by configuration file. Updates switchover instances.

**VM role:**

Multiple predefined images. Windows Server 2012 R2. Looks like a physical server. OS running in a VHD. 400 + options for Linux. Computers/applications.

VM sizing:

Basic vs standard. Compute intensive. Price is a factor.

A-series – general purpose. Optimized to run at high performance

D-series – designed for Performance. SSD, Faster processor and memory

DS-series – premium storage instead of temporary storage. Same pricing to Dv2

Dv2-series – more powerful. 33% faster. Premium storage (faster io access)

G-series – memory intensive application, faster processor and more disk space, 2 time memory, 4 times on storage. Premium storage. Graphic processor

Basic tier doesn’t have load balancing, etc.

**Availability set** – two or more VM’s running under a load balancer

**Fault domain (FD)** – rack of servers. Entire rack of servers fails the whole rack is affected

**Update domain** – define grouping of servers that can be updated as a set. Can be updated individually and doesn’t bring the application down

**VPN & Express Route:**

Connect to a network remotely. Encrypted traffic. Secure tunnel. Connects to offices together but needs a gateway on both ends

P2S (Point to Site) – dev on a database with only one person needing access. To be able to use it as it is local. 100 Mbps, 200 Mbps. Uses SSTP protocol.

S2S (Site to Site) – entire network can be connected to Azure. Hits the Gateway first. Speed Is limited. 100 Mbps. Performance sku only offers 200 Mbps. Outbound has cost associated with it. IPSEC or RRAS

ExpressRoute – More expensive. Doesn’t use public internet. Private fiber connection. IXP by ISP. A lot faster. 500 Mbps, 1 Gbps, 2 Gbps, 50,000 a month. Servers could be hosted at the IXP. Another is MPLS. Cost more with multi locations. Know the differences between P2S, S2S and Express Route

**Azure Services:**

Cisco CSR at the marketplace with 4vNIC. Apache, PHP, Linux options.

Know all the servers in terms of networking like VPN, S2S, Express Route.

Load Balancer: spreads the load out to other servers within the pool.

Round robin – cycling through the servers one by one. Monitors every 15 seconds.

Sticky session – same server responding to the user. Single point of failure

Vertical Scaling – increasing resources up.

DNS resolution points to the public IP of the LB.

Internal Load balancers – access services behind the scene. NAT with the internal load balancers to help security.

Application Gateway: Web based LB – HTTP/HTTPS. Firewall option. Cookie based affinity. SSL offloading. URL routing. Can have the same websites behind the LB. Application matched to more than 2 VM’s. LB operates at layer 4. Site behind the actual LB

Traffic Manager – same application can run in different regions across the globe. Helps reduce latency. DNS local. DNS points to traffic manager. No global DNS in this case. Refresh of information in the cache. Checks on the health of the locations. Couple minutes if a node fails to revert to the failover instance. Does support round robbin. Primary/Secondary. Global/region routing of traffic. Nested profiles allows you to point one top-level traffic manager profile to another traffic manager profile to combine two different load balancing methods.

**Azure Media Services:**

Ondemand streaming media services. Live events. Cloud based encoding. Upload video content and encode in multiple formats at scale like DRM and CDN.

**Azure CDN:**

VM to send static content that are closest to the user. Video/images/audio/css/js. Distribute files closest to the region as well. Increases performance of application by distribution CDN places static content closest to it’s users.

**Azure AD:**

Manages user access/identify management. Tying in corporate AD. Identity management of users. Multi-Factor like RSA.

**Microsoft Reddis Cache:**

High data store. Doesn’t have information stored in the database. Basic, Standard or Premium. Databases can be split into different databases. Temporary information or information that is searched through frequently. Sits in front of the database or in front of the Load balancer. You can also have the cache on the web server if needed.

**MultiFactor Authentication:**

Phone based authentication methods. SMS/call. SDK methods to build into your application.

**Azure Service Bus:**

Messaging platform to send messages between applications. Disconnected communication between applications like a cell phone.

Assignment 1 – create a virtual network, not public available. Add two basic web VM’s in available set. Configure point to site VPN.

**Secure Resources – Objective 2:**

AD as a secure option. AD Connect or DirSync

**Managed Identities:**

Azure AD. Multi-tenant cloud based identity. Keep users not seeing users from another company. SaaS model. IDMaaS – Identity Management as a Service

Handles 5 million organizations with this detail. 1 billion authentications every day. 1 Trillion authentications since Azure AD was put in place. To work with user applications. SSO and multi-platform support and multi-factor. 99.9% uptime.

Graph API:

Allow developrs to build web and mobile apps. REST API and can integrate with any API

CRUD, Customize, Read, User, Delete. JSON. All over HTTP. Need an authentication token. Query functions. Check changes between two time periods

OAUTH/OPENID – Opensource for authentication with untrusted clients. Trusted client would be a server. Untrusted is like a phone. Requires token. Can expire. Can be integrated into the backend network

**Hybrid Identities:**

Many environments have onpremise and in the cloud. Identity for all applications no matter where the infrastructure resides. Security, cost savings, legacy apps, requirements.

SAML claim. (SAML – Security Assertions Markup Langugage). Proof of their identity. Tokes are signed. First, requests SAML token. Issues token to client along with proof key. Provider signs token. Customer needs to sign the token via proof key. Application now trust its

Azure AD FS:

Federated identities. Turning over responsibility to a third party. AD FS passes it onto your AD. Avoids DirSync. Can keep all your identities in your managed premise.

AD Application proxy:

SSO for remote employees. Allowing access inside and outside your network. Not a vpn. Authenticates through the proxy and the proxy gets in your local network. Have to install a connector inside the network. All traffic goes through Azure. AADSync, DirSync, and Azure AD Connect are ways for synchronizing onpremise to Azure AD

Azure ACS:

Azure Access Control Service. Enable multiple identity providers. Identity provider choosen. Each provider has their own security token. Intermediary that does the work for you and deals with the external providers. Google, Facebook, Yahoo, OpenID, Azure AD, Twitter, Microsoft. Azure w/FS. App sends the user to authenticate. Provider responds with token. Client sends the token to ACS and coversits it. Sends it back to the app.

ASP.NET coding:

.NET Framework can provide the code to work with ACS but code is different for different providers. Active Directory B2C – cloud identity management solution for consumer facing web applications

Data Security:

NSG (Network Security Group) – virtual firewall. Define outbound and inbound rules. 5 elements – Protocol, Source IP, Source Port Range, Destination IP and Port. Can have multiple NIC’s or subnets. Each subnet can only have one NSG. Lower numbers take priority. Traffic within network, outbound and load balancer allows, deny all other traffic.

Data in transit:

SSL/TLS:HttpS must be used. Client side encryption. VPN is another option to encrypt traffic crossing the internet or S2S/P2S. ExpressRoute doesn’t travel the internet. Azure Rights Management – service that encrypts sensitive files and data. Provides ways to access that encrypted data for authorized and authenticated users.

Data at rest:

Azure SSE (Storage Service Encryption). Automatically encrypts data and decrypts. 256-bit AES. Block blobs, page, blobs and append blobs only works here. ARM only, not classic. Client side encryption. Encrypt disks used by VM’s.

Azure Operations Management Suite:

Security audits. Dashboard style interfaces. Helps to know a real operations center can map VM’s too. Visualization tool. Detect threats, monitor network, mitigate damage.

RBAC:

Don’t give everyone admin access. Abstraction of access control. Owner, contributor, reader standard roles. Can have custom roles. Subscription can only belong to one AAD. Same for resource groups and resource’s belong to only one group. There are limits to at the resource level. Contributor can’t change security but everything else. Inheritance does exist. Can’t give access to others.

Assignment #2 – Create a user, assign that user to a role, and grant that role access to a resource. Datacenters are no longer a requirement on the test.

**Azure Data Storage**

Table Storage:

NoSQL, no schema, structured, not RBDMS, name value pair metaphor. Rows are entities and can have up to 255 properties. Partition Key and RowKey are primary key. Row key is like an id key. Timestamp is mandatory. Paritiion key is like a table name. No indexes. Entities can have different numbers of properties. Azure sorts the table and automatically moves partitions.

SQL Storage:

Relational. Elastic database pools can allow you to provision tables as needed like autoscale. Hosted by Azure. Pay per use. Geo-replicated as an option. 99.99% SLA.

Document DB:

NoSQL model. JSON. Data is stored in text format. Performance tiers for pricing. $6 per month. 25-100 dollars per month.

Blob Storage:

Container model and have security. Binary large object. Files, videos, photos, backup images, etc. 500 TB of storage capacity.

Block – optimized for streaming and storing objects in the cloud. Images, videos, documents, etc.

Append blob – optimized for appending. Log files.

Page blob – random writes. Harddrive writes. VHD are stored as page blob.

Queue Storage:

Messaging between services that is persistent. Maximum 64KB in size. Read and delete. Temporary. Invisibility behavior. Once read becomes invisible for a short time. If not deleted, visible again.

File Storage:

Network shared with SMB 3.0. Rest API. Application like storing log or backups. Helps migrate legacy systems. All other storage types have the 500 TB limit. File share has 5 TB limit on it. Can create directories inside the share. Each file can be 1 TB.

SQL Server VM:

PaaS or IaaS to be consumed. VM provisioned and install software. Need a license. Choose a template and edition. Possible data migration issues. Disaster recovery issues – can backup to a blob in Azure.

Securing SQL Server:

Ensure the right people have access, etc. owner can have access at anytime. Public access given to read the contents. Authorization can be done through ACL. White list and Encryption. Lock your database down. Data can be encrypted at rest SSE. **Shared Access Signature (SAS)** – give a temporary access to a storage asset that expires. **Shared Access Policy (SAP)** – can be given to users and revoke as needed.

**Azure Mobile Apps**

Azure App Service like fully managed PaaS. Supports data storing, authentication, push notifications, and offline sync. Web, API, logic, mobile. Mobile Apps were called Mobile Services. It can autoscale, staging environments, continuous deployment. Virtual networking, isolated environments.

Cross Platforms:

Windows, IOS, Android, JavaScript, Apache Cordova, Xamarin using C#. Microsoft does provide SDK’s for each platform. You would need new Mobile app, new SQL database, server code, and quick start application.

Offline Sync:

Allows mobile clients to store and retrieve data locally until Internet is online. Improve responsiveness, operate Wi-Fi only devices without a SIM card. Sync data between multiple devices and handle conflicts. Limit network on metered connections. Can use app while offline.

Done through a local store or storage location on your devices. Xamarin is SQLlite. API’s can be used to sync table API’s. Application must push changes up to the network for all outstanding changes. Data is pulled from the network. Implicit push(outstanding changes in the local store by changes) and incremental pull to retrieve new data like Github.

Extended Mobile Apps:

SDK for .NET and Node.js and REST API for PHP, Java, Python. Exposes a new endpoint for your code that it can call. Example – custom authentication code, database sources, web services, use queues, and connecting to legacy systems.

Mobile Security:

Application security and infrastructure and platform security. 24 hour threat management, encryption using communicating over networks. App service apps are isolated from the internet. Application security – developer must ensure operates security. Inputs are sanitized, don’t trust requests, check safeguards, and session hijacking.

Penetration testing must be done when public facing components are added to their networks. Software available.

**Azure** **70-534 (Training for the Cert – Day1)**

* Design advanced application (20-25%)
* Know terminology. Tough exam. Focused on ARM.

Performance & Scale

* Point out the components at which the least common factor would slow it down.

Security & Compliance

Flexibility

* Don’t limit yourself. DR.

Resiliency

Cost Optimization

* 5 9’s are perfect but cost is expensive

**Azure Global Footprint**

32 regions online. 6 more announced. Each region has a sister region. Except for Brazil. 1 region coming up from failure is best. Make region closest to the customer. <https://azure.microsoft.com/en-us/regions/services>.

IaaS components not listed can be obtained from 3rd party marketplace. A Av2 D Dv2 F G H. A0-**A4 is not for production use.** Testing or development. N is for Nvidia graphic cards. Know VM sizes for workloads. Single instance is 99.9%. Multiinstance is 99.95%. VM as a set is like horizontal scaling.

**Storage** was related to PaaS. VM makes three copies in each local region. You can also have geo-redundant storage. Asynchronous. In sister region. But not really meant for DR. Temporary storage is for logs is local to the host. **Never use Drive E it is used as a DVD**. Begin with F and onward. Scale set must be stored on the OS disk or use premium storage. Premium storage for AD. SQL separate data disks or temporary disk with SSD or blob storage for backups. Standard can only allow 40 VM disks with 500 TB. Premium can have 35 TB is limit and bandwidth is <=bandwidth. Limits supposed by the platform.

You can define your own network range. Bring your own network. Public iP tied to network interface or LB. NSG can define rules for ingress/egress. Rules are stateful. Not Stateful. **OS and firewall must be configured to allow traffic.**

**Load balancing.** Layer 4. WAF available too with layer 7. Stay within region. Traffic manager would work between different regions. DNS would be used to route traffic with Traffic Manager. **Exam consists of multiple choice questions With 1 option or 2/3 options. Same with options and order. Powershell code. Case studies. Same question with different options.**

**Traffic Manager demo with failover.** Priority used to be called failover. FQDN. TTL is not exact. Other options F5, Nginx, Kemp, Barracude, Netscaler.

Architecting Azure Solutions

* Performance & Scalability
  + Performance for traffic manager puts the user to the region with the least hops.
  + Not all VM’s is available in all regions.
  + HPC Architecture. Traffic Manager Architecture review.
* Security & Compliance
  + Azure Application Gateway. Load balancer doesn’t support cookie session affinity. DS3 means it is backed up by SSD.
* Flexibility
  + JBOSS EAP architecture.
* Resiliency
  + SharePoint HA Farm in Azure
* Cost Optimization
  + Web App with API Tier & Service Bus. Architectures will show up on the exam. Mostly migrations. **NSG with Service Bus and Traffic manager on the exam.**

**Azure AD. Need to go over again.** Udemy covered some of this. Demo of resource group, networks, AD VM, availability set, you can download template and configure the VM. You can pass it around. Azure is IAM management. SLA for Traffic Manager are 99.99%. Storage account is used to store files in a container like a folder.

Tenant is representative of an organization that is hosted in Azure. Tenantname.onmicrosoft.com. Tenant is done by the Classic portable. Go over more. On-premise AD can be accessed via ADSI. Azure AD uses Graph API and REST and OAUTH2. **Comparing directories is important for the test.** Ports required for Azure AD -https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-ports

.

Multiple scenario’s with AD – cloud only, directory synchronization/Federated SSO. Azure AD premium to be able to change passwords via browser.

* Performance & Scalability
  + 99.9% SLA with AD basic and premium. Needs AD connect, 2 D2\_V2 with another data storage disk. vNET.
* Security & Compliance
  + Same Sign on or SSO
  + ADFS must be in place.
* Flexibility
  + B2B collaboration – resources shared, access managed
  + B2C – integration with third party social identity providers
  + AD Domain Services can be used instead of building IaaS DC’s. LDAP and Kerberos extended with this.
  + Data is not paid when going intra DC’s only egress.

**Implementing Azure Governance**

Go over a little more. Missed some due to cables. Readers/owners come up in the exam.

Go over resource manager, etc. Resource manager works together with RBAC. Use case is chargeback. Definitely powershell and Json on it. Demo on arm policies

Locks and auditing. Lock can be set by template, powershell, and more. Activity logs are retained for 90 days. PowerVI

**Architecting Cloud Connectivity**

You can bring your own networks. DNS label can be used to map to a DNS server. Similar NAT with Azure. IP’s will also be lost. User defined routes that the user can configure. User define route is like system routes but function like them. Vnet peering can be created in the same region as normal define routes go between different regions. VNET peering uses backbone. Can’t have address spaces that overlap. Can unlock virtual datacenters. Reduction of IaaS Server = reduces costs.

**Know P2S, S2S, Express Route on test.** S2S and P2S still traverse the internet but are encrypted. **Scenario questions around what option would be best to know.** VPN Gateway based are going to go away. There only ike v1. P2S uses SSTP protocol with certificates.

Can have full meshed network with BGP pointing from different vnet’s to provide redundancy. Active/active gateways is possible. Colocation exchange, IPVPN any to any and point to point connections with layer 2 or 3. There are prerequisties for express route like O365 subscriptions

Public or private peering, or Microsoft peering. **Know these.** Possible with path diversity with ExpressRoute. Has limits with how many vNET’s can be in them.

Data Center connectivity architecture. Hybrid network architecture. Enterprise Design.

Create Load Balancer, Create VM,

**Azure Training Day #2**

Lift and Shift Case Study. <https://intranet>. Identify a migration approach

Pg.135 in the lab guide.

**Architecting Devops Solutions in Azure Module:**

Introduction to DevOps:

Development & Operations. Operations minimize change and development introduces change. Development provides a software release and operations hacks it. Developers have partial agility with operations having downtime costs. Devops is not just tools like Chef, Puppet, Jenkins, Azure. Devops not just for Open Source or Startups.

**DevOps** integrates development and operations team in order to improve collaboration and productivity by: People, Process, Tools. People need trust respect and communication. <http://www.itproguy.com/devops-practices>. Process for how things should be doneTools. Develop, code repository, build, test, deploy, contoso app, monitor and improve.

Introduction to JavaScript Object Notation:

Intellisense/autocomplete support schemas. {} { “name” : “value”, number, string, Boolean, array, object}. Can have multiple objects nested. Array’s use [] to separate itself from another. Doesn’t need white space

Authoring ARM Templates:

Template anatomy: $schema, contentVersion, parameters, variables, resources, outputs. Resource section can get hairy. Can override separate parameters. Input options in the template. connectionString – variable can concat to functions together.

ARM templates helpers like specific conversion, string, and template helpers with array/arithmetic. Copy and copyindex can be used to create multiple instances of a resource. Dependencies can be specified for other resources.

Resource extensions can be used to automate deployed infrastructure. **Know this for exam.**

Demo of the arm templates and working with VS. Automation group that stores the PS scripts. Keeps checking to see if anything has changed. Definitely need to go over this more. More involved.

IaaS Case Study DevOps. Solution overview: Scale sets have availability sets implied. For autoscale. Chef extension script and a one-time initialization script

**Architecting Azure Solutions – Day 3**

**Architecting Cloud Security:**

Security is at the perimeter, building, and computer room. Vnet protection and DDos protection. NAT is used as well. Fabric controller helps isolates each customer environments. Functions as the kernel. Hyper-V hypervisor. Traffice is encrypted in transit. Data at rest can be encrypted by SSE (Storage Service Encryption). **Know type of encryption used like TLS/TDE/SSE**

**Prevent Breach** – defensive strategy aimed at predicting and preventing a security breach

**Assume Breach** – key operational practice that hardens cloud services. Monitoring and response. Threat intelligence. 9 step incident response. Temporary privilege granted by customer to look at incidents. DOS/IDS layer. VHD images aer provided for platform level incident. Lots of Certs available.

Two storage keys like SaS (Shared Access Signatures). Roll storage keys. Implemented stored access policies don’t support SaS. Shared access policies can be used with SAS.

CEK (Content Encrypted Key) can be used on the client side. Storage Explorer tool. TDE used for SQL encryption at rest. Data masking can be done on the SQL database to not allow unauthorized access.

**Application Identity:**

OAuth 2.0 – grant third party access to a users resource. Azure AD applications have client id’s which are like login and username. Three options to register an Azure AD. Classic/new portal and one more. Two options for SSO – Federatated or password based.

My applications users can discover which apps they have access too.

**Infrastructure Security:**

App Service environment with PaaS.

Storage key vault – offers encryption while storing the keys. Azure Security to provide monitoring. OMS Security is agent based. Custom Queries. Lists threat intelligences. Query’s can be saved as well. Storage must be enabled. Agent is autodeployed.

Hybrid Management – refers to the complex operational task of managing environments.

OMS (Operations Management Suite) – Need to go over this even more.

Provides log analystics. Solution packs. Integrated search. Possible big data with customized dashboard. (Design, Deploy, Support, Optimize, Assess)

Site Recovery for DR. Review configurations in Azure only with Azure Security Center. Different tiers like free standalone and oms. Log analystics is part of OMS. Log analystics follows 99.9% SLA. Data in transit is encrypted. Data at rest is not encrypted.

**Automation and Control:**

Assets (Schedules, Modules, Credentials, Certificates, Variables, Connections, etc.). Seems similar to minion jobs. DSC (Desired State Configuration). 99.9% SLA. In transit encrypted and encrypted at rest.

Azure Security Center. Stored in Azure rather than OMS.

**Architecting Business Continuity:**

**Data Protection or Disaster Recovery:**

Data protection is multiple points in time. DR is for quick restore. Data protection is a backup of the VHD image and like a snapshot. **Know Import export service or Azure Express Route with Data transfers.**

**Azure and Data Protection:** DPM (Data Protection Manager).

**Azure and Disaster Recovery:**Use cases include planned failover, migration, unplanned failover, testing and staging. Acts as a facilitator and doesn’t store the data. Data disks is limited and the type of t-shirt sized instance. Data in transit is encrypted. On prem to onprem or onprem to cloud. Ports will need to be opened -433. System Center Machine manager – hyperv must be installed on the servers when looking at on-prem. Most enterprises will need Express Router. Basic A servers don’t do encryption.

Case – Study – Architecting for a Hybrid Environment. Azure Recovery Vault. Recovery Plan of the failover with SQL.

**Architecture Azure Solutions – Day 4:**

**Designing for the cloud:**

Utilize hardware to consume it. Everything can fail. There are fallacies of distributed computing. http:aka.ms/azurelimits

**Platform as a Service:**

Move in ready. Build from the ground up. IaaS allows efficiency. PaaS allows innovation.

**Introduction to Cloud Design Patterns:**

Multiple patterns can solve multiple problems. Monitoring is important to make sure things continue to run. Service bus queues for messaging. Orders going through this message queue. Acts as a buffering zone to protect against things. Throttling pattern.

**Availability Patterns:**

Don’t let a customer consume or degrade the service for someone else. Can have more workers working on a queue. Priority queue patterns can also be asked. Best to place pairs in a region.

**Data Management Patterns:**

Good to have cache aside store. CQRS (Command and Query Responsibility Segregation). Event sourcing is stored separated. You can replay your events all in the new system with the fix. Requires lots of storage. Polyglock with index tables. Store the same data for the same app. Materlized views to keep the data in a different place. **No design questions on the exam for designing applications. Know how to store data stores, messages, queues.** Sharding – divide data store in horiztonal partitions. Compute Resource Consolidation Pattern – consolidate multiple tasks on a computational unit. Static content hosting – deploy static content on a storage service. Reduce expensive compute instances. External Configuration store – move configuration information out of the application into a centralized location. Leader Election Pattern – coordinate actions by collection of collaborating. Pipes and filters pattern – decompose a task that performs complex processing into elements that can be reused.

Runtime reconfiguration pattern – design an application that can be reconfigured without redployment or restarting the application.

Circuit Breaker pattern – handle faults that may take a vriable amount of time to rectify when connecting to a remote service or resource. Compensating transaction pattern. Retry pattern. Gatekeeper – protect applications and services by using a dedicated host instance that acts as a broker.

**Design and Implementation:**

**Management and Monitoring:**

**Security Patterns:**

**Architecting App Services:**

Functions will take over logic apps. Similar to Lambda on AWS. Consits of Web apps, api apps, logic apps, mobile apps. App service plans that you can use to plan out you’re application. Standard are for production workloads. Allow applications to login users without any code changes. Web app service comes with it. You just deploy the code. Functions replace web jobs. Traffic Routing and deployment slots. Deployment slots of their own URL. You can flip dev slots to different slots.

Demo on App Services. **Know Web Jobs on the exam. Know App Service within application settings with a checkbox /always on.** Used to host multiple apps within always on. Won’t ever hibernate. Web app includes web jobs.

Demo of function app. Serverless function. Only is consumed by code and how many minutes it is running. Apps can be deployed straight from source control.

**Mobile Apps:**

Makes an API, an optional database, gives an easy way to push notifications(Azure notification hub). Notification hub helps keep things connected. Can only choose Node.js or .NET framework and nothing else. Data manager connects the model to the Database and etc. .Net can handle dynamic Schemas. Offline sync allows you to store to a local database with like SQL lite.

**API Apps:**

API’s can be marketed in the marketplace. Similar to mobile apps. Client SDK can be made from the metadata. Metadata is known as swagger. Web apis to host api with swagger.

API Management – used to control access to throttling data caps and security around API’s that will publicly be hosted. Dashboard and managed in a centralized space.

**Logic Apps:**

Linux may require docker containers. API apps are good for legacy applications. Backbone is biztalk apis’. Graphical designer. No code designer. Billed for the amount of actions that are done. Triggers with workflows, and actions. Like Zendesk. Mobile app is limited to the guidelines that Azure sets. Custom Mobile Workforce app can be used to connect existing libraries. A little more flexible than mobile apps. Biztalk hybrid solution is like a VPN solution. Hockey app is a mobile testing platform. Simple digital marketing site with like CDN.

**Choosing the right Storage:**

**Azure Storage:**

Older storage service. Can copy to another region but region specific. Blob containers is where controls locks can be applied. File storage. No sub containers. Storage queues used asynchronous communication.

Table storage to store flexible datasets. Uses a row and partition key within the storage stable. These are the only values that are indexed. Schema free.

Storage files: Files to do network shares. SMB 3.0 up to 5TB. Data is always copied 3 different copies. LRS/ZRS/GRS/RAGS. GRS use to be the best option. SAS are needed to be able to share the data. Cool storage is cheaper with blob storage. Not necessarily needed that often. Hot storage is stuff that is accessed all the time. Blob storage is encrypted at rest. Storage explorer which is free. Can’t edit the snapshot but you can override it for versioning. Row key corresponds to the partition key. Storage accounts accessed through http://. No relationships with these data.

**SQL Database:**

RBaaS. Built ontop of a SQL service. Managed by Microsoft. Database is purchased. SQL is a container. Basic options/standard/premium. DTU (Database Throughput Unit) by performance. PIT recovery. Stores copy in another region and geo-replicated. Active Geo-replications. Elasticpools are a way to share multiple databases across multiple individual databases under one price. You can choose whole limits per the whole pool. Database auditing is still available.

**DocumentDB:**

NoSQL DBaaS. High Performance with SSD. Shredded and partitioned. Structured to the JSON objects but no schema. Queries can be done only one at a time. Indexes everything but tuning. Node.js engine. Demo of the system. Armviz.io and shows arm templates in there.

**Other Storage Options:**

Clear DB does a MogoLab. Done through mlab.com.

**Architecting Global Solutions:**

You can get throttled if you get close to the max. You can cache databases if you get to a to a bandwidth limit. Affinity cookies can be done through. Traffic Manager. Caching.

**Azure Architecting Solutions – Day 5:**

Case Study. Potential Solution – 3 different regions with web apps. CDN on each storage account. Our team presented. I drafted the visio together.

**Big Data and Analytics:**

New data sources, real-time requirements, and data increase. Volume. Velocity, variety. Lambda architecture has a speed(hot path) , batch (Cold path), and serving layer. Big Data tools don’t give much unless you build aspects to it that provide insight. Speed Event Hubs or IoT Hubs. Lots of services.

Azure Data Lake Store – hyperscale repository PaaS. HDFS (Hadoop File System). U-SQL (C# and SQL). Built on yarn.

Azure HDInsight – Hadoop as a Service. Managed by Microsoft. Horton Works. Uses different permissions than the standard set.

Demo of Azure Data Lake Store. T-SQL HDInsight can also connect to a Data Lake Store. Features are removed and added when the storage type is chosen. Will need to create an AD identity if using it. Don’t give access to the entire data store. 32 workers require worker nodes. Scaling can cause restarts if needed.

Ambani views are ways to manage a Hadoop cluster. Event hubs is a way to consume data. IoT hub gathers data events from specific devices. Stream analytics provides multiple streams per minute and can consume data from different locations. SQL used.

Azure Machine Learning – Predictive analytics. You’ll need experiment data and you’ll need to clean it up. Some names may be unique on the internet. Allowed two tester per account. Demo of Machine Learning

Cortana Intelligence Suite – Alacart flexibility. Some questions on machine learning and a scenario of which features would be leverage. Big data – what are ways to implement or azure jobs/batch.

**Architecting Scalable Services:**

**Microservices:**

Break a system into smaller programs. Can run without any other system and can be isolated. Microservices are independent programs that are used across hardware evenly versus servers have applications running on each piece of hardware.

**Service Fabric clusters:**

Service Fabrice is made up of microservices. Cluster manager dashboard shows all the different microservices. Service Fabric is polynimbus and can be used in different clouds. Cross Platform.

Can have different type of nodes. Microservices can have multiple hosts and won’t consume a lot of resources. Used in scale sets with a 99.95%. scale sets can go up to 100 VM’s. 3-5 fault domains and 5-20 update domains.

Different Durability Tier’s (Gold, Silver, Bronze). Reliability tiers with different replica capabilities (Platinium, Gold, Silver, Bronze). 3 fault domains or up to five in an availability set. Primary or secondary replica’s and self healing. There are rolling upgrades as well. Upgrades one at a time.

Cluster security can use security key vaults. Even with AD. Security can’t be changed later. Actors can parallelize work across most of them.

State management and partitioning.

Stateful or stateless. Can be fixed or non fixed instances with stateless. Stateless has unique URL’s. More partitions can only take advantage of up to 25.

Statemanager for stateful services that can be utilized. Data stored in one partition can’t be accessed from a different partition.

**Microsoft Azure IaaS Deep Dive Jump Start (February 14, 2014):**

**https://mva.microsoft.com/en-US/training-courses/microsoft-azure-iaas-deep-dive-jump-start-8287?l=S1oXqFXy\_2804984382**

Know AD, Windows Server, Hyper-V knowledge. SaaS (Consume), PaaS(Build), IaaS (Host)

SaaS is hosted on something. We are just not worried about it.

Cloud service – container or management grouping, virtual machine contained within a cloud service

Azure Virtual Network – networking overlay that allows you to create and manage virtual networks in Windows Azure and securely connect them to your own on-premises network.

Preview is kind of a like a beta.

**Virtual Machines:**

Azure runs thousands of physical hyper-v servers

VHD-file(disk) – provided by azure (image) and can be uploaded by the customer (uploaded by VHD-file). IaaS VM can be RDP would be your VM. (responsibility).

RDP inbound is enabled by default. Don’t use port 3389. Unlimited outbound network access.

Different sizes of VM’s by memory and processors. VM’s can be changed to bigger sizes. What’s a reasonable size. Wizard or Quick Create option for VM creation.

Sysprep VHD-file doesn’t have a name yet. RDP port “Auto” is something for not being 3389. Hyper-V integration components are in the system. VM’s have to go offline to make a size of the VM. Azure supports 76 markets worldwide.

DNS stays the same and even when the VM will be deleted it stays the same. Cloud service has one external IP address. Create more than 1 cloud service if more than 1 IP is needed. VM’s can be controlled by Powershell. Endpoints are ingress. Can’t ping the VM’s. LB’s use a probe to test if the VM’s are up or not. Endpoints have to be in the same region

**Fault domain** is a rack that can fail. (to close- single point of failure)

Update domain – updates can be done automatically and move the machine off something else and at different ttimes.

Availability sets to have them on different racks to avoid a fault domain.

Affinity groups – place near each other.

Stop VM – on same physical server but still counts “usage”

Stopped Deallocated means that you shut down a VM and deallocate the IP address and you don’t pay for it again.