**Assessment Notes- Claudiu Hobjila | August 2019**

**Storage Account with HNS enabled (ADLS Gen2)** (10 mins)

* deployed to West US 2
  + so we can initiate [a manual failover](https://docs.microsoft.com/en-us/azure/storage/common/storage-initiate-account-failover) to cover any DR ( disaster recovery) scenario.
  + This feature is in preview and is available only for West Us 2 & West Central US
* the access tier has been set to “Hot” assuming the data on this storage account is accessed frequently. This way we optimize costs for frequently accessed data.
* For a HNS account we can make it either a [BlobStorage Account or a GPV2 account](https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of-storage-accounts).
  + Assuming we might need other storage services like Tables or Queues & considering that Microsoft recommends using a GPV2 account in most scenarios, I create a gpv2 account with HNS enabled.
* Diagnostic Logs for the storage account (available under $log container in ASE).
  + As Blob APIs are not yet interoperable with ADLS Gen2 APIs we can`t yet enable logging
  + The interop is currently in public preview so we would have to sign up here

Multi-protocol access on Azure Data Lake Storage

<https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-multi-protocol-access>

* + This is another reason why I deployed the account to West US 2

**Key Vault** (20 mins)

* Deployed to the same region as the storage account
* Gave myself full control
* Also added another Access Policy allowing the web app to get and list the secrets.
* The secret created contains the access key for my ADLS Gen2 account

**Web App** <https://testwebappclaudiu.azurewebsites.net> (45 minutes)

* Deployed into the same region as the account & key vault
  + This way we avoid any transactional charges as Azure do not charge transaction within the same datacenter
    - NOTE: as I used my current Subscription and not a free one, there were some deployment constraints in West US2 at the time I was doing the assessment, so I deployed the web app to Central US. Ideally, I would have deployed it to the same region.
* I chose a Standard SKU => this way I will be able to integrate the web app with the vNet.
* Did not use Application Insights to monitor the web app, but in a production environment this would be highly recommended

**Load Balancer** (30 minutes)

* Not sure where and why the load balancer would be needed in this context. If we would have hosted the web site on multiple VM instances, that would make sense.
* Since we are using a Standard App Service plan we can configure custom autoscale rules based on metrics. This will scale out the app automatically (e.g. when the CPU is over 75% for more than 5 minutes), adding more instances as needed.
* A scale out operation is the equivalent of creating multiple copies of the web site and adding a load balancer to distribute the demand between them. When you scale out a web site in Windows Azure Web Sites there is no need to configure load balancing separately since this is already provided by the platform.
* This topic is discussed here in more details
* Scaling Up and Scaling Out in Windows Azure Web Sites

<https://azure.microsoft.com/en-us/blog/scaling-up-and-scaling-out-in-windows-azure-web-sites/>

**VNet** (70 minutes)

* Selected a larger address space to have enough addresses available in case it will be needed in the future
* I added a subnet called subnet1 with an address range of 256 addresses 10.0.0.0/24 – first ones are taken by Azure.
* I enabled service endpoints so I will be able to integrate the vnet with my storage account at a later step (added Microsoft.Storage service provider to my service endpoint)
* Also enabled Microsoft.KeyVault service endpoint to be able to integrate it with the Key Vault
* Now I enabled Firewall & Virtual Networks for my storage account
  + and I allowed only clients within this subnet to be able to access the account.
  + Also whitelisted my client IP address so I can access the account from my local machine
* Did the same with the Key Vault and with the Web App
* I created a vNet Gateway to be able to add the webapp to the vNet ( the deployment may take several minutes)
  + It has to be deployed to a dedicated subnet called gateway subnet- ideally you would have your gateway subnet address range as the first subnet in your vnet
  + A VPN gateway requires the -GatewayType Vpn.
  + VPN type is Route-Based- sa required by most configurations. Policy Based VPN can only be used with a Site so Site connection. More info [here](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#vpntype)

**Note**

* There might have been 2 errors while exporting the template so 2 resources may be missing ( access policies & storage containers). Not sure yet why that happen but I will take the time to investigate.
* Of course, the “solution” needs some fine tuning as it is not a “plug and play” configuration, but rather a concept.