AZ-106 All in One.

[**AZ-104: Manage identities and governance in Azure (15-20%)**](https://docs.microsoft.com/en-za/learn/paths/az-104-manage-identities-governance/)

1. **Create AAD** users and groups. 34m

* Add users, use group access to app and resources, B2B guest access.

Account can be restored, only when deleted within last 30 days, external org can only be guest, you can add Apps and assign to users and resend invites.

Assign member dynamically on AAD Premium 2.

1. **Manage AAD** users and groups. 50m

* AAD is not Windows AD, tenants, subs, users, manage roles, hybrid role AAD Connect.

An Azure subscription is a billing entity and security boundary

An AAD directory can be associated with many subs, a subs is always tied to a single directory.

An org can have more than 1 AAD directory. 2 types of groups: Security, and Microsoft 365.

Switch the current directory through the Directory + subs button in the **Azure portal header**.

Roles can be Owner, Contributor or Reader.

AAD Connect is a free tool to download, to sync local AD with AAD.

1. Setup AAD **Self-service password reset**. 31m

* Decide to use SSPR, implement requirements, customize SSPR.

Users can reset passwords when they can't sign in. User considered registered for SSPR when they've registered at least the number of methods that you've required to reset a password.

In AAD, Password reset. Enable ALL; one or two authentication methods, are users required to register for SSPR, notifications, customize: provide email address or URL to helpdesk.

Use SSPR to allow users to reset their forgotten or expired passwords. SSPR is secured by authentication methods of your choice. You can customize AAD branding.

1. **Manage access to subs** using RBAC (IAM). 20m

* Identify roles to assign to users, identify when a Global Admin needs temporary access **elevation,** Grant users **admin access** to subscription.

RBAC (IAM) resources and AAD resources have **independent permission** systems.

AAD has only one scope, the directory. The Azure RBAC scope covers management groups, subscriptions, resource groups, and resources.

**Assign owner** at subscription scope, to manage resources and billing.

Global Administrator can’t access Azure resources by default, they need elevation. E.g. when the subs admin user leaves, but. Verify subs in your directory, select (IAM), Role assignments, ensure that you have the Root (inherited) scope. Revoke when task is done.

1. **Secure resources** with RBAC. 37m

* Verify and Grant access to resources, View activity logs of RBAC changes.

Each Azure subscription is associated with a single Azure AD directory

RBAC(IAM) is built on ARM, provides fine-grained access management of resource.

Inheritance order for scope is Management group, Subscription, Resource Group, Resource.

3 elements: security principal (user), role definition, scope: "who", "what", and "where".

A Role (what) in Azure is a collection of permissions; use NotActions to customize collection.

Contributor can create and manage resources, but can't grant access to other users

Add and remove roles via Access control (IAM), view activity logs, add filters, etc.

1. **Create custom roles** with RBAC. 30m

* Identify role definition structure and properties. Create and manage custom role.

You can then create/assign/mange it via CLI,Portal or Pwsh.

The CLI can be used to create a Json file, with operations allowed for resources and the scope of permissions. Use 'az provider operation show' to find resource provider operations.

CLI: “az role definition create --role-definition newrole1.json” to create the custom role.

Before you can delete the custom role, you must delete any role assignments.

1. Control and organize resources with **ARM**. 46m

* Use resource groups , tags, apply policies to enforce standards, resource locks.

Organize resources by using RGs and Tags. Resources can be moved between RGs..

Tags at a RG level are NOT propagated. Tags in conjunction with Automation to schedule maintenance windows, associate a cost centre.

Search for policy, check definitions. Use Azure Policy to automatically add or enforce tags.

Create a policy with your naming requirements and assign it to the scope of your subscription.

Click + Policy definition to add. Select account location. Enter a name, description, new or existing, complete the JSON policy rule. Save. Assign policy definition to a scope (location) to a resource, using params, takes up to 30 mins. RBAC (IAM) for fine-grained access management.

Best practices: Segregate duties, grant users the lowest privilege level, use resource locks.

1. **Plan and manage costs**. 43m

* TCO calculator, describe ways to purchase, estimate costs with Pricing calculator, define major factors that affect cost and use recommendations to minimize.

Purchase through: Enterprise agreement, Web Direct on Portal, Cloud SP.

**Factors:** resource types, usage meters, resources are charged based on usage, Subs Types (free, pay as you go, membership), Marketplace, location,

Pricing calculator helps you take all of the preceding factors into account.

Perform cost analysis before you deploy, use Advisor to monitor usage, spending limits to prevent overspend, use Reservations to prepay, choose low-cost locations and regions, Research available cost-saving offers, Apply tags to identify cost owners, eliminate unprovisioned ExpressRoutes, use Cost Management + Billing, right-size or shutdown underutilized VMs,

1. Analyse costs and create budgets with **Cost Management**. 40m

* Use Cost Analysis. Build budgets, and alerts.

Customize a view in Cost Analysis and pin it to a dashboard and share it with the team.

Create an Azure subscription budget for a monthly, quarterly, or annual period. Your navigational content in the Azure portal determines whether you create a budget for a subscription or for a management group. Configure it to call an action group.

Three types of **cost alerts**: budget, credit and dept. spending quotas.

Enterprise Agreement supports all 3.

1. **Move resources** to another RG. 42m

* Identify if it can be moved, and how to do it.

RG resources can be in different regions. Assess (use tags if possible) if resources may be moved, validate a move operation, move and verify. Check the types at the “[move support for resources list](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/move-support-resources)” webpage. Can be moved: storage accounts. VMs, VNets.

VMs have their own **limitations** as all dependants must move too. **Can’t move VMs :** certificates in Key Vault between subscriptions, scale sets with std load balancers or std public IP, with managed disks in availability zones to different subscriptions.

AAD Domain Services, backup vault or application gateway can’t be moved.

Use the Azure REST API “validate move” to test/validate moves, by using the CLI “az rest --method post –uri <REST operation uri>” method.

Azure portal does an automatic validation. Powershell : Move-AzResource cmdlet.

1. **Manage device identity** with AAD join and Enterprise State Roaming. 25m

* Options to manage Device IDs in AD, config AD Join, config Enterprise State Roaming.

Device identity in AAD helps you control devices. Go to AAD > Devices > Device settings.

3 device registration options: AAD registered, joined (Win 10/Serv 19), or hybrid (Win 7 up).

Conditional access requires an Azure AD Premium P1 license or a Microsoft 365 Business license.

AD join supports an AD work account and password or Windows Hello, and supports MFA.

AD join options “Self-service by using the Windows out-of-box experience (OOBE), Windows Autopilot, or bulk enrolment”.

When a device isn't in the MDM scope the join finishes without enrolment.

Enterprise State Roaming (Windows 10, AD Premium or EMS license.) allows for settings to move with the user when they switch devices, Separation of corporate and consumer data, enhance security, better management and monitoring (who can sync and which device).

Any deleted data is automatically kept for a maximum of 90 days, stale data deleted after 1 year.

~ **Part 1 ID and Gov. The END** ~. Tony

**[2. AZ-104: Implement and manage storage in Azure (15-20%)](https://docs.microsoft.com/en-za/learn/paths/az-104-manage-storage/)**

9 mods 6 hrs

1. Create a **Storage account**. 30 min

* How many, settings, creating. Name must be globally unique.

Only stores Blobs, Files, Queues and Tables. (remember using “big fat qt”)

Advice is use Resource Manager model, and Storage V2 account type.

Settings: where, performance, replication, tier, secure transfer, VNets, Data Lake Gen2?

Storage Account lets you create a group of **data management rules** and apply them all at once.

1. Choose the right **disk storage** for your VM workload. 24 min

* Types and capabilities: HDD, SSD (Std, Ultra, Prem.) Uses: OS, data or temp.

Database access considerations: Production, warehouse, standby, admin ?

Managed, Ephemeral or unmanaged (not used much).

1. DR by **replicating storage data** across regions and failover. 46 min

• Choose the correct redundancy option. Initiate a storage failover. (DC=region).

**Data availability is business-critical. 6 Types.** (remember using “LGZ”)

1. Locally redundant storage (LRS) 3 copies to separate racks in a DC, in 1 region.

2. Geographically RS (GRS), as LRS but also to **2nd paired DC**, read only if LRS fails. 6 copies.

3. Read-Access-GRS (RAGRS), able to read from the 2nd DC, normally. 6 copies.

4. Zone RS (ZRS) 3 copies to storage clusters (3 availability zones) in a single region (DC).

5. Geo-zone-RS (GZRS) combines GRS with ZRS. 6 copies.

6. Read-access GZRS (RA-GZRS) able to read from the 2nd region. 6 copies.

**Live** Migrations done via **AZ Support**, with limitations. Manual more flexible, fixed date, AzCopy.

**Ex3:** Create GZRS storage. Create Blob container, create file, upload file. Failover process: data is async. copied to other DC, failure stops copy, possibly data loss. Manual or MS failover points storage to other DC, account is changed to LRS. **To start replication** configure for GRS or GZRS.

Use Az **Service Health** to track status and handle or report issues to you.

**Ex5:** Failover. “Prepare for failover” is enabled once initial replication is done. Click it, confirm. When complete the type is **now LRS**, reconfigure the account.

Now you need to estimate potential data loss. **Knowledge check.**

1. **Secure your Azure Storage** account. 45 min

• Security features, keys, SAS, NW access rules, Advanced Threat Protection, Data Lake Ent.

Data at rest is **encrypted**, BitLocker for Win Images. **In transit**, use HTTPS for TLS.

CORS (cross-origin resource sharing) is optional, **locks GET requests** to specific domains.

RBAC can be used to access data in the Account. Audit access using Storage Analytics, real-time.

Storage Account (shared) **keys** can be used; client embeds the shared key in the HTTP Author. header of every request: can regenerate keys, refresh keys as secondary, not for 3rd party – rather use shared access signature (SAS). There are Service-level and account-level SAS types , with lightweight service you can define permissions and the access interval.

NW access default is allow from anywhere, change this to **Selected networks.**

Azure **Defender for Storage** can be enabled under Settings, Advanced security, to be emailed, for Blob, Files and Data Lake G2. Review/manage security alerts from Az **Security Centre**.

Azure Data Lake Storage Gen2 provides a first-class solution that enables enterprises to consolidate their data, built on Azure Blob and inherits all the security features in this module.

**Knowledge check.**

1. Store and **share files** in your app with **Azure Files**. 51 min

• Features, configure Az Files, security, Pwsh commands can be used easily.

Choose storage type, access, redundancy, migration solution. File shares are simpler to use.

Secure access from on-premises, Azure file shares only support SMB version 3.0.

**Ex4/6**: Use **CLI** to Create/share . Setup fileshare on VM. Secure access to files. Enable secure transfer. Limit access to your LAN. Networking (Firewalls and VNets), **select Selected Networks,** “Add your client IP address”. Can map with powershell script presented under connect. You could “Enable and use Azure AD DS authentication”, but check costs for ADDS.

1. Upload/download/manage data with **Storage Explorer**. 37 min

* It’s a GUI, installed on a PC. Access data from B(lob), Fileshare, Q, T(able) or Data Lake.

You can also use a locally based Emulator (SQL12 Express), and Azurite (Node.js, uses API).

Many ways to connect: using Azure AD, SAS URI, account name and key, Data Lake.

**Ex3/5**. Connect Storage Explorer to storage account and Cosmos/Data Lake.

Obtain string to connect to Cosmos create/connect to Data Lake Gen2 (preview).

1. Export large amounts of data using **Import/Export.** 24 min

• Deciding to use Import/Export service, learn steps.

Offline solution only. These are **your drives** you must send to the Azure DC, using your courier.

The WAImportExport tool used to prep drives, and copy local data to drives to import to Azure.

Ver 1 for export (**Blob only**)/import, Ver 2 for import to Azure files.

To export, MS provides Bitlocker key, prep your own drives and send them to the DC, the Blob storage is copied and then sent back to you.

To import to Azure, enable Bitlocker using WAI tool or manually, copy data to drives, send to DC.

1. Import big data to the cloud choosing a **Data Box**. 25 min

• Device options, methods, **imports to Azure only**.

Must be supported by the region in which you are working. Device provided by Microsoft.

**5 products**: Offline - Disk (35TB), “Box” (80), Heavy (800).

Online – Stack Edge (12TB, AI on-premises device, Machine Learning, IOT), GateWay (virtual).

Azure **Data Factory** is a service that enables you to organize, move, and transform large quantities of data from many different sources; you create data pipelines that ingest data.

Any files copied to PageBlob or Blockblob are created as containers in Azure, use PageBlob folder for Vhdx files, AzureFile for files. Consider other option, using size, frequency and network bandwidth availability.

1. Extend LAN file share capacity using **File Sync**. 1 hr16

• Check Compatibility, deploy, Test and Troubleshoot.

Server 2012 R2 minimum. File Sync has a change detection job, initiated every 24 hrs.

**Terminology: 1.** Storage Sync Service is the resource for Azure File Sync. **2.** A sync group outlines the replication topology for a set of files or folders. **3.** A registered server represents the trust relationship between LAN server and the Sync Service. **4.** File Sync agent a package has 3 components: FileSyncSvc.exe. StorageSync.sys. PowerShell management cmdlets.

**5.** A server endpoint is a specific location on a registered server, e.g. a folder. **6.** The cloud endpoint is a file share in a sync group. **7.** Cloud tiering is an optional feature that archives files to free up space on file share.

**Deploy process:** 1. Run evalution cmdlet, 2. create resource (storage account, file share, sync service, sync group), 3. install agent, 4. Register Server with Storage Sync , 5. Create endpoint.

**Ex4:** Run evaluation, Invoke-AzStorageSyncCompatibilityCheck.

**Ex6.** create storage account (with file share, sync service, sync group).

**Ex8.** install agent, register your local Server, create endpoint.

**EX10**. Troubleshoot Azure File Sync. Watch the Video.

**Troubleshoot:** mount file share (open port 445 MS NW access), invalid filenames, check if you can connect to fileshare, view server health and metrics for Storage Sync Service, use Azure Monitor, view event logs, use PerfMon (AFS Bytes Transferred and AFS Sync Operations).

**Summary:** using File Sync, assess, resource setup, configure, troubleshoot.

**NB !! \*** <https://docs.microsoft.com/en-gb/learn/modules/extend-share-capacity-with-azure-file-sync/11-knowledge-check>

**~ Part 2 Storage . the END ~** Tony.

**[3. AZ-104: Deploy and manage Azure compute resources (20-25%)](https://docs.microsoft.com/en-za/learn/paths/az-104-manage-compute-resources/)**

14 modules 11h15m, **Lots of exercises.**

1. Create a **Linux VM** in Azure. 1hr23m

* Options for VMs, create VM, connect with SSH, install NW config software.

Need VM (CPU+RAM), storage account, disks, VNet, NW interface, optional Public IP (Pip).

Consider these **6 sizes**: **General** use computing/web: B, Dsv3, Dv3, DSv2, Dv2.

**Heavy computationa**l tasks: Fsv2, Fs, F. Large **memory** usage: Esv3, Ev3, M, GS, G, DSv2, Dv2.

**Data storage** and processing: Ls. Heavy **graphics** rendering or video editing, NV, NC, NCv2, NCv3, ND. **High-performance** computing (HPC): H.

Ex 3. Auth. Methods. Create SSH key pair. Copy the id\_rsa.pub key text for Ex4.

Ex 4. Create VM thru Portal, disks, NW.

Ex 6. IPs and SSH connect. Init disks. Install Linux software (if u want to?), Web.

Ex 8. Config Network and NSG, Allow inbound requests, ports.

Use any image to create a VM. Use of SSH, best using Private Key and passphrase.

Outbound request are allowed. Inbound traffic only allowed from within the VNet.

1. Create a **Windows VM.** 51m

* Options, use portal, RDP, install NW config software.

See Linux for sizes and resource needs. OS 2GB max. Ex 3,5. Connect via RDP. Initialize disk.

NSGs use rules to allow or deny traffic moving through the network. Deny all is final rule.

1. Manage (Linux) VM with **CLI.** 51m

* Create Linux VM, resize, managing VMs, connecting.

Ex2 Create VM. Ex3 Test the VM, connect with SSH. Ex4 explore other VM images; some are location-specific. Ex5 sizing, see Linux, to resize first stop the VM. Ex6 query VM list, IP address, etc. Ex7 start, stop, restart VM, see state. Ex8 install software, e.g. Nginx web server.

1. **Add and size disks** on VMs. 36 min

* Config drives and attach, determine disk needs, resize.

OS, Temp and Data storage drives. A VHD (stored as page blobs) can be uploaded to a storage account. Ex 3, Linux VM and commands.

4 Tiers of storage: Ultra disks, Premium SSD Disks, Std SSD (managed only), and Std HDD.

Data replication Zones, see [Implement and Manage Storage, Module 3 (replicating options).](https://docs.microsoft.com/en-us/learn/modules/provide-disaster-recovery-replicate-storage-data/2-evaluate-data-redundancy-options)

Ex 6. Resize a drive. Stop the VM. Backup data first!

1. **Secure VM disks** on Azure VM. 1hr

* Determine encryption method, encrypt disks with portal or Pwsh, modify ARM templates.

**SSE** data at rest cannot be disabled. **ADE** (Bitlocker) is owner managed, integrated with Key Vault for management of keys/secrets, and is required for VMs backed up to Recovery Vault.

Ex4 Pwsh. Create Key Vault, set the key vault access policy to use it to store ADE encryption keys. \*\*\* Setup VM , encrypt disks.

Ex6, use ARM templates. The Key Vault access policy must be set to support ADE. \*\*\* Decrypt the VM. Use MS template on GitHub.

1. Keep your **VMs updated.** 35 min

* Deploy update management, schedule updates, reports.

Support for most OSs, Windows from 2008.

\*\*\*Ex3 Create Windows VM. Needs Log Analytics workspace.

Wait for at \*\*\* least 15 minutes while Update Management configures the VM.

The VM created is listed as a system hybrid worker group.

Update Management will perform a compliance scan every 12 hours, sent to Log Analytics, but scheduled updates can be setup. Updates are installed by runbooks in Azure Automation.

\*\*\* Ex5. View Events on VM. Change/add schedules in Update Management. Use Log Analytics.

Update Management can generate a report indicating which machines are compliant.

1. Build **ARM templates**. 37 min

* Deploy a VM using CLI and prebuilt ARM template , customize template for a web server.

Declarative automation (JSON), define what resources you need, but not how to create them.

Templates: consistency, complexity (correct order), reduce errors, code, reuse, linkable.

JSON contains parameters, variables, functions, resources, outputs.

Ex4. Deploy VM using Quickstart template. Use the “dependsOn” element to define when one resource must exist before another can be deployed.

Ex6. Add a resource to a template.

1. Deploy **VMs from VHD** templates. 42 min

* Methods to create specialized VHD, create VM from managed disk, create a VM image, create a VM from existing VM image.

VHDs offer High Availability, physical security, durability, scalability, cost and performance.

After generalizing , in the portal, select Capture, this **original VM becomes unusable**.

?? ( Create a new virtual machine from a generalized image.

You can build a new virtual machine by using your generalized image. The simplest way is to use the Azure portal. Go to the page for your image, and select + Create VM. You'll be prompted for the machine-specific details, such as the virtual machine name, user account, virtual machine size, and network ports to open.) ??

Ex 4. Create VM **using CLI**, (install IIS), run sysprep then generalize and shutdown, deallocate and generalize (2nd time?), create a VM image from the VM, (update IIS web page, check it).

1. Build a scalable application with **VM scale sets** (VMSS). 57 min

* Features and capabilities (autoscale), when to use for apps, deploy app on VMSS.

VMSS usage include compute, big-data and container, workloads. Designed to allow you to deploy and manage many **load-balanced**, identical VMs. Don't require individual manual configuration instances.

Horizontal scaling “out” adds/removes VMs (by using rules based on metrics), Vertical scaling “up” resizes resources (CPU, disk space). This can be done by schedule or auto.

Low priority Scale Sets are available, for saving costs, but MS may remove them whenever Azure need the resources (deleted or deallocated).

Ex 3. Create a Linux SS using CLI, nginx, by default, a new VMSS 2instances and a L/B.

Ex5. Scaling can be manual, custom auto-scheduled or auto-metrics.

Ex7. A custom script ext runs on a VM, can automate the same tasks on all the VMs in the VMSS.

You can install an app, and update it with CLI, the policy can be automatic, rolling or manual.

1. **Protect your VM settings** with Automation State Configuration **(DSC)**. 54 min

* Identify capabilities of Automation, onboard VMs, auto-update VMs to maintain DSC.

It is a service used to write, manage, and compile PowerShell DSC configurations, import DSC resources, and assign configurations to target nodes.

To make sure that **VMs in a cluster** are in a consistent state, using a built-in pull server.

A PowerShell DSC script describes the desired state, can achieve idempotence, you use logic and error handling.

The Local Config. Manager (LCM) is a component of WMF, it Gets the state of the node, Test: compares this to compiled DSC script (.mof) and Set: updates the node to match the .mof file.

LCM is configured when the VM is registered with Azure Automation.

DSC supports most Windows OS (Win 7, Server 2008), and some Linux but not Debian or Ubuntu.

If nodes are located in a private network, DSC needs ports and URLs opened.

The DSC code contains config, node, resource and MyDSCConfiguration.

2 Architectures: **Push mode** is easily setup, handy for tests.

**Pull mode** is useful in enterprise for 100’s of VMs, it is more appropriate

**Ex 4**. Setup DSC. Create VM, an Automation account, a DSC script, compile it, register VM with Automation account, Check for compliance.

1. Deploy and run a **containerized web app** with Azure App Service. 46 min

* Create Docker images in Azure Container Registry (ACR vs. Docker hub), use App Service to run web apps from images, use webhooks to configure Continuous Deployment (CD).

A registry (instead of Docker Hub), has more security control, images can be signed, encryption at rest. In Azure the Registry can be replicated and is highly scalable, for enhanced throughput.

Ex3. Create registry, build a Docker image into the registry.

Ex5. To deploy a web app from a Docker image, you configure the **registry, image, tag, and the startup file, and** specify these to deploy from a repository in the ACR. (choose C# or Javascript).

Ex7 Modify the image and redeploy the web app.

This exercise does not create an Azure Container Registry task. Instead, you'll manually rebuild the Docker image for the sample app. The webhook will open when the new image is created.

**Use webhook, and ACR task** to enable Continuous Integration (CI). This will cause redeployment automatically if image changes. The web app has been updated and redeployed automatically based on the new image. The webhook service in your registry notified your web app that the container image had been modified, triggering an update

1. **Scale an App Service web app** to meet demand, scale out or up. 46 min

* Scale web app manually. (Need to scale up before scaling out more.)

Ex3 Create web App, build (~ 7mins) and deploy, monitor the app after added CPU workload, scale out (set to 5 instances), and verify CPU improvement. Stop app, set instances back to 1.

Ex5. Scale up to more powerful pricing tier, run app again, verify improvement.

1. Run **Docker containers** with Azure Container Instances. 48 min

* Run containers, control exits, configure startup, attach storage, troubleshoot issues.

Container instances: start fast, per sec billing, isolation (hypervisor security), custom CPU/memory sizes, mount file storage, both Windows/Linux using same API.

Ex 2-6. Create container to run web app, restart policies (always, never, OnFailure), “Always” is always best for long-running tasks. Deploy a Cosmos DB, create a container that connects with the DB. Variabless can be seen in portal or CLI. , it's a good security practice to ensure that sensitive information, such as connection keys, are not stored in plain text. Create 2nd container. Create a file share (storage account). Create files, view files.

Troubleshoot : Pull container logs, View container events, Attaching to a container instance and execute commands, Monitor CPU and memory usage. Use “az container attach” to view startup events.

1. Introduction to Azure **Kubernetes Service**. (AKS). 25 min

* Evaluate AKS, components, Docker file format, uses popular Management/Dev tools, Devops integration. The Kubernetes cluster master is managed by Azure and is free.

Containers are immutable, lightweight and start up fast. Easy to package and deploy containers, then scale out, less resource intensive. Kubernetes: isn't a full PaaS offering, not monolithic, doesn't limit the types of applications, doesn't provide middleware/ data-processing frameworks/ databases/ caches/cluster storage systems, and deployment is configured as a cluster. Kubernetes manages multiple containers. Per node VM is charged, you manage the agent nodes in the cluster. AKS supports the Docker image format that means that you can use any development environment to create a workload, package the workload as a container and deploy the container as a Kubernetes pod. You are charged Per node VM monthly. Use Storage volume support to use persisted storage. Use Dev spaces for testing.

[When to use Kubenetes ?](https://docs.microsoft.com/en-gb/learn/modules/intro-to-azure-kubernetes-service/4-when-to-use-azure-kubernetes-service) (<https://docs.microsoft.com/en-gb/learn/modules/intro-to-azure-kubernetes-service/4-when-to-use-azure-kubernetes-service>)

**~~ Part 3 Compute. The END ~~ Tony**

[**AZ-104: Configure and manage virtual networks for Azure administrators (25-30%)**](https://docs.microsoft.com/en-za/learn/paths/az-104-manage-virtual-networks/)

13 modules 12h7m

1. [**Configure the network for VMs.**](https://docs.microsoft.com/en-za/learn/modules/configure-network-for-azure-virtual-machines/) 1h34m

* Create VNets, VPN Gateway, work with ExpressRoute.

**VNets provide**: Isolation and segmentation, Internet comm, Communicate between resources, comms with LAN resources, Route network traffic, Filter network traffic, connect VNets.

Control routing and override settings with : **Custom route tables**, you define rules as to how traffic/packets are routed between subnets, or **Border Gateway Protocol** (ExpressRoute).

**Filter network traffic:** Network security groups (NSG), NVA (network virtual appliances).

Connect resources Like VMs and VMSSs across regions by **peering**, routing tables.

VNet of address space 10.1.0.0/16 has 65536 addresses, address range of 10.0.0.0/24 ranges from 10.0.0.1 - 10.0.0.254 = 256 addresses, mask uses first 24 bits.

Point-to-site VPN G/W type is Vpn, vpn type is RouteBased, and specify a G/W sku.

**Workflow :** Design connectivity topology, list address spaces, create VNet, create a VPN GW for the VNet, Create and configure connections (LAN or VNets), create point-to-site if needed.

On design consider: Subnets cannot **overlap**, IPs must be **unique**, it must have a G/W subnet called “**GatewaySubnet**”, which can be PolicyBased or RouteBased. Each Vnet can have **only one VPN gateway**.

**Ex5 -** Create an Azure VPN gateway > Setup a VPN gateway, making an encrypted client connection to a Vnet in Azure. Takes **almost an hour**, or longer. **Workflow:**

Design the topology, listing the address spaces for all connecting networks. Create an VNet.

Create a VPN G/W for the VNet. Create/config connections to LAN or other virtual networks, as required. If required, create/ config a point-to-site connection for your Azure VPN gateway.

Use Azure private peering for your Express route circuit where you need to allow direct connections to Azure compute resources.

1. [Design an IP addressing schema.](https://docs.microsoft.com/en-za/learn/paths/az-104-manage-virtual-networks/) 37m

* Identify private IP addressing capabilities, of VNets, public IPs, and requirements for IP addressing when integrating with LAN, plan an addressing schemafor infrastructure and create the VNets.

A dedicated subnet for the GW is required when you connect a VNet to LAN.

3 ranges of non-routable IPs that are designed for internal networks that won't be sent over internet routers: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

In Azure network design, we usually have these components: Vnets, Subnets, NSGs, F/Ws , LBs.

PiPs default method is dynamic (VM start or stop), static must be set explicitly.

PiPs are SKUs are Basic -static or dynamic, and Standard - only static, for availability zone use.

After a PIP prefix creation, the addresses are fixed, and a contiguous range.

Private IP addresses in a VNet are DHCP dynamic lease or static reservation.

Only 3 types of IP devices in Azure VNet: VM NICs, L/Bs and App GWs.

Plan IP addressing, gather requirements, plan for future expansion, sizing of subnets, devices.

**Ex5:** Design and implement IP addressing for Azure VNet.

1. Distribute services and integrate using **VNet peering**. 42m

* Identify VNet peering use cases, features and limits, configure pering.

Global peering connects VNets in different regions. Peering is **nontransitive**, you setup explicitly.

You can configure a single VNet as a hub, using VNet GWs as transit point peering.

Grant the peer subscription's administrator the **Network Contributor**, on each AAD tenant, when connecting cross-subscription VNet peering.

To enable GW transit, use Allow gateway transit option in the VNet hub where you deployed the GW connection to your LAN. Also configure the **“Use remote gateways”** in the spoke VNets.

GW transit currently isn't supported with Global VNet peering.

**Ex3-5:** Prepare VNets for peering by CLI, Vnet1 to VNet2, 2 to 3. Vnet1 cannot connect to 3 via 2.

Verify VNet peering by using SSH between VMs.

1. Secure and isolate access to resources using **NSGs and service endpoints**. 43m

* Capabilities/features of NSGs to restrict NW connectivity, VNet service endpoints, to control network traffic with Azure services.

The goal is prevent unwanted/unsecured network traffic from being able to reach key systems. NSGs are assigned to subnet (all NICs) or NIC, and each can only have one NSG.

5-tuple information : source, source port, destination, destination port, and protocol.

Default rules within NSG, any VM: all in to any VM, out to internet, in from L/B; within the same subnet, deny all external source in/out.

Augmented security rules to simplify the management of rules: Multiple IPS, ports, Service tags simplify security for VMs VNets, allowing restricted access by resources or services, App security groups for configure network security for resources used by specific apps.

**Ex3:** Create and manage NSGs. And using service endpoints. Service endpoints are available for:

Azure Storage, SQL Database, Cosmos DB, Key Vault, Service Bus, Data Lake.

Secure network access to PaaS services with VNet service endpoints.

In the route table the NEXT HOP TYPE will be “VirtualNetworkServiceEndpoint”.

**Ex5:** Restrict access to Storage by using service endpoints. Copy/paste.

1. [Connect to VMs in Azure portal using **Bastion**](https://docs.microsoft.com/en-za/learn/modules/connect-vm-with-azure-bastion/)40 mins

* Evaluate(replace jumpbox) and config Bastion, manage remote sessions by enabling diagnostic logs and monitoring them.

In the Azure portal, on a VM page, select Connect > Bastion > Use Bastion.

Uses TLS to connect in the Azure Portal to VMs, RDP or SSH, on Private IP. Avoids public exposure. **No NSG** needed, but can be used for extra security. File copy not supported.

**EX4.** Create VM, a subnet called **AzureBastionSubnet** on the same VNet or peering.

Can have address spaces with a /27 subnet mask or larger (26.25). Don't deploy other resources to this subnet or change the name.

**Ex6.** Use to monitor/manage remotes access, stream user session information to storage, log analytics (workspace). To View the current Azure Bastion connections look under Sessions.

Under Monitoring, select Diagnostics settings, Select Add diagnostic setting. Under Destination details, select Send to Log Analytics and Archive to storage account. The diagnostic logs take several hours to appear in your storage account. Find them in the storage account under Containers. Do the Knowledge check.

1. Host your domain on **Azure DNS**. 43m

* Configure Azure DNS to host your domain.

Map one or more IPs against a single domain using A or AAAA records.

**Security** features of Azure DNS: RBAC, activity logs, and **resource locking**.

Configure a public DNS zone: RG, Name, get the name servers, update the domain registrar, verify delegation of DNS, custom DNS settings (A or Cname).

Create private DNS zone, identify VNets, link them.

**Ex4:** Create a DNS zone and an A record by using Azure DNS. Use nslookup to resolve.

Azure **alias records** enable a zone apex domain to reference other resources from the DNS zone, they can point to: A Traffic Manager profile, Azure Content Delivery Network endpoints, A public IP resource, A front door profile.

4 **uses for alias records**: Prevents dangling DNS records, Updates DNS record set automatically when IP addresses change, Hosts load-balanced apps at the zone apex, Points zone apex to Azure Content Delivery Network endpoints.

**Ex6:** Create alias records for Azure DNS. A script creates **VNet, LB, and VMs**.

1. Manage and **control traffic flow with routes**. 50m

* Identify routing capabilities of VNets, config routing within a VNet, deploy a basic NVA, config routing to send traffic through a NVA (Network Virtual Applieance).

NVA to control incoming traffic from perimeter network and allow only traffic that meets security requirements to pass. UDR (User Defined Routing) overrides the default system routes so that traffic can be routed through firewalls or NVAs.

System routes - VM on a VNet can communicate with all VMs in subnets in the VNet.

VNet peering and Service chaining lets you override these routes by creating UDRs, VNet GW to send encrypted traffic , VNet service endpoint provides direct connection to resources, as you enable endpoints, the routes are added to the route table to direct this traffic. BGP offers network stability because routers can quickly change connections.

**Ex3:** Create **custom routes**. Create route table, custom route, subnets, then associate the route table with the public subnet. A **subnet can only have** **one routing table**.

To deploy a NVA, you can use a VM enable IP forwarding after routing tables, user-defined routes, and subnets have been updated or an image from Marketplace. The goal is to prevent unwanted or **unsecured network traffic** from reaching key systems.

**Ex5:** **Create NVA** and VM. The NVA itself and its NIC must both have IP forwarding enabled.

**Ex6:** **Route traffic** through the **NVA**. Create a public and private VM.

You've now configured routing between subnets to direct traffic from the public internet through the dmzsubnet subnet before it reaches the private subnet.

1. Connect **LAN to Azure with VPN** GW. 39m

* Fetaures and use of VPN GW, setup VPN GW, site-to-site VPN GWs.

VPNs use an encrypted tunnel within another network, to connect trusted private networks over an untrusted network (internet). VPN GWs are deployed in VNets to enable the connection, either site-site, point-site or Azure VNet-VNet, either **route-based or policy-based** (IKEv1 only, legacy), both use pre-shared key. 4 GW SKUs basic, VpnGw#/Az, # is 1 or 2 or 3.

**6 AZ Resources** needed: a VNet, “**GatewaySubnet**” (at least /27 mask). **PIP address**, Local network GW, VNet GW, Connection resource(s) setup. (“VGPLVC” ☺)

Connect LAN to VPN GW: LAN needs VPN GW device (policy or route-based), PubIP.

Now with the BGP protocol, you can also deploy VPN gateways in an active/active config.

In regions with availability zones, VPN and ExpressRoute GWs can use a zone-redundant config.

**Ex3:** Prep VNet and LAN using CLI. Simulate a LAN. Create 2 x VNet, 2 x subnet (with “GatewaySubnet”), 2 x LGWs (local network gateways).

**Ex4:** create site-site VPN GW using CLI. Create 2 x PiPs, 2 x VGW (VNet GWs), 2 x Connectors.

GW take **30m+ to create** .Test connectivity.

1. Connect using **ExpressRoute (EXPR)**. 40m

* features and capabilities of EXPR, describe use cases.

Extends LAN into Azure, dedicated and private, built-in redundancy.

EXPR Global Reach can connect private DCs through Expr circuits, e.g., Dallas to Texas DC.

ExpressRoute uses BGP routing . (Encrypted network communication is NOT a benefit.)

3 ways: CloudExchange co-location, Point-point Ethernet connect, Any-any connect (WAN).

Pre-requisites: connectivity provider, subscription registered with provider, an active Account.

Required: redundant BGP sessions to routing domains, public IP NAT service, reserved IP blocks.

Send the provider the Service key field to configure the connection. This can take days; there are a lot of configuration settings to be done. Use instead of site-site connectivity to handle enterprise-class and mission-critical workloads.

Microsoft peering enables a connection from the LAN to PaaS, MS 365/Dynamics 365.

1. Improve application scalability/resiliency by using **Load Balancer (LB).** 47m

* Identify the features and capabilities, deploy and config.

To minimize the effect of failures and increase resilience and stability. Main advantage of an availability set is VMS are available across physical server failures.

Use Availability sets within same DC, zones for regional DCs.

Basic LB allows sets; Std allows zones, Monitor, https probes etc. Internal or Ext types.

Distribution for traffic is 5-tuple hash, can be set to source IP affinity, by changing the value for Source affinity must be used for RDP and for media uploads (Session persistence to Client IP).

To create a LB rule, **one backend pool and one probe** must exist.

**Ex4:** Configure a public LB (Test it) and an internal LB. **Internal LB VMs must be on the same Vnet.** Create a resilient portal that's capable of adapting to meet the application requirements of session affinity. Differences between an internal/external LB.

1. **Troubleshoot** inbound NW connectivity for **LB**. 1h38

* Identify common problems, identify steps to resolve VMs response to health probe.

Consists of front IP, pool of VM IPs, routing rule(s), health probe, VMs in a VNet.

LB only sends requests to available VMs via health probe, only sends to healthy VMs.

**Probe** issues: wrong URL or port, or VM response fails if required port is closed.

**Data path** issues: NSG or FW blocking, VM down or failing, app isn’t responding, overload,port.

**Ex4:** Setup with script (up to 25m to run), test and create health charts.

**Ex5:** Identify and resolve inbound network connectivity, by reconfiguring using script.

Use Azure Monitor to check connectivity, visualize metrics for LB from Metrics in LB, the most important metrics are Data Path Availability and Health Probe Status.

In Azure Monitor, select Service Health > Resource Health > select LB as the resource type.

Check packet count. Use Ping internally to check NSG, FWs, VM stopped , etc.

1. Load **balance your web service traffic** with **Application Gateway** (AGW). 1h32

* Capabilities of LB of AppGW, create and config, use URL path-based routing

2 primary methods of routing : path-based routing (vid/images) and multiple site hosting.

AGW will automatically LB requests to servers in each pool using a **round-robin** mechanism.

AGWs use one or more listeners. If not setup, AGW creates a default health probe used to send a request to a server. A routing rule binds a listener to the back-end pools, which reference web servers. The hostname, port, and path in the URL of the request, routes to webserver.

**Ex3:** create 2 websites using CLI. Deploy sites.

**Ex5:** create and config AGW. Create Vnet, and subnet, AGW PiP, AGW, back-end pool of VMs, FW, temp listener, rule that routes and balances requests, create front-end port, and a listener. Add a health probe, config path-based routing, delete the unused rule.

**Ex6:** Testing. Go to the url (In DNS under AGW overview) test failover.

Optional: **web application FW (WAF)** to handle (**common threats**) requests before the listener.

Summary: load balance and app routing of AppGW. deploy multiple web sites across different services, and used AppGW to ensure availability of those services. use path-based routing to route requests based on the requested URL. deploy AppGW with the WAF enabled to take advantage of the built-in security that this feature provides.

1. Monitor/troubleshoot **end-to-end Network** using Network monitoring tools. 1hr

* Identify the Tools available; select the correct tools for various uses.

Network Monitor Consists of **Monitoring and Diagnostic** Tools.

**3 Monitoring:** 1. Topology (graphical), 2. Connection (catch config changes in NSGs**, latency**, probing IPs, RDP/HTTP or FQDN) 3. Performance, dropped packets, monitor **end-to-end**: Between branches and datacenters, VNets, connections LAN to Azure, ExpressRoute.

**6 Diagnostics:** 1. **IP flow** verify packets allowed/denied for a VM. 2**. Next hop** shows packet flow from a VM to target. 3. Effective Security rules, shows all **effective NSGs rules** applied to a NIC, and also unnecessarily open ports. 4. **Packet capture**, install Network Watcher **Agent VM Extension**. 5. Connection troubleshoot, check TCP between a source and destination VM, if unsuccessful you get details of the fault types. 6. VPN troubleshoot, diagnose problems with VNet GW connections. The request is a long-running transaction.

Use cases: connectivity issues in a single-VM, VPN faulty, servers aren’t listening on ports.

**Ex3:** Troubleshoot using monitoring/diagnostics, CLI. Use Network Watcher to see the topology. Create a Connection Monitor, to diagnose problems.

**Metrics and Logs:** 3 log display tools: Flow logs (store data in a JSON file, Power BI to visualize), Diagnostic logs (import into Power BI), Traffic analytics (requires Log Analytics workspace).

**Ex5:** Troubleshoot using **Network Watcher** metrics and logs.

**NSG flow logging requires:** 1. registration of the Microsoft.Insights provider, under Subscriptions> Resource providers. 2. create a storage account, 3. create a **Log analytics workspace.** 4. In NSG enable flow logs, configure link to storage account, enable Traffic Analytics status (on) and interval , select the workspace, SAVE.

Go to Network Watcher, under Logs select Traffic Analysis, and the workspace. Diagnose the problem(s) via views.

Summary: tools: Connection Monitor, IP flow verify, Next hop, Packet capture, Connection troubleshoot, Effective security rules, NSG flow logs, Diagnostic logs.

**~ Part 4 the END ~** Tony.

**[5. AZ-104: Monitor and back up Azure resources (10-15%)](https://docs.microsoft.com/en-za/learn/paths/az-104-monitor-backup-resources/)**

8 modules 6 hr 27 min

1. Holistic **monitoring strategy**. 57m

* Select monitoring solutions, integrate solutions into a strategy.

**Full stack monitoring** is a complete approach to the monitoring, triage, and diagnosis of application, infrastructure, and security issues that includes telemetry collection, tracking key **performance** indicators and the capability to isolate problems and perform root cause analysis.

Collect, analyse the info. you've collected, respond appropriately and more effectively to issues, to gain better insight. **The services** store the collected data in **workspaces** in Azure Monitor.

**Azure Sentinel**, begins to collect data from sources as soon as you create them, collect data on the devices, users, infrastructure, and applications, detailed overview of your organization, potentially across multiple clouds and on-premises, correct tools, identify and handle threats.

**Playbooks (**by creating a logic app**) automate your response** to alerts, using Logic Apps. Use hunting queries. Use notebooks to automate your investigations. Notebooks are playbooks that can consist of investigation or hunting steps that you reuse or share with others. Use Azure Notebooks for Azure Sentinel to develop and run your notebooks.

Create a **Log Analytics workspace**, add to **Sentinel**. write queries. Use the Log Analytics agent.

**Application Insights** automatically gathers information related to performance, errors, and exceptions in applications, availability tests different geographic locations,

Use the investigation map, drill down into incident, look for user entities affected by the alert.

Use cross-resource query to check Azure Security Center and App. Insights workspaces together.

Use alert rules to dictate how alerts should be handled. Send notifications through email or text message, or use runbooks and webhooks to respond to alerts in an automated way.

Enable **Azure Monitor VM insights** to adds the required extensions and configuration to your VMs and VMs scales sets to collect/store a fixed set of usage and performance measurements.

**Security Centre** gives detailed analyses of data security, network security, identity and access, and application security, is integrated into PaaS. For IaaS services, enable automatic provisioning. Use JIT access to prevent persistent access to VMs.

**Metrics** , how the resource is performing and resources consumed.

**Logs** contain records (times, events) that show created or modified resources.

* With **Azure Monitor and VM insights**, you analyze and address issues that affect the health and performance of your environment, and query to analyze data in a single location. **Security Center**, to identify and address risks to your security posture.

**Sentinel**, to have security incident management, investigation, and response capabilities.

1. **Monitor health** of VM using Metric Explorer and metric Alerts. 43m

* Identify collectable metrics and diagnostic data, configure, diagnose.

Enable **basic metrics** by creating and associating with a storage account, VM with **Boot diags enabled** , in Metrics, add Cpu %, inbound flows.

**Overview** there are 4 default graphs, CPU, Disk Bytes and operations, and NW.

**Diagnostics** extension: set OS guest diagnostics to On (before VM creation), or Enable Guest-level monitoring (after creation). Select metrics.

Custom dashboard is especially helpful when you have to monitor more than one VM.

To create alert for DDOS attacks, Monitor, metrics, specify the PubIP address as resource.

Create alert rules, under scope select resource, add action and create action groups.

1. Analyse Infrastructure using Azure **Monitor logs** 36m (?)

* Identify the features and capabilities; create basic queries to extract info.

**Logs** contain time-stamped info about **when** changes are made to resources. **Metrics**: values that describe aspects of a system at a point in near real time, shows performance of resources.

For VMS, you can install the **Log Analytics agent** and configure it to send to a LA Workspace.

Query logs with the **Kusto** query language, also used by Azure Data Explorer.

1. Monitor performance of VMS using Monitor for VMs. 48m

* Evaluate Azure Monitor Log and Monitor for VMs, config a LA workspace, build queries.

Monitor Logs collects and organizes **log data** from Azure resources, and stored in **LA workspace**.

Native Data is collected from Azure tenant, subscriptions, resources, Guest OS, Application.

Resource-context LA deployment, when only needing to query logs generated from resources.

Monitor for VMs provides access to log data without exposing the user to underlying queries.

**Exercise** - Set up a Log Analytics workspace and Azure Monitor for VMs.

Query logs with the Kusto query language, also used by Azure Data Explorer. Azure Monitor organizes log data into tables. LA uses a schema to build tables.

1. Improve incident response **with alerting.** 53m

* Configure Alerts, use smart groups to reduce noise.

Native Data is collected from Azure tenant, subscriptions, resources, Guest OS, Application.

Alert rule: Resource, trigger, actions (+groups), alert details. 3 alerts: New, Ack’d and Closed.

E.g. Log data type: HTTP response records. i.e. Not metric, no values.

Dynamic metrics > look-back period and number of violations.

Dimensions enable monitoring from multiple targets. A scaling metric alert (only VMs) is individual to the resource that triggered it.

**Log alerts** use log data (from any resource) to assess the rule logic and possibly trigger an alert. Search rules: query, Time period, Frequency, trigger. Results: number of records or metric value.

**Activity log alerts,** to receive notifications when: **Specific changes** occur on a resource, e.g. a VM is deleted or roles are assigned. **Service health events**: notice of incidents and maintenance.

When creating an activity log alert, select Activity Log for the **signal type**.

Creating a **service health alert**, no need to select a resource, as the alert is for a whole region.

**Alert actions** > send email, send SMS, create an Azure app push notification, make a voice call, call an Azure function, trigger a logic app, send a notification to a webhook, create ITSM ticket, use a runbook (to restart a VM, or scale a VM up or down).

**Smart groups,** a dynamic filter applied to all the alerts, reduces noise by 90%, automatically created by Monitor, using ML algorithms. 2 ways to get to smart groups: from the Alert Summary pane, or All Alerts pane. Next, select Alerts by Smart Group.

1. Application **Insights runtime** on an Azure **web app**. 45m

* Monitor a web app, e.g. page load times, events and metrics, charts.

To send telemetry data to an Application Insights resource from an app, you need to configure the app with the instrumentation key of the **Application Insights** resource.

**Runtime** instrumentation and auto client-side instrumentation is supported only on Windows, App monitoring is enabled without code changes using auto-instrumentation or codeless attach.

For Linux, **Build-time** instrumentation must be used.

Use Alerts to make sure admins know a web app becomes overloaded.

Add a new app setting APPINSIGHTS\_JAVASCRIPT\_ENABLED to enable automatic client-side telemetry and set it true.

Re-publish the Application Insights dashboard, if other users can’t see it. Application Insights resource stores telemetry data for the app. Data visualization: Portal, power BI, Visual Studio and Custom with API. Custom charts on **Metrics** page.

1. Protect VMs with **Backup**. 35m

* Identify needs, backup and restore a VM. Backup maintains copies of stateful data.

Options: VMs, On-premises (MARS, MABS, DPM), Azure files, SQL server, SAP HANA.

Recovery Point Objective (RPO) is frequency you take backups. Recovery Time Objective (RTO) is the amount of downtime a business can tolerate. For HA: LRS, GRS, and RA-GRS replication.

Soft delete, the backup data is retained an additional 2 weeks.

Recovery Services vault gives built-in monitoring and alerting capabilities.

Azure VMs are backed up by taking snapshots, to the Vault as per defined policy.

Snapshot (5 days)> Application (uses VSS), file system or Crash consistency (VM was off).

Restore types: create new VM in same region, restore disk, replace (existing) disk, cross region.

Recover files by mounting snapshot using the iSCSI initiator.

Restore encrypted VM> whole VM only, Replace existing VM option isn't available.

Restore a VM, create a storage account to use as a staging location. Stop theVM, go to Backups on VM, select restore VM, select restore point, select Restore Type as replace Disks

1. Azure **Site Recovery -** **ASR**. 1hr

* Protect VMs with ASR, run a DR drill, failover and failback.

Replicates VMs to other regions, mirrors availability sets, VNets, LAN premises migration.

Creates snapshots and recovery points, DR drills are enabled for testing configs, Failover and Failback. DR drills have no impact on production.

Needs a Recovery Services Vault (needs storage account), to install Site **Recovery mobility service** extension. Resources are appended with the “ASR” suffix.

**Ex4. Prepare for DR**: Create RG with VM region A, VNet and storage account, create RG in region B. 1. Setup resource “Backup and Site Recovery”, in region B. Add a Recovery Services Vault. For a VM to register in Site Recovery, the latest root certificates must be installed. 2. Configure target resources, in region B, storage account and match VM size. Automated if migrating LAN VMs to Azure. 3. If migrating from LAN, configure outbound network connectivity URLs.

4. Set up replication, to enable replication on a VM, must have RBAC rights.

Under Recovery Services Vault, select Monitoring, select Site Recovery jobs, approx. 10 mins.

**Ex 6.** Disaster recovery drill, see RPO and RTOs. **Recovery plans** support grouping of multiple VMs and workloads, to test infrastructure combinations. Setup a new plan in the vault under Recovery Plans (Site Recovery). Give it a name. select items, OK, Create.

When complete, go to the plan, Test Failover. Network config can take several minutes to autocomplete, and do initial sync. Running a failover test may not be available for a while.

After Test failover, if you Commit the failover, then Site Recovery deletes all the source VM recovery points, and completes the failover.

**Ex8.** Failover and failback. After failover, reprotection is needed for replication to restart, and failback to be available.

3 most common issues: quotas, added more disks, check that the latest root certificates are installed (and latest updates).

1. **Reliable** Well-Architected framework. 1hr

* Design a high availability (HA) app, incorporate DR capabilities, protect the application from data loss or corruption, i.e. an app available and recoverable, by HA, DR and backups.

**HA:** Evaluate: SLAs, HA capabilities of app, HA capabilities of dependents.

Availability sets, Availability zones, Load balancing, Platform as a service (PaaS) HA.

**DR:** A DR plan is a doc that details the procedures that required to recover from data loss and downtime caused by a disaster, and identifies who's in charge of directing those procedures.

Recovery Point Objective **(RPO):** The max duration of acceptable data (down) loss. RPO is measured in units of time: "30 min of data" or "4 hrs of data”. RPO is about limiting and recovering from data loss, **not data theft**. How far **back in time** can you go ?

Recovery Time Objective **(RTO):** The max duration of acceptable downtime, where "downtime" needs to be defined by your spec. E.g. if the acceptable downtime duration is 8 hrs in the event of a disaster, then your RTO is 8 hrs.

Designing for disaster recovery, data recovery and replication (starage, SQL, Cosmos), Azure Site Recovery (ASR), Test the DR. How to: restore backups, failover (replication), fix NW connectivity.

**Backup/Restore:** Azure Backup is a family of backup products that back up data to ASR.

Recovery Service vaults is storage that are dedicated to holding data/config backups for MMs, servers, and individual workstations and workloads.

**4 products:** Backup Agent, Data Protection Manager, Backup Server, IaaS VM Backup.

Backup systems are incomplete without a strategy to: verify backups, test restore procedures.

Use availability sets and availability zones, load balance with Traffic manager, Application g/w and LB. Use DR and know how to define RPO and RTO. Use ASR, test the recovery plans.

Incorporate backup/restore into the strategy.

~ **Part 5 the END** ~ Tony.

END AZ104