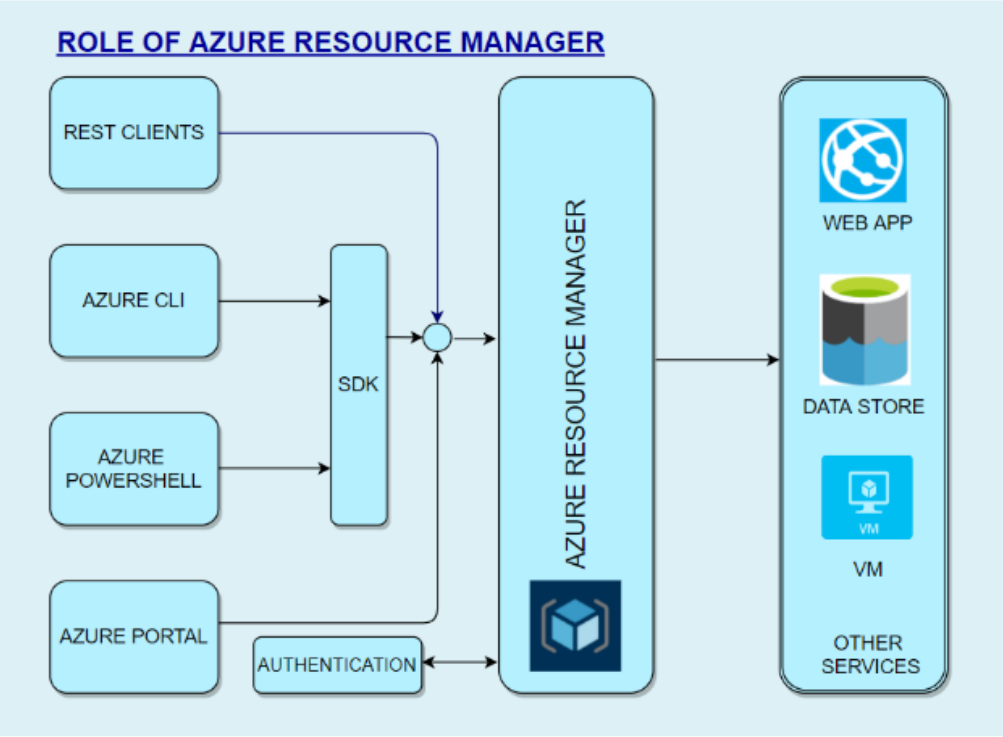
**Azure resource group is different from Azure resource manager. /**

**Azure Resource Manager ( ARM )**

* Azure Resource Manager provides a management layer to create, update, and delete resources in your Azure account
* ARM uses management features, like access control, locks, and tags, to secure and organize your resources after deployment.
* When a user sends a request from any of the tools, ( azure portal, Azure CLI, Azure Powershell, Rest APIs, SDKs ) the ARM receives the request and authenticates/authorizes it.
* Then it sends the requests to azure services to take action.
* Since it acts as a central point, it leads to consistent results.



**Benefits of Resource Manager**

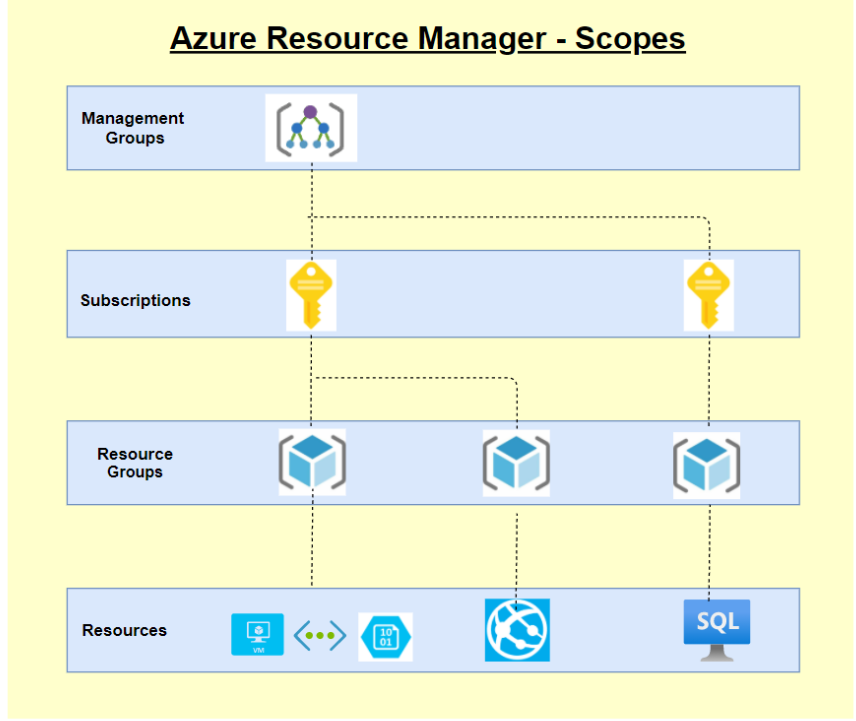
* Declarative templates so we don’t have to worry about the current state.
* Applies access-control via RBAC natively.
* Applies tags to organize resources logically
* Define dependencies so the correct order of deployment is done.
* Allows group deployments
* Allows for redeployment and have confidence that same results will be achieved

**Scopes**

4 levels/scopes are available for deploying/applying changes to resouces )

1. Management Groups
2. Subscriptions
3. Resource Groups
4. Resouce

* **Management Groups**:  
  At this level, we can combine multiple subscriptions to apply changes at an Organizational level.   
  We can combine subscriptions with a hierarchy where there is one management group at the root level. This is called Nesting.
* **Subscriptions**:  
  Subscription is a logical container used to provision resources.   
  We will be billed at the subscription level.   
  We can have multiple subscriptions
* **Resource Groups:**We can logically group resources at a resource group level. We can create multiple resources in a resource group.   
  We can delete an entire resource group, and all resources will be deleted within the resource group.   
  We can even move a whole resource group with all objects within it.
* **Resource**  
  This is the lowest manageable item in Azure resources.   
    
  Examples of Azure resources are Virtual machines, storage accounts, web apps, databases, virtual networks, and tags.   
  Management groups, Subscriptions, Resource groups are also examples of resources.



**Azure Pricing**

Azure is one of the market leaders in Cloud services and has some of SQL and Windows’s best pricing. It can leverage several features to save costs, and Azure provides several tools that can help calculate costs and cost-effectively plan our infrastructure and service.   
  
**Some of the available tools are:**

1. Azure Pricing Calculator
2. Cost Management Center​
3. Billing Data API & Advisor​
4. DB & Cosmos DB Capacity calculator
5. Migration planning (( Estimation, Workload, and right-sizing​ ))

**Some of the features that we can leverage to save costs are as follows:**

1. **Azure Hybrid Benefit** –   
   We can use our existing Windows & SQL licenses to save on costs
2. **Spot Virtual machines** -   
   This feature allows us to take advantage of the unused CPU at a significantly lower cost at almost 90% savings.
3. **Reservations -**   
   We can commit to 1-year or 3-year and choose to pay upfront or monthly to buy RIs. ( Reserved Instances)
4. **Azure Dev/test pricing –**   
   For development environments, we can get special discounted rates

**Ways to optimize Cost**

1. Azure Hybrid benefit
2. Choose the right azure compute service
3. Right size underused resources
4. Configure autoscaling
5. RI’s for consistent workloads. ( Reservation of Instances )
6. Shut-down unused resources
7. Setup budgets

**Are there any other ways to save costs?**

1. **EA – Enterprise Agreements –**   
   With this, we can get good pricing offers from Azure.
2. **Price Match with AWS –**This might not be known to all, but we can ask MS to do a price match.

**Azure Security Center**

**Introduction:**

In today’s world, Security has been a biggest concern for any application hosted/built in either on-premises or cloud and it is the foremost duty of a developer to prevent unwanted access to applications and prevent all other security issues. So security in the cloud is foremost important and it should also provide accurate and timely information about security.

**Azure Security Center:**

The Azure Security Center in Azure Cloud is a unified infrastructure security management system that can be used to strengthen the overall infrastructure and data security and provide advanced threat protection across various workloads such as Azure cloud or any other cloud providers or even on-premises infrastructure and data.

* When an application is being moved to Azure IaaS, the customer has more responsibility on securing the data when compared to moving to PaaS.
* So the security center offers various tools that can be used to harden the network and secure the various cloud services.

**The security center can be used to address the 3 major security challenges:**

1. **Strengthen the environment:**   
   The security center assesses the whole azure environment and all the resources deployed on it.   
   It understands the security status of the same.   
   By doing so, it provides detailed security related information.
2. **Protect against modern threats:**   
   Today we have various threats that can easily take over the application.   
   So a security center can be used to provide various threat prevention recommendations by assessing the deployed workloads and also provides timely security alerts.
3. **Secure the environment faster:**   
   Since the security center is natively built in azure cloud, it can be used to quickly secure the cloud environment and also protect against various threats.

**Key Pointers:**

1. Since the Security center is natively part of Azure, various PaaS services, SQL Database and storage accounts can automatically be monitored by the security center without making any additional deployment.
2. The Azure VMs are auto-provisioned in the security center when they are deployed and do not require any additional installations.
3. Security center can be used to protect not only azure services but also applications deployed in other cloud providers or even in on-premises infrastructures and applications.
4. To perform protecting non-azure infrastructures and applications, a log analytics agent needs to be installed in the external application.
5. Through the log analytics agent installed in the external systems, Azure will be collecting various information and the same will be processed in the security engine to provide detailed recommendations and actions to secure the data and the workload.
6. It is also very important that these recommendations should be considered and necessary actions should be taken. By doing so, the environment can be highly secured and malicious activities can be prevented.

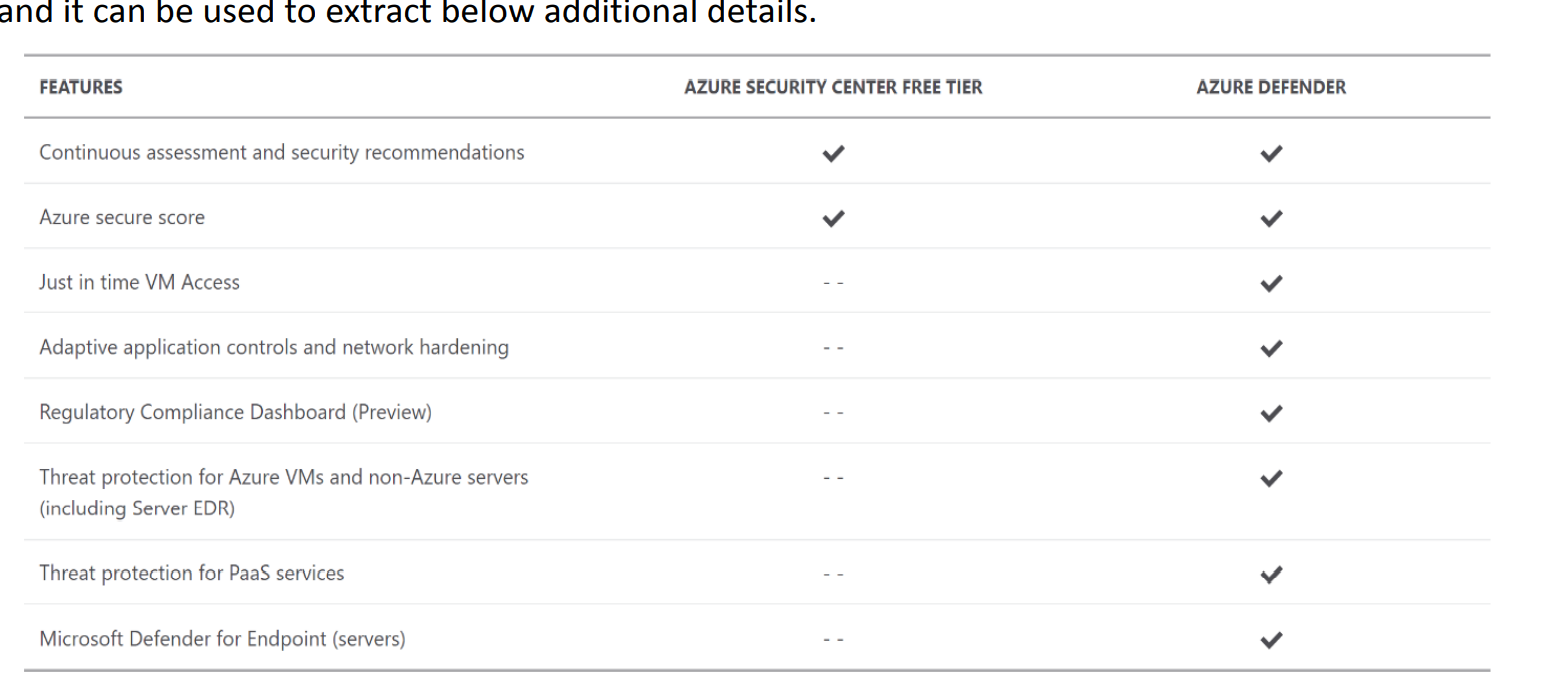
**Environment assessment:**

* The security center continuously monitors all the resources deployed in the cloud and provides various recommendations to secure it.
* Based on the recommendations, it also displays the necessary action to be taken to secure the resources.
* Also based on the analysis, it provides a security score which as per recommendation should be 100%. Below is the image of the security center portal.
* The details here are filtered based on a subscription in which it displays the security posture of various resources in the subscription.
* The red bar on the right denotes that the particular security recommendation “Remediate vulnerabilities” was not implemented and some resources may be affected due to this.
* If a recommendation is clicked, it displays further more information about the recommendations, severity of it and total number of affected resources.
* Also it is the user’s/Administrator’s choice whether to perform or skip a particular security center’s recommendation.
* It is not mandatory to perform all the recommendations and Microsoft does not produce any discounts/credits if the security score is kept 100%.
* If a user chooses to skip a recommendation, he/she can go inside the recommendation and give “Exempt” to overcome this recommendation.
* It is also possible to enforce a particular recommendation and by doing so, it will be creating a template deployment which will make sure to use the “DeployIfNotExist” policy and create the resource with this security recommendation.

All these recommendations and security alerts provided by the security center provides a great insight of what all security threats may occur to the resources and how to prevent it well before-hand.

**Cost of Azure Security Center:**

The azure security center itself is a free service but to have more features other than providing recommendations and actions, a paid service called the azure defender is available and it can be used to extract below additional details.



1. Just in time VM Access
2. Adaptive application controls and network hardening
3. Regulatory compliance Dashboard
4. Threat protection for Azure VMs and non-Azure servers ( Including server EDR )
5. Threat protection for PaaS services
6. Microsoft Defender for Endpoint ( servers )

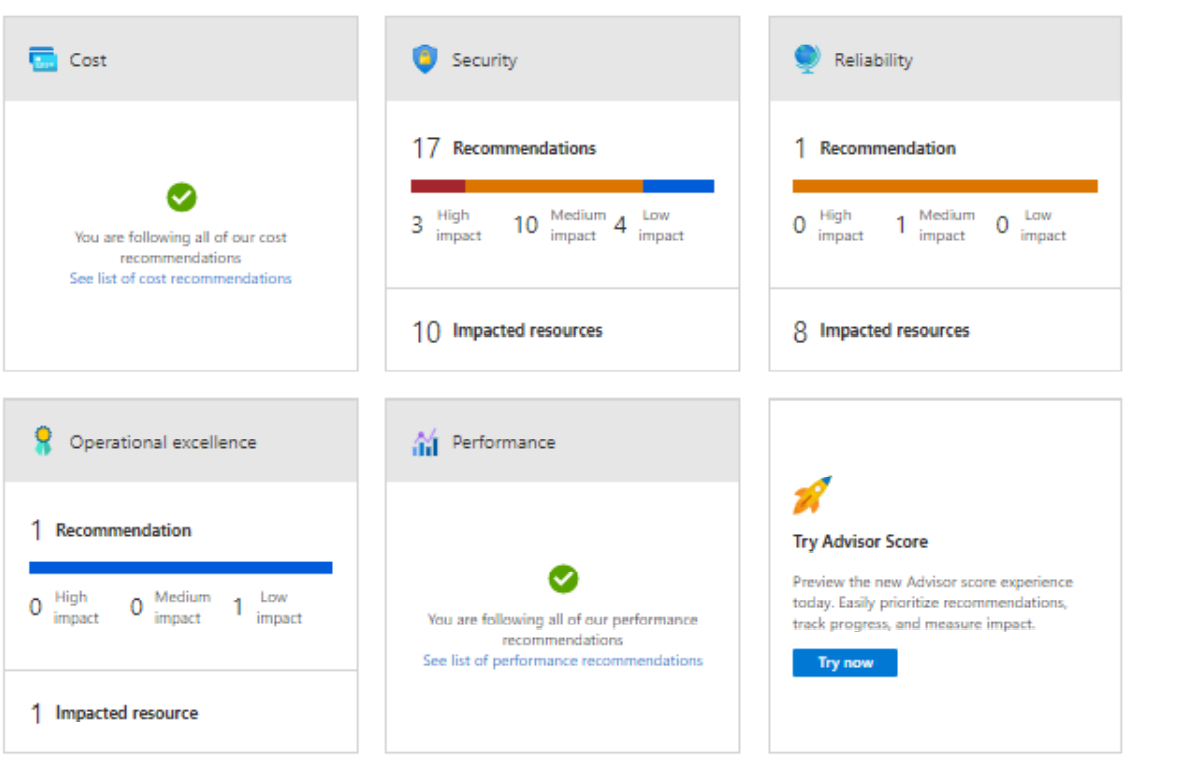
**Azure Advisor**

Azure has 5 pillars called the Azure well-architected framework which provides best practices to help build and deliver great solutions.

1. Operational excellence
2. Performance efficiency
3. Security
4. Reliability
5. Cost optimization

To enable customers to follow these best practices and optimize the cloud deployments, Azure has a free tool called Azure advisor. Azure advisor analyses the configurations and usage logs and offers recommendations which are customized and can be executed.

On each of the 5 pillars, we will be given recommendations to optimize. Please see below.



If we click on each of these recommendations, we can see what the recommendations are.

If we further click on each of the line items, we will give the list of resources that are not compliant and will provide manual and in some cases remediation action which can be deployed directly.

You can also note from the above that these recommendations are setup with the help of Azure policies.

* We can see the Policy definition and we can exempt the policy itself from being flagged as non-compliant.
* We can enable the deny action also in which case the resource will be prevented from being created.
* Here we have the policy which is audit and hence the resource is created and marked as non-compliant.

Sample remediation code:

{

"properties": {

"allowBlobPublicAccess": false

}

}

We can download these recommendations as a CSV or PDF file.

Azure Advisor also has 2 features in preview.

1. Security Advisor Alerts
2. Security Advisor Scores

One feature is alerts which are yet to be generally available (GA).

The other feature is the Advisor score which gives us on a percentage basis if we are following best practices

