**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.