ABDULHADI

AZ 103
Azure Administrator

Preparation Handbook

Eng. Abdulhadi Bakhash

Abdulhadi.Bakhash@hotmail.com

Version 1.0

1/10/2019 Utrecht

ABDULHADI

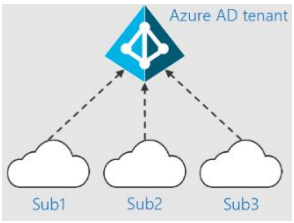
Contents

1 Manage Azure subscriptions and resources (15 -20%)

1.1 Manage Azure Subscription

1.1.1 Azure Account, Manage Group, Tenant and Subscriptions[1]

- **Azure Account** is the email and password that allow you to login into Azure.
- An **Azure account** is a user **identity**, one or more Azure subscriptions, and an associated set of Azure resources.
- The person who creates the account is the **Account Administrator** for all subscriptions created in that account. That person is also the **default Service Administrator** for the subscription.
- Azure **subscriptions** help you organize **access** to Azure resources.
- Each subscription can have a **different billing and payment setup**, so you can have different subscriptions and different plans by office, department, project, and so on.
- Every service **belongs** to a subscription, and the **subscription ID** may be required for programmatic operations.
- **Multiple** subscriptions can trust the **same Active directory**, but each subscription trusts **only** one Active directory.



- A **Tenant** is a **dedicated** Azure AD service instance that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Office 365.
- **Each** Azure AD tenant is **distinct** and **separate** from other Azure AD tenants.
- A **tenant** is an instance of Azure Active Directory. **contosoblue.onmicrosoft.com** is an example of a tenant.
- **Billing** for Azure services is done on a **per-subscription basis**. If your account is the only account associated with a subscription, then you are responsible for billing.
- **Azure AD** is identity system for Microsoft business services.
- If you create a subscription with a personal account, an Azure AD tenant is created for you.
- Subscriptions **can be transferred** between Azure AD tenants.

[1] https://bit.ly/2KOj7uq

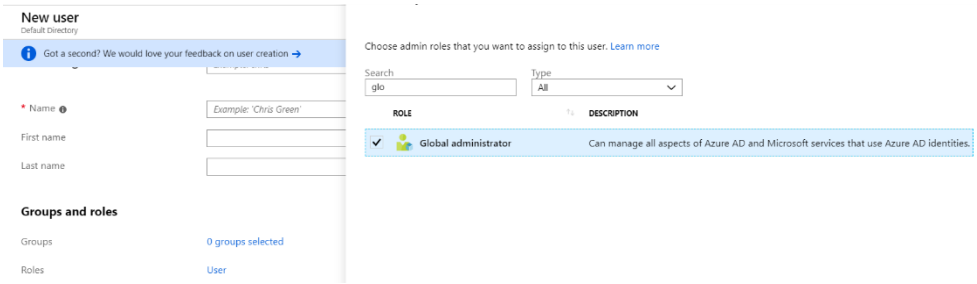
1.1.2 Azure Deployment Models[2]:

- There are two way to deploy your resources is Azure: The Classic and the Resource Manager Model.
- For this exam (Azure 103) and due to MS recommendations, we are only interested in **Azure Resource Manager (ARM)** Deployment Model.
- In **classic** Model, each resource is **independent**, no way to group resources.
- In **ARM** Model, you can use Resource Group to group all the dependent resources together.
- Terminology:
  i. **Resource**: The Azure service that you create: VM, VNet …
  ii. **Resource Group**: **Container** that hold the related resources for an Azure solution.
  iii. **Resource Provider**: A **service** that supply the resources: Microsoft.compute, Microsoft.Storage….
  iv. **Resource Manager Template:** A Java Script Object Notation **(JSON)** file that define azure resources.
- You **can't** unregister a **resource provider** when you still have resource types from that resource provider in your subscription.
- The **resources** in a Resource Group can allocated in **different regions**. But each resource can **only** be a member in one resource group.
- In **PowerShell**, to list all the available resource provider:
  i. Get-AzResourceProvider -ListAvailable
  ii. Get-AzResourceProvider -ProviderNamespace Microsoft.compute
- Bu using a **JSON** file you can deploy the whole Azure Solution together, **whereas** in the PowerShell or Power CLI you need to deploy each resource **individually**.
- https://github.com/Azure/azure-quickstart-templates : here you can find many prebuild JSON file for Azure solutions.

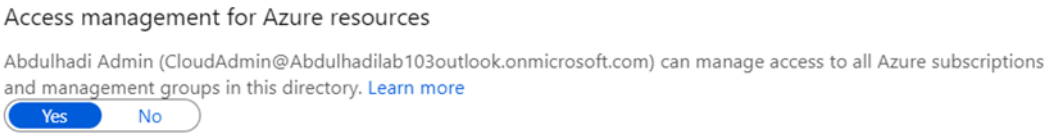
1.1.3 Assign Administrative Permissions[3]

[2] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model
[3] https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

- We need to distinguish between the role granted to the user through the **Directory rules** in the Azure AD and the **RBAC** roles for **granting** administrative permissions to the Subscription.
- **Granting Directory Rules:**
  i. Add users/Guest users to Azure AD and give them through Directory Role the **Global Administrative roles.**
  ii. All users' names in the Azure AD will be formed like: username@Abdulhadilab103outlook.onmicrosoft.com.
  you can add you own domain name by using: **Add custom domain** feature within the Azure AD blade.
  iii. Giving a user the role of Global Administrator and then the owner
    1. Owner User → AD → New User → Add roles → Global Administrator



2. From the **new User Account**→ AD → Probertites → Yes (Access management for Azure resources) [4]



- **RBAC roles:**
  i. Subscription → Access control (IAM) → Add → Role (Owner) for the wanted user.

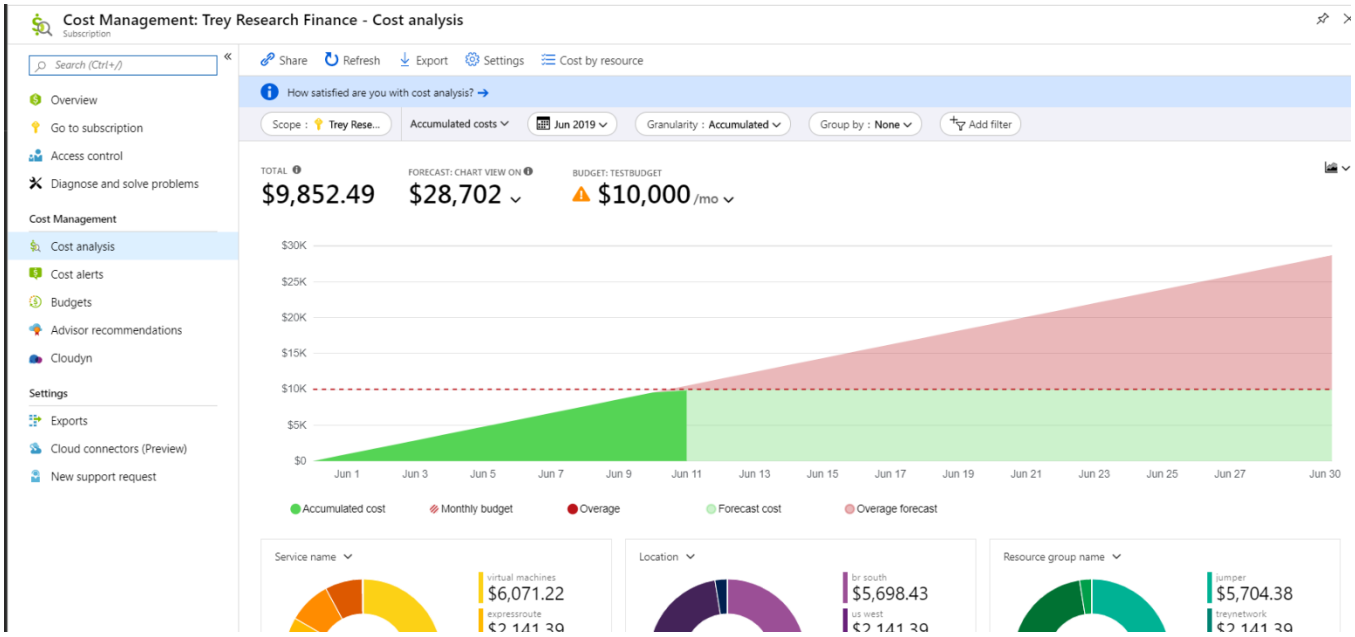
1.1.4 Configure Cost Center Quotas and Tagging[5]

- The most used ways to manage costs in Azure:
  i. Filters inside Subscription → Cost Analysis → Resource groups
  ii. Filters inside Subscription → Cost Analysis →Tag

[4] https://docs.microsoft.com/en-gb/azure/role-based-access-control/elevate-access-global-admin
[5] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

iii. Multiple Subscriptions

- Tag is used to **logically** organize resources for billing purpose: the form of the tag is: [Name] : [Value]
- You could add a **policy** to force adding tags to **Subscriptions** and **Resource groups**.

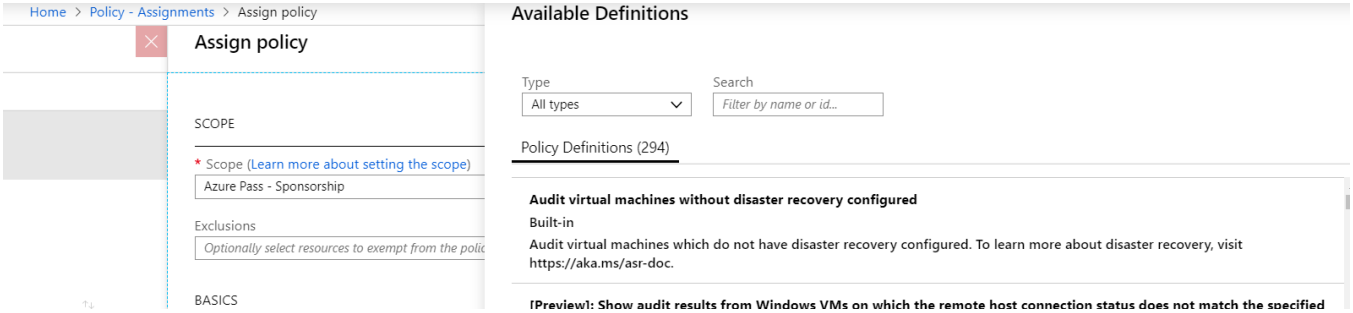


1.1.5 Configure Subscription Policies[6]

- **Azure Policy** is a service in Azure used to create, assign and manage policies.
- These policies will **enforce** rules to the resources to stay compliant with the corporate standard. Examples:
  i. Allow only a certain SKU size of virtual machines in your environment
  ii. Ensure that all SQL servers use version 12.0
  iii. Restrict the locations to use when deploying resources
  iv. Enforce resource tagging,
  v. Allow creation of the resources only within West Europe.
- **After** applying a Policy, azure will evaluate the **whole** subscription and exam the procreated resources to evaluate their compliant and will prevent any new resources to be created without the complaint to the new policy. Evaluations happen about **once an hour.**

[6] https://docs.microsoft.com/en-us/azure/governance/policy/overview

- A policy can **only** assigned to **Management groups**, **subscription** and **resource group** level.
- From Policy Definition → Build in/Custom policies (currently 294 policy)



- Apply multiple policies and aggregate policy states with **policy initiative**
- Each Policy has its own **Parameters** that need to be assigned.
- The policy evaluation needs around **one hour**.
- And if the compliance blade did not give a report, make sure that the subscription is registered to: **Microsoft.policyInsight** resource provider:
  i. Get-AzResourceProvider -ProviderNamespace Microsoft.policyInsights
  ii. Register-AzResourceProvider -ProviderNamespace Microsoft.PolicyInsights
- You could use the built-in policies or great your own policy:
  i. In PS
    1. To defined a Policy: New-AzPolicyDefinition …
    2. To Assign a Policy : New-AzPolicyAssignment …
  ii. In Bash (CLI)
    1. To defined a Policy: az policy definition create …
    2. To Assign a Policy : az policy assignment create …
- When a Policy is evaluated, the **Disable effect** is evaluated first to decide whether the rule should be evaluated afterwards.

1.1.6 Scripting:

- There are many ways for scripting in Azure
  i. Cloud Shell
  ii. PowerShell Az
  iii. Bash /CLI
  iv. JSON for template

- In both PowerShell and CLI, you need to **download** the **Azure model** inside them.
  i. Install-Module -Name Az -AllowClobber
  ii. Install-Module -Name Az -AllowClobber -Force
- Updating the Az is **not possible**, so to get the latest update, you need to **reinstall**.
- **CLI** command **works** in PowerShell and Cloud Shell

1.1.7 PowerShell Basics[7]

- If you already have **AzureRM** Modules installed on your computer, you'll need to uninstall the existing AzureRM Modules before installing the new **AZ Modules**, as the modules **cannot function side-by-side**.
- https://github.com/PowerShell/PowerShell/releases
- To connect to Azure from PS:
  - Connect-AzAccount
- For VM
  - Get-AZ VM (New/Remove…)
- For VNet
  - Get-AZVirtualNetwrok (New/Remove…)
  - Get-AZVirtualNetwrokSubnetConfig (New/Remove…)

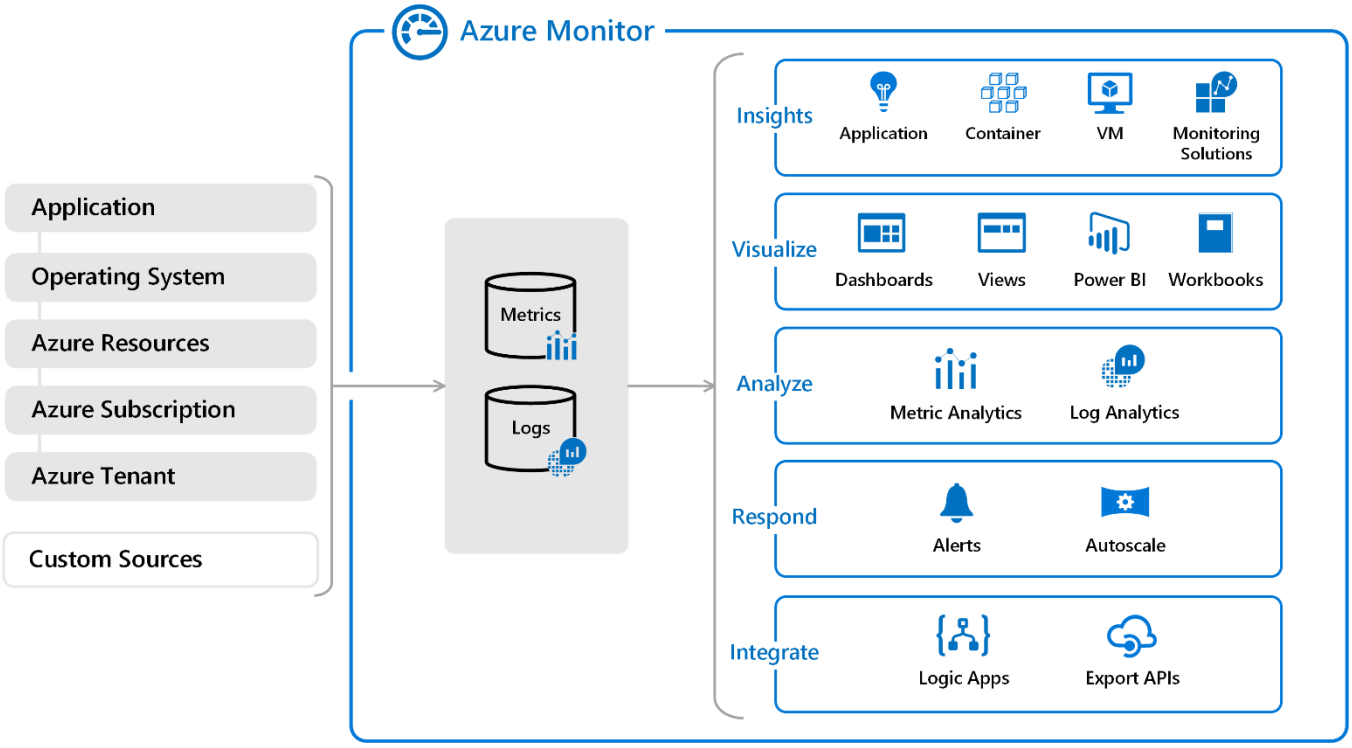
1.1.8 Azure CLI[8]

- Azure CLI is **cross-platform tool** available for **Windows**, **OSX** and **Linux**
- For VM
  i. Az vm list / create/delete …
- For VNet
  i. Az network vent list / create/delete …
  ii. Az network vent subnet list / create/delete …

[7] https://channel9.msdn.com/Blogs/Taste-of-Premier/PowerShellBasicsPart1
[8] https://docs.microsoft.com/en-us/cli/azure/ad/app?view=azure-cli-latest

1.2 Analyse Azure Utilization and Consumption:

- **Azure Monitor** collects and aggregates data from a variety of sources into a common **data platform** where it can be used for analysis, visualization, and alerting.



- **Data platform** is Storage and we have 4 types of storage in Azure Storage Account:
  i. Blobs
  ii. Files
  iii. Tables
  iv. Queues
- Storage analytics **metrics** are available for blobs, files, tables, and queues.
- Storage analytics **logging** are available for blobs, tables, and queues.
- All metrics data is written by the services of a storage account. As a result, each **write operation** performed by Storage Analytics is **billable**.
- By default, storage analytics retention is set to zero (**0**) days. This means storage metrics and logs are kept **indefinitely** and you are **responsible for cleaning up the storage**.

1.2.1 Configure Diagnostic setting on Resources[9]

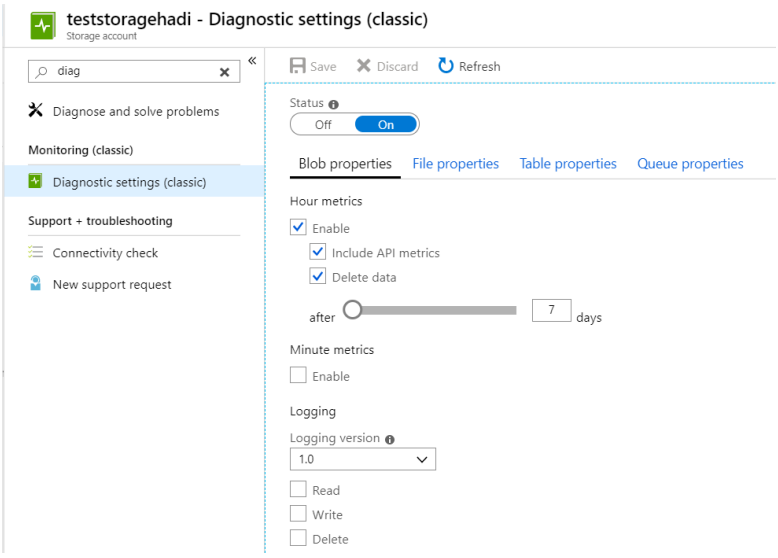
[9] https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/resource-logs-overview#resource-diagnostic-settings

- Azure **Resource logs** are **platform logs** emitted by Azure resources that describe their internal operation.
- All resource logs share a common top-level schema with the flexibility for each service to emit unique properties for their own events.
- Resource logs are **automatically** generated by supported Azure resources, but they aren't **collected** unless you configure them using a **diagnostic setting**.
- Create a diagnostic setting for each Azure resource to forward the logs to the following destinations:

Destination	Scenario
Log Analytics workspace	Analyze the logs with other monitoring data and leverage Azure Monitor features such as log queries and log alerts.
Azure storage	Archive the logs for auditing or backup.
Event hub	Stream the logs to third-party logging and telemetry systems.

- **Resource logs** were **previously** known as **diagnostic logs**.
- Resource logs **Vs** Activity logs:
  i. Activity logs: provide information about the operations on a resource from the **outside**.
  ii. Resource logs: provides information about the operation in the resource from the **inside**.
- To collect the Diagnostic Log, we need to **turn on** the diagnostic setting feature from the resource blade.
- Retrieving Diagnostic data **differ** between Azure resources, we will cover three different resource:
  i. Storage Account → Diagnostic logs
  ii. Web App service → App service logs
  iii. Virtual Machine → Diagnostic logs

- From **Storage account blade**: Diagnostic settings (classic) →

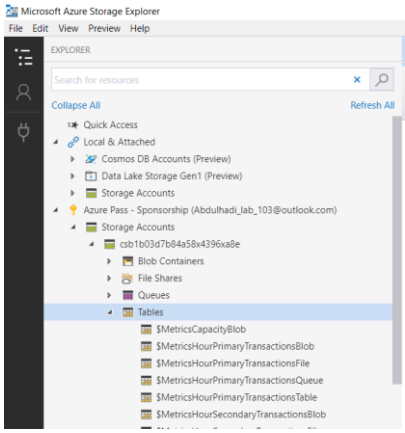


  i. We can diagnose **metrics** data and **logging** data for Blob, Table and Queue.

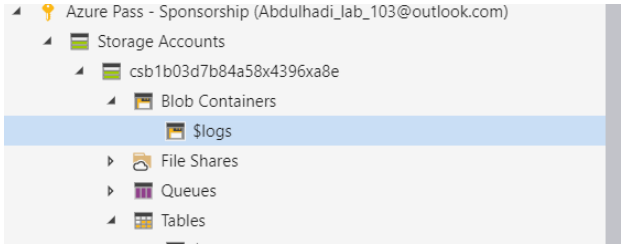
  ii. For the **File** properties, we can **only** diagnose the metric data.

  iii. **Metric** information is captured within the **table storage** in the same storage account.

  iv. From storage account → Overview → Tables. here you can't see the metric data because Azure portal **does not show data for metric data**. You need to install **Azure Storage Explorer**.



  v. The **Logs** information is captured within the **Blob storage**. And also, you only can see it through the **Azure Storage Explorer**.

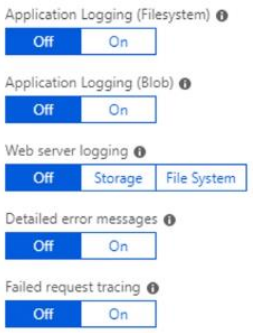


- To recap: In Storage Account:

  i. **Metric** data is storage in **Tables**, can be only seen in **Azure Storage Explorer**

  ii. **Logs** data is storage in **Blobs**, can be only seen in **Azure Storage Explorer**

- From **Web App service** blade → App service logs →

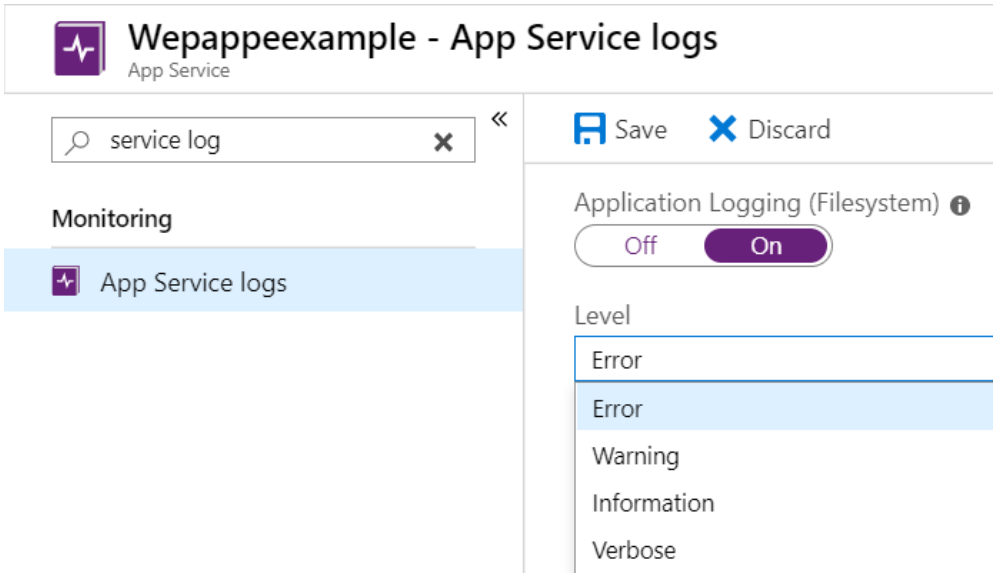


  i. Web App service is **PaaS**.

  ii. We can capture both the **Application** and **Web server** logging. And for both of them the storage type should be defined.

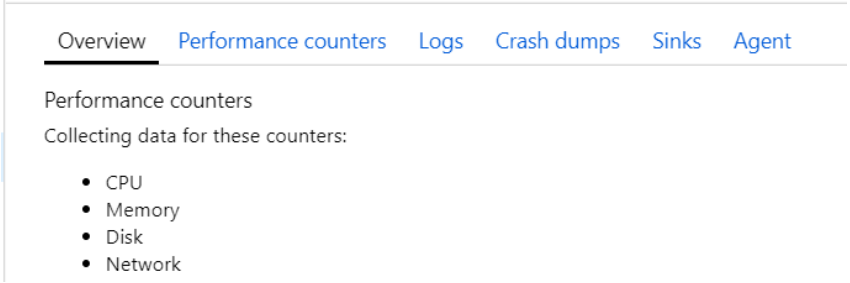
    1. Blob storage is uses for keeping history
    2. File system is used for **streaming logging**.

  iii. One of the options in the Access level of the Application logging is **Verbose**, which means that you want to capture the whole information.



  iv. You can see the logs information through the **Log Stream** feature within the Web App blade.

- From **Virtual Machine** blade → Diagnostic setting



  i. Azure Monitoring collects two levels of metrics:

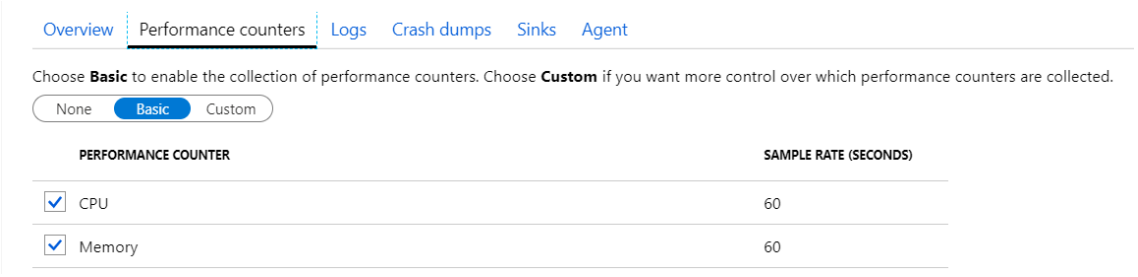
    1. **Host-level metrics:** Done by default**,** like CPU utilization, disk and network usage – for all virtual machines without any additional software.

2. **Guest-level metrics:** For more insight into VM, you can collect, logs, and other diagnostic data using the **Azure Diagnostics agent**. You can also send diagnostic data to other services like **Application Insights.**

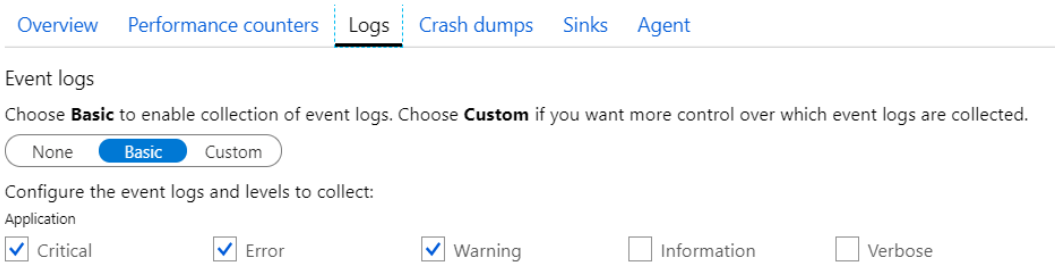
ii. We need to install the **Azure Diagnostic agent** on the Virtual machine to enable the VM's Guest-level metrics diagnostic in Azure.

iii. The Diagnostic require a **storage account** that cost **money**.

iv. Performance counters:



v. **Logs**: Similar to Windows Event logs in the Windows Systems:



vi. **Crash Dump**: To investigate the context of the memory and other advanced metrics, its disabled by default.

vii. **Sink**: External services, like Application Insights.

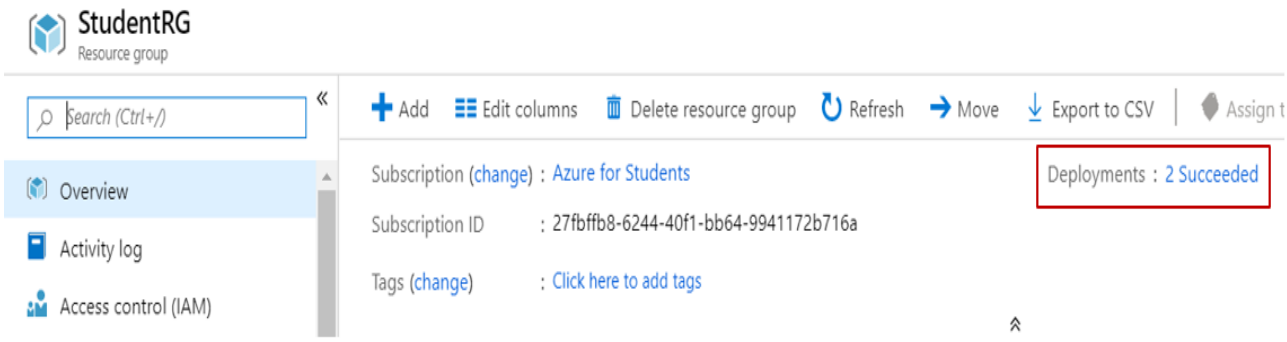
- From **Monitor** service, you could check the Virtual Machine from **Insight**→ Virtual Machines on the left side of the blade.

1.2.2 Create baseline for resources[10]

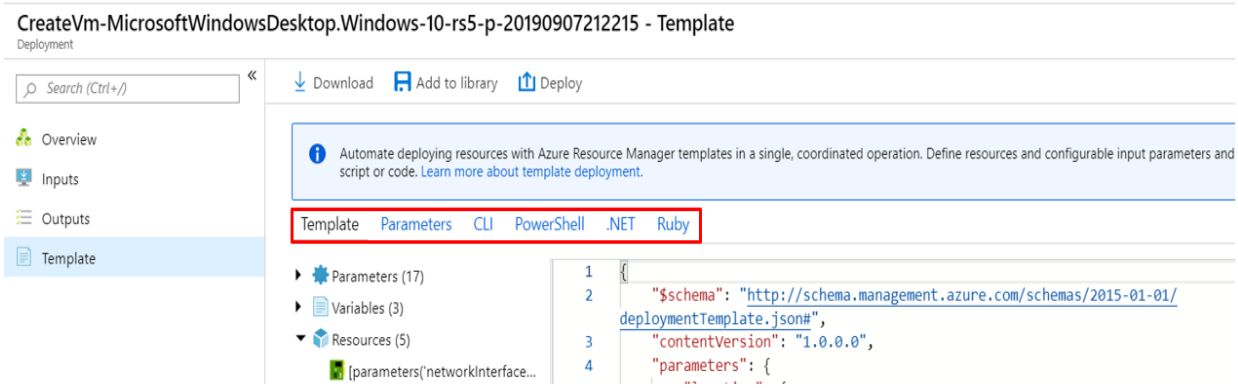
- A baseline is used to keep your resources operating within specified limits. This can be done by:
  - A script (PS, CLI)
  - An ARM templates.

[10] https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/alerts-dynamic-thresholds

- **Azure Resource Manager (ARM)** is the deployment and management service for Azure.
- It provides a consistent management layer that enables you to create, update, and delete resources in your Azure subscription.
- You could reach the deployment for most of the resources in the RG from the Overview blade and see the **Deployments**.

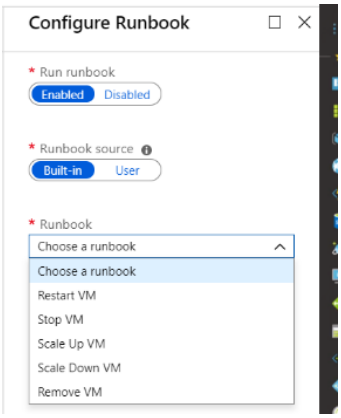


- The **Template deployment** are saved as **JSON** files. For resource Groups



- The first 2 tabs are the most important (**Template and Parameters**), the other 4 tabs(scripts) are only to redeploy the JSON file.
- These files can be saved or download or Re-deploy.
- For **individual** resources, you can find the deployment under the tab **Automation Script** or **Export Template**. But the JSON file is more **readable** than the files in the Deployment section in the RG.
- **Not** all resources can be deployed in a JSON file like RG.
- You can check the created template from the **Template resource**.

1.2.3 Create Action Group[11]



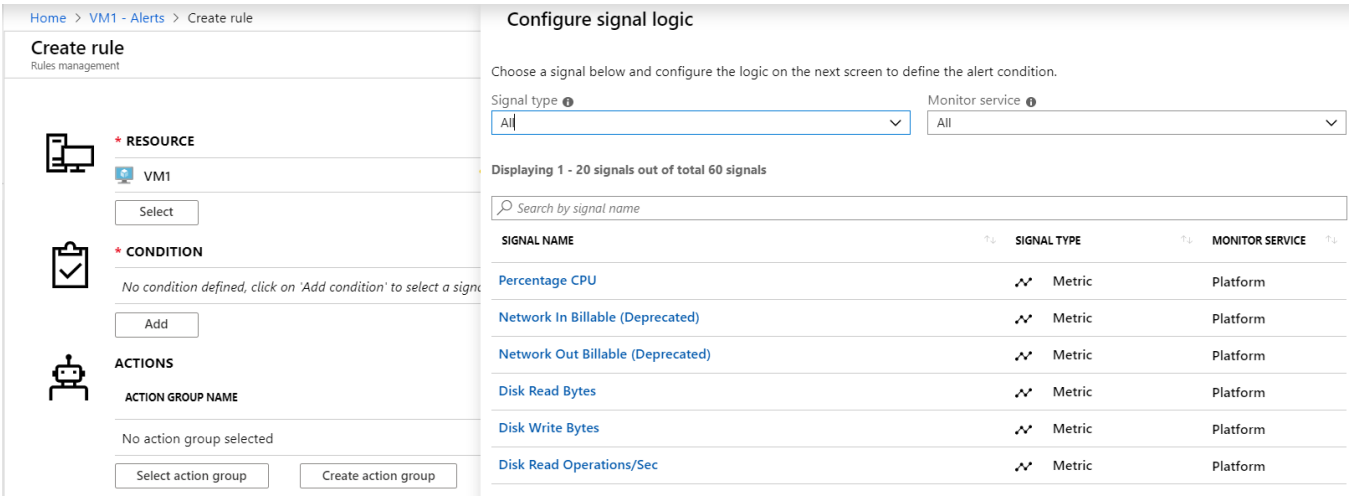
- Azure resources like: **Azure monitor** and **service health alert** are configured to use **specific action group** whenever an alert is triggered.
- We can add **multiple** actions groups for one Alert
- Monitor blade → **Alerts** → Manage Action → Add action group
- One of the Action types is **Runbook**: Which give some option to control the Azure VMs.

1.2.4 Create and test Alert[12]

- After **collecting** the data in **Monitor service**, the logical things to do is define some alerts rules.
- You can configure Alerts **either** in individual resource level or in Azure Monitor blade.
- Azure **Monitor** is the **core monitoring service** in Azure, other monitoring services like **Log Analytics** and **Application Insights** are part of Azure monitoring.
  i. **Log Analytics**: Provide infrastructure monitoring level, stores the data from Application insights, Azure security centre and other log data and provide **Analytics** capabilities.
  ii. **Application Insights**: provide application level monitoring for the **Web Application**.
- Alerts Types are:
  i. **Metric Alerts**: Evaluate at regular intervals.
  ii. **Activity Log Alerts**: They activated when new activity log is accrues that matches the conditions specified in the alert.
  iii. **Log Alerts**: Consist of log search rules created for Azure **Log Analytics or Application Insights.**

[11] https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/action-groups
[12] https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/alerts-metric

- Creating an Alert consist of 3 steps:



i. Define a **RESOURCE**: Subscription, VM, RG ….

ii. Define a **CONDITION**: Available signal types depends on the chosen recourse

iii. Define an **ACTION**. The Action Group Name

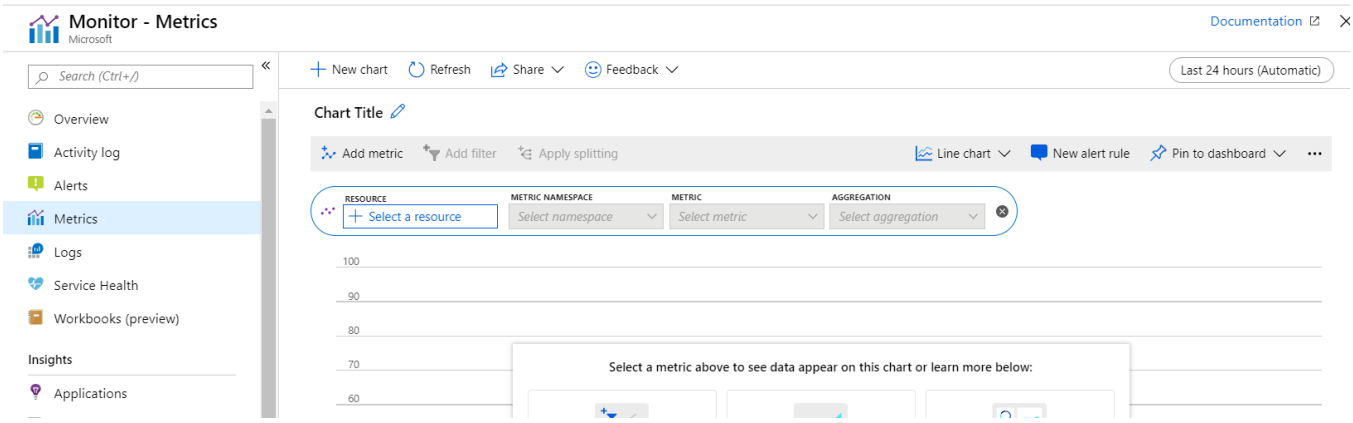
- When Selecting the resource(s) you want to monitor. **Available signals** for your selection will show up on the bottom right.
- For **Log Alert**: you need to choose either Log Analytics or Application Insight as a source in the first step of creating an Alert.

1.2.5 Analyse metrics across subscription[13]

- The Azure Monitor data platform is based on two fundamental data types: **Metrics** and **Logs.**
- Metrics are **numerical values** that describe some aspect of a system at a **particular time**.
- Metrics are collected at **regular intervals** and are useful for alerting because they can be sampled frequently, and an **alert** can be fired quickly with relatively simple logic.
- Basically, metrics are used when creating charts is needed.

[13] https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-metrics

- If you want to save your charts, you need to **Pin to dashboard**.

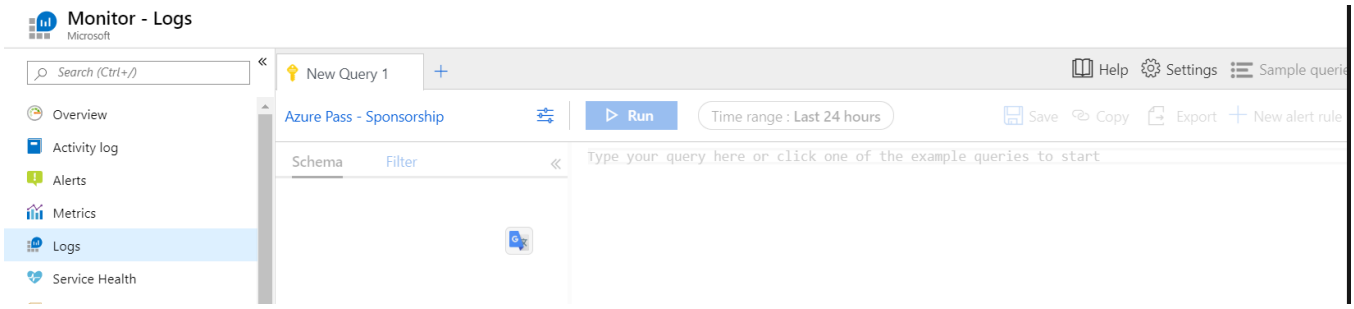


1.2.6 Logs in Azure Monitor[14]

- All data collected by Azure Monitor fits into one of two fundamental types, **Metrics and Logs.**
- Logs in Azure Monitor contain **different kinds** of data organized into **records** with different sets of properties for each type.
- Logs in Azure Monitor are especially useful for performing **complex analysis** across data from a variety of sources.
- Logs **can** contain **numeric values** like Azure Monitor Metrics but typically contain **text** data with detailed descriptions.
- They further differ from metric data in that they **vary in their structure** and are often **not** collected at **regular intervals**.
- Data in Azure Monitor Logs is retrieved using a **log query** written with the Kusto query language, which allows you to quickly retrieve, consolidate, and analyze collected data.
- Use **Log Analytics** to write and test log queries in the Azure portal.
- You can start Log Analytics from **several places** in the Azure portal. The **scope** of the data available to Log Analytics is determined by **how you start it**.

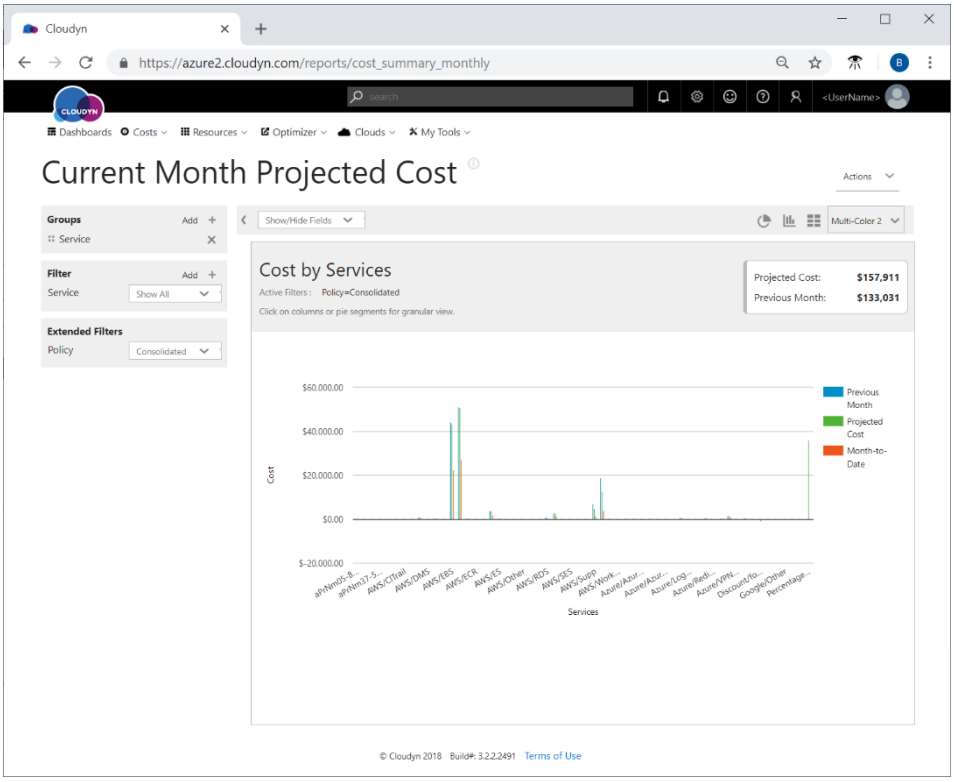
[14] https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-logs

- Azure Monitor → Logs →



1.2.7 Monitor Spend[15]

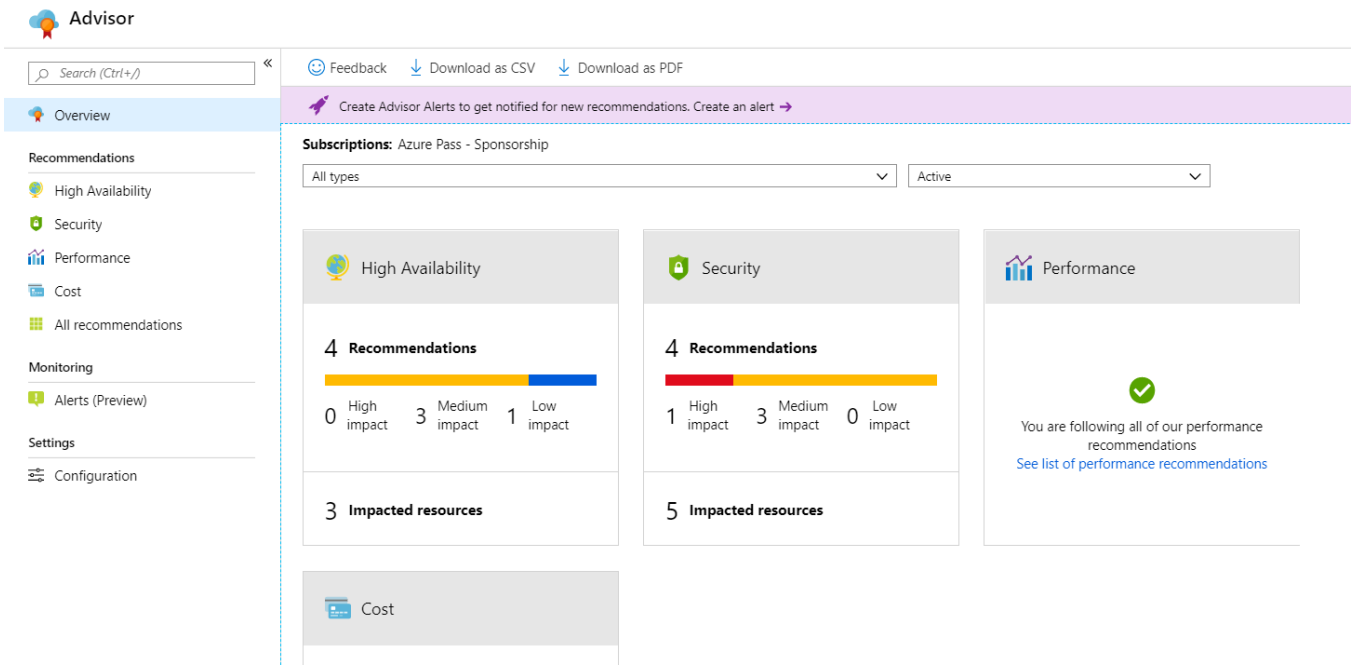
- Subscription → Overview → Spending rate and forecast.
- **Cost Management + Billing blade** shows the cost for the whole account.
- Some factures are only **available** for special type subscription: **Cost Analysis** and **Budget**.
- **Cloudyn** was bought by Microsoft.



1.2.8 Azure Advisor

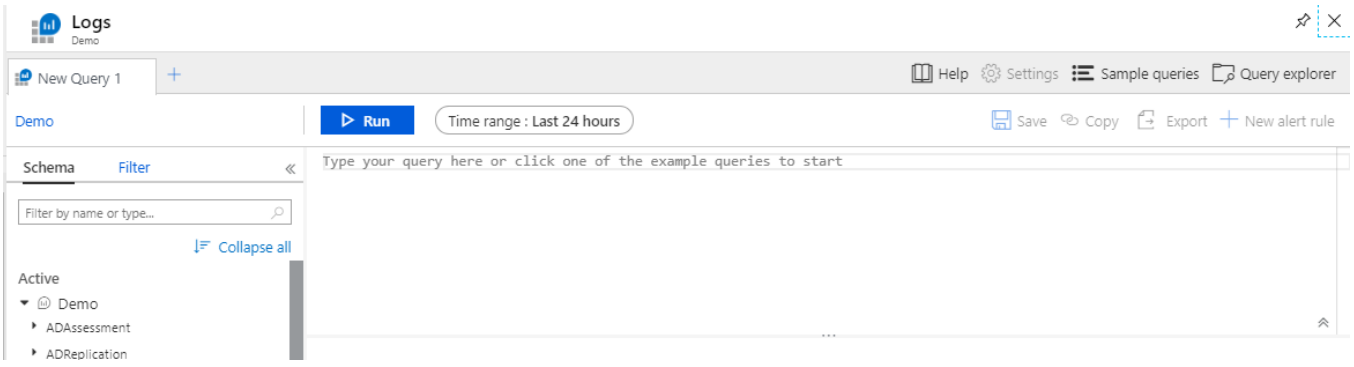
[15] https://docs.microsoft.com/en-us/azure/cost-management/cost-mgt-alerts-monitor-usage-spending

- Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments
- Its stand-alone service or integrated within different services
- The recommendations are divided into four categories as shown:



1.2.9 Utilize Log Search query functions:

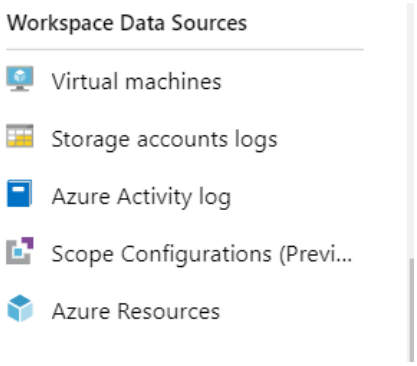
- **Log queries** help you to fully leverage the value of the data collected in **Azure Monitor Logs**.
- Define a **Log analytics workspace** (standalone resource) and then connect the resource to it. And from Monitor → Logs→ you can apply the **Query Functions**.



- Log Analytics and Application Insight are part of Azure Monitor
- Log Data collected by Azure Monitor is **stored** in Log Analytics which provide a query language for advance analytics of the Log data.
- Log Analytics is a part of the Microsoft's Operations Management Suits (**OMS**) and require OMS **workspace**.

- Log Analytics is a storage space and to collect data you need to define the data resource within the blade: An **agent** will be installed on the chosen resource that will send the log data to the Log Analytics workspace.
- The Query language is Kusto Query Language (KQL).
  https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch
  i. The KOL is case sensitive, some Data types: t: text, #: integer, Watch Symbol: date/time.
  ii. The query usually starts with Table name or search command.

1.2.10 View Alerts in Log Analytics[16]



- Log Analytics requires a container called **Workspace**.
- To add resources to the Workspace it needs to be connected.
  we have two type of connection:
  i. Metric
  ii. Diagnostics

The type of the resource will determine which type of connection is more important

- How to **convert** the Search Query using (KQL) into Alert Conditions.
- Log Analytics workspaces → Logs → (The upper right corner) Query explorer. Here you can find many written queries to be used as Alert.
- After creating the Query, you need to save it. After choosing Log Analytics as Source. Then Log Analytics workspaces → Alerts→ Add → condition (inside the signal name list)

1.2.11 Spending

- Create reports, download prior invoices, unused resources (deallocate)
- Cost Management + Billing → Invoices
- **Unused** disk can be detect using **Azure Storage Explores**.

1.3 Manage Resource Group

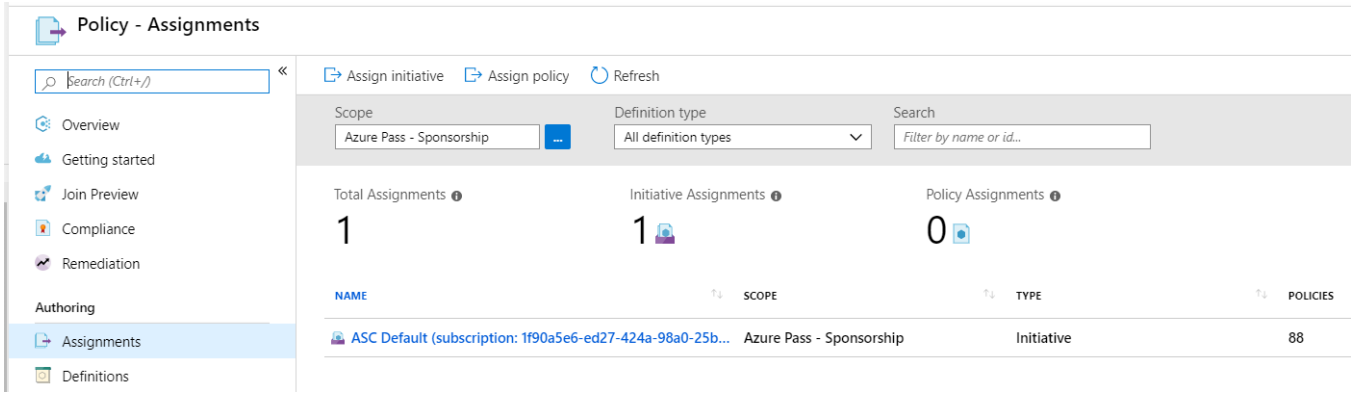
- Every resource **must** exist in one and only one resource group
- Resource groups can span regions
- **Nesting** of resource groups is **not** supported

[16] https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/alert-management-solution

- Only Subscription **Owners** can create resource groups
- The RG name have to be **unique** for the **account**, even if they exist in two different regions.

1.3.1 Use Azure policies for resource groups[17]

- Azure Policy is a service in Azure that you use to create, assign, and manage policies.
- Azure Policy's compliance evaluation is now provided **for all assignments** regardless of pricing tier.
- If your assignments do not show the compliance data, please ensure that the subscription is registered with the **Microsoft.PolicyInsights** resource provider.
- Policies can be implanted on RM, subscription and RGs level only.
- **Policies Vs RBAC**
  i. RBAC focuses on **user actions** at different scopes.
  ii. Azure Policy focuses on **resource properties** during deployment and for already existing resources.
- **Azure Policy is a default allow and explicit deny system**

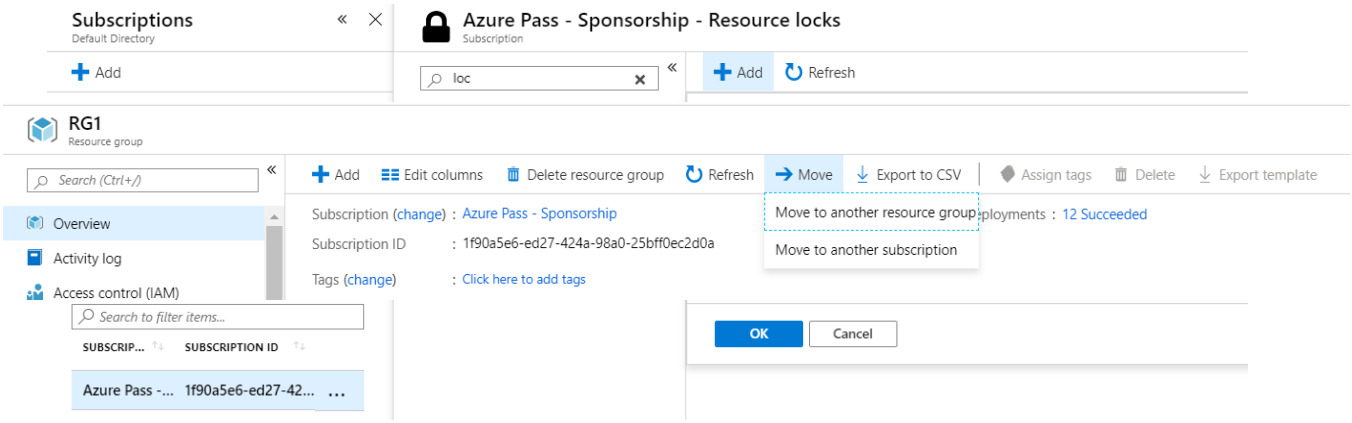


1.3.2 Configure Resource Locks[18]

- Locks are used to prevent accidental modifying or deleting resources.
- We have 2 locks level: **CanNotDelete** and **ReadOnly**
- The lock in **inherited**.

[17] https://docs.microsoft.com/en-us/azure/governance/policy/overview
[18] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

- The lock can only apply to **operations** in the **management** plane. For example, if you lock a SQL database, the data inside it can be updated or deleted.



1.3.3 Move resources Across resources groups[19]

- Azure resources can be moved to either another Azure **subscription** or another **resource group** under the **same subscription**.
- Important steps to do before moving a resource:
  i. The resources you want to move must **support** the move operation.
  ii. Some services have specific **limitations** or requirements when moving resources.
  iii. The source and destination subscriptions must be **active**.
  iv. The source and destination subscriptions must exist within the **same Azure Active Directory tenant**.
- By moving resources, both resource and the **target** resource groups are **locked** during the operation. But **neither** of them is frozen.
- You **can't** Move Azure resources between different regions useless you use **Site Recovery Vault.**
- Moving a resource can only be achieved on the **RG** level
- If you want to move a Manged disk, we should register the resource provider: **CLI**
  i. az feature register --namespace Microsoft.comput --name ManagedResourcesMove

1.3.4 Remove A resource Group[20]

- **In PS**: Remove-AzResourceGroup -Name "RGName"

[19] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-move-resources
[20] https://docs.microsoft.com/en-gb/azure/azure-resource-manager/manage-resources-portal#move-resources

- By removing an RG, you delete all the resources inside it.
- **Using PS:**
  i. **Example 1**: Remove a resource group

     Remove-AZResourceGroup -Name "ContosoRG01"

  ii. **Example 2**: Remove a resource group without confirmation

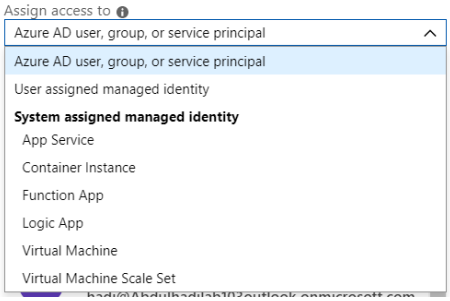
     Get-AZResourceGroup -Name "ContosoRG01" | **Remove**-AZResourceGroup -Verbose -Force

  iii. **Example 3**: Remove all resource groups

     Get-AZResourceGroup | **Remove**-AZResourceGroup

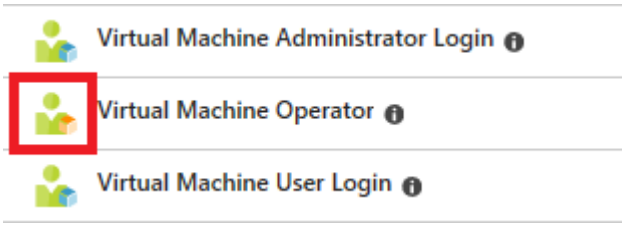
1.4 Manage Role- Based Access Control (RBAC)

- Known also as: **Identity and Access Management (IAM)**
- Provide a mechanism to **provide access** to resources.
- There are many **inbuilt** roles available.
- The role can be **assigned** to



1.4.1 Build A custom Roles[21]

- If the built-in roles for Azure resources don't meet the specific needs of your organization, you can create your own custom roles.
- Custom roles are **stored** in an Azure Active Directory (**Azure AD**) directory and can be shared across subscriptions.
- Each directory can have up to **5000** custom roles, (For **specialized clouds**, such as Azure Government, Azure Germany, and Azure China 21Vianet, the limit is **2000** custom roles.)
- Custom roles can be created using Azure **PowerShell**, **Azure CLI**, or the **REST API**.
- When you create a custom role, it appears in the Azure portal with an **orange resource icon**.

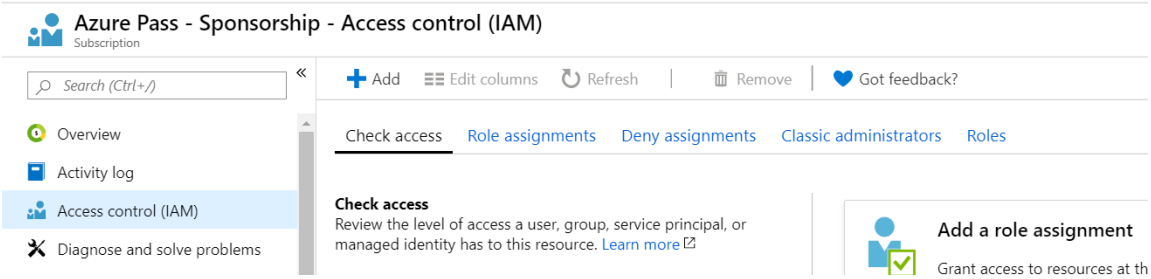


[21] https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles

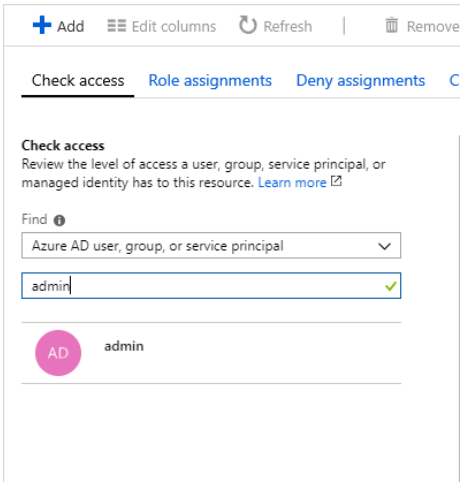
- You can **Build** a role from the **in-built roles** that are already available.
  i. Get-AzRoleDefinition
  ii. Use ConvertrTo-Json to get the Json content so that you can build your own role.
  iii. Use New-AZRoleDefinition. to create your own role
- **Example**: Cosmos DB Operator
  i. Get-AzRoleDefinition "Cosmos DB Operator" | ConvertTo-Json

1.4.2 Configure access to Azure resources by assigning roles[22]

- Role-based access control (**RBAC**) is the way that you manage access to Azure resources.
- RBAC is also known as identity and access management and appears in several locations in the Azure portal.



- View role assignments for a single user
  i. Access control (IAM) → Check access



- View all role assignments at a scope
  i. Access control (IAM) → Role assignments
  ii. On the Role assignments tab, you can see who has access at this scope.

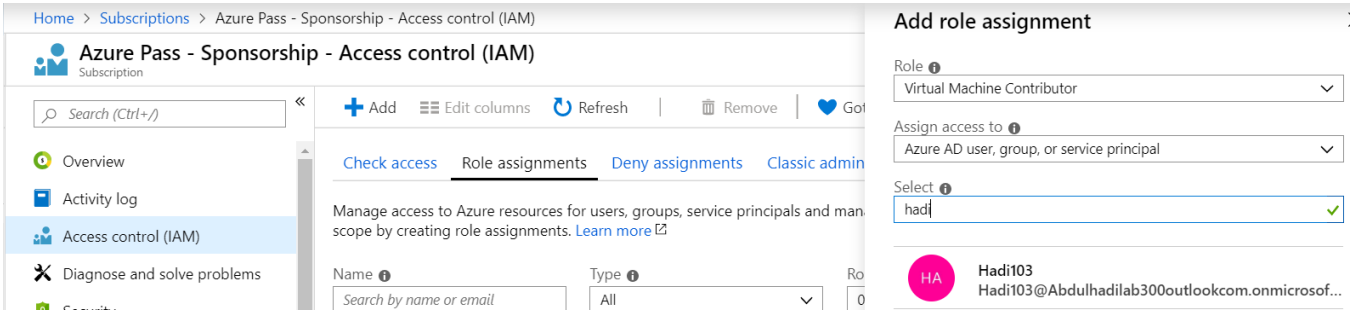
[22] https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

iii. Some roles are scoped to **This resource** while others are (**Inherited**) from another scope.

iv. Access is either assigned **specifically** to this resource or **inherited** from an assignment to the **parent scope**.

- **Add a role assignment**

i. Access control (IAM) → Role assignments → +Add



1.4.3 Assign a user as an administrator of a subscription

ii. Subscription → Access control (IAM) → Role assignments → +Add

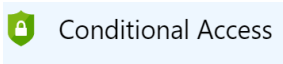
iii. In the **Role** drop-down list, select the **Owner** role.

iv. In the Select list, select a user.

1.4.4 Configure management access to Azure[23]

- **Conditional Access**

i. Premium **P1** and **P2** feature

ii. Can be access within the AD blade or as a standalone service. 

iii. Conditional Access is basically a policy that you can set that will turn on security feature (like: MFA) only under specific circumstances.

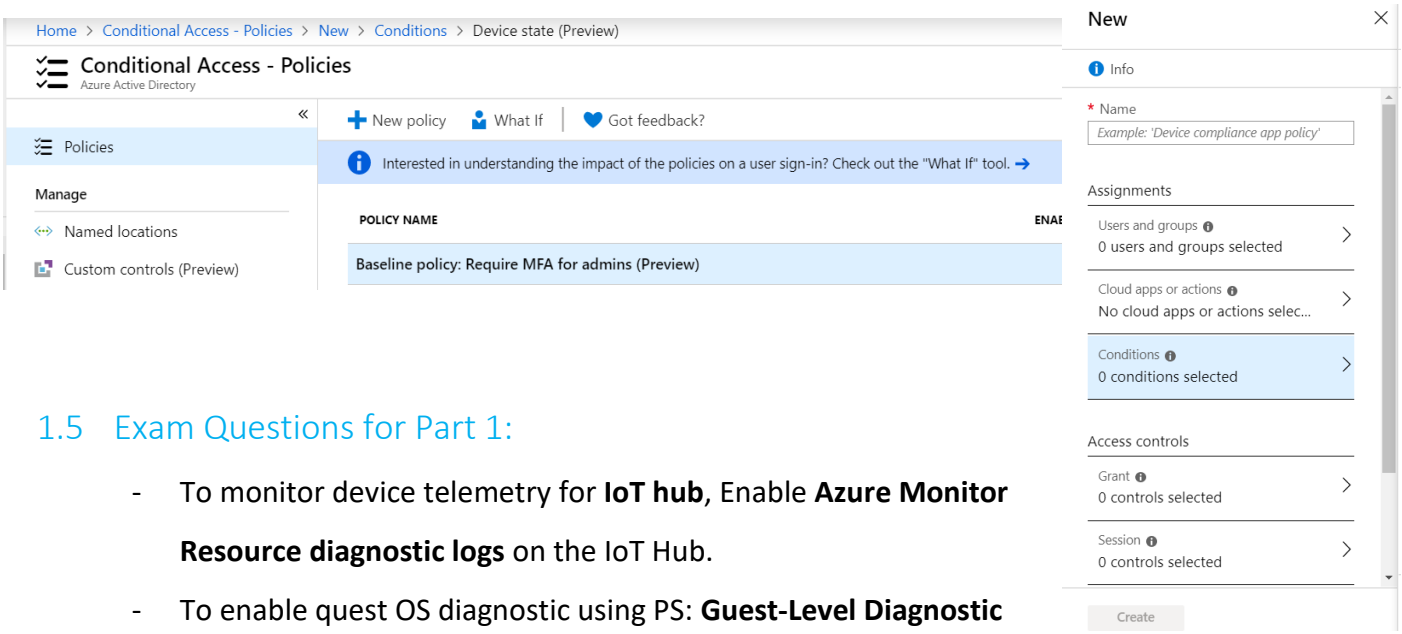
iv. Conditional Access in Azure Active Directory (Azure AD) controls **access** to cloud apps based on specific **conditions** that you specify.

v. **To allow access**, you create Conditional Access policies that allow or block access based on whether or not the requirements in the policy are met.

vi. Conditional Access policies at their simplest are **if-then statements**, if a user wants to access a resource, then they must complete an action

[23] https://docs.microsoft.com/en-us/azure/role-based-access-control/conditional-access-azure-management

vii. Resources → Conditional Access → + New Policy



1.5 Exam Questions for Part 1:

- To monitor device telemetry for **IoT hub**, Enable **Azure Monitor Resource diagnostic logs** on the IoT Hub.
- To enable quest OS diagnostic using PS: **Guest-Level Diagnostic** Set-AzVMDiagnosticsExtension -ResourceGroupName $RGName -VMName $VmName -DiagnosticsConfigurationPath $Path

2 Implement and manage storage (15-20%)

2.1 Create and configure storage accounts[24]

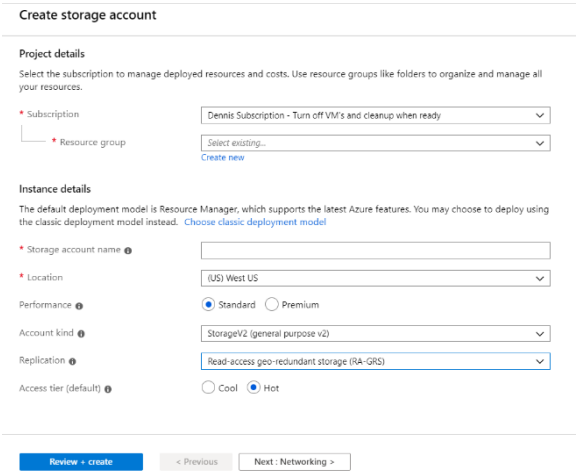
- An Azure storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks.
- The storage account data is accessible through **HTTP or HTTPS**.
- Data in your Azure storage account is **durable** and **highly available**, **secure**, and **massively scalable**.

- New-AzStorageAccount -ResourceGroupName $RGname -name $SAname -SkuName Standard_ZRS -Location 'West Europe' -Kind Storage

- az storage account create --location 'West Europe' --name 'SAname' --resource-group 'RGname' --sku 'Standard_ZRS'

[24] https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

- Azure portal → Storage Account → +Add
- The name should **be globally unique**.
- Azure provide 4 data services: Blobs, Files, Queues, Tables
- **Blobs**: It's the Microsoft's object storage solution for the massive unstructured data
- **Files**: Enable to setup File Network Share that can be access using Server Message Block (**SMB**) Protocol
    i. **Multiple** VMs can **share** the same file



- **Queues**: use to store and retrieve messages, each message can be up to 64 Kb. (FIFO)
- **Table**: Its now part of Azure Cosmo DB and stored NoSQL data in cloud.
- **Performance types**:
    i. **Standard** storage accounts are backed by magnetic drives (**HDD**) and provide the lowest cost per GB.
- **Premium** storage accounts are backed by solid state drives (**SSD**) and offer consistent low-latency performance.
- **Account Type**: Blob storage, Storage(V1), Storage (V2)

Type	Services	Performance Tiers	Access Tiers	Replication options
General Purpose v1	Blob, File, Queue, Table, and Page Blobs	Standard, Premium	N/A	LRS, GRS, RA-GRS
General Purpose v2	Blob, File, Queue, Table, and Page Blobs	Standard, Premium	Hot, Cool, Archive	LRS, ZRS, GRS, RA-GRS
Blob	Blob only	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS
Premium Blob	Blob only	Premium	N/A	LRS

- Microsoft recommends using a **general-purpose v2** storage account for most scenarios.
- You can easily upgrade a general-purpose v1 or Blob storage account to a general-purpose v2 account with no downtime and without the need to copy data.
- **Access Tier**: Hot, Cold:
    i. Changing the access tier for an existing storage account or blob may **result in additional charges.**

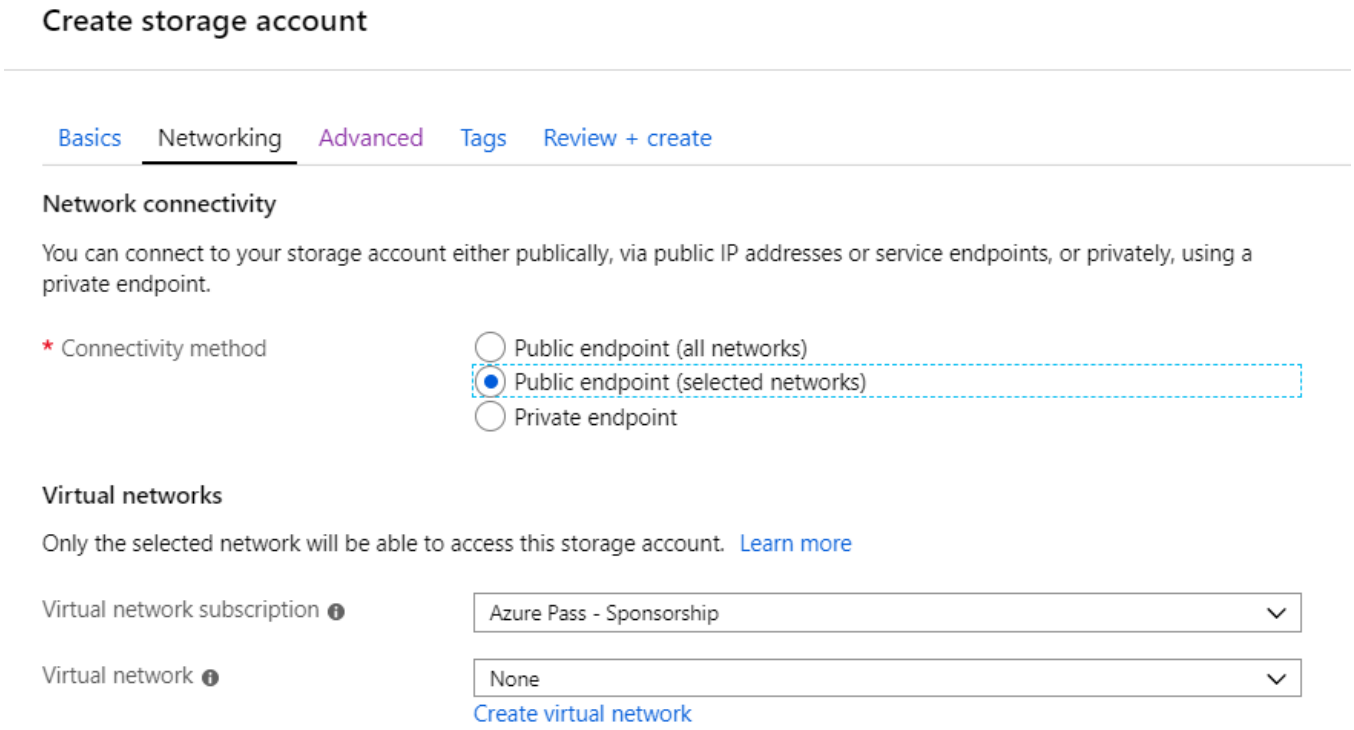
- The data in your Microsoft Azure storage account is **always replicated** to ensure **durability** and **high availability**. When you create a storage account, you have four replication options:
  i. **LRS:** Locally (3 copies, 1 Data centre, 1 region)
  ii. **ZRS:** Zone (3 copies, 2-3 Data centres, 1 region)
  iii. **GRS:** Geo (6 (3*2) copies, 3 in primary region and 3 in secondary region)
  iv. **RA-GRS:** Read-Access (we can read from the secondary region)

- Azure Storage Offerings:

Queues	Tables	Blobs	Disks	Files
Reliable messaging at scale for cloud services	Massive auto scaling NoSQL data store	Highly scalable, REST based cloud object store	Persistent disks for Azure IaaS VMs	File share like access to Azure storage"

2.1.1 Configure network access to the storage account[25]

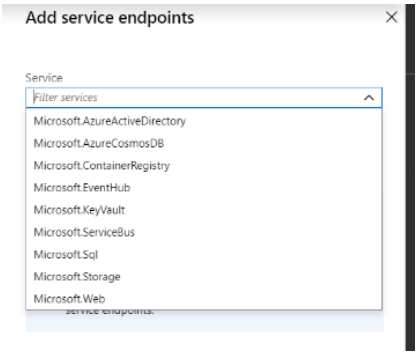
Create a Storage account → Networking



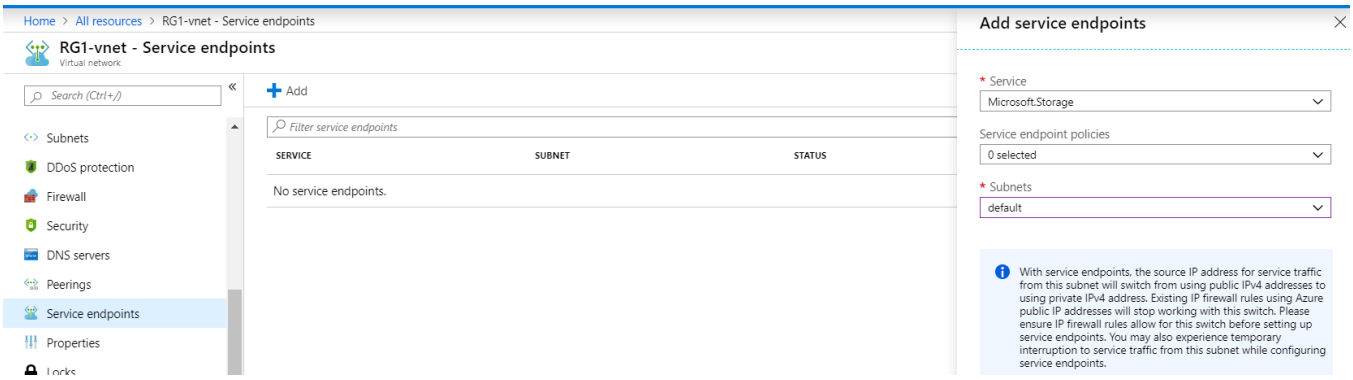
- Here we can define who have the permission to access our storage account.

[25] https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

- After chosen the **allowed** VNETs, By Default, all resources in the **same VNET can communicate with each other**, the public internet and the on-prims. But they can't communicate with the Azure outside services, such as Azure Storage Account. So, to allow VNet to communicate with storage account, we need to create a **service endpoint** in our VNet.



- VNet → Service Endpoints → +Add → Service [Microsoft.Storage] → Add



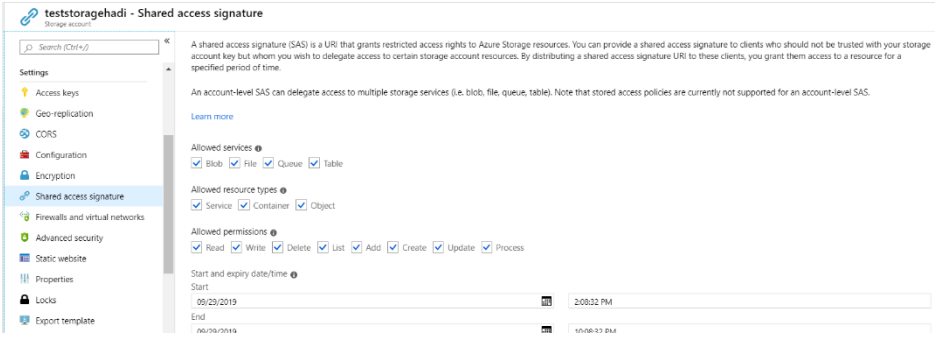
- The VMs inside the VNet will **still have access** to the Storage account even if we did not configure the Service Endpoint, but this will be similar to access through public internet.
- **The Storage Account should be on the same region as the VNet**

2.1.2 Generate Shared Access Signature (SAS)[26]

- A shared access signature provides **delegated** access to resources in your storage account.
- With a SAS, you can grant clients access to resources in your storage account, without sharing your account keys.
- Storage Account → Access Keys

[26] https://docs.microsoft.com/en-gb/azure/storage/common/storage-sas-overview

- Account storage keys are similar to the root passwords for your storage account. So, you should never share is with others. The solution is **shared access signature (SAS)**.
- An **account-level SAS** can delegate access to **multiple storage services** (i.e. blob, file, queue, table).
- Note that **stored access policies** are currently not **supported** for an account-level SAS.
- Whit SAS we can grant restricted access to our storage account.



2.1.3 Install and use Azure Storage Explorer

- https://azure.microsoft.com/en-us/features/storage-explorer/

2.1.4 Manage access keys

- We have two keys is the Access keys, so when you regenerate one of the keys, you can make the connection using the other keys. Key 1 is Primary, Key 2 is Secondary.

2.1.5 Monitor activity log by using Log Analytics

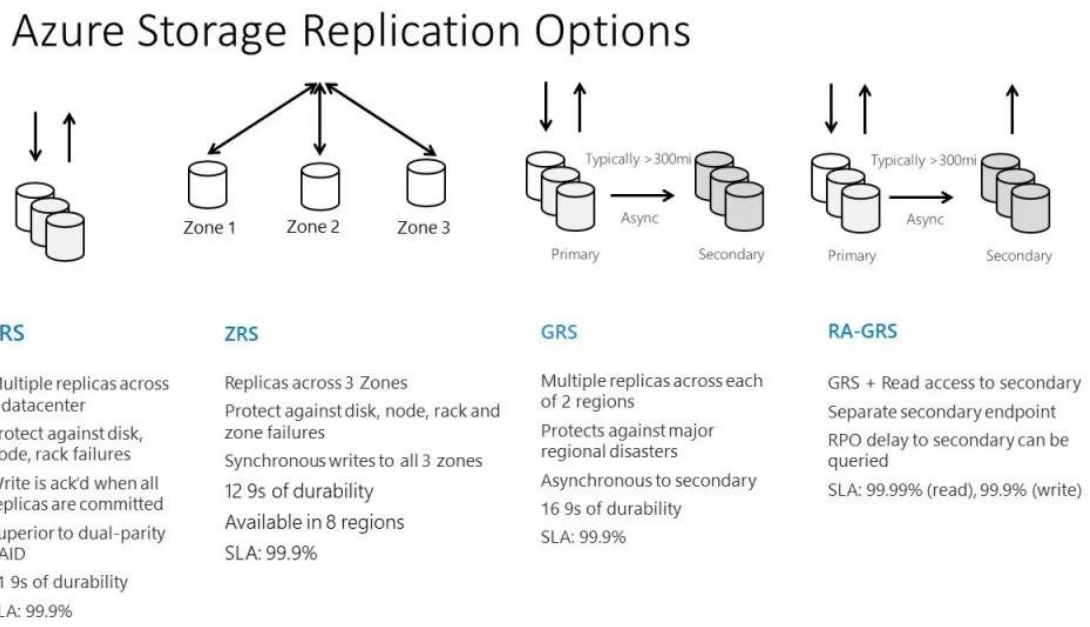
- Metrics and Activity logs are gathered inside azure from resources/services. And then they can be analyse using **Log Analytics**.
- The diagnostic data from application/web app is collected inside the **Application Insight service**.
- Azure Monitor → Activity log

- We can create alerts from the activity logs:

  Alert→ New Alert Rule → Condition (we can here choose the Activity log signal type)

SIGNAL NAME	SIGNAL TYPE	MONITOR SERVICE
All Administrative operations	Activity Log	Administrative
Create or Update server (84codes.CloudAMQP/servers)	Activity Log	Administrative
Delete server (84codes.CloudAMQP/servers)	Activity Log	Administrative
List Secrets (84codes.CloudAMQP/servers)	Activity Log	Administrative
Regenerate Keys (84codes.CloudAMQP/servers)	Activity Log	Administrative

2.1.6 Implement Azure storage replication[27]



- We have 4 different replication options:

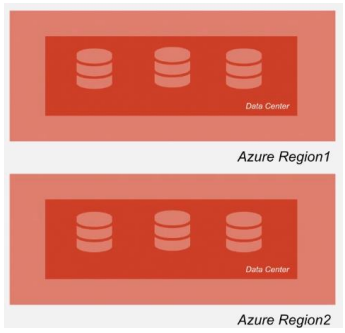
  i. Locally redundant storage (**LRS**) (3 copies/ 1 data Center/ 1 region)

[27] https://www.jamesserra.com/archive/2019/02/azure-data-lake-store-gen2-is-ga/azure-storage-replication-options/

ii. Zone Redundant Storage (**ZRS**) (3 copies/ (2-3)Datacenters/ 1 region)

iii. Geo-Redundant Storage (**GRS**) (6 copies/ 2 data centers/ 2 region 'Primary and secondary')

In GRS, the secondary region is only availbale to be read only if Microsoft initiate a fail over from the primary region to the secondary region.



iv. Read Access Geo-Redundant Storage (**RA-GRS**)

In RA-GRS, you can read the data from the secondary region regardless even if Microsoft did not initiate a fail over from the primary region to the secondary region.

- Suppose Primary storage is: Test.**blob.core.windows.net**

Then the Secondary storage will be: Test-secondary.**blob.core.windows.net**

And the **Access keys** will be the **same** for both storages.

2.2 Import and export data to Azure

- Azure Import/Export data are used to securely import/export **large amount** of data to Azure blob and Azure files by using **Disk drives**.
- We can use our **own disk drives** or the ones **provided** from Microsoft.
- Import/Export components:
  i. Import/Export service: Azure portal
  ii. **WAImportExport** tool: installed on-premises side, Command line tools that encrypt data with BitLocker, copying data to the drive, generate journal files…

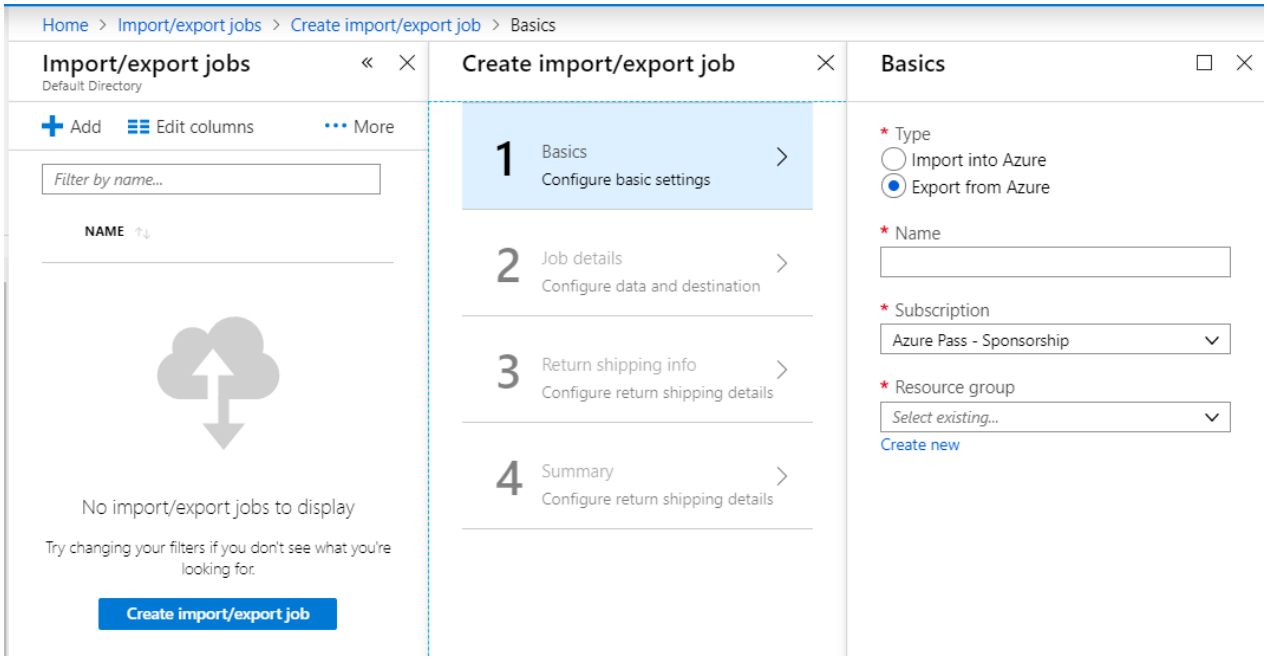
iii. Disk drive itself.

2.2.1 Create export from Azure job[28]

- **Export from Azure**:
  i. Securely export large amounts of data from Azure Blob storage.
  ii. The service requires you to ship empty drives to the Azure datacentre.
  iii. The service exports data from your storage account to the drives and then ships the drives back.
- **Import to Azure**: Send my data inside a disk to Azure.
- We need a **Journal file** so we need to download the **WAImportExport** tool **on-premises** which will generate the Journal file.
- If the blob to be exported is in **use during data copy**, Azure Import/Export service takes a **snapshot** of the blob and copies the snapshot.
- Export from
- **4** steps to export from Azure:
  i. **Step 1**: Create an export job
  Import/export jobs→ create new job → 1 basics -Type: Export from Azure
  ii. **Step 2**: Ship the empty drives
  iii. **Step 3**: Update the job with tracking information
    1. After shipping the disks, return to the Import/Export page on the Azure portal.
    2. If the tracking number is **not** updated within **2 weeks** of creating the job, the job **expires**.
  iv. Step 4: Receive the disks

[28] https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs

1. When the dashboard reports the job is complete, the disks are shipped to you and the tracking number for the shipment is available on the portal.



2.2.2 Use Azure Data Box[29]

- The Azure Data Box family offers products of **differing storage capacities** to help send terabytes (TB) of data to Azure in a **quick**, **inexpensive**, and **reliable** way.
- To transfer large amount of data from/to Azure.
- **Offline data transfer**: For limited to no network bandwidth
  i. Azure Data Box Disk: < 40 TB
  ii. Azure Data Box: 40 – 500 TB
  iii. Azure Data Box Heavy: > 500 TB
- **Online data transfer:** Over the network transfer
  i. **Azure Data Box Gateway[30]: Install**
     1. It is a storage solution that enables you to seamlessly send data to Azure.
     2. The i.Azure Data Box Gateway resides in your **premises** and you write data to it using the **NFS** and **SMB** protocols.

[29] https://docs.microsoft.com/en-us/azure/databox-family/
[30] https://docs.microsoft.com/en-us/azure/databox-online/data-box-gateway-overview

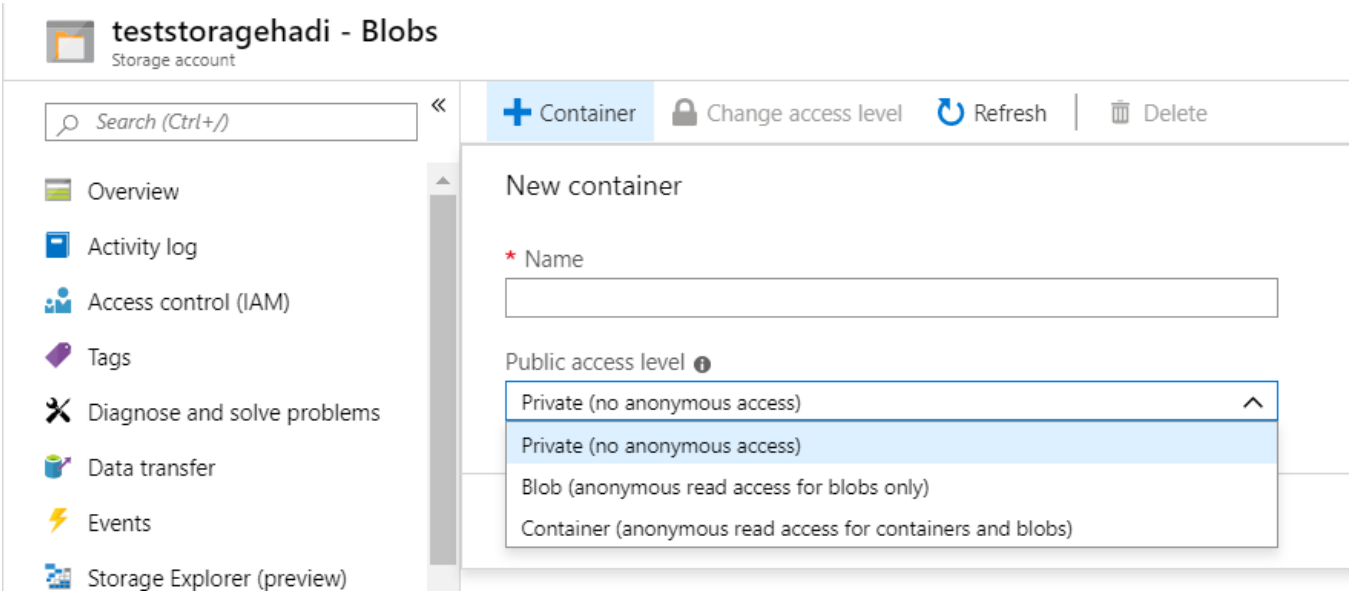
3. The device then transfers your data to Azure **block blob, page blob**, or **Azure Files**.

ii. **Azure Data Box Edge**:

1. This is a **Hardware-as-a-service solution** device provided by Microsoft **installed on-promises** environment.
2. **NFS** and **SMB** protocols are used to write to the device.

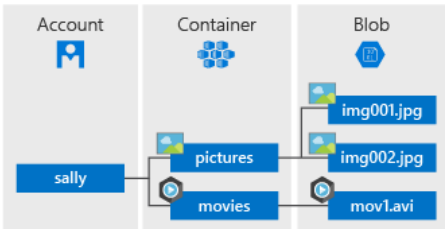
2.2.3 Blob Storage[31]

- Azure Blob storage is a **service** that stores **unstructured** data in the cloud as **objects/blobs**.
- Blob storage can store any type of text or **binary** data, such as a document, media file, or application installer. Blob storage is also referred to as object storage.
- Highly scalable, **REST** based cloud object store.
- Data sharing, Big Data, Backups
- Unstructured storage of binary and text data
- Storage Account → Blobs → +Containers (folder for the Blob) → Access level (Private, Blob, and Container)

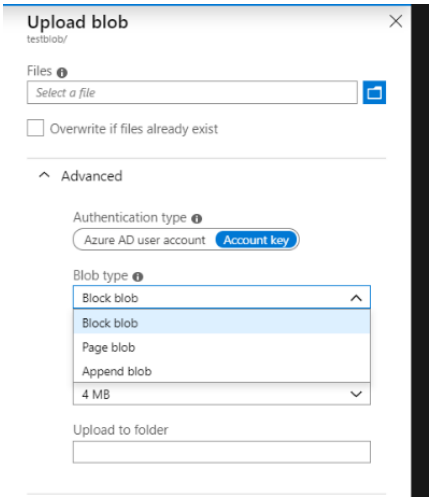


[31] https://docs.microsoft.com/en-us/azure/storage/blobs/

- **Container**: A container provides a grouping of a set of blobs. All blobs must be in a container.
- An **account** can contain an **unlimited** number of containers. A **container** can store an **unlimited** number of **blobs**. Note that the container name must be lowercase.



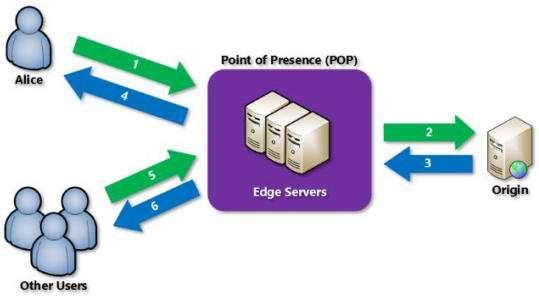
- Inside the containers we can **upload** blobs.
- Blob Types are:
  i. **Block Blob:** Read and write data in blocks. Optimized for **sequential IO**. Most **cost-effective** Storage. Ideal for files, documents & media, the Maximum size is: **4.7 TB**. The blocks can be managed individually and have different sizes.
  ii. **Page Blob:** Random access **files**, **8 TB**. It stores the **VHD** (Virtual Hard Disk) files that **backup** the VMS. The **disks** attached to the VMs are page blob. Optimized for random access and can be up to **8 TB** in size. **IaaS** VM OS & data disks are of this type.
  iii. **Append Blob:** similar to Block blobs but for append operations (like, logging data from VM)



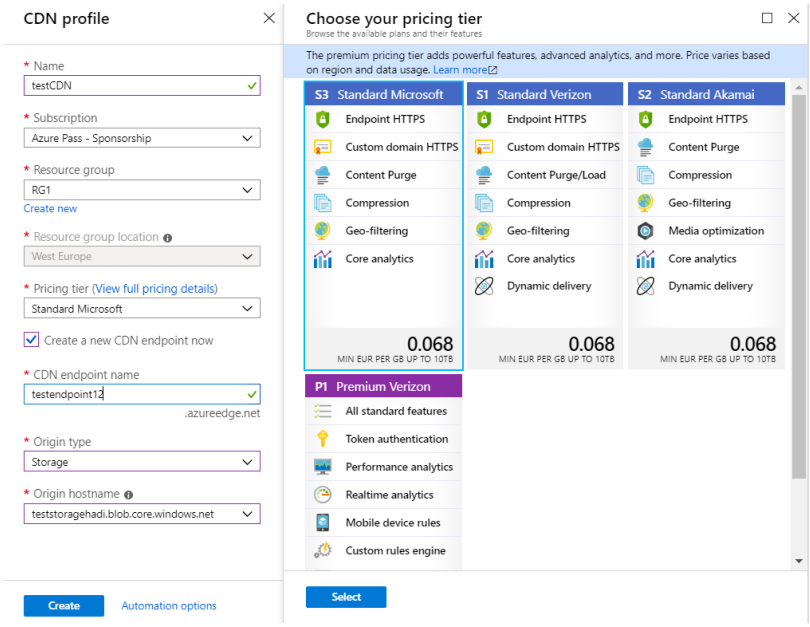
- Container **nesting** is not available. But we can upload a file to a specific **folder** inside the container.
- There are two Azure PowerShell cmdlets of interest, both provide a very efficient way for moving these large files.
  i. Add-AzVHD - Uploads a virtual hard disk from an on-premises virtual machine to a blob in a cloud storage account in Azure.
  ii. Save-AzVHD - Saves downloaded .VHD images locally. From on-prem to Azure.
- Inside the blob → **Snapshots** will take a snapshot of the blob (read only version)
- http://bit.ly/2lS6vta

2.2.4 Configure Azure content delivery network (CDN) endpoints[32]

- CDN is a distributed network of **Edge** servers that deliver contents to the end users. Is mostly for delivering **static** files to the user.
- CDNs store **cached** content on edge servers in point-of-presence (**POP**) locations that are close to end users, to **minimize latency**.
- You **can't** choose the CDN region because CDN is a global resource.



- Purge is used to update the files in the endpoint
- Azure has given the domain name [filename**. azureedge.net**] to all CDN endpoints.
- The **DNS** is responsible for **routing** the request to the best performance edge server which usually is the closest geographical one.
- The cashed file inside the edge servers will stay until the **TTL** end, the default TTL is **7 days**.
- Azure (all services) → CDN profiles →

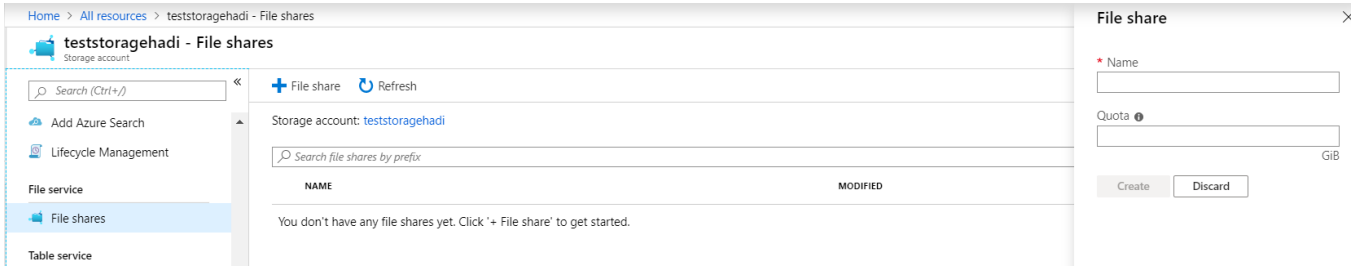


[32] https://docs.microsoft.com/en-us/azure/cdn/cdn-overview

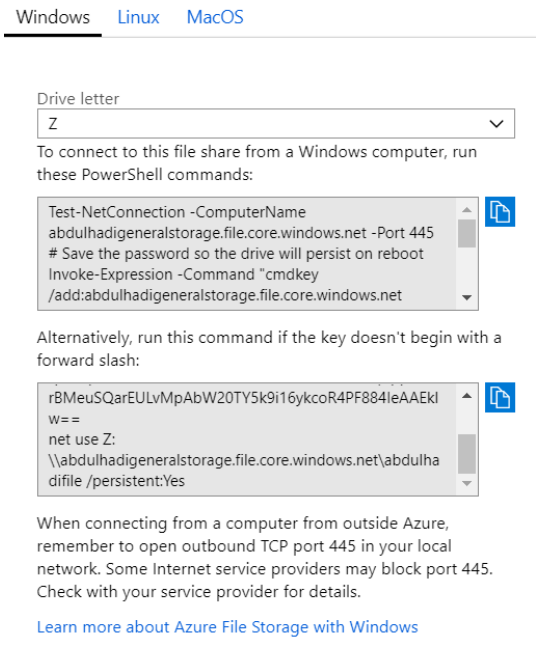
2.3 Configure Azure file[33]:

2.3.1 Create Azure file share[34]:

- Simply, this means creating a drive on you on-premises PC connected immediately to the Azure cloud.
- Azure File shares support the industry standard **SMB protocol**, meaning you can **seamlessly replace** your on-premises file shares with Azure File shares without worrying about application compatibility.
- Being able to share a file system across **multiple machines**, applications/instances is a significant advantage with Azure Files for applications that need **shareability**.
- Blob storage **can't** be amount to a computer/VMs, but Files storage can.
- Storage Account → files → +File Share New-AzureStorageShare

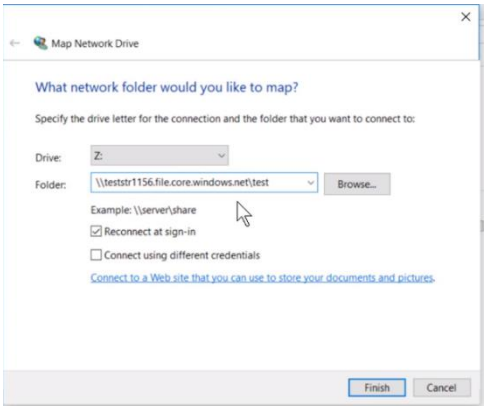


- The maximum Quota is **5** TB.
- To use Azure file share **outside** the Azure region (**On-prem**), we need to have OS that support **SMB** protocol and the **port 445** is open because **SMB** use it for connections.
- Many ISP **block** port 445 (TCP port 445, Server Message Block SMB Protocol) for security purposes, this port is used by Microsoft for file share, so it's difficult to connect our file and give it a drive letter on our local PC.
- To use the created file in Azure in the VMs, we need to mounted it to a drive letter inside the VMs. This is being done through the connect bottom in the File blade.



[33] https://www.youtube.com/watch?v=hm576LVcQn4
[34] https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share

- From within the **VMs/ PC → Map network drive**



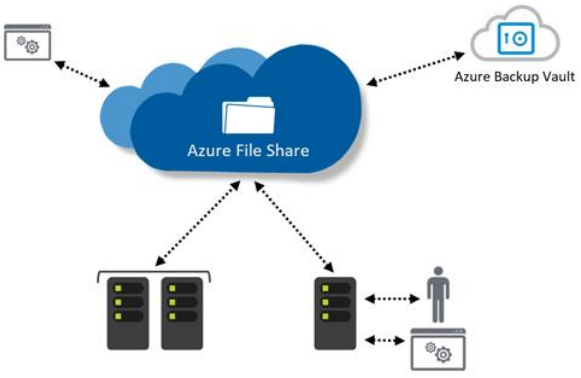
All details are being driven from the Connect blade: Folder Path, User name and Password. In our Example: from the **net use** command:

```
cmdkey
/add:abdulhadigeneralstorage.file.core.windows.net
/user:Azure\abdulhadigeneralstorage
/pass:pY4CwfnnJmoukKScSEkoXBWshMCBMK7qVpp2F4ZrBMeuSQarEULvMpAbW20TY5k9i16y
kcoR4PF884IeAAEklw==
net use Z: \\abdulhadigeneralstorage.file.core.windows.net\abdulhadifile /persistent:Yes
```

- The previous steps will result in a disk drive letter Z allocated in the VM/PC, and any file that will be copied/created in it will automatically be seen in the Azure File inside Azure.
- We can create **Directories** inside the File share storage.
- You would like to use PowerShell to upload a local file to a file share directory. Which cmdlet can you use?
    i. Set-AzureStorageFileContent

2.3.2 Azure file sync[35]:

- Azure File Sync in combination with Azure file shares allows you to **centralize** your organization's file shares in Azure, while keeping the **flexibility**, **performance**, and **compatibility** of an **on-premises file server**.

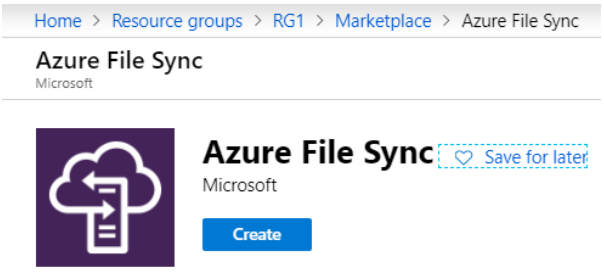


- Azure file Sync required two resources: **Storage Account** and Azure **file Sync resource**.

[35] https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-planning

- We use **Azure file sync agent** which work on Windows server OS.
- **Azure File Sync** can be found in the Markplats, All resources.

- https://www.youtube.com/watch?v=Zm2w8-TRn-o
- https://www.youtube.com/watch?v=n3R9GqOrBOY&t=76s
- The location of the Azure file sync **should** be the same as the **storage account**.
- +**Sync Group**: we defined the file to be synchronised inside it.
- **Cloud endpoint** for the Sync group is the **Azure file share**.



- **Server endpoint** is the **on-promises windows server**.
- We can't add **cloud points** to our Sync group but we can **Add multiple server endpoints**
- You can **only** add the **registered servers** as endpoint servers
- To register an endpoint server, we need to download the **Azure file Sync agent** at the server.

2- Azure File Sync troubleshooting[36]

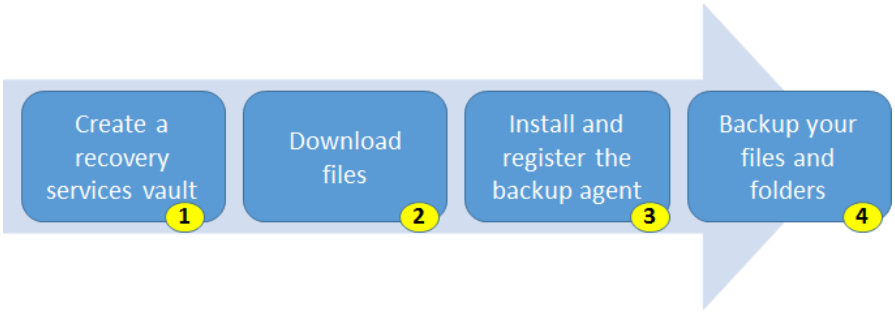
- **Azure file share** can only be used by one **cloud endpoint**. To solve this problem, delete the metadata for the Cloud endpoint file share.
- To create Cloud end point, you should be the **Owner** or **User Access Administrator**.
- Azure File Sync requires AzureRm **5** and above to be installed on the servers.
- Should I remove my endpoint when I had problems? **NOOOO**.
- **Unable** to delete a server from the Server Endpoint, go to **Registered servers'** blade and choose **unregistered server** and then try to delete the server again.

2.4 Implement Azure Backup[37]

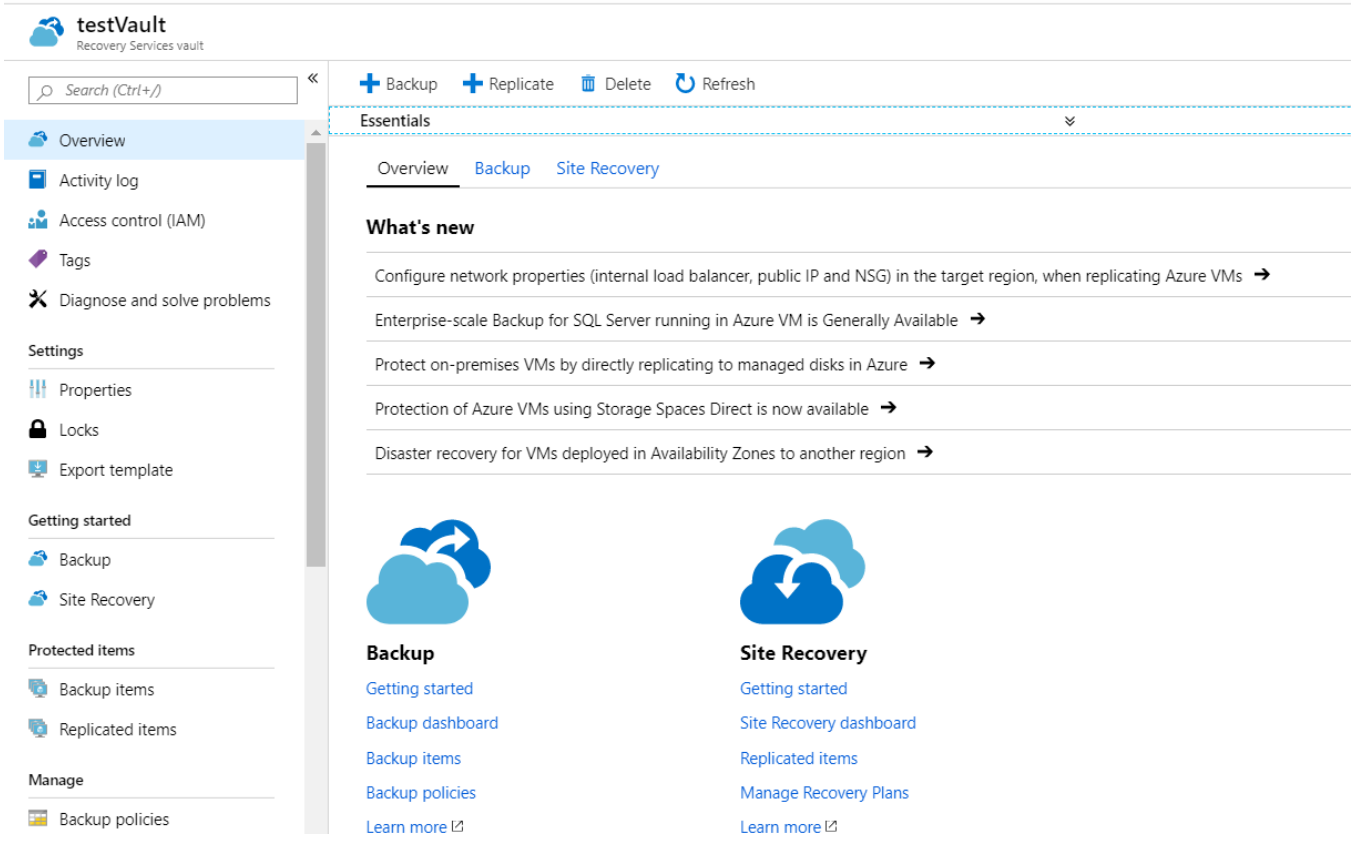
- Azure backup solution is a straightforward process:
  - the first step is the creation of a **recovery services vault**.
  - With the vault created it can then be prepared **to host backups**.
  - Once the vault is deployed and prepared, backup policies can be created and deployed
  - with policies deployed backups can begin.

[36] https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-troubleshoot?tabs=portal1%2Cazure-portal
[37] https://www.youtube.com/watch?v=i7CKoZeMAR4

- **Recovery service vault** is the storage entity for the backup resources such as: VMs and SQL data basis.



- **Azure backup uses cached files**. You should allow at least 10% of the production server disk for caching. Azure will **encrypt** and **decrypt** your files using a **passphrase** that you supply. If you lose the passphrase your backup cannot be **recovered**.



2.4.1 Configure and review backup reports[38]:

- Backup operation is presented in Azure as **Recovery Service Vault**.

[38] https://docs.microsoft.com/en-us/azure/backup/backup-azure-configure-reports

- **Recovery Service Vault** require a **storage account** which can be connected to **PowerBI** for analysing and generating **reports**. Both the **Service Vault** and the **storage account** should be in the **same region**.
- By **default**, the recovery service vault has the **Geo-redundant storage (GRS),** you can change the replication type but **only** before configuring any backup to the backup recovery service vault.
- The recovery service vault and the virtual machine / resources **should** be in the same **region**.
- Backup Reports data will be fully available in the storage account after **24** hours from configuration.
- Backup reports are **supported** only for **VM** and **file** and folder backup.
- The resource provider for reports is **Microsoft.insights**
- All service → **Recovery Service Vault** → +Add
- From the Vault → Backup reports → Link to Diagnostics Setting

2.4.2 Perform Backup operation[39]

- Azure Backup is used to backup and restore data in Azure.
- Azure Backup can be implemented by downloading multiple components for on-prom and the cloud. Such as: **MARS, System Center DPM, Azure Backup server and Azure IaaS VM Backup.**
- Backup Types:
  i. Full Backup
  ii. Differential Backup
  iii. Incremental Backup
- Azure backup in default perform an **incremental** backup as a backup type.
- **Recovery service Vault** stores all the Backup data and **recovery points** (there are a limited number of recovery vault allowed for each recovery vault)
- **Site Recovery** is for disaster recovery**, Backup** is for governance purposes or restore a specific area.
- Azure Backup **Vs** Azure site recovery

[39] https://docs.microsoft.com/en-us/azure/backup/quick-backup-vm-portal

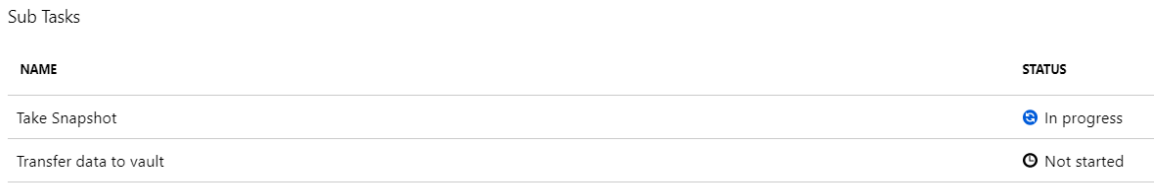
i. **site recovery**: To replicate the configuration of a VM across data centre (keep the workloads running in case of outage)

ii. **Azure Backup**: If a file on a system gets corrupted (keep the data safe and recoverable).

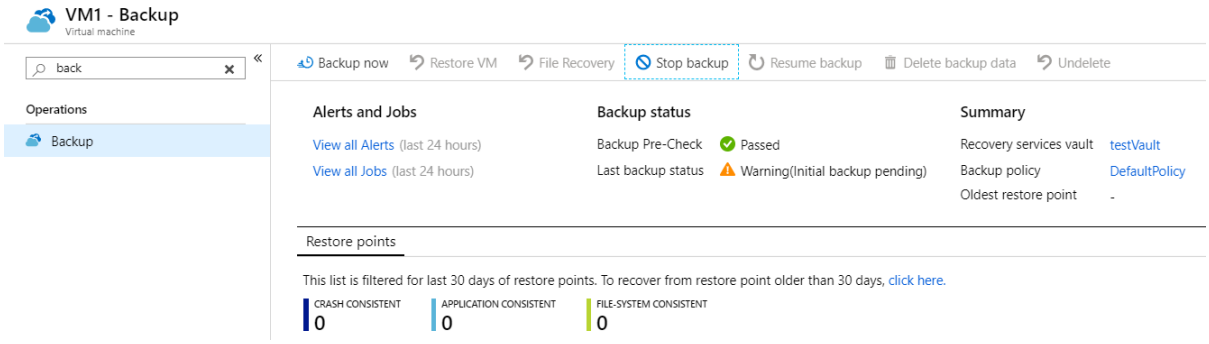
- **Backup a VM**:

i. VM → Backup → … Enable Backup

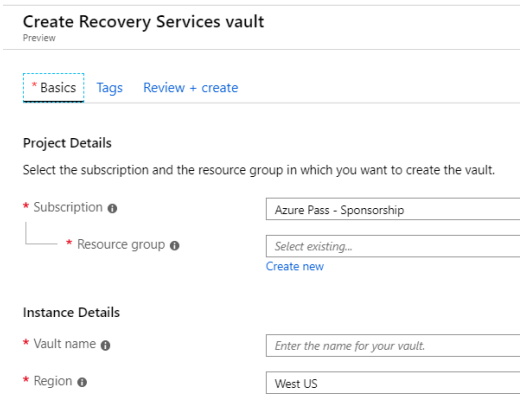
VM backup consists of two steps:



ii. After Enable Backup:



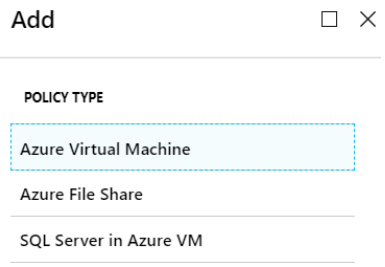
2.4.3 Create Recovery service vault



- Home → Recovery Services vaults →
- You **cannot** delete a Recovery Services vault that has dependencies such as protected servers or backup management servers associated with the vault.
- We can use all the different components such as: **MARS**, System Center DPM, Azure Backup server and Azure IaaS VM Backup.

- Recovery Service Vault contains **RBAC**

2.4.4 Backup policy



- You can configure the policy in either **VM** (will be apply only on the current virtual machine) or in the **Azure recovery service vault** (the policy then will be applied to all virtual machines or file shares or SQL server).

2.4.5 Perform a restore operation:

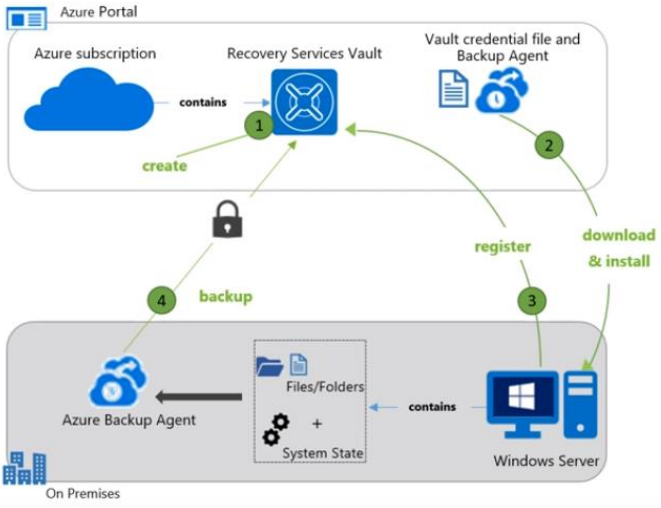
- When backup a resource, a recovery point will be created. From which we can restore our resource.
- **Recovery Vault**→ Backup Items→ VMs→ Restore VM → Create new/Replace existing

2.4.6 On-premises Backup:

- We need to install **recovery service agent** on our on-premises environment.
- To back up the **Bare Metal Recovery** (everything below the OS upwards) then we need to download the **Backup server**

2.4.7 The Microsoft Azure Restore Service (MARS) agent

- https://www.youtube.com/watch?v=3wHXJVsbEvU
- MARS agent can Backup files and system state directly to Azure without the need for any local storage.
- Backing Windows Server is a 4-step process:
-



2.4.8 AzCopy Command Line Interface

- AzCopy is a Windows command-line utility designed for **copying** data **to and from** Microsoft Azure **Blob, File, and Table storage** using simple commands with optimal performance. You can copy data from one object to another **within** your storage account, or **between** storage accounts.
- AzCopy uses case-sensitive matching when the /Source is a blob container or blob virtual directory, and uses case-insensitive matching in all the other cases.
- The basic syntax for AzCopy commands:

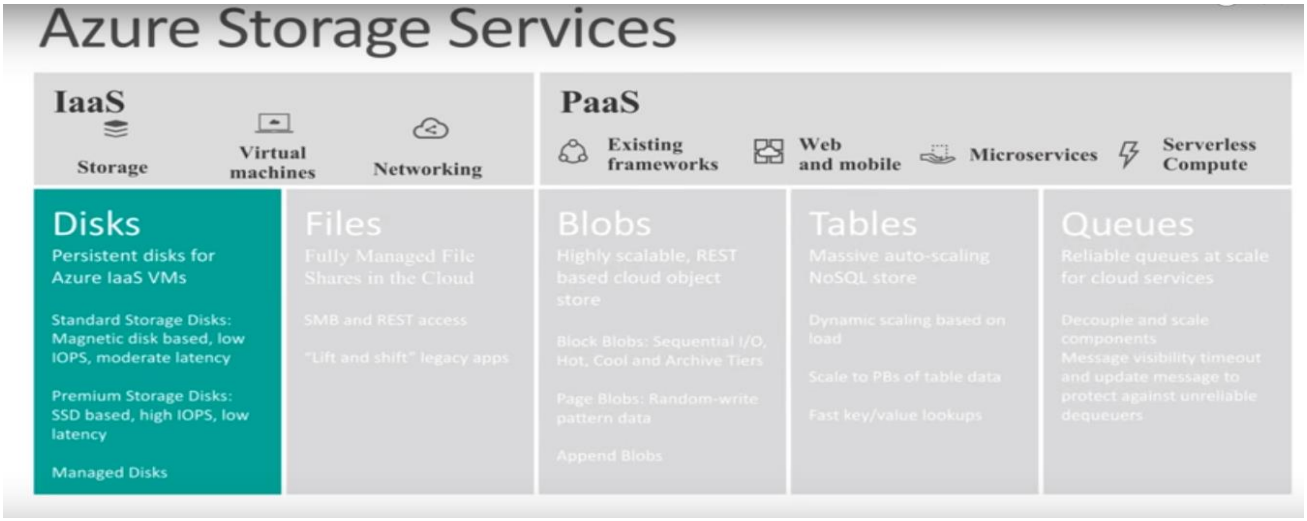
  AzCopy /source:C:\Azcopy_data /dest:

  https://canitproblob.blob.core.windows.net/canitprocontainer /destkey:"container access key" /s.

  Let's break down the command:

  i. Azcopy = the action
  ii. /Source = the local folder
  iii. /Dest = the blob container
  iv. /Destkey = the blob access key
  v. /s = copies the directory structure

2.5 Virtual Machine Storage:



- **Disks** are how virtual machines store their **VHD** files. Whether it's Premium (SSD), Standard (HHD), Managed or Unmanaged.
- Disks used by VM's:

i. Operating system disk (Automatic)
   - 2 GB disk mounted as C.

ii. Temporary Disk (Automatic)
   - Temporary disk for page file

iii. Data Disk (User Defined)
   - VHD used to store application data
   - Max 4 GB in size
   - Number of disks determined by size of VM

-

Unmanaged vs. managed disks

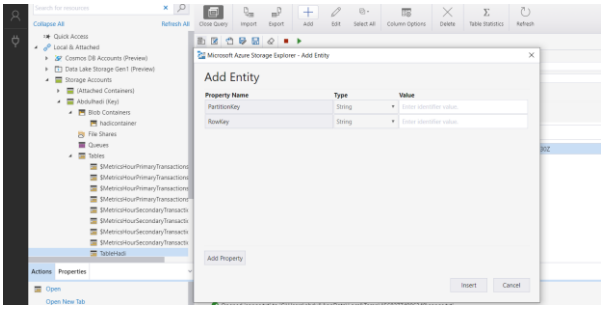
	Unmanaged disks	Managed disks
RBAC	Storage account level	Disk level
Tags	Storage account level	Disk level
Locks	Storage account level	Disk level
Replication	LRS, GRS, RA-GRS	LRS
Encryption	ADE, SSE	ADE, SSE on by default
Pricing	• Standard per used GB • Premium per disk size	Per disk size
Storage account placement	Manual selection	Automatic
Storage account visibility	Visible	Not visible
Disk accessibility	• Storage account name and key • SAS	One time SAS, generated for export

-

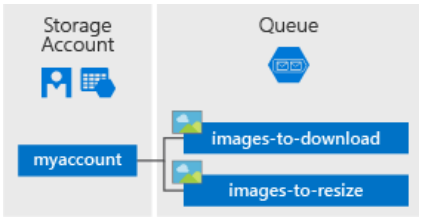
- Which two of the following virtual machines can support **premium** storage?
   i. DS-series
   ii. FS-series

2.6 Table storage

- The Azure Table storage service stores large amounts of **structured** data.
- The service is a **NoSQL** data store which accepts authenticated calls from inside and outside the Azure cloud.
- Azure tables are ideal for storing structured, non-relational data. Think of tables more as a spreadsheet of information where there is no linkage or relationship (joins) between the information.
- **Table storage** supports transactions for entities in the same table and table partition, but not across tables or partitions.
- An Azure table entry can have a maximum of **255** properties?
- A **table** is a collection of **entities** and the **entities** are a collection of **properties**.

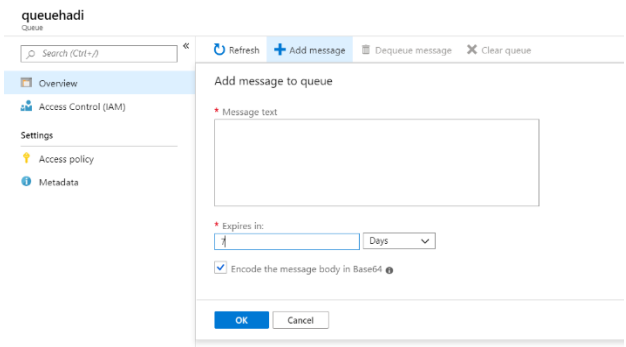
- We can't add entities or manipulate the table content within Azure portal, but this is possible within Azure Storage Explorer.
- 

2.7 Queue Storage:

- Azure Queue storage is a service for storing large numbers of **messages** that can be accessed from anywhere in the world via authenticated calls using HTTP or HTTPS.
- A single queue message can be up to **64** KB in size, and a queue can contain millions of messages, up to the total capacity limit of a storage account.
- Common uses of Queue storage include:
  i. Creating a backlog of work to process asynchronously
  ii. Passing messages from an Azure web role to an Azure worker role
- 

- How many days can a message remain in the queue? **7** days.
- Get-AzureStorageQueue

  display the approximate number of messages in a storage queue associated with an Azure Storage account.

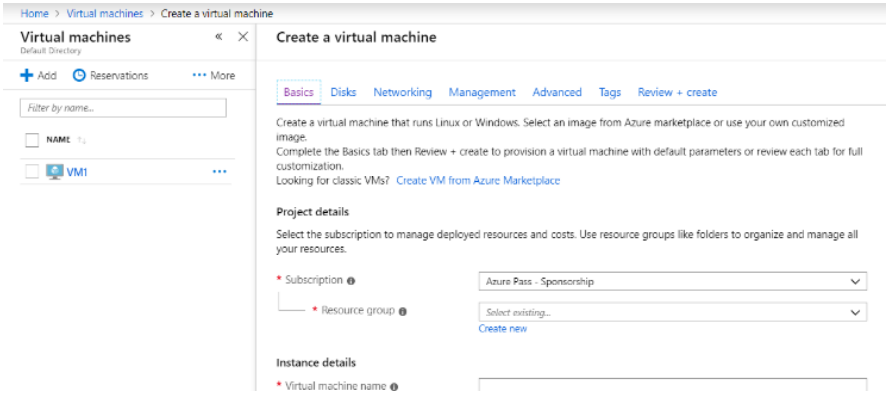


3 Deploy and manage virtual machines (VMs) (15-20%)

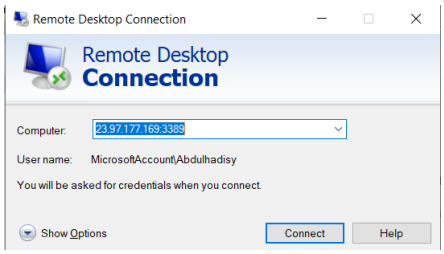
3.1 Create and configure a VM for Windows and Linux

3.1.1 Create a virtual Machine

- An Azure Virtual Machine is an on-demand, scalable computing resource deployed on Azure through various methods.
- Home → Virtual machine → +Add



- Not all regions have the **availability zone** option.
- **Accelerated networking**: means that two virtual machines at the same VNet can communicate much faster than the standard networking, it provides Ultra-low network latency.
  i. Not all VMs sizes support this option.
  ii. This connection is between the **NIC** and the **VM**.
  iii. Single Root – Input/output visualization (**SR-IOV**)
- The public IP address **is not directly connected** to the VM, rather its connected to the Network Interface Card **NIC**. And the NIC connected to the VM.
- You can connect to the virtual machine by using the **Connect** button In the Azure portal or by copying the **Public IP address** or **DNA** name and past it in the **RDP** connection.



- **RDP** is used for windows machines, **SSH** is used for Linux.
- Connect to the Virtual Machine: We can connect VMs through either RDP (**3389**) or SSL (**22**).
- Create Multiple VMs using **PS**:

```
# Great a resource group
New-AzResourceGroup -Name testPS -Location westeurope
#capture the input parameter in a variable
# prompt for a username and password for the VMs admin account and capture the result in a variable
# We use Get-Credentia to save the chosen user name and password
$adminCredential = Get-Credential -
Message "Enter a username and password for the VM administrator."
# Add a loop that executes three times to create a new VM for each loop iteration
  For ($i = 1; $i -le 3; $i++) # I = 1 & 2 & 3
  {
  # create a name for each VM, store it in a variable and output it to the console
  # We will get: Azdemo1, Azdemo2, Azdemo3
  $vmName = "AzDemo" + $i
  Write-Host "Creating VM: " $vmName
  # create a VM using the $vmName variable
  New-AzVm -ResourceGroupName testPS -Name $vmName -Credential $adminCredential -Image "UbuntuLTS"
}
```

3.1.2 Configure high availability, Windows[40], Linux[41]

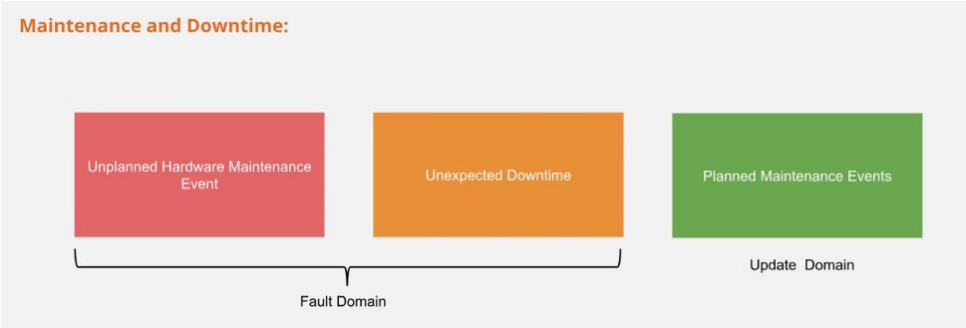
- The Downtime for a VM can happens in three scenarios:
  i. **Unplanned Hardware Maintenance Event**: Azure predict a failure, then use **Live Migration Technology** (A feature of **Hyper-V**) to migrate the VM from the failure HW to a healthy HW. In this scenario VM will **not experience downtime**, but the performance **might** change for a while.

[40] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability
[41] https://docs.microsoft.com/en-us/azure/virtual-machines/linux/manage-availability

ii. **Unexpected downtime**: The HW fail **unexpectedly**, the Live migration technology **can't** be used, Azure Automatically migrate the VM to a healthy HW in the **same Datacentre**, the VM will experience downtime during migration and **all data on the temporary disks (D drive) will be lost**.

The aforementioned two scenarios are solved in Azure using **Fault Domain (FD)** within the **Availability set** solution.

iii. **Planned Maintenance Events**: periodic update planned by Microsoft for the infrastructure, this is handled by **Update Domain (UD).**



- **Four** tasks should be performed to maintain the VM in high availability:

i. Add multiple Virtual Machines in an availability set (**AS**)

ii. Use **managed** disks for VMs in AS

iii. Add each **app tier** in a separate AS

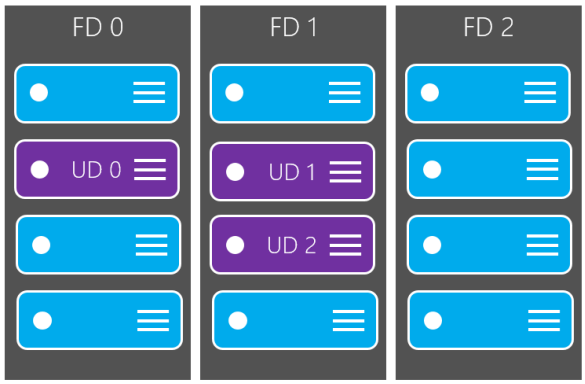
iv. Configure a **Load Balancer**.

- In Azure we have two features of VMs to configure high availability:

i. **Availability sets**: (SLA 99.95%) An availability set is a **logical** grouping of VMs within **one** datacentre that allows Azure to understand how your application is built to provide **redundancy and availability**. Its **only** protect your VMs from **HW** outages, not OS's or specific app failure.

An availability set is composed of two additional groupings that protect against hardware failures and allow updates to safely be applied:

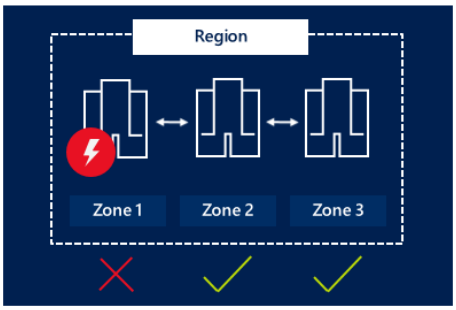
- **Fault domains:** A fault domain is a **logical** group of underlying hardware that share a common power source and network switch, similar to a **rack** within an on-premises datacentre.



- **Update domains:** An update domain is a **logical** group of underlying hardware that can undergo maintenance or be rebooted at the same time.

ii. **Availability zones (AZ):**[42] (SLA 99.99%)

- Each **zone** is made up one or more datacentres and is logically separated from other AZ in the same region.
- An Availability Zone is a **physically** separated zone within an Azure region.
- There are **three** Availability Zones per supported Azure region.
- Each Availability Zone has a distinct power source, network, and cooling.
- Availability zone provide **resiliency** across the entire region.
- Availability zone required a **managed disk**.

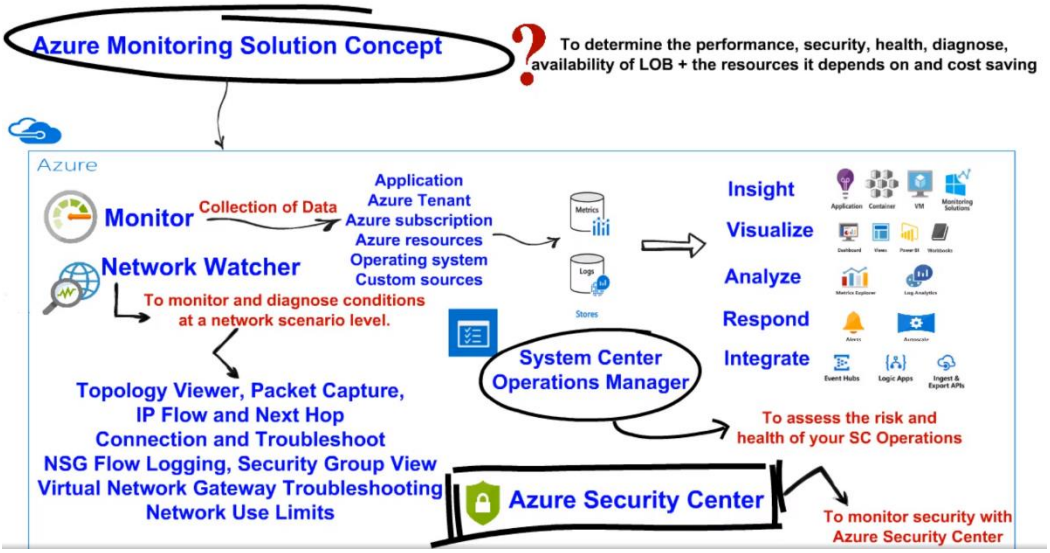


- Neither availability set nor Availability zones provide **load balancing.**
- Deploying VMs in Availability set/zones will increase the **SLA**.
-
- During any planned maintainous events the VMs in a single update domain are rebooted and they might be unavailable.
- **Managed disks** (SLA 99.9%). increase the availability through **isolating** the disks from each other to prevent **single point of failure**. Each disk has his **own** storage account.
- Not all azure regions have support for availability zones.
- Availability zone requires **manage disks**, and a **public IP address**.
- If you deploy either availability set or availability zone, you are not going to get **load balancer**, you need to deploy a load balancer to be sure that the traffic is evenly distributed.

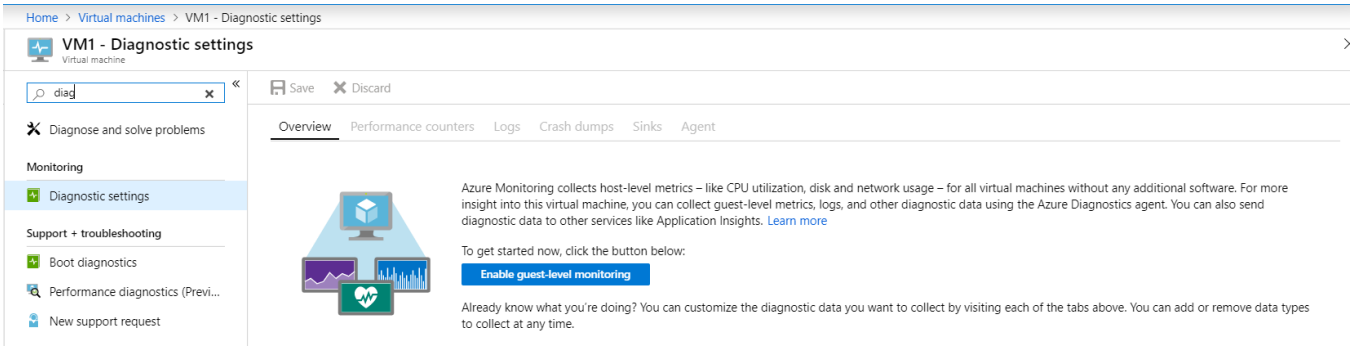
3.1.3 Monitoring, Networking, and Virtual machine size

[42] https://docs.microsoft.com/en-us/azure/availability-zones/az-overview

- **Monitoring[43]:**



- Azure Monitoring collects host-level metrics – like CPU utilization, disk and network usage – for all virtual machines without any additional software.
- For more **insight** into this virtual machine, you can collect **guest-level metrics**, **logs**, and other diagnostic data using the **Azure Diagnostics agent**.
- We need to collects the logs/data for a virtual machine, we need to install the **Azure Diagnostic Agent** at the Diagnostic setting blade. This can be done automatically by **enabling monitoring**. This should be done **per** VM.
- In **Sinks** blade, you can send the collected data to other service for more analytics, like **Application insight**, this will cost money.

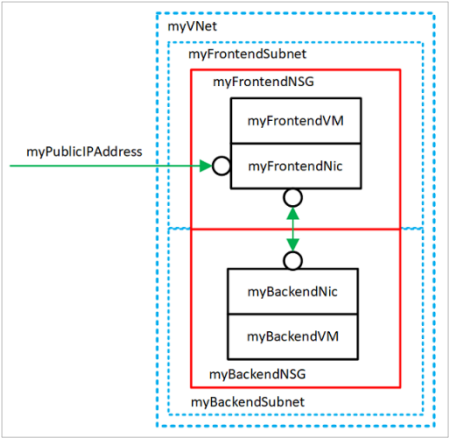


- **Networking[44]:**

- Azure VMs are located within a subnet within a VNet.

[43] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/monitor
[44] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-virtual-network

- Azure virtual machines use **Azure networking** (VNet) for **internal** and **external** network communication.
- Azure virtual networks enable **secure** network connections between virtual machines, the internet, and other Azure services such as Azure SQL database.
- Virtual networks are broken down into logical segments called **subnets**.
- **Subnets** are used to control network flow, and as a security boundary.



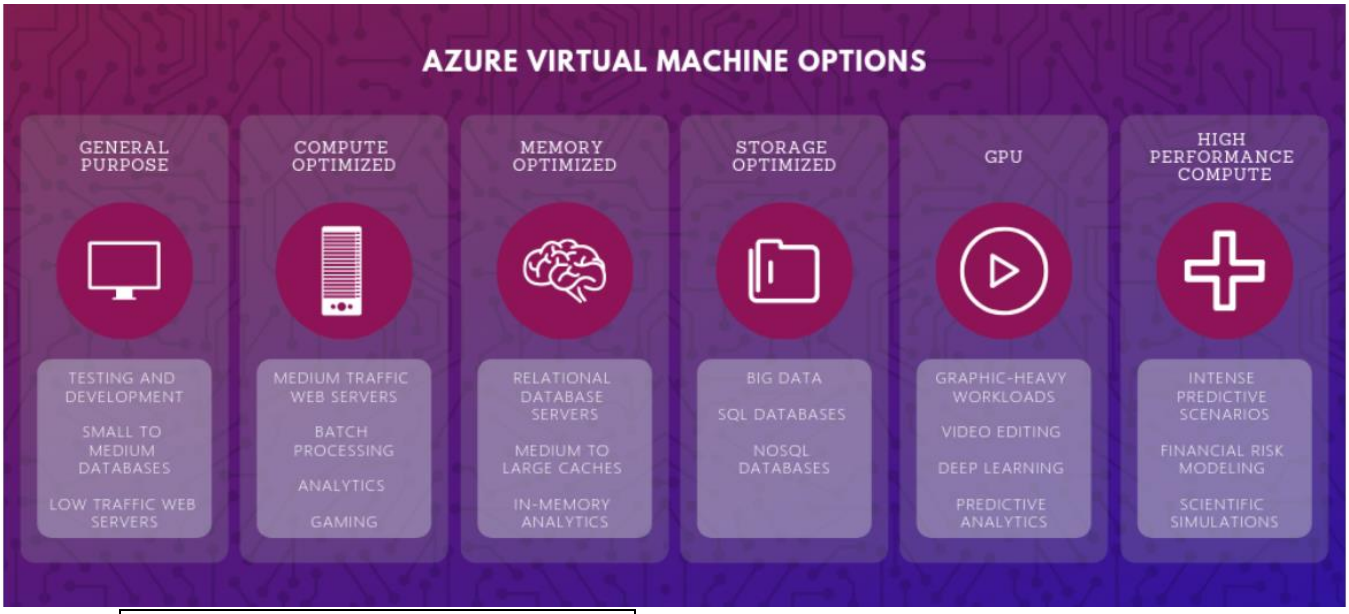
- Most of the VMs can have **more** than one NIC (not all VM **sizes** support multiple VMs).
- **Public IP**: is **standalone** source to connect the virtual machine with sources out of the VN. It's not connected directly to the VM, instead its **connected** to the **NIC** which in role connected to the VM.

Top-level resource	IP Address association	Dynamic	Static
Virtual machine	Network interface	Yes	Yes
Internet-facing Load balancer	Front-end configuration	Yes	Yes
VPN gateway	Gateway IP configuration	Yes	No
Application gateway	Front-end configuration	Yes (V1 only)	Yes (V2 only)

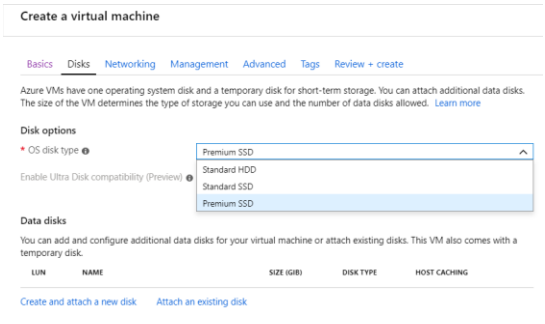
Private IP: to communicate with other VMs in the **same** VNet or on-premises network but then using **VPN gateway**.

- Network Security Group **NSG** can be assigned to a subnet or an Individual NIC (Individual VM).

- **Virtual Machine size:** [45]



- Get-AzVMUsage -Location "West Europ"
- Not all series of the VMs are available in all the regions.
- **VM Storage**[46]
- Each VM has by default two disks, OS disk (stored in Azure storage account "C drive by default") and temporary disk drive "D drive by default" which is a part of the **host machine**.
- In case of **failures** in the Host machine, Azure will move the VM to another Host Machines, this will cause the **loose** of all the data in the **temporary disk** but not the data within the OS disk.
- The OS disk is a **SATA** drive
- Data disk and OS disk are VHD (virtual hard **disk)** stored in an Azure storage account.
- The **size** of the VM determine how many Data Disks you can attached to the VM and the type of storage you can use to host the disks.
- **Types of VM disks**:



i. **Standard HDD**: Low Performance, reliable

- Use Cases:
  a. Dev/Test
  b. Less critical workloads
  c. Data Storage (file servers)

[45] https://www.nigelfrank.com/blog/microsoft-azure-virtual-machines-for-the-confused/
[46] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/attach-managed-disk-portal

ii. **Standard SSD** (recommend by Microsoft): **Consistent Performance**, **lower latency**, Better reliability and better availability.

- Use Cases
    a. Web Servers
    b. Low IOPS application servers
    c. Light to medium use enterprise applications

iii. **Premium SSD**: High Performance, Low latency, capacity guarantee, available on most VMs and 99.9%SLA

iv. (**Ultra-SSD**): High throughput, High IOPS. **Extremely** expensive.

- Limitations
    a. Only available as **data disk**
    b. Only supported on ES/DS V3 VMS

- **Temp Disk:**

i. Physical SSD on the Hyper-V host

ii. Subject to potential loss at any time

- Deallocation. Redeploy, Restart, Service healing related moves

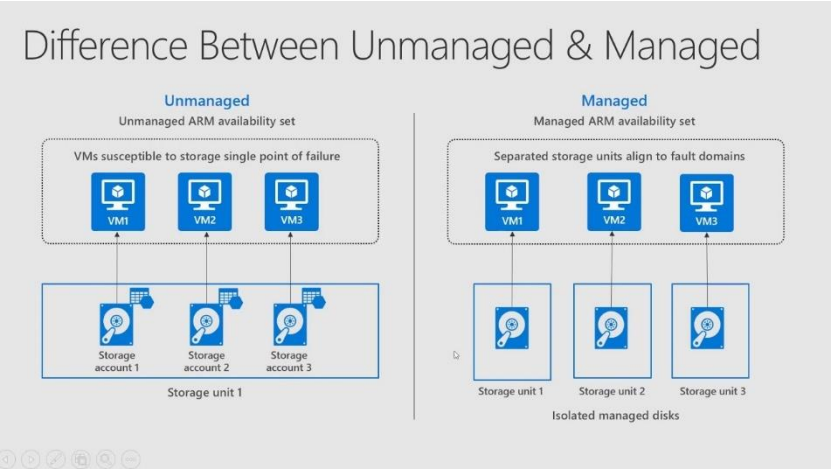
iii. No data recovery possibility

iv. Used to save the system paging file

- Can also be used for
    a. DB caching
    b. Swap files
    c. Processing data

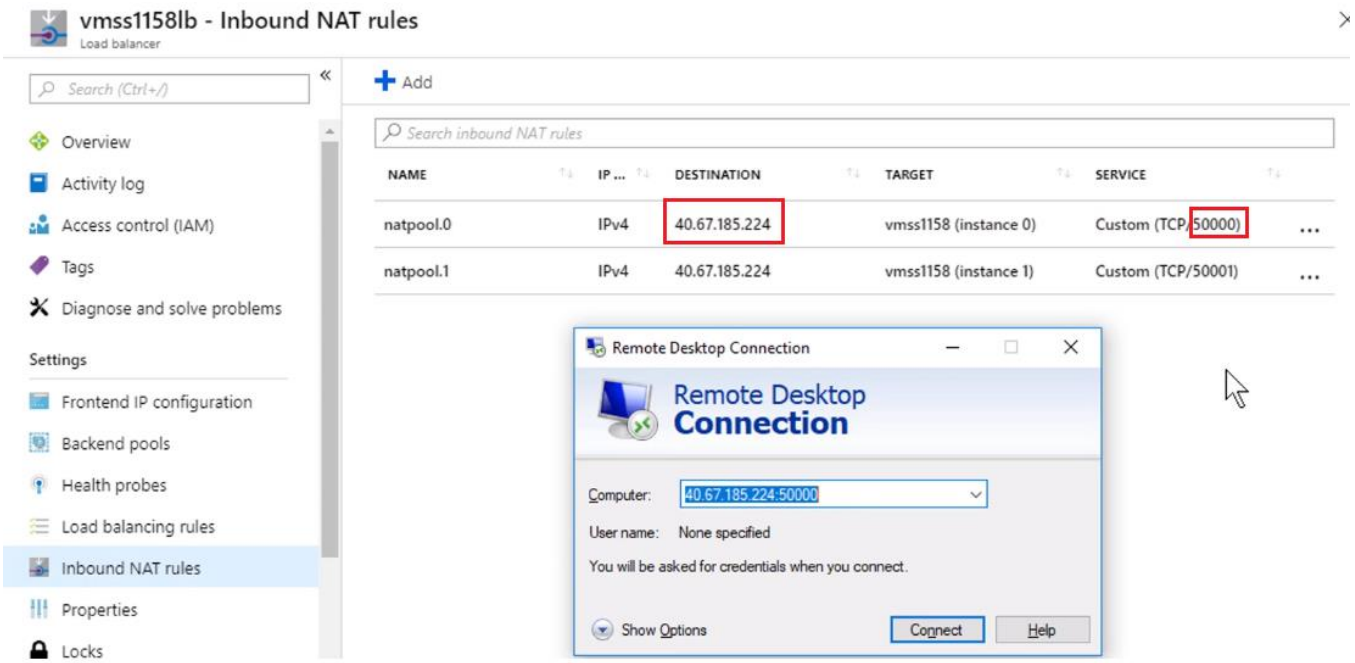
- **Managed Vs Unmanaged Disk**

- When deploying several unmanaged disks in 1 storage account we will face the scalability target problem, since each Storage Account can handle only around 20,000 IOPS.



3.1.4 Virtual Machine Scale Set (VMSS)[47]

- VMSS allow you to **scale out/in** your infrastructure on demand.
- Used for **VMs** and **Web App**
- It creates **identical** VMs / Web Apps
- VMs or Web App can be placed behind **Load Balancer** or **Application Gateway**.
- All the VMs in the VMSS are **identical** and have the same image.
- Deploy as **low priority** option during the creation of the VMSS means that the azure platform will take back these VMs at any time whenever it need capacity, this will low the cost up to (80%). In this case all VMs are located in the same Fault Domain and azure will not guarantee High Availability.
- By default, VMSS are deployed in an **Availability set**, but we have the option to deploy it in **availability zone**.
- When creating a **load balancer (LB)** inside the VMSS, both the LB and the VMSS will have the same **Public IP**. We could create a different PIP for each VM, but this is not recommended.
- To communicate with each VM individually, we use the **Inbound NAT rules** from the LB blade.



- The LB uses **Health prob** to check the state of the VMs on the **Backend pool**

[47] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-create-vmss

3.2 Automate deployment of VMs

3.2.1 Create VM in PowerShell

```
New-AzResourceGroup -Name myResourceGroup -Location EastUS

New-AzVm `

    -ResourceGroupName "myResourceGroup" `

    -Name "myVM" `

    -Location "East US" `

    -VirtualNetworkName "myVnet" `

    -SubnetName "mySubnet" `

    -SecurityGroupName "myNetworkSecurityGroup" `

    -PublicIpAddressName "myPublicIpAddress" `

    -OpenPorts 80,3389
```

3.2.2 Start and Stop a VM in PowerShell

```
Stop-AzVM -ResourceGroupName "RG-name" -Name "VM-name"

Start-AzVM -ResourceGroupName "RG-name" -Name "VM-name"
```

3.2.3 Modify Azure Resource Manager (ARM) template[48]

- Azure Resource Manager is the **deployment and management service** for Azure.
- It provides a management layer that enables you to create, update, and delete resources in your Azure subscription.
- Resource Manager templates are **JSON (**JavaScript Object Notation) files that define the resources you need to deploy for your solution.

[48] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-quickstart-create-templates-use-the-portal

- https://www.youtube.com/watch?v=MZTb9NtZOh4
- An ARM template is **idempotent**, which means it can be executed as many times as you wish, and the result will be the same every time. The user declares the **type** of **resources** and its properties and then the API will either great a new object that either matches those details or if the object already exists with the same name and type then it will just update its properties.
- **ARM template Syntax**:

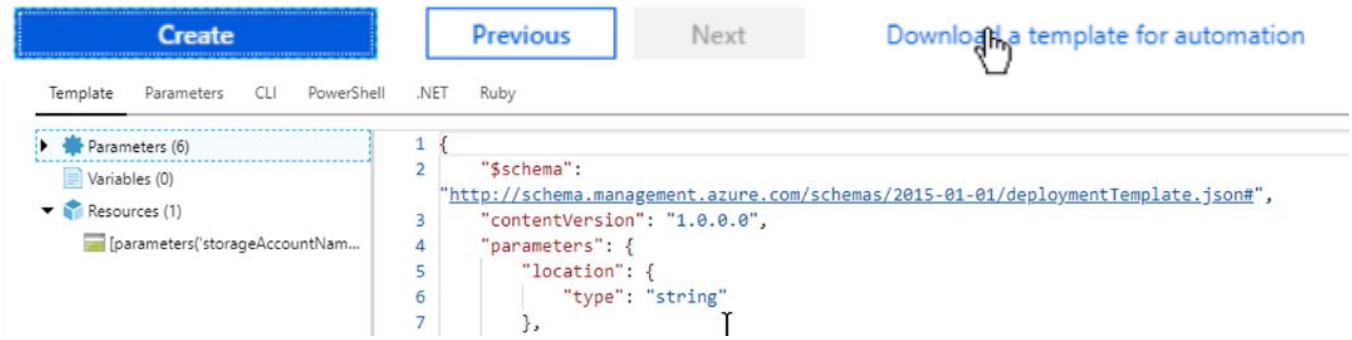
Components in Detail

Element	Required	JSON Type	Description
$schema	Yes	String Value	Location of the JSON schema file that describes the version of the template language.
contentVersion	Yes	String Value	Version of the template (such as 1.2.0.20). When deploying resources using the template, this value can be used to make sure that the right template is being used.
parameters	No	JSON Object	Values that are provided by the end user (manually or via a parameters file) when deployment is executed to customize resource deployment.
variables	No	JSON Object	Values that are reused multiple times in the template. You can update these values. They are different from Parameters as their value is known and they are not required as inputs from the end user.
resources	Yes	Array of Objects	Types of services that are deployed or updated in a resource group. Each JSON object in this Array denotes an Azure Resource.
outputs	No	JSON Object	Values that are returned after deployment.

-

- **JSON syntax**: JavaScript Object Notation.
  i. Objects are unordered sets of name and value pairs
  ii. An object begins with left curly brace and ends with right curly brace
  iii. Each name and value are enclosed by double quotes
  iv. Names and values are delimited by a colon
  v. Name and value pairs are delimited by a comma
- Generate an ARM template in Azure portal

i. After finishing configuring most of the resources and before the final create execution, you



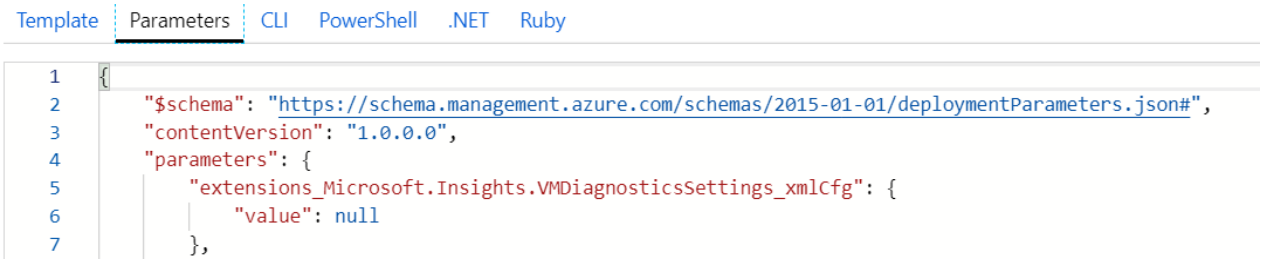
will get the option "**Download a template for automation**"

In the template blade, the CLI, PowerShell, .Net, Ruby only exist to execute the template, they are not the equivalent of the template.

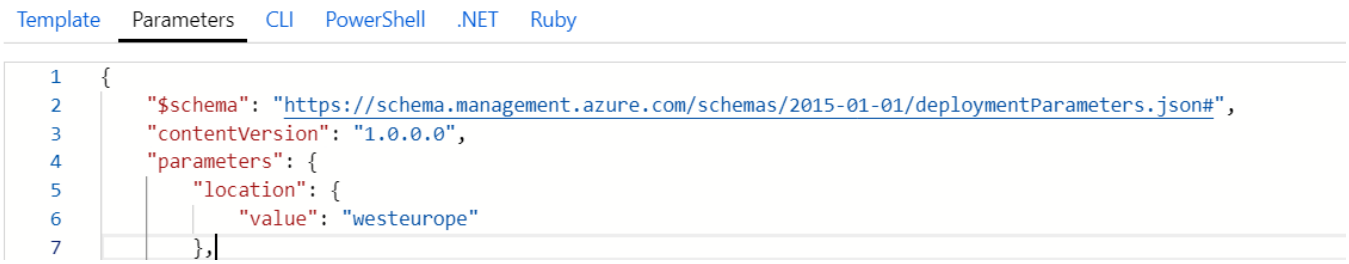
ii. To update a downloaded template, use **Template Deployment** service.

iii. Different resources have different ways to reach their ARM template:

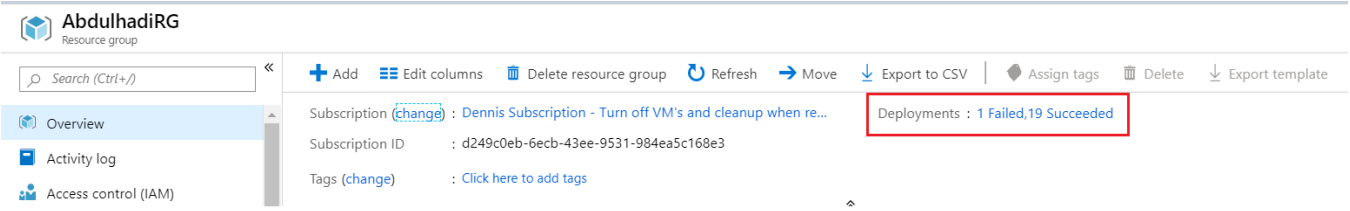
- Resource blade→ Export Template: will give us an **unfriendly code**.



- RG → deployment (for the resources deployment inside the RG): this is more



readable and contains the latest changes in the resource.

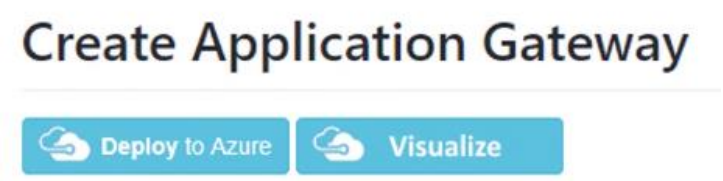


- In JSON template, **variables** are similar to **parameters**, but they are **computed values**.
- **DSC: Desired State Configuration.** Happens when you deploy a JSON template with similar configurations and then Azure will not do nothing. (see 3.3.3)
- **Deploying a template:**

i. From **Template Deployment service** within Azure and deploy the JSON file

ii. Using PowerShell → cd (to the PS file location on the hard disk) → ./file.ps1

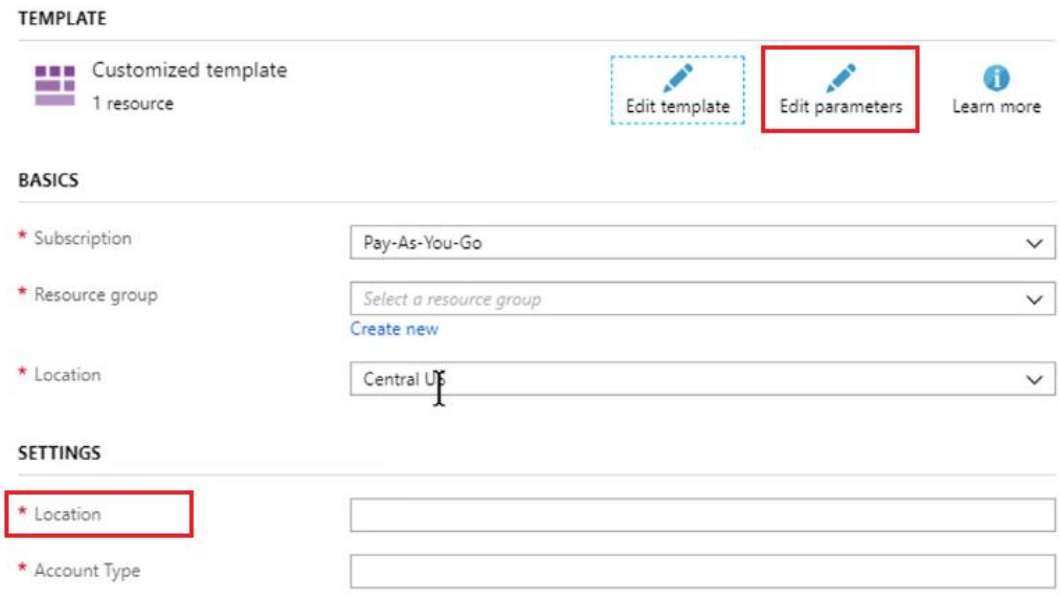
iii. Some templates founded in **GitHub** and can directory deploy to Azure.



- https://github.com/Azure/azure-quickstart-templat

3.2.4 configure location of new VMs

- An existing VM → Export Template → Download
- **Template Deployment** → Load File (load the downloaded template and parameters file from first step) –



update the template and press save → the Template Purchase blade will be shown: Here you can update the Location

- We could also update the Template.Json file:

```
{
            "type": "Microsoft.Compute/virtualMachines",
            "apiVersion": "2019-03-01",
            "name": "[parameters('virtualMachineName')]",
            "location": "[parameters('location')]",
```

- And Also, we could update the Parameter.json file.

```
"parameters": {
       "location": {
        "value": "westeurope"
        },
```

3.2.5 Configure VHD template[49]

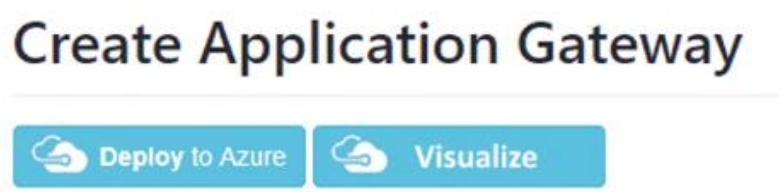
- **VHD: Virtual hard disk**
- Using PS:
  i. Create the virtual machine with New-AzVM.
  ii. Create the initial configuration with New-AzDiskConfig.
  iii. Create the data disk with the New-AzDisk.
  iv. Get the virtual machine that you want to add the data disk to with the Get-AzVM.
  v. Add the data disk to the virtual machine configuration with the Add-AzVMDataDisk.
  vi. Update the virtual machine with the Update-AzVM.

3.2.6 Deploy from template[50]

- From **Template Deployment** service within Azure and deploy the JSON file
- Using PowerShell → cd (to the PS file location on the hard disk)→ ./file.ps1

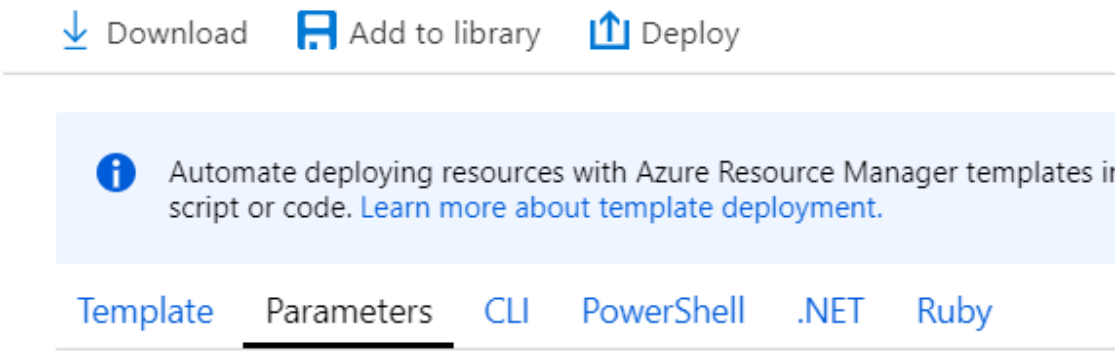
[49] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-manage-data-disk
[50] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy

- Some templates founded in GitHub and can directory deploy to Azure.



3.2.7 Save a deployment as an ARM template[51]

- Any template blade has the download button, which will download the 6 files: Template.Json, Parameter.json, CLI, …
- Within the template blade, we have **Add to library**



- To view the template: **Template** service. And then you can **Edit** and **Deploy**.

3.2.8 Deploy Windows and Linux VMs[52]

- First, we create the Template.Json file using any of the different editors available (Azure Template Deployment, VS code…) and save it.
- Create the Parameter.json file
- Deploying the file can be done in different ways. Some them are explained in **3.2.6 Deploy from template** section.

3.3 Manage Azure VM

3.3.1 Add Data Disk to VM[53]

- The size of the VM **determined** how many data disks you can attach.
- The managed disk blade inside the VM is a **separate resource**.

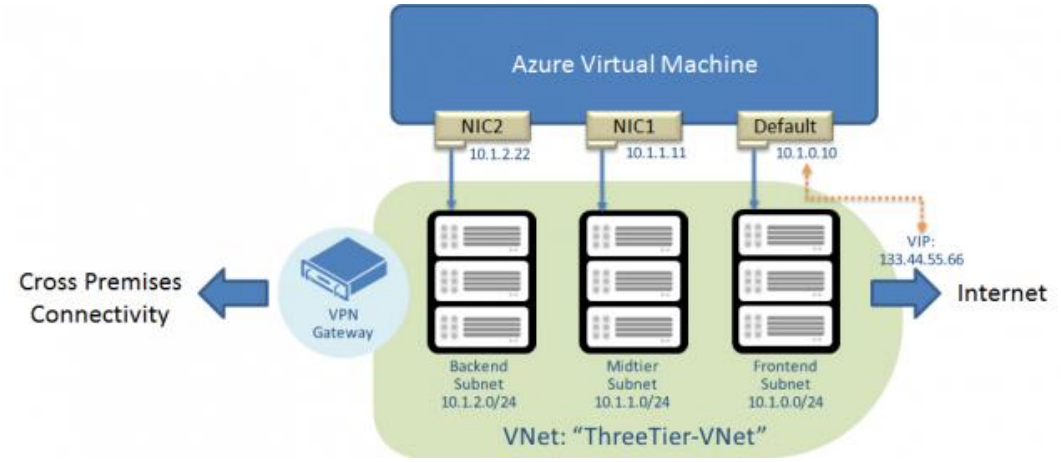
---

[51] https://blogs.msdn.microsoft.com/benjaminperkins/2018/05/16/how-to-usecreate-arm-templates-for-deployments/
[52] https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy-portal
[53] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/attach-managed-disk-portal

- When crating a disk from the VM, by default the location of my disk is the **same** as the VM.
- **Host caching** will give **better performance** for your Disks, host caching can be for **Read** operation or for **Read/Write** operations.
- After creating a Disk, you should **initialize** it to the VM, this can be inside the VM image operating system, in Windows by using **Disk Management tool**.
- Each Disk can be attached to **only on VM at a time**, you can de-attached a disk and attach it to another VM.

3.3.2 Add Network interface to the VM[54]

- Each VM can have **multiple** NICs, where each have its **own** public IP address.
- But all of them should be at the **same VNet**. And they can be attached to **different Subnets**.
- The number of possible NICs attached to VM **depends** on the size of the VM.
- **NSG** used to filter network traffic and work on either subnet level or NIC level.
- **NIC** should be in the **same location** as the VM and the VNet
- **NIC** should **not** be in the same resource group for the VM and the VNet.
- We need to **stop** the VM before attaching the NIC.
- Azure only create a Default gateway (Public IP) to the **first** NIC, but it doesn't do that for the second one. Therefore, you are **unable to connect** to the resources outside the subnets from the second attached NIC by default.
- Once you have multiple NICs, you need to configure the OS within the VM to use them correctly.



[54] https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface

3.3.3 PowerShell Desired State Configuration (DSC)[55][56]

- https://app.pluralsight.com/player?course=practical-desired-state-configuration&author=josh-duffney&name=practical-desired-state-configuration-m0&clip=0&mode=live
- **Desired State Configuration (DSC)** is a management platform in Windows PowerShell that enables deploying and managing **configuration data** for software services and managing the environment in which these services run.
- DSC provides a set of Windows PowerShell language extensions, Windows PowerShell cmdlets, and resources that you can use to declaratively specify how you want your software environment to be configured.
- It also provides a means to maintain and manage existing configurations.
- DSC centers around creating **configurations**. A configuration is an easy-to-read script that describes an environment made up of computers (nodes) with specific characteristics.
- In this example we are installing IIS on the localhost. The configuration will be saved as a .ps1 file.

```
configuration IISInstall
        {
         Node “localhost”
         {
         WindowsFeature IIS
         {
         Ensure = “Present”
         Name = “Web-Server”
}}}
```

- The DSC script consists of the following:

i. The Configuration blocks.
ii. One or more Node blocks.
iii. One or more resource blocks.

[55] https://docs.microsoft.com/en-us/azure/automation/automation-dsc-overview
[56] https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-dsc-configuration

- **DSC:** Desired State Configuration. Happens when you deploy a JSON template with similar configurations and then Azure will not do nothing.
- The location in the Automation **might be** in different location as the resources (VM, DB …) but it prefers to have all in the same location for performance considerations.
- Built-In Windows PowerShell Desired State Configuration Resources - https://docs.microsoft.com/en-us/powershell/dsc/resources/resources#built-in-resources
- **Example**:

  Your company has Windows Server 2012 R2 VMs and Ubuntu Linux VMs in Microsoft Azure. The company has a new project to standardize the configuration of servers across the Azure environment. The company opts to use **Desired State Configuration (DSC)** across all VMs. You need to ensure that DSC can be used across all the VMs. What two things should you do?

  i. Deploy the DSC extension for Windows Server VMs.

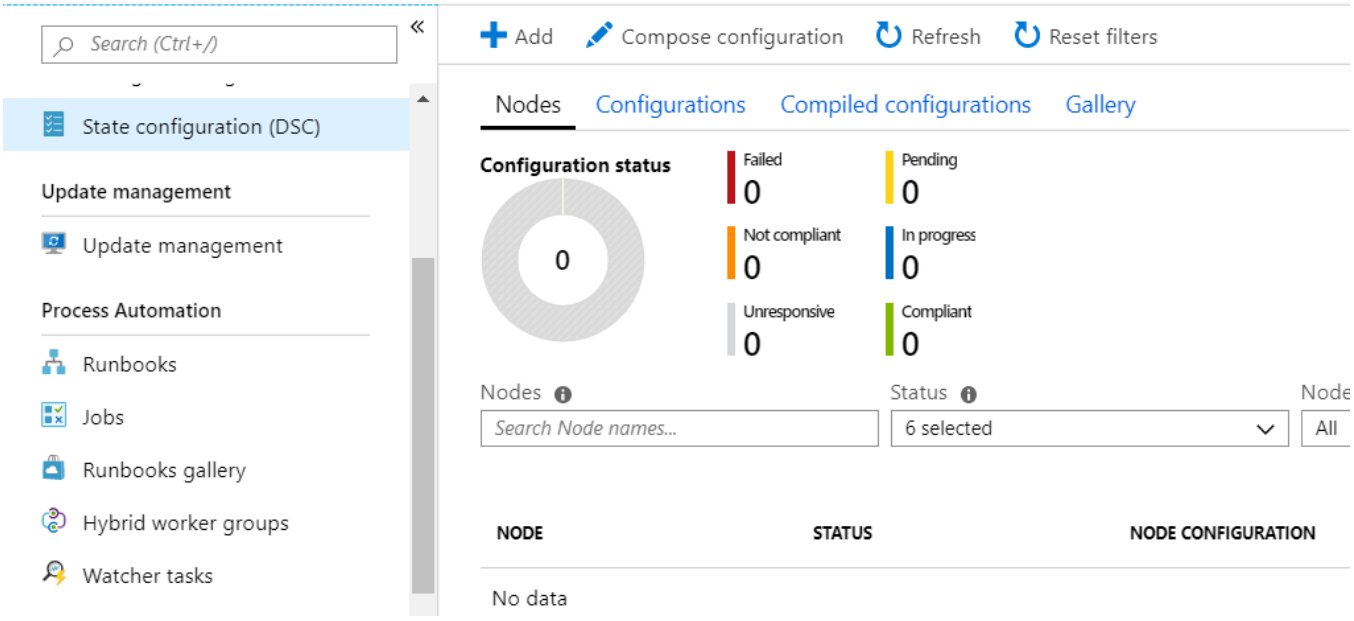
  ii. Deploy the DSC extension for Linux VMs.

  Explanation

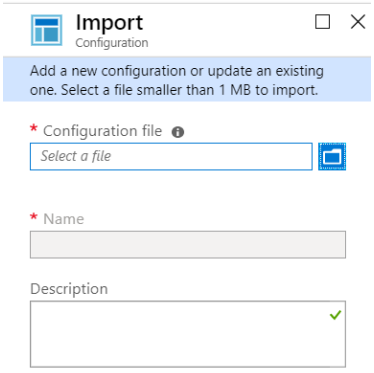
  Desired State Configuration (DSC) is available for Windows Server and Linux-based VMs. In this scenario, you just need to deploy the extensions to the existing VMs to start using DSC.

- **Azure Automation**: is a service in Azure that is used to configure the DSC resources.
- **Azure → Automation Accounts→ +Add → name (TestDSC)**

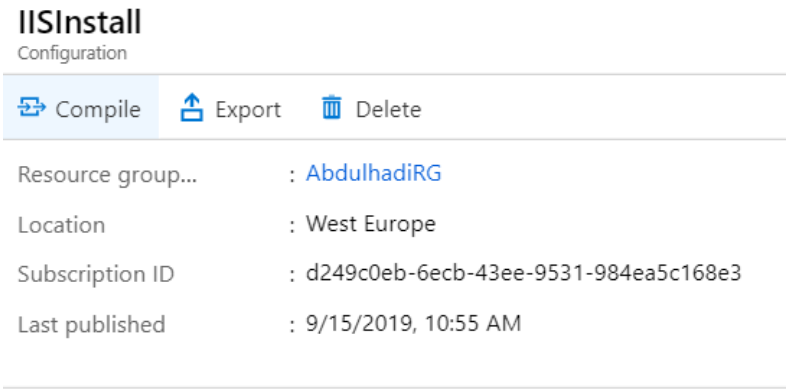
  i. TestDSC → State Configuration: we add the node and the configuration her.



ii. After writing the DSC file, add it in the configuration tab:



iii. **Before** applying a DSC file to a specific node, the file should be compiled to node configuration document known as: MUF document and paled on the automation pull server. This can be done with the DSC file blade→ Compile



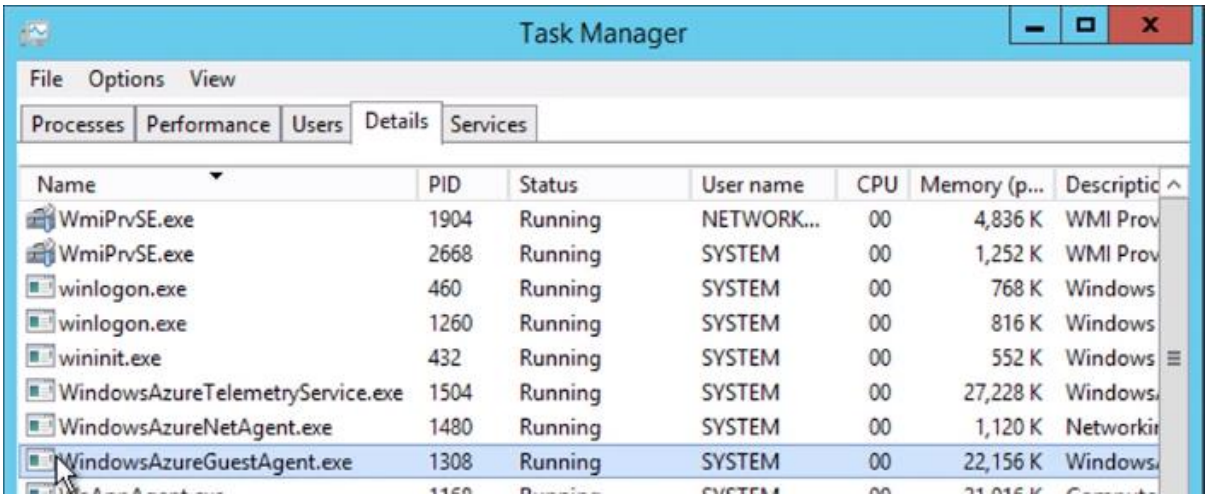
3.3.4 Automate Configuration Management with VM agent using Custom Script Extension

- **VM agent**:

i. VM agent is secure **lightweight** process that manages VM interactions with the Azure **Fabric** controller.

ii. It enables executing Azure VM extensions.

iii. VM agent is installed by default in Windows.



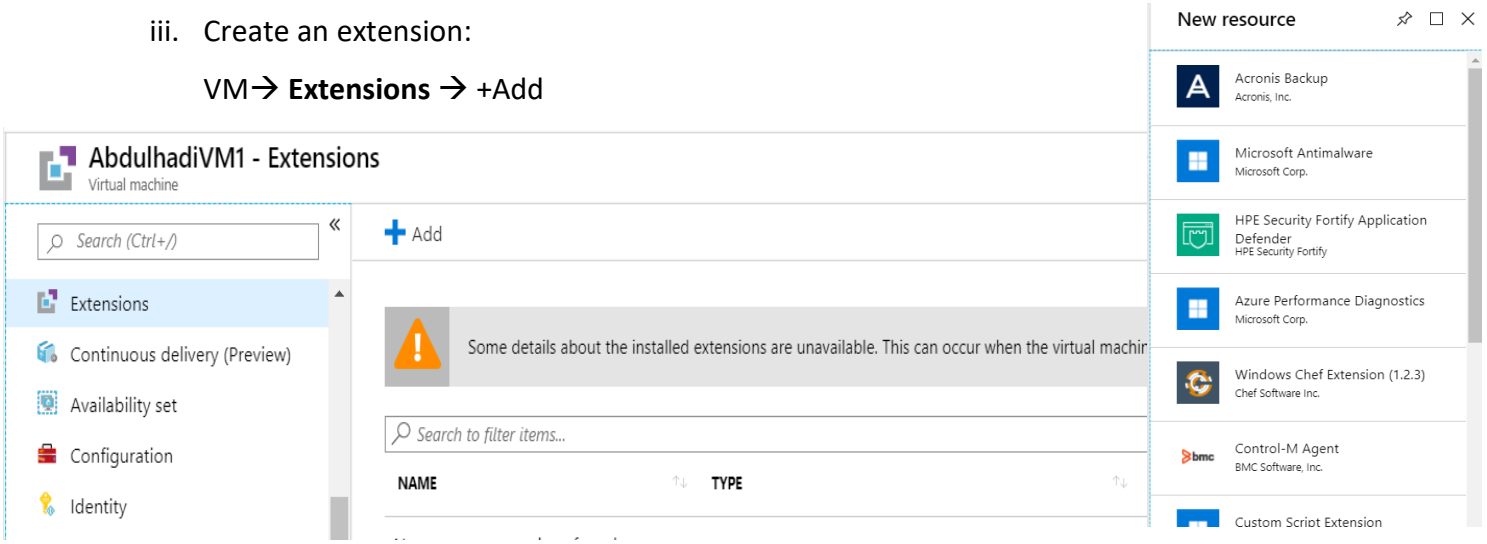
- **VM extensions:**

i. Small **application** that provide post-deployment configuration and automation task over the VM.

ii. There are many inbuild extensions in Azure and you can also build a customise script extensions.

iii. Create an extension:

VM→ **Extensions** → +Add



3.3.5 manage VM sizes; move VMs from one resource group to another[57]

- **VM size:**

i. We can see the VM size and change it from the VM blade VM → Size

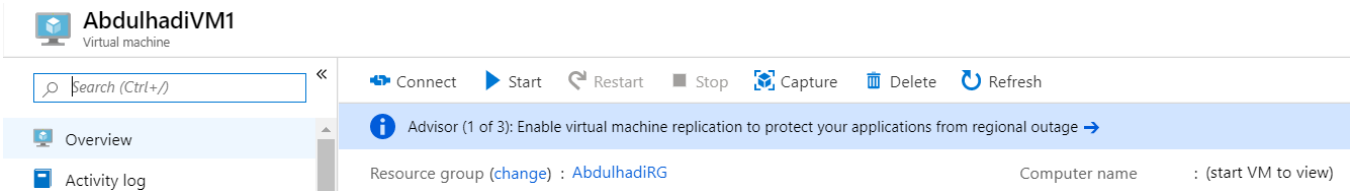
[57] https://docs.microsoft.com/en-us/azure/virtual-machines/windows/move-vm

ii. Changing the VM size will cause the VM to **stop** and will cause a **downtime**.

- **Moving VMs: Two ways**

i. RG level → Move → Move to another resource group

ii. VM blade → Overview → Resource group (change)



iii. Using PS:

```
Move-AzResource
```

3.3.6 Redeploy VM

- When deploying VM, Azure will shut down the VM and **move** it to a new **node**.
- In redeploy you will keep all you setting, but all data in temporary **(D drive**) will be **lost**.
- VM blade → Redeploy
- Using PS

```
set-azvm -Redeploy
```

3.4 Manage VM backups

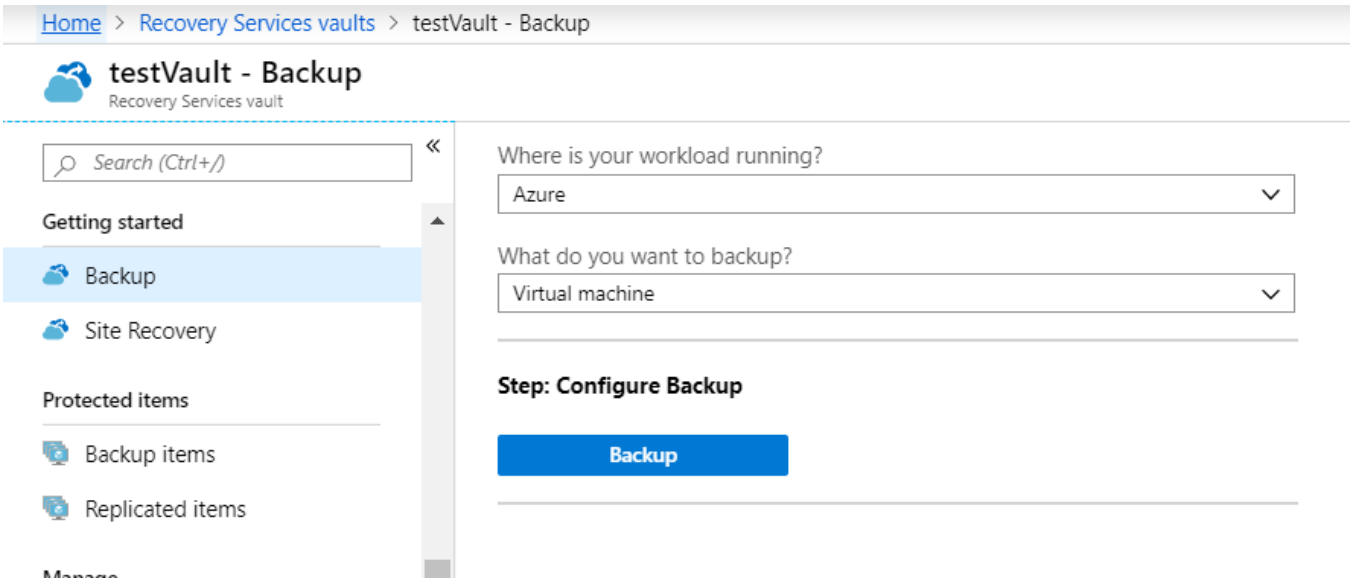
3.4.1 configure VM backup

- There are many ways to backup the VMs:

i. **Recovery Services Vault (RSV)** holds the backup copies and you can monitor backup using this vault. The RSV should be in the same region as the VM.

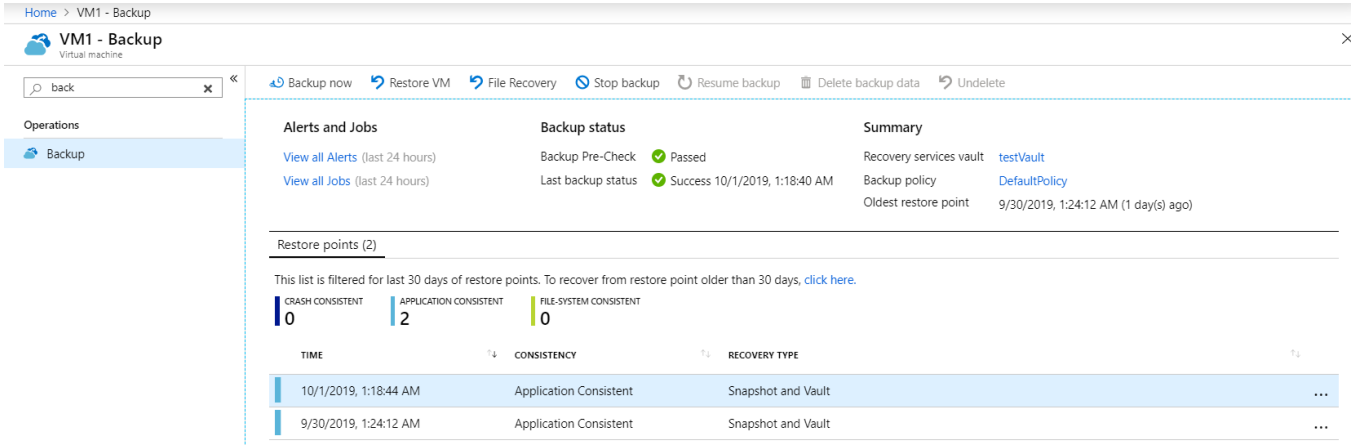
- Home → Recovery Services Vault (RSV) → +Add

a. Recovery Services Vault (RSV) → [Vault name] → Backup → Virtual Machine



- **From the VM blade:**

i. VM blade → Backup → Backup now



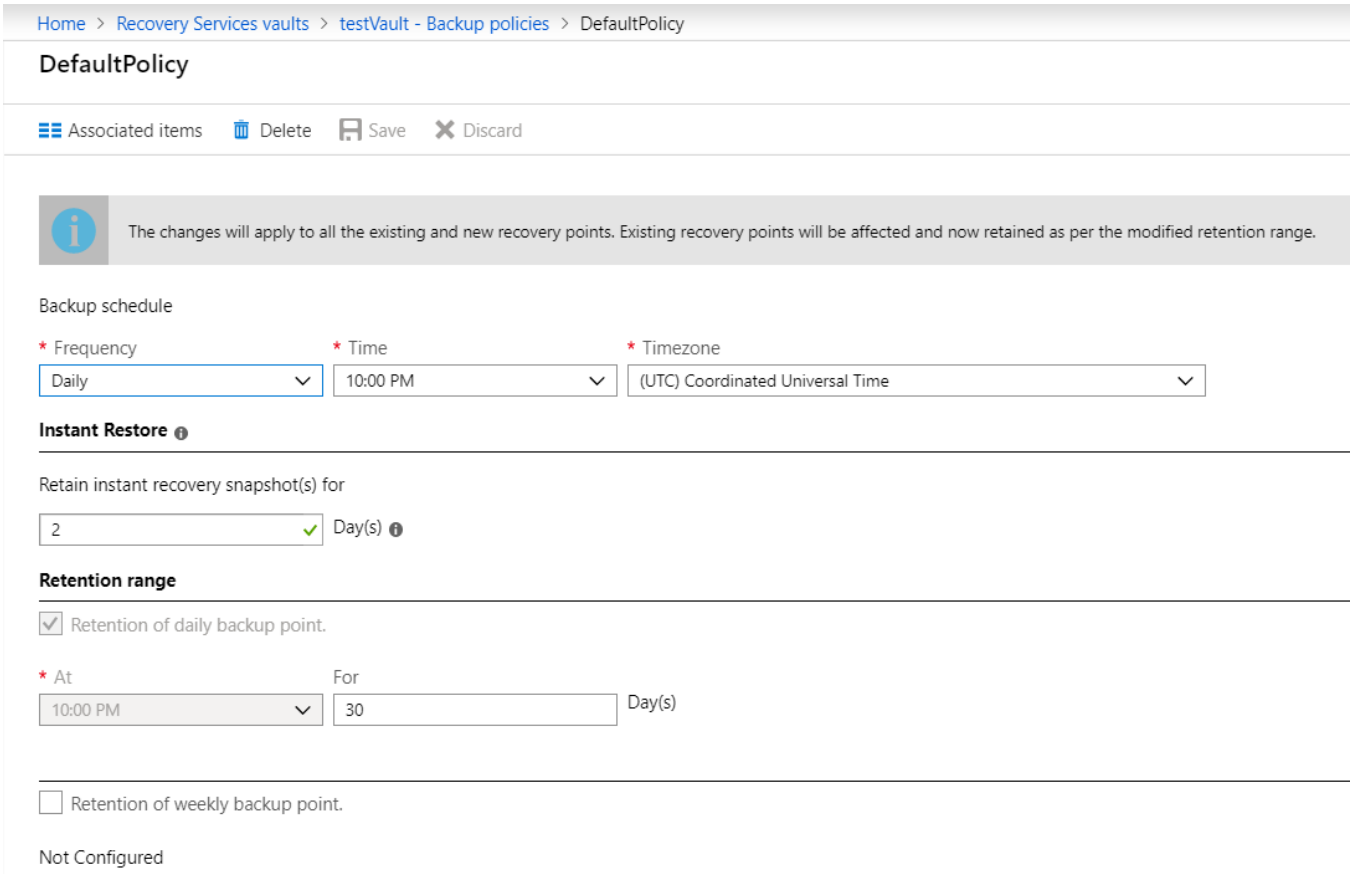
ii. The recovery service vault has to be in the **same** region as the VM.

iii.

3.4.2 Define backup policies

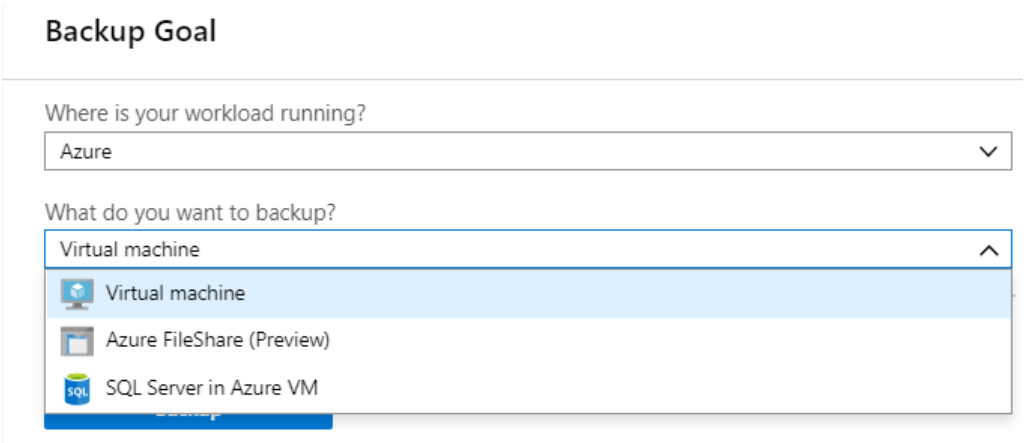
- Backup policy specifies **frequency and time** at which items will be backed up and how long backup copies are retained.
- Backup Policies can be configured during the creation of the backup.
- You can use the default policy or create your own ploicy
- If you need to change the backup policy for a VM after creation the backup, you can do thos from the Recovery service vault

i. Recovery service vault → Backup policies → DefaultPolicy



The changes will apply to all the **existing and new recovery** points. Existing recovery points will be affected and now retained as per the modified retention range.

ii. Associated Item → +Add →



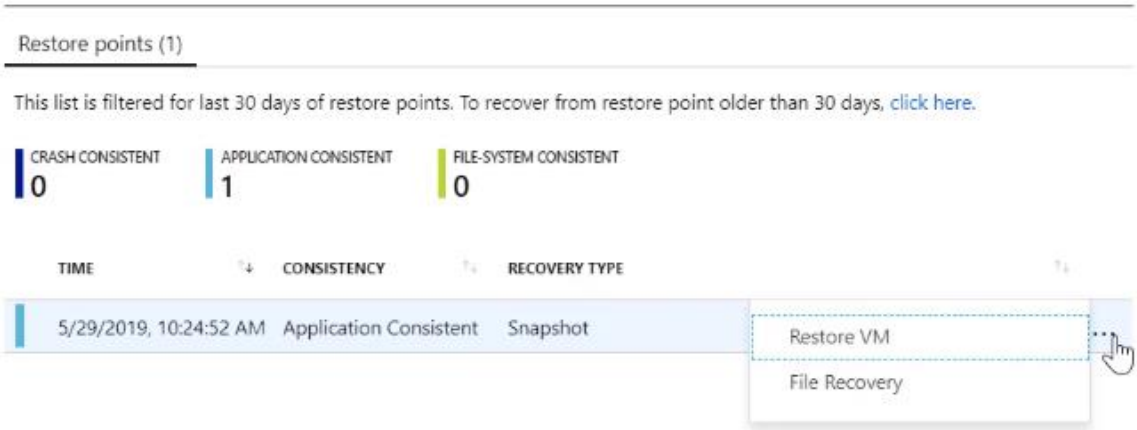
- **Retention ranges** is important

3.4.3 Restore a Virtual Machine

- Of taking a backup of a VM, we can restore it using the various restore points.

- After creating the backup → backup → **Restore VM**

- **Restore options**:
  i. Create new
  ii. Replace existing
- **Restore Type**
  i. Create virtual machine
  ii. Restore disks



-

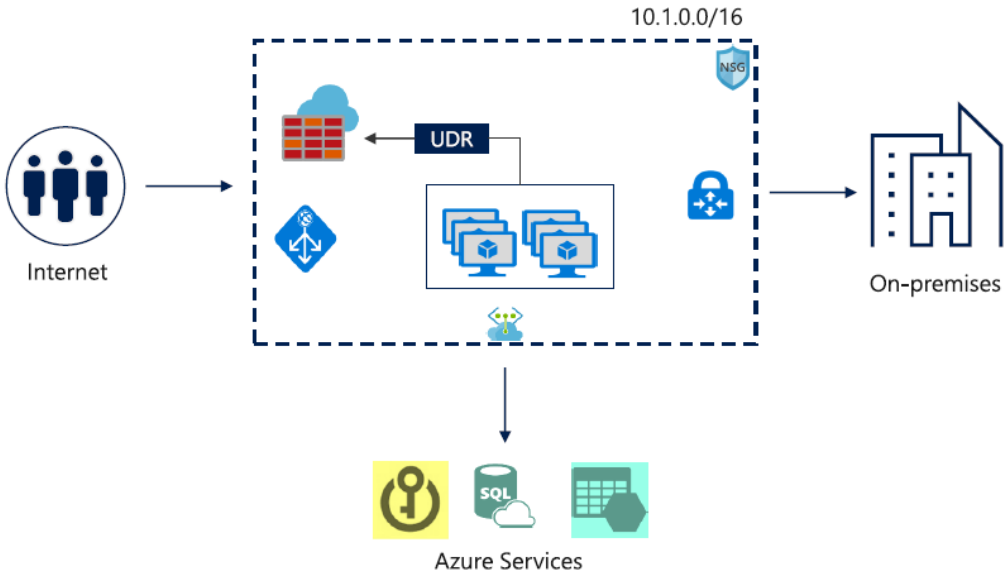
3.4.4 Azure Site Recovery[58]

- Azure Site Recovery **orchestrates** and **manages disaster recovery** for Azure VMs, and on-premises VMs and physical servers.
- You can use Azure Site Recovery to replicate on-premises physical or virtual machines running Windows or Linux.
- You can replicate data from your on-premises datacentre to Azure or to a secondary site.
- **For example,** should a virtual machine or service fail in your datacentre, you can use Azure Site Recovery to failover to the replicated resource in either Azure or your secondary site.
- **Orchestration** is built in with Azure Site Recovery, which means that the management of replication, failover, and recovery is included.

[58] - https://www.youtube.com/watch?v=ErYUPsyGazA

4 Configure and Manage a Virtual Network (30-35%)[59]

- **Virtual network (VNet):** Is a communication and security boundary that enables Azure resources (VMs, Storage Accounts, App Services apps, Azure SQL database instances) to communicate with each other securely.
- Each **Subscription** is limited to **a 50 VNets** and can be extended to **100**.
- VNets provides network **isolation** and **segmentation**.
- All VMs within VNet can communicate with each other by default, except any rules you implement using **user-defined routes** and **NSGs**. VMs in different VNets **can't** communicate with each other.
- Azure Provided **DNS** enables VMs within VNets to automatically **resolve** each other names.
- We can do **traffic filtering** using **NSGs** and network virtual appliance **NVA**. An NVA is any VM that performs one of the network functions (such **routing**).
- **Virtual Private Network (VPN):** A **secure** connection over an **unsecure** medium. Azure site-to-site VPNs use **IPsec/IKE** tunnels.
- In Azure VNets, you can **add** an Address space to an existing VNet address space and you can delete one, but you **can't modify** it.
- In VNet connections, VNet-to-VNet or On-prem-to-Azure, Addresses ranges should never **overlap**.

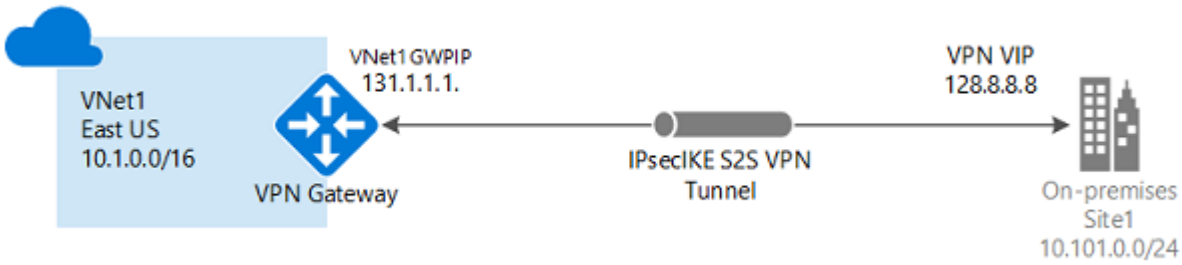


[59] https://app.pluralsight.com/library/courses/microsoft-azure-connecting-virtual-networks/table-of-contents

- **Subnets**
  i. Must be unique address rang within VNet.
  ii. VMs can communicate in and cross subnets.
  iii. Some Azure services create/need their own subnets. Like gateways, they are placed in gateway subnet.
  iv. Understand Default routing behaviour.
  v. Can limit traffics out of Azure service.
  vi. Allow or deny Traffic with NSGs.
  vii. By default, each VNet has outbound internet access (**NAT**).

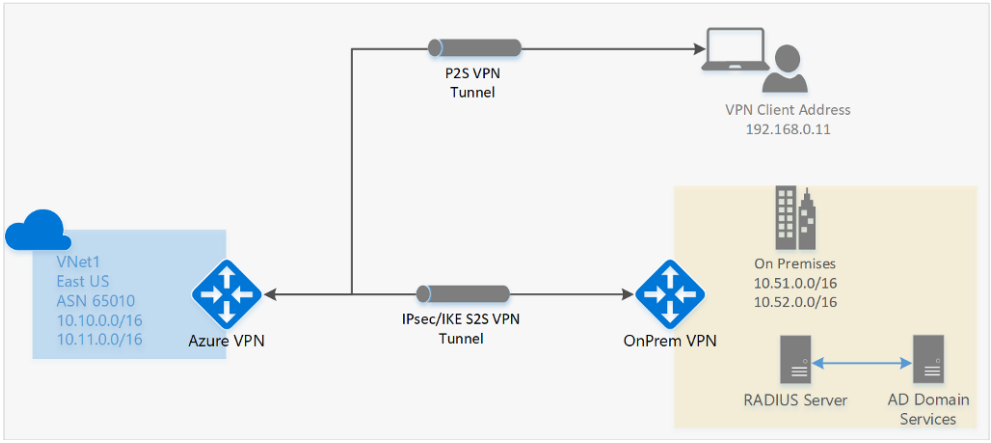
4.1 Create connectivity between Virtual Networks (VNET to VNET)

- Connection Options in Azure:
  i. **Site to Site VPN (S2S VPN):** to connect Azure VNET to the on-premises network, we use VPN gateway, the data is travelling over the internet but the connection is **secure** and **encrypted**, a **VPN device** with a Virtual IP (**VIP**) should be installed on the on-premises side. All the PC's on-premises will use the VIP to communicate with Azure.



  ii. **Point-to-site VPN (P2S VPN):** Used to connect the Azure VPN with individual devices in different locations all over the word, each device has a **VPN client** installed on it.
  The VPN Gateway in Azure is a **Route-based VPN** (this means it has a **routing table** to decide how to route the data to the different connected devices).

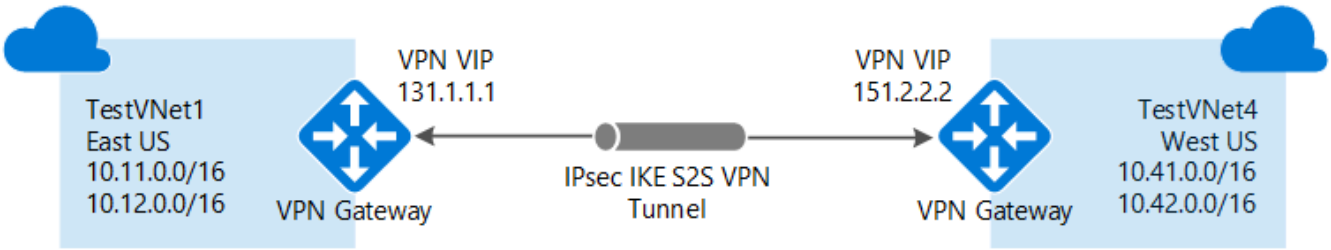
The other type of the VPN Gateway is the **Policy-based VPN** in which it takes the address prefix (X.X.X.X/Y) for the source and the destination and then decide how to route the data to the destination.



iii. **VNET to VNET:** You can connect two VPNs from different location and different subscriptions and **deployed differently** in the Azure cloud**.**

4.1.1 Create and configure VNET to VNET[60]

- You can connect two VPNs from **different location** and **different subscriptions**. And also, have been deployed differently.



- **To create a VPN to VPN connection:**
  - i. Create two VNets and make sure the address space doesn't overlap.

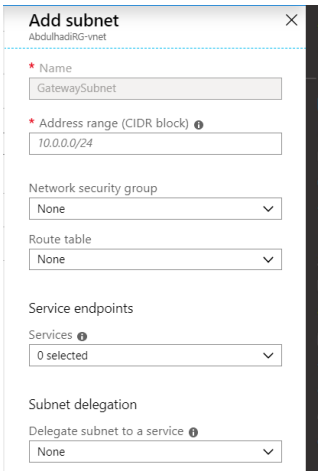
    Create a resource → Virtual networks → +Add

[60] https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal

ii. Create a **Gateway subnet** within the two VNETs, it contains the IP addresses that are used by the VPN Gateway.

VNet→ Subnet → + **Gateway Subnet**

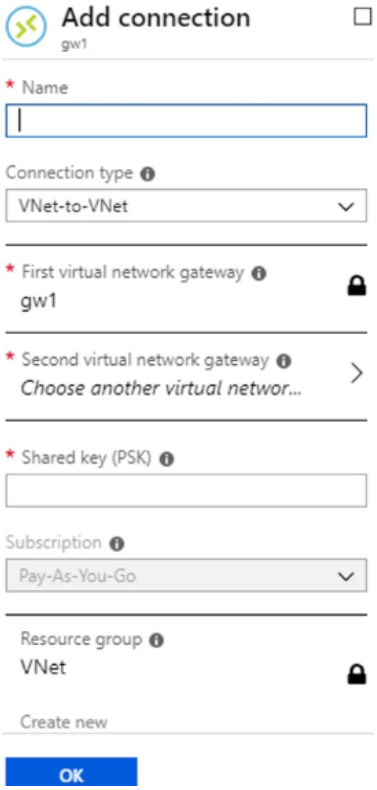
- The name of the Gateway subnet has to be **GatewaySubnet**



iii. Create a **VPN Gateway** and deployed within the Gateway subnet.

Create a resource →Virtual network gateway → + Add

- **Gateway type:**
  a. **VPN:** The traffic in VPN travels over the internet
  b. **ExpressRoute:** The traffic travels over a private network.
- **VPN type:**
  a. **Route Based:** It has a routing table to decide how to route the data to the different connected devices
  b. **Policy-Based:** it takes the address prefix (X.X.X.X/Y) for the source and the destination and then decide how to route the data to the destination.
- **SKU**
- **Public IP address:** we need to attach a PIP address to our VPN Gateway; the **VPN gateway** will only support a **dynamic** IP address.



- Each VNet can have **only** one **VPN gateway**.
- VNet → Connected Devices (you should see her the attached GW)
- At this stage I have 2 VNets, 2 VPN GWs and 2 PIP address, now I can connect the two VNets together:
  i. GW1 → Connections → +Add
  ii. Coneection type :
    - VNet-to-VNet
    - Site-to-Site (IPsex)
    - ExpressRoute

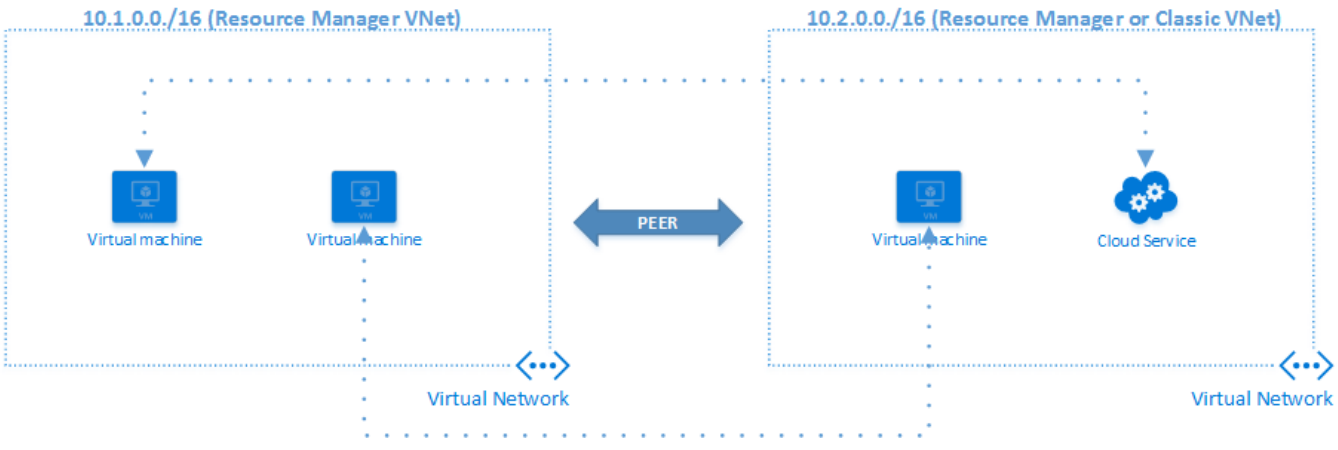
They all require VPN Gateway

iii. **In shared Key (PSK):** Just type the same key for both VNets, this key will also be used for inceyption purboses.

iv. We need to define the connection **individually** for both sides.

4.1.2 Create and configure VNET peering[61]

- Network Peering: A seamless connection between two VNets. **Logically**, the peered networks appear as one, for connectivity purposes.
- It is a way to connect two VNets over the backbone of Azure's network **rather** than creating an **Azure VPN Gateway** between the two.
- Some good points about using VNet peering over a Gateway are:
  i. the cost saving, bandwidth limitations and latency.
  ii. VNet peering also fully supports, NSG (Network Security Groups), NVA (Network Virtual Appliances), UDR (User defined Routes), Internal Load Balancers, and probably more.
- Virtual machines (VM) in the peered VNETs can communicate with each other **directly** by using **private** IP addresses.
- The **Domain name resolution (DNS) does not** flow through the peering relation, which mean that creating a **private Azure DNS zone** is needed.
- VNet peering is an alternative for VNET to VNET because **it doesn't** require to create two **gateways**.



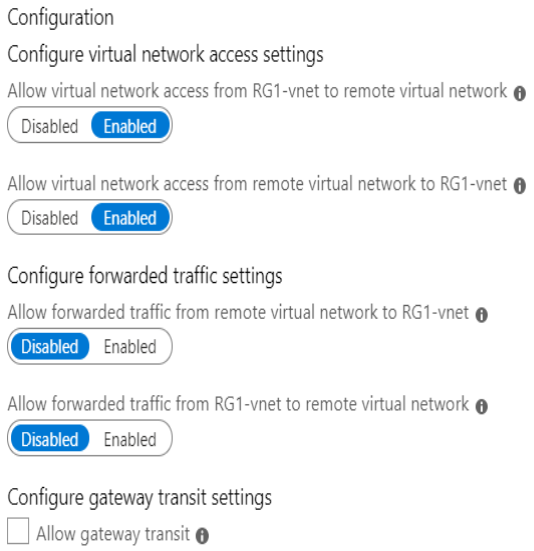
- VNets peering types:

[61] https://pixelrobots.co.uk/2018/07/step-by-step-guide-on-setting-up-azure-vnet-peering/

i. **Global VNet Peering**: In two different locations.

ii. **VNet peering**: In the same region: **VNet peering**.

- Once the connection is established, resources from both sides can communicate with each other with the same **latency** and **bandwidth**.
- In VNet peering, the traffic is kept on the **Microsoft Backbone network**, and there is no used of the public internet.
- You **can't peer** two VNets if they have the **same IP** address range.
- In VNet peering, you pay **per GB**, In VNet to VNet gateway you pay on the **Bandwidth**
- To establish peering:
  i. VNet1 → Peerings → + Add → Virtual Network (VNet2)
  ii. VNet2 → Peerings → + Add → Virtual Network (VNet1)
- Configuration Options:
  i. Configure virtual network access settings
  This is usually used for trouble shooting issue, so you might want to **temporarily** pause the peering relationship.
  ii. Configure **forwarded** traffic settings using scenario: We have 3 VNets, 1 – 2 are peered, 2 -3 are peered. Enable/Disable 1 – 3 to connect in peered relation through 2.
  iii. Configure **gateway transit** settings
  Gateway transit is a peering property that enables one virtual network to utilize the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. **To simplify it**, Enable/Disable other VNet to use my VNet gateway as a **remote** gateway.



- Global VNet Peering is not only across region, is also **across subscription.**

4.1.3 Verify virtual network connectivity[62]

- Many ways to verify your connectivity:

[62] https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal#VerifyConnection

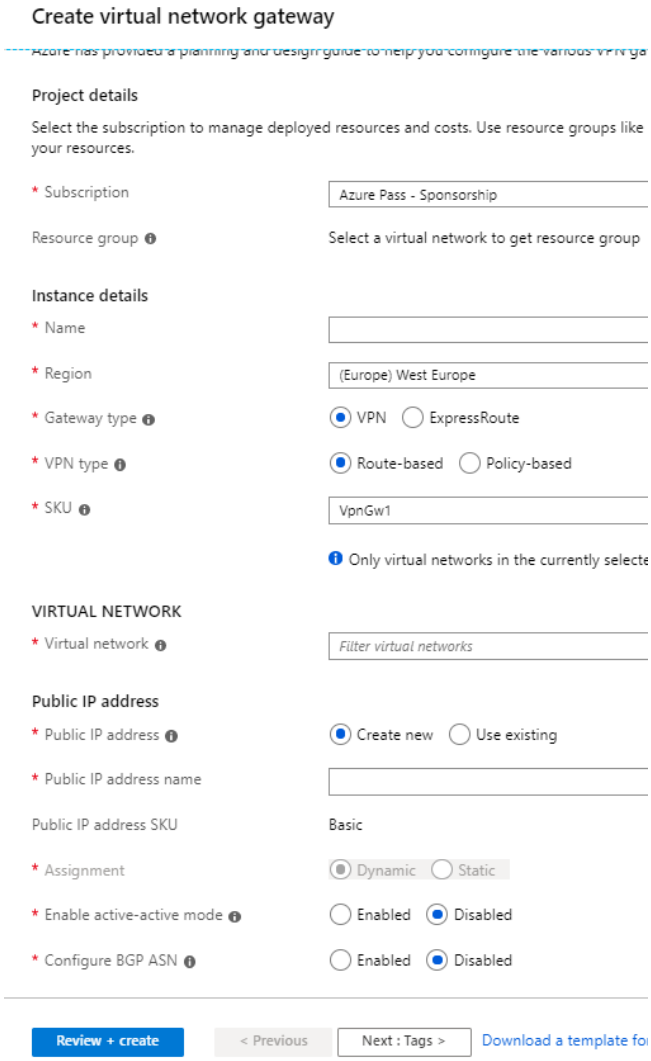
i. Create VM in each VNet and test connectivity using Ping.

ii. VNet to VNet: go to one of the Gateway:

NAME	STATUS	CONNECTION TYPE	PEER	
vnet1tovnet2	Connected	VNet-to-VNet	gw1	...
vnet2tovnet1	Connected	VNet-to-VNet	gw1	...

Gateway → Connections

4.1.4 Create virtual network gateway[63]



iii. Create a resource →Virtual network gateway → + Add

- **Gateway type:**
  a. **VPN:** The traffic in VPN travels over the internet
  b. **ExpressRoute:** The traffic travels over a private network.
- **VPN type:**
  a. **Route Based:** It has a routing table to decide how to route the data to the different connected devices
  b. **Policy-Based:** it takes the address prefix (X.X.X.X/Y) for the source and the destination and then decide how to route the data to the destination.
- **SKU:**
  a. Basic, VpnGw1 ..., VpnGw1AZ…

[63] https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

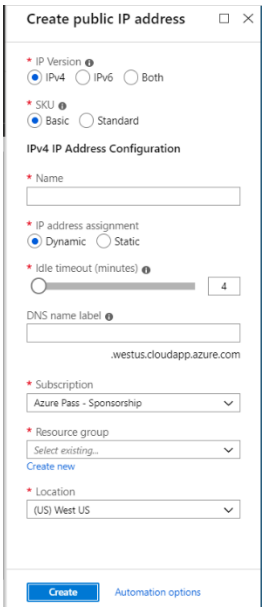
- **Public IP address:** we need to attach a PIP address to our VPN Gateway; the VPN gateway will only support a **dynamic** IP address.

4.2 Implement and manage virtual networking[64]

4.2.1 Configure private and public IP addresses

- **Private IP addresses:**
  i. Used for communication within an Azure VNet, it can be used also for connecting the on-prem network whenever you have a **VPN gateway** or **ExpressRoute**.
  ii. It can associate to:
    - NICs
    - Internal Load Balancer ILB
    - Application Gateway
  iii. Azure reserve the **first 4 addresses** and the **last one** in each subnet
  iv. Two types of Private IP:
    - **Dynamic**: Azure assign the **next** unallocated private IP address to resource Private IP.
    - **Static**: Static addresses are only releases if only the VNet is **deleted**

- **Public IP addresses**
  i. Used to communicate with the **Internet**
  ii. A separate instance/service. It can assign to: NICs, LB, VPN Gateway, Application Gateway.
  iii. When choose **Both** in the Public IP creation blade, Two IP addresses will be created: one IPv4 address and one IPv6 address.
  iv. Azure resources can still communicate outbound without the Public IP, and then azure will assign a dynamic IP address to the resource.



[64] https://docs.microsoft.com/en-us/azure/networking/networking-overview

v. The **SKU** (pricing) of the Public IP must **match** the SKU of the **load balancer**. Basic/**Standard**.

	Standard SKU	Basic SKU
Availability Zones	In Standard SKU, zone-redundant and zonal frontends for inbound and outbound, outbound flows mappings survive zone failure, cross-zone load balancing.	Not available.
SLA	99.99% for data path with two healthy virtual machines.	Not applicable.
Pricing	Charged based on number of rules, data processed inbound and outbound associated with resource.	No charge.

- Public IP types:
    - **Dynamic**: IP address will be **released** after **stop** using the resource and we refer to the IP by using its name.
    - **Static**: PIP will not change and used for specific situation, such as
    a. **DNS** name resolution
    b. IP address-based **security** model
    c. SSL **certificate** linked to an IP address
    d. **Firewall** rules that allow and deny IP addresses
    e. **Role-based VMs** such as Domain Controllers

4.2.2 Configure network routes:

- Route Table is a **standalone** resource.
- Azure uses System route to direct network traffic between **VMs**, **On-prem networks** and the **Internet**.
- A Rout table contains a set of **rules** (IP addresses ranges) called **route** that specified how a packet should be routed in a VNet.
- Using cases:
    i. Traffic between VMs in the same/different subnet
    ii. Traffic from the VM to the Internet
    iii. Traffic between VMs in VNet to VNet, Site to Site and ExpressRoute.
- Routes are stored in a **Route table** which is associated to a **subnet** or a **NIC** and each packet leaving a subnet is handled based on the Route table.
- By **default**, Azure manage all the traffics, but you can create **User-defined routes (UDRs)** by specifying the next hope of the traffic flow.
- **UDRs** controls network traffic by defining route that specifying the next hope of the traffic flow.

- Each **route table** can be associated **to multiple subnets**, but a subnet can only be associated to one route table (**as NSG**).
- When **outbound** traffic is sent from a subnet, azure select a route depending on the destination IP address using the **longest prefix match algorithm**.
- Example:

Address prefix	Next hop type
10.0.3.0/24	Virtual Network gateway
10.0.3.0/16	Internet
0.0.0.0/0	Internet

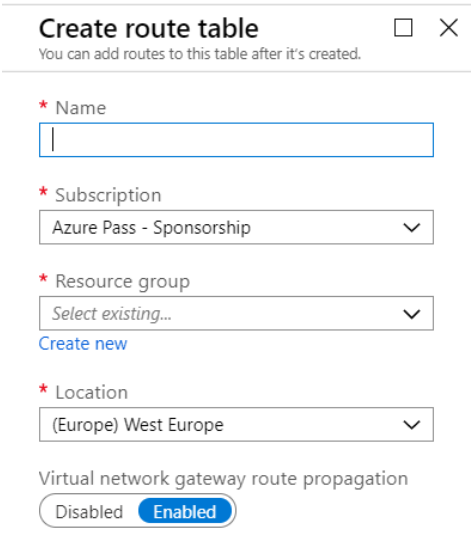
10.0.3.5 → Virtual Network Gateway.

- The **prefix length** is the number of bits set in the subnet mask; for instance, if the subnet mask is 255.255.255.0, there are 24 in the binary version of the subnet mask, so the prefix length is 24 bits.
- If multiple route contains the same address prefix, Azure select the route type based on the following priorities:
  i. User-defined route (UDR)
  ii. BGP route
  iii. System Route
- **Create a Route Table**:

  Azure resource → Route tables → +Add

  Building the Routes

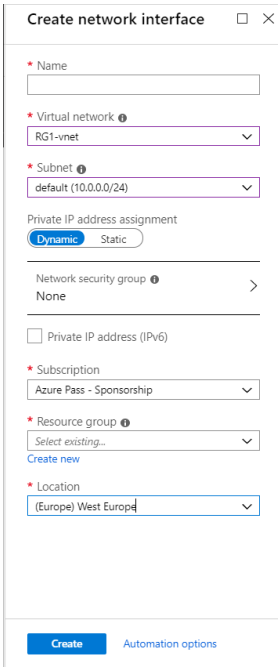
  Route table → Routes (to add routes)



Associate Route table to a Subnet

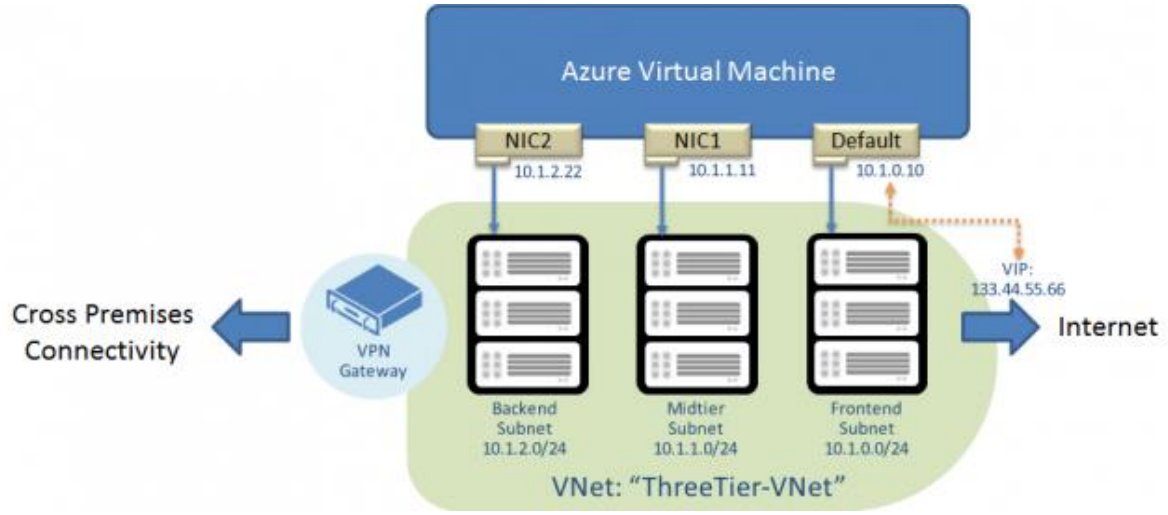
VNet→ Subnets → (Default) → Route table

- In the Route table blade, distinguish between Address **prefix** (X.X.X.X/Y) and Next hope **address** (X.X.X.X)



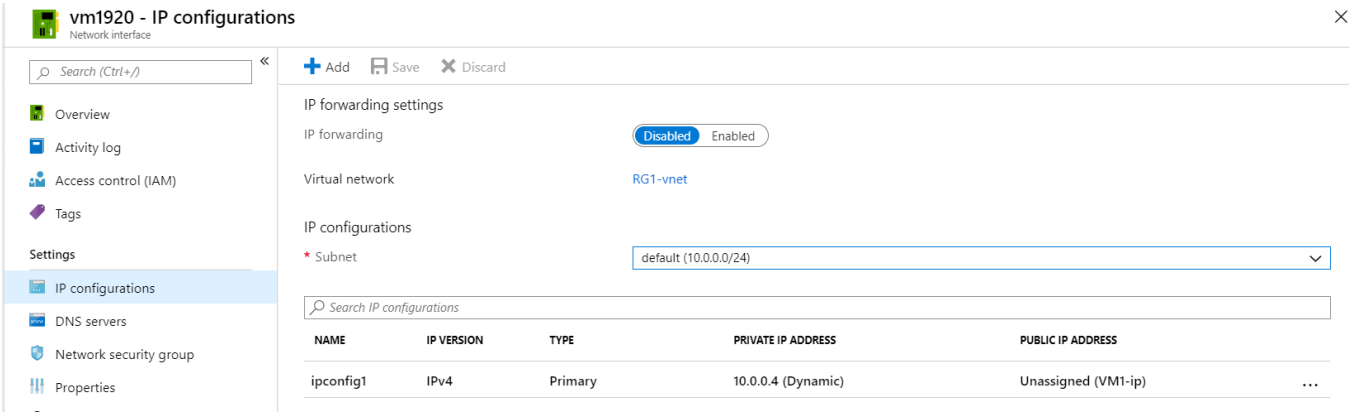
4.2.3 Network interface (NIC)

- **NIC** is a standalone resource.
- Some VMs (Depends on the size) can have a **multiple** NICs, but each NIC should be associated to **one VM**.
- NIC can have:
  i. 1 Private IP Static or Dynamic
  ii. 1 Public IP Static or Dynamic
  iii. 1 LB VIP Static or Dynamic



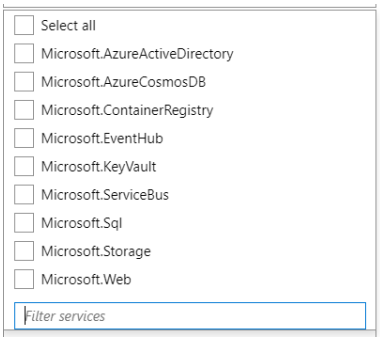
- The **public IP** is connected to NIC which in turn connected to the VM.
- Most of the operations regarding NIC require the VM to be **Restarted**.
- **NIC** allows Azure virtual machines to communicates with Internet, Azure or on-prem resources.
- We can change the Subnet for a NIC, and also the DNS servers for the NIC.

- **NSG** can be attached either to a **Subnet** or to **NIC**.

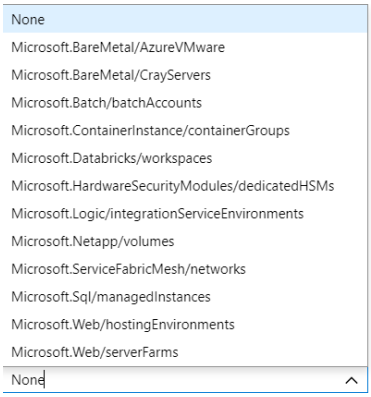


4.2.4 Configure Subnets

- VNet → Subnets → + Subnet
- The address range (CIDR block) must be contained within the address range of the VNet.
- NSG & Route table can be associated to either Subnet or NIC, as best practice its preferred to associate them to the Subnet.
- **Service endpoints:**
  - i. A subnet can have **zero** service endpoint or **Multiple** service endpoints.
  - ii. For example: if I chose Microsoft.storage as service endpoint, then I can control and restrict the access to the **storage to be only within** this subnet.
  - iii. It's a way to secure access to your azure services and limited only to a specific subnet within a VNet.

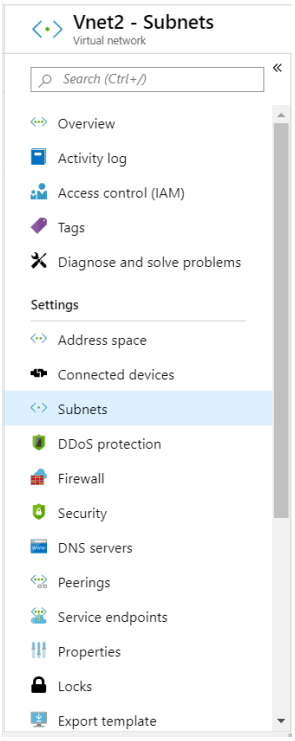


- **Subnet Delegation**:
  - i. A subnet can have **zero** or **one** delegation enabled for it.
  - ii. It gives **explicit permission** to Azure services to create service-specific resources in the subnet by using some unique identifiers.



iii. For example: if I want to use this subnet only to deploy containers group, then I will select **containerGroups**. By doing this, none of the other Azure service will be allowed to be deployed within this particular subnet and only the containerGroups can be deployed.

4.2.5 Configure Virtual Network



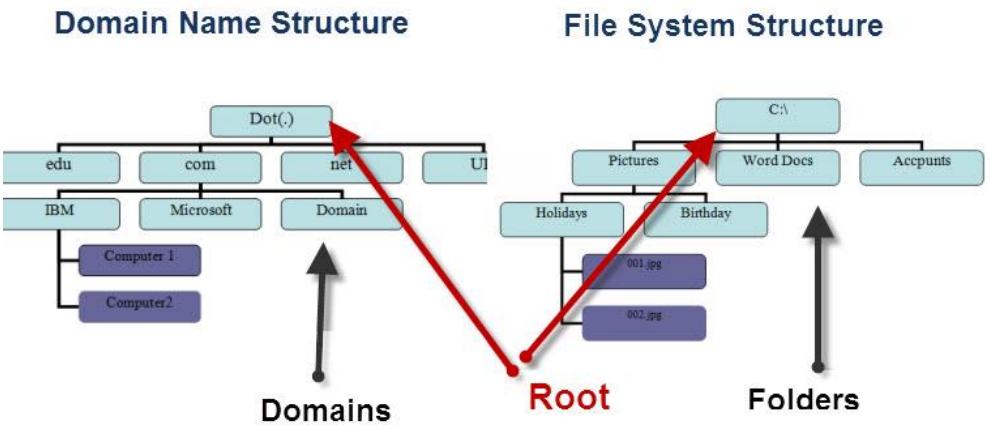
- From VNet blade: Address space, Connected device …
- DDoS protection: **Basic** and **Standard**
  i. **Basic**: Automatically enabled, traffic monitoring and real time protection of common network attacks
  ii. **Standard**: Real time telemetry, rich attack mitigation analytic.
- **Firewall**: **Expensive**.
  i. It's a managed cloud base Network security service that protect your Azure VNet service.
  ii. It uses a **static** public IP address for you VNet resources that allows outside firewalls to identify traffic generated from your VNet.
  iii. Fully integrated with Azure monitoring for logging and analytics.
  iv. Will located on an **induvial** Subnet called **AzureFirewallSubnet**
- **NSG Vs Firewall:**
  i. Azure Firewall service compliment NSG functionality**.**
  ii. NSG provide distributed Network layer traffic filtering to limit traffic to resources within the VNet whereas Azure firewall provide **both** network and application level protection across VNet.
- **DNS servers:**
  i. By default, you can use an Azure provided DNS server, or you can specify your own.
  ii. DNS server is used to **resolve** names within the VNet.
  iii. Connecting VNet to other VNet, using VNet peering or VNet to VNet, require using of **Custom DNS server.** And also, this is needed when connection Azure to on-prem network, **either** by site to site or ExpressRout.

4.3 Configure name resolution

- **Name Resolution on VNet**
  i. Azure creates name resolution automatically to all VMs within a VNet.
  ii. It does not work outside the VNet or in peering's.
  iii. For that you need Azure DNS or a custom server.
- **Azure DNS**
  i. Manage DNS seamlessly with your Azure services.
  ii. Globally distributed architecture, resilient to multiple region failure.
  iii. Fast global DNS name resolution.
  iv. **99.99%** Availability **SLA** for all common DNS record types.

4.3.1 Understanding DNSs[65]

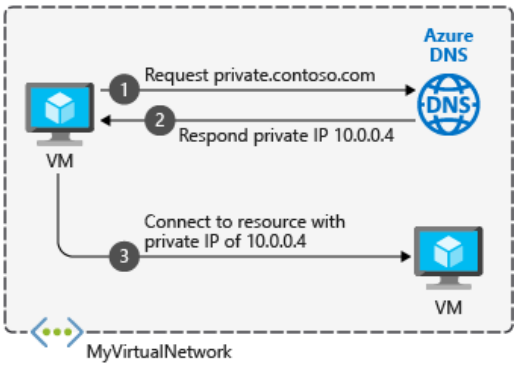
- **DNS** (Domain Name System) is one of the most important technologies/services on the internet, as without it the Internet would be very difficult to use.
- DNS provides a **name to number** (IP address) **mapping or translation**, allowing internet users to use, easy to remember names, and not numbers to access resources on a network and the Internet.
- Domain Names Structure **Vs** File System Structure



[65] http://www.steves-internet-guide.com/dns-guide-beginners/

4.3.2 Configure Azure DNS[66]

- **Azure Private DNS zone**



  i. A Private DNS zone provides name resolution services **within** virtual networks.

  ii. A Private DNS zone is accessible **only** from the virtual networks that it is linked to and **can't be** accessed over internet. For example, you can create a Private DNS zone named **contoso.com** and then create DNS **records** like **www.contoso.com** in this zone. You can then link the zone to a one or more virtual networks.

  iii. The private DNS zone provides **secure and reliable** name resolution for VNets in Azure.

  iv. Private DNS zones **prevent** the need to setup and manage **custom DNS servers**. Some of the advantages of using Private DNS zones are:

    - They provide name resolution both within a VNet and across VNets.
    - The Private DNS zones can **cross** different regions and subscriptions.

  v. Two main concepts in the DNS zones:

    - **Resolution Virtual Networks**: the **list** of the VNets that are allowed to **resolve records** the DNS zone.
    - **Registration Virtual Networks**: in which Azure DNS maintains host name records whenever adding/deleting a VM, automatically, the DNS record will be added to the DNS zone.

- **In PowerShell:**

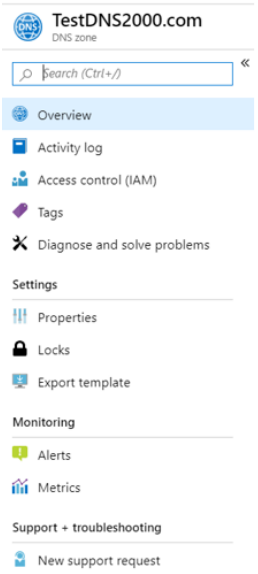
```
New-AzResourceGroup -Name dnsgroup -Location westeurope

New-AzDnsZone -name theazureguy.ca -ResourceGroupName dnsgroup

New-AzDnsRecordSet -name www -RecordType A -ZoneName theazureguy.ca -
ResourceGroupName

dnsgroup -Ttl 3600 -DnsRecords (New-AzDnsRecordConfig -
Ipv4Address "40.86.225.89")
```

[66] https://docs.microsoft.com/en-us/azure/dns/dns-getstarted-portal

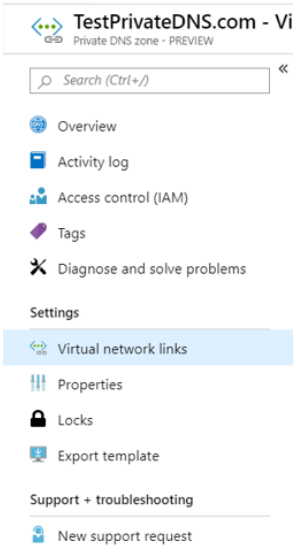
```
Get-AzDnsRecordSet -ZoneName theazureguy.ca -ResourceGroupName dnsgroup
```

- In Azure Portal we have **two** different DNS services, DNS zone and Private DNS zone
- **DNS zone**: A DNS zone is used to host the DNS records for a particular domain. **For example**, the domain 'contoso.com' may contain a number of DNS **records** such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create.

DNS zone



Private DNS zone



-

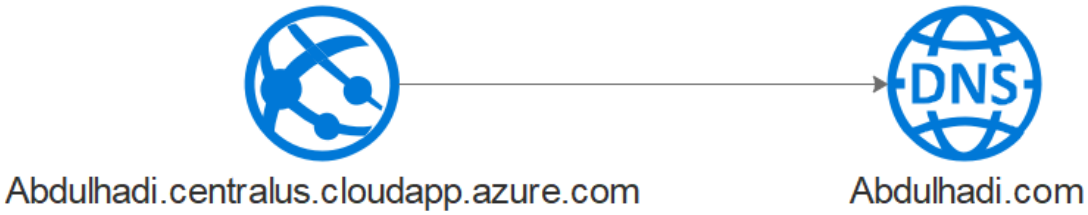
4.3.3 Configure private and public DNS zones[67]

- **Public DNS** is what most people are familiar with. They are generally provided to your business by your **ISP**. A public DNS maintains a record of publicly available domain names reachable from any device with internet access.
  VM → Overview → DNS name: Configure
- **Private DNS** resides behind a company **firewall** and maintains **records** of internal sites. Employees of the company use the private DNS to access internal sites and services without having to remember IP addresses.
  Home → DNS zones → +Add

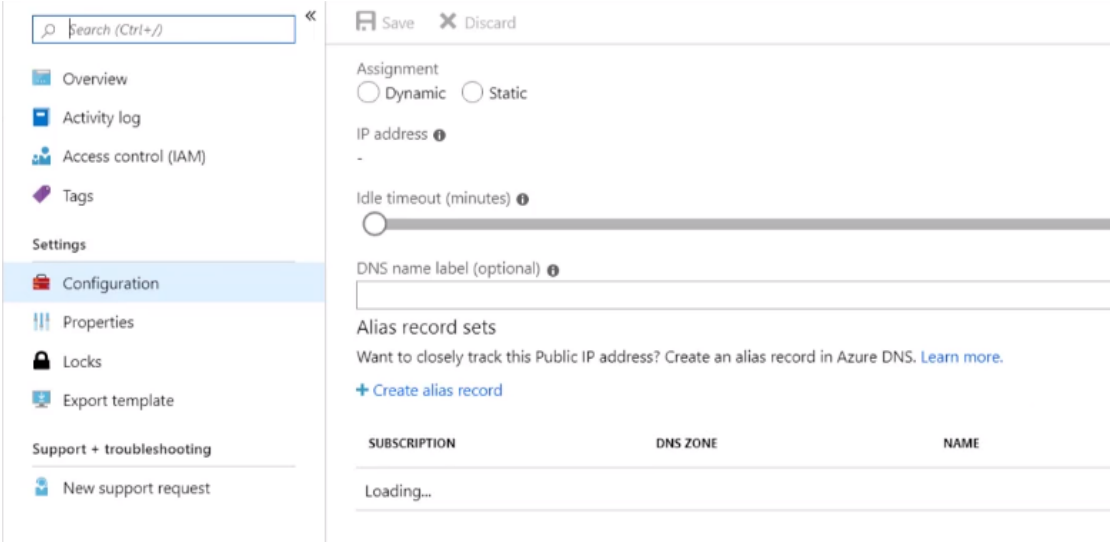
[67] https://docs.microsoft.com/en-us/azure/dns/dns-zones-records

4.3.4 Configure custom DNS settings

- **A small scenario**:
  i. You have a web application that have the domain name: **Abdulhadi.centralus.cloudapp.azure.com.** this is a very long name to be used by the end user.
  ii. You want the end user to enter only **Abdulhadi.com**
  iii. You can achieve that by using the Azure DNS.



- **Create DNS server**:
  i. Create **DNS** zone
  ii. Copy the **nameservers** for the DNS zone to our domain register
  iii. Create a resource **record** to ensure the main domain name in linked to a public IP address of the server.
- **Create and test a DNS service**
  i. Create VM with IIS, we can see the IIS through the Public IP address.
  ii. The goal is to define a DNS for our VM.
  iii. VM → Overview → DNS name: Configure →



iv. By adding a DNS name lable, the name will be located with the Azure domain: Abdulhadi.centralus.cloudapp.azure.com. so, users her can use this link to connect our VM, but still this is relatively a long name.

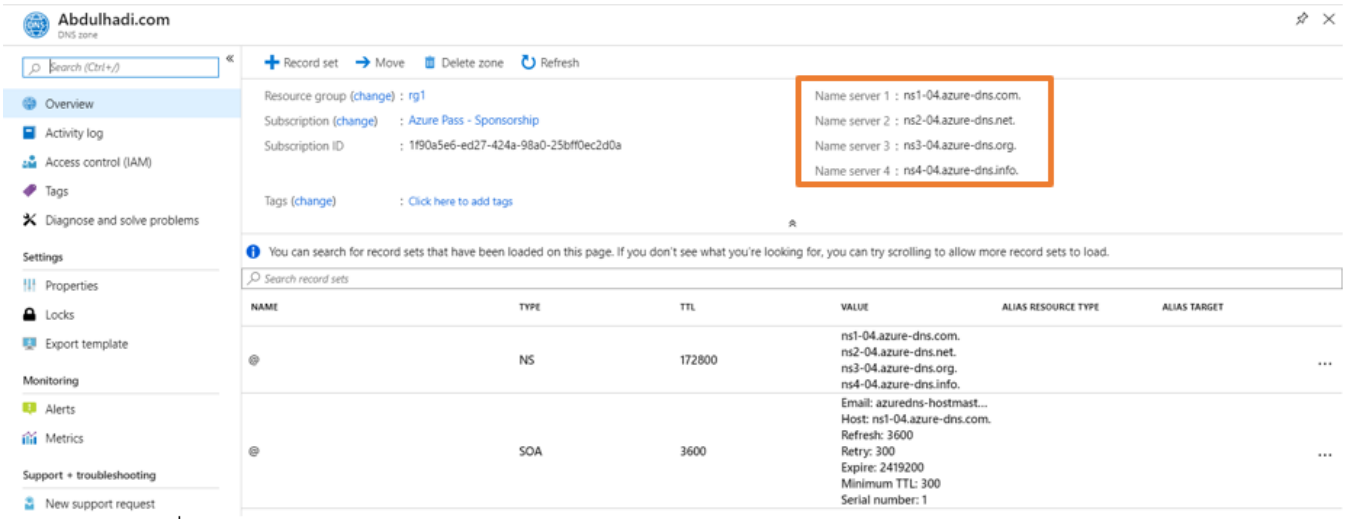
v. Instead you can great your **own DNS name** using **Azure DNS service**.

1- Create DNS zone

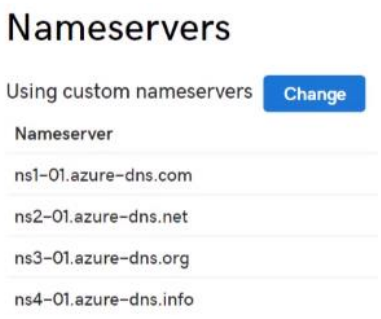
i. Home → DNS zones → +Add

ii. The domain name should be bought from a third party to be used here. We insert the domain name in the **Instance Details**: Name. For Example:

Abdulhadi.com: this will be our DNS zone, by doing this we created a DNS zone that map our domain.



2- **Copy the nameservers for the DNS zone to our domain Register**



   i. DNS zone → Abdulhadi.com → overview → Getting the name servers

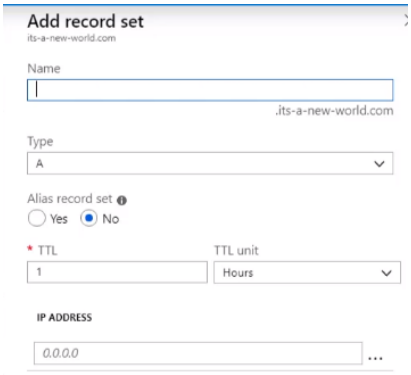
   ii. Mapping the DNS zone in Azure to our reserved domain, each domain name providers has a list of **nameservers**, which need to be changed to match our Azure DNS zone nameservers.

3- **Create a resource record**

   i. DNS zone (Abdulhadi.com) → Overview → + **Record set**

   To ensure that whenever the users are contacting Abdulhadi.com, they are **redirected** to IIS homepage of our VM.

   ii. Insert the Public IP address for the VM in the IP address field of the Add record blade.



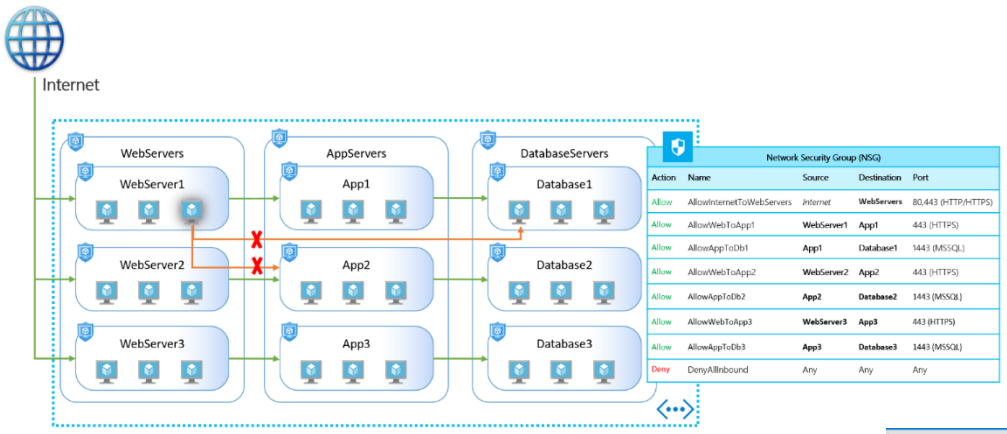
4.4 Create and configure a Network Security Group (NSG)

4.4.1 Application Security Group (ASG)[68]

- We need to **distinguish** between the Network Security Group (**NSG**) and the Application Security Group (**ASG**)
- **ASG** allows for logically grouping for VMs in the VNet and apply network security group rules to them.
- **ASGs** enable you to define fine-grained network security policies based on workloads, centralized on applications, instead of explicit IP addresses.

[68] https://azure.microsoft.com/en-us/blog/applicationsecuritygroups/

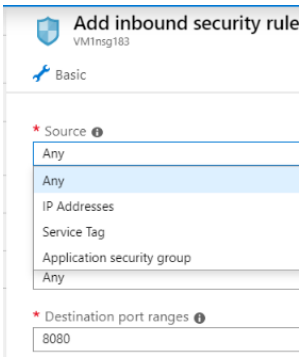
- This feature provides security micro-segmentation for your virtual networks in Azure.

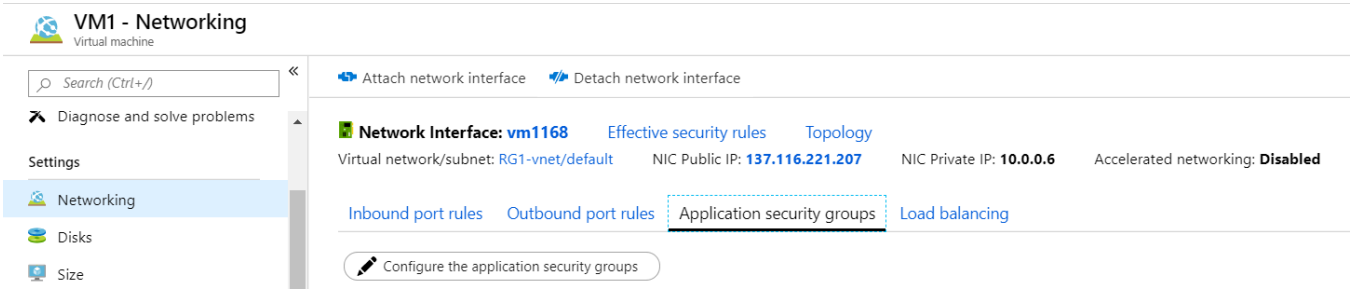


Home → Application Security group → Create

- To associate the ASG to an NSG: when creating a rule: In both Source and Destination you can choose the application security group.
- To associate the ASG to a specific VM:

  VM → Networking → Application Security Group

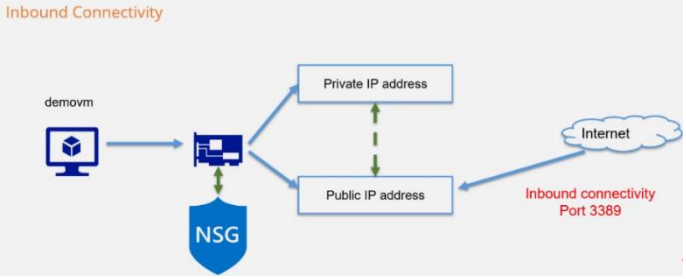




4.4.2 Create security rules

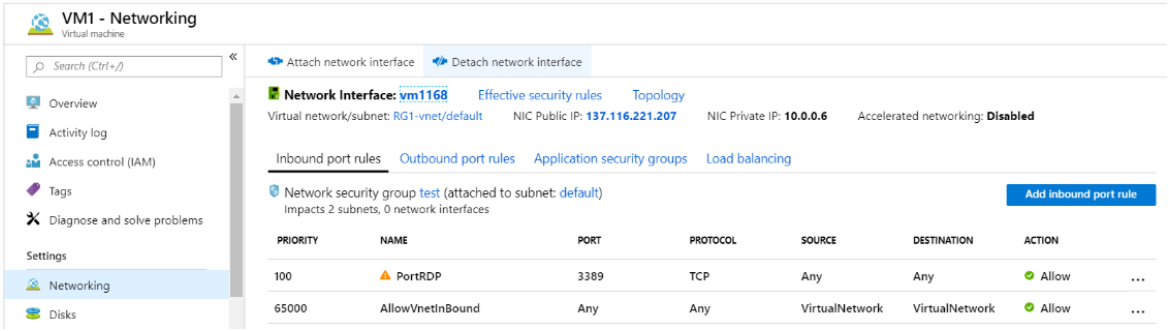
- **NSG** is the main tool to enforce and control network traffic rules at the network level.
- **NSG** is a standalone resource, which can be configured during the VM creation or separately and then associated to the specific NIC or a Subnet
- If we create the NSG during VM creation, it will be then automatically associated to the **NIC**. You can later associate an NSG to the subnet.
- NSG is essential for VM connectivity.
- Used to control traffic into subnets or virtual machines.
- Consist of rules for Inbound and Outbound traffic.

- By default, the NSG will be created automatically with the VM and associated to the NIC.
- The allowed ports (HTTP, HTTP, SSL, RDP) during the creation of the VN are Inbound security Rules.
- The change in the NSG's rules have an immediate effect.
- In VNet, traffic is allowed automatically, but you need to explicitly allow traffic from the internet.

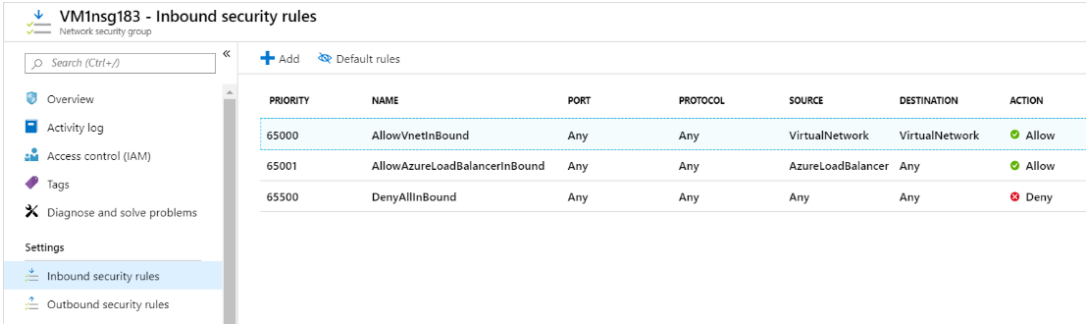


- We can assign the NSG to either NIC or Subnet
- When associating the **NSG** to a **subnet** then the rules are applied to all the VMs and NICs in the **subnet**. Application Security Group (**ASG**): allow you to **logically** group a number of VMs in the same **VNet** and apply on them a NSG rules.
- (HTTP: **80**, HTTPS: **443**, RDP:**3389**)
- ASG is a standalone service, which can be created first and then associate the VMs to it.
- To create Rules:

  VM → Networking →Add inbound port rule



Azure → Network security group → Inbound Security rules /Outbound security rules



- You can't delete the three default rules, but you create a new rule with a lower priority.

4.4.3 associate NSG to a subnet or network interface

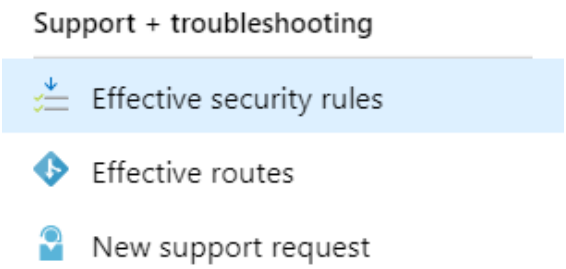
- VNet → Subnets → Network Security group →
- NSG → Network Interfaces / Subnets → + Associate
- NIC →Network Security group → Edit

4.4.4 identify required ports

- **HTTP:** 80**, HTTPS:** 443**, RDP:**3389**, SSH:**22

4.4.5 evaluate effective security rules

- Select a network interface to see the effective security rules and network security groups associated with it.
- VM → Networking → Effective security rules
- NIC → Effective security rules

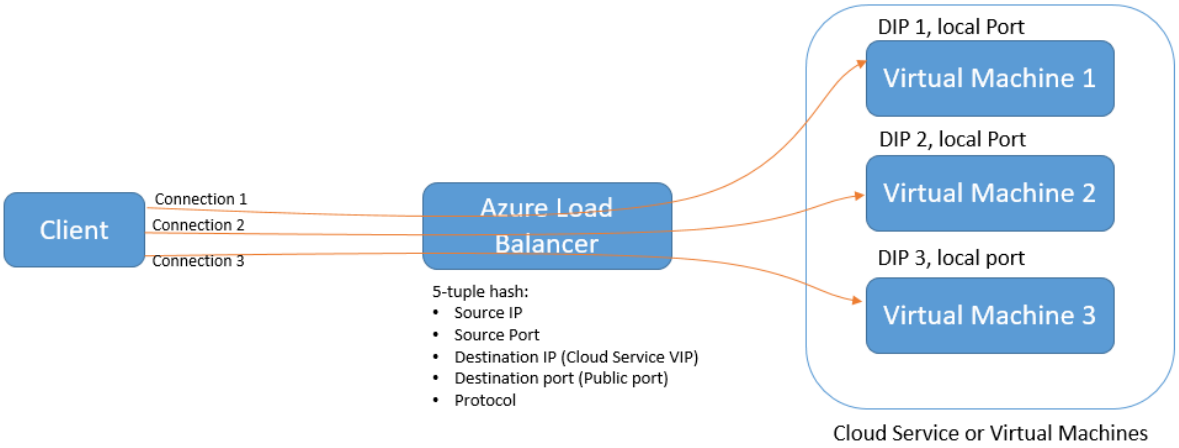


4.5 Implement Azure load balancer

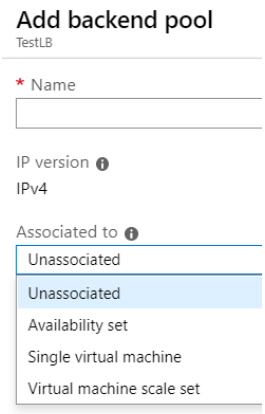
4.5.1 General Understanding

- LB provide **high availability**, fully managed service by azure and distribute traffic to the Backend VMs.
- It's called also **Layer 4 Load Balance**. Where Application gateway is **Layer 7** load balancer.
- LB ensure an **equal** distribution of the requests from the users to the backend VMs.
- **Health Probe** is used to determine whether the VM at the Backend of the LB is healthy or not. An example for that is the Heart Beat which can be: Protocol **TCP**, **Port** number or **Interval** for the health probe.
- LB SKUs**: Basic and Standard.**
- The Backend pool could be a **single VM**, **VMs scale set** or **Availability set**, and in the **standard** LB the backend pool can be also multiple VMs or combination of the aforementioned options.
- **Session Persistence**: the request from the same client (IP or IP and protocol) can be directed to the same backend VMs.

- **NAT** (Net address Translation) **forwarding Rules**: allow you to remotely connect to the backend VMs.
- The public IPs for the VMs in the backend should have the **same type** as the load balancer: **Basic** or **standard**.



- Load Balancer make decisions depending on **5** factors: Source/ Destination IP/Port and Protocol.
- Load Balancer support **IP V6**.
- The backbone recourses (VMs, Availability set, scale set) must exist in **the same region** as the LB.
- There are two typed of LB:
  i. **Internal Load Balancer**: Only balance traffic inside resources in a VNet.
  ii. **Public Load Balancer**: This can be used to load balance internet traffic to VMs.
- We can Add a public IP addresses to the LB **frontend IP**. And then we can create specific LB rules for each Frontend IP address.



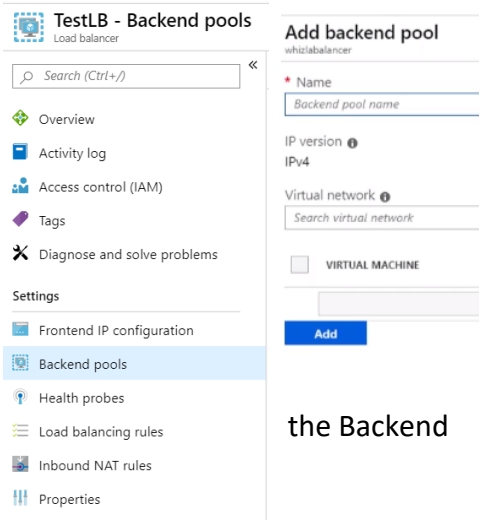
4.5.2 Configure internal load balancer[69]

1. Create a virtual network with a subnet
2. Create VMs
3. Create a **Basic** load balancer
   a. Azure resources → Load Balancer → create
   b. Type: **internal**
   c. We don't have to choose a Public IP address, since this is an Internal LB.

[69] https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-basic-internal-portal

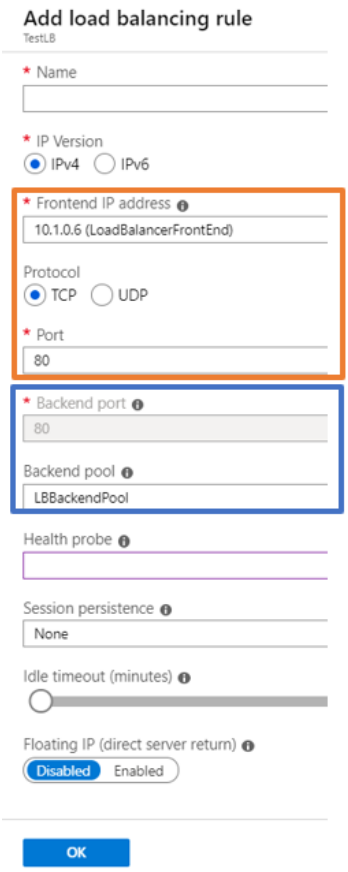
d. If I choose IP address assignment: **static** then the Private IP **address**: Type an address that is in the address space of your virtual network and subnet

4. Create Basic load balancer Setting:
    a. LB → Backend pools → +Add
    b. Backend pools → + Add
    c. Health Probe → + Add



4.5.3 Configure load balancing rules

- A probe health must exist before creating a rule.
- This determine how the request will flow from the LB to the Backend VMs
- LB → Load Backend rules → +Add
- You can read this blade like this:
    i. When ever a request in coming to the Frontend IP address of the LB on the specific Protocole (TCP) and Port (80)
    ii. Then they should be directed to the Backend port (80) and Backend pool (LBBackendPool)
    iii. Then we have the health Probe and we can enable the session persistence.



4.5.4 Configure public load balancer

- This can be used to load balance internet traffic to VMs.
- In the type: Public and we need to specify the Public IP address
- **Public IP address name**: we need to use an unused PIP or create new, because after creating LB the requests will come to the LB instead of the VMs on the Backend pool.

4.5.5 Configure Frontend IP

- By default, the Frontend IP address for the LB is the same as the specified Public IP address or the Private IP address which was configured during the creation stage.
- Frontend IP is the Public IP (if it's a Public LB) or the Private IP (if It's a private LB)

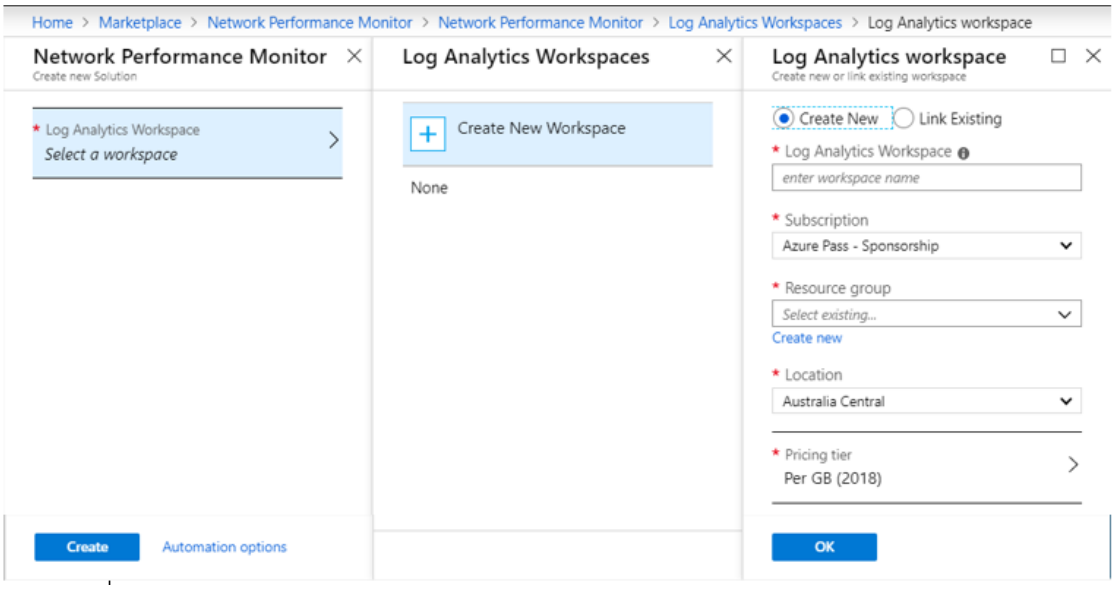
- We can Add a **second** public IP addresses to the LB frontend IP. And then we can create **specific LB rules** for each Frontend IP address. All these rules could be affecting the same Backend Pool.

4.6 Monitor and troubleshoot virtual networking

- Azure Monitor lets you collect data from multiple sources, including Azure and on-premises resources.
- Behind the scenes, Log Analytics performs log collection and searching, which is now part of Azure Monitor along with Application Insight, Azure Advisor, and other services.

4.6.1 Monitor on-premises connectivity

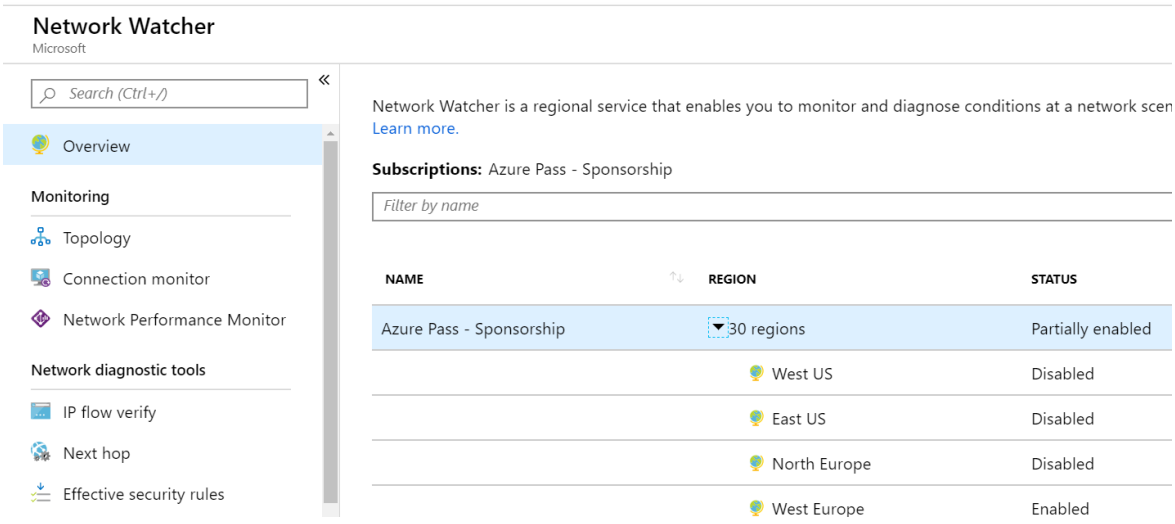
- **Network Performance Monitor (NPM)**[70]
  i. **NPM** is a cloud-based monitoring solution allows you to monitor various parts of the network infrastructure.
  ii. **NPM** allows you to monitor Service-endpoints, Application-endpoints and the performance of ExpressRoute.
  iii. **NPM** includes **on-promises monitoring.**
  iv. The on-prem monitoring requires **Microsoft Monitoring Agent** installing on the on-prem devices.
  v. **NPM** is a part of **Operation Management Suite (OMS)** and it require an **OMS workspace.**
- Home → Marketplace → Network Performance Monitor →Create



[70] https://channel9.msdn.com/Series/Operations-Management--Security/Network-Performance-Monitor-Deep-Dive

4.6.2 Network Watcher:

- https://courses.skylinesacademy.com/courses/az-100/lectures/10091102
- This service provides tools that can be used to monitor and diagnose network connectivity.
- It's also used to **enable/disable logs** for resources in Azure VNet.
- To use monitor Watcher, we need to install the **Network watcher agent** in the machines that will be connected to be watched.
- To install this agent in the VM, from the **Extensions** on the left side of the **VM** blade, search for **Network Watcher Extension**.
- Also, before using the Network watcher, we **need to enable it** for the particular region.

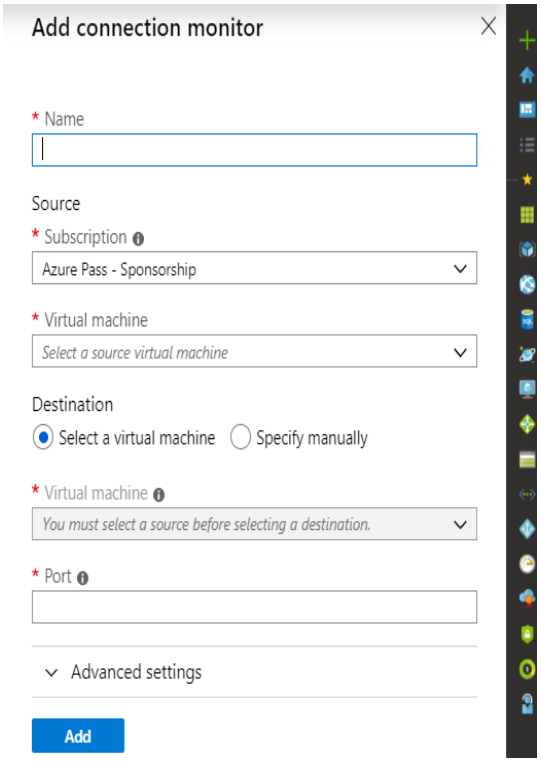


- The most important tools in the Network watcher are:

1. **Connection Monitor**: **Continuous** Checking
    i. To check the connectivity between two endpoints.
    ii. The **source** endpoint is a VM in Azure
    iii. The **destination** endpoint is: VM, URI, IP address or FQDN (Fully Qualified Domain Name). We use the **Port** number.
2. **Connection Troubleshoot**: **Instance** Checking
    i. The same as Connection Monitoring, but it can be only defined from **one side**.
3. **IP flow Verify**:
    i. Check if **Packets** are allowed or denied to/form **VM**, usually to check **security rules (NSG).**
    ii. You can her mention the Local/Remote IP address/Port

4. **Next Hop**:
    i. What is the next hop to a destination IP?
5. **Packet Capture**:
    i. Capture the **detailed** network placket that are send/received from **VM**.

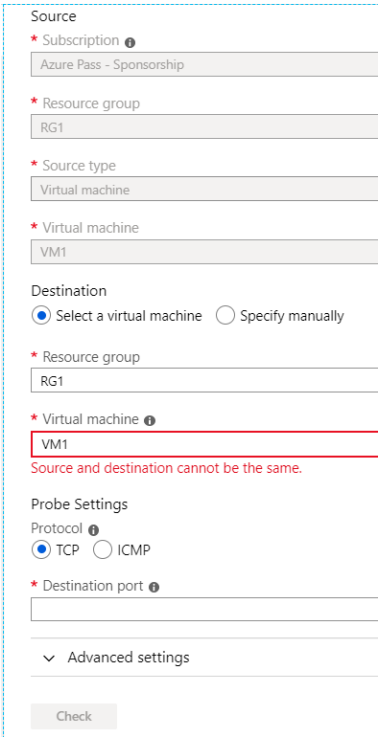
4.6.3 Monitoring tools in Portal



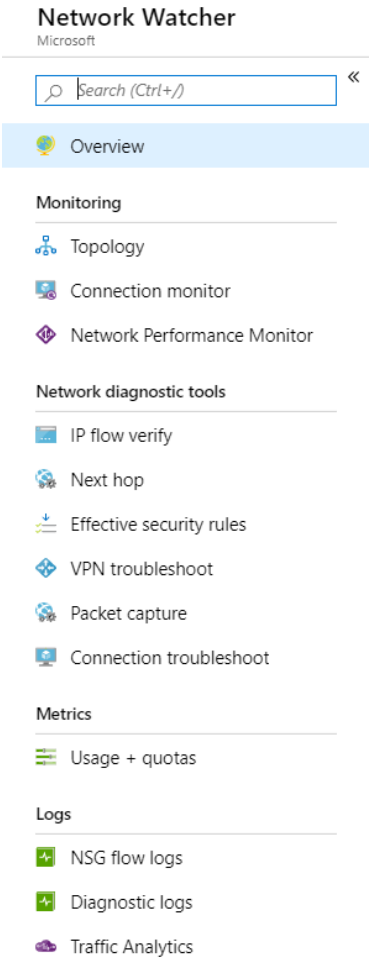
1- Within the VM, we have two tools
    i. Connection Monitor
    ii. Connection troubleshoots

- **Connection Monitor**
    i. It provides a **continuous** connectivity troubleshooting at particular intervals between a source VM and a destination VM.
    ii. The **default** Probing interval is **60 seconds**
    iii. Network Watcher Connection Monitor enables you to configure and track connection reachability, latency, and network topology changes.
    iv. If there is an issue, it tells you why it occurred and how to fix it.
    v. It will check the connection between a source machine and a destination machine.
    vi. VM → Connection monitor → + Add.
    vii. We can choose a different VM as **source** VM than the one we are doing the creation within it.
    viii. In the destination , you can select a VM or specify mannualy (URI, FQDN or IPv4)

ix. For the port: we choose the port that is being used by the service inside the destination VM, for example, if I have IIS working on my desination VM, I will choose then the port 80.



- **Connection troubleshoots**
  - i. It provides **Instance** connectivity troubleshooting between a source VM and a destination VM.
  - ii. Network Watcher Connection Troubleshoot provides the capability to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IPv4 address.
  - iii. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Check".
  - **iv. VM→ Connection troubleshoots**
  - v. The source type and VM can't be changed, the source is the VM that we check the connection from it.



2- For other tools, we need to go to the Network watcher it itself:
   - Azure services → Network watcher
   - **IP flow verify:**
     - i. Network Watcher **IP flow verify** checks if a packet is allowed or denied to or from a virtual machine based on 5-tuple information.
     - ii. The **5-tuple** of the flow (source IP address, source port, IP transport protocol, destination IP address, destination port) must be unique.
     - iii. The **NSG** decision and the name of the rule that denied the packet is returned.
     - iv. Specify a target virtual machine with associated network security groups, then run an inbound or

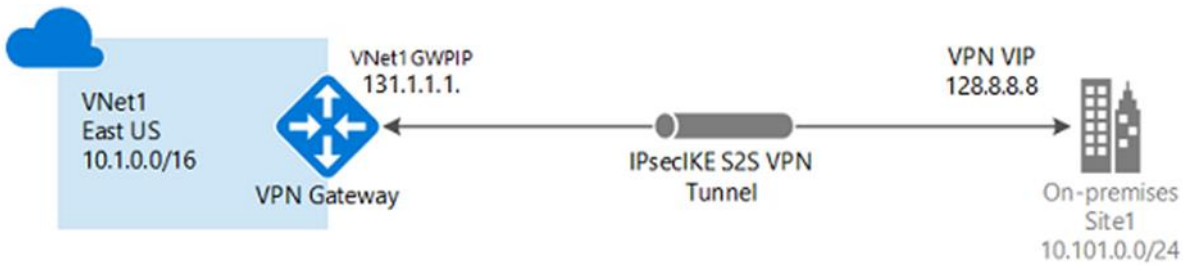
outbound packet to see if access is allowed or denied.

- **Next Hop**
  i. Provides the next hop from the target virtual machine to the destination IP address.
  ii. Specify a target virtual machine and destination IP address to view the next hop.
- **Packet Capture**:
  i. Allows you to capture all the packet that are moving to/from a VM
  ii. It's used when you need more details over the moving packets
  iii. The packet capture output file **(.cap)** can be stored in a storage account and/or on the target VM.

4.7 Integrate on premises network with Azure virtual network[71]

4.7.1 Hybrid cloud

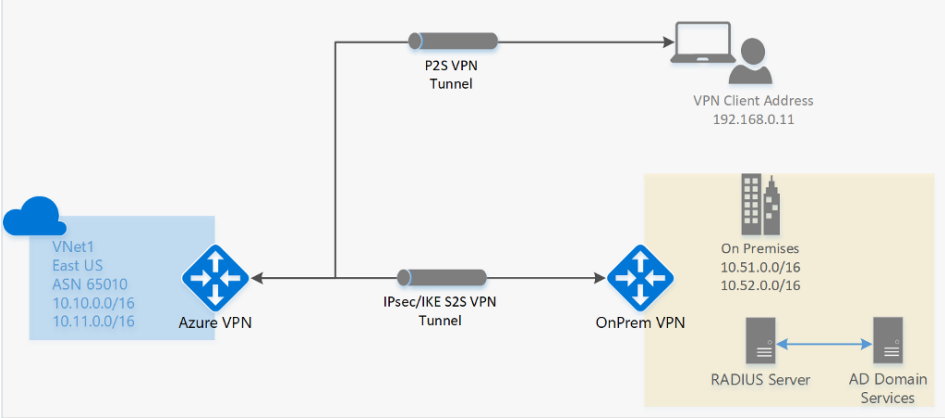
- When establishing a seamless network that combines the on-prem devices and the Azure VNets.
- Using scenarios:
  i. Manage Azure VMs with on-premises infrastructure.
  ii. Manage on-premises infrastructure with Azure solutions.
  iii. Azure as a recovery site
  iv. Secure WAN cloud between headquarters (HQs) and branch offices.
- **Site to Site VPN (S2S VPN):**
  i. To connect Azure VNET to the on-premises network, we use VPN gateway, the data is travelling over the internet but the connection is **secure** and **encrypted**.
  ii. VPN device with a Virtual IP (VIP) should be installed on the on-premises side. All the PC's on-premises will use the VIP to communicate with Azure.



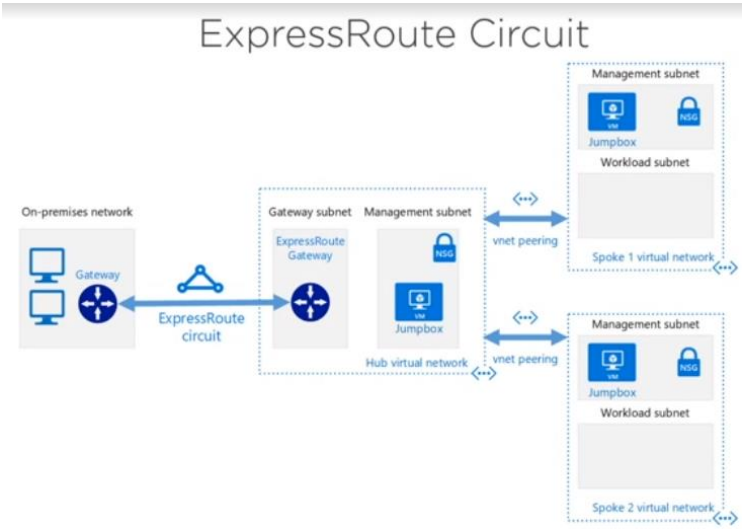
[71] https://app.pluralsight.com/course-player?course=microsoft-azure-on-premises-networks-virtual-networks-connecting&author=tim-warner&name=18327c4f-8cbd-45f9-b886-d4707d17c861&clip=0&mode=live

iii. In S2S, you need to install a gateway on-prem which is a hardware device, on the other hand, the Gateway on Azure side is only a Software (A service).

- **Point-to-site VPN (P2S VPN):**
  i. Used to connect the Azure VPN with individual devices in different locations all over the word, each device has a **VPN client** installed on it.
  ii. The **VPN Gateway** in Azure is a **Route-based VPN** (this means it has a routing table to decide how to route the data to the different connected devices).
  iii. The other type of the VPN Gateway is the **Policy-based VPN** in which it takes the address prefix (X.X.X.X/Y) for the source and the destination and then decide how to route the data to the destination.
  iv. Configuring P2S is as simple as installing a software on your computer (**VPN client**) to get your credential on the Azure VNet.



- **ExpressRoute**
  i. If virtual private network doesn't give the needed speed, or if there are concerned about data traffic in the public internet, then ExpressRoute is a solution.
  ii. It's used to connect the on-premises network to the Azure VNet over a private



connection. Its reliable and dedicated hybrid connection. The data will not flow over the Internet.

iii. ExpressRoute is a very high-speed technology that uses **MPLS**, Multiprotocol Label Switching.

iv. You can get ExpressRoute circuits up to 10 Gbps.

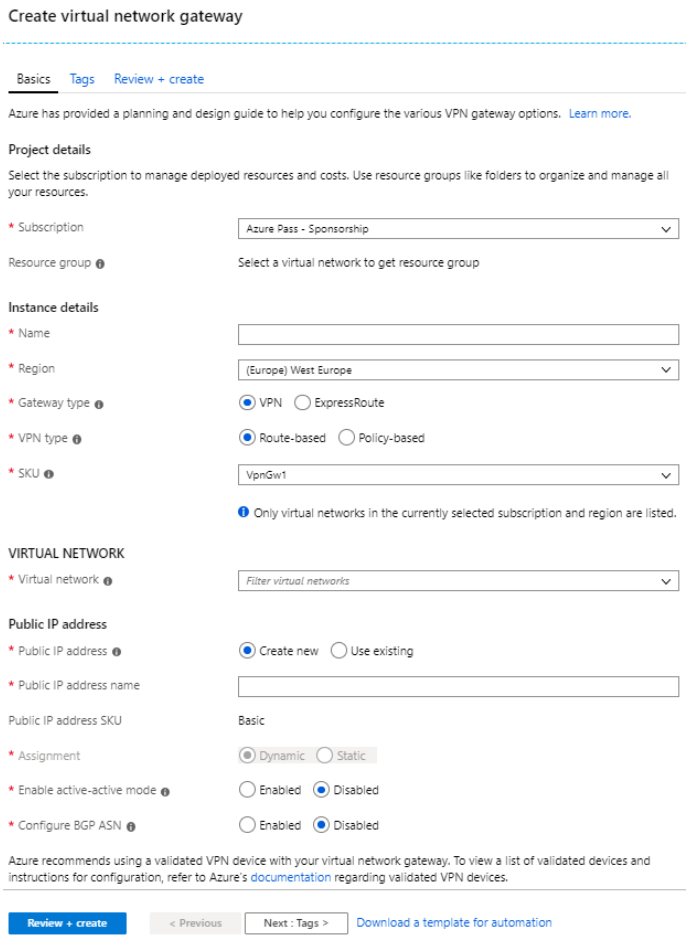
v. In this diagram we are using a design pattern called **Hub and Spoke** where the virtual network that's linked to on-prem is a hub, and then we take advantage of what's called VNet peering to create a logical connection between other VNets.

4.7.2 Create and configure Azure VPN Gateway,[72]

- A **VPN gateway** is a specific type of virtual network gateway that is used to send **encrypted** traffic between an Azure VNet and an **on-premises** location over the **public Internet**.
- You can **also** use a VPN gateway to send encrypted traffic between Azure virtual networks over the **Microsoft network**.
- **Each** virtual network can have **only** one VPN gateway.
- However, you can create **multiple connections** to the **same** VPN gateway. And then all VPN tunnels share the **available** gateway **bandwidth**.
- A virtual network gateway is composed of two or more virtual machines that are deployed to a specific **subnet** you create, which is called the **gateway subnet**.
- The VMs that are located in the gateway subnet are **created** when you **create** the virtual network gateway.
- Virtual network gateway VMs are configured to contain **routing tables** and **gateway services** specific to the gateway.
- You **can't directly configure** the VMs that are part of the virtual network gateway and you **should never deploy** additional resources to the gateway subnet.
- VPN gateways can be deployed in **Azure Availability Zones**. This brings **resiliency**, **scalability**, and **higher availability** to virtual network gateways.
- Deploying gateways in Azure Availability Zones **physically and logically separates** gateways within a **region**, while protecting your **on-premises** network **connectivity** to Azure from **zone-level failures**.

[72] https://docs.microsoft.com/en-us/azure/vpn-gateway/

- The Azure VPN Gateway connection options are:
    i. **On-premises connection** (**Local network gateway**): connecting the on-prem to another Azure resource that represents your on-premises VPN endpoint.
    ii. **VNet-to-VNet VPN**: Its preferred to use Global VNet peering instead.
    iii. **Point-to-Side VPN (P2S VPN)**
    iv. **ExpressRout Circuit:** Gateways are used in the ExpressRout as they are used in the VPN connections.
- The used protocols here are: IPsec, IKEv2, BGP to create the VPN tunnel.
- VPN Gateway Policies Configuration types:
    i. **Policy-based gateway** that uses static routing.
    ii. **Route-based gateway**, the preferred way, where you unlock all the feature set and that uses dynamic routing.
- **Configuring a VPN Gateway**
    i. Azure → Virtual network gateways
    ii. Gateway type: VPN, ExpressRoute
    iii. VPN type: Mostly Route-based because we are using Dynamic route.
    iv. Determine VNet
    v. Public IP SKU: Basic and for **zone redundant** we need to chose **Standard**.
    vi. BGP: Border Gateway Protocol
    vii. Configure BGP ASN: Can be only configured with Route based VPN Gateway with supported SKU type of VpnGw1, VpnGw2, VpnGw3.
    viii. Press Create: it will take about **45** minutes.

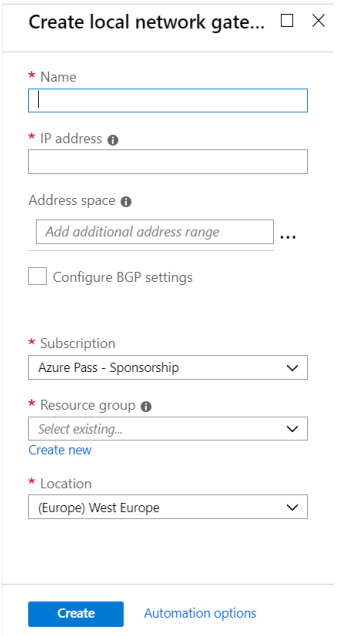


- After creating the VPN Gateway:
    i. VPN Gateway → Connection → + **Add**: Here we are going to make a link to a local network gateway.

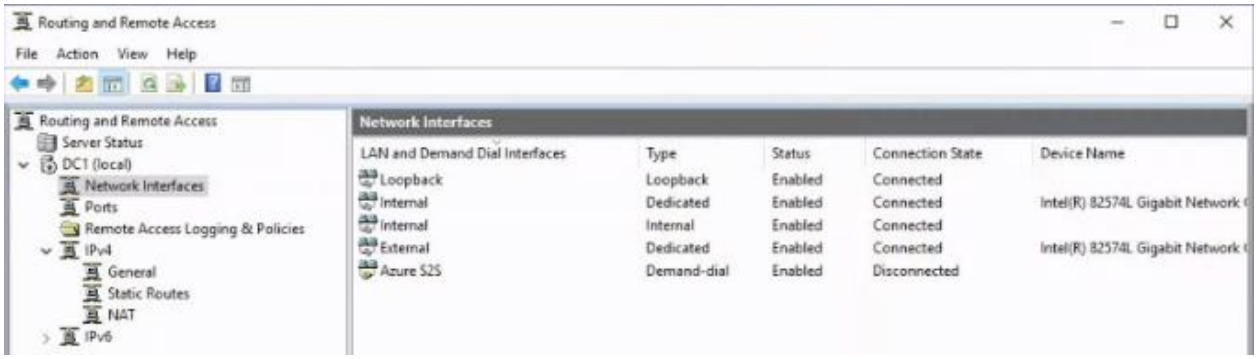
ii. VPN Gateway → Point-to-site configuration: We can configure this from the same VPN Gateway. Address pool: they are the address from the Gateway Subnet.
After completing the P2S configuration, the **Download VPN client** will be enabled to be givern to the users.

4.7.3 Create and configure site to site VPN

- S2S configuration composed of the following:
  i. Configure on-prem **VPN gateway**
  ii. Create a **local network gateway** in Azure (it's the Azure representation of the on-prem VPN device)
  iii. Establish and troubleshoot VPN connection.
- **Local Network Gateway**
  i. Create a local network gateway to represent the on-premises site that you want to connect to a virtual network.
  ii. The local network gateway specifies the public IP address of the VPN device and IP address ranges located on the on-premises site.
  iii. Azure → Local network gateways → +Add
    - IP Address: The public IP address of your local gateway.
    - Address Space: One or more IP address ranges (in CIDR notation) that define your local network's address space. For example: 192.168.0.0/16. If you plan to use this local network gateway in a BGP-enabled connection, then the **minimum prefix** you need to declare is the host address of your BGP Peer IP address on your VPN device.
    - After creating the Local Network gateway, we need to go to the on-prem machine and continue setting up.



iv. On-prem DC → Routing and Remote Access → Network Interface → External.



- We have the External interface to connect with Azure
- The Azure S2S. a demand dial connection, on the property you add the Public IP address of the remote Gateway (Azure VPN Public IP).

- For Security we use a pre-shared key.

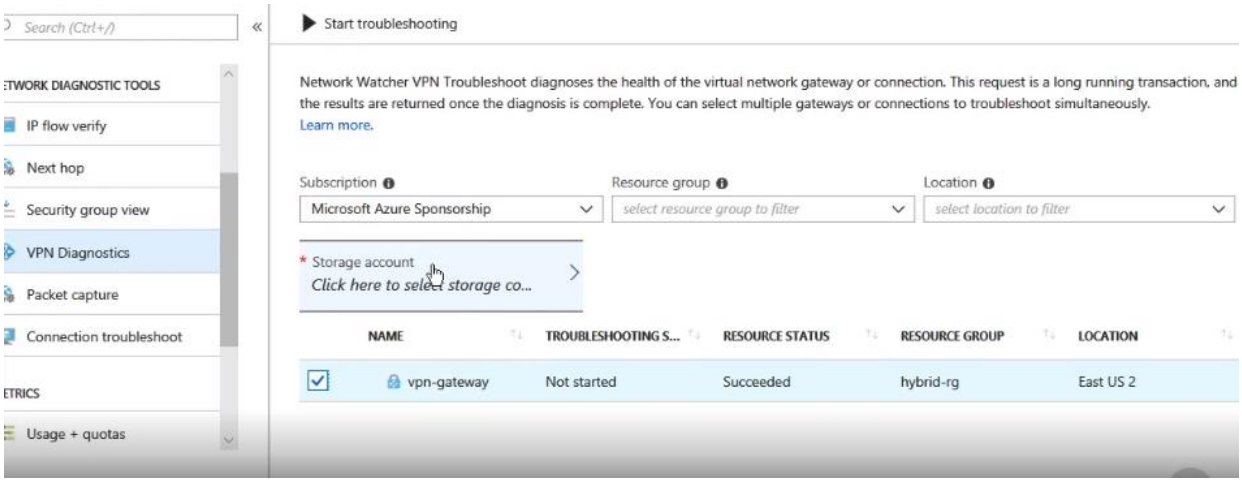
4.7.4 Configure Express Route

- **Premium Add-On** feature in ExpressRoute is Primarily used to allow access to the VNets from the ExpressRout circuits, which means that customers can access to VNets all over the world using ExpressRoute
- **Premium Add-On** increase the number of VNets you can connect from 10 VNets to a number depends on the Bandwidth.
- ExpressRoute is **expensive** and you pay only for the **Outbound** traffic from Azure to your on-prem. Another option is **Unlimited Data**, then its more expensive.

- **ExpressRoute Direct:**
    i. ExpressRout require that you make an individual contract with one of the Internet Service Provider in your region to connect with Azure cloud. But with ExpressRoute Direct toy can directly connect with the global Microsoft backbone.
    ii. ExpressRoute Direct gives you the ability to connect **directly** into Microsoft's global network at peering locations strategically distributed across the world.
    iii. ExpressRoute Direct provides dual **100** Gbps or **10** Gbps connectivity, which supports Active/Active connectivity at scale.

4.7.5 Network Watcher - VPN troubleshoot

- **Network Watcher VPN Troubleshoot** diagnoses the **health** of the VNet **gateway** or **connection**.
- This request is a **long running** transaction, and the results are returned once the diagnosis is complete.
- You can select **multiple** gateways or **connections** to troubleshoot simultaneously.
- We select our gateway or connection from the list and denote a location to store the troubleshoot data. (**storage Account**)

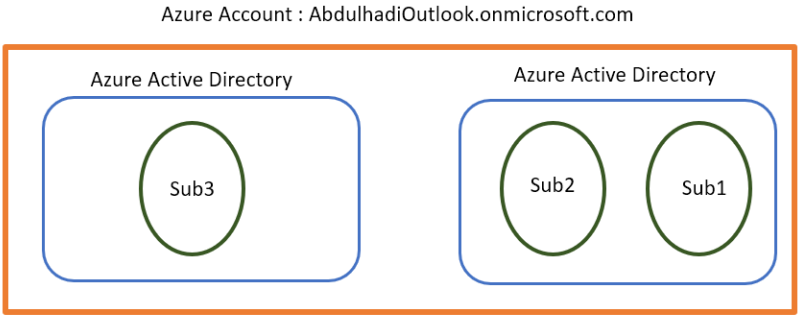


5 Manage Identities: (15 -20%)

5.1 Manage Azure Active Directory (AAD)

5.1.1 Azure Active Directory (AAD)[73]

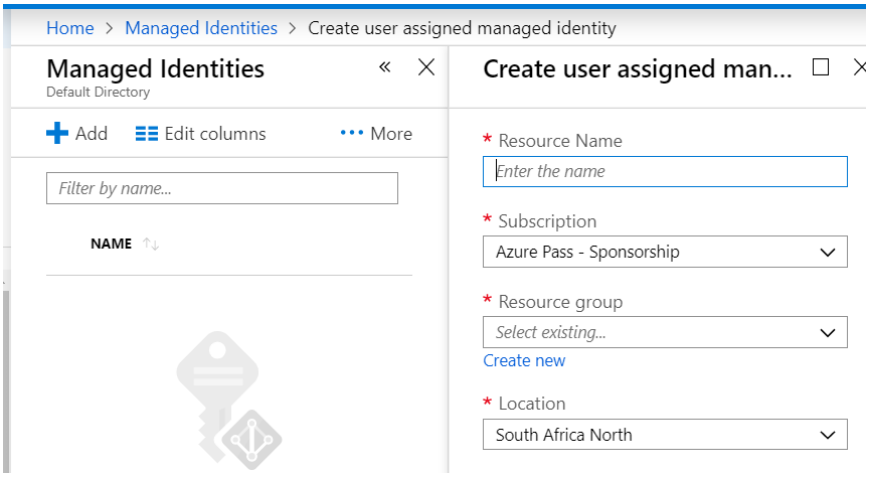
- https://www.youtube.com/watch?v=OQwQmikCLs4
- https://www.youtube.com/watch?v=5tJ5Uz2GlsQ
- https://bit.ly/30cRt0o
- Azure Active Directory (Azure AD) is Microsoft's **cloud-based** identity and access management service, which helps your employees **sign in and access resources** in:
  - External resources, such as Microsoft Office 365, the Azure portal, and thousands of other **SaaS** applications.
  - Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.
- The Subscription is created **inside** the AAD, so **changing** the Directory (AAD) will cause the need to create a new subscription.
- Each account (email address) can contains **multiple** AADs
- Each **AAD** can have **multiple** subscriptions



- To create a new Active Directory (Tenant):

[73] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

- Create a resource,→ Identity→ Azure Active Directory.



- **Important**: The person who **creates** the tenant is automatically the **Global administrator** for that tenant. The Global administrator can add additional administrators to the tenant.

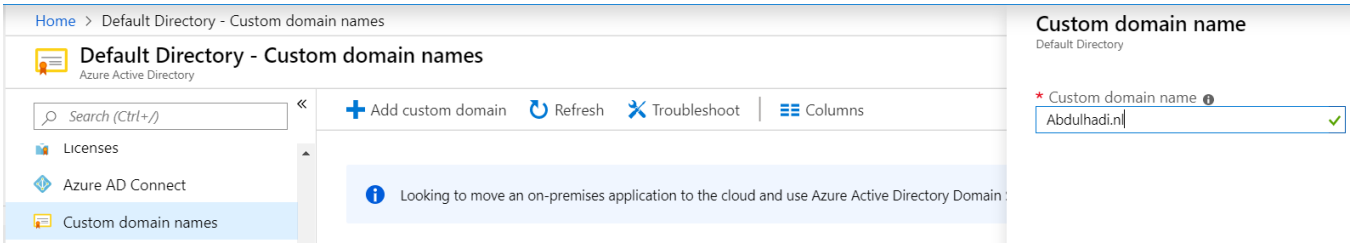
- AAD **Vs** ADDS (Active Directory Domain service):
  - AAD is an **identity** solution, designed for internet-based application and use **HTTP** and **HTTPS** communications.
  - AAD uses **REST** API for querying not **LDAP**
  - AAD **doesn't use** Kerberos authentication.
  - AAD include **Federation** (third party) services.
  - AAD users and groups use **a flat structure**, there are **no** Organizational Units (**OUs**) or Group Policy Objects (**GPOs**).
- AAD is a **managed service**, you only manage users, groups and policies. On the other hand, deploying ADDS **within a VM** means that need to manage deployment, configuration, VMs …

- **Azure AD pricing:**

	FREE	BASIC	PREMIUM P1	PREMIUM P2
Single Sign-On (SSO)	10 apps per user	10 apps per user	No Limit	No Limit
Self-Service Password Reset		Yes	Yes	Yes
Company Branding		Yes	Yes	Yes
SLA 99.9%		Yes	Yes	Yes
Advanced group features			Yes	Yes
Multi-Factor Authentication (MFA)			Yes	Yes
Conditional Access			Yes	Yes
Identity Protection				Yes
Privileged Identity Management				Yes
Access reviews				Yes

5.1.2 Add Custom Domains:[74]

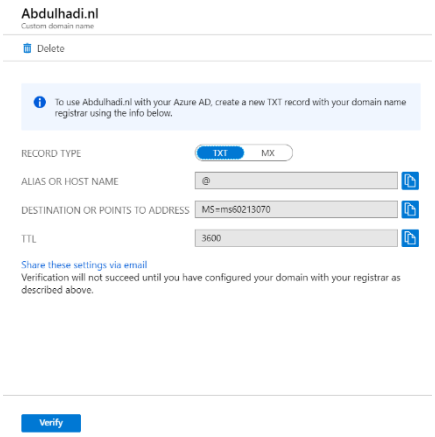
- Each AAD **tenant** come with an initial domain name: **domainname.onmicrosoft.com**
- You can't change or delete the initial domain name, but you can add your organization domain names into the list. This is called: **Custom domain names**.
- Adding custom domain names helps you to create user names that are **familiar** to your users, such as alain@contoso.com.
- To use a specific domain name with your Azure AD, create a new TXT record with your domain name registrar (**Registrar**: A company designed to provide domain registration service to other companies or individuals that would like to own a particular web address).
- The domain name **shouldn't** be already used in another directory.
- A Domain Name can **only be verified** in one directory (AAD)
- AAD → Custom Domain names → + Add Custom domain



[74] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain

- To add a domain, you must already **own** a domain name and have the necessary sign-in credentials to update the DNS records with your domain name **registrar**.

- After click add domain, a TEXT record will be grated and you need to verify it from the registrar.
- To verify a domain and prof to Azure that you are the owner for this Domain Name you need to **copy** the TXT record and **enter** it within the Domain Name **registrar**.



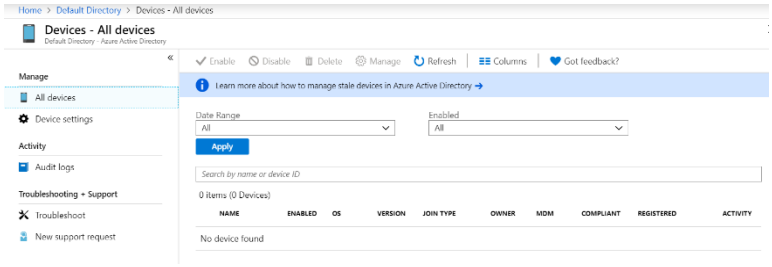
5.1.3 Azure AD Join[75]

- Join your work device to your organization's network
- BYOD: Bring your own device.
- We have two options to Add a device to AAD:
  - **Registering**:
    - Register your personal device (typically a phone or tablet) on your organization's network. After your device is registered, it will be able to access your organization's restricted resources.
    - When a device is registered the AAD device registration provide the device with an Identify, which is used to authenticate the device when a user is sign in to AAD.
    - This identity can then be use to enable or disabled the device.
  - **Joining**:
    - It's an extension of Registering a device, sine it also changes the **local state** of a device?
    - Changing the Local State allow the users to sign in suing the work account or school account instead of your personal account.
    - Allowed users can join their unregistered devices.

[75] https://docs.microsoft.com/en-gb/azure/active-directory/user-help/user-help-join-device-on-network

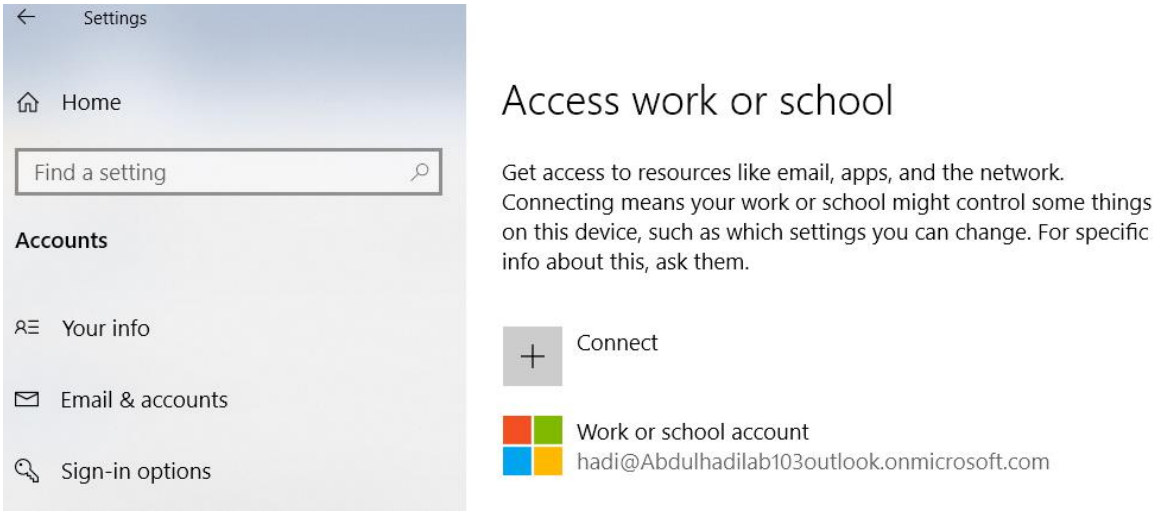
- To see the listed joined devices is AAD:

  ADD → Devices



- To add a device to AAD:

  - From your device: Setting → Accounts→Access work or school → Connect and then enter the Microsoft account to connect to AAD.



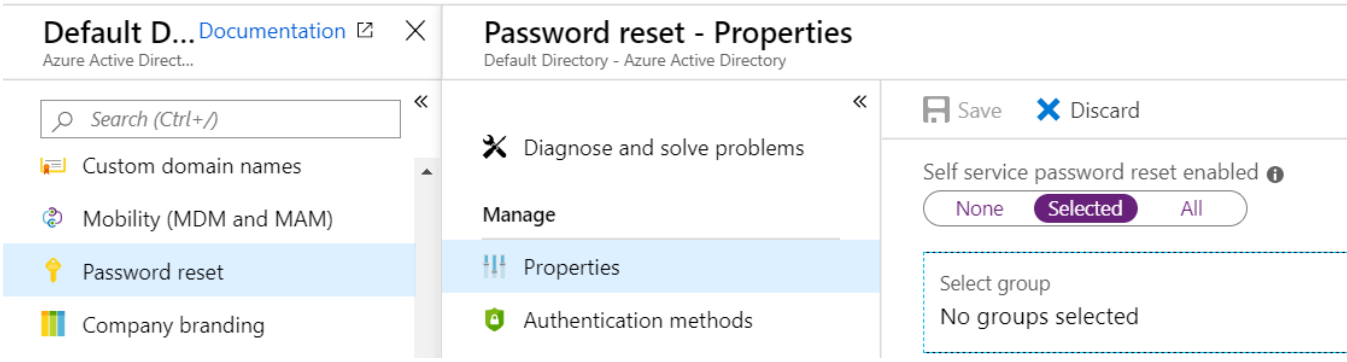
5.1.4 Configure self-service password reset (SSPR)[76]

- It's a part of the AAD features, available in all AD types **except** the **Free** one.
- Enabling Self Service Password Reset means that users form AAD can freely changing their passwords.
- To enable the SSPR, you need first to upgrade your AAD type from Azure AD Free to Basic, Premium P1 or Premium P2 type. Azure offers 1-month **free trial** of Premium P2.

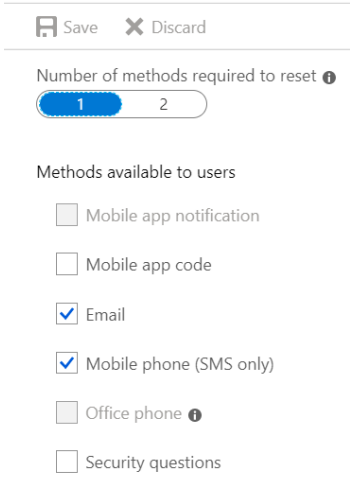
[76] https://docs.microsoft.com/en-gb/azure/active-directory/authentication/concept-sspr-howitworks

- You could enable the SSPS to All or to **AAD Group**.

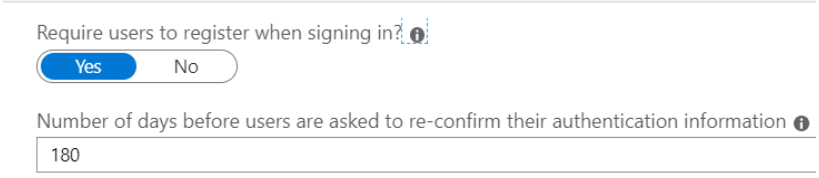
  AAD→ Password reset → Properties →



- After Enabling the SSPS, you need to go to the Authentication Methods to define the number of methods required to reset and choose the wanted method:

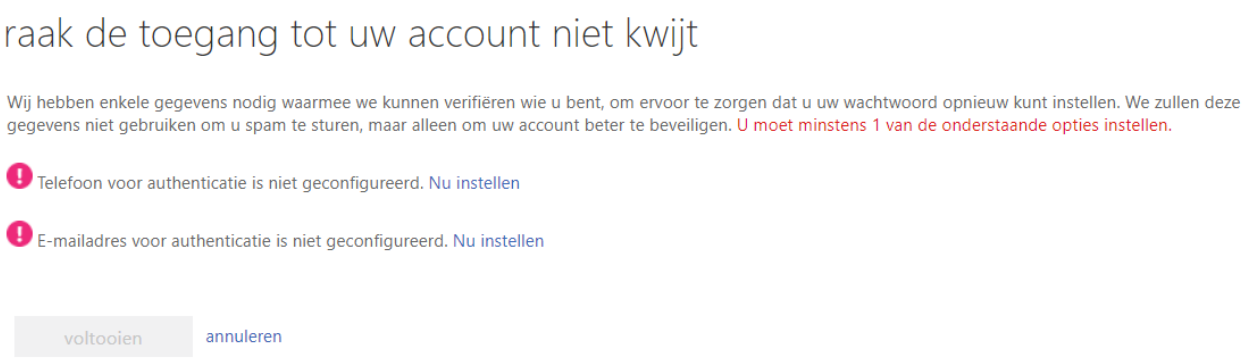


- In **registration** section, make sure that user are required to register when signing in:



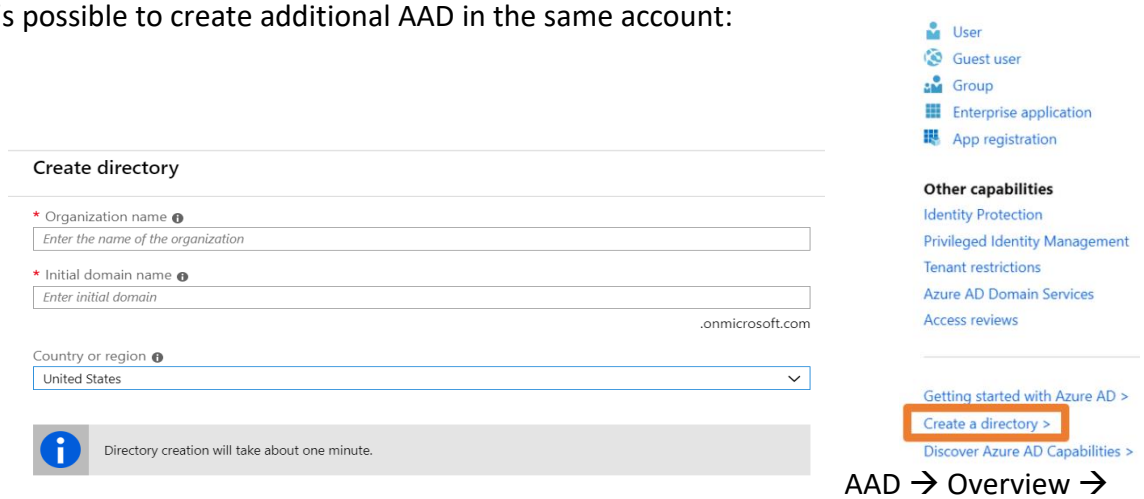
  - Designates whether unregistered users are prompted to **register** their **own** authentication information when they sign in for the first time. If set to "**No**," administrators must manually specify the necessary password reset authentication information in the properties for each user in this directory, or instruct users to go to the registration portal URL directly

- To test SSPR:
  - Log in poratle.azure.com using the user credential, and then you will be asked to verify the authentication details:



5.1.5 Manage multiple directories

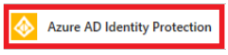
- By default, an active directory will be created when you create your account is created, this is the Default Directory.
- The subscription will be placed in the default directory.
- It's possible to create additional AAD in the same account:



AAD → Overview → Create a directory

- By default, a **basic domain name** at **onmicrosoft.com** is included with your directory. Later, you can **add** a domain name that your organization already uses, such as contoso.com.
- To see the created Directory,
  AAD → Overview → Switch directory
- The new created AAD has **no** Subscription associated to it.
- You need to **associate** a subscription to the new AAD to be able to use Azure resources.

5.1.6 Configure Azure AD Identity Protection (AAD-IP)[77]

- PREMIUM P2 Feature, standalone service. 

That enables you to:
  - Detect potential vulnerabilities for identities
  - Automate responses to suspicious actions
  - Investigate suspicious incident and take actions.
- The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Because of that we need to:

[77] https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview

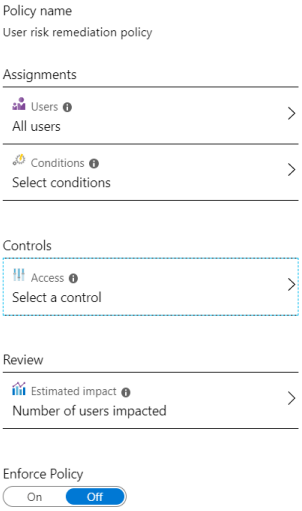
- Protect all identities regardless of their privilege level
- Proactively prevent compromised identities from being abused

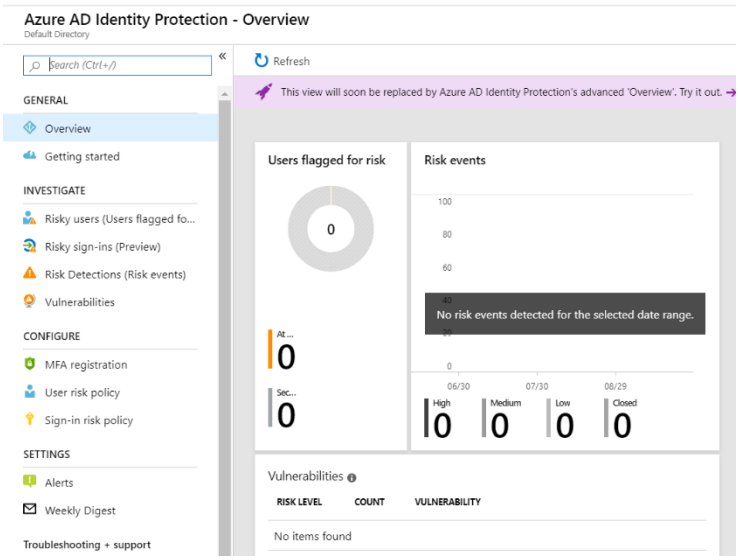
- We can within AAD Identity protection configure **risk-based policies** that automatically respond to detected issues when a specified risk level has been reached.
- AAD uses **ML algorithms** to detect anomalies and generates a risk report determining risk level.
  - AAD Identity Protection detects the **Vulnerabilities**:
    - Weakness in your environment that can be detected by the attacker.
    - The AAD-IP can detect several vulnerabilities, such as:
      a. Multi-Factor Authentication (MFA) not configured
      b. Unmanaged cloud app (the AAD Cloud App Discovery service is used)
      c. Security Alert from Privileged Identity Management
- The Risk level of an Event:
  - This will help you to **priorities** your actions. Azure currently select **6** types of risk events:

Event	Risk Level
User with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical location	Medium
Sign-ins from IP addresses with suspicious activities	Medium
Sign-ins from unfamiliar locations	Medium
Sign-ins from infected devices	Low

- **Configure Azure AD Identity Protection:**
  - Marketplace → Identity → Azure AD Identity Protection → Create (Premium P2 feature)

- For each Risk event or Venerability, we need to assign the **User Risk Policy**





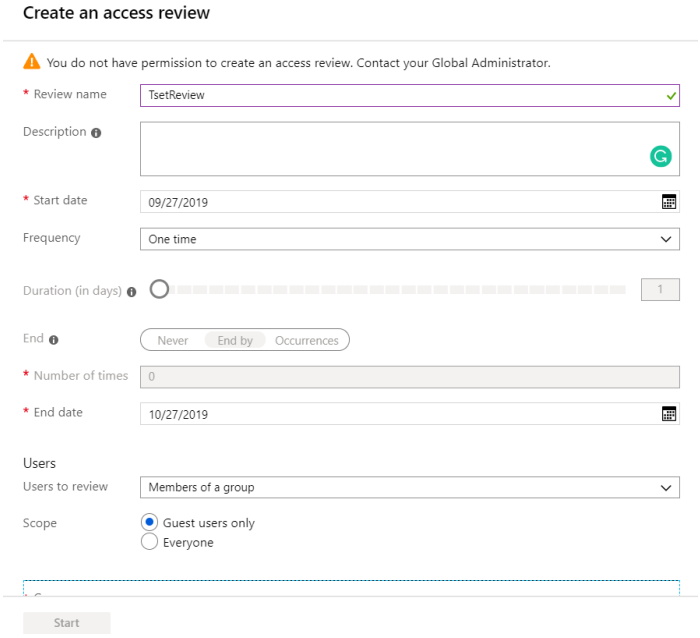
5.1.7 Access Reviews[78]

- PREMIUM **P2** feature. A standalone service.
- Ensure the right people have the right access at the right time.
- Enable organizations to **manage** group memberships, application access, and privileged role assignments.
- User's access can be reviewed on a regular basis to make sure only the right people have continued access.
- **Access reviews using scenario:**
  - As **new employees** join, how do you ensure they have the right access to be productive?

[78] https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

- As people **move** teams or leave the company, how do you ensure their old access is **removed**, especially when it involves guests?
- Dealing with excess access rights

- **Perform an Access Review:**
  - Resource → Identity Governance → Create an Access reviews.
  - Click on "**Onboard**" in the left navigation menu to start using Access reviews now.



5.2 Manage Azure AD objects (users, groups, and devices)[79]

5.2.1 Azure Roles type[80]

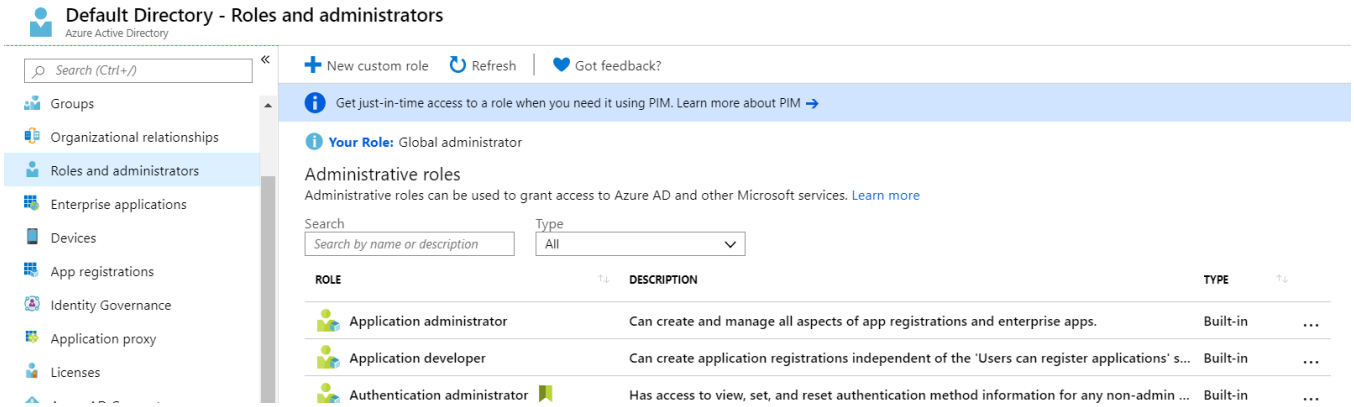
- The Azure Roles types are:
  - Classic subscription administrator roles
  - Azure role-based access control (RBAC) roles
  - Azure Active Directory (Azure AD) administrator roles
- **Azure RBAC roles**
  - Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management to Azure resources, such as compute and storage.
  - There are four fundamental RBAC roles. The first three apply to all resource types:

Azure RBAC role	Permissions	Notes
Owner	Full access to all resources Delegate access to others	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope
Contributor	Create and manage all of types of Azure resources Cannot grant access to others	Applies to all resource types.
Reader	View Azure resources	Applies to all resource types.
User Access Administrator	Manage user access to Azure resources	Applies to all resource types.

- **Azure AD administrator roles:**

[79] https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/index
[80] https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles

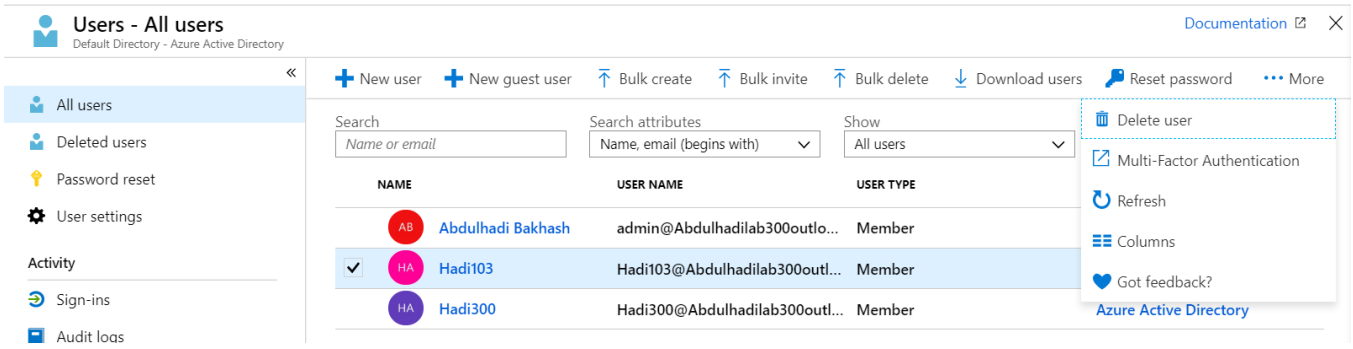
- Azure AD administrator roles are used to manage Azure AD **resources** in a directory such as create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains.
- **Important** Azure AD administrator roles are: Global Administrator, User Administrator and Billing Administrator.
- AAD → Roles and administrators



- **Azure RBAC roles Vs. Azure AD administrator roles**[81]
  - At a high level, Azure RBAC roles control permissions to manage Azure resources,
  - while Azure AD administrator roles control permissions to manage Azure Active Directory resources.

5.2.2 Create users and groups

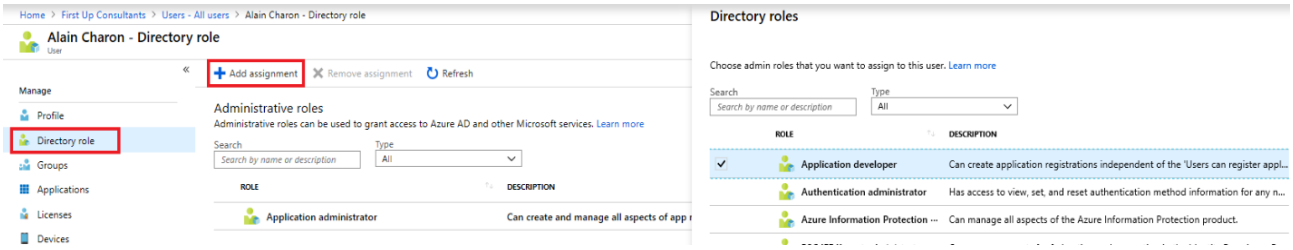
- **Azure Users:**
- You can create a new **user** using the Azure Active Directory portal.
- Azure Active Directory → Users → + New user **or** + New guest user



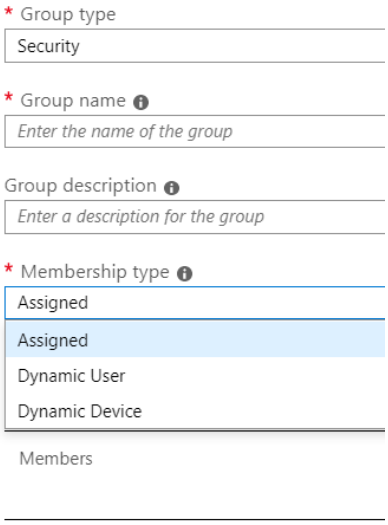
[81] https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles?context=azure/active-directory/users-groups-roles/context/ugr-context

- Users Types:
  - **Create user**: Create a **new user** in your organization. This user will have a user name like alice@domainneme.onmicrosoft.com.
  - **Invite user**: Invite a **new guest user** to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
- If a user in your organization needs **permission** to manage Azure Active Directory (Azure AD) resources, you must assign the user an appropriate **role in Azure AD**, these roles are called **Directory roles.**
  - Assign the roles during the user creation.

    AAD → Users → UserName → Directory role → + Add Assignment



- **Azure Groups**
- **AAD → Groups → + New group**
- Group types: **Security**, **Office 365**.
- While creating groups, you need to choose the Membership type: Assigned. Dynamic user, Dynamic device:
  - **Assigned**: user will be assigned to this groups manually.
  - **Dynamic User**: you will add a rule and users will be added to this group based on this rule.

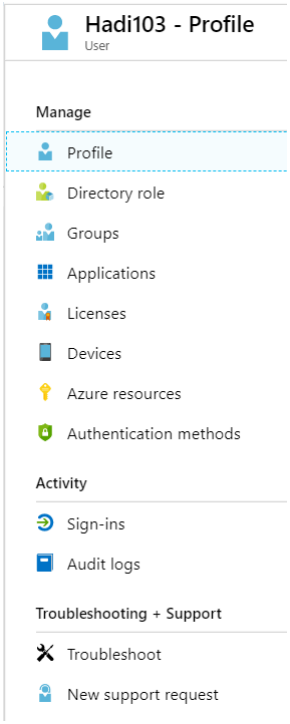


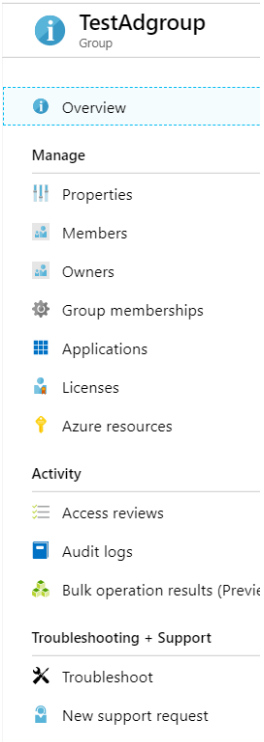
- **Dynamic Device**: To see a device in the device blade, the device should be **registered**. In windows 10, **Connect app** is used to connect your PC to Azure. You need to connect the device by using an **account from the users inside the AAD**.

5.2.3 manage user and group properties

AAD → **Users** → All users → [AAD user] →

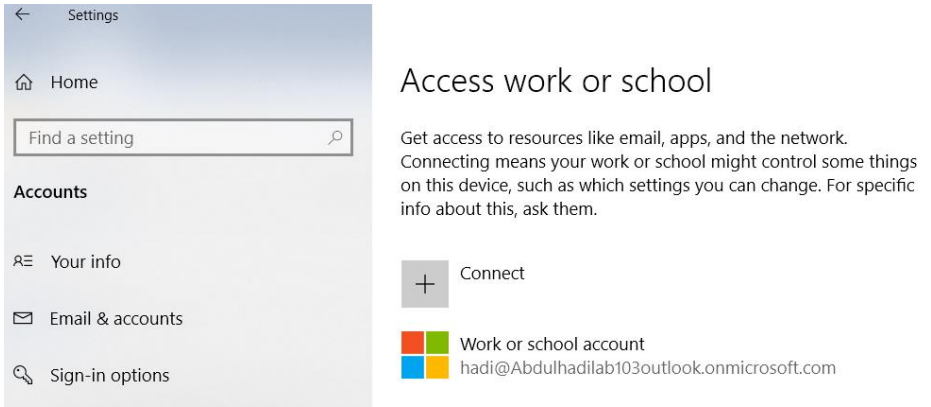
AAD → **Groups** → All Groups → [AAD group] →





5.2.4 manage device settings

- To list all the devices registered to AAD
  - AAD → Devices
- To add a device to AAD: From your device: Setting → Accounts→Access work or school → Connect and then enter the Microsoft account to connect to AAD.



- After adding the device, you can Disable or Delete it from the AAD. The best practice is just to Disable a device to keep its credentials for future **re-join**.

5.2.5 Perform Bulk User Updates:

- Update all the details of user simultaneously.
  - For example: add department to all the users in a specific AAD group.
  - Using Azure cloud – **PowerShell**

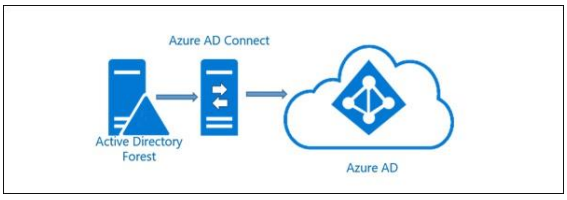
```
$groupname = "a43e656b-865c-4f93-a532-4582345acb9f"
$users = Get-AzureADGroupMember -ObjectId $groupname
foreach ($u in $users)
 {Set-AzureADuser -ObjectId $u.UserPrincipalName
  -Department "HR"
 }
```

5.2.6 Manage guest accounts

- B2B collaboration user
- Azure Active Directory → Users → + New guest user
- **Invite user**: Invite a **new guest** user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
- Note:
  - The User Type has **no relation** to how the user signs in, the directory role of the user, and so on.
  - This property simply indicates the user's **relationship** to the host organization and allows the organization to **enforce policies** that depend on this property.

5.3 Implement and manage hybrid identities[82]

- Microsoft's identity solutions **span on-premises** and cloud-based capabilities.
- These solutions create a common user identity for authentication and authorization to all resources, **regardless of location**. We call this **hybrid identity**.
- **Azure AD Connect** is the Microsoft tool designed to meet and accomplish your hybrid identity goals.



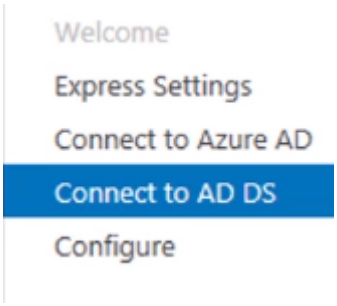
- The **authentication methods** used to achieve Hybrid Identity, depending on your scenarios:
  - Password hash synchronization (PHS)
  - Pass-through authentication (PTA)

[82] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

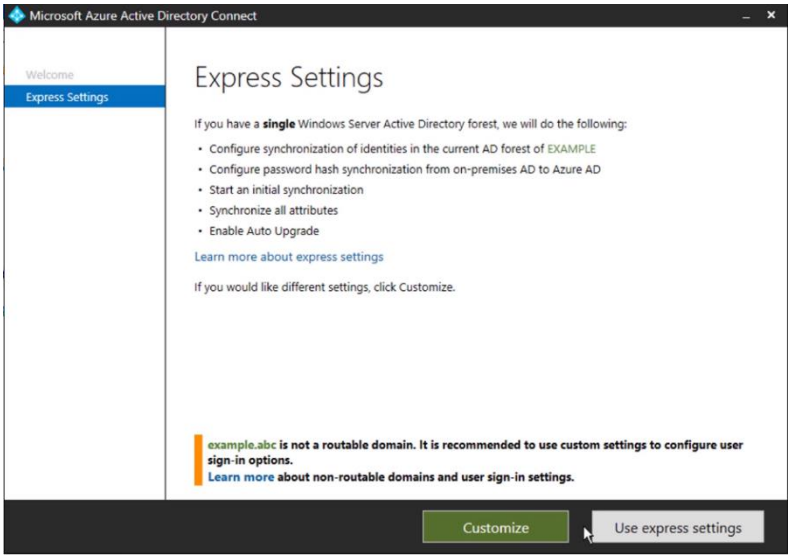
- Federation (AD FS)

5.3.1 install Azure AD Connect[83]

- Hybrid in Azure, points to a combination of on-prem services with Microsoft Azure services.
- Azure AD connect can **sync** the objects from on-prom AD to AAD
- The Azure AD connect provides a number of features:
  - Password hash synchronization
  - Pass-through authentication
  - Federation integration
  - Synchronization
- Health Monitoring
- **Install and configure Azure AD Connect:**
  - **Download** the AAD Connect to your PC and then paste it in Azure VM: https://www.microsoft.com/en-us/download/details.aspx?id=47594
  - In **Azure VM** (represent the on-prem device): Install **Azure Active Directory Domain Services** role. And then the AAD Connect to synchronise the users.
  - In Azure VM, create a user and make him a member of **Enterprise Admins**. This is needed because AAD AD connect will attach one user from the AD DS and one user from the AAD for the synchronization.
  - Download the AAD AD connect in the Azure VM, you can use either Express Setting or Customize.
  - You will need to enter the credentials for both user's side: Azure AD and AD DS.

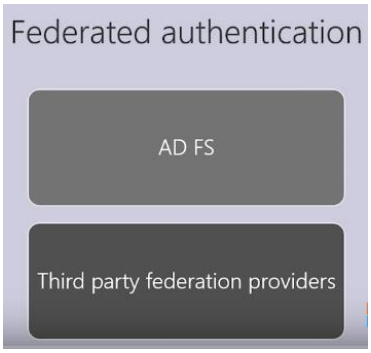


[83] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect



- **Authentication Methods:**
  - Once you choose your authentication methods, it's hard to change, because it will disrupt your user sign-in experience.

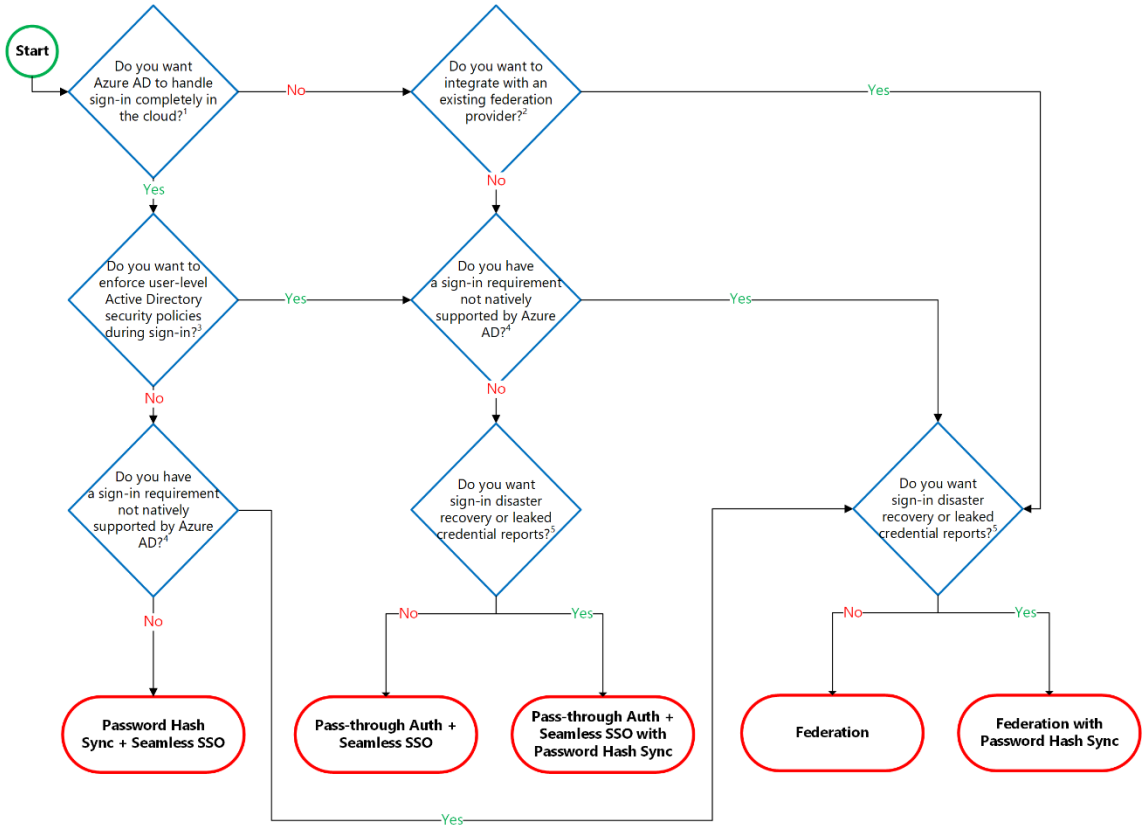
  - **Cloud Authentication:**
    - **Cloud-only**
      a. This is for Born-in cloud organizations with no on-premises infrastructure.
      b. Here you can establish user identities **directly in the cloud** and Azure AD handles all of the authentications completely in the cloud.
    - **Password Hash Sync:**
      a. Users can actually sign in to cloud-based applications using the **same usernames and passwords** that they use with their on-premises Active Directory.
      b. Password hash sync also provides user and password protection.
    - **Pass-through authentication**
      a. It is very similar to password hash sync, but it's for organizations where their **security policies** or something that they would like to **reuse** in the cloud.



  - **Federated Authentication:** In this case Azure AD actually hands-off the authentication to a trusted authentication system to handle all of the authentication.
    - **Microsoft's AD FS**

- **Third-party compatible Federation providers.**

- **Seamless single sign-on (SSO):**
  - Its means that you don't have to enter your credentials for each service or application, one sign-in will be enough.
- In **Azure AD Connect,** a number of **options** can be setup in order to implement hybrid identity. These options are[84]: **Decision Tree**



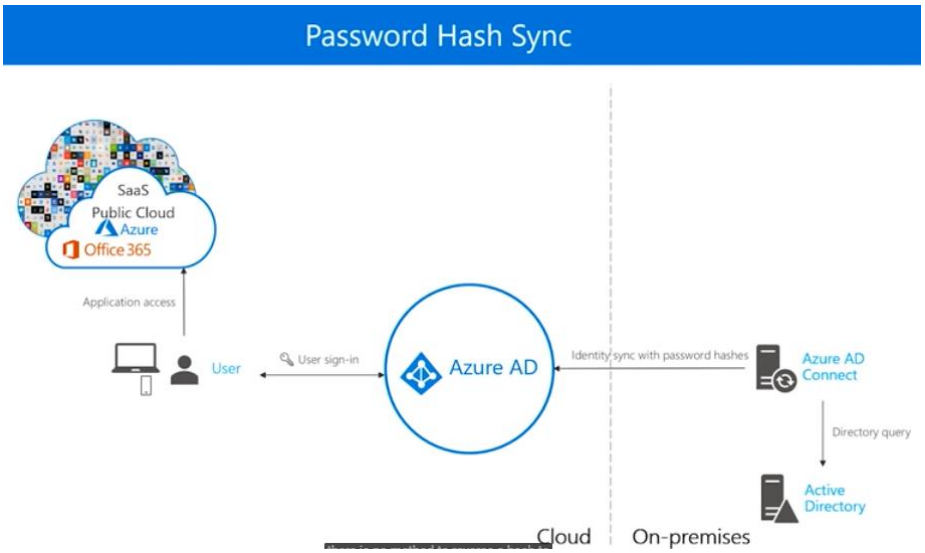
5.3.2 Password hash synchronization with Azure AD[85]

- Users can actually sign in to cloud-based applications using the same usernames and passwords that they use with their on-premises Active Directory.
- Password hash sync also provides user and password protection.
- Synchronize on-prem Active Directory **with** ADD. In this case AAD become an **extension** of your already existing on-prem AD.
- Configured via **AD Connect.**
- Syncs a hash, of the hash, of the user's password.
- Password hash synchronization can:

[84] https://docs.microsoft.com/en-us/azure/security/fundamentals/choose-ad-authn
[85] https://docs.microsoft.com/en-gb/azure/active-directory/hybrid/whatis-phs

- Improve the productivity of your users.
- Reduce your helpdesk costs

- Microsoft searches for compromised passwords on the dark web
- Can be combined with SSO.

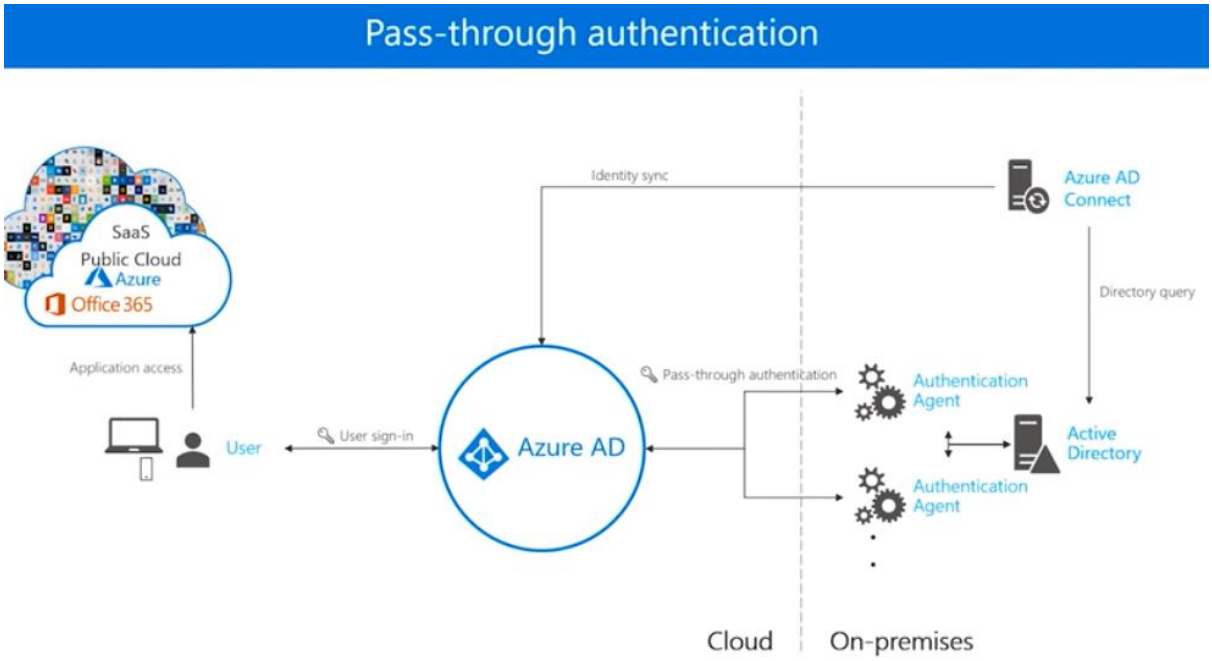


5.3.3 Azure Active Directory Pass-through Authentication[86]

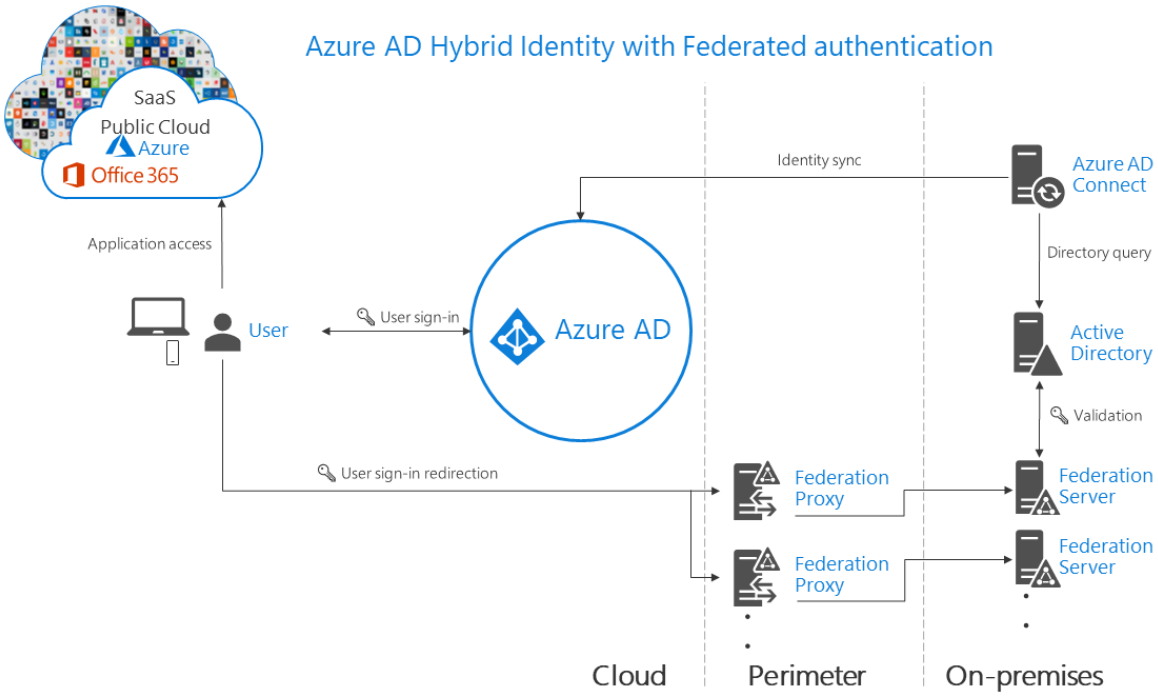
- It is very similar to password hash sync, but it's for organizations where their security policies or something that they would like to reuse in the cloud.
- Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to **both** on-premises and cloud-based applications using the **same passwords**.
- This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations.
- However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
- Configured via an **AD connect agent** outbound connection
- Authentication is done in the cloud after a secure password verification exchange with the on-premises authentication agent
- Does not sync the password but Azure AD validates against the on premise

[86] https://docs.microsoft.com/en-gb/azure/active-directory/hybrid/how-to-connect-pta

- Can be combined with SSO.



5.3.4 federation with Azure AD[87]



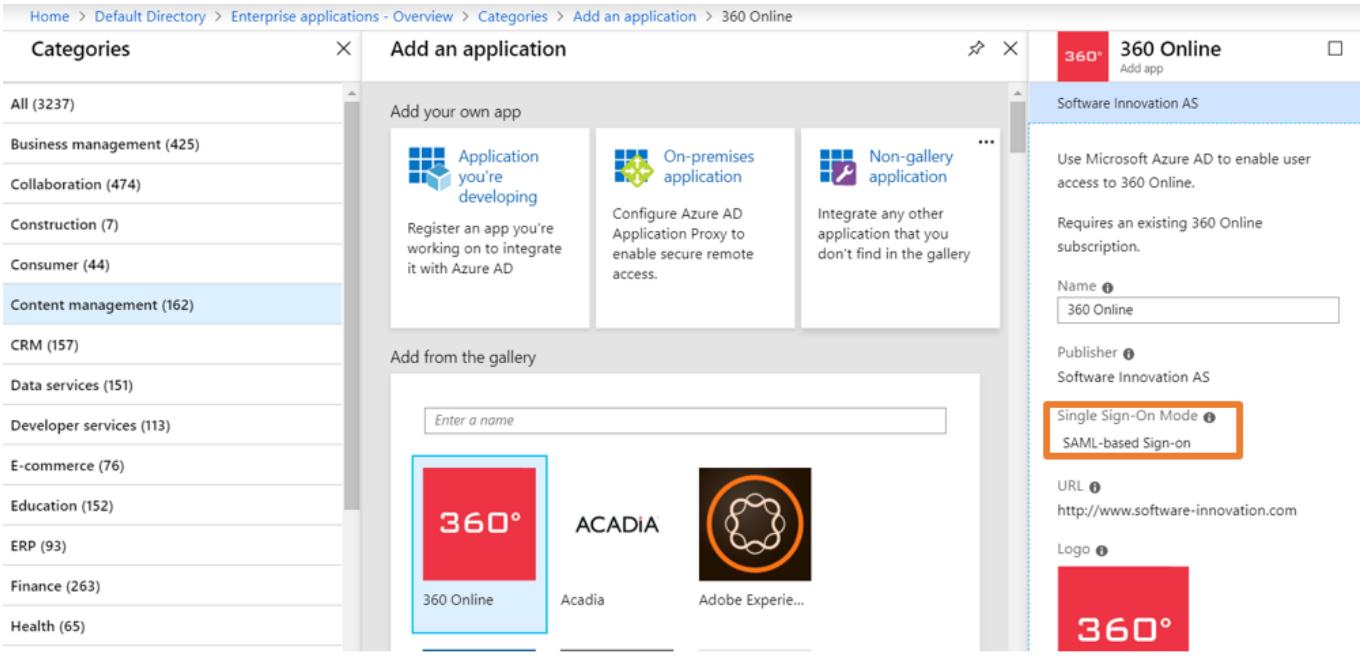
[87] https://docs.microsoft.com/en-gb/azure/active-directory/hybrid/whatis-fed

- Federation is a collection of domains that have established trust.
- The level of trust may vary, but **typically** includes **authentication** and **almost always includes authorization.**
- In this case Azure AD actually **hands-off** the authentication to a trusted authentication system to handle all of the authentication.
- All user authentication **occurs on-premises**.
- If the federation fails or is down you will be out of Azure, to avoid it combine it with Pass-through Authentication as a backup

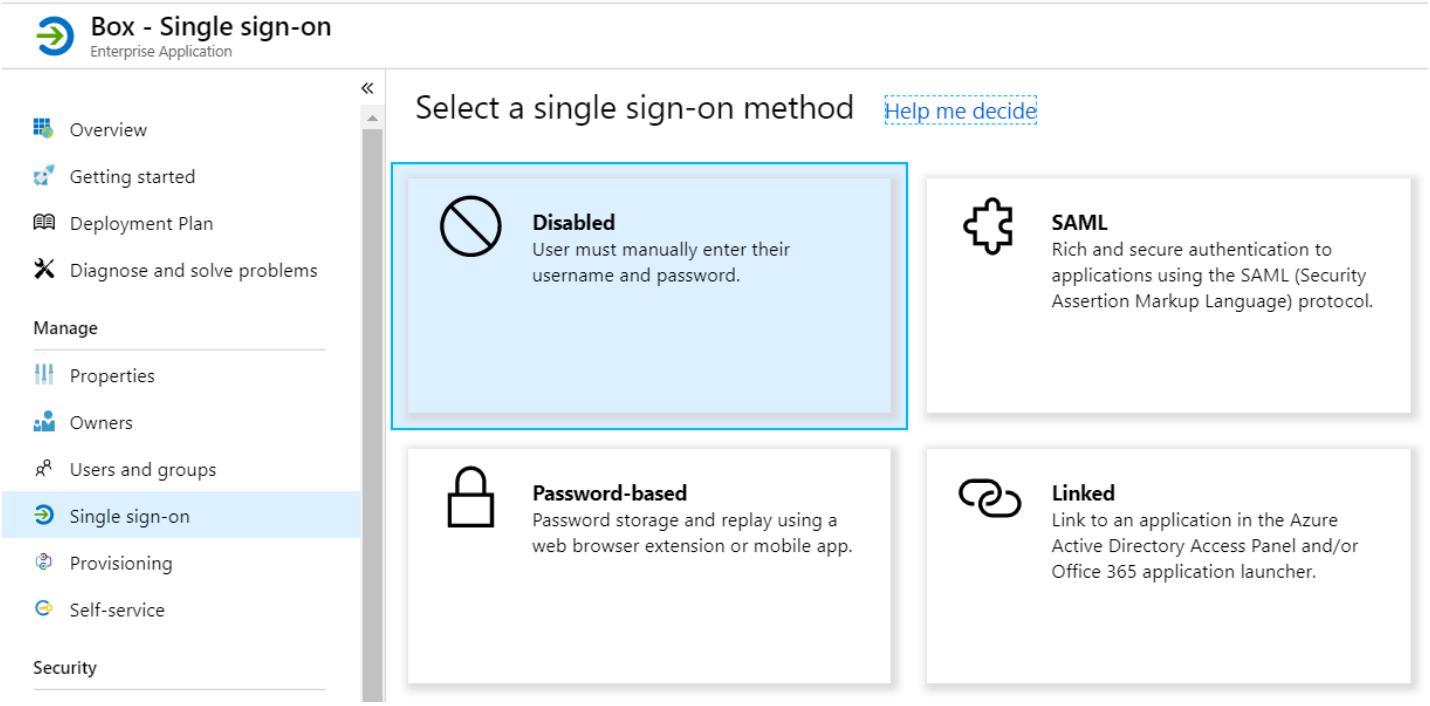
5.3.5 Azure Active Directory Seamless Single Sign-On (SSO)[88]

- Its means that you don't have to enter your credentials for each service or application, one sign-in will be enough.
- Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network.
- When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames.
- Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.
- Seamless SSO is not applicable to Active Directory Federation Services (ADFS).
- **Federation Vs SSO**
  - Federation Beyond the organization boundary whereas SSO is only within an organization boundary.
  - If you are doing federation, this means you are also doing SSO. But if you are doing SSO that doesn't mean that you are doing Federation.
- **Configuring SSO:**
  - AAD → Enterprise applications → Overview → + New Application: if you choose any of the applications you can detect the SSO Mode for it:

[88] https://docs.microsoft.com/en-gb/azure/active-directory/hybrid/how-to-connect-sso

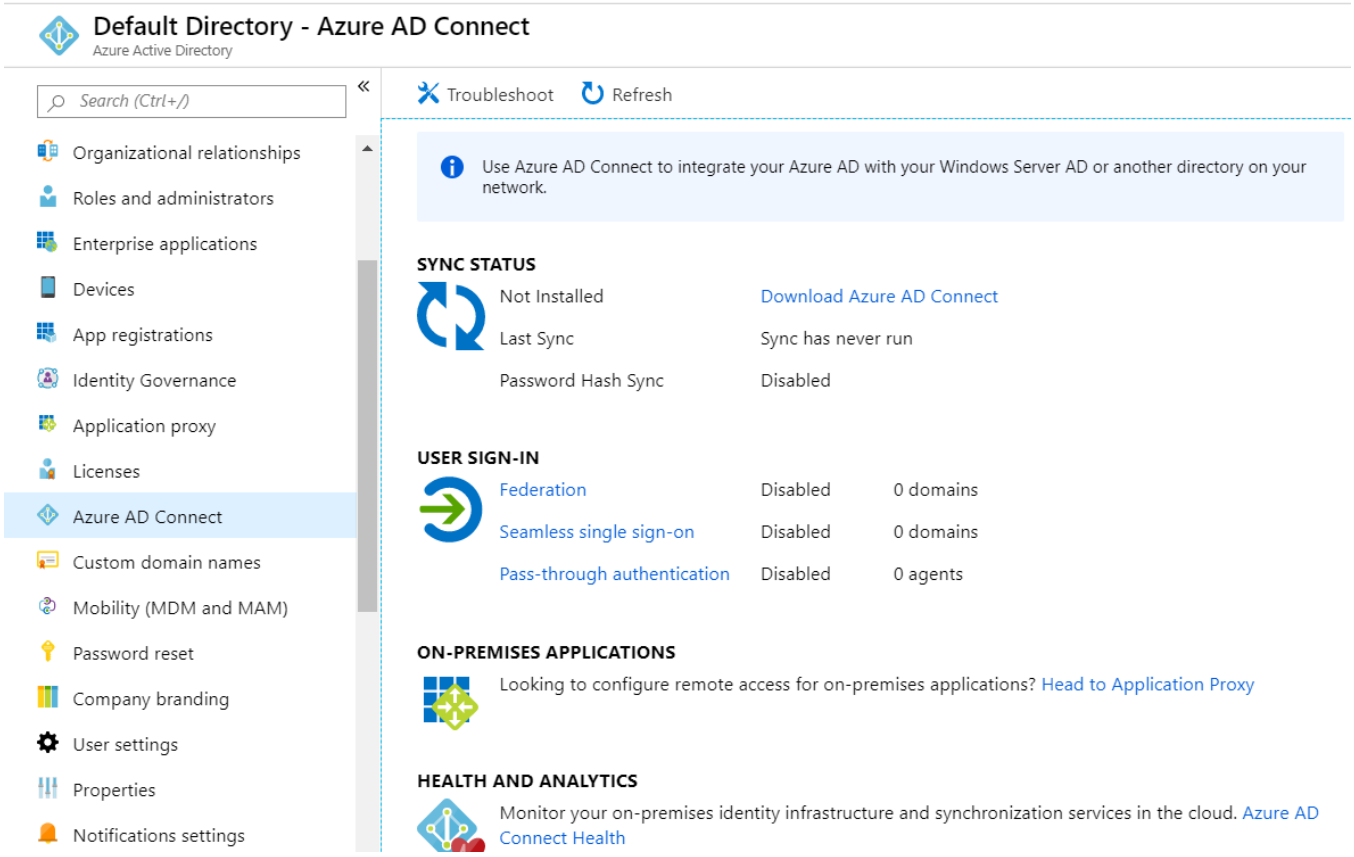


- **Single Sign-On Mode:** This is the type of Single Sign-on the application supports:
  - **SAML/OpenID** Connect based SSO will allow your users to allow apps using their organizational accounts hosted in your Identity Provider.
  - **Password-based Sign-on** enables administrators to securely store passwords in the cloud, and assign those passwords to user or groups.
- After adding the specific application to the AAD, for example: **BOX** → Single Sign-on



5.3.6 Manage Azure AD Connect

- Use Azure AD Connect to integrate your Azure AD with your Windows Server AD or another directory on your network.
- AAD → Azure AD Connect

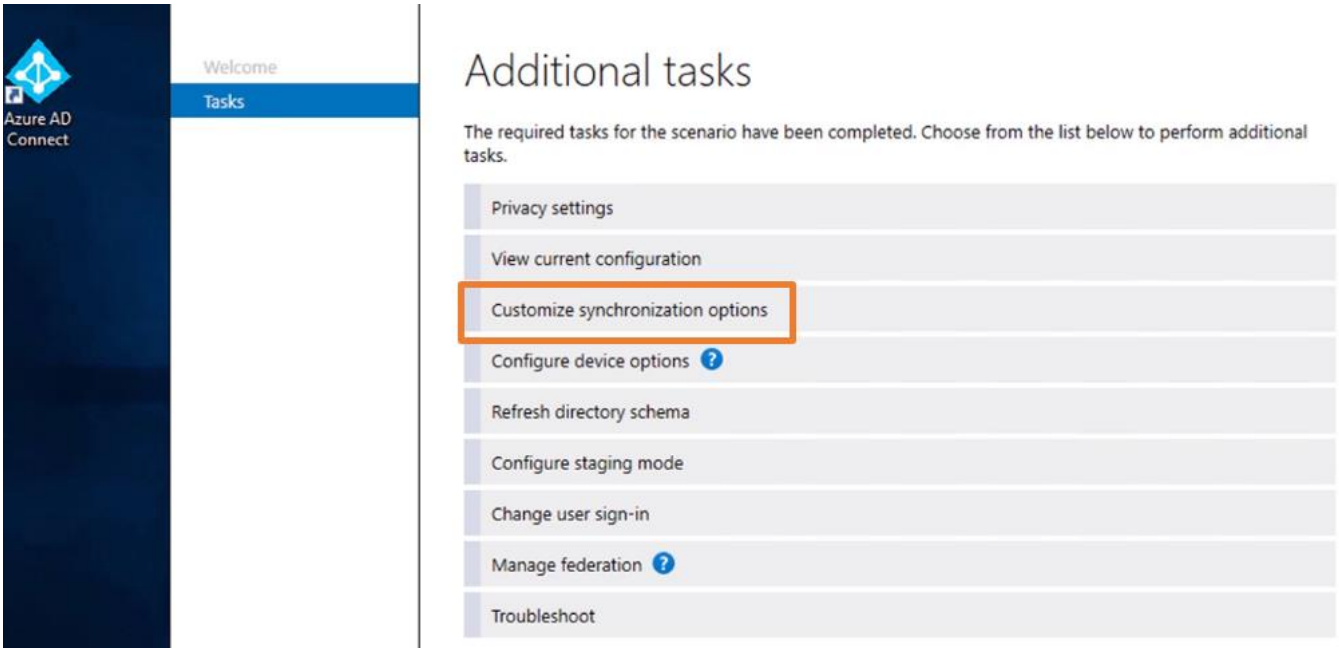


5.3.7 manage password sync and password writeback[89]

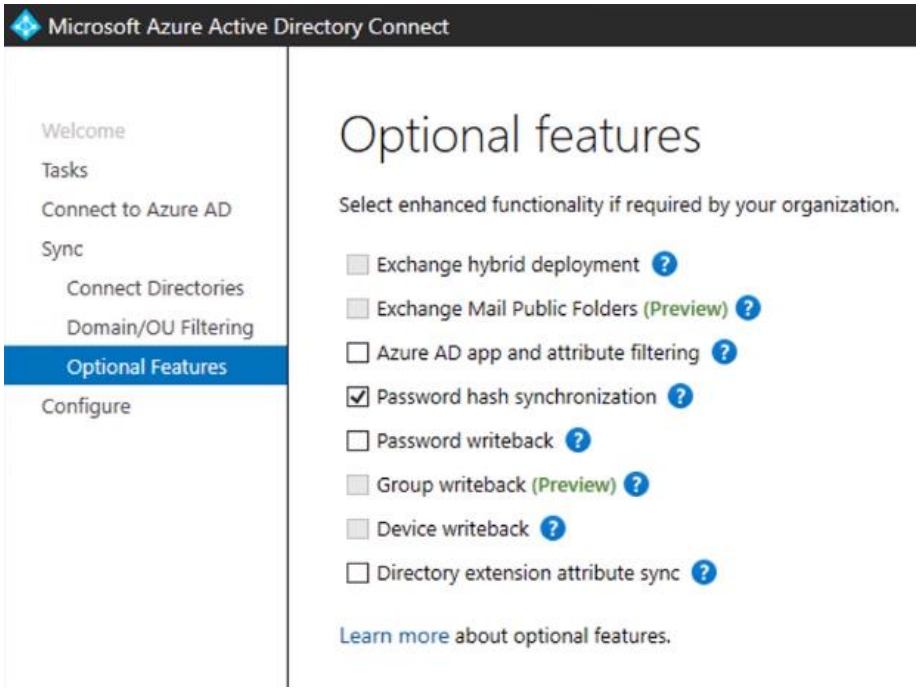
- Password writeback is a feature enabled with AAD Connect that allows passwords changes in the cloud to written back to the on-premises directory in real time.
- Enabling Password Writeback:

[89] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-writeback

- Within the server that we installed the AAD connect in it → Azure AD Connect → Configure → Tasks → Customise synchronization options → enter

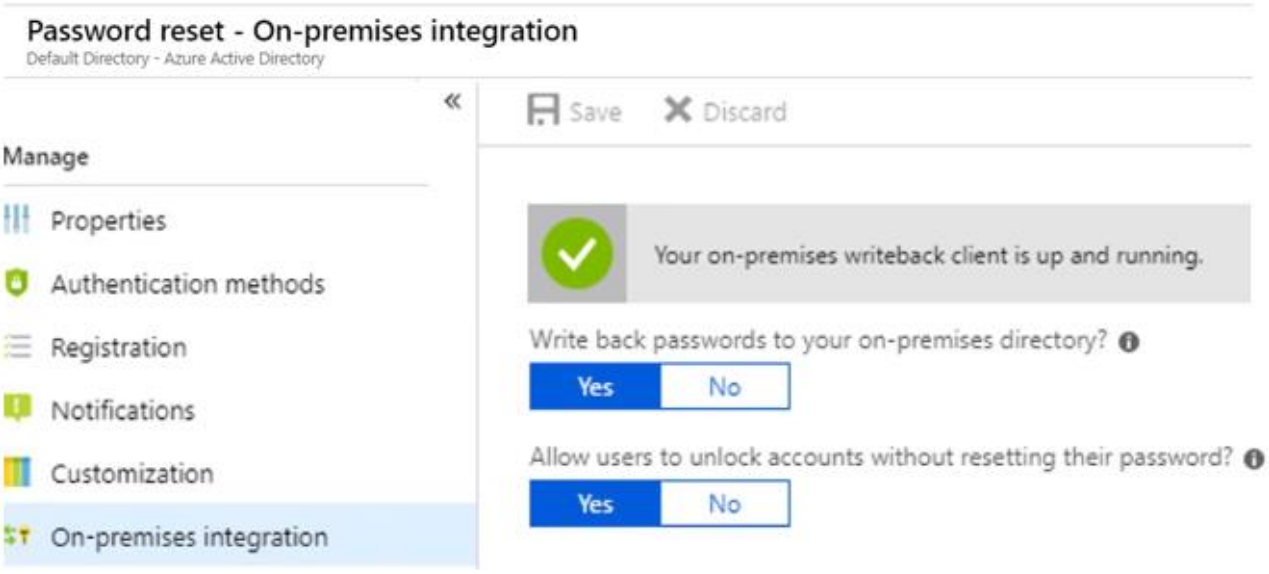


the required information until reaching the **optional Features**: Check the Password writeback



- This will enable the Password writeback on the on-prem side, we need next to allow self-service password reset to use the Password writeback. To do that:

- AAD → Password reset → On-premises Integration



5.4 Implement multi-factor authentication (MFA)[90]

- MFA works by requiring **two or more** of the following authentication methods:
  - Something you **know** (typically a password)
  - Something you **have** (a trusted device that is not easily duplicated, like a phone)
  - Something you **are** (biometrics)
- MFA is included for **free** in the Azure **AD Premium P2**, but it's **billable per user** for the other types of AAD.

5.4.1 Configure user accounts for MFA

- There are many ways of deploying MFA with Azure AD.
  - Cloud-based MFA: when we enable the MFA to users, we will redirected to a separate wen page.
  - Server Setting: AAD → MFA→ Server Setting, where you download the server software and make it running in your own environment.
- The best way is to use Azure MFA in the cloud and to apply it to your users using **conditional access**.

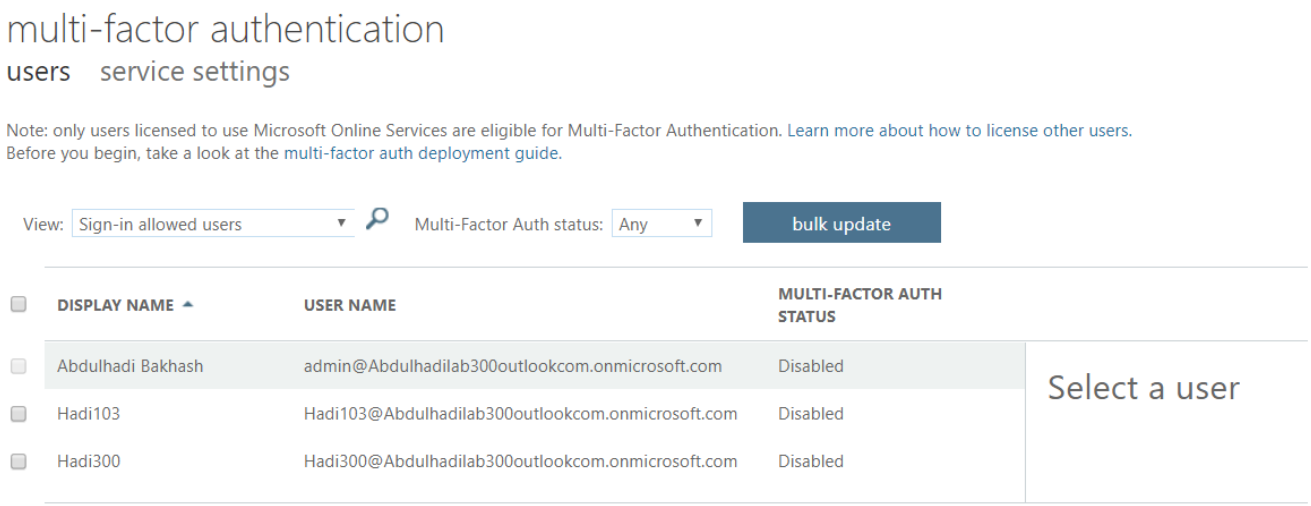
[90] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

- You can only apply MFA to AAD users, **not to the Guest users**.
- AAD → Users → All users → Multi-Factor Authentication

This will send you to a separate web site

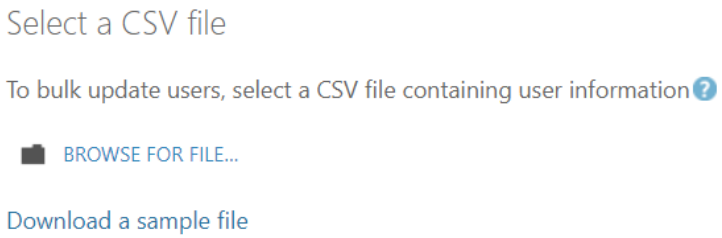
https://account.activedirectory.windowsazure.com/

- Within this page, I can Enable the MFA for the AAD users.



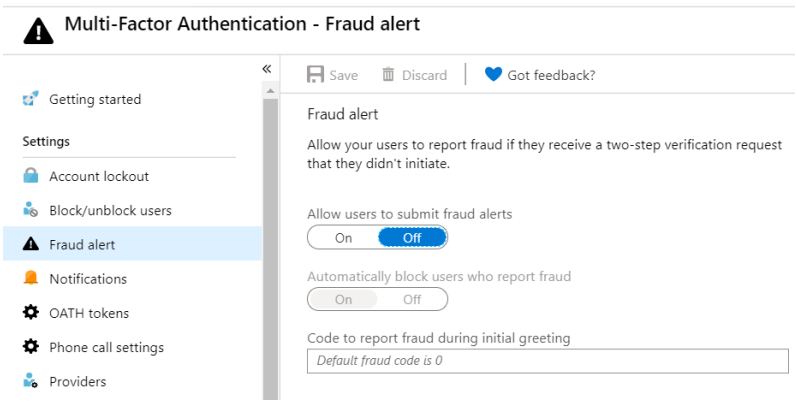
5.4.2 enable MFA by using bulk update

- In the MFA web page select Bulk Update link:



5.4.3 configure fraud alerts

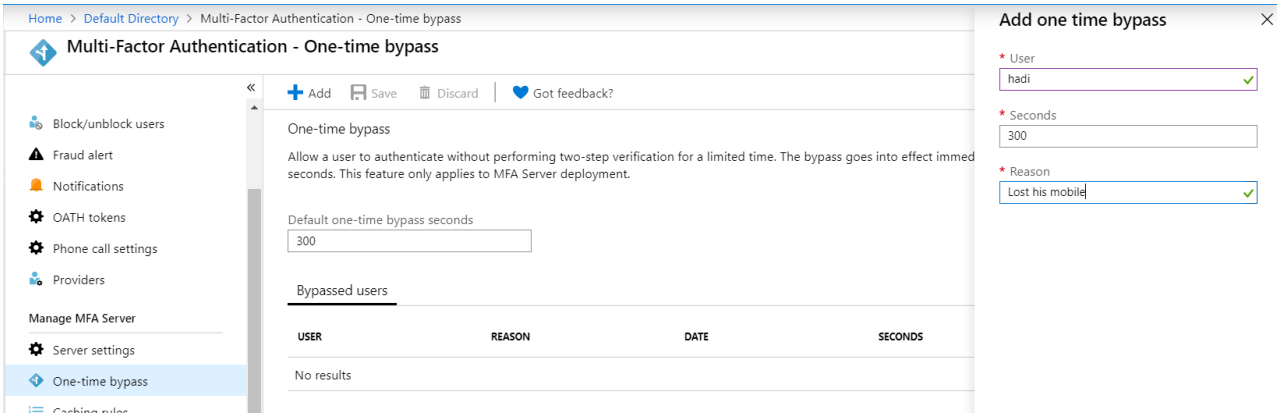
- Allow your users to report fraud if they receive a two-step verification request that they didn't initiate.
- AAD → **MFA** → Fraud alert
- By Default, Fraud alert is set to off.
- If you set: Automatically block users who report fraud to **On,** then the blocked users will move to Block/unblock users tab within the Fraud Alert blade.



- **Block/unblock users**
  - A blocked user will not receive Multi-Factor Authentication requests.
  - Authentication attempts for that user will be automatically denied.
  - A user will remain blocked for **90** days from the time they are blocked.
  - To manually unblock a user, click the “Unblock” action.

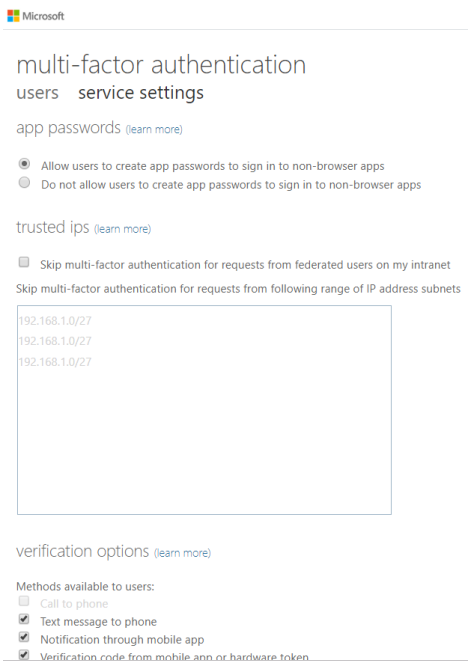
5.4.4 Configure bypass options

- Allow a user to authenticate without performing two-step verification for a limited time.
- The bypass goes into effect immediately, and expires after the specified number of seconds.
- This feature only applies to MFA Server deployment.
- AAD → **MFA** →On-Time bypass → + Add



5.4.5 Configure Trusted IPs and configure verification methods

- AAD → MFA → Getting Started → Configure Additional cloud-based MFA setting
- https://account.activedirectory.windowsazure.com/
- You can determine the trusted IPs and the verification options
- Enabling trusted IPs: Skip multi-factor authentication for requests from federated users on my intranet.



6 Hands-on Labs

- https://microsoftlearning.github.io/AZ-103-MicrosoftAzureAdministrator/
- https://linuxacademy.com/library/topics/Azure/type/Hands-On%20Lab/

7 References

- https://www.whizlabs.com
- https://www.udemy.com/
- https://docs.microsoft.com/en-us/azure/
- https://www.edx.org/
- https://www.pluralsight.com/
- https://skillpipe.com/
- https://www.youtube.com/
- https://pixelrobots.co.uk/2019/03/study-resources-for-the-az-103-microsoft-certified-azure-administrator/'
- https://channel9.msdn.com/register?ReturnUrl=%2Fevents%2FIgnite%2FAustralia-2017%2FCLD321%3Fterm%3Darm%20templates%26lang-en%3Dtrue