CYBRARY

Study Guide

AZ-900 Microsoft Azure Fundamentals

Toddy Mladenov, Instructor
www.toddysm.com

Created By:
Samuel Mitchell
Teaching Assistant
August 2019

Introduction

This study guide is intended to prepare students for the Microsoft Exam AZ-900: Microsoft Azure Fundamentals. This study guide covers the main principles and explains the concepts of cloud computing and how those are implemented in Azure. Then, it explores the breath of cloud services offered by Microsoft Azure including compute, storage, networking and security. This study guide is intended for non-technical students who would like to get a basic understanding of the cloud and Microsoft Azure and achieve Azure Fundamentals certification.

Objectives

- Understand cloud concepts
- Understand core Azure services
- Understand security, privacy, compliance, and trust in Azure
- Understand Azure pricing and support

Prerequisite

- Basic computer skills
- Understanding how to use the command line
- Basic networking knowledge
- Enthusiasm and willingness to learn
- No prior knowledge of cloud or Azure

What else will you need?

- **Computer with an Internet** connection and a **browser**
- Operating System:
    - **Windows 10 users**: enable the SSH client features
    - **Other Windows versions users**:
        - PuTTY https://putty.org/ or another SSH client
        - CygWin https://www.cygwin.com/install.html

    - **MacOS users**: will need Remote Desktop Client
    - **Linux users**: will need Rdesktop https://www.rdesktop.org/
- **A Text Editor** (e.g. vscode https://code.visualstudio.com/download)
- ***PowerShell Core (Optional)***
    - https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell?view=powershell-6

About the Instructor

The instructor name is Toddy Mladenov and he is the Co-Founder of Agitare Technologies, Inc. which is a consulting and managed services company offering cloud services technology for health care, manufacturing and education companies. Toddy has 20 years of experience in technologies ranging from hardware to networking, software, architecting and designing during which 10 years is with cloud technologies. Toddy was one of the early members of the Azure team from 2009 to 2012 and from ever since he has a passion for the Cloud. Toddy was involved in numerous Azure projects which includes customers migrating from other cloud platforms such as AWS and Google. Toddy has his master's in Electronics and Automation while specializing in Information Technology. In his spare time, he enjoys skiing in the winter and biking or sailing in the summer.

Module 1
Principles of Cloud Computing

Module Introduction

In this module we are going to cover the following topics:

- What is cloud computing?
- Benefits of the cloud
- Compliance requirements and terms
- Capital and operational expenditures
- Cloud deployment models
- Cloud service models

Lesson 1.1: What is cloud computing

Skills Learned From This Lesson: Cloud Computing, Compute, Storage, Network

NIST Definition of Cloud Computing

*"The capability provided to the consumer is to provision processing, storage, networks, and other **fundamental computing resources** where the consumer is able **to deploy and run arbitrary software**, which can include operating systems and applications. The consumer **does not manage or control the underlying cloud infrastructure** but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."*

NIST SP 800-145 The NIST Definition of Cloud Computing
https://csrc.nist.gov/publications/detail/sp/800-145/final

Assessing the definition from NIST, there are a few important things to remember about the Cloud are:

- It allows you to provisions ***fundamental computing resources***: we will expound more on this later.
- It allows you to ***deploy and run arbitrary software*** which mean any software can run in the cloud
- You ***do not manage or control the underlying cloud infrastructure*** which means you have certain restricted to what you have access to or what you can control.

Cloud Computing and Utilities

Now let us compare Cloud Computing to what we are familiar with, electricity.

Everyone knows that when we turn the switch ON the light comes ON.

We never think actual what happens behind the scenes, how the electricity gets generated in the power plant and how it gets delivered to our house. If we press on the switch, the light goes out.

It is the same way with Cloud, the expectation is that when you press on the switch, a server or some computing power gets provision for you somewhere in the Cloud. It does not matter how that happens, it is important for you that you can use this computing power to run some application or store your data. If you don't need it, you can click a button and the server goes away.

What Cloud Resources Can You Rent?

Everything boils down to:

1. Compute
    a. The computing power that allows you to run algorithms, make calculations and run your applications.

2. Storage
    a. This is the ability to store data which can be personal data, purchase or images.
3. Networking
    a. This allows the communication between your client, your business client or the cloud or all the applications running in the cloud.

Compute Services

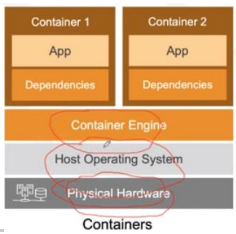
This is services that can be used to run your application, process a request or execute a business logic in order to do something for your client.

One of the ways to rent compute power is through ***virtual machines***. The virtual machines are virtualized hardware similar to your laptop or desktop that you use at home. However, instead of having real hardware, the virtual machines that presents this hardware in a virtual way.

Virtual Machines

The cloud provider has the physical hardware in their data center. On this physical hardware, they installed the host operating system. The host operating system is only accessible by the service provider. There is an abstraction layer on this host operating system which is called the Hypervisor. What the Hypervisor does is to virtualizes all of the physical hardware resources and present them to every customer that actual runs on this hardware. What this means is that the virtual machine is an actual representation of some part of the physical hardware that is given to you for its use. You have complete control over this virtual machine to install any arbitrary software required to run your application.

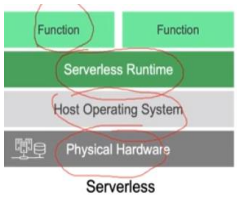
Another way to rent compute power is by using **Containers**. This is how it works, you will still have the physical hardware and the host operating system managed by the cloud service provider. The only difference is that there is a Container engine running on top of the host operating system which facilitates the use of Containers. The Containers provides a sandbox



Containers

environment for the customer to install the applications and their dependencies supporting the App. Once the Application has been satisfied with all it's dependencies, it can run on the container engine.

The last method of accessing compute power is using **serverless** runtime. Serverless is even less footprint which still run on the host operating system. The serverless runtime provides everything needed for the application to run. In this case, the particular applications are not called application but Function and is only a piece of code that executes a business logic. One thing to remember is that serverless or functions are only paid for while the code is executed. On the other hand, the virtual machine and containers are paid for while they are running whether or not the applications is executed.



Serverless

Storage Services

Let us look at the various types of storage services that can be rented in the cloud.

- Virtual Disk - it is used to store the data from the virtual machines.
- File Share - it allows multiple virtual machines to access the same data from a central location.
- Relational Database - you can create a database to store information for example from a shopping site.
- Document Database - this is a non-SQL database
- Blob
- Key/Value Storage
- Queue Storage

Network Services

- Virtual Network - this service is similar to your physical network where you can create a network in the cloud similar to your network on site.
- Global Traffic Management - this service allows a client to access the application from the nearest node to the customer network site for faster access.
- DNS - this is the services that resolves domain names
- Firewall - this is the services that protects your applications
- Load Balancer -

Video reference: https://cybrary.app.box.com/s/59zxq7d94ylpu3t6k7smywbjmr6gok7v/file/487510513718?sb=/details

Lesson 1.2: Benefits of cloud computing

Skills Learned From This Lesson: Cloud Computing, Cost, Benefits

Why is the cloud so important? Why does everybody wants to go in the Cloud?

- **Cost Effective**
  - You only pay for the usage
  - Pay-as-you-go / consumption based model
  - There is no upfront costs
  - You can stop paying for resources that you don't need
  - Better cost predictions
    - If you have spikes, you can plan for it

- **Scalable**
  - You have unlimited resources
  - Vertically scaling (scale up)
    - You can add more CPU or memory
  - Horizontally scaling (scale out)
    - You add more capacity by adding more servers
  - Manual or automatic scaling
    - You can use a script to auto scale the server
    - You can also manually add more servers

- **Elastic**
  - Increase or decrease based on demand
  - You can add more servers when during peak seasons
  - You can also reduce the servers during low seasons
  - Accommodate unexpected spikes
  - Reduce consumption during low use

- **Up-to-date**
  - You can leverage the latest hardware
  - You don't need a large investment to purchase new hardware
  - You get the latest software without paying for license fees

- **Reliable**
  - Redundant data centers
  - Redundant (fault-tolerant) services

    - Data backup and replication
    - Disaster recovery
        - Redundant generators
- **Global**
    - Redundant data-centers around the world
    - Closer to your customers
    - Meet data residence and compliance laws

- **Secure**
    - Physical security
    - Established policies and controls
    - Experienced personnel
    - Shared security model

- **Economics of Scale**
    - Efficiency
    - Lower cost per unit
    - Tax and utilities saving

Lesson 1.3: Compliance requirements and terms

Skills Learned From This Lesson: Azure, Compliance, Terms, CCM, NIST, HIPAA,CJIS, PCI-DSS, GDPR, ISO

Compliance

When you choose a cloud provider, it is important to understand how this provider can assist you to comply with the Standards and Regulations based on the industry that the business operates in.

Azure Compliance Offerings

Let us discuss a few of the compliance offerings in Azure. This is not a comprehensive list but it will demonstrate the extent that Azure goes to ensure that you have all that you need to run your application in the Cloud.
We will start with some of the generic security standards:

- Cloud Security Alliance Task certification
    - In order to achieve this certification, Azure need to achieve ISO 27001 certification
    - Also Azure needed to meet the criteria in the Cloud Controls Matrix
- National Institute of Standards and Technologies Cybersecurity frameworks (NIST)
    - This a voluntary frameworks that consist of standards, guidelines and best practices to manage cybersecurity related risks.

These are some of the industry specific certifications:

- AICPA SOC - Service Organizations Controls
    - There are three (3) levels of SOC
    - Microsoft services is audited against the SOC report framework annually using an independent auditor.
- Health Insurance Portability and Accountability Act (HIPAA)
    - It is a US federal law that regulates patient protected health information
    - Azure offers its customers a business associate agreement in compliance with security and privacy provisions in the HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).
- Payment Card Industry Data Security Standards (PCI-DSS)

    - PCI is proprietary information security standard for organizations that handles branded credit cards. Those are credit cards from the major credit card issuing companies such as Visa, Mastercard, American Express, Discover and JCB.
    - Azure is certified to host workloads that provides transaction information or processing according to the PCI-DSS standards.
- Criminal Justice Information Systems (CJIS)
    - If you develop applications for any US states or local agents and need to access to the criminal justice information services from the FBI. You need to adhere to the CJIS security policies.

The standards covered so far were mostly US-based. Next, we discuss some of the international standards:

- General Data Protection Regulations (GDPR)
    - This is one of the biggest regulations that took effective on May 28, 2018 in the european union.
    - This is a law that imposes new rules on anybody who collects private information from european citizens. This law in the GDPR applies no matter where you are in the world.
- UK Government GCloud
    - It is a certification for cloud computing, products and services used by government entities in the United Kingdom.
    - Azure has an official accreditation from the UK government for such services.
- Multi Tier Cloud Security Assessment
    - This assessment is conducted by the MTCS certification body which is apart of the Media Development Authority in Singapore

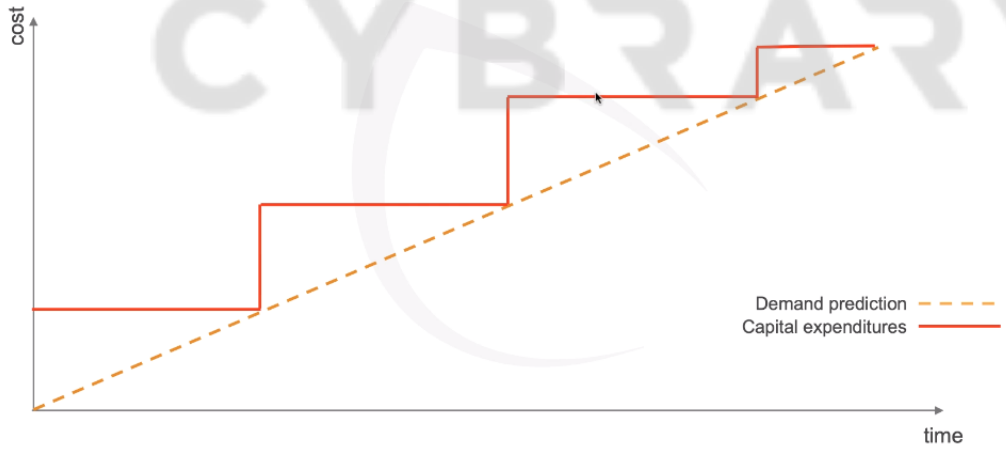
This list gives you a glimpse of some of the compliance offerings from Azure. For a complete list of the compliance, you can visit the Azure website listed as reference below.

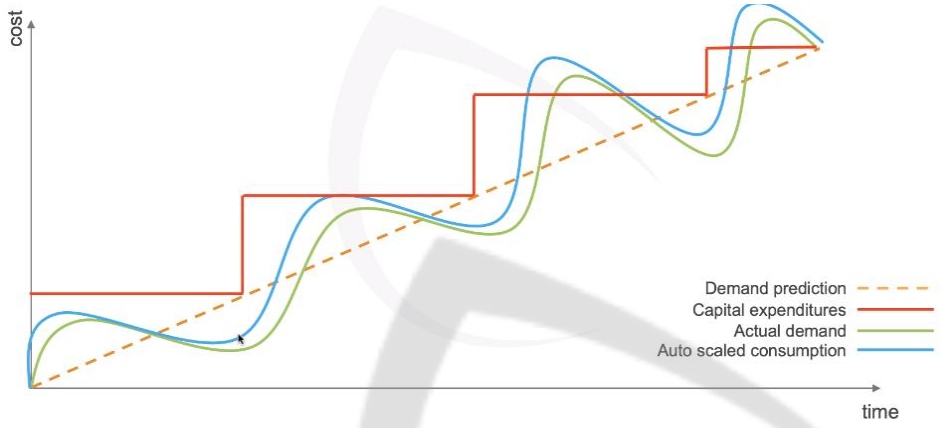
Reference: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

Lesson 1.4: CapEx vs OpEx

Skills Learned From This Lesson: OpEx, CapEx, Benefits, Budget, Cost

- CapEx
    - Is an upfront cost with value that reduces over time
    - Server costs
    - Storage costs
    - Network costs
    - Backup and archival costs
    - Business continuity and disaster recovery costs
    - Datacenter infrastructure costs
    - Technical personnel
- Benefits of the CapEx Model
    - Fixed cost
    - Budget-friendly
    - Easy of planning
- OpEx
    - Is an expense that you incur every month in which you consume services or products
    - Leasing cloud infrastructure
    - Leasing cloud software
    - Charges for scaling resources
    - Per-user billing
- Benefits of the OpEx Model
    -




cost
time
Demand prediction
Capital expenditures
Actual demand
Auto scaled consumption

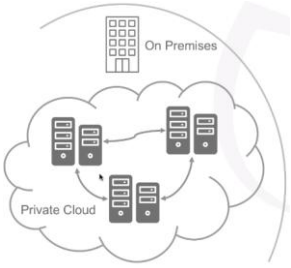
Lesson 1.5: Cloud deployment models

Skills Learned From This Lesson: Private Cloud, Public Cloud, Hybrid Cloud, Advantages, Disadvantages

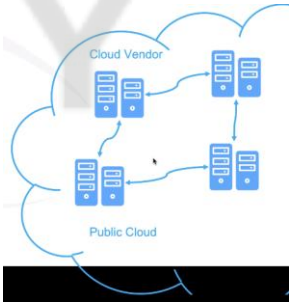
The Type of Cloud deployment models

The cloud deployment model defines where your data is stored and the application is running.

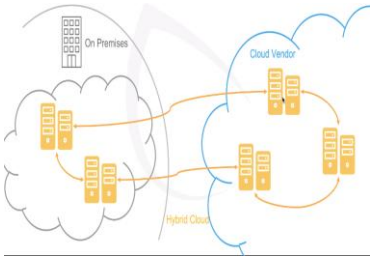
1. **Private Cloud-** your data or applications is running on-premise.
    - Advantages
        - Supports any scenario (legacy support)
        - Complete control over infrastructure and security
        - Meet security compliance and legal requirements
    - Disadvantages
        - Significant initial costs
        - Limits to agility
        - Demand for IT skills and expertise



2. **Public Cloud -** your data or application is running on infrastructure managed by cloud vendor such as Azure, AWS or Google.
    - Advantages
        - High scale and agility
        - Pay-as-you-go pricing
        - No hardware and datacenter maintenance requirements
        - Lower technical skills requirements
    - Disadvantages
        - Cannot support all legacy scenarios
        - May not be able to meet all compliance needs
        - No control over hardware and services
        - Some security requirements may not be met



3. **Hybrid Cloud -** some of your data or application is running on-premise while part of it is running on infrastructure managed by a cloud vendor.
    - Advantages
        - Can support any scenario including legacy
        - Flexibility of choice for applications
        - Implement specific security and compliance requirements
        - Take advantage of economies of scale
    - Disadvantages
        - Requires initial investment
        - May be hard to set up and maintain

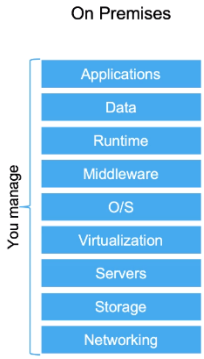


Lesson 1.6: Cloud Service Models

Skills Learned From This Lesson: Cloud, Service, Models, IaaS, SaaS, PaaS, On-premise

NIST outlines three different service models that are crucial for understanding the cloud. Those three service models are compared to the traditional model for hosting software application in your own datacenter also called on premises model.

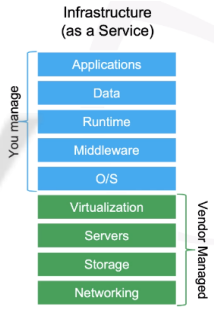
On Premises



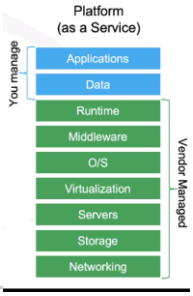
- You are responsible for buying and setting up and managing the host for your applications.
- This includes hardware like network, storage and servers
- You are also need to installing the virtualization, operating system and set up any middleware and runtimes that your application needs.
- Last you need to deploy your application and manage the data it stores and uses.

The Type of Cloud Service Models

1. Infrastructure as a Service (IaaS)
   - It is similar to the on premise model except the cloud vendor is responsible for managing the physical hardware and virtualization.
   - It gives you complete control over the operating system and the rest of the stack
   - You don't have to worry about spending money on buying hardware,acquiring a building or pay utilities.

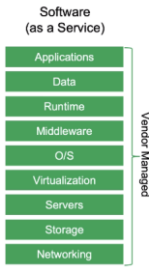


2. Platform as a Service (PaaS)
   - In this model, the vendor manages everything else except your applications or data



- This useful for rapid development of applications because the applications team don't need to spend time managing the infrastructure or the runtime components.

3. Software as a Service (SaaS)
   - In this model the cloud vendor manages everything and you just consumes to software.



Module Summary

In this module we have completed the following topics:

- Cloud computing definition
    - Cloud Computing
    - Compute services
    - Network Services
    - Storage services
- Benefits of the cloud
- Security standards and compliance requirements
- Expenditure models
    - CapEx
    - OpEx
- Cloud deployment models
    - Private Cloud
    - Public Cloud
    - Hybrid Cloud
- Cloud service models
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
    - Software as a Service (SaaS)

Module 2 Introduction to Azure

Module Introduction

In this module we will learn more about Azure.

The list of topics covered in this module are:

- What Azure is and what it offers?
- Brief history of Azure
- And explore the Azure services

Lesson 2.1: What is Azure?

Skills Learned From This Lesson: Azure, Fabric Controller, Orchestrator, Virtualization

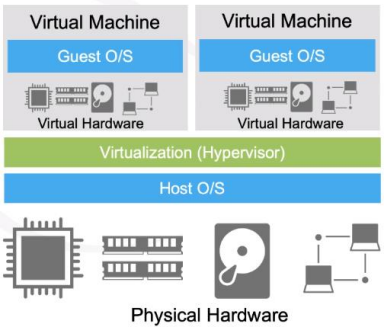
What is Azure?

1. Azure is Microsoft's cloud computing platform
2. Azure gives you the tools to build, manage and deploy applications on a global scale
3. Azure is targeted for developers and IT teams unlike Office365 or Microsoft 365 which is offered as a SaaS to the end-users.
4. Azure offers 100 or more services that allows you to accomplish different scenarios from running legacy applications from virtual machines to developing advanced machine learning model to building bots with artificial intelligence.

Virtualization

Let's see now how Azure works behind the scenes. To offer its cloud services, azure uses a technology known as virtualization. In the previous module, we looked at the application stack and one of the components was known as Virtualization. It fits right above the hardware and it is apart of the host operating system.
Virtualization is a technology that represents the underlying hardware as software. This is how it works:

- You have the actual server of physical hardware components such as CPU, memory, disk drives and one or more network interfaces.
- You install an operating system which is called the Host operating system.
- Every modern operating system has a feature called hypervisor that you can turn on, that all of this feature is to represent the signals from the physical hardware as software equivalent that can be used on Virtual machines that starts on the host.



- In addition to the function mentioned, the hypervisor has few other important functions:
    - It ensures that no one virtual machine consumes more resources than what was allocated to it.
    - It ensures that the data written to the physical disk by one virtual machine cannot be accessible by another one. This function is also true for data in memory.
    - It exposes programming interfaces which allows you write software that tells the hypervisor what to do. For example, to create a new virtual machine with certain parameters for the virtual hardware.

There are other functions performed by virtualization but those are the important ones now.

Azure Behind the Scenes

This is how azure works behind the scenes:

- In each datacenter operated by Microsoft, there are hundreds or thousands of racks full of hardware servers.
- Each hardware servers has Windows server operating system installed on it with the hypervisor features enabled. This means that you can run multiple virtual machines on each hardware server.
- A network switch provides connectivity to each one of the servers in the rack.

Fabric Controller

- One server in each rack runs a special software calls a Fabric Controller.
    - This software is responsible for managing the servers in the rack.
    - It communicates with the hypervisor in each rack which instructs them to create a virtual machine, dedicated storage or configure the networking.
    - All Fabric Controllers in the datacenter are managed by a centralized software called an Orchestrator

Orchestrator

- The Orchestrator is responsible for managing the resources in the entire datacenter in contrast to the Fabric controller which is responsible only for one individual rack.

Now you know what Azure is, what technology it uses and how it operates behind the scenes.

Lesson 2.2: Brief History of Azure

Skills Learned From This Lesson: Azure history, Red Dog, PaaS

Azure History

Although it is not important for any exams or certifications,knowing a bit aboutAzure history will assist you in casual conversation.

5. Azure started off as a Microsoft research project called “Red Dog”
6. It was official announced in the Microsoft professional developer conference in the fall of 2008.
7. It was free to use for almost one and a half year.
8. Platform as a service (PaaS) was the focus of the project at the time.
9. There were a few services that was offered at the time: Compute which was called Cloud services and Storage services which involved Blob, tables and cubes.

- In 2011, Scott Guthrie took over large parts of Azure; initially the developer experiences and later on the complete platform.
- At this time, Azure started to add more services to it’s platform and became a viable competitor to AWS.

In the next lesson, we will take a 30,000 foot view of the Azure services.

Lesson 2.3: Azure services

Skills Learned From This Lesson: Azure Services, Infrastructure Services, Security and Management, Platform Services and Hybrid Cloud

Now let us take a quick look at the different services offered by Azure. As previously stated, Azure offers more than 100 services. Official Microsoft offers 21 categories of services as listed below:

1. AI and ML
2. Analytics
3. Blockchain
4. Compute
5. Containers
6. Databases
7. Developer Tools
8. DevOps
9. Identity
10. Integration
11. Internet of Things
12. Management and Governance
13. Media
14. Microsoft Azure Stack
15. Migration
16. Mixed Reality
17. Mobile
18. Networking
19. Security
20. Storage
21. Web

Keep in mind that some services can fall into more than one category For example, Azure Kubernetes can fall into two categories:

- Compute
- Container

The important thing to note is that the variety of services Azure offers, gives you the ability to practical do anything you want.

Another way to look at the Services:

There are 4 four main categories:

1. **Infrastructures Services:**
   This category includes the following services.
   a. Compute
      i. This service include Azure VMs and Azure Kubernete service
   b. Storage
      i. This service include Blob, Files, Disk and Queue
   c. Networking

i. This service includes virtual network, load balancer, DNS, express route, traffic manager, VPN gateway and application gateway.

2. **Platform Services**

This category can be split into the eight (8) sub-categories:

a. Compute
   i. This category includes services like Azure Batch, VMs scale sets and Dev test labs
b. Data
   i. This category includes services like Azure SQL, Cosmos DB, Azure Cache for Redis and Table Storage
c. Integration
   i. This category includes services like API Management, Logic Apps and Service Bus
d. Application Platform
   i. This category includes services like Web Apps, Mobile Apps, API Apps, Functions, Service Fabric and Notification Apps.
e. Developer Services
   i. This category includes services like Application Insights and developers tools and frameworks such as Visual Studio and Mobile Engagement in Visual Studio App center.
f. Media and Content Delivery
   i. This category includes services like Media Services, Media Analytics and Content Delivery Networks.
g. Intelligence
   i. This category includes services like Machine Learning.
h. Analytics and IoT
   i. This category includes services like HDInsight, Stream Analytics, Data Catalog, Data Lake, IoT Event and Data Factory.

3. **Security and Management**
   a. This is the 3rd category which include services like Security Center, Azure Active Directory, Key Vault, Azure Portal, Azure Automation, RestAPI and Command Line interfaces.
4. **Hybrid Cloud**
   a. This is the last category which includes services like Azure AD Connect, Health, Backup and Site Recovery and Azure Monitor.

Now you have a quick glimpse of the Azure services that can assist in developing your applications.

Module Summary

In this module you have learnt:

- What is Azure?
- What technologies Azure leverages?
- How Azure works behind the scenes?
- Brief history of Azure?
- Overview of the Azure services?

In the next module, you will learn the Azure Global Structure and what are the Service Level Agreements.

Module 3
Azure Global Infrastructure and SLAs

Module Introduction

In this module, we will learn about:

- Azure datacenters and regions
- Availability zones
- Service SLAs
- Calculating application SLAs

Lesson 3.1: Azure Datacenters and regions

Skills Learned From This Lesson: Azure Datacenter, Azure Global Infrastructure, Azure Geographies, Azure Region, Region Pair

Let us see how Azure is able to provide it services around the world.

This is a map of Azure services around the world:
reference: https://azure.microsoft.com/en-us/global-infrastructure/regions/

- Each blue dot on the map represents a region. A region is a geographical area with at least one data center but sometimes multiple datacenters. Azure controls the resources in each region to ensure that they are appropriately balanced.
- When you create a resource in Azure, you may be required to select a Region. Some services are only available in certain regions.
- For example, not all virtual machines sizes are available in all regions.

- There are services that are available global and does not require selecting a region such as Azure Active Directory, Azure Traffic Manager and Azure DNS.

10. You should note that there is a certain limit of resources that you can create within a regions. If you reach this limit, you should create a support ticket to extended the limit or create the resources in another region where this limit has not been reached.
11. Some regions are special and you can use them for building applications that meet certain compliance or legal requirements. You may also not be allowed to port to those regions if you don't need those compliance requirements.
12. The US Government and the Department of Defence regions are viable for US government agents and partners. They are operated by personnel with higher clearance and have additional security clearance.
13. China Regions are offered in partnership with third party providers and Microsoft does not maintain the data centers.
14. Germany Region are viable via German data trustee models where the data trustee is the Deutsche Telekom company called T-Systems International. This is the company that ensures the data resides in Germany.

Why Azure needs so much data centers in so many regions?

- It allows you to bring your application and your data closer to your customers.
- It provides better scalability and redundancy
- It reserves the data residence for your user and assist to stay compliant with your users requirements.

Azure services are offered in four (4) Geographics

15. Americas
16. Europe
17. Middle East and Africa
18. Asia Pacific

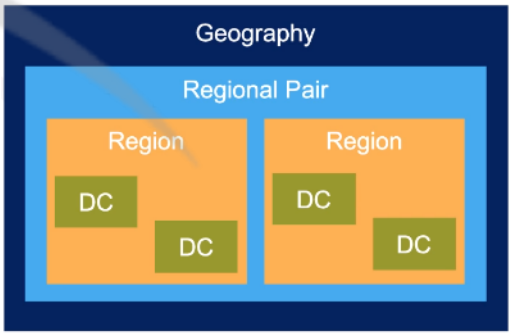
A geography is described market with two or more regions that reserves residence and

compliances boundaries. Why does Azure subdivided into geographies? There are some legal and compliances reasons which are:

1. They ensure that data residence and sovereignty requirements are hang up within the geographical boundaries.
2. They are fault tolerant to withstand complete region failure.

One typical example of data residence is with the law of the GDPR which requires the data of european citizens must remain on European soil.

Region Pair



Another important point about the geographies is that every region is paired with another region within the same geography which is called a Region Pair.

19. Region pair is helpful when considering Business Continuity and Disaster Recovery (BCDR) plan
20. Region pair must be directly connected and must be at least 300 miles away from each other. This ensures that in the case of a disaster that your workload will still continue running even if one of the regions is down.
21. Some services offer automatic geo-redundant data replication of data using region pairs.
22. One advantage of Region pair is that in the case of extensive Azure outage, one of the regions is prioritizes to reduce the downtime.
23. Planned updates are rolled out to the regions one at a time.
24. Data continues to reside within the same geography even if disaster occurs.

Examples of Regions Pairs

- East US/West US

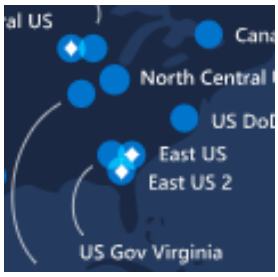
25. North Europe/West Europe
26. East Asia/Southeast Asia
27. Exception: Brazil South/South Central US

In the next lesson, we will cover what redundancy is provided within the same region.

Lesson 3.2: Availability zones

Skills Learned From This Lesson: Availability Zones, Data center, Region

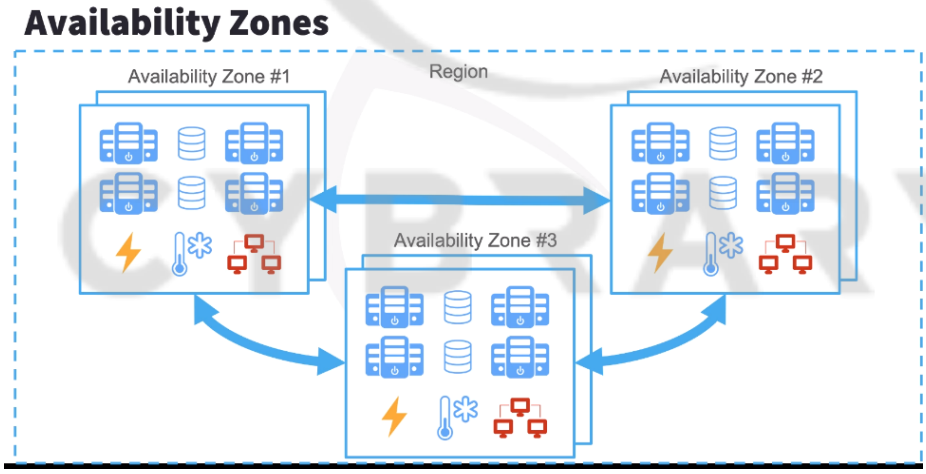
Let us look at how Azure provide redundancy within a Region.
If you look closely at the map, you will see that some region has a diamond and the legend states that those are Availability Zones. Examples are West US 2, Central US and East US 2.



What are Availability Zones?

- Availability Zones are physical separate data centers within a region.

28. Unlike Region pair that needs to be at least 300 miles apart, Availability zones are in a closer proximity and are connected through a private high speed fiber optic network.
29. Each Availability Zones are consist of more than one data centers equipped with its own power, cooling and networking.



30. Similar to the region pair, if one goes down , the other continues working.
31. Availability Zones are important for core infrastructure services such as virtual machines, managed disk, ip addresses, load balancers or SQL databases.

32. You can architect your application for high availability by co-locating you compute, storage, networking and data resources within a single availability zones and duplicate the same resources into another zone.
33. Be aware that there may be a cost for duplicating your resources in multiple zones.

There are two categories of resources that support availability zones:

1. VMs, managed disk or IP Addresses whether you specify via availability zones at creations.
2. Storage or SQL database services where the platform automatically replicates across zones.

This brings us to Service Level Agreement.

Lesson 3.3: Azure service SLAs

Skills Learned From This Lesson: SLA, Service Credit, Performance Targets

What are Azure Service Level Agreement (SLA)?

- Service Level Agreement (SLAs) is a formal document that specifies Microsoft commitment to operate the service.
- SLAs defines the performance targets such as uptime and connectivity guarantees that applies to that service.
- SLAs also outlines what happens if the performance targets are not met or the service does not meet the specific standards which could include services credits.
- Every product or service in Azure has their own SLAs. For example virtual machines will have their own SLA different from storage which will be different from Databases.
- There are also some special requirements on how the product/service should be used or configured in order to meet the SLAs.
- It is therefore important to read the conditions of the SLAs of the service you plan to use, to understand the impact of the services on your application.

Performance Targets

- Very often the performance target of the services is expressed in the form of Uptime and Latency.
- Typical example is the Azure Cosmos DB with 99.999% uptime and 10 ms latency on db read and write operations.
- You will hear that services will have three nines (99.9%) or five nines (99.999%) which is usually referred to the service uptime expressed as a percent.
- Below is a table that shows the SLAs expressed in percent while the downtimes are expressed in hours.

SLA %	Downtime/Week	Downtime/Month	Downtime/Year
95%	8h 24m 00s	1d 12h 31m 27s	18d 6h 17m 28s
99%	1h 40m 48s	7h 18m 18s	3d 15h 39m 30s
99.9% "three nines"	10m 05s	43m 50s	8h 45m 57s
99.999% "five mimes"	6s	26s	5m 16s

    - The table shows that for three nines (99.9%) SLAs, the services is guaranteed to not be inaccessible for more than 43m 50s for the month while for five nines

(99.999%) SLA, the service is guaranteed to not be inaccessible for only 26s. This tables show a huge difference in the SLAs.

Service Credits

34. Based on Azure Cosmos DB SLA with 99.999%, you should expect that the service should be available all the time. If this is not the case, you can complain to Microsoft and you should be credit for the services lost.
35. If Microsoft is not able to maintain the performance targets for an Azure services. They are committed to compensate you for that. This compensation could be in the form of a credit to your monthly bill for that particular service.
36. The following table shows what service credit you are able to receive for services that does not meet the specified SLAs.

Uptime	Service Credit
< 99.9%	10%
< 99%	25%
< 95%	100%

37. What the table shows is that if the services uptime is less than 99.9% or three nines, you will receive a 10% service credit towards your bill.
38. Please note that the service credit is only towards the under performing service.
39. For example if you are using virtual machine and storage services, if the performance is low is due to the virtual machine. You will only receive credit towards the virtual machine but you will still need to pay the full bill for the storage consumption.

To request a credit, you will need to make a service request to the Azure support team. We will learn how to do that in a future lesson.

Lesson 3.4: Calculating application SLAs

Skills Learned From This Lesson: Resiliency, Availability , Cost, Calculation, Services, SLAs

How Azure SLAs can impact your Application?

- Any system can experience a failure. Hardware breaks, networking has trojans and failures and software has bugs and crashed.
- Even with all the redundancies built into Azure, services and sometimes an entire regions can still have disruptions.
- Amongst the many things that you need to think about when architecting your application is also it's reliability.
- Knowing your application requirements can assist you in making a more informed decision of what Azure services to use to achieve your application performance goals.

Resiliency, Availability and Cost

- Using Azure SLAs in your application architecture, you can build your own application SLAs that you provide to your customers.

Application SLAs =∫ (Azure SLAs)

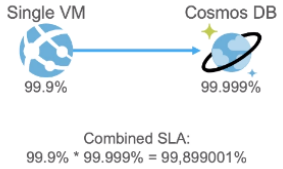
40. Resiliency is the ability of a system to recover from failures. The aim is not to prevent failures but to avoid downtime and prevent data loss.
41. Important components of Resiliency is High Availability and Disaster Recovery.
42. When designing your application, you should design for resiliency.
43. One of the common traps that application designer falls into is designing the application to maximize high availability but implement measures to prevent failures. A challenge with this methodology is that implementing measures to prevent failures can be difficult and expensive. Preventative measures also complicate the system.
44. Increase Availability always includes increase complexity which then increase cost.

SLA considerations

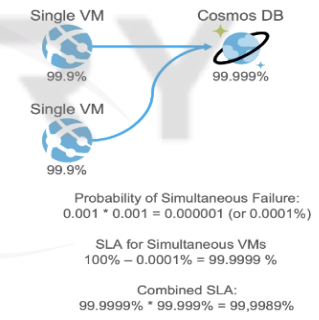
There are a few key areas to consider when designing your application SLAs:

45. The level of automation built in your application. If your application requires manual intervention and has no built-in self healing capabilities. Achieving high SLAs will be difficult.
46. SLAs higher than three nines (99.9%) is harder to achieve. You should ensure that the effort warrants the return on investment.
47. The smaller the time windows for your performance target, the lower is it's tolerance to consider. Do not use hourly uptime in your SLAs, a small failure can throw off your metrics.

Calculations of Application SLAs



- Here is how you can approach the calculations of your Application SLAs:
- Let us say that you have a single VM for storing data in Cosmos DB.
- The VM SLA is 99.9% and Cosmos DB SLA is 99.999%.
- To get the SLA for this Application, you will multiply both SLAs (99.9% * 99.999%) to achieve the Application SLA of 99.899001% which is less than each individual SLAs.
- If this Application SLA is not satisfactory, then you can add another VM to the architecture.
- The probability of simultaneous failure:
  [single VM failure] * [single VM failure] = [0.001] * [0.001] = 0.000001 (0.0001%)
- SLA for simultaneous VMs: 100% - 0.0001% = 99.9999%
- Combined SLA: 99.9999% * 99.999% = 99.9989%
- This demonstrates that you can achieve a much higher SLA which is much closer to the SLA of Cosmos DB.
- You will notice that the complexity and redundancy has increased with the addition of a new VM which will require maintenance and incur additional cost.



Now you know how Azure SLAs can impact your application and how to combine services to improve those.

Module Summary

In the module we have covered the following topics:

- Regions, Region pairs and geographies
- Availability Zones
- Azure SLAs
- Application SLAs

Module 4
Azure Account

Module Introduction

In this module we are going to cover the following topics:

- Azure account and subscriptions
- Introduction to Azure Active Directory (AAD) and Azure Billing
- Azure support options

Lesson 4.1: Azure accounts and subscriptions

Skills Learned From This Lesson: Azure Account, Azure Subscription, Type of Accounts

Azure Account

- Azure Account is associated with a specific identity which can be your email address.
- In addition to the email address, this information can contain your name , contact details and payment information.

Two types of Azure account

1. Work/School which is issued by your employer.
2. Personal - you can sign up on any microsoft web property.

Sign into Azure Management Portal

- You can use your Microsoft account to sign into Azure web portal to access any resources.
- If you have signed up for any microsoft services such as Office 365, Outlook email or XBox Live, you already have a Microsoft account that you can use to sign up for Azure.

Azure subscription

- You can use your Azure account to create more than one subscription.
- Azure subscription is logical grouping of resources.
- You can use subscriptions for various purposes.

Types of Subscription

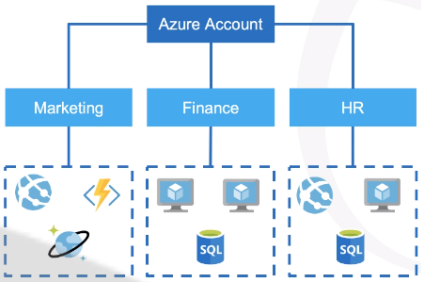
- Free subscription
    - It offers $200 US to spend in the first month.
    - Free access to some of the most popular Azure services for 12 months.
    - Access to 25 services that are always free within some limit.
    - For example: you can create 10 Web Mobile apps for free up to 1 Million function request per month without charge.

    - To create a free account you need a Microsoft account, phone number and credit card information for verification purposes.
    - No charges will be billed to the credit card and if your charges reach the $200 limit. All resources that are billed will be shutdown.
- Student subscription
    - This subscription is also free and offers $100 credit to be used within 12 months.
    - It also includes the same set of standards such as the free one.
    - It does require a credit card to sign up but you will need to prove student status by signing up with your educational email address ending with edu.
- Pay-as-you-go (PAYG)
    - This is a regular paid subscription for services at retail price.
    - It is appropriate for every type of Azure customers from individual to corporate customer who does not want any terms commitment for consumption.
- Enterprise Agreement (EA)
    - This subscription offers the option to buy cloud services and software licenses under the same agreement.
    - This option is offered with some discount rate and software assurance agreement but requires the customer to commit to a minimum annual spending amount. This amount can be spent for Azure services, additional support or software licenses.
    - This option is target for Enterprises.
- Cloud service provider (CSP)
    - CSP subscription can be purchase from Microsoft authorized partners.
    - It is usually bundled with additional services offered by the Microsoft partners.

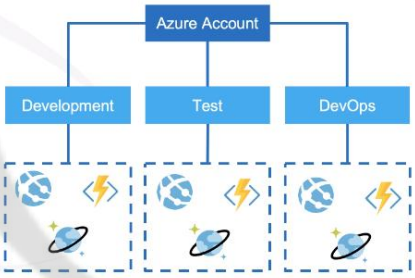
Multiple subscriptions

As we mentioned you can have multiple subscription under a microsoft account:

- One way to utilize the multiple subscription is create a subscription for each Department within your organization. This subscription will the billing and resources to be handled by one department within the company.



- Another way is to create multiple subscriptions for different teams in the company. Each team will be responsible for their individual resources.

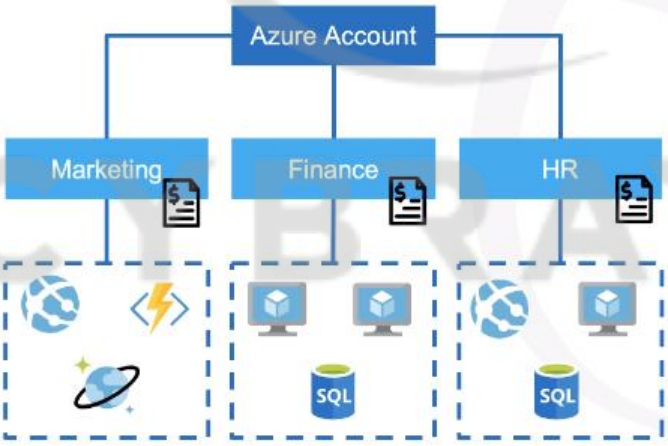


Lesson 4.2: Introduction to AAD and Azure billing

Skills Learned From This Lesson: AAD, Billing, Azure, Services, Tenants, Subscription

Let us see how Azure bills you for the resources and how you can restrict access to company resources.

Azure Billing

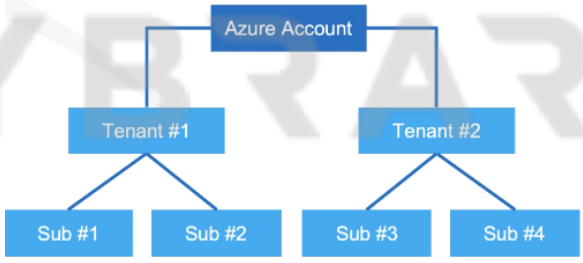
1. We will use the previous example of having subscriptions for each department within the enterprise.
2. A billing is generated for each subscription on a monthly basis.
3. Charges show up 10 days after on the associated credit card after billing period ends
4. Although the subscription are billed, the account owner is still responsible for the bill payment
5. In our example, the Marketing, Finance and HR department will have their separate bill in which you can apply towards the budget of each department.
6. In this way, you can keep track of the departments individual spending and you are better enabled to control their individual cost.
   - 

7. You can also use different payment option for different subscriptions. For example, different credit cards for each department.
8. You can create a budget for each department and get notified if the department exceeds it's budget.

9. If you need additional tools for managing the billing process, there is a tool called the Cost Management and Billing service that you can use to get a better understanding of you billing charges and drill down into these costs.

Azure Active Directory

- Restricting access to resources and services is crucial for security in the cloud.
- Authentication in Azure is performed by Azure Active Directory or AAD
- Azure Active Directory is a cloud-based identity provider that supports multiple authentication protocol that includes modern standards like Open ID and OAuth.
- You can use AAD to register users, applications, create groups and identities which makes it a complete directory services.
- Entities that registers with AAD are not handled by a single instance of the service. instead , Azure Active Directory are partitioned into tenants,
- A tenant is an isolated dedicated instance of Azure Active Directory and is managed by a single organization.
- Azure Active Directory is used by other cloud services in Microsoft including Office365, Microsoft Intunes and Dynamics365.
- When you sign up for any microsoft services, an instance of AAD is automatically created for you.
- Keep in mind that there is no one-to-one relationship between your organization and the Azure Active Directory tenants.



10. Each one of the tenants can have multiple subscriptions associated with it.
11. Each tenant has only one account.
12. A subscription can be associated with a single tenant.
13. You can transfer subscriptions between tenant if you need to.

Using Azure Active Directory, you can manage access to every resources and subscription underneath individually.This gives you a lot of flexibility to model your organization access within Azure.

Lesson 4.3: Azure support options

Skills Learned From This Lesson: Azure Support type, Support Ticket, Azure Documentation, Azure subscription

The last thing we will look at in this model is Azure support options.
Microsoft offers two options for Azure support:

1. Free
2. Paid

Free Support

This options include:

14. Billing and subscription support
    - If you have any questions about your bill or subscription, you can submit a ticket in the Azure portal.
15. Twitter support account @AzureSupport
    - Azure support team can be contacted via their twitter account but remember that it is a public interface so ensure that you do not include any private or confidential information.
16. Azure Knowledge Center
    - This is a searchable database with solutions to common support problems.
    - This database is built by a community of Azure experts, users and developers.
17. Azure Documentation
    - This official documentation is freely available on Azure website which includes quick guide and tutorials along with references of APIs, SDKs and much more.
18. Community Forums

    There are several community forums where you can ask questions and post answers about Azure. Some forums are:
    - MSDN (Microsoft Developer Network) forums
    - Stack Overflow - for developers related questions
    - Server vault - for administrative and management questions

Paid Support

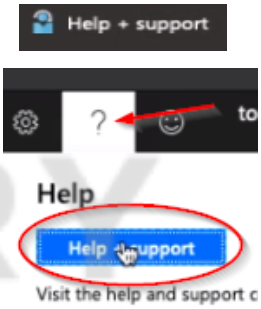
Microsoft offers several paid options for support which is targeted for customers who require deeper technical and operational support.
Those include:

1. Developer
    a. This support is the lowest level of paid support and it is intended for trail and non-production environment.
    b. Support is only available via email and response can take up to 8 hours.
    c. Hence, this support should not be used for issues with business impact.

    All other support options are available 24/7 with email and phone support.
2. Standard

    These other support offers additional services such as architect guidance delivered by solution architect and additional levels of training.
3. Professional Direct
4. Premier

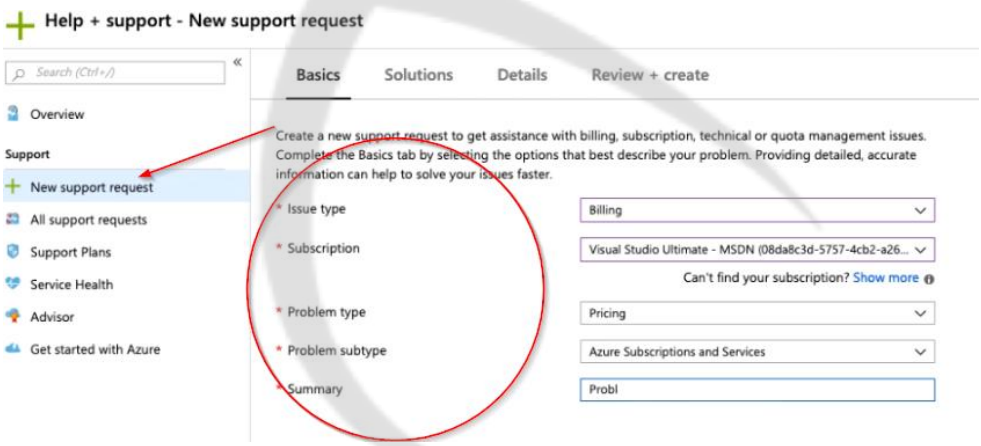
Submitting a support Ticket



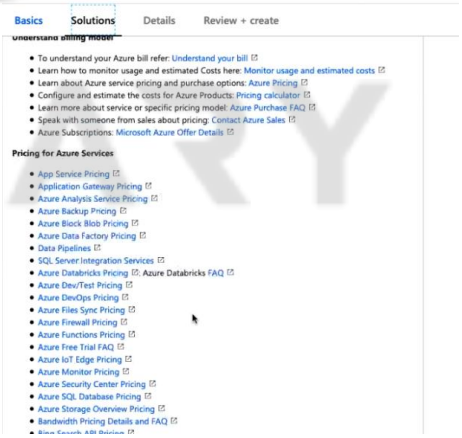
You can use the Azure portal to submit a support ticket.
To submit a ticket you will select the help + support icon or the question sign:

- Once you are on the Help + Support page
- Select New Support request
- Select the Issue type:
    a. Billing
    b. Service and subscription limits (quotas)

    c. Subscription management
    d. Technical
        - This type requires a support contract
- Next select your Subscription
- Next select Problem type
- Next select Problem subtype
- Enter your problems



The support portal suggests a list of solutions to the common problem types before you submit a ticket.



If you do not use any of the suggestions, you would select Next Details:

- Enter the start and end date
- Provide more details about your issue
- Select the Severity
- Then the preferred method of contact:
    - Phone or Email.
- Then you will submit your ticket.

Module Summary

The following topics were covered in this module:

- What is Azure Account?
- Azure Subscriptions
- Azure Billing
- Azure Active Directory
- Azure Support options
- Submitting an Azure Support Request

Module 5
Azure Management Portal

Module Introduction

In this module you will learn the following:

- Azure Management options
- Azure Portal
- Portal Dashboards
- Private and public preview features.

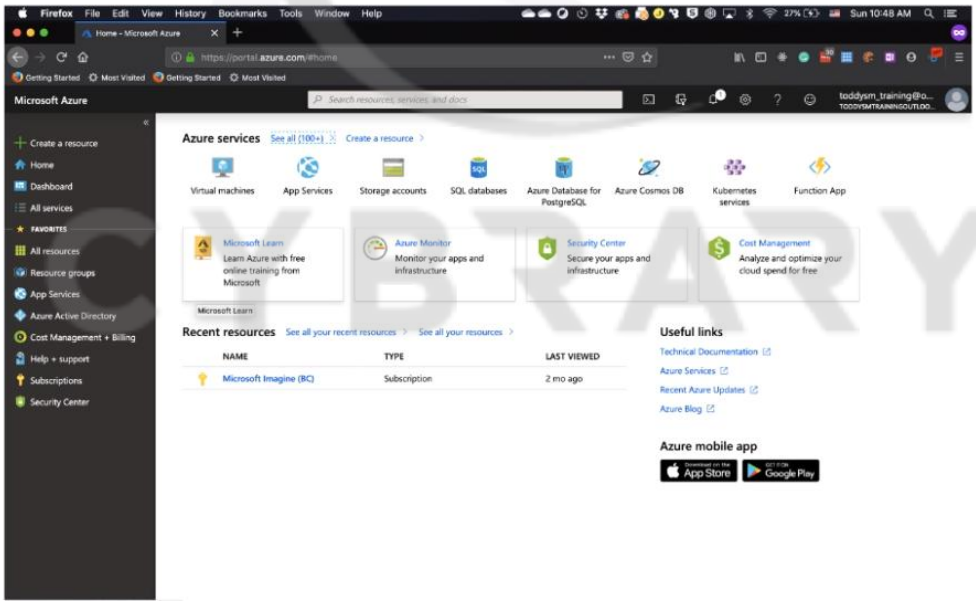
Lesson 5.1: Management options in Azure

Skills Learned From This Lesson: Azure, Management, Portal, CLI, Cloud Shell, PowerShell, Mobile App

What options do you have to management Azure resources?

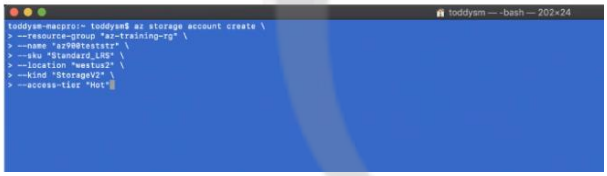
Microsoft Azure offers a wide range of options; there web app, mobile options, command line options as well as numerous SDKs that you can use to implement you own management functionality.

- Azure Portal:
    a. This option is where most novice user starts with.
    b. The Azure Portal is a web-based management portal that allows you to access it using any web browser. It is the best way to learn about Azure.
    c. Although great for learning, the Azure portal does not allow you to automate tasks which makes its use time consuming.

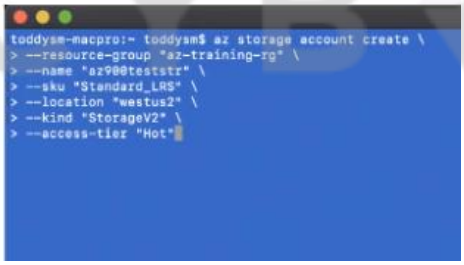


- Azure Powershell
    a. It is a module that you can install in PowerShell on Windows, Linux or MacOS
    b. This module adds additional cmdlets to Powershell to allows you to manage Azure resources.
    c. Using Azure Powershell, you can create administrative scripts and automate your workflows instead of spending time doing this manually in the portal.
    d. You can run this script on any operating system using the powershell core. Although powershell core is cross-platform, it does not come pre-installed in the operating system.
    e. Thus, if you want to use powershell as your scripting language, you will need to install the PowerShell first and then install the Azure PowerShell module.

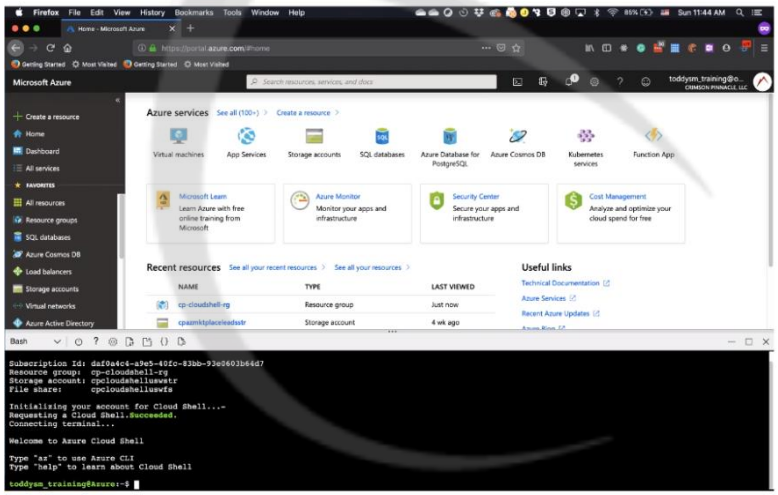
Installation reference: https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell?view=powershell-6



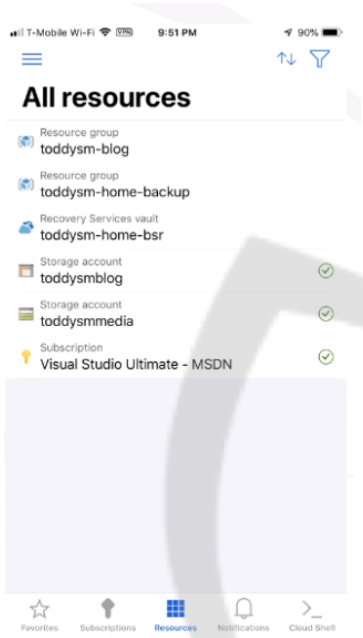
- Azure CLI
    a. It is a cross-platform command line tool that you can use to create and use resources in Azure.
    b. It is Python-based and can run on any OS with python installed.



- Azure Cloud Shell
    a. It is a powerful command line interface that is run within your browser and it is access from the Azure portal.
    b. Cloud Shell give you the option of using Azure CLI or PowerShell cmdlets.
    c. In Addition to the CLI, cloud shell has a lot development tools available like Python, .Net, NodeJS, Java and Go.
    d. Cloud shell is backed by an azure file share drive where you can upload your reference scripts or attached to your local drive.



- Azure Mobile App
    a. This app gives you the ability to manage Azure resources on the go.
    b. You can view the current status of resources and check important metrics, received and review alerts.
    c. You can start/stop/restart and connect to virtual machines, use cloud shell to run scripts and alot more from your mobile device.
    d. cloud shell to manipulate scripts



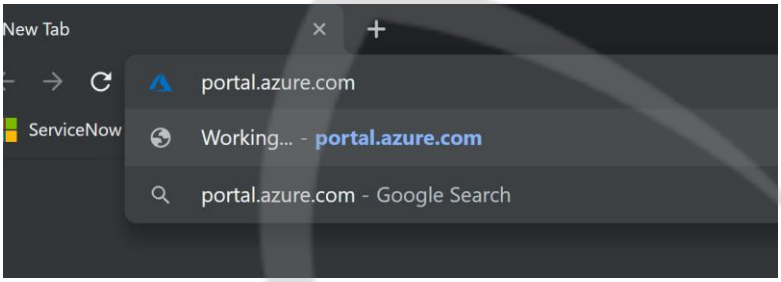
As we mentioned earlier, Azure offers software development kits in various languages used to implement your own management functionality. If there is no SDK for your preferred language, you can use the restAPIs to implement the functionality by yourself. Because Azure Portal is the easiest to learn about Azure, we are going to look at it in the next lesson.

Lesson 5.2: Overview of Azure Management Portal

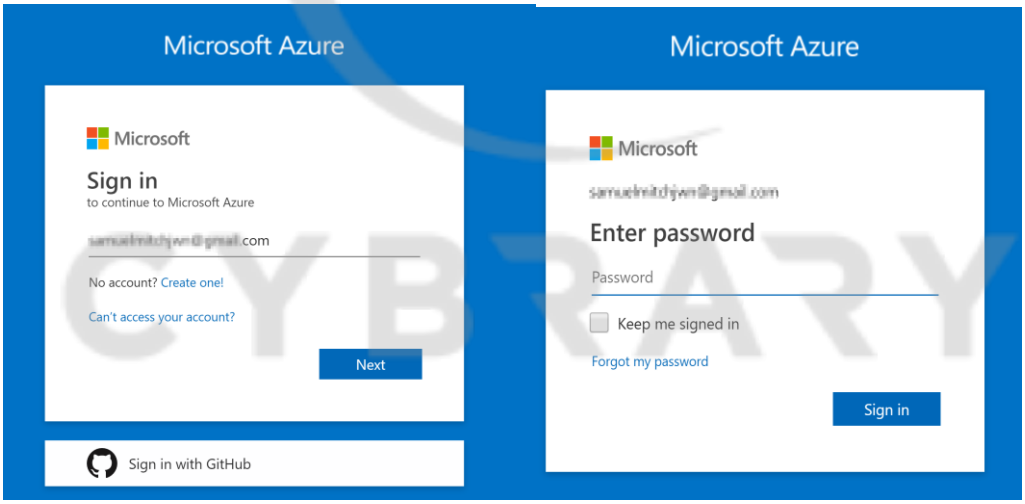
Skills Learned From This Lesson: Azure Portal, Azure Marketplace, Azure Cloud Shell, Azure Blade

Access the Azure Portal

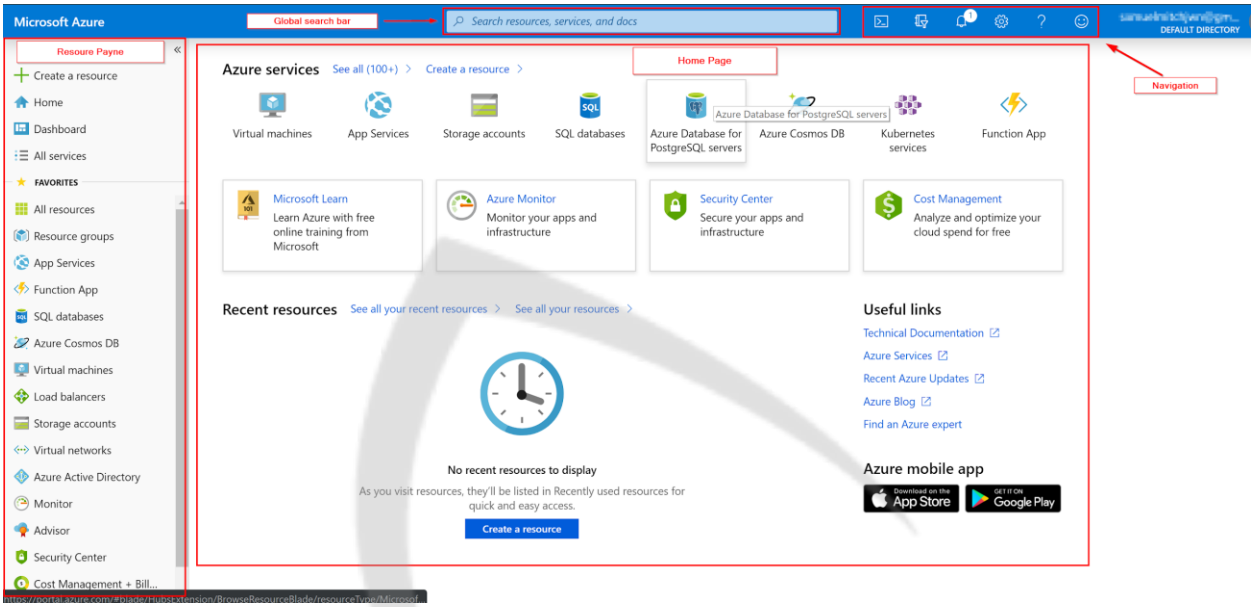
- Access it using url https://portal.azure.com



- Login using your Microsoft account

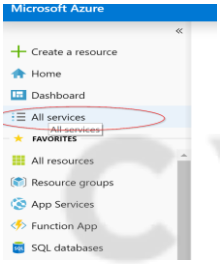


- On the Portal, there are a number sections listed:
- Resource payne
- Home page
- The navigation bar
- Global search bar

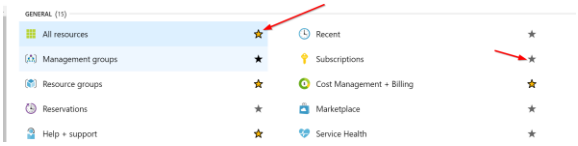


To Add or Remove the Resources from the payne:

- Select All services



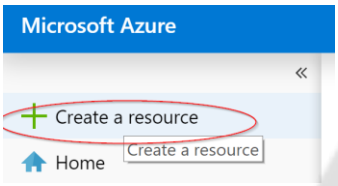
- Select the star beside the service you desire to add the payne.



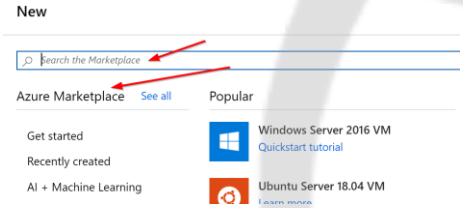
- It will show there

Azure Marketplace

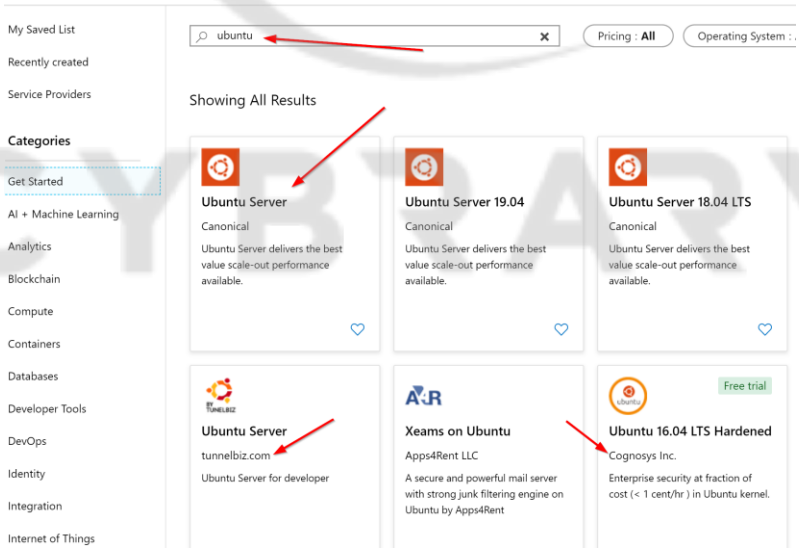
- When you select Create a resource



- You will see the option to search the Azure Marketplace

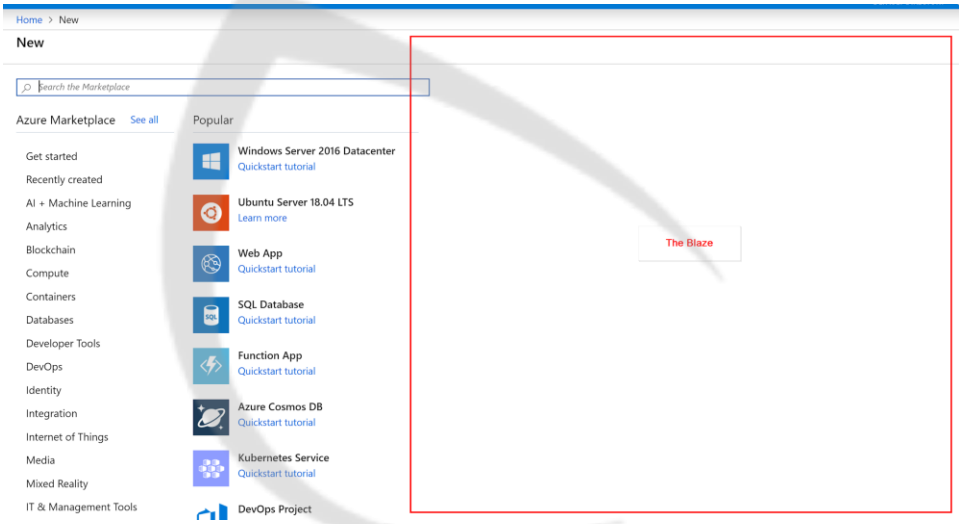


  - In the Azure Marketplace, you will not only have available the standard Azure resources but also different solutions published by our Azure partner independent of our vendors.
  - For example searching for ubuntu, you will see resources from various vendors which can also be filtered based on a specific category.

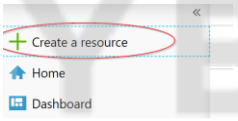


The Azure Blade

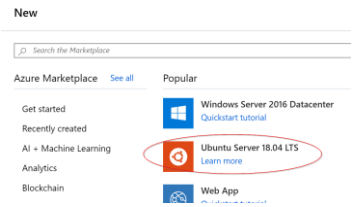
- There is something you should notice that when you are at the Home page and when you click on Create a resource. There is a white part on the right side of the home page. In Azure terminology this section or area is referred to as the **Blades** which is stuck to the right of the screen and can display additional information depending on the workflow or resource you choose.



- This is how the **blades** works:
  - Let us say that you want to create an ubuntu server
  - You select Create a resource

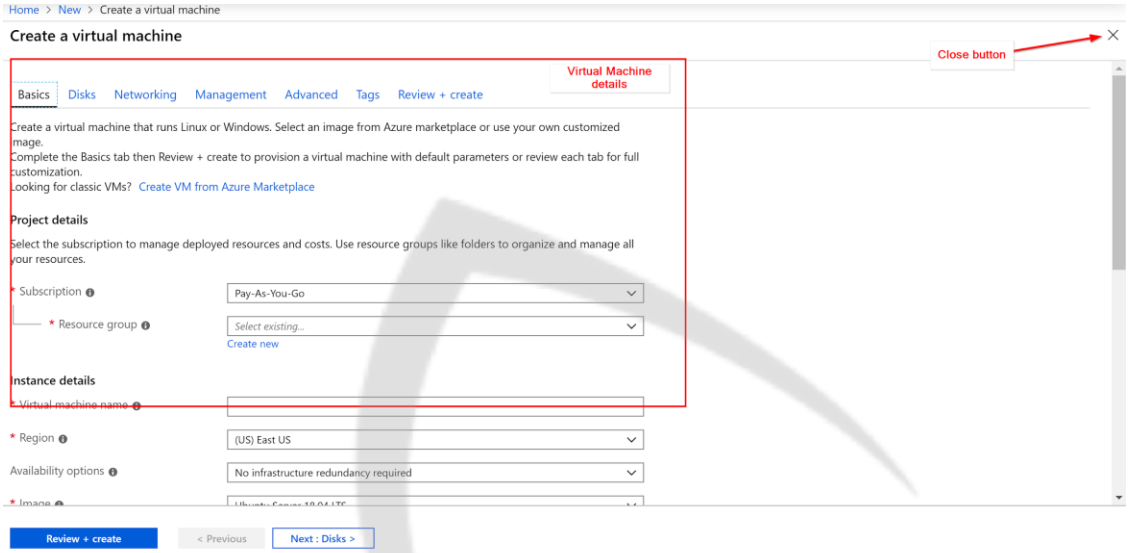


  - Click Ubuntu Server

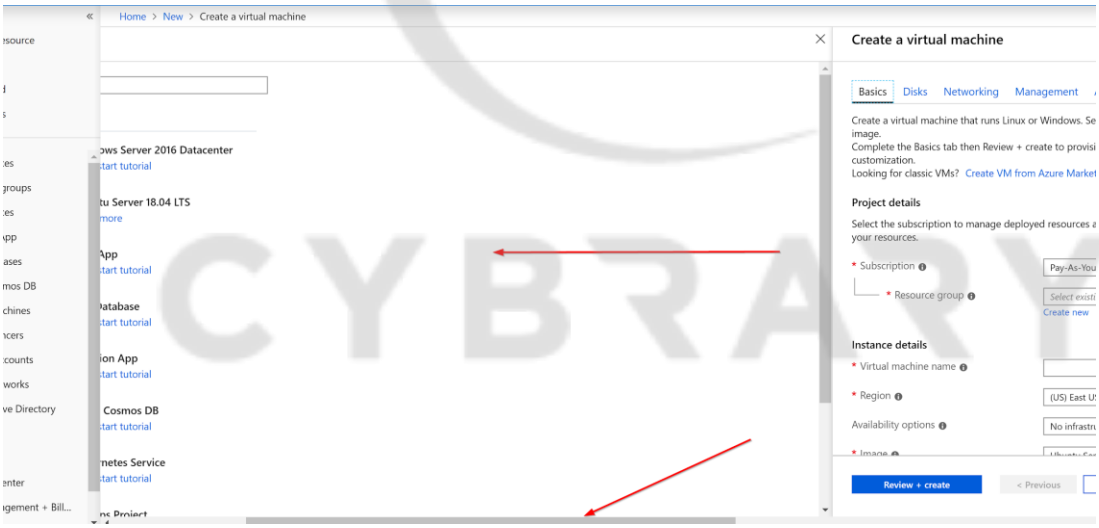


  - The virtual machine details will show up in the Blade

- There is an X that you will press to go back to the original option

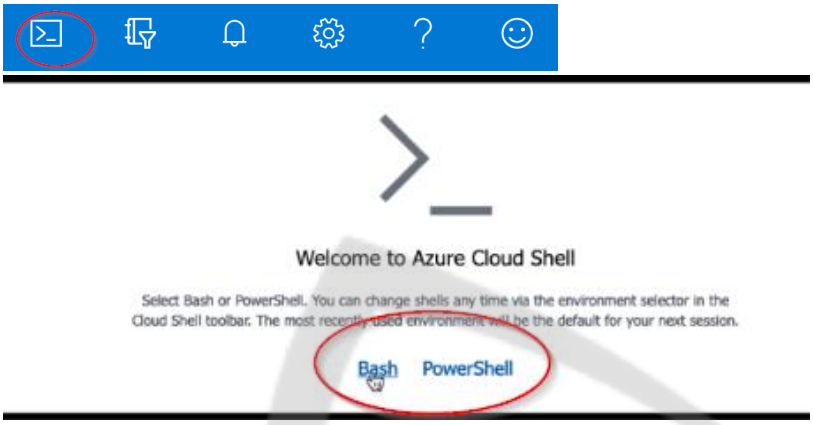


- Or you can scroll the horizontal bar to the left to see the original page.



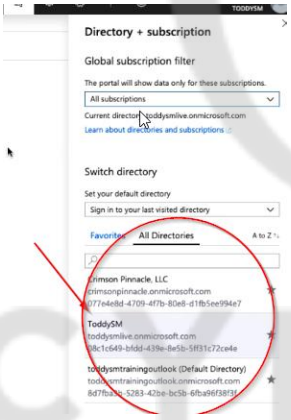
Options on the Navigation Bar:

- Azure Cloud Shell
  - Option to use BASH or PowerShell



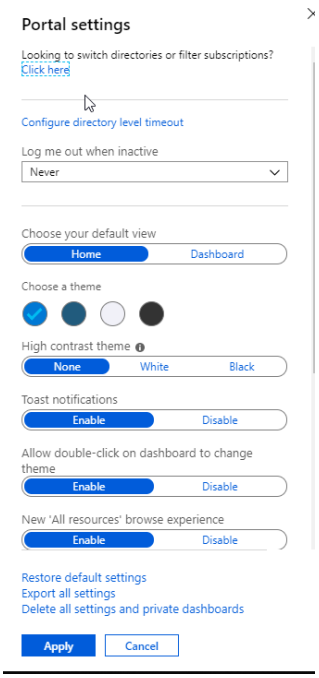
- switching between Azure Active Directory

  - It gives you the option to choose between tenants

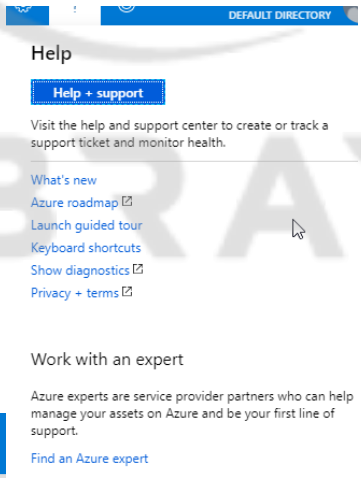


  - Notifications of tasks

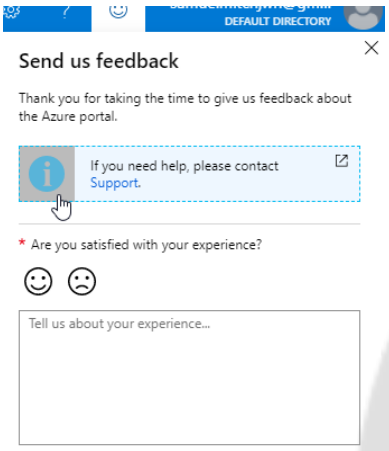
- Customizing the portal



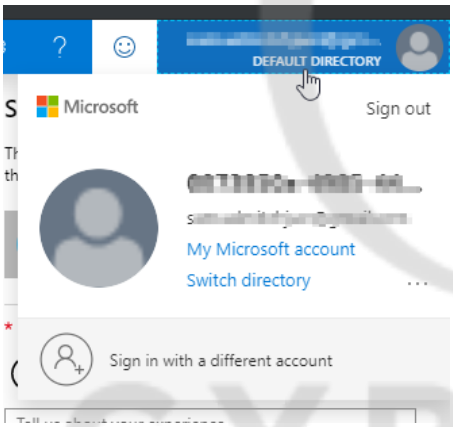
- Help icon



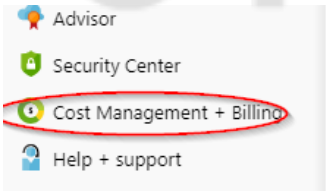
- Feedback icon

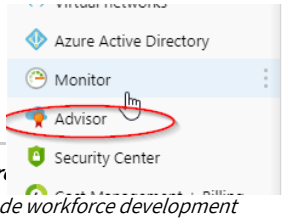


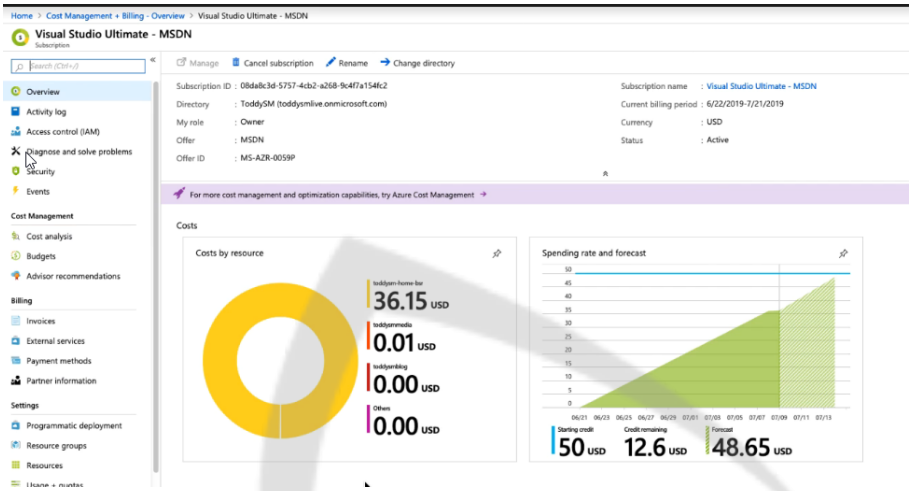
- Account information

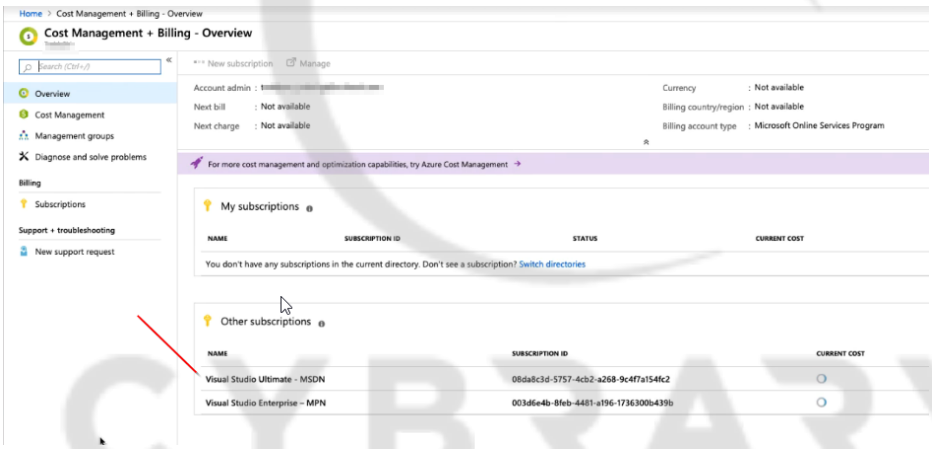


Cost Management + Billing



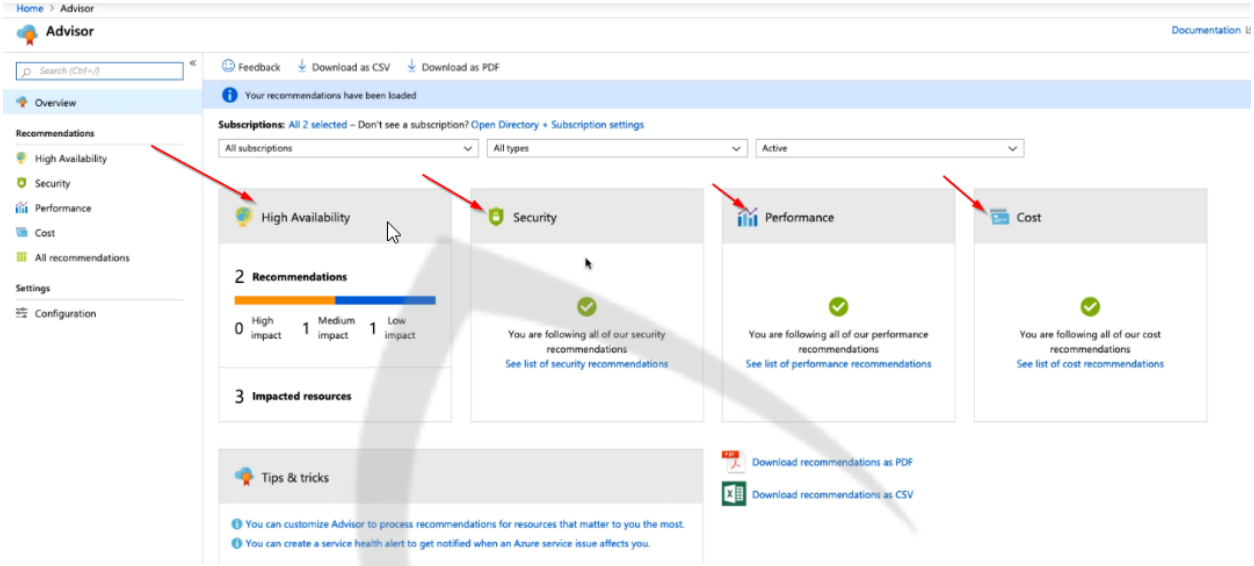






Advisor

- It provides recommendations for the following areas:
  - High Availability
  - Security
  - Performance
  - Cost

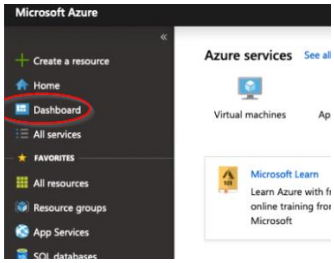

Home > Advisor
Advisor
Documentation
Search (Ctrl+/)
Overview
Recommendations
High Availability
Security
Performance
Cost
All recommendations
Settings
Configuration
Feedback
Download as CSV
Download as PDF
Your recommendations have been loaded
Subscriptions: All 2 selected – Don't see a subscription? Open Directory + Subscription settings
All subscriptions
All types
Active
High Availability
2 Recommendations
0 High impact
1 Medium impact
1 Low impact
3 Impacted resources
Security
You are following all of our security recommendations
See list of security recommendations
Performance
You are following all of our performance recommendations
See list of performance recommendations
Cost
You are following all of our cost recommendations
See list of cost recommendations
Tips & tricks
You can customize Advisor to process recommendations for resources that matter to you the most.
You can create a service health alert to get notified when an Azure service issue affects you.
Download recommendations as PDF
Download recommendations as CSV

Lesson 5.3: Azure Portal dashboards

Skills Learned From This Lesson: Azure Portal, Dashboard, Customize Dashboard

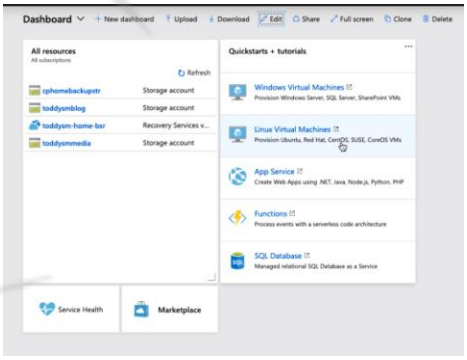
What is Azure Dashboard?

Azure Dashboards are customizable collections of UI tiles you can display in the portal. You can access the dashboards by clicking on the Dashboard button in the resources area.



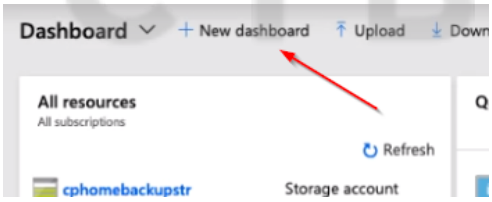
Customize the Azure Portal Dashboard

- There is a default dashboard created for you
- In the default dashboard, there are default tiles that are created for you:
  - All resources
  - Service Health
  - Marketplace
  - Quickstarts + tutorials

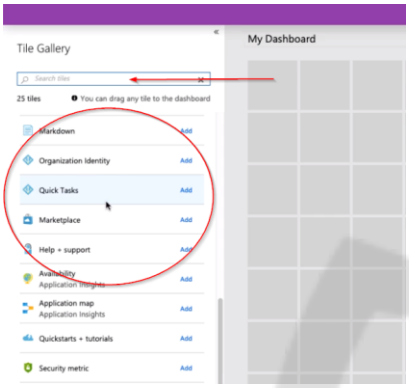


Create a New Dashboard

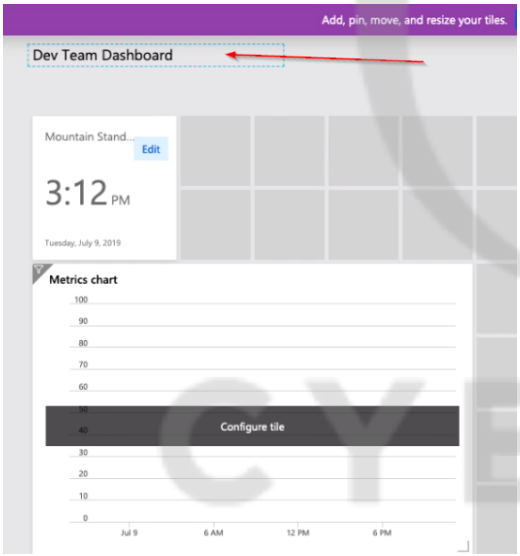
- You can create a new dashboard by clicking on the **New dashboard** button



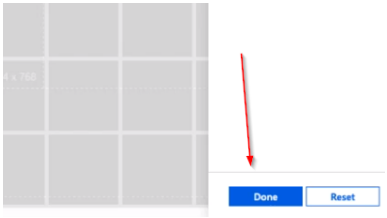
- On the left, there is a list of tiles that you can choose from



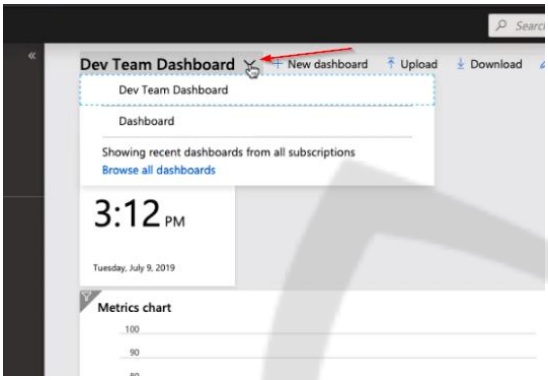
- Keep in mind that some of the tiles are query based which means they are automatically updated when the data changes.
- You can change the name of the Dashboard at the top



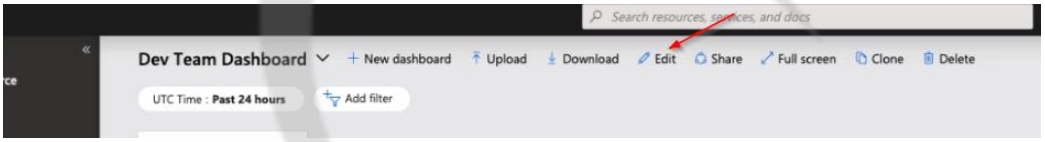
- When are you finish editing, click on **Done** to exit



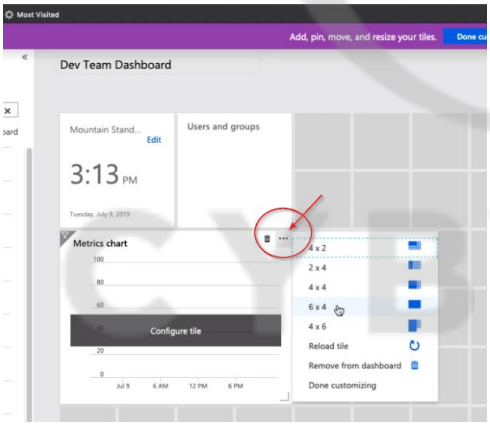
- You can change the Dashboard by selecting the Dashboard name and click the desired Dashboard



- You can edit an existing Dashboard by clicking on the Edit button

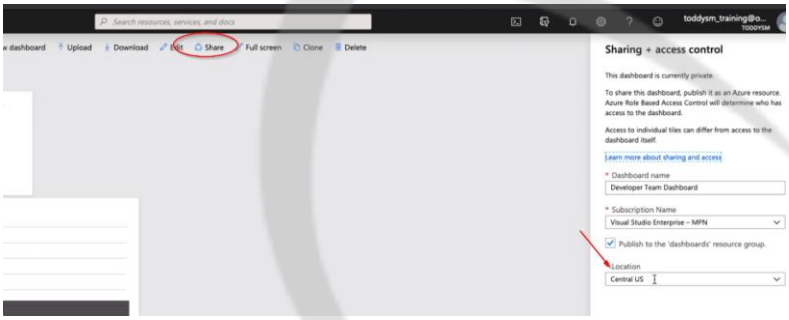


- You can resize the tiles by clicking on the edge or use the … to select a predefined size

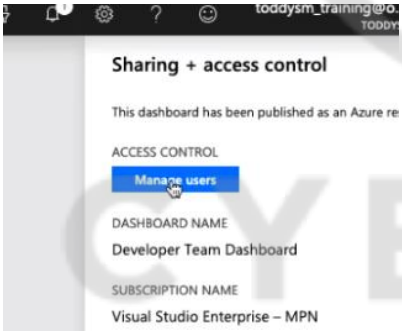


- The dashboard can be downloaded and are saved as json

- You can share the dashboard

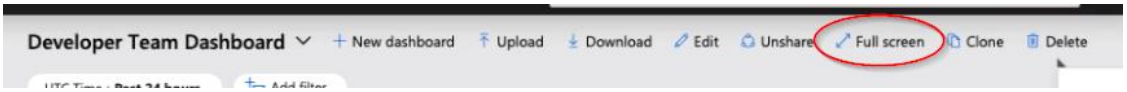


- You can restrict access to the dashboard

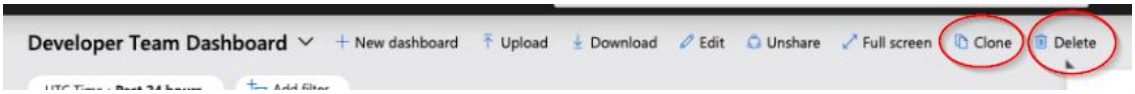


- You will select the users or groups to access the dashboard

- You can full screen the dashboard



- You can clone and delete a dashboard



Now you know how to use a dashboard to keep everyone in your team informed.

Lesson 5.4: Private and public preview features in Azure

Skills Learned From This Lesson: Private Preview, Public Preview, General Availability

Preview Features

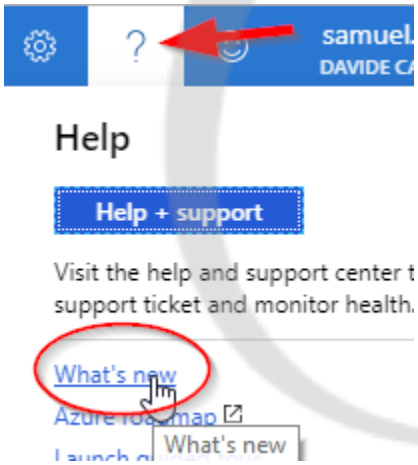
- Microsoft releases features for Preview or you may also know them as Beta features.
- Those can be new services or enhancements to existing services, API changes, new VMs or storage types.
- Preview features are released under certain terms that are specific to each features. Keeping in mind that certain preview features may not be covered by Support.

Let's look at the different Preview options:

1. Private preview features
    a. This is available to selected customers for evaluation. These customers are usual insiders who are active in submitting feedback about the functionality.
    b. Most of the time these preview features are under the Non-disclosure Agreement (NDA) and public information about them is restricted.
    c. Those features are usually driven by the product team who is developing the functionality.
2. Public preview features
    a. These previews are available to everyone to evaluate.
    b. You can visit the RSS feed and listed at https://azure.microsoft.com/services/preview where you can find out about the previews features and how you can evaluate them.
    c. You may sometimes require to send a request to get access to evaluate the feature.
    d. Some of the features also shows up in Azure marketplace
3. Preview Portal features
    a. You can also access the preview features via this Portal link https://preview.portal.azure.com
    b. The preview portal has an orange banner that advise you that this is a preview version of the portal

c. Although, the features are enticing to use, they may have bugs as it is still in the preview stage.

4. General Availability (GA) features
   a. Once the features have been fully tested by the product team and customers, then it is released, it is referred to General Availability.
   b. You can read the GA announces on Azure update page https://azure.microsoft.com/updates
   c. The GA is also available in the What's New link in Azure Portal



Module Summary

In this module, you have learnt about:

- Azure Portal,
- PowerShell,
- Azure CLI,
- Azure Cloud Shell
- Azure Mobile App
- Azure Portal UI and blades
- Customizing the Portal Dashboard
- Private and Public Preview features in Azure

Module 6
Azure compute services

Module Introduction

In this module, you will learn about:

- Azure compute concepts
- Azure Virtual Machines
- Azure container services
- Azure App Service
- Azure serverless computing

Lesson 6.1: Azure compute concepts

Skills Learned From This Lesson: Virtual Machine, Containers, App Services, Serverless

Azure offers four (4) ways to provide compute services:

1. Virtual Machines
    - VM provides a software emulation of a physical computer.
    - VM has a virtual processor, memory, hard drive and networking interfaces and requires an operating system to be installed on them

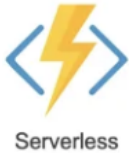
    - You will need a remote connection software such as Remote Desktop Connection for windows or ssh client for linux to use them similar to sitting in front of the computer screen.
    - VM offers the most control and you can install any application on them using the legacy off-the-shelf software.
2. Containers
    - Similar to virtual machines, the containers sits on top a host operating system but they do not require their own operating system installed inside the container.
    - They bundle all the dependencies needed by the applications and use the kernel of the host OS to run the container

    - If several containers are running on a server with linux, all those containers share the same Linux kernel. This means that you have less flexibility mixing and matching different OS on the same server.
    - Therefore if you need to run containers that requires Linux, you will require a Linux host and the same goes for a container that requires Windows, it needs a Windows host
3. App Service
    - App service is the platform as a service (PaaS) compute offering in Azure
    - It is designed to host highly scalable enterprise grade web applications

    - You can create an instance of the service and choose the run-time from predefined platforms like .Net, PHP, NodeJS or Java and deploy your own custom code.

- You do not need to maintain the underlying infrastructure but you have some control over the runtime configuration that allows you to meet different requirements with lower maintenance costs such as:
  - Performance
  - Scalability
  - Security
  - Complianance

4. Serverless
   - It offers cloud execution environment of your custom code with complete abstraction of underlying infrastructure.
   - You can deploy your custom code and run it based on various triggers like:
     - A schedule
     - HTTP request
     - Event triggers
   - Serverless has execution environment for different languages like C#, JavaScript, Python, Java and PowerShell are available and Azure handles all the infrastructure management. This means that you have no control of the environment configuration.



Depending on the needs of your application, you may choose more than one compute services. For example, you have an online shopping website deployed on Azure Web Service and submit the processing of each order to a serverless app. In order to properly design your application, you need to be aware of the capabilities and restrictions of each options. We will look into the details of each option in the next few lessons.

Lesson 6.2: Azure virtual machines

Skills Learned From This Lesson: Azure Virtual Machines, Availability Sets, Fault Domains, Update Domains, Scale Sets, Azure Batch

In this lesson, we will look deeper into the Virtual machine capabilities on Azure.

Azure Virtual Machines

1. It is a service that allows you to create Virtual Machines in the Cloud
2. You have complete control of the software running on the Virtual Machines
3. You can install the Operating System of your choice and configure it according to your requirements.
4. You can install and run custom software almost without any restrictions..
5. You manage the VM by connecting to it remotely via RDP client for Windows or SSH client for Linux.
6. You can provision a Virtual Machines in minutes by using pre-configured images that are available from the Azure marketplace. The image is a template of the virtual machine which includes operating system and other software such as hosting environment, web servers and databases or complete applications.
7. You can also create custom images from your on-premise environment and run them in Azure with almost no effort. This is a very helpful way to migrate your existing on-premises workload to Azure with low effort. It is referred to as “lift-and-shift”.

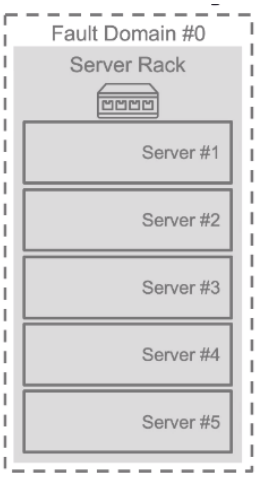
Running a single VM for development and testing purposes is helpful but Azure offers advanced high availability features for applications running on Virtual machines. One of those features is availability sets.

Availability Set

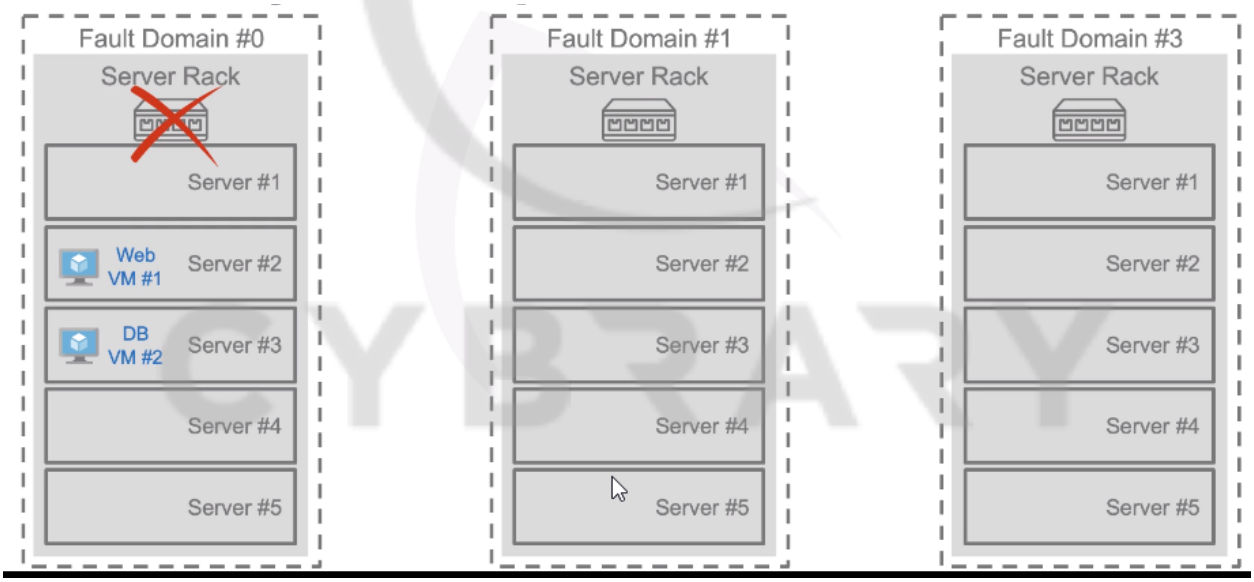
- It is a logical grouping of two or Virtual machines that helps to keep the application available during planned and unplanned maintenance
- It uses a concept called Fault Domains and Update Domains.
- When your VM are in an availability sets, Azure ensure that they are placed across fault domains.

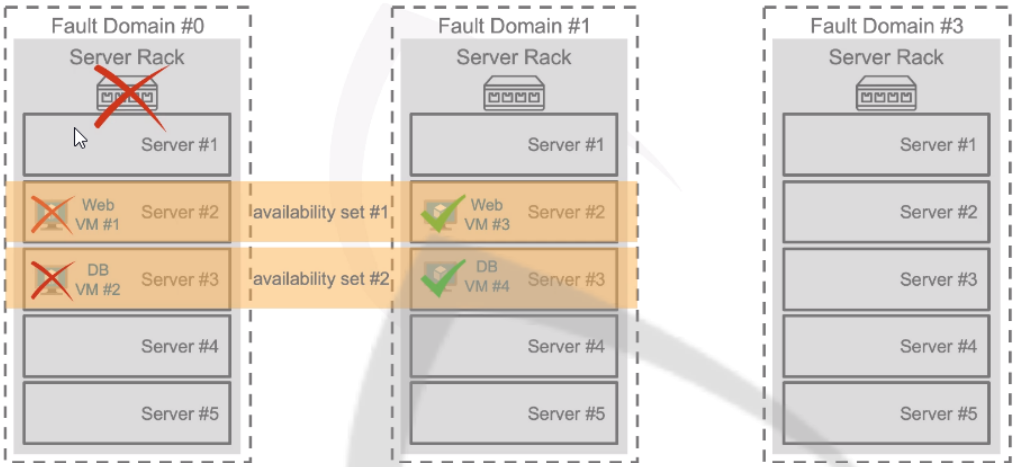
- Availability sets does not cost but the number of VMs that you run in the Azure

Fault Domains



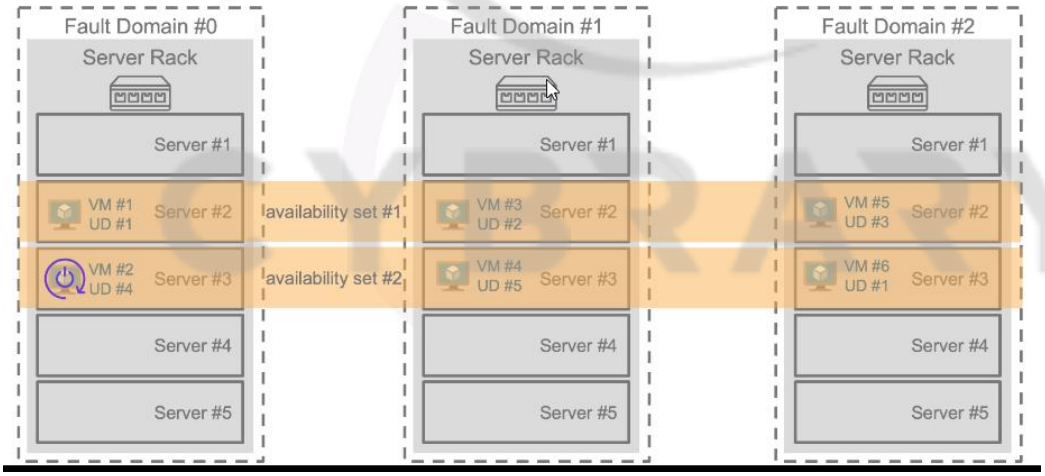
1. In Azure, a fault domain is a single server rack that has the following independent components:
    - Power
    - Cooling
    - Network switch
    - Physical hardware
2. You can have up to three (3) Fault Domains for your workloads
3. The more VMs you have per tier the more fault tolerance you will have for your applications





Update Domains

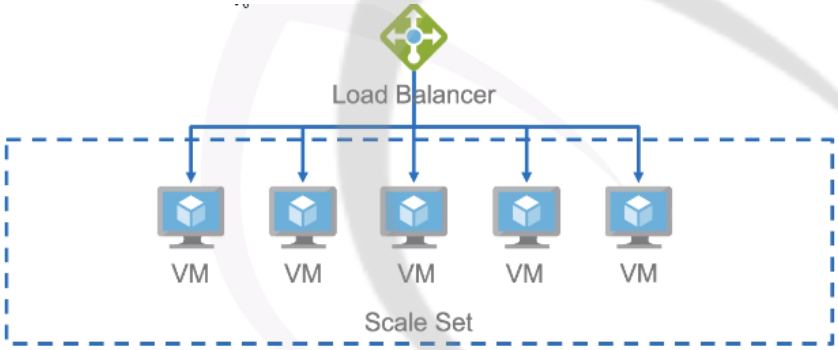
4. Another important feature is the Update Domain which is important during a planned maintenance when a VM needs to be restarted
5. The VMs are assigned to UD groups using a proprietary algorithm and the users has no impact on this method.



SSD are not apart of SLA so it is important to

Scale Sets

6. This is a service that allows you to manage a group of identical servers e.g. a web farm running apache servers in parallel serving user's request.
7. The VMs are placed behind a load balancer to balance the traffic between them
8. Many times if there is an increased workload, the VMs can be added on-demand or on a predefined schedule.
9. Azure Load balancer has built-in integration with the scale sets and they can automatically add the VMs to the load balancing pool. Once the load decreases, the load balancer can stop the traffic from going to the VMs that has been removed.



Azure Batch

- Azure batch can assist when you need a large scale job scheduling service.
- It can be used to scale to hundreds or thousands of VMs simultaneously and run parallel calculations e.g. encoding videos in different formats, rendering animations or process large datasets on schedule.
- It is responsible for starting the pool of VMs, install the applications, staging the data, run the jobs, identify failures and scale down when the pools work is complete.
- It allows you to choose between windows or Linux OS to run your jobs.

Now you have a good knowledge of VM-based compute option in Azure. In the next lesson, we are going to discuss Azure Containers.

Lesson 6.3: Azure container services

Skills Learned From This Lesson: VM Downsides, Azure Containers, Microservices, Orchestrator, Kubernetes, ACI, AKS, ACR

What are containers and how can you use them in Azure?

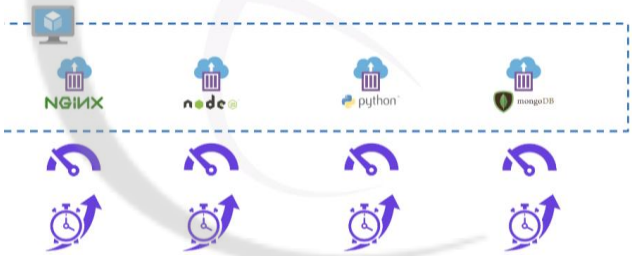
VM Downsides

- Virtual machines and virtualized hardware are good for migrating legacy applications from on-premise to Microsoft Azure but they have some disadvantages.
- For example If your App has components that require different run-time environments, you will need multiple VMs to run it.

- Here is an example where you have:
  - NGINX for your web proxy
  - NodeJs run-time for your business logic
  - Python run-time for your batch processing
  - mongoDB as your database
- Of course you can install all of them on the same VM but you have no way to restrict the resource usage of one component so that it does not impact the other.
- Also installing all the components on one machine compromises the security of the application. This is why it is better to use multiple VMs.
- Because VMs are emulating full computers, task like starting and stopping VMs are slow and often takes a few minutes.
- Another challenge with the VM is the guest OS consumes CPU and memory which cannot be made available to the application impacting the efficiency of the VMs.

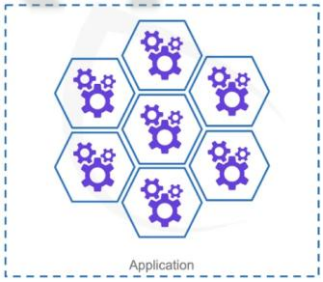
Containers

- If you need to achieve the same isolation as the VM approach but want to increase the efficiency of your infrastructure, you can use containers.
- You can deploy multiple container on the same host, installing only a single OS avoiding the overhead of multiple VMs and operating system.
- Containers are light weight because they do not require a full OS boot and they can be created, scaled out and stopped within seconds.This allows you to respond quickly to changes in demand.
- Because containers does not require an additional OS, all resources are dedicated to the application system. This significantly increases the efficiency of the infrastructure.
- Containers unlike VMs, virtualizes the Operating System and allow the application to run on-top of a single OS.



Microservices

- Container are closely related to a new trend in the application architect, called microservices architecture.
- Microservices is a service that has a small well defined scope and it is loosely coupled from many other services.
- Instead of building one analytical application, you build many small services that each fulfill a single business function. Then you coupled those services together and provide the business logic of the application.
- Each service can be deployed as a set of containers that are configured to work together.



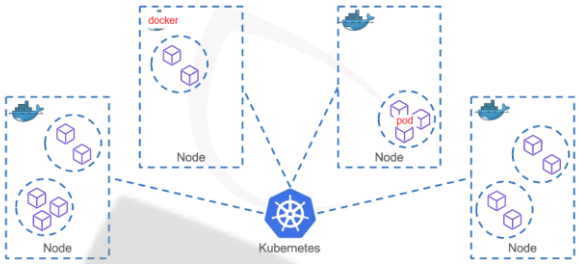
Benefits of Microservices

This is all good but what are the benefits of using microservices.

- The microservices can be developed by separate team with the expertise to create the functionality.
- They can use different technologies, frameworks and programming languages. You are not required to use the single stack for all the services. This best helps you leverage your team's expertise and makes hiring developers easier.
- You can release and deploy microservices independent of each other as often as you want.
- The deployment could be light-weight and does not require a lot of time.
- Because microservices are small pieces of business functionality, they require a smaller code base which makes them easy to maintain and easy to rollback if a bug is discovered.
- Microservices can be scaled independently. You can just increase the number of instances of the microservices that is a bottleneck in your application and leave the remaining services as is.

Container Orchestration with Kubernetes

- Because one application can consist of multiple services, each one which can be comprised of multiple containers; deploying, managing and scaling those services can become impractical.
- This is why containers with orchestration solutions like Kubernetes is needed.
- With the help of kubernetes, you can handle the demand of managing containerized applications at scale.
- This is how it works, a kubernetes cluster consist of multiple nodes. Those can be a virtual machine with a container engine installed on them.
- One of the most popular container engine is Docker.
- Kubernetes manages the placements of pod which can consist of multiple containers.
- You can think of a pod as a single microservices.



- Because Kubernetes communicate with the Nodes and the pod, it can move dynamically move pots between nodes.
- Let us say one of the pod fails, Kubernetes can restart the pod. If the Node fails, the pod can be redeployed on another Node.
- Kubernetes can scale a pod by increasing the number containers within.
- Kubernetes can staged deployment of a pod to reduce the downtime or rollback the deployment if something fails.
- Kubernetes can manage the storage. Persistent storage can be attached to more than containers to keep the data persistent between pods restart. In this way, if the Node fails, and the pod needs to be deployed on another Node, the data will be available when the new pod instance starts.
- Of course application running on Kubernetes can use any cloud-based storage solutions to persist their data
- Kubernetes networking plugins enable functionality like network isolation, policy-driven network security like firewalls, load balancing and exposing pods to the internet. Those plugins can also effectively manage name resolutions between the pods.
- Kubernetes has a set of APIs that can be used to automate deployment, management as well as to extend the platform with richer functionality.

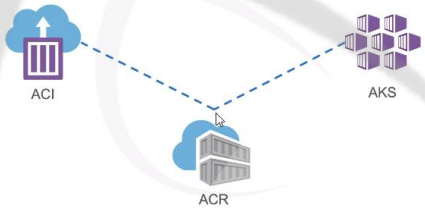
Azure supports Docker containers for Linux workloads and windows containers for Windows.

Azure Container Services

Now let us look at services for running containers:

- ACI - Azure Container Instances is a services that allows you to run a container without the need to manage a virtual machine and the docker engine. You just upload your container and run it.

- AKS - Azure Kubernetes Services is a complete orchestration service for containers that can be scale to hundreds or thousands of nodes.
- ACR - Azure Container Registry allows you to upload and version your container images.
    - ACR is similar to Docker Hub and it is fully compliant with Docker container registry API.
    - Using ACR, you can create your own private container repository and use only approved container images within your application.
    - You can configure ACI and AKS to pull the images from the ACR.



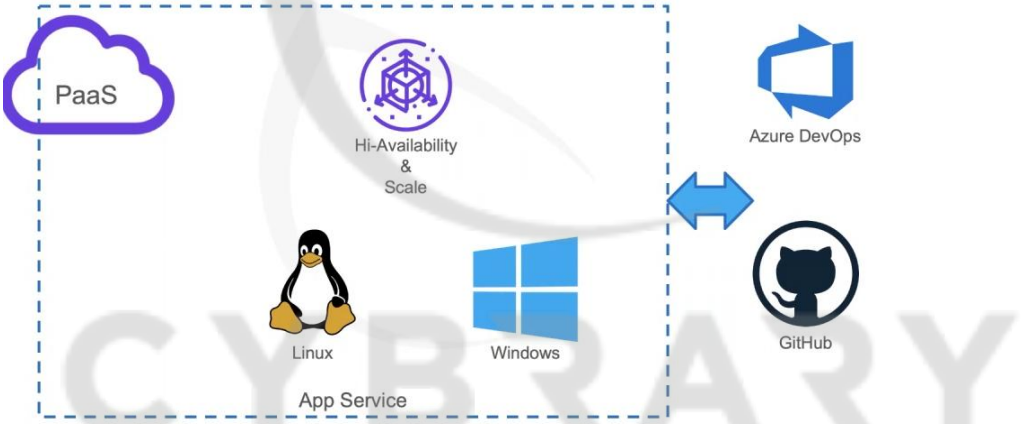
This covers the container technology services available in Azure. In the next lesson, we will look at the platform as a service option for compute, Azure App service.

Lesson 6.4: Azure App Service

Skills Learned From This Lesson: Azure App Service, App Service Plan, App Types

What is Azure App Services:

- Azure App services is a Platform as a Service (PaaS) that allows you to manage web applications, restful APIs , mobile apps and background jobs.
- Azure manages this infrastructure allowing the customer to focus on their application.
- Azure app services offers high availability and auto-scaling.
- Azure App services supports both linux and windows workloads.
- Azure App services integrate with tools such as Azure DevOps and GitHub to support a continuous deployment model.
- Azure App services integrates with other Azure services to ensure it is highly secure and highly performance.



Azure App Service Plan

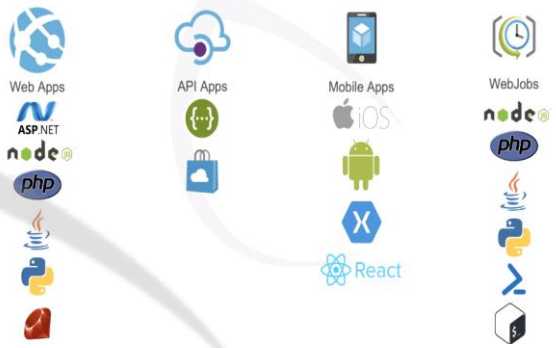
- Depending on the Azure App service plan you choose, it determines how much you pay for the compute resources and how much resources is dedicated to your web host.
- You can choose between Dedicated or Shared resources.
- There is also Free App service plan that you can used to host low traffic sites.
- You can start small and easily scale up the service to a different tier within the Azure Portal.

App Types

Azure Apps services supports four (4) different services Apps:

1. Web Apps develops in one of the following apps:
    - ASP.Net
    - NodeJS
    - PHP
    - Java
    - Python
    - Ruby

    Azure manages the complete web hosting environment and you can choose between Linux or Windows hosting.



2. API Apps
    - API Apps can used to host restfulAPIs developed in one of the supporting languages.
    - API Apps has full Swagger support and integration within the Azure marketplace for publish your App APIs.
3. Mobile App
    - Mobile App offers complete full mobile backend support including cloud-based SQL database, push notifications and authentication with social identity providers like Facebook, Twitter, Google and Microsoft.
    - You can write custom backend logic using NodeJs and c# and there are SDKs for native IOS and Android development and React native
4. WebJobs
    - WebJob allows you to run a job with the context of a Web API or Mobile App
    - The jobs can be programmed in NodeJs, PHP, Python or Java or compiled executables. They can also be PowerShell or Bash script
    - You can use those to do a background process in your application and trigger them on request or on schedule.

You now have a good understanding of Azure enterprise grade applications.

Lesson 6.5: Serverless on Azure

Skills Learned From This Lesson: Serverless, Functions, Logic Apps,

Serverless

- The terminology serverless is misunderstood as having no servers which is not correct. This is not the case, your code is executed on a server in the cloud.
- The server that executes your code is determined by the cloud platforms
- There is no guarantee that the next time your code execute will be on the same server as before.
- Your code executes as a result of a trigger.
    - This can be scheduled triggers, HTTP trigger or event trigger
    - This gives you the flexibility to implement different solutions using serverless computing.
    - For example, you can use HTTP triggers to implement restful APIs that are access from mobile devices or use schedule trigger to run background jobs every hour or event trigger to raise an alert when a sensor detects high temperature.
- Because the cloud provider manages the infrastructure and you don't have control over it, there are things you should consider when implementing your functions.
- Normally, the serverless application is considered stateless
- Although each one of the servers that executes your code has a local storage attached, you should not use the storage for data you want to preserve between execution. You may write and read data from the local storage while it is executing but after the execution is completed you will not have access to that data.
- Keep in mind that the execution environment is shared and therefore storing private data there will not be a good idea.
- If you need to pass data between executions, you should use stateful serverless services which use cloud-based storage for storing data from your stateless Apps.
- Another thing to consider is that the execution time for your code has a time limit for example Functions has a time limit of 5 minutes by default which can be increased to 10 minutes but this may not be enough.
- If you need to use a function that runs longer, you should consider using another of Azure services.

Two types of Serverless

Azure has two types of compute services that run serverless code:

1. Azure Functions
    - It use a Code-first approach or in-productive developer approach
        - This means that you write a code that gets executed in the cloud
        - You can write your functions in C#, F#, Javascript, PowerShell, Python and TypeScript.
    - Azure Functions can be stateless or stateful
        - Stateful functions are also called Durable Functions and they pass context between execution allowing you to track parameter.
    - There is a dozen builtin binding and triggers for Azure functions
        - For example schedule and HTTP trigger or event triggers based on storage block creations, events create events or storage queue message.
    - You can develop custom bindings
    - Azure functions can developed locally using the Azure functions Core tools and extension for Visual Studio or VS Code.
    - You can manage Azure Functions from the Azure Portal, Visual Studio, VS Codes, PowerShell or AzureCLI.
2. Logic Apps
    - Logic Apps uses designer-first or declarative approach
    - You build workflows using pre built connectors or processing blocks
    - There are more than 200 connectors and processing blocks including enterprise and social services like Office 365, Dynamics 365, SalesForce, SAP, Twitter, facebook. You can also build custom connectors.
    - You implement the workflow in Azure Portal or Visual Studio and can persist those in a JSON format with predefined schema. This allows you to automate the deployment of workflows.
    - The management can be done from the Azure Portal, Visual Studio or Azure CLI
    - The last thing to remember is that they are stateful and can persist data between executions.

Module Summary

In this module you learnt about:

- Availability sets including fault domains and update domains
- Scale sets
- Container orchestration and microservices
- Serverless computing
- Azure compute services

Module 7
Azure storage services

Module Introduction

In this module you are going to learn about:
• Different types of data
• Azure data storage services
• Benefits of the loud storage

Lesson 7.1: Data Types

Skills Learned From This Lesson: Data Types, Structure Data, Semi-Structured Data, Unstructured Data, Big Data

Before we look at the storage options, we need to look at the data types enterprise collects.

Data Types

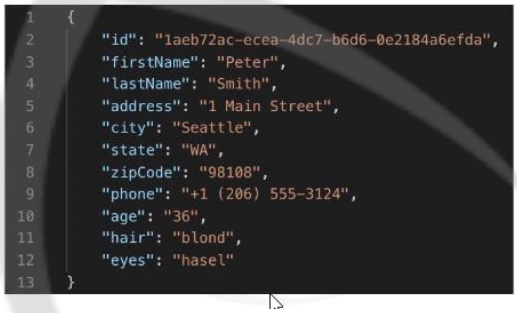
- Structure Data
    - It is confined to a predefined schema and are stored in tables with rows and columns.
    - Before the data is stored in the table, the data is normalized to reduced the amount of information stored in the tables. During normalization, the data is split into subsets and store into separate tables. Those tables are linked with the help of keys to indicate the relationship between the roles in separate tables.This is why structured data is also referred to as relational data.
    - Each column in the table can store a specific data types such as integer, character, string or date. The data type are enforced and it will throw an error if the data type does not conform.

CustomerName	CustomerAddress	CustomerPhone	OrderId	Item	Quantity	Price	ItemTotal	OrderSubtotal	OrderTax	OrderTotal
Peter Smith	1 Main Street, Seattle WA 98108	+1 (206) 555-3124	ADC123	Colored pencils	2	$5.99	$11.98	$89.55	$8.96	$98.51
Peter Smith	1 Main Street, Seattle WA 98108	+1 (206) 555-3124	ADC123	Notepads	8	$2.99	$23.92	$89.55	$8.96	$98.51
Peter Smith	1 Main Street, Seattle WA 98108	+1 (206) 555-3124	ADC123	PostIt Notes	10	$1.99	$19.90	$89.55	$8.96	$98.51
Peter Smith	1 Main Street, Seattle WA 98108	+1 (206) 555-3124	ADC123	Pens	15	$1.59	$23.85	$89.55	$8.96	$98.51
Peter Smith	1 Main Street, Seattle WA 98108	+1 (206) 555-3124	ADC123	Scissors	2	$4.95	$9.90	$89.55	$8.96	$98.51
Jane Mullish	10123 1st St NE, Bellevue, WA 98004	+1 (425) 546-4673	BFE456	Journals	2	$11.99	$23.98	$23.98	$2.40	$26.38
Ellie Smith	11217 2nd Ave NE, Redmond, WA 98052	+1 (425) 791-1823	JHI786	Journals	2	$12.95	$25.90	$68.63	$6.86	$75.49
Ellie Smith	11217 2nd Ave NE, Redmond, WA 98052	+1 (425) 791-1823	JHI786	Notepads	7	$2.99	$20.93	$68.63	$6.86	$75.49
Ellie Smith	11217 2nd Ave NE, Redmond, WA 98052	+1 (425) 791-1823	JHI786	Pens	4	$5.45	$21.80	$68.63	$6.86	$75.49

- Semi-Structured Data
    - It does not fit in to tables or does not have predetermined schema
    - Instead it use key store to organize the data and to provide hierarchy
    - Typical example of key-value data is that it can be of any type.
    - Key-value data can be represented with two columns, a key column and a value column. There is no limit on the amount of data that can store in each column.

Key	Value
key1	some value
5	some other value
{"id":"12345","somekey":"somedata"}	12.678
key2	{"id":"12345","somekey":"somedata"}

  - Example of key-value data is a JSON object.



- Unstructured Data
  - It can be anything, there is no restriction on the format and the structure
  - It can be a PDF, Word documents, media files, pictures or text files.
  - Very often you can attach metadata to put some classifications to it.
- Big Data
  - We already generate a lot of data today, tweets, facebook, instagram images, monitoring and analytical data, security data, sensor data and whatever else.
  - It is expected we will generate 1.7 MB per seconds per person by 2020.
  - Gardner defines the Big Data using three (3) criteria:
    - High Volume
    - High Velocity
    - High Variety
  - Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.
  - Reference: https://www.gartner.com/it-glossary/big-data

Lesson 7.2: Azure Data Storage Options

Skills Learned From This Lesson: Azure SQL database, Azure Cosmos DB, Azure Storage Blob, Azure File Share, Azure Disk Storage, Azure Data Lake Storage, Azure Queue Storage

Azure offers various data storage services that can store any type of data. Let us look at the options in detail.

Azure SQL database

- It is a relational database as a services (DaaS).
- It is based on the latest version of Microsoft SQL server database engine.
- It is applicable for a variety of modern applications because it allows you processes relational and non-relational structures like graphs, spatial data and json and XML data.
- It has advanced query processing features include intelligent query processing like advanced joints and interleaved execution and high performance in-memory technologies like in-memory OLTP, custom column store indexes.
- It allows you to easily migrate on-premise SQL server database with little or no down time using Azure database migration services.
- It is ideal for structured data.

Azure Cosmos DB

- It is a globally distributed, schema-less database service.
- Ir is a multi-model database and supports different APIs for access include Cassandra API, MongoDB API, SQL API, Gremlin API and table API. It means that you can migrate your data from one of those database options and offer global read-write capabilities.
- It has support for built-in Apache Spark enabling real-time of machine learning over global distributed datasets
- It offers five (5) nines 99.999% SLA
- It offers multi-master support allow you to write data from multiple locations.
- It is ideal for semi-structured data

Azure Storage Blob

- It is a highly scalable and unstructured storage which you can use to store any kind of data.
- Blob can be accessing from HTTP/HTTPS endpoints from any in the world which means that you can access that data using any web client.
- It has a built-in Geo-redundancy that you can be leveraged for disaster recovery and global access
- It also offers strong consistency and verifies the writes across all replicas to ensure you always have access to the latest data.
- There are three (3) types of Blob
    - Block Blob
    - Page blob
    - Append Blob
- You can use Storage Blob for streaming apps like videos and audio stream or storing large amount of data like monitoring and logging data
- Storage Blob also provides different Tiers of storage such as Hot, Cool, Archive and Premium that you can use to satisfy different any application or business continuity needs.

Azure Data Lake Storage

- It is an object type of storage that includes a set of capabilities dedicated to big data analytics
- It is built on top of the Azure storage Blob and leverages its low cost and tiered access but adds additional features such as file system semantics, directory/file level security
- It can be used to store structured and unstructured data
- It has Hadoop compatible access for advanced analytics
- It's foundation for building enterprise data lakes allowing you to classify and analyze any type of data.

Azure Queue storage

- It is a simple cost effective durable message services that offers asynchronous messaging capabilities.

- It allows you to build flexible, loosely coupled applications that can scale independently. services
- It offers http/https endpoints that can be accessible around the World.
- You can use it to have multiple senders to send messages that are processed by more than one receiver.

Azure Disk Storage

- It provides disk storage for Virtual Machines. You can use the disk as primary boot disk for the VM that has the OS installed or for storing application that is not accessible outside the VM.
- Azure offers several disk options starting from start-up spinning HDD for applications with infrequently data access needs and low cost requirements to various tier SSD drives for performance demanding applications.
- Azure disk can be managed and unmanaged. Unmanaged disk are completely managed by the customer while Managed disk offered additional features like 99.999% SLA and integration with the availability sets and availability zones, Azure backup support and granular access control.
- Managed disk also offer two types of encryption:
    - Azure Disk Encryption (ADE) - that allows you encrypt the OS and data disk for the VMs.
    - Azure Storage Service Encryption (SSE)- that allow you to encrypt the disk at rest.

Azure File Share

- It offers fully managed file share via server message block (SMB) protocol
- It can be mounted and accessed by any Windows, Linux and Mac OS machine on-premise or in the cloud.
- You can use it to share data between multiple VMs in Azure using high performance file share built on Azure premium storage tier or extend your on-premise file shares to the cloud with Azure file sync.

Now you have a good grasp of Azure storage options.

Lesson 7.3: Benefits of Cloud Data Storage

Skills Learned From This Lesson: SQL database, Storage Blobs, Storage Tiers, Cloud storage benefits

We will be looking at the benefits of using cloud data storage in comparison to on-premise options.

Cloud Benefits

- Azure offers value storage types that you can leverage to implement any type of applications including structured types of storage like SQL database, semi-structured types like Cosmos DB or unstructured type like Storage Blobs.
- Implementing those options on-premise will require numerous servers and storage devices that needed to precured, configured and maintained. That not only increase your application time to market but the on-going cost of the application.
- Using Azure, you can provision those storage in minutes and start using them immediately in a cost effective way. You will pay for only what you need and in this way you can better manage your budget allowing it to scale with your business.
- The ability to use on-demand storage services increases the agility of your developing team and allow you to adapt to changes and take on new opportunities.
- On-premise solutions requires new hardware procurement which is time consuming.

Azure Cloud storage offers different storage Tiers:

- Hot storage - optimized for frequent access
- Cold storage - for data that is infrequently access and is stored for at least 30 days.
- Archive storage - for data that is rarely access which is stored for at least 180 days.

Benefits Continues

- Implementing different storage tiers on-premise at least doubles your on-premise infrastructure storage investment and significantly increases your maintenance cost.
- Not only that but cloud storage increases the reliability of your application by providing automatic replication, backup and restore capabilities across data centers and regions. Sometimes that will require significant capital investment for on-premise storage.

- Cloud storage has built-in security, including encryption during transfer, encryption at rest and role-based access control.

With this we wrap up with the benefits of cloud-based storage.

Module Summary

In this module you have learnt about:

- Structured, semi-structured and unstructured data types
- Azure data storage services
- Benefits of Cloud storage

Module 8
Azure networking services

Module Introduction

In this module, we are going to discuss the following topics:

- Azure Virtual Networks
- Azure Load Balancer and Azure Application Gateway
- Azure Traffic Manager
- Other networking concepts

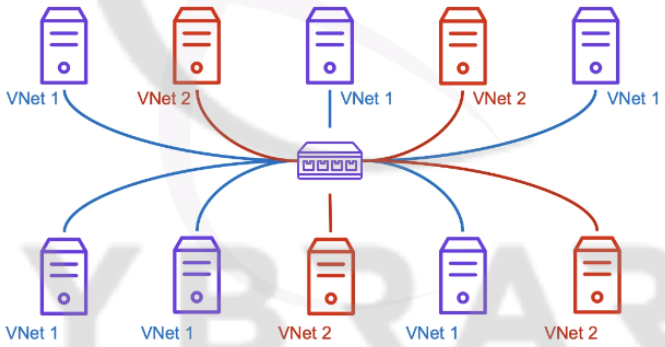
Lesson 8.1: Azure Virtual Networks

Skills Learned From This Lesson: Azure Virtual Networks, Subnets, Network Security Group, Routing tables, Internet Gateway, VPN Gateway

Let us see how Azure segregate traffic for different customers. To understand that we need to learn how virtual networks or VNET works.

What is a Virtual Network (VNET)?

- Every machine in the local network is connected to a network switch.
- The switch is responsible for managing the traffic on the network and allow two machines to communicate efficiently with the other.
- This is great but if you have more than one customer on this network, you do not want first customer to sniff the traffic of second customer and visa versa.
- The network switches has the capability to securely segregate the traffic between virtual machines and isolate the traffic. This is called a Virtual Network.



- In our example we have two virtual networks, one for the blue servers and one for the red servers.
- Virtual networks are highly leveraged by cloud provides to secure and isolate the network traffic for different customers.
- Using a virtual networks, your network traffic is logical isolated from other customer networks and you can configure your virtual network according to your needs. Also you should not worry that others can listen to your traffic because the traffic are not sent to other virtual machines that do not participate in your network.

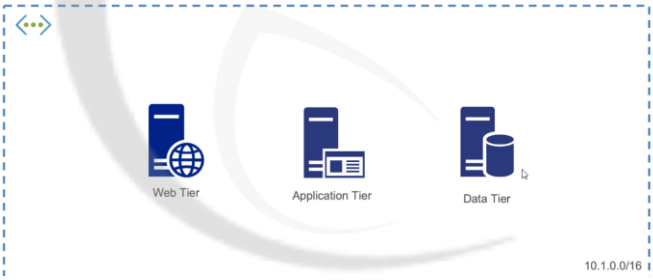
- The virtual network is your private network in the cloud and Azure allows you to create your network in the cloud where you can deploy your workloads.

What are Subnets?

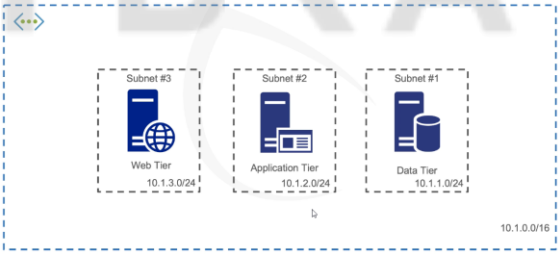
VNETs isolate your traffic from other customers in the cloud but how do you isolate the traffic within your own virtual network.
Let us look at a typical example by designing the network for a three Tier application environment. A typical web application can consist of three logical Tiers:

- Web Tier - like apache web application
- Application Tier - tomcat for running your application
- Data Tier - SQL database server for storing the data

Each Tier can consist of multiple virtual machines. All three Tiers are deployed in the same virtual network that has private address space 10.1.0.0/16.



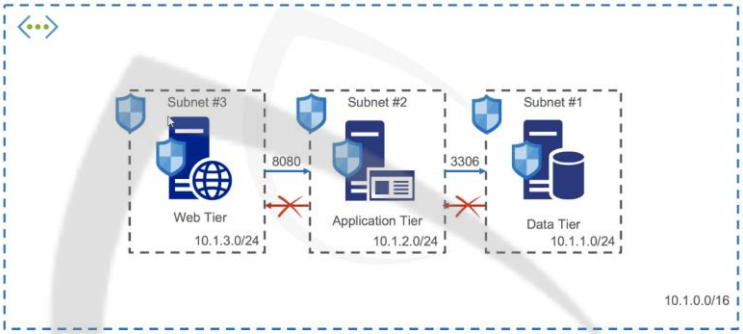
However, you want to secure access from your Data Tier from your Application Tier and access from the Application Tier from the Web Tier. To do this, you can segment your VNET into subnets. You can create three subnets, one for each Tier. Each one of the subnets will have its own address range which is a subset of the virtual network 10.1.0.0/16.



- You can protect each resources from undesired network traffic with an Azure Network Security Group (NSG).

Network security group (NSG)

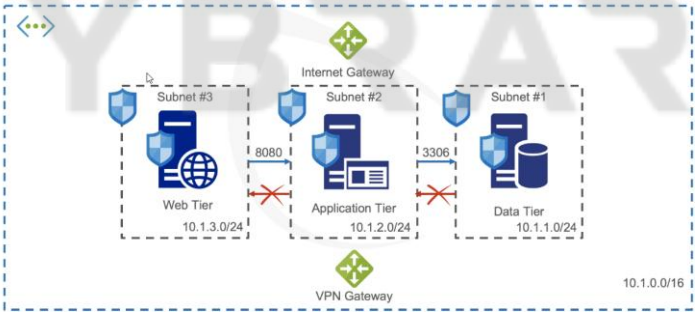
- It is a virtual firewall that allows or denies traffic to the resources.
- You can configure a network security group for subnets as well as the virtual machine in each Tier.



- In our example you can create a NSG for the Data Tier for accepting incoming traffic on port 3306 only and the NSG for our Application Tier for accepting incoming traffic on port 8080 only and all outgoing traffic can be denied.

Internet and VPN Gateway

- Let us say that your Application Tier need to make calls to an external web services via the internet. To do that, you can configure an internet gateway for your application.
- If your application Tier needs to communicate with your on-premise network, you can create a VPN Gateway that connects to your on-premise network.



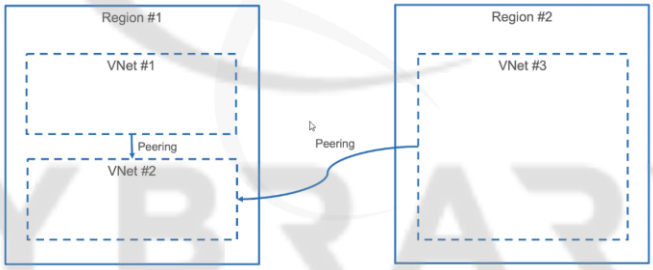
- This way, Azure VNET can become an extension of the on-premises network and you can easily transfer data between on-premise and the cloud and connect to your legacy application.
- As you remember from previous lesson, this is referred to as a Hybrid Cloud.

Routing tables

- You can describe all the possible routes for connectivity within the Routing Table in Azure.
- A Routing Table is created per virtual network.
- Most of the time, the Routing Tables are automatically updated when you create new resources like Internet Gateway or VPN Gateway. You can also create custom entries to overwrite the routes.

Azure Virtual Network

- You can create one or more virtual networks per Region.
- VNets are scope to a Region which means you cannot create a virtual network that spans multiple Regions.
- If you need to communicate between two virtual networks, you need to create a peer between the virtual networks.
- For example, if you have an Application servers in VNet #1 in Region 1 and VNet #3 in Region 2 that needs to communicate with another Application server in VNet #2 in Region 1, you need to establish peering connections between the VNet.



- Using VNets, you can deploy instances of your applications across the Globe and establish peering connections to allow those instances to communicate with each other to replicate data.

Now you know how virtual networks and how Azure allows you to create your own VNet in the Cloud and to extend your on-premise network.
In the next lesson, we will learn how you can extend your application using load balancers.

Lesson 8.2: Azure Load Balancer and Application Gateway

Skills Learned From This Lesson: Load Balancer, Application Gateway,Web Application Firewall

In this lesson, we will look at two more network services in Azure that allow you to deploy highly availability applications, Load balancer and Application Gateway.

We had discussed Availability and Resiliency before. In our lesson about SLAs, we had discussed on how we can increase the availability of our application by adding an additional VM to service web requests. But how do we configure the VM to do respond to users' request without the user knowing anything about them. You use a device called a Load balancer.

Load Balancer

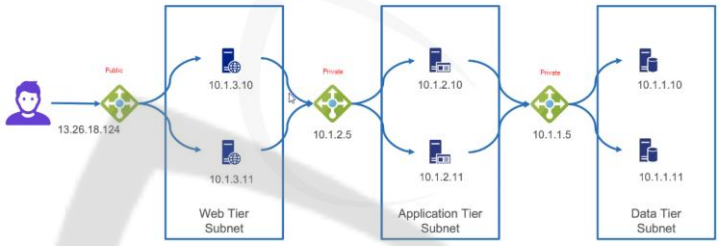
- It is a devices that distribute the traffic between devices within a pool or a cluster.
- In our particular case, we have two web applications and use the load balancer to balance the traffic between them. This is helpful because if one of the machines fails, it can redirect the traffic to the next working server.

- You can have as many machines as you desire behind the load balancer.
- They don't have to be identical although having identical machine is the most common approach.
- There are also different algorithms to distribute the traffic but the most common one is Round Robin where each new request are sent to the next machine in the pool. Once the machines are iterated, the traffic starts over with the first machine in the pool.

More About the Load Balancer

- The load balancer is a specialized device that does one simple thing, switching traffic.
- This allows it to handle high traffic load and connects many servers behind it.
- The load balancer can be exposed to the internet with a public IP address and the end user request gets forward to it. Then the load balancer forwards the traffic to the internal servers using the private IP address. This is referred to as Public load balancer.

- You can replicate the same setup for the other tiers of your application, but the only difference is that they are not exposed to the internet. Those are called Private load balancers.



- One important thing about the load balancer is that you can specify the port for the traffic you want to be balanced.
- You can use a friendly DNS name to point to the load balancer IP address

Azure Load Balancer

- It is a fully managed service that you use to balance TCP and UDP traffic
- It supports balancing both incoming and outgoing traffic.
- It also provides low latency and high throughput via needs
- You don't need to maintain any infrastructure, you just configure the service and defined the rule and Azure will handle the rest.

Azure Application Gateway

- Application Gateway is another load balancing application.
- It can balances web traffic only
- Application Gateway provides additional features that can protect your application using Web Application Firewall (WAF) which protects your application against SQL injection, cross-site scripting and brute force attacks.
- You can terminate SSL at the application gateway level to reduce encryption overhead or configure SSL encryption end to end for your application.
- You can configure custom URL-based routes, add or remove or rewrite HTTP headers of the request
- You can configure session affinity and send the request from the same client to the same servers and maintain the session.

- Keep in mind, that this may impact the performance of the application which is typical for legacy applications but discourage for the modern ones.

Now you know how you can scale your application providing resiliency and high availability using load balancer services offered by Azure.

Lesson 8.3: Reduce service latency with Azure Traffic Manager

Skills Learned From This Lesson: Azure Traffic Manager, Azure CDN, Load Balancing, Network latency

In this lesson, we will see how we can use Azure Traffic Manager to scale application globally.

Network Latency

You can use a load balancer to achieve resiliency and high availability for your application within a single region. But what if you have customers around the world.

Let's say you have your application deployed in the US West Region but your users are in Germany that needs to access this application. Every traffic will have to travel to US Westcoast and back to Germany. It doesn't matter how fast your data center processes the data or the how fast the user's internet is, it will take time for the data to travel from let us say Berlin to Washington.
The trip time is referred to as latency and it is measured in milliseconds (ms).
Now wouldn't it be faster for the traffic to travel to Germany North Region instead of US West Region.
Having your application deployed around the world will significantly improve the users experience because it will reduce the network latency for the user request. But how do you implement that.

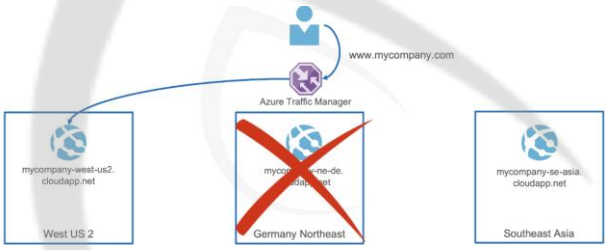
Azure Traffic Manager

- You can use a service that provides global load balancing service like Azure Traffic Manager.

This is how it works:

- You deploy exact copies of your application in each region where you have customers.
- Each deployment is accessible via a Deployment specific name.
- You configure the Azure traffic manager with those three endpoints.

- When a user types the URL of your website, the request is first evaluated by the Azure Traffic Manager.
- The traffic is sent to the closeth deployment of the application with the region of the user. The user traffic does not go through the Azure Traffic Manager, it only provide the DNS entry to the user to the closest deployment of the application.
- What the Azure Traffic Manager also does is if a region fails, the traffic will be pointed to another Region that is closest to the user request.
- Azure traffic manager works similar to the load balancer but on a global scale.



Azure Content Delivery Network (CDN)

- Another way to improve the user's experience when access applications is the Azure Content Delivery Network.
- It is a distributed network of servers that cache content around the world.
- Those servers can be hosted in the cloud or at the local service provider network.
- This makes the process of accessing the application even faster because the traffic does not have to travel to the nearest Azure data center but it can be even access the cache connected to the local service provider.
- Typical usage of the content delivery is to catch HTML, Java, OCS files, images, videos or other multimedia content or large downloads. Typical those require high bandwidth connections for faster downloads incase you need to improve the user’s experience.

With this we will wrap up the module with Azure Networking services.

Module Summary

In this lesson we learnt about the following topics:

- Virtual networks and subnets
- Azure Load Balancer and Application Gateway
- Azure Traffic Manager and CDN

Module 9
Security and trust in Azure

Module Introduction

- Shared responsibility model
- Azure Security Center overview
- Manage users and access with MD
- Encryption in Azure
- Restricting network access in Azure
- Azure Advanced Threat Protection

Lesson 9.1: Shared responsibility model

Skills Learned From This Lesson: Defense in Depth, Physical security, Digital Security, Policies and Procedures

Before we look at the tools and services available to secure your application and data in Azure. Let us take a look at the security responsibility in the Cloud.

Traditional Data Center Security

Let us start with how security is done in the traditional way where each enterprise have their own data center.

- Physical Security:
  - The first thing to think about is the physical security of the data center
  - Restricting access to the building
  - Installing security surveillance camera
  - Hiring guards and so on

- IT Security Policies and Procedures:
  - Next, you need to ensure that the personnel who are working in the datacenter and the users of the equipment such as developers, IT administrators comply with certain IT security policies and following IT security procedures.
  - These can include things like registering visitors requiring valid identification document for registration
  - Requiring strong passwords, etc.

- Digital Security:
  - The last thing is Digital Security that deals with securing the digital infrastructure like network segmentation, firewalls, application and user access and others.
  - As you can see, ensuring the security of your own datacenter is not a trivial job and requires a lot of expertise.

How do these responsibilities change in the Cloud?

- When you use the cloud, you do not maintain the data center. Microsoft is fully responsible for the physical securing the facilities, surveilling the building and hiring physical security personnel. Microsoft is solely responsible for the physical security of the data center.
- Microsoft is also responsible for establishing the IT security policies and procedures when it pertains to the data center or the hardware and the infrastructure in it. They are also responsible for any policies and procedures relating to the Azure platform itself. However, you as the customer is responsible for establishing the policies and procedures for your own applications and the data it handles.
- Last but not least, Microsoft is responsible for the Digital Security of the Azure platform. This includes the platform itself that it cannot be compromised tenants residing on the platform are authenticated and or only authorized to use their own resources, management APIs and so on. However, you as the customer is responsible for the digital security of your application and the data that it handles. This means that you should ensure that user should of the application are properly authenticated, the data is properly encrypted and so on.

Shared Responsibility in Azure

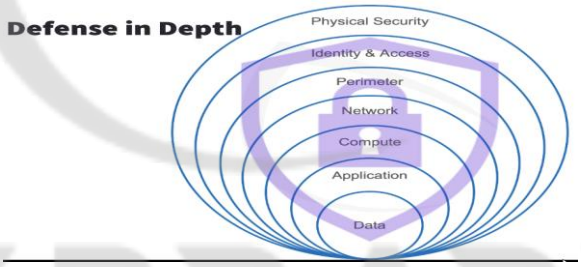
We are now going to look at the different layers in the application stack and let us identify who is the responsibilities for each of them:

Responsibilities	On-Premise	IaaS	PaaS	Saas
Data governance & rights mgmt	customer	customer	customer	customer
Client endpoints	customer	customer	customer	customer
Account & access management	customer	customer	customer	customer
Identity & directory infrastructure	customer	customer	Customer + Microsoft	Customer + Microsoft
Application	customer	customer	Customer + Microsoft	Microsoft
Network controls	customer	customer	Customer +	Microsoft

			Microsoft	
Operating System	customer	customer	Microsoft	Microsoft
Physical hosts	customer	Microsoft	Microsoft	Microsoft
Physical network	customer	Microsoft	Microsoft	Microsoft
Physical datacenter	customer	Microsoft	Microsoft	Microsoft

Defense in Depth

- Microsoft apply a layered approach to security that is known as Defense in Depth.
- Defence in Depth is a strategy that deploys a series of mechanism to slow the advancement of an attack targeted to acquiring access to information.
- It can be visualized as concentric circles with the data to be secured in the data center.
- Each layer provides protection but if one of the layers is breached, the others are in



place to prevent further exposure.

- Data Layer
  - it is the inner layer of the circle
  - The customer is responsible for the security of the data and controlling the access to it. Quite often there are compliance and regulatory requirements that dictate the controls and processes that needs to be in place to ensure the Confidentiality, Integrity and Availability (CIA) of the data.
  - Things you can do at this layer are to ensure that data is encrypted at rest, in transit, and restrict the access to data on a need to know basis.
- Application Layer
  - This is the next layer.

    - By integrating security in the application lifecycle, the application owners can ensure that application is secure by default.
    - Making security a requirement as part of the application design, will reduce the number of vulnerabilities present in the code.
    - Make sure the security is included in the application design, the code is free from vulnerability and secrets are taken out of the configuration files and stored in a secure storage.
- Compute Layer
    - Securing the compute infrastructure ensure proper access controls and endpoint protection are in place.
    - Patching and updating are an integral part of securing the infrastructure of your application.
- Network Layer
    - The goal is to limit the connectivity between system to the minimum required. By doing this, you can prevent that lateral movement throughout the network.
    - Ensure that you deny access by default, and only allow ports and systems that need to interact.
- Perimeter Layer
    - At this layer, you protect the access of your network from external attackers utilizing the firewall functionality will allow you to identify and alert on malicious activity against your network.
    - DDoS protection services filters large scale attacks before reaching you or your endpoints.
- Identity & Access Layer
    - This layer ensures that identities are not compromised and access is granted to authorized parties and activities are monitored.
    - This ensures that login attempts are logged and alert on and your users use Single Sign On (SSO) for the easy management and multi-factor authentication for stronger protection.
- Physical Security
    - This layer is the first line of defense and its goal is to prevent unauthorized physical access to the assets and by-pass the other security measures.

In the next lesson, we will be looking at the tools Azure offers to apply the Defence in Depth security.

Lesson 9.2: Overview of Azure Security Center

Skills Learned From This Lesson: Azure Security Center (ASC), ASC Capabilities, ASC Scenarios

Azure Security Center (ASC) is monitoring service that provides threat protection not only for your Azure workload but also for your on-premise ones.
Let us see what you can do with it.

Azure Security Center Capabilities

- ASC is a central place where you can monitor the security posture of your cloud workload and solutions.
- It can continuously monitor all your solutions and to perform automatic security assessments to identify vulnerabilities and provide recommendations.
- It uses machine learning intelligences to block malware from being installed on your virtual machine. You can configure a list of allowed applications that the system should not deviate from.
- It can Identify potential inbound attack against your network and assist you investigate threats, do forensic analysis of possible breach activities.
- It enables you to do Just-in-time access for ports and users and help you reduce your attack surface.
- It monitors security settings across on-premise and cloud workloads to help you manage your complete application infrastructure.
- Azure Security Center comes in two Tiers:
    - Free Tier - limited to assessment and recommendations.
    - Standard Tier - that includes continuous monitoring, threat detection, Just-in-time access and more.
- The Free Tier is included with your Azure subscription while the standard tier

Azure Security Center Scenarios

- Azure Security Center can assist you in two main scenarios:
    a. To enhance your security of the cloud in the Cloud with the help of the security recommendations. You can leverage the building and create your own security

that Azure security center can evaluate and give you recommendations, if those are not followed for resources or applications. Once you evaluate those recommendations, you can perform the corrective actions that need to be made.

b. You can also use the Azure Security Center has part of your Incident Response plan. Azure security center is very helpful in the Detect--Assess-->Diagnosis stages allowing you to discover the first indication of an event, perform an assessment and gather information about the suspicious activity and perform a technical investigation to determine containment and potential mitigation actions.

Now that you know how to review your security posture in Azure, let us see how you can manage access.

Lesson 9.3: Manage users and access with AAD

Skills Learned From This Lesson: Authentication, Authorization, Role-based Authentication Control, Privileged Identity Management, MFA, AAD, Service Principal, MSI

Now let us see how we can manage users and access in Azure.

Authentication and Authorizations

- Authentication and Authorization are the fundamental concepts when discussing Identity and Access Management (IAM). let us take a look at what is the differences between those.

AuthN

Authentication (abbreviated AuthN)

- This is the process of establishing identity of a person or an Application looking to gain access to the resource or data.
- In essene, it confirms who they say they are?
- Authentication is not new to the world, the use of passports, drivers license or other identification methods are all examples of authentication in the offline world.
- Authentication is the basis of creating security principle to can be used to access resources

Authorization (abbreviated AuthZ)

- Authorization on the other hand establishes the level of access the principles as.
- It determines what data or resources, they are allowed to access. For example, an employee can access their own payroll information while an accountant can access the payroll information for the entire company.

AuthZ

Azure Active Directory

We already had a brief discussion our Azure Active Directory but let us look a bit deeper into it.

- Azure Active Directory (AAD) is a cloud-based identity that you can use to synchronized their on-premise entities with other enterprise software

like Office365 and Dynamics365. This means that you can use the same identity across applications.

- AAD provides services like:
    - Authentication
    - Single Sign On (SSO)
    - Business-to-Business (B2B)
    - Business-to-Consumer (B2C)
    - Application Management
    - Device Management

Single Sign On (SSO)

- The more identities that a user has to manage, the greater the risk of credential-related security incident.
- Different applications have different password policies and with the growth of complexity, managing those become challenging.
- On the other side, if a user leaves the organization, removing the user's credential from every application will be a tedious task.
- With SSO, users will need to remember only one password which will simplify the security model.
- Using Azure Active Directory for SSO, you also have the ability to create intelligent security graph that you can use to do a threat management and offer a real-time identity protection for all your users.

Multi-Factor Authentication (MFA)

- Another technology that provides the protection of user's identity is the Multi-Factor Authentication.
- MFA is also known as Two-Form Factor Authentication (2FA) because it requires two or more elements for a full authentication.
- Those elements fall into the following categories:
    - Something you Know - like password or a security question
    - Something you Have - like an authenticator app or a text message to your phone

    - Something you Are - like your fingerprint or iris or face
- MFA increase the security of the user's accounts because the probability of a hacker to have access to all the above factors is extremely low.
- Azure AD has built-in capabilities to manage MFA and can integrate with external MFA providers.
- The functionality is free of charge for users of designated global administrators in Azure AD because those are highly sensitive accounts.
- Other user accounts can have MFA enabled but after purchasing a licenses.

Security Identities

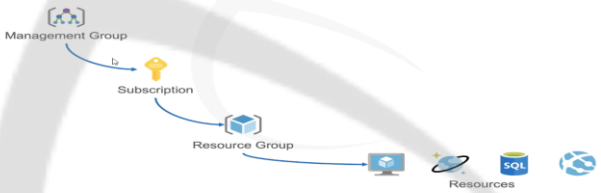
- Azure Active Directory also allows you to create service identity.
- Service Identities are keep in Azure and eliminate the need to store those in configuration file, thus reducing the exposure of the credentials.
- AAD has two ways to handle service identities:
    - The first one is the use of a service principal. To understand what a service principal is, let us look at the difference between a service principal and identity. Identity is a thing that can be authenticated. This can be a user with a username and password or it can be an application or server that can authenticate with a certificates and keys. Principal is an identity that acts with a certain claims and roles assigned to it. A service principal requires a configuration step that makes them a tedious process. You need to create the principal, configure the server and the application to use it. Then you have to maintain, the principal throughout the application lifecycle.
    - The use of managed services identity (MSI) is much easier, because all the work of configuration and administration is done by Azure. The infrastructure is responsible for establishing the identity and authenticating with the service. Within your application, you can use this identity as any ordinary Azure AD user Identity. Not all services in Azure supports the Managed Service Identity (MSI) as of now but the list is constantly growing.

Role-Based Access Control (RBAC)

We mentioned the roles in previously but what are they really useful for?

- Roles are sets of granular permissions that can be assigned to users.

- Azure has a builtin roles for Reader, Contributor and Global Administrator but you can create custom ones if builtin ones does not satisfies you.
- Identity are mapped to roles either directly or through a group membership.
- Roles can be granted at the individual resource level but they can also be flowing down the Azure Hierarchy.
- Roles assigned at the higher level of the hierarchy is considered in effect at the lower levels.



Privilege Identity Management (PIM)

- Azure does not only give you the tools to manage the access for your users but those tools to audit your own members.
- Azure Privileged Identity Management completes the set of tools you need to achieve a high level of regulatory compliance for your workloads in Azure.
- Azure PIM is a paid offering available to customers who purchase:
    - Azure Premium (P2)
    - Or Enterprise Mobility Security (E5)
    - Or Microsoft 365 (M5).

In the next lesson, we are going to learn how we can utilize encryption in Azure.

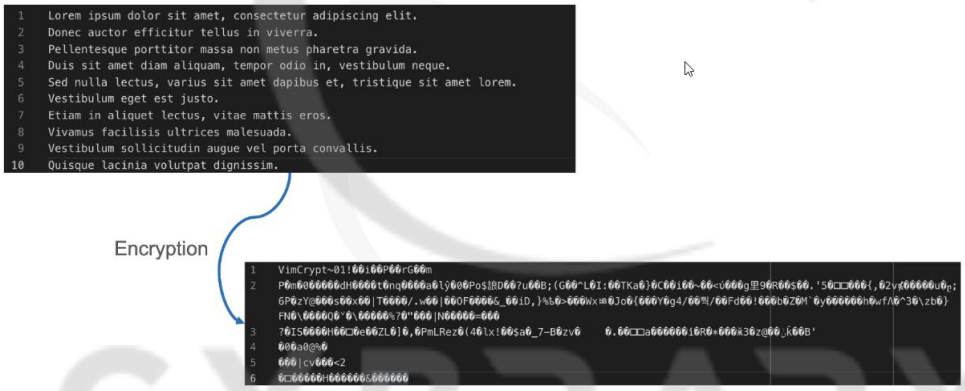
Lesson 9.4: Encryption in Azure

Skills Learned From This Lesson: Encryption, Symmetric Encryption, Asymmetric Encryption, Encryption in Transit, Encryption at Rest, Encryptions in Azure, Azure Key Vault

Encryption is the last line of defense for your data, let us see how azure helps encrypts your data and protect it even if a breach occurs.

What is Encryption?

- Encryption is the process of encoding information in a way that only authorized parties can read it. For example where the plain lorem ipsum text file is encrypted with a Vim encryption command. Unless you know the encryption key, you will not be able to decode the file and read its content.



- There are two types of encryption
  - Symmetric Encryption
  - Asymmetric Encryption

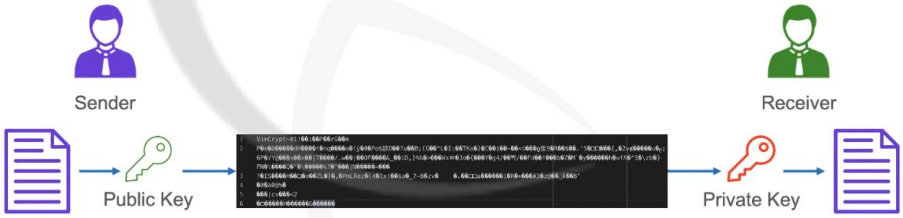
Symmetric Encryption

- Here is how it works, the sender uses the key to encrypt the data and on the receiver side the same key is used to decrypt the data.
- If the receiver needs to resend the data, the receiver will use the same key and then send it over.

- Because the key needs to remain secret, both parties need to find a way to distribute the key without compromising it.
- This makes it difficult to distribute the key over public infrastructure.

Asymmetric Encryption

- to solve this issue of the distribution of keys, hence the asymmetric encryption was created.
- Instead of a single key, two related keys are generated: a public key and a private key.
- The public key is derived from the private key, however you cannot use the public key to generate the private key.
- The public is published in a way that is accessible to everybody. While the private key remains secure at the receiving party.
- When a sender wants to send information to the receiver, the sender uses the public key to encrypt the information. The receiver uses the private key to decrypt the information to read its content.



- Asymmetric encryption is used to implement a part of a series of negotiation protocol like Transport Layer Security (TLS) as well as message signing where only the owner of the private key can sign the message and everybody else can verify the signature using the public key.

Encryption in Transit

- Data in transit is when the data is actively moving from one location to another. The purpose of encryption is to protect the data from outside intruders and limiting the exposure.
- You can achieve this by encrypting the data before sending it over the network.
- Protocols such as IPSec, TLS, SSH, HTTPS helps you to do that at the application layer.
- You can also use a secure channel like VPN which encrypts all the traffic between the two parties transparent to the application.

Encryption at Rest

- Data at rest is data that is stored on a physical media. The purpose of encryption is that if an unauthorized party gains access to the remote storage, it renders the data unusable without the encryption key.
- Regulatory requirements states that sensitive data should be encrypted at rest and in transit.

Encryption in Azure

Azure provides several features to help you with encryption of your data. You should utilize those if you are looking to comply with regulatory compliance or certifications.

- Azure Storage Service Encryption (SSE) is a feature of Azure storage that automatically encrypt that data before persisting it to Azure Blob, Azure Disk, Azure Files or Azure Queue.
- Azure Disk Encryption (ADE) is a feature that helps to encrypts your virtual machines. It leverages bitlocker on Windows and vimcrypt for linux to provide encryption for the operating system and the data disk attached to the virtual machines.
    - ADE is integrated with Azure key vault to store the encryption keys and uses managed services identity functionality to obtain the key used to decrypt the disk.
- Transparent Data Encryption [TDE] - is used to protect SQL databases and Azure data warehouses against malicious activities.
    - TDE encrypts and decrypts the database, any associated backup files as well as the transactions logs in realtime and it is transparent to your application.
    - It does this using an asymmetric key called the Database Encryption Key that is generated for each unique database instances.
    - It integrates with Azure Key Vault allows you to also bring your own key.
- Azure Key Vault - in addition to integrating with many services in Azure and storing encryption key.
    - It can be used to store and manage application secrets. You can configure your application to use and manage services identity and retrieve the necessary services secret from the key vault using API calls. This way you remove the need to store secrets in configuration files.

- Azure key vault can also be used for certificate management. It integrates with external Certificate Authority (CA) and allows easily allows you to provision, deploy and manage SSL/TLS certificates for your application.
- Azure Key Vault keys and secrets can be protected by a software or a hardware security module call HSM validated by FIPS 140-2 Level 2.

Here wraps up out discussion on encryption in Azure. In the next lesson, we will take a look at Restricting networks access in Azure.

Lesson 9.5: Restrict network access in Azure

Skills Learned From This Lesson: Network Access, Firewall, DDoS Protection,VPN Gateway

Let us look at the Azure tools that can assist you with your network protection.

Protection at the Perimeter

We had discussed the layered approach of the security model. Protecting the perimeter of your network is an essential part of this approach. You can use Azure security center to identify the part of your networks that are currently exposed but are not protected by a firewall.

- A firewall is a device or service that inspects the network traffic and grants access based on the originating IP address, network protocol and port. You can create firewall rules that specify the IP address or IP ranges, protocol or some ports to ensure that only the allowed request are forwarded to the target resources.

Azure Firewall Options

- Azure provides several firewall options for you to protect your network from external attacks.
- Azure firewall - is a full-managed services that protects resources in your virtual network.
    - It has a builtin high availability and it can scale on demand.
    - Azure firewall is a layer 3 firewall and can protect you from not only HTTP/HTTPS attacks but also other protocol attacks like SSH or desktop protocol like FTP.
- Azure Application Gateway
    - It has a builtin web application firewall that can protect you web workloads from common attacks such as cross-site scripting and SQL injection.
- Network Virtual Appliances (NVAs)
    - The Azure marketplace has offers for third party network virtual appliances that are similar to hardware appliances and offer advanced configuration for applications and solutions that require granular configurations.

Distributed Denial of Service (DDoS) Protection

- Any resources exposes to the internet is prone to Distributed Denial of Service (DDoS) attacks.
- The attackers goal is to overwhelm the endpoints by sending so many requests that the resource becomes unresponsive.
- Azure DDoS protection service can be used to provide the defense against DDoS attacks.
- Azure DDoS monitors the traffic at the network perimeter and if an attack is detected you will be notified using the Azure monitor metrics.
- The service comes with two Tiers:
    - Basic - that is automatically enabled with the Azure platform. It uses the same algorithm that provide protection for all other Microsoft services.
    - Standard - that provides additional capabilities that are tuned based on the traffic that is used in the Azure network.
- Azure DDoS protection uses machine learning to learn the communication patterns of the resources deployed within the VNet and mitigate against various types of attacks like the metric ones where an attack tries to simulate legitimate traffic, protocol attacks where protocols are exploited or resource layout where application traffic is disruptive.

Protection Inside the Network

- You need to also include protection inside your network and prevent the lateral movement of attackers if one of your defences fails.
- As we discussed previously, Network Security Group is critical to protect your internal resources.
- Network Security Groups are resource base firewalls that allows you to block inbound and outbound traffic based on IP addresses, protocols and ports.
- It is recommended to deny all communicates between systems that are not a work of your applications.
- You can remove the public access of your services by restricting access to the service endpoints practically limiting the traffic to the VNet only.
- Communication with your on-premise workloads can be configured via Virtual Private Network that communicates with the VPN device on the on-premises or via a dedicated connection via the ExpressRoute that allows you to also have a private connection to

other Microsoft services like Office365 and Dynamics365. This limits the exposure to DDoS services as well.

In the next lesson, we will see how we can use the Azure Advanced Threat Protection to detect threats against your workload infrastructure.

Lesson 9.6: Azure Advanced Threat Protection

Skills Learned From This Lesson: Azure Advanced Threat Protection, Azure Intelligence Graph, Azure ATP Portal

ATP - Advanced Threat Protection

- ATP is a cloud service that helps you to investigate Adv threats, malicious insight activity and compromised identities.
- It consists of three (3) components:.
    - Azure ATP Portal (https://portal.atp.azure.com)
    - Azure ATP Sensors
    - Azure ATP Service

Azure Advanced Threat Protection (ATP) Portal

- You can access the Portal from the url https://portal.atp.azure.com
- In the portal you can monitor and respond to suspicious activity as well as manage and investigate threat in your network environment.
- You must be assigned Azure ATP Administrator role for your instance to have access the ATP Portal

Azure ATP Sensors - monitoring data displayed in the portal are collected by ATP sensors that are installed on the DC

Azure ATP Services

- Azure ATP services are connected to Microsoft Azure intelligent Graph and run some Azure infrastructure reports in the USA, Europe and Asia
- Azure ATP is a part of the Enterprise Mobility & Security (EC5) sweet or you can purchase it to extend your long licenses.
- It is not available for purchase through Azure Portal

In the next module, we will discuss monitoring compliance with Azure Policy.

Module Summary

Shared security responsibility model

- Defense in depth
- Overview of Azure Security Center
- Azure Active Directory capabilities
- Symmetric and asymmetric encryption
- Encryption in transit and at rest
- Protecting Azure Virtual Network
- Azure Threat Protection
- Shared security responsibility model

Module 10
Monitor compliance with Azure Policy

Module Introduction

In this module, we are going to discuss the following topics:

- Azure policies and initiatives
- Enterprise governance in Azure
- Compliance and trust resources
- Monitoring workload in Azure

Lesson 10.1: Introduction to Azure Policy

Skills Learned From This Lesson: Azure Policy, Policy Effects, Initiatives, Policy Definition, Policy Scope

Let us see how we can create standards for cloud usage in your organization.

What is a Policy?

- Policy is a set of rules and standards that you defined
- Policies can be of any kind. An example of a policy is that a developer can only use a B1S virtual machines for development purposes or that production machines must have endpoint protection installed on them or that our resources must follow a certain naming convention and have a standard set of text applied.
- Having well developed policies and standards on how the employees use the resources can assist you to stay compliant, reduces cost and provide consistent service to your customers.

Azure Policy

- Azure Policy is a service that allows you to define, assign and manage your standards for your workloads.
- Using Azure Policy can prevent the creation of disallowed resources and ensuring resources have certain configurations settings and run evaluation for policy compliance.
- Steps to follow when creating a policy are:
    - Create a definition
    - Assigned this definition to a scope of resources
    - And view the results of the Policy evaluation

Policy Definition

- A policy definition describes what needs to be evaluated and what corrective actions to take.
- One example is that the policy checks what is VM SKUs is selected during creation, if the SKU is not in the outline, the creation is disallowed.
- Policy definitions are written as JSON files and can be imported/exported out of Azure and can be easily automated.

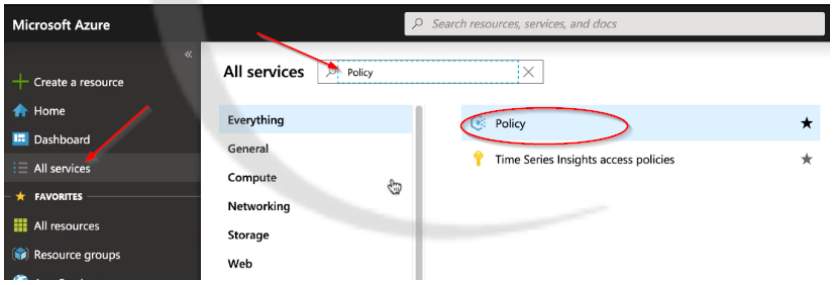
- Azure comes with a builtin policy out of the box.
- The Azure policies are available in the definition section of the Azure policy blade.
- You can also download a lot of policy definition from GitHub.

Policy Scope

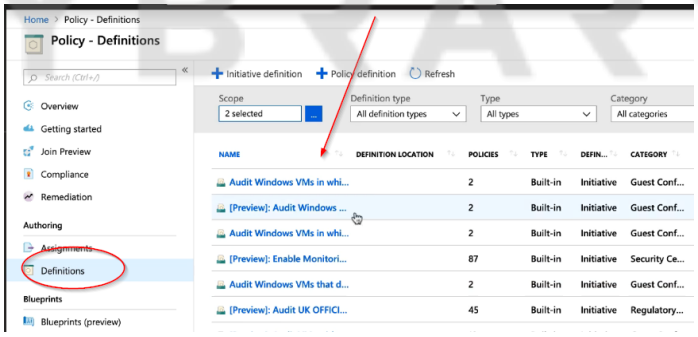
- Once you create a policy definition, you need to assign it to a scope.
- The scope can be add a subscription level which means it is applied to everything within the subscription.
- The scope can also be at the resource group level which means it will apply to every resource within the resource group.
- You can also exclude the subscription scope from the assignment.

This is how it is done in the Azure portal:

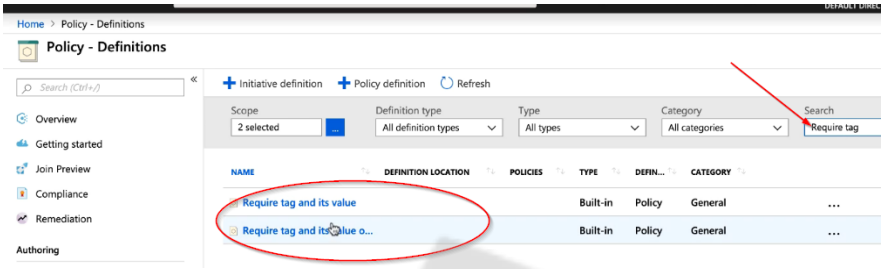
1. Go to Policy through the search in **All services**



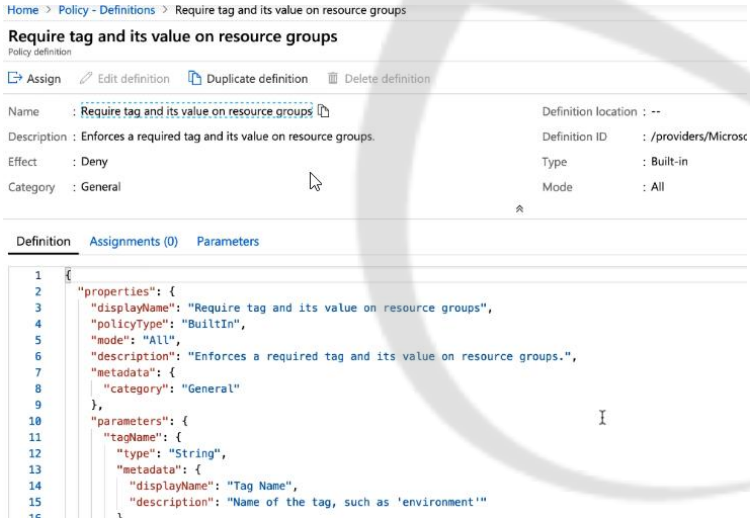
2. Select **Policy**
3. Select **Definitions**



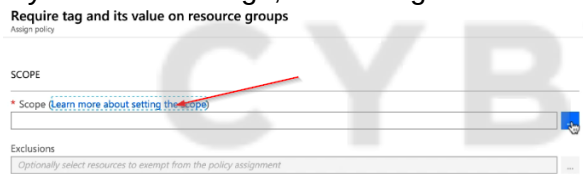
You will see all the available policies in Azure with the out of the box policies.
You can search for a policy like “require tag”



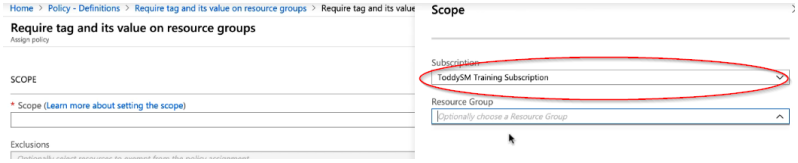
You can click on a policy to review it before assigning it.



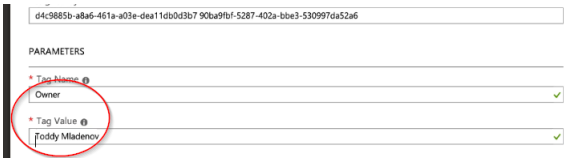
If you click on assign, it will bring the new blade where you can assign the scope of the policy.



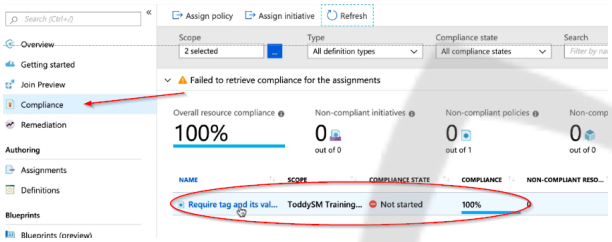
You will then select your scope, in this case the subscription “ToddySM Training Subscription”



Because this policy is about tags you will scroll down and enter the parameters Tag name and value



Once done, it will assign the policy but note that it will take some time to evaluate.



Policy Effects

- Every request to create and update resources in Azure resource manager is evaluated by Azure policy.
- Each policy definition has a single effect. The effect will tell me what happens if the policy rule matches.

Here is a list of policy effects.

Policy Effects	Results	Policy Example(s)
Disabled	The rule is normally ignored. The effect is used for testing	
Append	Adds additional fields to the requested resource during creation or update	Tax on resources such as owner or cost center.
Deny	Prevents the resource request that doesn't match defined standards through a policy definition and fails the request	To not deploy expensive VMs for development environment if chosen.
Audit	Creates a warning event in	To raise an awareness if the

	the activity log when evaluating a non-compliant resource, but doesn't stop the request	encryption policy is not on for a SQL database
AuditIfNotExist	Enables auditing on resources that match the if condition, but doesn't have the components specified in the details of the then condition	To check if Anti-malware software is not installed on a VM and if not, raise an alert
DeployIfNotExist	Executes a template deployment when the condition is met	To deploy a Anti-malware software if it does not exist.
EnforceRegoPolicy	This effect is used with a policy definition mode of Microsoft.ContainerService.Data. It's used to pass admission control rules defined with Reqo to Open Policy Agent (CPA) on Azure Kubernetes Service.	It is a preview policy specifically for the Kubernetes service.

Now you know how to define, assign and review the policy results.

Initiatives

- Enterprises may have hundreds of policies defined. Assigning those one by one can be cumbersome and error prone. It will also be good to group the policies by some criteria.
- For example, you may want to group them by environment: Development, Production and Test.
- You can do this Azure with the help of Initiatives. Initiatives follows the same process as policies, you create a definition of policies, then you assign the initiatives to a scope.
- The scope for initiative assignments can range from management group to resource group.

In the next lesson, we will discuss what management groups are.

Lesson 10.2: Enterprise Governance With Management Groups and Blueprints

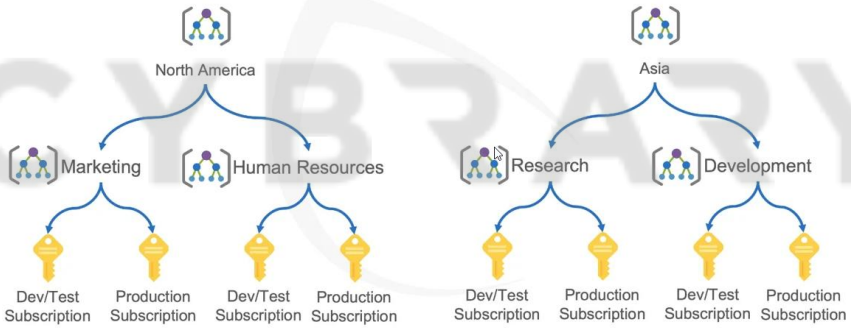
Skills Learned From This Lesson: Management Groups, Azure Blueprint, Enterprise Governance, subscriptions

Let us see how you can bring enterprise governance to your cloud workloads.

Management Groups

We have seen how we can manage the policies and the role-based access control at a subscription level. But at the beginning of the course, we discussed how you can separate workloads by environment, department, region and so on.

- When you have multiple subscriptions, you can use management groups to manage access to policies and compliance.
- Management Groups are containers that allow you to bring organization to your Azure resources across subscriptions.
- All subscription within a management group can carry the access settings and policy settings that is carried by the group.
- Also a policy assignment done, at the management group level cannot be modified by the subscription owner which means that you are protected from improper governance.



Azure Blueprint

- To assist you even further with compliance requirements, traceability and auditing of your deployment, Azure provided the Azure Blueprint service.

- Azure Blueprint allows you to define a repeatable set of Azure resources that follows your organizational standards.
- For example by using Azure blueprint, your development or IT teams can ensure that deployment are consist with the environments policies.
- Azure Blueprint uses a declarative way describe and orchestrate the deployment of resources and other artifacts such as roles and policy assignment, ARM templates, etc,
- Unlike Azure Resource Manager (ARM) templates, the Azure blueprint preserves the relationship between the definition and what is deployed. This allows you to track and audit your deployment. This approach is very useful in DevOPS scenarios where blueprints are associated with the specific built artifacts and releases.

Now you know what tools you can use for enterprise governance for your organization.

Lesson 10.3: Explore Microsoft Compliance and Trust Resources

Skills Learned From This Lesson: Microsoft Compliance, Microsoft Trust Center, Service Trust Portal, Compliance Manager

We have discussed the shared responsibilities of the Cloud Security in the previous lesson. Compliance is not any different, in addition to governing your resources, you also need to understand what standards and policies Microsoft uses to manage the underlying infrastructure. Microsoft is very transparent about how they manage their infrastructure. The entry point to learn about Microsoft certifications and policies is through Microsoft Trust Center.

Microsoft Trust Center

- Microsoft Trust Center is a website where you can find information on how Microsoft apply security, how they deal with privacy and how they comply with Government regulations around the world. Reference: https:// www.microsoft.com/en-us/trust-center
- Microsoft Trust Center applies to all microsoft products including Azure, Office365, Dynamics365 and Microsoft 365.
- Things that you can find here are solutions and recommendations for implementing secure workloads on Azure.
- Microsoft privacy statement and documentation helping you how Microsoft handles yours and your customer's private data.
- A comprehensive list of Compliance offerings for Azure including regional compliance and other important documentation that provides transparency of how Microsoft operates.

Service Trust Portal (STP)

- Service Trust Portal is microsoft public websites from publishing auditing reports and other compliance related information that is related to Microsoft cloud services.
- You can use the service trust portal (https://servicetrust.microsoft.com) to download the audit reports from external auditor, penetration testing and security assessment reports as well as internal microsoft reports.
- At the STP portal, you can find information about your own compliance standards and regulations like GDPR, HIPAA, NIST, ISO and many more.

Compliance Manager

- The STP host the Microsoft Compliance Manager - which is a workflow based risk assessment dashboard that allow you to track your organization compliance. It offers features like: (reference: https://servicetrust.microsoft.com/compliancemanager
    - Self assessment of organization compliance with difference standards
    - Enables you to assign and track your progress on different controls.
    - It provides resource repository for managing artifacts relating to compliance activities producing rich reports that can be submitted to Auditors and Compliance auditors.
    - It also provides recommended action.

Now you know how you can find information on regulatory compliance on Azure.

Lesson 10.4: Monitor Your Workloads

Skills Learned From This Lesson:Azure Monitor, Azure Service Health, Application Insight, Autoscale, Azure Monitor for Containers and VMs

Whether you have workloads running on-premise or in the cloud, you need to have a way to know if they are working as expected. For workloads in the cloud, you should know whether the vendor infrastructure is available or your application is up and running.
Azure provides two services that can help you monitor the health of your applications.

Azure Monitor

- Azure monitor is a service that allows you to collect, analyze and act on telemetry data from your on-premise and cloud environments.
- You can collect data from various sources, application data like performance and function data.
- You can collect data from any type of customer applications regardless of language or framework it is written in.
    - Data about the guest OS, your application is running on. It can be running on Linux, Windows or the Cloud.
    - Data about the operation or resources you are leveraging, subscription data relating to your organization or the management of your Azure subscriptions.
    - Data about the operation of global Azure resources like Azure Active Directory or any other activities performed under your tenant account.
    - Last but not least, it collects data about Azure itself.

Diagnostics Settings

- There are various things you can configure and monitor.
- You can enable activity logs of your subscription to collect information of any changes that is happening for example creating or resources, VM shutdown or access change.
- This is very important for Compliance auditing.
- You can also enable guest-level monitoring and configure guest-agents for windows and linux.

- You can collect performance counters for your application resources, things like CPU and memory utilization and collect event logs for things that are happening in your Application or VMs as well as VM crash dumps.
- You can also forwards to the other tools like splunk using Sinks.

Azure monitor has other tools that are targets for specialized use cases.

Azure Monitor - Application Insights

- Application insights allows you to monitor the performance and availability of your web applications.
- You can use the Application Insights running an Azure as well as on-premise or other clouds and you can easily integrate it into your OPS process.

Azure Monitor for Containers

- Azure monitor for containers is a service that is designed to monitor the performance of your container based workloads deployed to Azure kubernetes services.
- It collects performance and monitoring data from containers and Nodes that available via Kubernetes APIs or as well as container logs.

Azure Monitor for VMs

- Azure monitor for VMs is a service that allows you to monitor the health of your Windows and Linux VMs.

Integrating those with Azure service health, helps you to understand if the health of your partial services impacts the performance and health of your own workloads. We will look at the Azure Service Health later on in this lesson.

Azure Monitor Alert and Visualization

- Effective monitoring solutions do not only provide the tools to correct and analyze the data but also give you the tools to log and respond to events.
- Azure monitoring uses a logs to proactively notify you if critical conditions within your environment occurs.
- You can configure notifications via email, SMS or integration tools like Slack.

- A lot of it can be like near real-time based metrics like CPU and memory utilization or can use analytics for more complex environment.

Azure monitor - Autoscale

- Azure monitor can also allow you to create rules that can be determine if new resources need to be provisioned in order to handle the increased load.
- Autoscale can manage your cost by automatically increasing or decreasing the number of resources when demand changes.

Azure monitor provides its own visualization capabilities which also leverages other tools like Azure Dashboard to PowerBI to send customer reports that represents the data.

Azure Service Health

- Azure Service Health is a sweet of services that provide an overview of the health of Azure services across regions as well as personalized guidance and support for services that directly affects you.
- You can receive notifications that can help you to understand the impact of Azure health of your services that prepares you for scheduled maintenance.
- Azure Status is publicly available website that provides a global view of the health of Azure services. Reference: https://status.azure.com/en-gb/status
- Service Health is a customized service that is available within Azure portal, it tracks the state of Azure services that you use in the regions you have your workload deployed.
- With Azure service Health, you can track the state of ongoing issues and upcoming maintenance windows or get relevant health advisories.
- Events are kept in your health history for up to 90 days.
- You can create health alert from within service health.
- Resources Health is a part of the Service Health blade in the azure portal. It shows the details about the current and pass health of you individual resources.
- You can use it to identify the times in the past where your service has not been available because of Azure outages and help you to understand if the SLAs has been violated.

Azure Monitor and Azure Service Health components offers a comprehensive view of the health of your cloud workload.

Module Summary

In this module, you have learnt about the following topics:

- Azure Policy and Azure Initiatives
- Azure Management Groups and Azure Blueprints
- Microsoft Trust Center and Service Trust Portal
- Compliance Manager
- Azure Monitor and Service Health

Module 11
Azure Resource Manager

Module Introduction

In this module, you are going to learn about:

- Azure Resource Groups
- Tagging resources in Azure
- Resource locks

Lesson 11.1: Azure Resource Groups

Skills Learned From This Lesson: Azure Resource Manager, Azure resource group, Organizational principles

Azure Resource Manager (ARM)

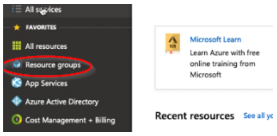
- Azure Resource Manager is a set of features that allow you to organize, deploy and detect resources.
- For example you can Azure resource group and tags to organize the resources
- ARM Templates to deploy resources
- Resource lock to protect resources from modification and deletion.

Azure Resource Groups

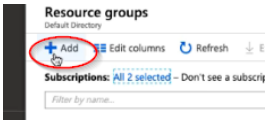
- Azure resource groups are logical containers for resources deployed in Azure.
- Every resource in Azure must belong to a single resource group.
- Resource groups are created within subscription and are used to organize resources with a single subscription.
- You can move resources between resource groups if you determine their placement is not appropriate.
- Resource groups are used to apply role-based access control for easier management.
- If you delete a resource group, all the resources within that group are also deleted.
- This makes it easy to cleanup temporary environment easily but it can be dangerous if someone deletes a production resource group.
- We will see how we can protect from such mistakes later on in this module.
- You can create resource group in different ways using the portal, using Azure PowerShell, Azure CLI, Blueprint and Azure SDK.

Demonstrate the creation of a Resource Group

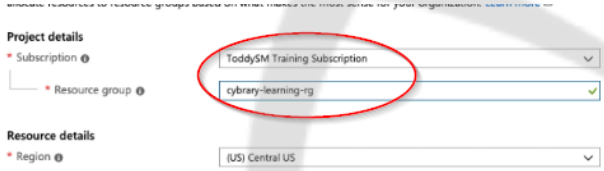
Let us see how we can create a resource group in the Portal

1. Start by clicking on Resource groups 

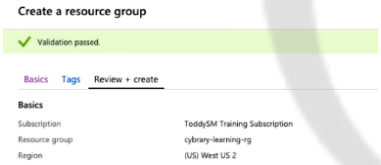
2. Under the resource group, click Add



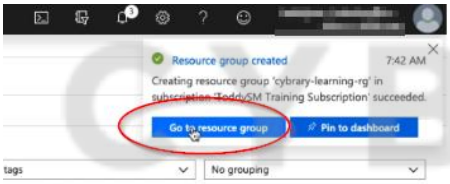
3. Select the subscription you want to associate with this resource group with and enter a name and select the Region to host the RG.



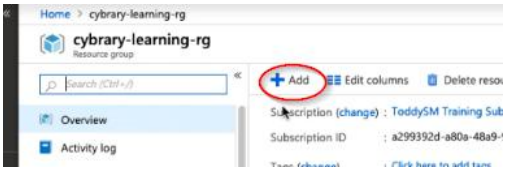
4. Select **Review + create**



5. Then you can go to the resource group and select the resource group created (cybrary-learning-rg)

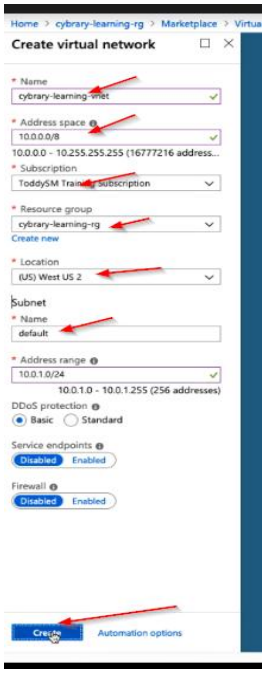


6. Select Add to add a resource to the resource group.



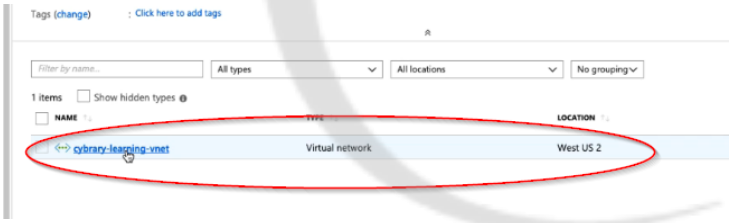
7. Search the marketplace for virtual networks, select it

8. Then select create button for the virtual networks



9. Enter the parameters for the virtual network: name, address space, subscription, resource group (created one), Location (this region is not required to be the same as the resource group) and the other parameters.

10. Select Create
11. Then the virtual network will be created in the resource group.
12. You can go the resource group and see that the virtual network is present.



Organizational principles

As we mentioned, we can use the resource group to organize our resources. There is no one right method for organizations but it all depends on your needs. Here are some guidelines:

- Develop a consistent naming convention for your resource groups. The name should give an indication of what the resource group is used for. Example cybrary-marketing-frontend-rg
- There are many different ways to organize your resources. You can use resource type for example. Here we have resources organized in networking, security, compute and databases:

- You can use development lifecycle of the organization. Here we have naming based on environment: 

- You can organize the resources based on department. Here we have HR, marketing and finance: 

- You can combine the types for example department and environment:


- Last but not least, you can organize your resources based on billing purposes. This way you can detailed spending information for each one of your environment in the specific departments.

When you are thinking about your organization resource group, you must think about who needs access to those resources which will assist in assigning the appropriate resources to specific groups.

Lesson 11.2: Tagging Resources

Skills Learned From This Lesson: Tagging, Organizing Resources, Applying Tagging

What is Tagging?

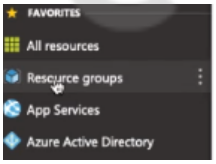
- This is a feature that allows you to arrange your resources or resource groups in Azure.
- Tags are named value/key pairs that can be applied to Azure resources or resources groups. Tags can be considered as text metadata that you can add to your resources.
- Tags can be used to add information to your resources that are meaningful to your organization.
- Each resources can have up to 15 Tags.
- Each Tag key is limited to 512 Characters except for storage resources such as Blobs, Tables and Cubes which is limited to 128 Characters.
- On the other hand Tag values are limited to 256 characters.
- Tags are no inherited from the parent resources. For example, if a tag is applied to a resource group, the tag is not applied to resources within the group.
- Importantly, not all resources supports tagging as yet.

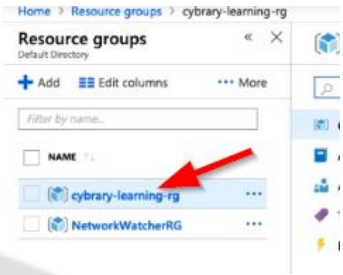
Applying Tagging

The first demonstration will be to apply the tagging to a resource group

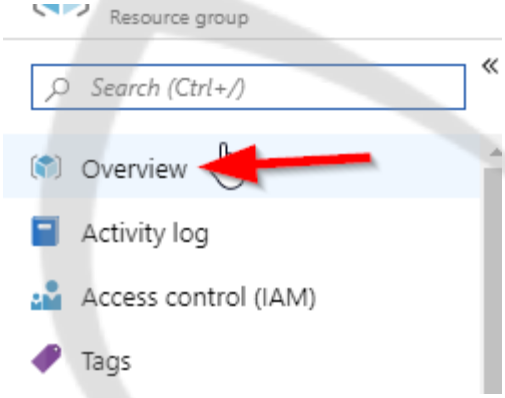
1. Log into the Azure Portal http://portal.azure.com

2. Click on Resource group from left panel

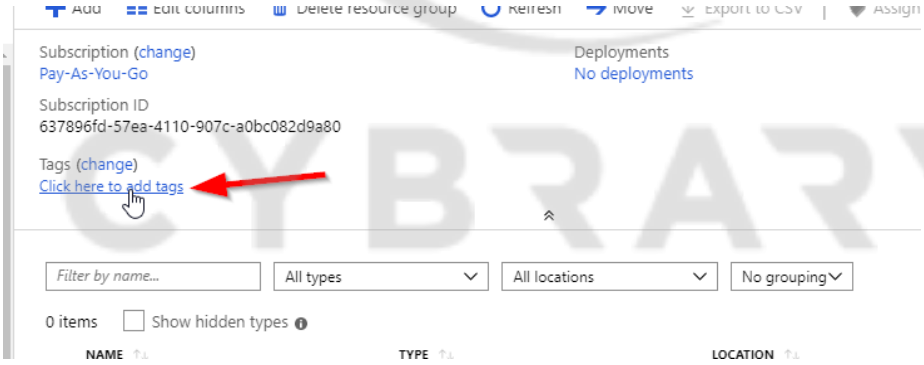




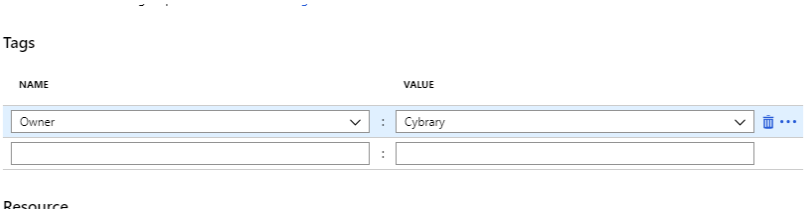
3. Highlight your resource group



4. Select Overview
5. At the top of the resource listing, select change (tags) or click here to add tags

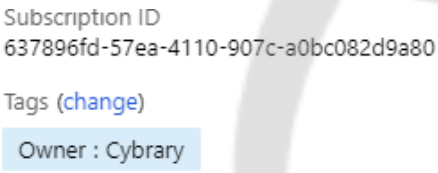


6. Enter the name and the value of choice, here it is:
    a. Name: Owner

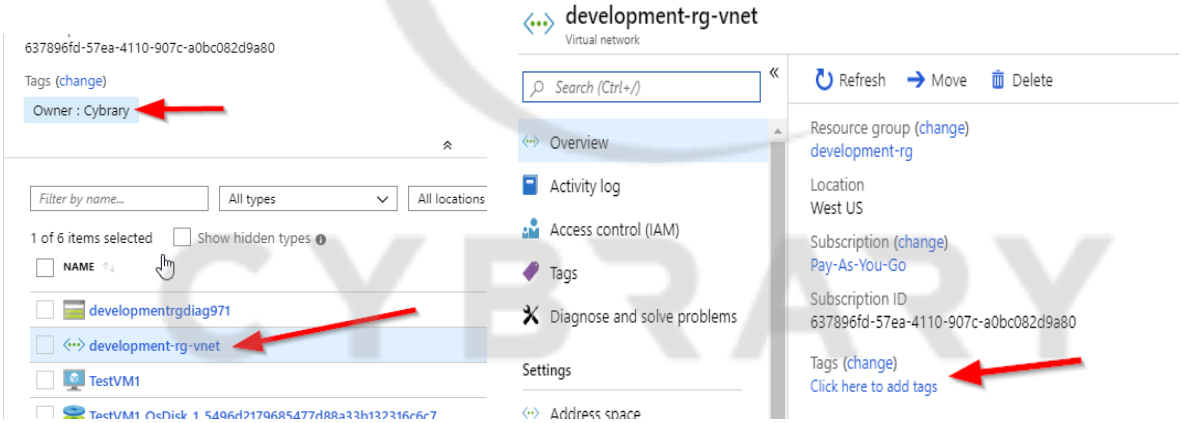


b. Value: Cybrary

7. Select **Save**
8. It will be displayed under the Tags



9. You will notice that as stated the tags that are applied to the resource group is not applied to the resources within the group:



10. To add Tags to the resource, follow the same instructions for the resource groups.

Organizing resources with Tags

- You can use tags in my different ways:
- Organizing for Billing

    - You can tag each resources with a Cost Center
    - You can use this tag to pull the resources consumption for the cost center using the tag.
    - You can use the Cost Management APIs to pull reports or export reports from the Cost Management Blades in Azure portal.
- Organizing for management and releases
    - For example you want to deploy a version 2 of your product and then shut down the resources for version 1 after a period of time. This can be accomplished by referencing tags
- Organizing for monitoring
    - You can use tags for reference to ownership of resources and when a resources goes down, you can know which owner to notify of the failure.
    - You can set-up an alerts that is configured to use the tag to alert the owners
- Use for Automation
    - You can configure tags that start the start up time and shut down time of the resources and then configure a batch to execute the states based on the tag value
- Use for Azure Policy
    - You can use tags to apply policies and enforce standards.

Now you know how to use tags to add an additional organizational principles to your resources in Azure.

Lesson 11.3: Resource Locks

Skills Learned From This Lesson: Resource Locks, Creating Resource Locks, Deleting Resource locks.

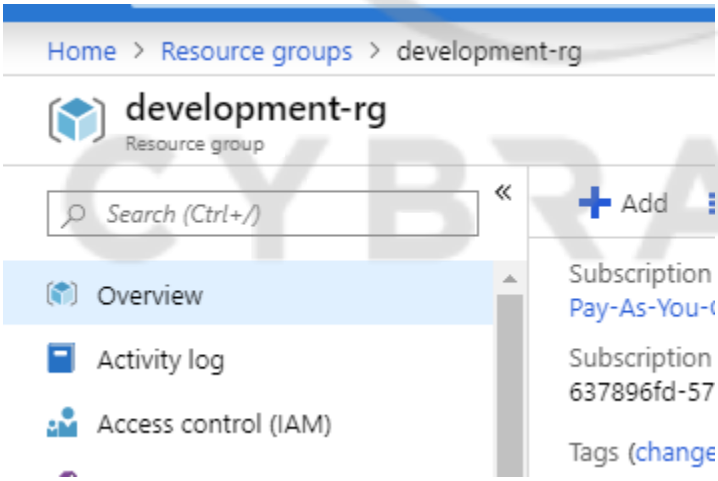
What is resource locks?

Organization is great but how do you protect your resources from accidental deletions or modification. This task can be accomplished by using Resource Locks.
:

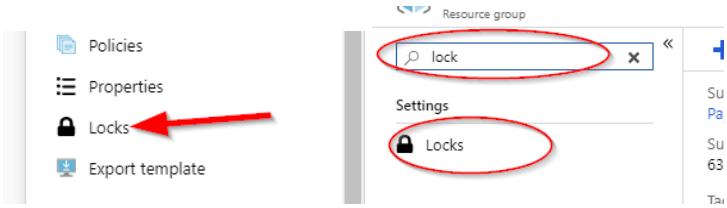
- It is a setting that can be applied to a setting
- It is a restAPI
- Resources lock types
    - Delete
    - Read-only
        - Prevent users from accessing the storage key

Creating a resource lock

1. Go to the resource group

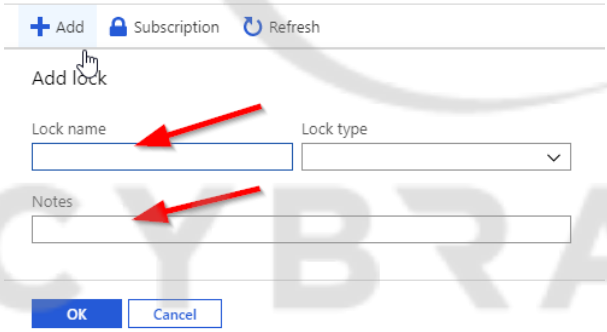


2. Select or search for Locks



3. Select Add

4. Enter details:
    a. Lock Name
    b. Select Lock type: Read-only or Delete
    c. Lock note



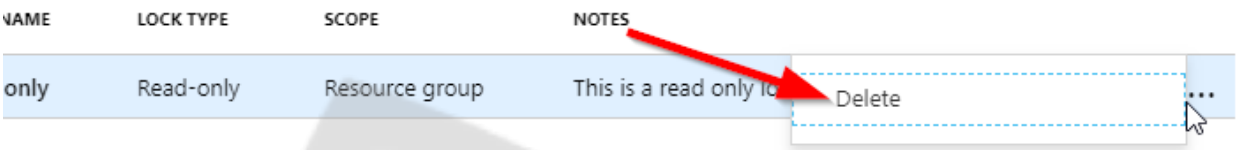
5. Select OK

6. You will see the lock setting listed under the lock blade:

LOCK NAME	LOCK TYPE	SCOPE	NOTES
Read-only	Read-only	Resource group	This is a read only lock on rg

Deleting Resource Lock

1. Select the … beside the lock
2. Click on Delete



3. The lock is now removed.

Module Summary

In this module, we have learnt about the following topics:

- Azure Resource Manager (ARM) and Azure Resource Groups
- Custom organization with tags
- Prevent modification with resource locks

Module 12 Monitor Costs and Control Expense in Azure

Module Introduction

In this module, we will learn:

- Purchasing services and billing in Azure
- Estimate costs with Azure Pricing CalcuLator
- Monitor spending on Azure
- Calculating TCO
- Reducing costs on Azure

Lesson 12.1: Purchasing and BIlling for Azure Services

Skills Learned From This Lesson: Azure Purchase Options, Usage Meters, Factors Affecting Cost, Billing

Before we look at the cost management and optimization in Azure, let us take a look at the different ways you can purchase Azure services.

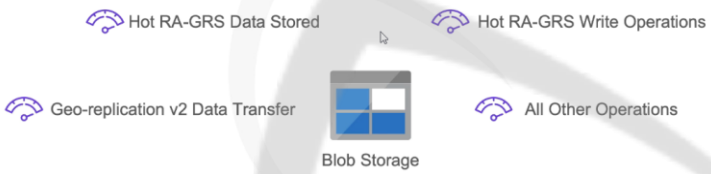
Azure Purchasing Options

There are three (3) ways you can purchase Azure services:

- Web Direct:
  - The standard way to purchase Azure is through the standard website.
  - It is called Web Direct or it is referred to as Pay-as-you-go
  - Web direct customers pay retail price of the services and are billed at a monthly basis.
- Enterprise Agreement
  - If you are an enterprise and plan to deploy many applications in Azure, you can sign an enterprise agreement with Microsoft.
  - In this agreement you commit to certain spending per year and prepaid upfront for the year.
  - Although this can be a significant investment, you can benefit from the customized pricing that Azure offers and purchase services at a significant discount.
  - You can purchase enterprise agreement from authorize Microsoft Partners.
- Cloud Solutions Partner
  - One last method of purchasing service for Azure is through a Cloud Solution Partner.
  - Those are Microsoft partners who can sell Azure and other Microsoft products and services.
  - Quite often those are bundles with additional services from the Partners for example managed services.

Usage Meters

- It does not matter how you purchase Azure services, the billing that is done is the same.
- When you provision a resource in Azure, the platform creates a so called usage meter for the resources.
- Each meter tracks particular type of usage.
- for example, the Blob Storage may have the following meters:



  - RA-GRS data stored- that keep track of the data stored in the Blob
  - Hot RA-GRS write operations that keep tracks of the writes done to the Blob
  - Geo-Replication v2 Data transfer- that keeps track of the data during replication transfer
  - And there is a meter for All other operations.
  - In addition, you may have Data transfer Out (Bandwidth) - that keeps track of data that is read from outside the Azure.
- At the end of the billing cycle, the user is charged to their subscription payment method and then the meters are reset.
- You can download your usage any time from the Azure Portal.
- The most important thing to remember is that you are charged based on usage.
- If you have resources that you don't need, you should terminate them.
- You should be careful about stopping versus terminating resources because although you are not charged CPU or memory for a stopped VM, you will incur charges for the storage disk.

Factors Affecting Cost

- There are several factors affecting the cost of your services.
- Different resources types has different cost as well as different usage meter supply.
- The way you purchase resources also impact the cost. As we mentioned, the enterprise agreement prices can have discounts and the price differs from the Web direct and Service Provider prices. Also if you purchase third party products from Azure

marketplace, you will be paying not only Azure resources but also licenses and subscription fees for the third party applications.

- Location of the resources also plays a role in the pricing. Different locations has different infrastructure cost like electricity, cooling, local taxes that can impact the resource pricing.
- Last but not least, bandwidth pricing depend on the so-called Azure billing zones. Inbound data transfer (ingress) is normally free but outbound data transfer (egress) is charged according to the billing zones. The billing zones is a grouping of two or more regions for billing purposes. Here is the grouping Azure uses:

Zone	Areas
Zone 1	UA, Canada, UK, Europe (except Germany)
Zone 2	Asia Pacific, Japan, Australia, India. Korea
Zone 3	Brazil
DE Zone 1	Germany

For most zones, the first 5GB of data transfer is free.

Now you know how to purchase Azure and the billing is done.

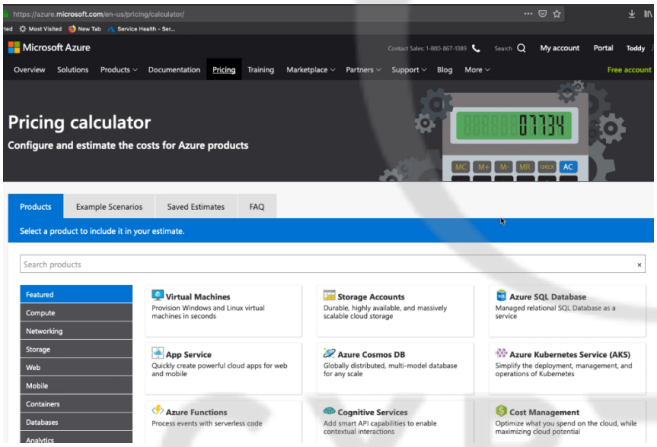
Lesson 12.2: Azure Pricing Calculator

Skills Learned From This Lesson: Azure Price Calculator, Estimated Cost for Application Gateway, Estimated Cost for App Services, Estimated Cost for Azure SQL Database

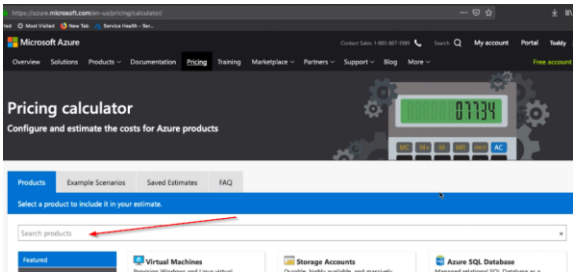
Now that you know how to purchase Azure services, let us look at how we can calculate our billing in Azure.

Azure Pricing Calculator

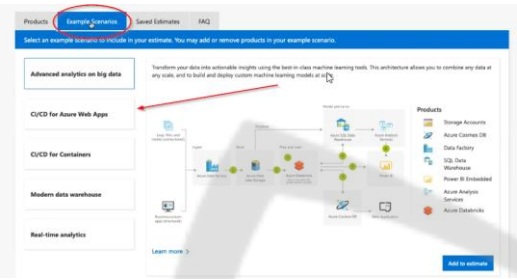
- The Azure pricing calculator can be accessed at the url https://azure.microsoft.com/en-us/pricing/calculator
- Here is a look at the pricing calculator



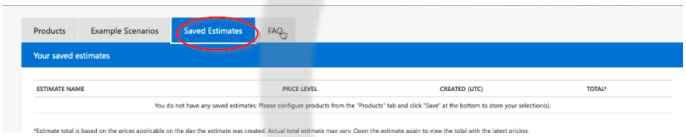
- It is a free web-based tool that allows you to select Azure services and modify the options and get a pricing estimate. As you will see on the website, there is a list of all the services you can choose from or you can search for the service using the Search bar.



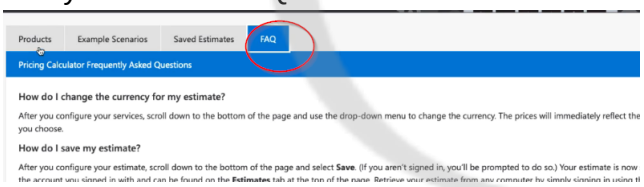
- When you search for the service, the estimate will show up at the bottom of the page allowing you to modify the settings.
- You can also choose from a number of examples by selecting Examples Scenarios tab:



- You can also save the estimates for later use:

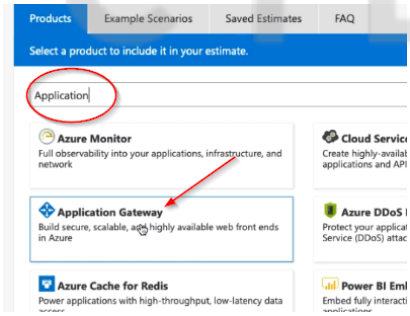


- And you can see FAQs:

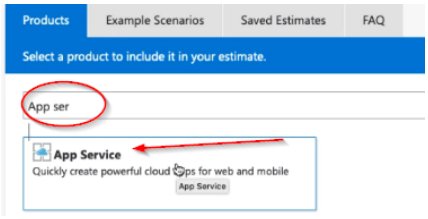


Adding Azure Services for Estimations

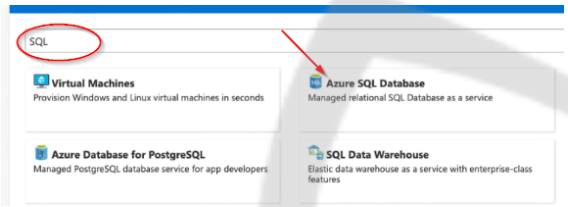
- Let use say we are going to estimate cost of Application Gateway:
- Enter “Application” in the search bar and select Application Gateway



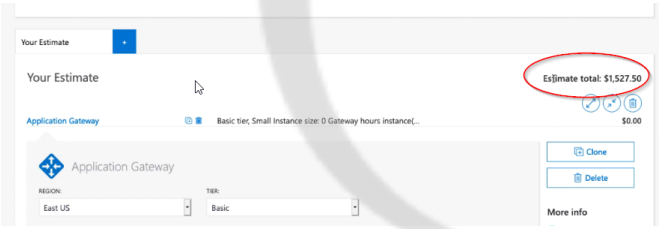
- Next we search for App services and then added it



- Then we are going to add Azure SQL Database



- Most of the information provided will be a general estimate. You will notice that the estimated cost will be about $1,527.00

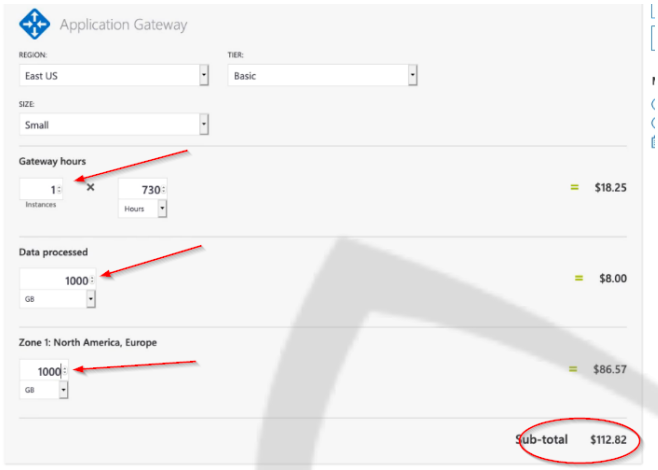


- The reason for this high cost is because the Azure SQL database is pre-populated with data.

What we are going to do is modify the settings of easy Azure services in order to match our environment.

Estimate Cost for Application Gateway

- We will assume that we will have one application gateway processing 1TB of data with a transfer rate of 1 TB which is configured below.



- Estimated cost is $113 for defined parameters.

Estimate Cost for App Service

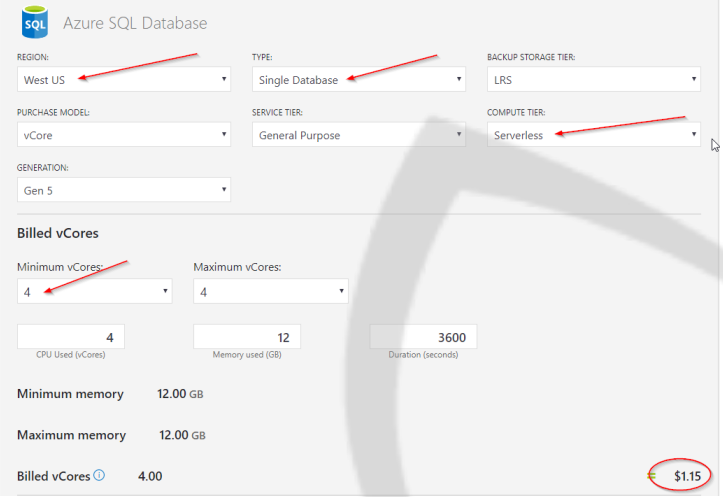
- We will configure the App service to be in US West, using a Basic Tier B1 Windows instance:

- The estimated cost is approximately $55.00 per month.

Estimate Cost for Azure SQL Database

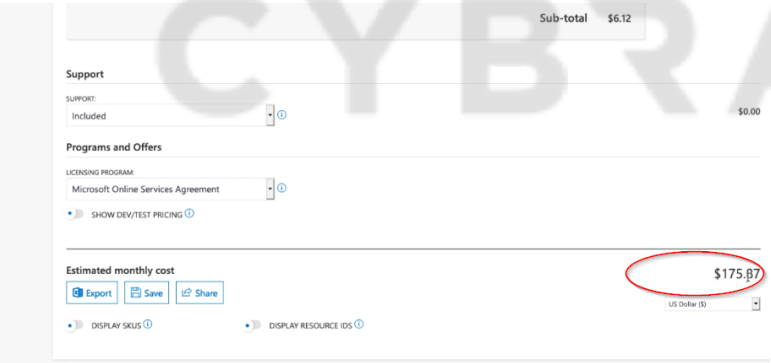
- Next we will configure the Azure SQL database with the following settings:
    - Region: West US

- Type: Single Database
- Compute Tier: Serverless
- vCore: 4



- You will notice that the estimate for SQL database dropped significantly, when choosing Tier to serverless. Also it is recommended to use type managed instance, because it gives you the best SLA.
- You will see the estimated cost is $ 1.15 per month

When you scrolled down to the bottom of the estimate, you will see the total for all services combined. It will cost approximately $176 per month.



From there you can Export, Save or Share the report estimate. You can export it in an Excel format. If you are logged into Azure, it will automatically save it when you select Save. When you Share the report, you will get a URL link to share with others.

Now you know how you to use the Azure Pricing calculator to estimate the cost of your Azure services.

Lesson 12.3: Exploring Azure Cost Management Tools

Skills Learned From This Lesson: Azure Advisor, Azure Cost Management, Cost Analysis

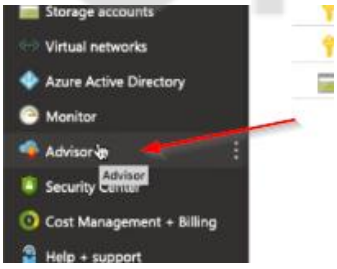
You can estimate your cost with Azure Pricing calculator but you will also want to track your spending one you have workloads deployed on Azure. Let us look at a few tools that can assist you with that.

Azure Advisor Recommendations

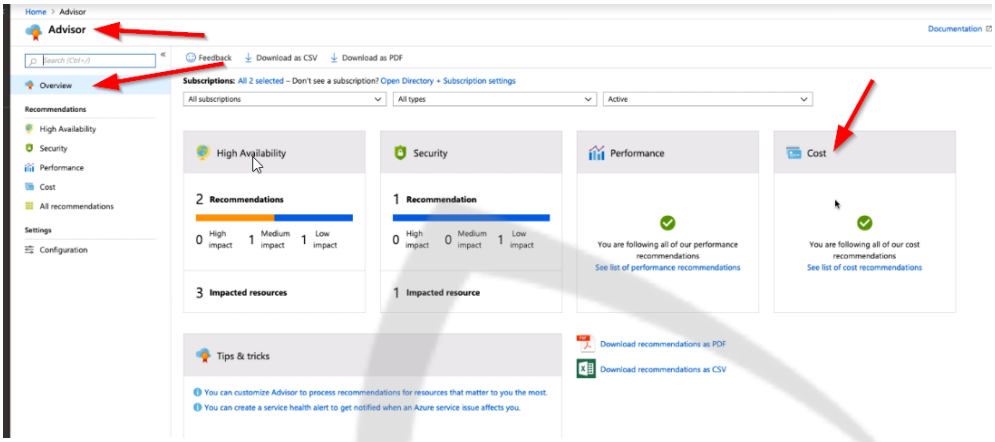
- We have mentioned Azure Advisor in the previous lesson when we discuss about compliance. However, Azure Advisor can assist you with financial governance. There are three (3) areas where Azure advisor can give you cost recommendations.
- Azure monitors virtual machines over a period of 14 days and identifies underutilized virtual machines. You can play with the parameters that determine if a VM is underutilized but by default those are less than 5% of average CPU utilization and less than 5 MB network usage. If you see such VMs, you may want to resize them to smaller instance sizes.
- In addition, Azure can analyze the use of your VMs over a 30 days period and give you recommendations whether you can save money using reserved instances. It gives you the regions and sizes where you can have more savings.
- If you use ExpressRoute for connectivity to on-premise, Azure advisor can identify unprovision circuits and advise you to delete those to reduce the cost.

Let us see how you can find Azure Advisor in the Portal:

- As usual, you can find the Azure Advisor in the favourites list or you can go to All services and search for it.

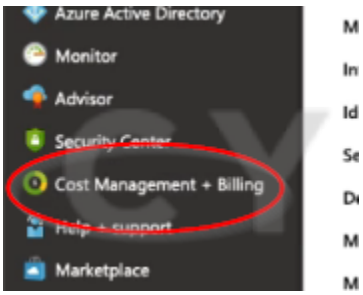


- When you go to Azure Advisor, you will see a number of recommendations for High Availability, Security and Performance but Cost is the area you will explore.

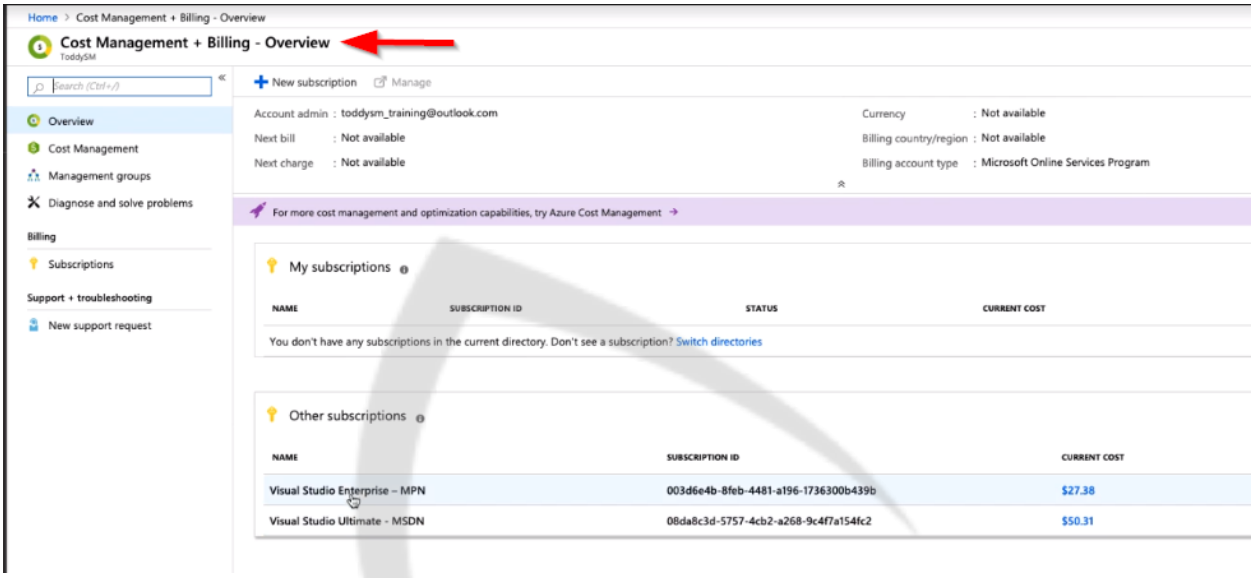


Azure Cost Management

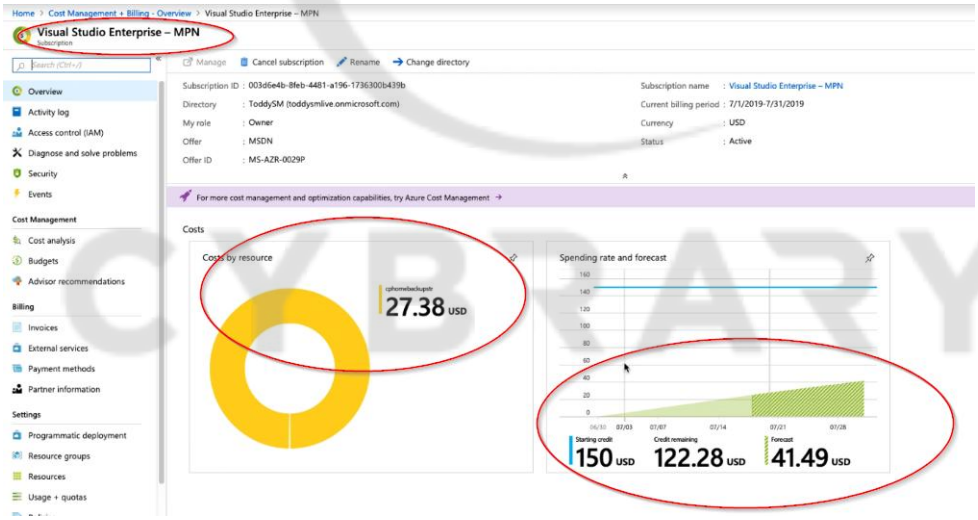
- Another free tool you can use to explore cost in Azure is the Azure Cost Management.
- You can do analysis of the data and break down the cost into resources types and meters.
- Let us see how you can get to the Azure Cost Management in the Portal:



- When you go to it, it will give you an overview of all the subscriptions that you have. Your own subscriptions as well as the subscriptions that you have access to view the cost.



- In this portal, the Visual Studio Enterprise - MPN will be selected to see a sample of the costing breakdown.

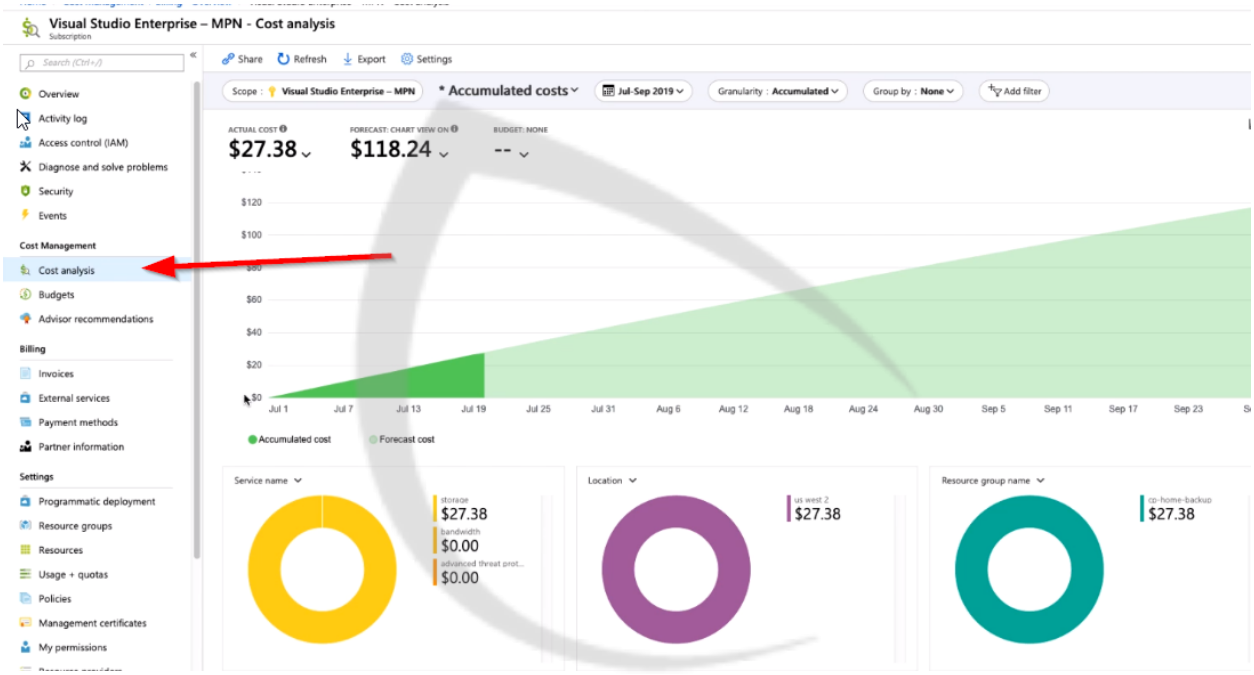


- In the image, it shows the spending rate, forecast and the billing date.

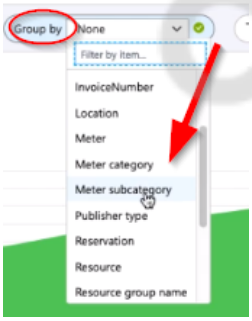
If you want to go deeper you will go to the Cost analysis.

Cost Analysis

- The cost analysis will allow you to change the parameters to see further reports, for example the spending cost for the quarter July - Sep 2019 as seen below:



- You can group the information by different parameters or conditions outlined below



- And filter by a resource group name

With the cost analysis, you can export the cost and send it via email or share it as an XML file.

Now you know how you can get recommendations for reducing your cost and how to manage your cost in Azure.

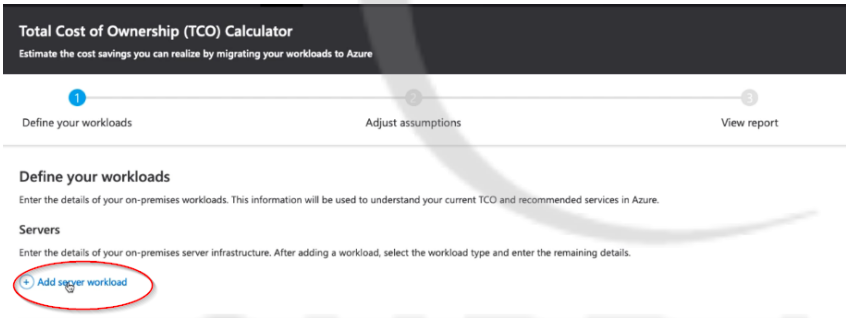
Lesson 12.4: Exploring Azure TCO Calculator

Skills Learned From This Lesson: Total Cost of Ownership, TCO for Server, Database Workloads and Storage, Adjusting TCO Assumptions.

Exploring TCO Calculator

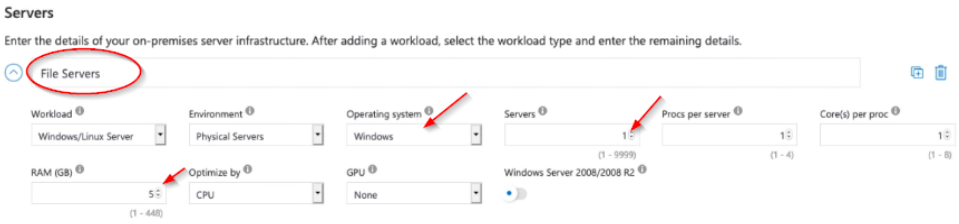
- Microsoft offers a tool where you can determine your total cost of ownership and potential savings to migrate your on-premise workloads to Azure. Let us take a look at it.
- The TCO calculator can be access via web using URL: https://azure.microsoft.com/en-us/pricing/tco/calculator
- It is a web based tool that is free to use whether you are an Azure customer or not and you can go and add your on-premise workloads, adjust your assumptions and get a report of what will be your savings in Azure.

Let us see what we can do:



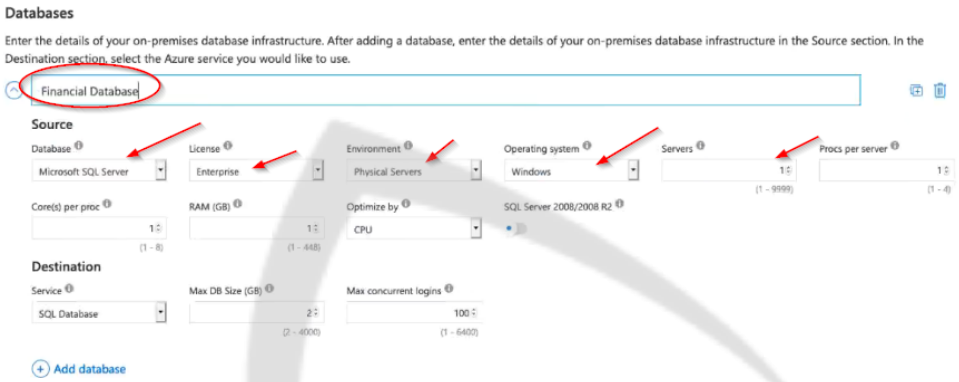
Server Workloads

- You can add server workloads such as a Windows File server



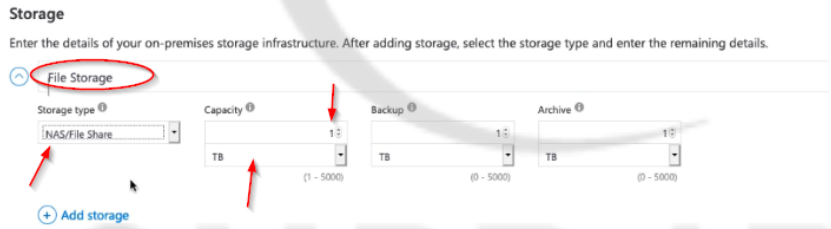
Database workloads

- You can added Database workloads such as Microsoft SQL server



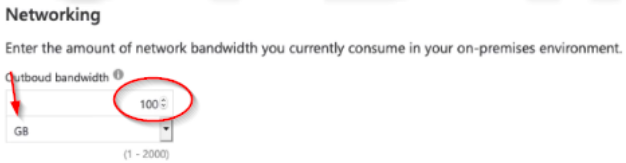
Storage Device

- You can add a storage device such as a NAS with 1 TB of data:



Networking Utilization

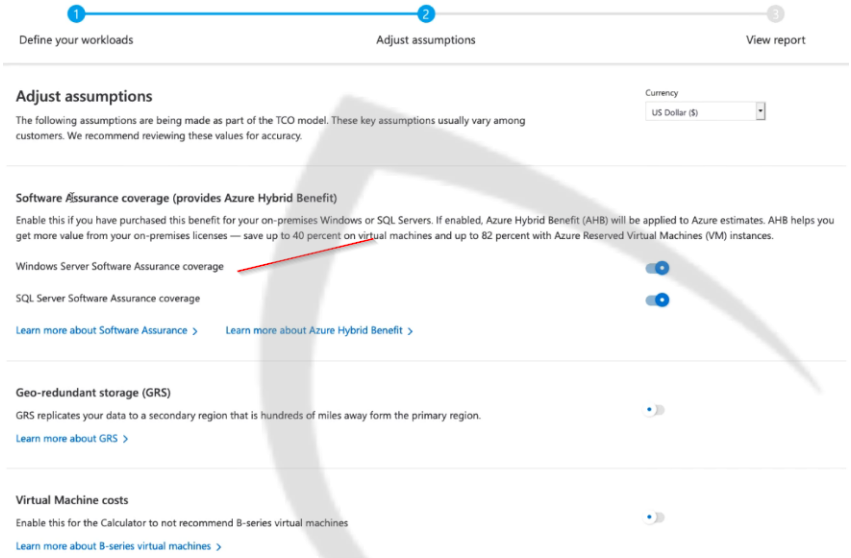
- You can also add the network utilization per month such as 100 GB.



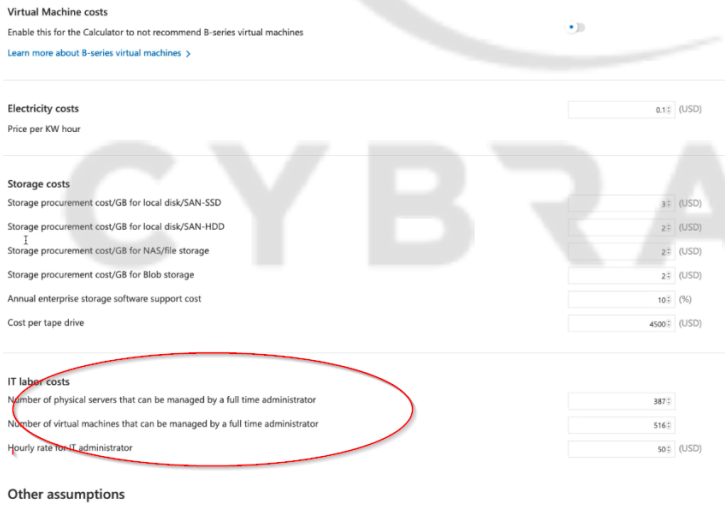
Select Next to go and adjust the assumptions.

Adjust Assumptions

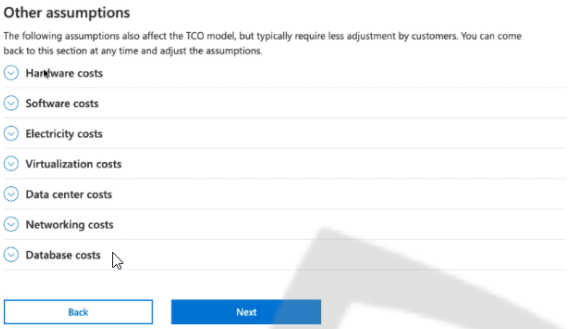
- You can add Windows and SQL server software assurance coverage for hybrid environment.



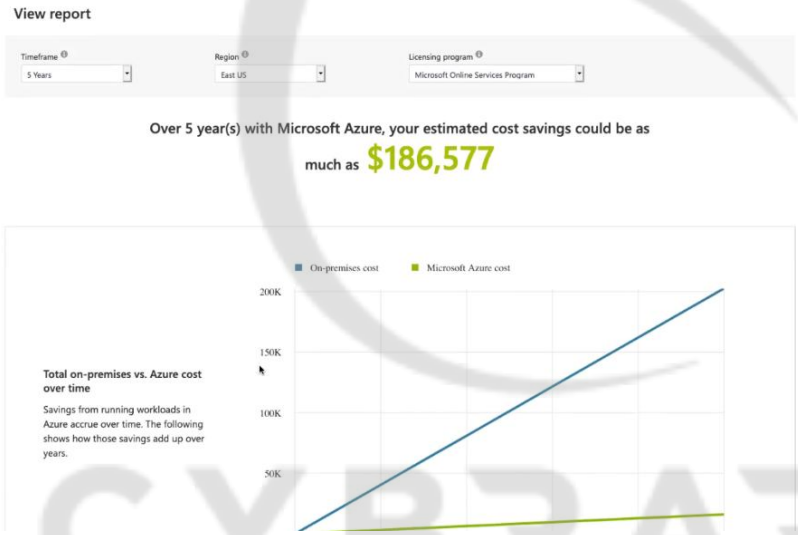
- You can include IT labor for your on-premise support



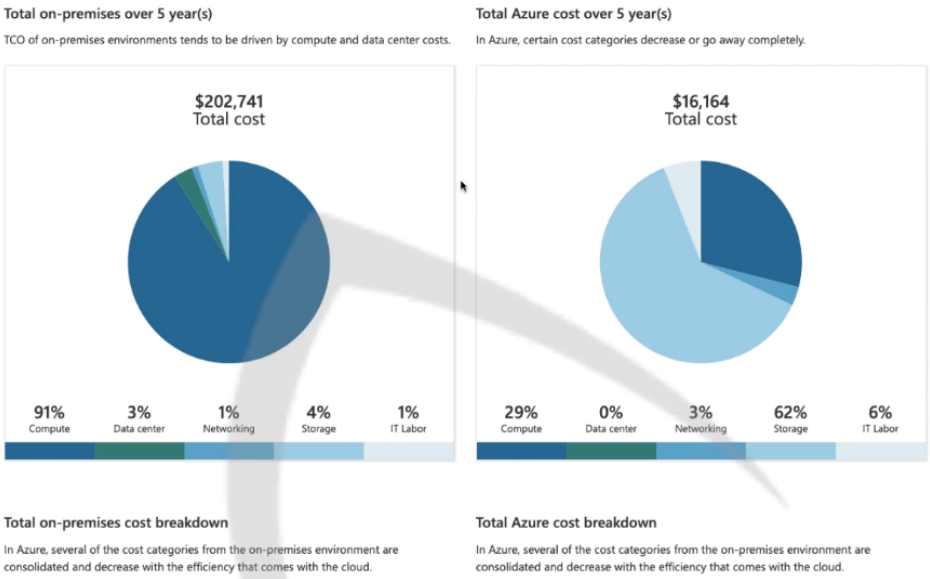
- You can add the other related cost of hosting the equipment on-premise such as Hardware, software, electricity, virtualization, data center, networking and database cost.



- Select next to view the reports



- According to Azure report, you will get a cost saving of $189,577 over a 5 years period.



- The report also displays the cost for on-premise versus Azure hosting over a 5 years period.

This is a very simple example of how you can project you cost for your on-premise and what it will cost if you decide to migrate that same workload to Azure.
By now you should have a good grasp of the tools that Azure offers you to plan your migration to Azure, to estimate your cost and also to monitor your expense once you have migrated to Azure.

In the next lesson, we are going to take a look at some strategies you can take to use reduce the cost once you are in Azure.

Lesson 12.5: Reducing Costs on Azure

Skills Learned From This Lesson: Reducing Infrastructure Costs, Reducing Licensing Costs, Azure Costs

Now that we know how to estimate and monitor our Cloud cost, now let us look at ways of reducing those.

Reducing Infrastructure Costs

- Using reserved instance for starting workloads can reduce your cost between 70% - 80%. Purchasing reserved instances is done on an annual or 3 years term and you need to prepaid for the whole term. However, if you plan to run those for a long time and combine the purchase with hybrid benefits, you can get up to 80% discount.
- Right-sizing VMs is of course the other option we discuss. You can leverage Azure advisor to assist you with that. Azure VM cost is linear and doubles within VM family and you can reduce you VM costing by choosing a one size smaller VM.
- As we mentioned before, regions has different pricing for the same resource types. If not critical, choose a location that is cheaper.
- Not all virtual machines needs to be on all the time, you can save a lot of compute charges if you deallocate the VMs during off hours.
- You can use Azure automation to start and stop virtual machines overnight when your employees are not working.
- It may be obvious, but you will be surprised how many resources will be available in the Cloud although nobody is using them. You can develop an automation that run periodically scans that notify the owners of unused resources and advise them to delete them.
- Certain subscription like Visual Studio subscriptions have Azure credits applied to them. Visual Studio professional has a $50 per month while Visual Studio Enterprise has a $100 per month. Your developers can use those for learning, developing and testing activities.
- Visual Studio subscriptions has a so called limits, once you exceed the limits, all resources in the subscription are disabled and you are not charged for those. When the billing period ends and there are credits remaining in the resources that are activated, then you can use them again.

- Not all subscription types allows you to have spending limits. If this is the case, you can set a budget and at least get notifications when the budget is exceeded.
- You can migrate to PaaS or SaaS services that offers significant cost savings. Depending on the application, this might pose a challenge with this approach as it may require significant development effort.

Reducing licensing Costs

- License is another area where you can save on cost.
- There is a difference in pricing in Linux and Windows workloads because Windows cost includes the licensing cost for the operating system. If you do not require Windows operating system, you may want to choose Linux to save on cost.
- You can use Dev/Test subscription to save on cost for your non-production environment. Both enterprise and pay-as-you-go subscription has the option for Dev/Test environment. There are some restrictions:
    - Those are limited to non-production environments only.
    - Any users of the workload must be covered by the Visual Studio subscriptions.
- Another option for saving on licensing cost is to use the hybrid benefits for Windows Server. If you have already invested in licenses for your on-premises servers, this can be a good option. You can use those licenses for virtual machines in Azure. To be eligible for that, your license for Windows must be covered by Software Assurance. Here is how they work:
    - Each two Processor or 16 core licenses is entitled to two instances of up to 8 cores or 1 instances up to 16 cores in Azure.
    - Standard edition licenses can be used either on-premise or in Azure but no simultaneously in both.
    - Datacenter edition licenses can be used simultaneously on-premise and in Azure which means that you can cover two VMs with the same licenses.
- SQL server is another Microsoft product that is licensed per CPU. similar to the Windows benefits, you need to have Software Assurance to use those. You can use your hybrid benefits for Azure SQL vCore or SQL server on VMs.
    - If you have Standard edition per core license, you can one core in the general purpose service tier of Azure SQL database.
    - If you have Enterprise edition per core license, you can one vCore in the business critical service tier of Azure SQL.

    - If you have highly virtualized Enterprise edition per core license, you can get 4 vCore in the business critical service tier of Azure SQL.
    - For SQL server on Azure VMs, the license match one-to-one.
- If you have Enterprise Agreements and you have freed up licenses from your on-premise workloads, you can use those on Azure or bring your own license (BYOL) resources in Azure marketplace.
- You can also use the SQL Server Developer edition for your non-production workloads. This is a free product offered by Microsoft and you can find it in the Azure marketplace.
- You can use constraint instances for workloads that require a lot of memory, storage or IOP bandwidth but does not require a lot of CPU cores. This way you will need to pay less licensing fee per cores. Such instances types are the DS,ES, GS, MS series.

With this we are wrapping up our discussion on managing cost and savings in Azure.

Module Summary

In this module, we have learnt about:

- Purchase options for Azure
- Billing based on usage meters
- Estimate costs with Azure Pricing Calculator
- Manage costs with Azure Advisor and Azure Cost Management
- Calculate TCO for migration
- Reduce infrastructure costs

Course Wrap-Up

Course Summary

In this course we have discussed the following topics:

- Principles of the cloud and what are the benefits
    - This topic included CapEX, OpEX, Cloud Deployment and service models
- Overview and History of Azure and it's services
- Azure Global Infrastructure
- Azure Account and Azure Management Portal
    - Topics included Azure tenants, supports options and preview features
- Core services: compute, storage, and networking
    - Topics covered are like Virtual Machine, Containers, serverless, databases, Blob and Queues, virtual networks, load balancers and Azure traffic manager
- Security, compliance and monitoring in Azure
    - The topics involved encryption, RBAC, Cloud security and standardizing workloads using Azure Policy & Initiatives, Compliance audits, Azure trust center and Azure monitor
- Azure Resource Manager
    - This topic included resource groups and tags and resource lock
- Purchase services and manage costs in Azure
    - This topic included purchasing services via Web Direct (Pay-As-You-Go), Enterprise Agreement and through the Cloud Service Providers. It also included topics on reducing, managing and determining costs in your Azure.

I hope this book was helpful in providing the solid foundational knowledge of Azure and i hope it helps you in pursuing your Azure certifications.

Azure certifications references: https://www.microsoft.com/en-us/learning/azure-exams.aspx