**Chapter 1 DESCRIBE CLOUD CONCEPTS**

**CAPEX** is the spending of money on physical infrastructure upfront and then deducting that expense from your tax bill over time. CapEx is an **upfront cost**, which has a value that reduces over time and usually has **no recurring cost**.  
  
**OpEx** is your operating costs, the expenses to run the day-to-day business, like services and consumable items that get used up and are paid for according to use. You can deduct this expense from your tax bill in the same year. There’s**no upfront cost**but has a **recurring cost**. You pay for a service or product as you use it i.e. **pay-as-you-go pricing.**

**Network outage  
Application failure**: Application Insights that integrates with your application to give you detailed information about the performance and reliability of your application. Application developers can often use this information to get right to the code where a problem is happening, dramatically reducing the time needed for troubleshooting.  
  
**System outage  
Power outage**: Cloud providers invest heavily in battery operated power backups and other redundant systems in order to prevent availability problems caused by power outages.  
In a situation where a large geographic area is affected by a power outage, cloud providers offer you the ability to run your application from another region that isn’t affected

**Scaling and elasticity**  
Scaling is the process of adding additional resources or additional power for your application.   
**There are two variations of scaling:**   
**Horizontal scaling** (*often referred to as scaling out*) - You add additional VMs for your application. Each VM you add is identical to other VMs servicing your application.  
**Vertical scaling** (often referred to as scaling up) - Scaling out provides additional resources to handle additional load. *For example, you might determine that you need a more powerful CPU and more memory for your application. In that case, scaling up will allow you to move your application to a more powerful VM.*

**The concept of automatically scaling is referred to as elasticity.  
Speed and flexibility in the cloud is often called cloud agility.**  
  
**Don’t confuse fault tolerance with scaling:**Scaling allows you to react to additional load or resource needs, but it’s always assumed that **all the VMs you are using are healthy**.   
**Fault tolerance** happens without any interaction from you, and **it’s designed to automatically move you from an unhealthy system to a healthy system if things go wrong**  
  
**Disaster Recovery** **and** **Governments**   
Depending on what kind of data you store, you might be required to have a disaster recovery plan in place. Cloud providers typically comply with standards imposed by laws such as the **Health Insurance Portability and Accountability Act** **(HIPAA),** and they often provide compliance tools you can use to ensure compliance.  
**Disaster recovery** not only means having **reliable backups of important data**, but it also means that the **cloud infrastructure can replicate your application’s resources in an unaffected region** so that your data is safe and your application availability isn’t affected.   
**Disaster recovery** plans are commonly referred to as **Business Continuity and Disaster Recovery (BCDR)** plans, and most cloud providers have services that can help you develop and implement a plan that works for your particular needs

**SKILL 1.2: DESCRIBE THE DIFFERENCES BETWEEN INFRASTRUCTURE-AS-ASERVICE (IAAS), PLATFORMAS-A-SERVICE (PAAS), AND SOFTWARE-AS-A-SERVICE (SAAS)**

**IAAS**  
Once you have an IaaS VM running in the cloud, you gain access to many services the cloud provider offers. For example, Microsoft offers **Azure Security Center** to ensure the security of your IaaS VMs, **Azure Backup** to make backing up data easy, **Azure Log Analytics** to help with troubleshooting any problems you might have, and much more  
IaaS is also a great choice if you want your application and configuration in the cloud, but you want the option of not paying for it when you aren’t using it. By stopping your VM, you can avoid the costs associated with it, and when you need to use your application again, you can simply start your VM and pick up right where you left off.

**PAAS**  
If you are deploying your own application to the cloud and you want to minimize your management investment, a PaaS service is often the best choice.  
A PaaS service also uses VMs provided by the cloud provider. However, a user typically has no visibility into those VMs. In most cases, they’re entirely managed by the cloud provider.

* **Azure App Service** one of the PaaS offerings in Azure. It has been created on a VM that’s maintained by Microsoft. Notice the option to choose either Linux or Windows, but the operating system is still managed by Microsoft. We also have the option to enable Application Insights, a service in Azure that provides deep insight into how an application is performing, making it easier to troubleshoot problems if they occur.

In Azure App Service, you don’t have to worry about Docker installation or configuration. It’s automatically included on all App Service VMs as part of Microsoft’s PaaS offering, and it’s completely managed and maintained by Microsoft. Examples: **Azure CDN, Azure Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Storage, Azure Synapse Analytics**

**Lift-and-shift** It’s a concept that you can often move your application from on-premises to a cloud environment by simply deploying it to the cloud

**SAAS**  
SaaS service is software provided by a cloud provider that’s installed on infrastructure completely controlled by the hosting provider. Examples: Microsoft 365, Xbox Live & One Drive.

**SKILL 1.3: DESCRIBE THE DIFFERENCES BETWEEN PUBLIC, PRIVATE, AND HYBRID CLOUD MODELS**

**The public cloud**  
The most common cloud model is the public cloud. In a public cloud model, you use shared infrastructure that is accessible on a public network. The network, storage, and VMs that your application uses are provided by a cloud provider and shared between all consumers of the public cloud. Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform are examples of public clouds.

**The private cloud**  
The private cloud model provides many of the attractive benefits of the cloud (things like easy scaling and elasticity) in a private environment that is dedicated to a single company. A private cloud can be hosted in an on-premises environment, but it can also be hosted on a thirdparty hosting provider.

**The hybrid cloud**  
As you might expect, hybrid clouds are a mixture of public and private clouds.

**Chapter 2 DESCRIBE CORE AZURE SERVICES**

**Azure regions**   
Within the United States geography, there are many regions, including the Central US region in Iowa, the East US region in Virginia, the West US region in California, and the South Central US region in Texas.  
Microsoft also operates isolated regions that are completely dedicated to government data because of the additional regulations that governmental data requires

**Regional pair  
E**ach regional pair contains two regions within the geography. **When Microsoft has to perform updates to the Azure platform, they perform those updates on one region in the regional pair. Once those updates are complete, they move to the next region in the regional pair. This ensures that your services operating within a regional pair aren’t impacted by updates.**

The fact that each **geography contains at least two regions separated by a large physical distance is important. That’s how Azure maintains disaster recovery.**

*When a customer is creating Azure resources, only the region is visible.* ***The concept of geographies is an internal implementation of Azure*** *that customers don’t really have visibility of when using Azure.***Customers also don’t have visibility into the concept of regional pairs, but they can see each region within a regional pair.**

In order to ensure that applications are still performing as quickly as possible, **Microsoft guarantees round-trip network performance of 2 milliseconds or less between regions.**

**Availability zones**  
Important that data and applications maintain availability **when a problem occurs at a particular datacenter within a region**. For that reason, Microsoft developed availability zones.

Currently, availability zones are supported with the following Azure services: <https://docs.microsoft.com/en-us/azure/availability-zones/az-region>

Don’t confuse availability zones with availability sets.  
**Availability sets**   
Allow you to create two or more virtual machines in different physical server racks in an Azure datacenter. Microsoft guarantees a **99.95 percent SLA with an availability set.   
Availability zone**  
Allows you to deploy **two or more Azure services into two distinct datacenters within a region.** Microsoft guarantees a **99.99 percent SLA with availability zones.**

**Zonal services** – A resource can be deployed to a specific, self-selected Availability Zone to achieve more stringent latency or performance requirements. Resiliency is self-architected by replicating applications and data to one or more zones within the region. Resources can be pinned to a specific zone. For example, virtual machines, managed disks, or standard IP addresses can be pinned to a specific zone, which allows for increased resilience by having one or more instances of resources spread across zones.

**Zone-redundant services** – Azure platform replicates the resource and data across zones. Microsoft manages the delivery of high availability since Azure automatically replicates and distributes instances within the region. ZRS, for example, replicates the data across three zones so that a zone failure does not impact the HA of the data.

**Non-regional services** – Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.  
 **Resource group**If you have access to multiple Azure subscriptions, you can also have resources from multiple subscriptions in a single resource group.

An Azure resource can only exist in one resource group. In other words, you can’t have a virtual machine in a resource group called WebStorefront and also in a resource group called SalesMarketing, because **it must be in one group or the other. You can move Azure resources from one resource group to another**

**Azure subscriptions**Each Azure subscription has limits (sometimes called quotas) assigned to it.   
For example, you can have up to **250 Azure Storage accounts per region in a subscription**, **up to 25,000 virtual machines per region, and up to 980 resource groups per subscription across all regions.**

*Microsoft support can increase limits in some scenarios if you have a good business justification. Some limits, however, cannot be increased.*

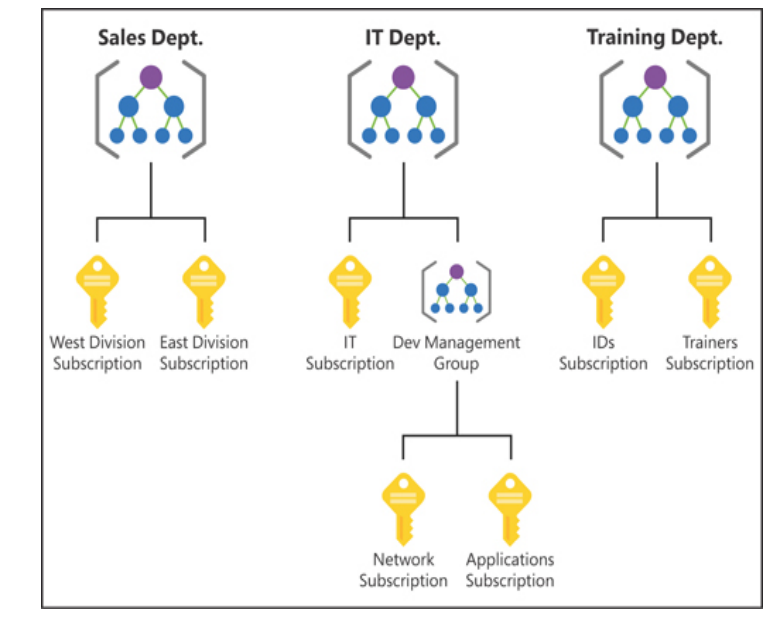
**Free Trial Provides** free access to Azure resources for a limited time.

**Pay-As-You-Go** You pay only for those resources you use in Azure. There’s no up-front cost, and you can cancel the subscription at any time.

**Pay-As-You-Go Dev. / Test** A special subscription for subscribers to Visual Studio that can be used for development and testing. This subscription offers discounted rates on VMs, but you cannot use this for production applications.

*Each subscription is associated with a unique identifier called a* ***subscription ID****. You can give each subscription a descriptive name to help you identify it, but Azure will always use the subscription ID to identify your subscription. When you talk to Microsoft about your Azure account, they’ll also often ask for your subscription ID.*

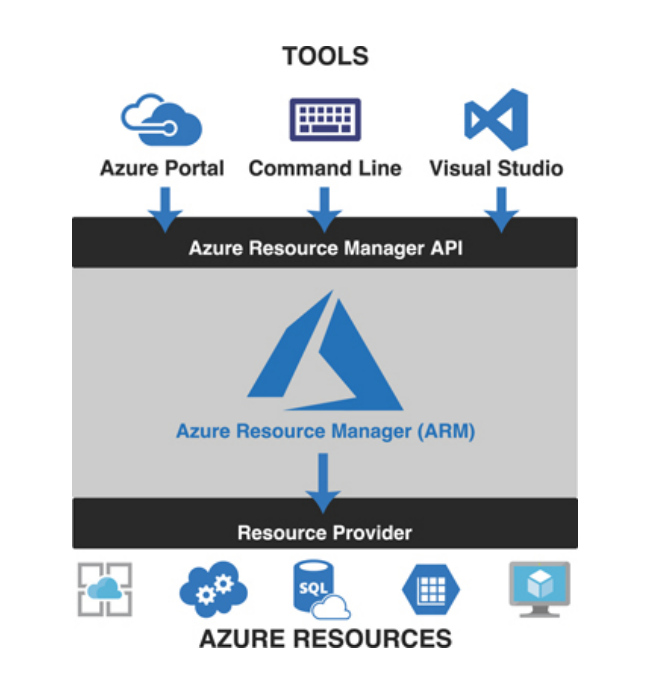
**Management groups  
A convenient way to apply policies and access control to your Azure resources.** Much like a resource group, a management group **is a container for organizing your resources**. However, management groups can contain only **Azure subscriptions or other management groups**.



*By organizing the subscriptions using management groups, you can have more precise control over who has access to which resources. You can also control the configuration of resources created within those subscriptions.*

There are, however, a few limitations: **You’re limited to a total of 10,000 management groups**. A management group hierarchy can only **support up to six levels**. You cannot have multiple parents for a single management group or subscription.

**Azure Resource Manager (ARM)**In order to make it easier to deploy and manage Azure services, Microsoft developed Azure Resource Manager, or ARM. **ARM is a service that runs in Azure, and it’s responsible for all interaction with Azure services.** When you create a new Azure service, ARM authenticates you to make sure you have the right access to create that resource, and then it talks to a resource provider for the service you’re creating. For example, **if you’re creating a new web app in Azure App Service, ARM will pass your request on to the Microsoft.Web resource provider because it knows all about web apps and how to create them.**



**You don’t have to tell ARM how to do what you want. You simply have to tell it what you want.** To do that, ARM uses files that are encoded in JavaScript Object Notation (or JSON) called ARM templates.

ARM allows you to specify dependencies so you can avoid issues like this.

* **ARM allows you to easily deploy multiple Azure resources at once.**
* ARM makes it possible to reproduce any deployment with consistent results at any point in the future.
* ARM allows you to create declarative templates for deployment instead of requiring you to write and maintain complex deployment scripts.
* **ARM makes it possible to set up dependencies so that your resources are deployed in the right order every time.**

**SKILL 2.2: DESCRIBE CORE WORKLOAD PRODUCTS AVAILABLE IN AZURE**

**Azure virtual machines**   
Because the VMs running on a host use the physical systems on that host, if you have a need for a powerful VM, you’ll need a powerful physical computer to host it.

When you click Create to create your VM, the Azure portal is actually using an ARM template to deploy your VM. That ARM template contains parameters that are replaced with the information you entered for your VM. Every VM that is created in Azure is created using an ARM template. This ensures that the deployments are consistent.

**Keep in mind that unless you have configured a static IP address for your VM, your IP address will likely change the next time you start it.**

**You can also stop a VM from within the guest operating system on the VM, but when you do that, you will still be charged for the resources the VM uses because it’s still allocated to you.**

**Planned maintenance**   
Includes things like operating system updates, driver updates, and so on.

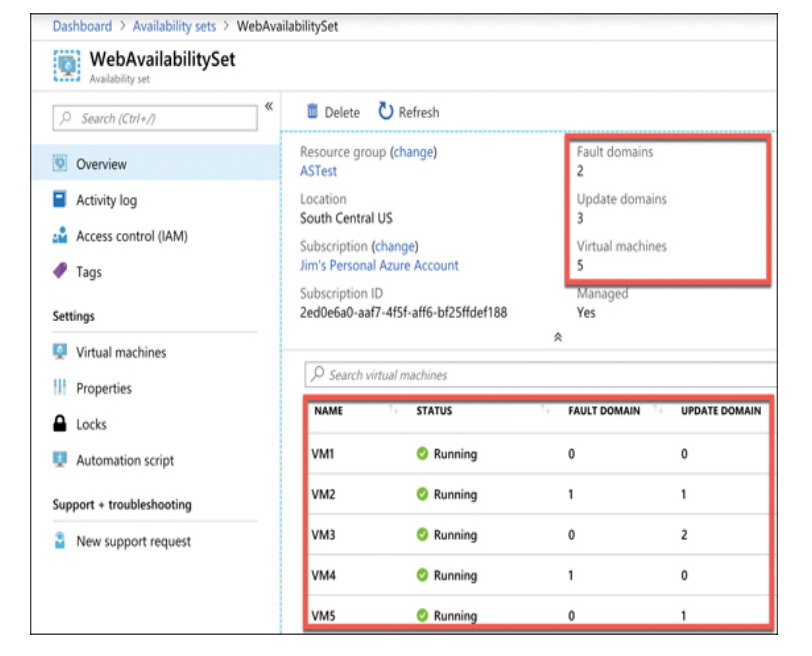
Azure has underlying systems that constantly monitor the health of computer components. If one of these underlying systems detects that a component within the host computer might fail soon, Azure will flag the computer for unplanned maintenance.   
  
**Unplanned maintenance**Azure will attempt to move your VM to a healthy host computer. When it does this, it preserves the state of the VM, including what’s in memory and any files that are open. It only takes Azure a short time to move the VM, during which time it’s in a paused state. In a case where the move operation fails, the VM will experience **unexpected downtime**.

*In order to ensure reliability when a failure occurs in a rack within the Azure datacenter, you can (and you should) take advantage of a feature called availability sets.* **Availability sets** *protect you from maintenance events and downtime caused by hardware failures. To do that, Azure creates some underlying entities in an availability set called update domains and fault domains. (In order to protect yourself in the event of maintenance events or downtime, you must deploy at least two VMs into your availability set.)*

**Fault domains**   
**A logical representation of the physical rack in which a host computer is installed**. By default, Azure assigns two fault domains to an availability set. If a problem occurs in one fault domain (one computer rack), the VMs in that fault domain will be affected, but VMs in the second fault domain will not. **This protects you from unplanned maintenance events and unexpected downtime.**

**Update domains**   
Designed to protect you from a situation where the host computer is being rebooted. **When you create an availability set, Azure creates five update domains by default**. These update domains are spread across the fault domains in the availability set.   
If a reboot is required on computers in the availability set (whether host computers or VMs within the availability set), **Azure will only reboot computers in one update domain at a time and it will wait 30 minutes for computers to recover from the reboot before it moves on to the next update domain. Update domains protect you from planned maintenance events.**





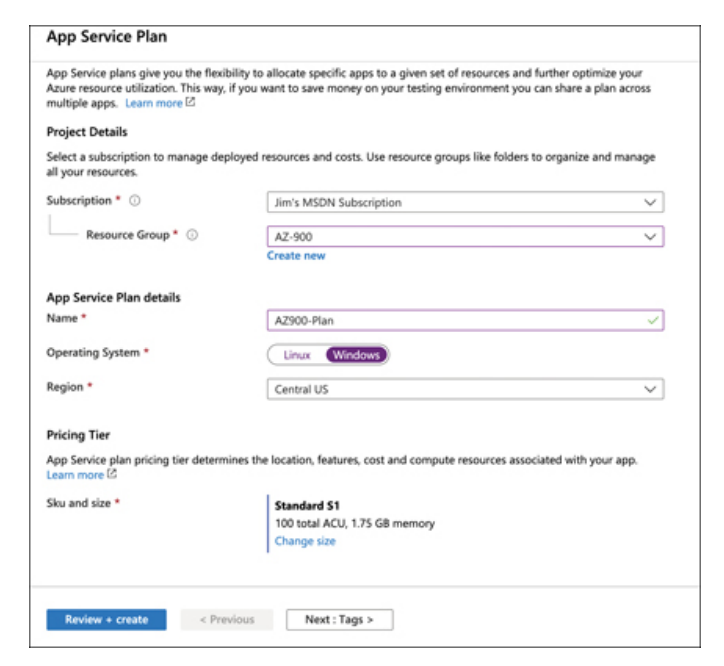
*If your availability set is servicing a website hosted on the VMs, you’ll need to configure a load balancer that will handle the job of routing users of your website to the VMs that are running it.*

**Scale set**When you create a scale set, **you tell Azure what operating system you want to run and then you tell Azure how many VMs you want in your scale set**. You have many other options such as creating a load balancer or gateway and so forth. Azure will create as many VMs as you specify (up to 1,000) in one easy step.

***Scale sets provide that functionality by using Azure’s auto-scale feature. You define scaling rules that use metrics like CPU, disk usage, network usage, and so forth.*** You can configure when Azure should add additional instances and when it should scale back and deallocate  
*VMs in a scale set are also compatible with availability zones, so you are protected from problems in an Azure datacenter.*

**App Service plans**Every web app you create in App Service runs inside of an App Service plan. An App Serviceplan is created within a specific Azure region, and it specifies how many VMs your app runs on and the properties of those VMs.  
Depending on the tier of service you use when you create your app, it will either run on a VM that is shared among many users or a VM that is dedicated to you.

**Multiple apps can run inside of a single App Service plan. All apps in an App Service plan will share the same VMs in that App Service plan.**

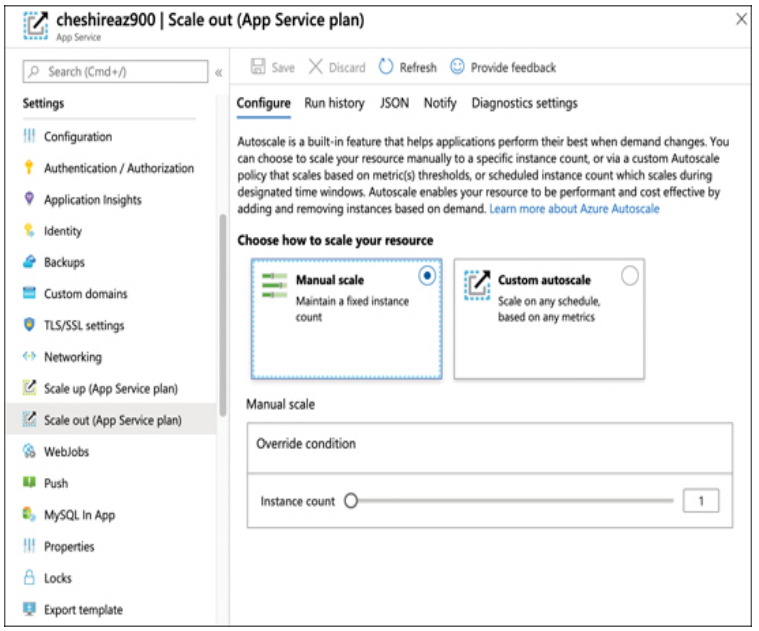


* **Free** A no-cost tier for testing only that runs on VMs shared with other App Service customers.
* **Shared** A low-cost tier for testing only with some additional features not offered in the Free tier. Runs on VMs shared with other App Service customers.
* **Basic, Standard, Premium, and PremiumV2** Highercost tiers that offer many additional features. Runs on dedicated VMs that are not shared with other customers.

**You are charged for App Service plans even when no web apps are running in them. If you do have web apps in your App Service plan, you are still charged if you stop the web apps. The only way to avoid being billed for an App Service plan is to delete it.**

*Creating a web app in App Service is very fast and scaling it out to multiple instances is also very fast. That’s because the VMs that are running App Service web apps are already up and running. When you create a web app, you are simply allocating an existing VM for your use.*

**App Service**   
Allows you to choose between a VM preconfigured with a runtime stack (such as Java, .NET, PHP, and so forth) to run your app or a Docker container.

**You can see many of the features available in App Service, including the ability to quickly and easily scale out when needed.**  


**Azure Container Instances (ACI)  
Azure creates server resources as needed to run your container, but you’re not paying for an underlying VM. Instead, you pay for the memory and CPU that your container uses.**

***ACI*** *is designed to work with simple applications. You can define a container group and run multiple containers within an ACI instance, but ACI isn’t a good choice for you if you have an application that is used heavily by many people and that might need to take advantage of scaling. Instead, Azure Kubernetes Service (AKS) would be a better choice.  
  
You can’t change the DNS Name Label after the instance is created. You also can’t change the image your instance uses. If you want to change these settings, you’ll need to delete the instance and re-create it. However, doing so might mean that you lose your public IP address, so it’s best to plan ahead before you create your instance.*

**Azure Kubernetes Service (AKS)**Kubernetes creates containers in a pod. A pod is a group of related containers, and containers within a pod can share resources.  
However, a container in one pod is not able to share resources with a container in another pod.  
The computer that Kubernetes pods are running on is called a node or a worker.  
In addition to pods, the node also runs several services that are required for Kubernetes to manage the pods and so on.

There will typically be multiple nodes within a Kubernetes instance, and they are all controlled by a master node called the Kubernetes master. The entire environment of the master and all its nodes is called a **Kubernetes cluster.**

When you create a Kubernetes cluster in AKS, Azure creates the master and the nodes for you. All you have to do is deploy your containers and you’re up and running with a managed Kubernetes cluster.

**AKS in Azure is free. You only pay for the Azure compute resources you use within your cluster**

**Windows Virtual Desktop**In a desktop virtualization model, a business installs an operating system and applications on one central server. The desktop virtualization infrastructure makes it possible for employees to access the operating system and applications from virtually any device, provided it has access to the network.

To use Windows Virtual Desktop (WVD), you first create a **WVD tenant**.   
**Tenant** is a collection of one or more host pools, and a host pool consists of both session hosts and one or more app groups that represent the applications and OS desktops users should be able to access. These session hosts are simply Azure VMs that you’ve configured for WVD.

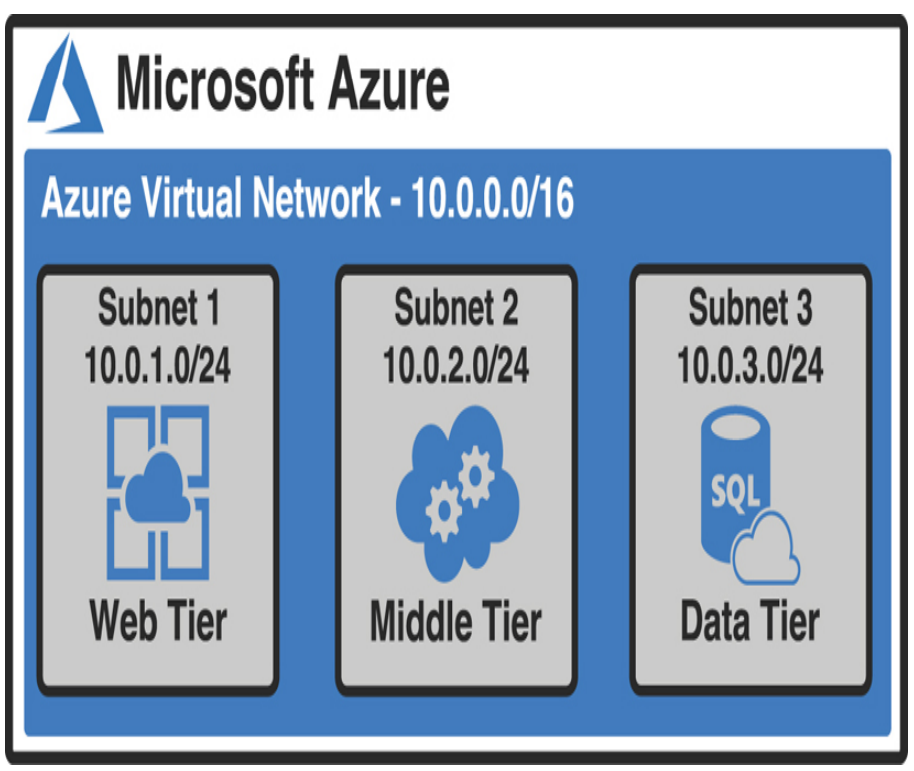
Once you’ve set up the tenant, you can add users from your **Azure Active Directory** so that they can access the OSes and apps in your tenant and assign permissions to them. Those users can then access WVD using the following methods.

* Using the WVD client app for Windows
* Using the WVD client app for MacOS
* Using the WVD client for iOS
* Using the WVD client for Android
* Using the web-based client from any web browser

**Virtual networks** (often called a VNet)  
**Allows Azure services to communicate with each other and with the Internet.   
You can even use a VNet to communicate between your on-premises**

**When you create a VM in Azure, a VNet is created automatically.**

You can’t connect a VM to a VNet after it’s been created. For that reason, if you wanted to use your own VNet instead of the one Azure creates automatically, you would create your VNet before you create your VM.

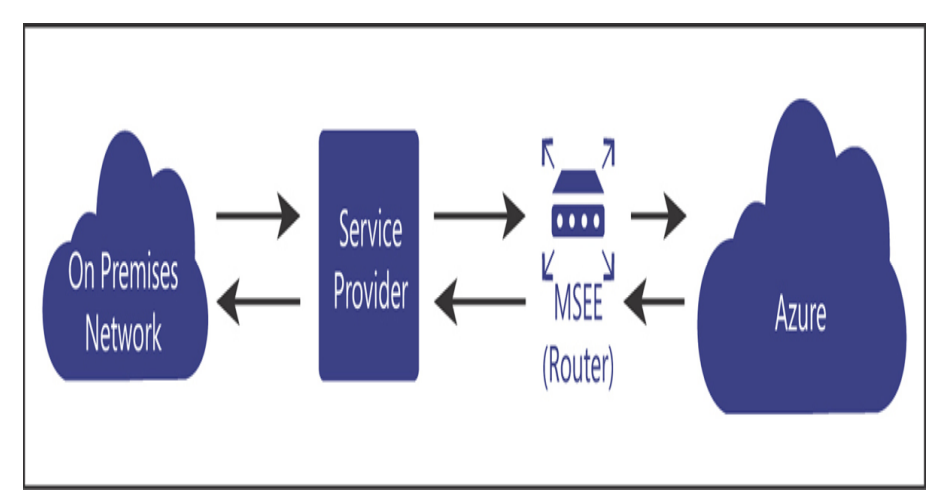


The IP addresses within the VNet at this point are all private IP addresses. They allow resources within the VNet to talk to each other, but you can’t use a private IP address on the Internet. You need a public IP address in order to give the Internet access to your web tier.

**ExpressRoute**VPN is limited to a maximum of 1.25 Gbps in network speed. If a customer needs more speed than that, VPN isn’t a good choice. **For this reason, Azure offers a service called ExpressRoute that can offer speeds up to 10 Gbps over dedicated fiber-optic connections.**

When you use ExpressRoute, you connect from your on-premises network to **a Microsoft Enterprise Edge router (MSEE)**, and that MSEE router then connects you to Azure.

The **MSEE** router sits on the edge of Microsoft’s network, and in most cases, your connection will also be from a router in your on-premises network that is on the edge of your network.



Microsoft calls an ExpressRoute connection a circuit.  
**Because data in ExpressRoute doesn’t traverse the public Internet, bandwidth is much more reliable. However, the ExpressRoute configuration you see in Figure does require that you trust the service provider with the data flowing through the circuit.**

If you want to remove the service provider from the picture, you can use an offering called **ExpressRoute Direct** that allows you to connect directly to a physical port on the MSEE router.

**Container (blob) storage  
Azure Blob Storage is designed for storing unstructured data**, which has no defined structure. That includes **text files, images, videos, documents, and much more.**

* **Block blobs** Used to store files used by an application
* **Append blobs** They are like block blobs, but append blobs are specialized for append operations. For that reason, they are often used to store constantly updated data like diagnostic logs.
* **Page blobs** They are used to store virtual hard disk (.vhd) files that are used in Azure virtual machines. We’ll cover these in Azure Disk Storage later in this chapter.

**Azure Storage Explorer** a free tool available from Microsoft, to upload data.  
**Data Box** if you want to move a large amount of data

**Disk storage**Disks that are used in virtual machines. (Temporary storage when you create a VM)  
If you need to store data for a longer period of time that will persist between VM deployments and maintenance events, you can create a disk using an image stored in Azure Storage.

**Unmanaged disks**   
They use an Azure Storage account in your Azure subscription, and you must manage that account. This is particularly troublesome because there are limitations in Azure Storage, and if you have heavy disk usage, you might end up experiencing downtime because of throttling.

**Managed disks**   
Microsoft handles the storage account, and all storage limitations are removed. All you need to worry about is your disk. You can leave the storage account in Microsoft’s hands.  
(you avoid a possible single point of failure in your VM)

*Microsoft recommends managed disks for all new VMs. They also recommend that all VMs currently using unmanaged disks be moved to managed disks.*

**Azure Files**if you just need disk space in the cloud, it doesn’t make sense to take on the burden of managing a virtual machine and its operating system. In those situations, Azure Files is the perfect solution. **Azure Files is a completely managed file share that you can mount just like any SMB (Server Message Block) file share***. Because Azure Files shares use SMB,* you’ll need to make sure that TCP port 445 is open on your network.

**Azure File Sync**   
When users or applications need to access those files, they can access the local copy quickly. Any changes you make to the centralized Azure Files share are synchronized to servers running Azure File Sync.

**Storage tiers**Storage that are priced according to how often the data is accessed

**Hot storage** tier is for data you need to access often. It has the highest cost of storage, but the cost for accessing the data is low.   
**Cool storage** tier is for data that you intend to store for a longer period and not access quite as often. It has a lower storage cost than the Hot tier, but the access costs are higher. *You’re also required to* ***keep data in storage for at least 30 days.*****Archive storage** tier Data stored in the Archive tier enjoys the lowest storage costs available, but the access costs are the highest. You must keep data in storage for a **minimum of 180 days** in the Archive tier or you can be subjected to an early deletion charge.  
 *In fact, while the Hot and Cool access tiers guarantee access to the first byte of data within milliseconds,* ***the Archive tier only guarantees access to the first byte within 15 hours.***

**Cosmos DB**Supports all the NoSQL database types. Microsoft has built some custom code around Cosmos DB so that developers can use their existing skills with other database systems with a Cosmos DB database.

There are four types of NoSQL database systems: **key-value, column, document, and graph.**

* **Core (SQL)** Creates a document database that you can query using SQL syntax that you might be familiar with from using relational databases.
* **Azure Cosmos DB for MongoDB API** Used for migrating a MongoDB database to Cosmos DB. MongoDB databases are document databases.
* **Cassandra** Used for migrating a Cassandra database to Cosmos DB. Cassandra databases are column databases.
* **Azure Table Used** for migrating data stored in Azure Table Storage to Cosmos DB. This creates a key-value database.
* **Gremlin** Used for migrating Gremlin databases to Cosmos DB. Gremlin databases are graph databases.

*Another huge advantage to Cosmos DB is a feature known as turnkey global distribution. This feature takes advantage of the horizontal scalability of NoSQL databases and allows you to replicate your data globally with a few clicks.*

**Azure SQL Database**Is a PaaS offering for SQL Server database hosting. Microsoft manages the platform, so all you must worry about is your database and the data in it.  
Azure offers three different deployment options for Azure SQL Database: single database, elastic pool, and managed instance.

**A single database** is simply a database running in a hosted SQL Server instance running in Azure. Microsoft manages the database server, so all you have to worry about is the database itself. Microsoft provides two different purchase models for single databases: Database Transaction Unit (DTU) and virtual core (vCore).

**A DTU represents a collection of CPU, memory, and data reads and writes. There are three tiers in the DTU model: Basic, Standard, and Premium. Each tier offers a higher level of CPU, memory, and data transfer.**

**The vCore model uses a virtual CPU, and it makes it easy to configure the exact hardware configuration you need.**  
  
*You can choose between a provisioned tier (where you choose the CPU, memory, and other resources that are always available) and a serverless tier where you choose a range of resource needs so you can control costs more effectively.*

An **elastic pool** consists of more than one database (and often many databases) all managed by the same SQL Database server. This solution is geared toward SaaS offerings where you might want to have multiple users (or maybe even each user) to be assigned their own database. You can easily move databases in and out of an elastic pool, making it ideal for SaaS.

*In some cases, being able to scale a single database to add additional power is sufficient. However, if your application has wide variations in usage and you find it hard to predict usage (such as with a SaaS service), the ability to add more databases to a pool is much more desirable.*

***While you can scale up and down easily with Azure SQL Database by moving to a higher tier or adding compute, memory, and storage resources, relational databases don’t scale horizontally.*** *There are some options available for scaling out a read-only copy of your database, but in general, relational databases don’t offer the capability of scaling out to provide additional copies of your data in multiple regions.*

**DMS** Database Migration Service works by walking you through a wizard experience to tell Azure which database(s) and table(s) you want to migrate from your source database to Azure SQL Database.

**Azure Database for MySQL  
Azure Database for PostgreSQL**

**The Azure Marketplace and its usage scenarios**

*All the templates in the Azure Marketplace are ARM templates that deploy one or more Azure services. Remember from our earlier discussion of Azure Resource Manager that all ARM deployments are deployed using ARM templates. The Marketplace is no different.*

**Chapter 3 DESCRIBE CORE SOLUTIONS AND MANAGEMENT TOOLS IN AZURE**

**SKILL 3.1: DESCRIBE CORE SOLUTIONS AVAILABLE IN**

**Azure IoT Hub**IoT Hub can easily solve all these problems.

* **They must update firmware on the IoT** devices easily and in a staged way so they aren’t all updated at the same time.
* **They must alter the settings on the devices, such as changing alert levels**, but these settings are specific to the physical location of the devices in the building
* **They must ensure that any connectivity to the devices is completely secure**

From IoT Hub, you can send messages to devices (**called cloud-to-device, or C2D messaging**) or from your device to IoT Hub (**called device-to-cloud, or D2C messaging**).   
You can also intelligently route messages to Event Hub, Azure Storage, and Service Bus based on the content in the message

In addition to messages, you can also use IoT Hub to send files to your devices. This allows you to easily update the firmware on your devices in a secure way.

**Device twin:** Every IoT device in IoT Hub has a logical equivalent that’s stored in IoT Hub in JSON format. This JSON representation of the device is called a device twin, and it provides important capabilities.

Each device twin can contain metadata that adds additional categorization for the device. This metadata is stored as tags in the JSON for the device twin, and it’s not known to the actual device. Only IoT Hub can see this metadata.

To help with users who want to add a large number of IoT devices to IoT Hub, Microsoft offers the **IoT Hub Device Provisioning Service**, or **DPS**

**The DPS** uses enrollment groups to add devices to your IoT Hub. The concept is that once the device wakes up (often, for the first time if it’s a new device), it needs to know that it should connect to your IoT Hub. In order to do that, the DPS needs to uniquely identify the device, and it does that with either a certificate or via a trusted platform module chip.

*There are two pricing tiers for IoT Hub: Basic and Standard. Each tier offers multiple editions that offer pricing based on the number of messages per day for each IoT Hub unit.*

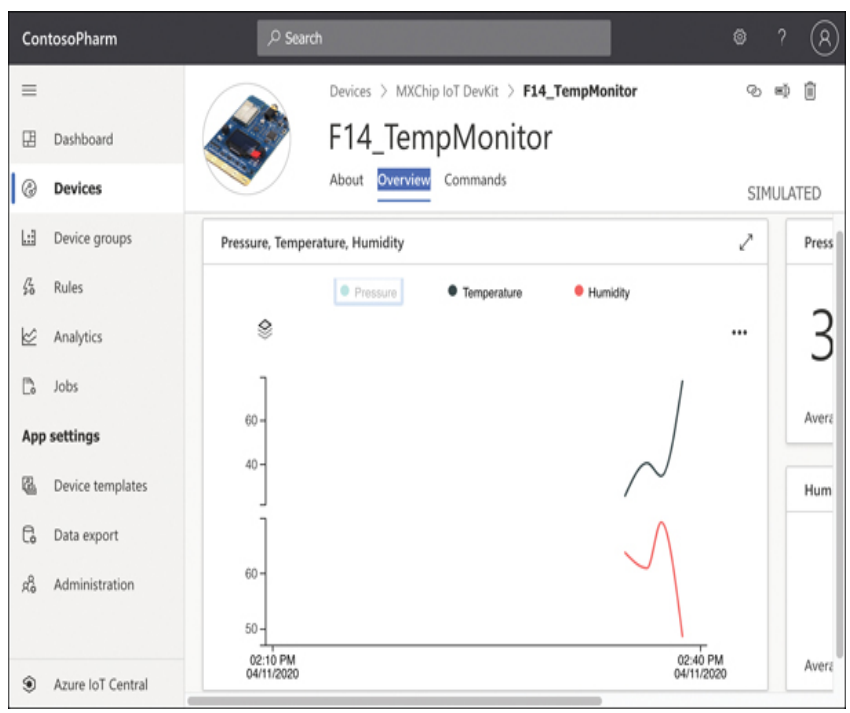
**IoT Central**IoT Hub is a great way to manage and provision devices, and it provides a robust means of dealing with messages.  
**IoT Central is a SaaS offering for IoT devices**. Unlike IoT Hub, you don’t have to create any Azure resources to use IoT Central. Instead, you browse to https://apps.azureiotcentral.com and create your app within the web browser interface

*The ability to create a simulated device is specific to IoT Central. IoT Hub doesn’t offer this capability.*

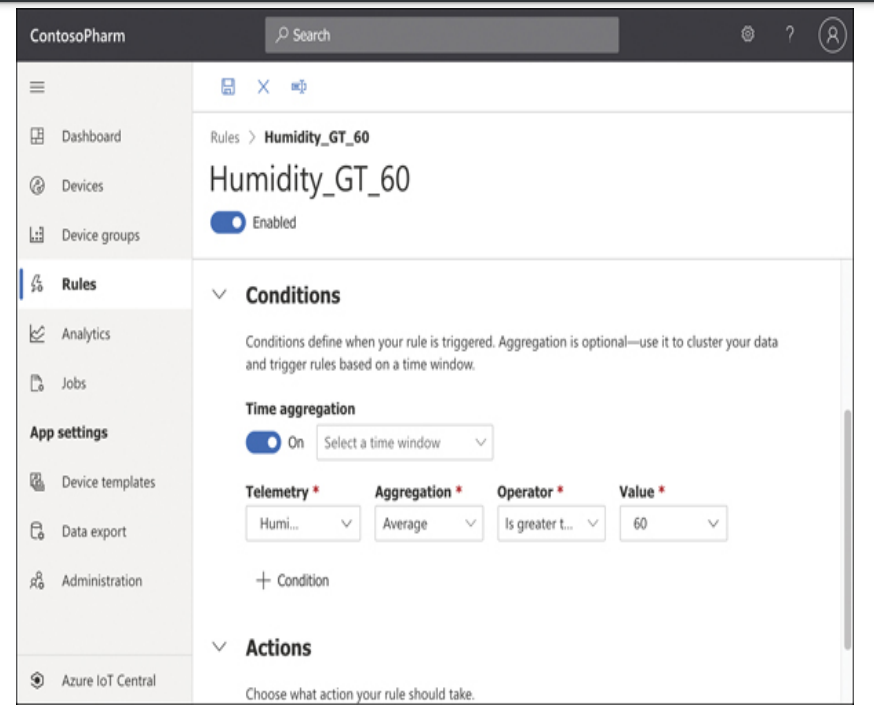
IoT Central gives you control over who can do what using roles. There are three built-in roles to which you can assign a user.

* **Administrator** Users in this role have full access to the application and can edit pages and add new users.
* **Builder** Users in this role can edit pages, but they can’t perform any administrative tasks, such as adding users, changing user roles, changing application settings, and so on.
* **Operator** Users in this role can use the application, but they can’t edit any pages and they can’t perform administrative tasks.

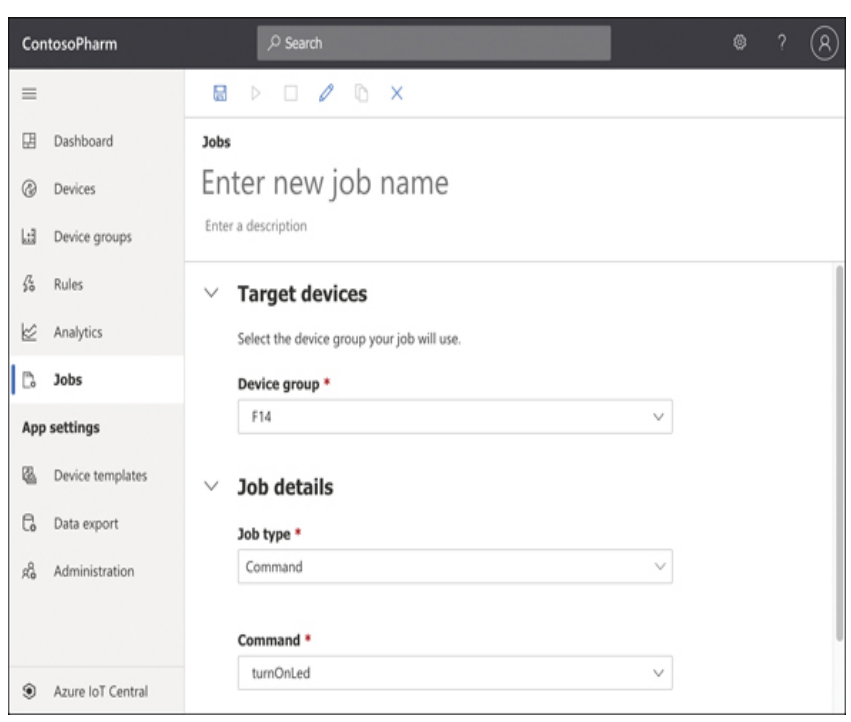
If you click a device, you can look at information coming from the device’s sensors. In Figure 3-11, you can see the Humidity and Temperature sensors on the F14\_TempMonitor device.



IoT Central also allows you to easily configure rules that will monitor your devices and perform an action you choose when your rule is activated. In Figure 3-12, we are configuring a rule that will activate when the Humidity is above 60.



A job can modify properties, change settings, or send commands to devices. In Figure 3-14, we’re creating a job that will turn on the LEDs for all devices in our device set.



**Azure Sphere**Is based on Microsoft’s decades of experience and indepth research that Microsoft conducted on securing devices

**Azure Sphere is actually an entire ecosystem, and it starts with the chip, or the microprocessor unit (MCU). Microsoft has developed an Azure Sphere MCU that contains security components embedded in the chip.**Third parties can use these MCUs to run code that is specific to their needs, and that code runs on the Azure Sphere operating system, which is a customized version of Linux developed for Azure Sphere.  
**This ecosystem provides a secure environment for running embedded code, but it also enforces secure communication between devices.**

**Azure Synapse Analytics**The problem of actually doing anything with the vast data we collect is common across all businesses, and this is what we mean by **big data.**

Analyzing big data requires **a powerful system for storing data, the ability to query the data in multiple ways, enormous power to execute large queries, assurance that the data is secure, and much more.** That’s exactly what **Azure Synapse analytics provides**.

*Azure Synapse is the next evolution of another Azure service called* ***SQL Data Warehouse****. While it’s true to say* ***that Azure Synapse is the replacement for SQL Data Warehouse****, it’s also important to note that Azure Synapse adds much more functionality.* **SQL Data Warehouse was focused primarily on storage of big data (called warehousing), but Azure Synapse provides that functionality in addition to powerful analytics features.**

Azure Synapse runs in an **Azure Synapse cluster**. A cluster is a combination of four different components:

* Synapse SQL
* Apache Spark integration
* Data integration of Spark and Azure Data Lake Storage
* A web-based user interface called Azure Synapse Studio

**Synapse SQL** is the data warehousing portion of Azure Synapse. Using Synapse SQL, you can run powerful queries against your big data.  
Each compute node also runs a component called the Data Movement Service (DMS) that moves data efficiently between compute nodes.

**Azure Data Lake Storage** is designed for storing large amounts of data that you’d like to analyze, but Data Lake Storage is designed for a wide array of data instead of relational data. In a data lake, data is stored in containers. Each container typically contains related data.

*The terms data lake and data warehouse aren’t specific to Azure.* They are generic terms.  
**A data lake refers to a repository of unordered data, and a data warehouse refers to a repository of ordered data.**

**HDInsight**  
**Microsoft’s managed service that provides a cloud-based implementation of a popular data analytics platform called Hadoop (The Apache Hadoop software library is a framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models.).**Create and manage clusters of computers on a common framework designed to perform distributed processing of big data.

HDInsight supported cluster types

**Apache Hadoop:** A framework that uses HDFS, YARN resource management, and a simple MapReduce programming model to process and analyze batch data in parallel.  
**Apache Spark:** A parallel processing framework that supports in-memory processing to boost the performance of big-data analysis applications. Spark works for SQL, streaming data, and machine learning. See What is Apache Spark in HDInsight?  
**Apache HBase:** A NoSQL database built on Hadoop that provides random access and strong consistency for large amounts of unstructured and semi-structured data–potentially billions of rows times millions of columns. See What is HBase on HDInsight?  
**Microsoft R Server:** A server for hosting and managing parallel, distributed R processes. It provides data scientists, statisticians, and R programmers with on-demand access to scalable, distributed methods of analytics on HDInsight. See Overview of R Server on HDInsight.  
**Apache Storm:** A distributed, real-time computation system for processing large streams of data fast. Storm is offered as a managed cluster in HDInsight. See Analyze real-time sensor data using Storm and Hadoop.  
**Apache Interactive Query preview (AKA: Live Long and Process):** In-memory caching for interactive and faster Hive queries. See Use Interactive Query in HDInsight.  
**Apache Kafka:** An open-source platform that’s used for building streaming data pipelines and applications. Kafka also provides message-queue functionality that allows you to publish and subscribe to data streams. See Introduction to Apache Kafka on HDInsight.

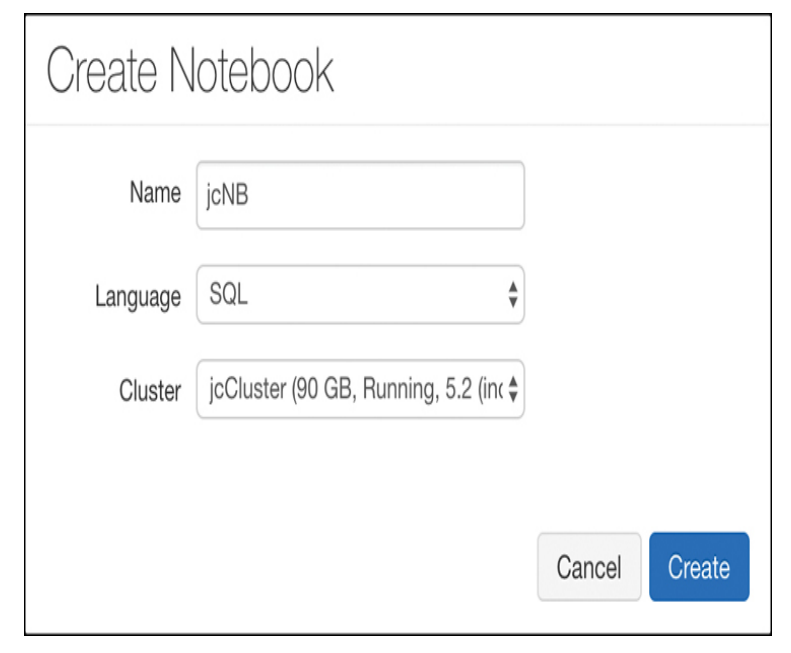
With HDInsight, Microsoft does all the heavy lifting on its own infrastructure. You benefit from a secure environment—one **that is easily scalable to handle huge data processing tasks.***HD Insight clusters are billed on a per hour basis, and you pay more per hour based on how powerful the machines are* ***in your cluster.***

**Azure Databricks  
Is a data analytics platform optimized for the Microsoft Azure cloud services platform.**Data that gets stored in a data warehouse or data lake is typically raw data that is often unstructured and difficult to consume. Also, you might need data that comes from multiple sources, some of which might even be outside of Azure.   
**Azure Databricks is an ideal solution for accumulating data and for forming the data (called data modeling) so that it’s optimal for machine learning models.**

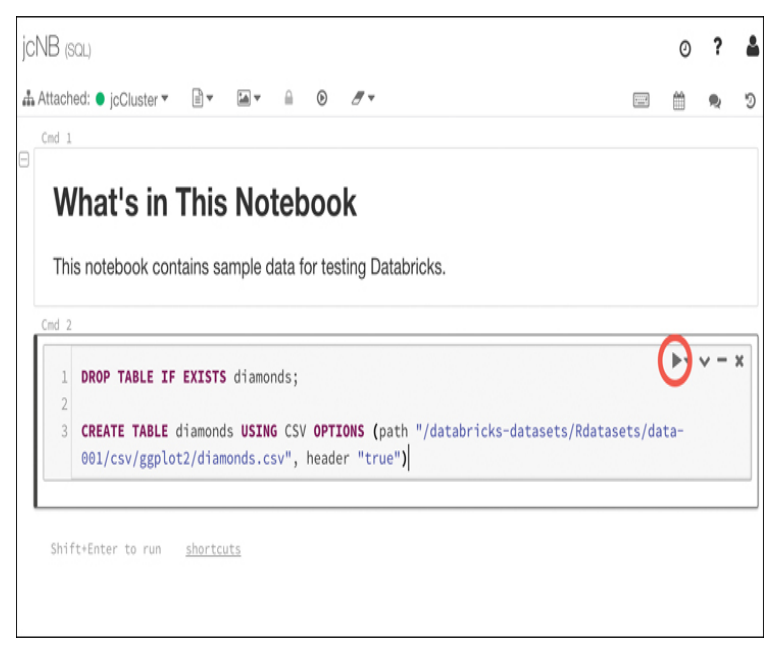
***Databricks*** *is actually the name of a company that originally developed* ***Apache Spark.*** *It now operates a* ***data analytics platform called Databricks****. You might be tempted to think of Azure Databricks as the Databricks platform running as a service in Azure, but it’s much more than that. In fact, Microsoft natively built the Databricks Runtime to run in Azure, and Azure Databricks provides many more unique features outside the Databricks platform developed by Databricks*

Databricks does all its work using clusters, which are the compute resources.

Next, we’ll create a notebook. **Notebooks are a powerful way to present and interact with related data.** Each notebook contains data as well as visualizations and documentation to help us understand the data. Once your data is in your notebook, you can run commands against machine learning frameworks in order to build your machine learning model right inside your notebook.



*Documentation in notebooks is entered using Markdown, a language that’s well-suited to writing documentation*



*When you run commands in a cell, Databricks creates a job that runs on the compute resources you allocated to your cluster.* ***Databricks uses a serverless model of computing****. That means that when you’re not running any jobs, you don’t have any VMs or compute resources assigned to you.*

**You can use data in Databricks for training machine learning algorithms. The Databricks Runtime ML includes several popular libraries for machine learning, including: Keras, PyTorch, TensorFlow, and XGBoost.**

***The important point to remember is that Databricks works with third-party machine learning frameworks to allow you to build machine learning models.***

Once you’ve built your machine learning model in Databricks, you can export it for use in an external machine learning system. This process is referred to as productionalizing the machinelearning pipeline, and Databricks allows you to productionalize using two different methods: MLeap and Databricks ML Model Export.

**MLeap** is a system that can execute a machine learning model and make predictions based on that model.  
**Databricks ML Model Export** is designed to export your machine learning models and pipeline so that they can be used in other machine learning platforms.

**Azure Machine Learning**  
Is designed to make ML approachable to just about anyone. It offers SDKs for both Python and R, and it also offers a drag-and-drop environment and an automated mode for more easily creating and training ML models in a visual way

Azure Machine Learning is available in two editions:  
**The Basic edition** offers only access to ML SDKs and notebooks.  
**The Enterprise edition** offers the features of the Basic edition, but it adds many additional features, including the visual designers.

*Azure Machine Learning is priced based upon your usage. You’re billed for a VM where your  
Azure Machine Learning assets run. You are also charged a machine learning surcharge and a small amount per hour for usage.*

**Cognitive Services  
SaaS ML models that you can use directly in your ML solutions without the expense of developing your own.**

Computer Vision can do things like

* Recognize objects or recognize a scene
* Recognize inappropriate content so you
* Moderate images.

**Video Indexer API**

* Can analyze video content and extract information from that content.
* You can easily add closed captioning in multiple languages recognize people and objects, and search for videos that contain specific words, people, or even emotions

**Speech Translation**

* Language translation in real-time to Speaker Recognition
* Analyze speech and identify the speaker.

Pricing for Azure Cognitive Services is

**Transactional** that means that you pay a small amount for transactions that you process through the service.

**Azure Bot Service**Is a PaaS offering that runs on Azure App Service. That means that it inherits all the features of App Service such as easy scaling and simple configuration.

This includes editing the source code, building the source code, viewing analytics, and so forth. All these tasks are part of the Bot Framework that Microsoft developed to streamline the creation of bots.

*Azure Bot Service can be connected to many popular services such as Slack, Facebook Messenger, Microsoft Teams, and more. Each of these is considered a channel within the Bot Service, and the channels that Microsoft provides are called standard channels. However, you can also use what Microsoft calls Direct Line to connect your bot to your own application or website. Direct Line is considered a premium channel, and it will cost a small amount for the messages it uses.*

**Because Bot Service runs on Azure App Service, you are also charged for an App Service plan when you create a Bot Service.**

**Serverless computing**Sometimes, you just need to “borrow” a computer in order to run a computation or perform a quick task. In those situations, a serverless environment is ideal.   
In a serverless situation, you pay only when your code is running on a VM.   
When your code’s not running, you don’t pay anything.

All cloud providers need surplus capacity so they can meet the needs of customers, but when VMs are sitting there waiting for a customer who might want to use them, it means lost revenue for the cloud provider.   
To solve that problem, cloud providers created consumption-based plans that allow you to run your code on these surplus VMs, and you pay only for your use while your code is running.

*Cognitive Services is an example of a serverless service, but Azure has many other serverless services*

**Azure Functions**Azure Functions is the compute component of Azure’s serverless offerings. That means that you can use Functions to write code without having to worry about deploying that code or creating VMs to run your code.

**You can choose to create your Function App in an App Service plan, but if you do, you won’t benefit from the consumption model of paying only when your code runs.**

A **proxy** allows you to configure multiple endpoints for your Function App but expose them all via a single URL

**Slots** allow you to create a copy of your Function App that isn’t public facing.  
**You can configure a daily quota for your Function App. Once you reach the quota, Azure will stop the Function App until the next day.**

*If you want to protect your Function App from unauthorized use, you should use authentication features available in App Service to require authentication. You can also use Microsoft API Management to add security requirements to your Function App.*

**Logic Apps  
Similar to Function Apps in that they are kicked off by a trigger,** but what happens after that is completely different. **Unlike Function Apps, you don’t have to write code to create some powerful workflows with Logic Apps.**

A workflow simply means that a Logic App reacts to something happening and responds by performing a series of tasks, such as:

* Sending an email
* Transferring data to a database

For example, when a customer orders a product from your ecommerce site, you might want to:

* Update your inventory count of the product
* Generate an invoice for the item
* Email the invoice to the customer
* Sign the customer up for your newsletter
* Generate a shipping label for the item

**There are three components in Logic Apps that make workflows possible: connectors, triggers, and actions:**

* **A connector** is a component that connects your Logic App to something, such as another Azure service, a third-party service, an FTP server, and so forth. Each connector will have one or more triggers and actions specific to that connector.
* **A trigger** is a specific action that will cause your Logic App workflow to run
* **An action** is what your Logic App will do as an output.

*As you’re configuring triggers and actions in the Logic Apps designer, Logic Apps is writing code for you under the hood that will implement your workflow. Logic App workflows are defined using JSON files, and the designer generates this* ***JSON*** *code as you are configuring your app.*

**Event Grid**Event Grid provides that functionality: **Enable an Azure service to trigger an event when something specific happens and configures another Azure service to listen for that event so it can react to it**

**Both Azure Functions and Azure Logic Apps** are integrated with Event Grid. You can configure a function to run when an Event Grid event occurs.

The primary benefit of using Event Grid in this way is the rapid development of solutions. You also benefit from Event Grid reliably triggering your events. If an Event Grid event fails to trigger for any reason, Event Grid will continue to retry triggering the event for up to 24 hours.

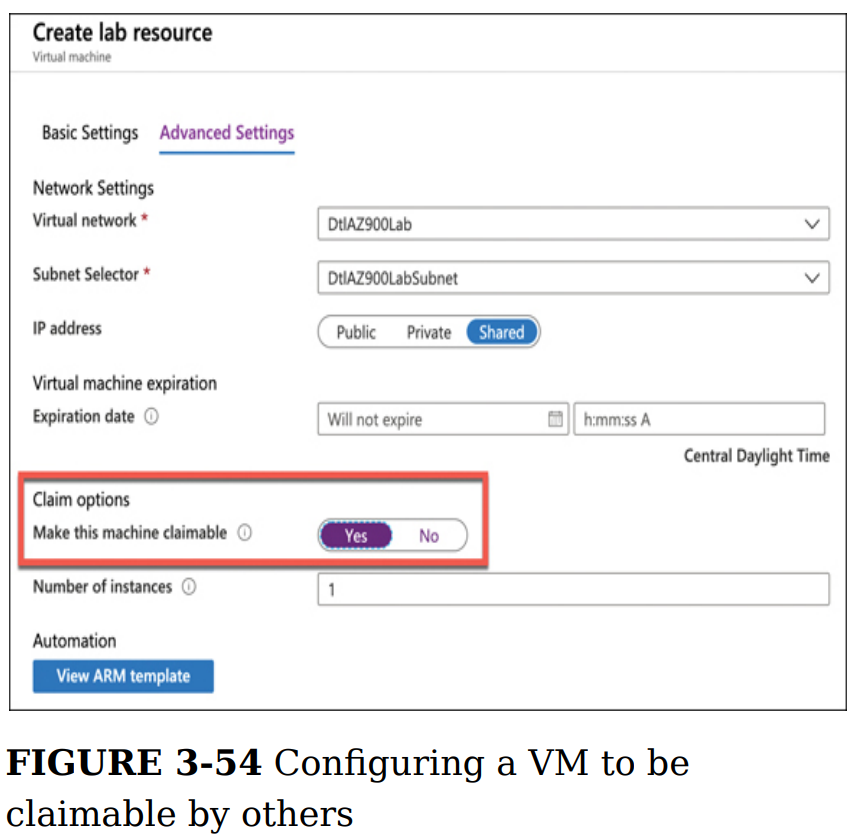
**Azure DevOps  
Offers a collection of tools that make it much easier to plan, track, and manage such projects.**

* **Azure Boards** A visual way to manage and track work for your team using tiles displayed in a drag-and-drop interface
* **Azure Repos** Source and version control using either Team Foundation Version Control or Git
* **Azure Pipelines Manage** software releases through build, test, and release automation
* **Azure Test Plans** Create and track tests to ensure reliable software releases
* **Azure Artifacts** Use popular package feeds from both public and private sources

Many software applications use packaged components from third parties or from within the developer’s own organization. These packaged components are frequently referred to as artifacts, and **Azure Artifacts** provides an easy way to keep these artifacts organized. Azure Artifacts also provides the ability to integrate these packages into the build process, including builds that happen within Azure Pipelines.

**Azure DevTest Lab**Enables developers on teams to efficiently self-manage virtual machines (VMs) and PaaS resources without waiting for approvals.  
DevTest Labs creates labs consisting of pre-configured bases or Azure Resource Manager templates. These have all the necessary tools and software that you can use to create environments. You can create environments in a few minutes, as opposed to hours or days.  
VMs can be created in a DevTest Lab that are preconfigured for specific purposes. When developers need to use a VM for testing, they simply look at a list of available VMs and claim the VM they need. That VM is then allocated to them until they unclaim it. Claiming a VM takes only seconds because the VM doesn’t have to be created again when it’s claimed.

It’s very important to understand that when a VM is created in DevTest Labs, it defaults to being dedicated to a single user and is not claimable. **If you are creating a VM that you want others to be able to claim and use, you must click Advanced Settings at the top of the screen shown previously in Figure 3-53 and configure the machine to be claimable,** as shown in Figure 3-54.

****

*You can’t easily add one of your existing VMs into a DevTest Lab. In order to do that, you have to jump through some hoops to copy the VM’s VHD image into the Azure Storage container that the DevTest Lab is using and then create a new VM from the custom image.*

Custom images and formulas are similar, but there is one key difference. A custom image is an image that is based on a VHD from an existing VM. A formula is also based on a VHD, but a formula also contains settings that are specific to DevTest Labs, such as VM size, included artifacts, and so forth. A formula, however, often uses a custom image as a base.

**SKILL 3.2: DESCRIBE AZURE MANAGEMENT TOOLS**

**Azure portal  
Everything that you do in the Azure portal calls ARM on the back end.**To the right of the search box is a button that will launch **Azure Cloud Shell**. Cloud Shell is a web-based command shell where you can interact with Azure from the command line. You can create Azure resources and more.

*You can reorder items on the menu. Click and hold an item, and then drag it to a new location in the menu.*

**Azure PowerShell**The PowerShell Az module uses the .NET Standard library for functionality, which means it will run with PowerShell version 5.x, 6.x, or 7.x. **PowerShell 6.x and 7.x are cross-platform and can run on Windows, Linux, or macOS.** If you’re running Windows 7 or later and you have PowerShell 5.x, you’ll also need to install .NET Framework 4.7.2.

**Before you can use the PowerShell Az module, you’ll need to install it. To do that, you first need to run PowerShell elevated.**

To install the module, run the following command.   
**Install-Module -Name Az –AllowClobber**

If you are unable to run PowerShell elevated, you can install the module for your user ID only by using the following command:  
**Install-Module -Name Az -AllowClobber -Scope CurrentUser**

Once you’ve installed the module, you need to sign in with your Azure account. To do that, run the following command:   
**Connect-AzAccount**

**This command will display a token in the PowerShell window***. You’ll need to browse to https://microsoft.com/devicelogin and enter the code in order to authenticate your PowerShell session. If you close PowerShell, you’ll have to run the command again in your next session.*

For example, the following command will create a resource group called MyRG in the South Central US region:  
**New-AzResourceGroup -Name MyRG -Location "South Central US"**

To remove the resource group, run the following command:  
**Remove-AzResourceGroup -Name MyRG**You can use the -Force parameter to bypass the prompt. (Y)  
**Remove-AzResourceGroup -Name MyRG -Force**

**Azure CLI**Azure CLI can be scripted using shell scripts in various languages like Python, Ruby, and so on.

Once you install the Azure CLI, you’ll need to log in to your Azure account.  
**az login**

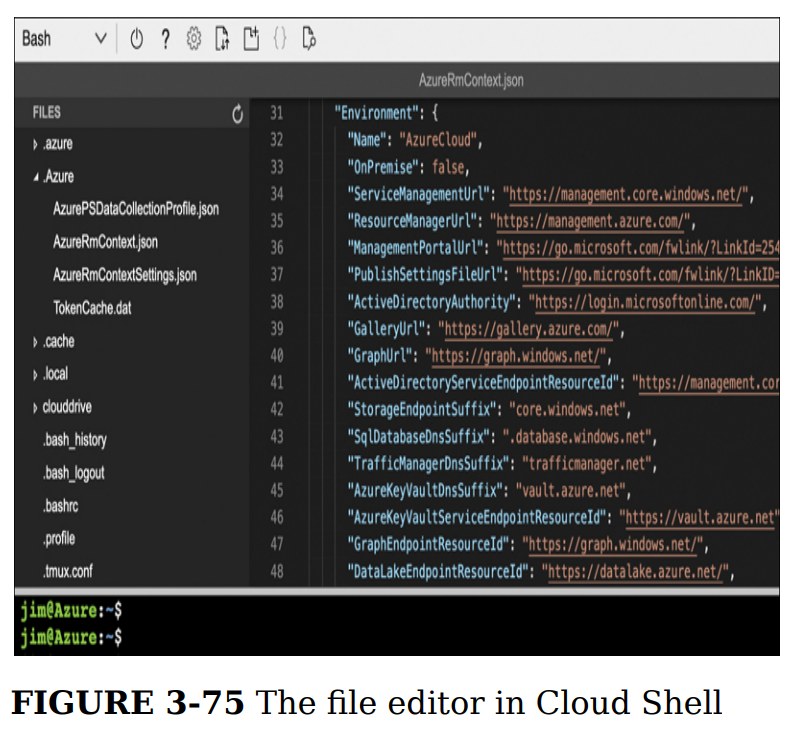
You can set the default subscription by entering the following command:  
**az account set --subscription "subscription\_id"**

You can, for example, run the following command to get help on the syntax for az resource create:  
**az resource create –help**

**Azure CLI help:** An even easier way to learn the CLI is to switch into interactive mode. This provides you with auto-complete, the scoping of commands, and more. To switch into interactive mode, enter az interactive at the command prompt. The CLI will install an extension to add this functionality.

***az extension list-available --output table*az extension add --name extension\_name**

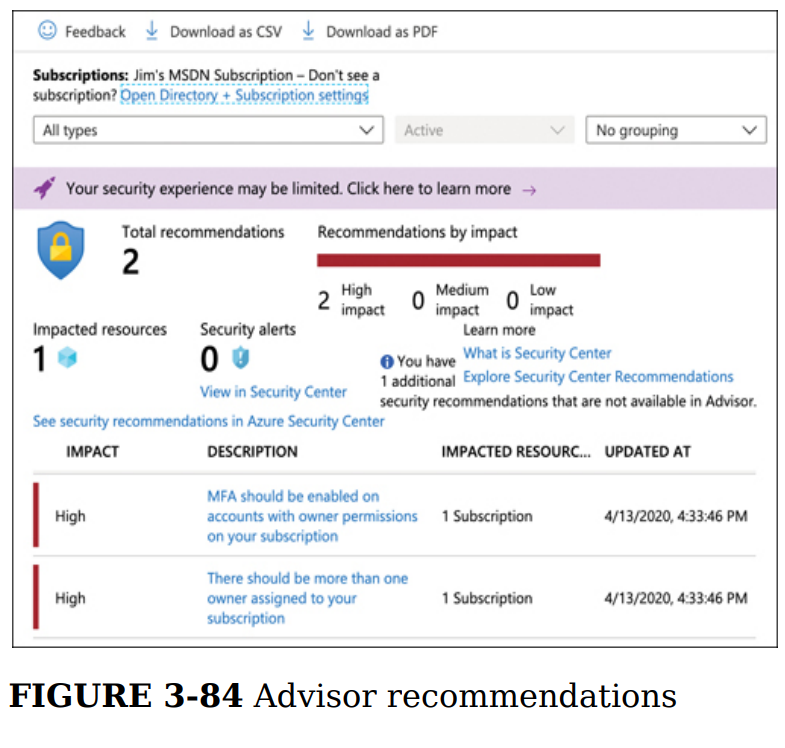
**Azure Cloud Shell**The first time you launch Cloud Shell, you’ll need to select the environment you want to use. **You can choose between Bash and PowerShell**, but if you change your mind later, you can change it at any time.  
Once you select an environment, you’ll also need to create an Azure storage account. Cloud Shell persists anything you install and your settings throughout all your devices, so you need a storage account to persist those.  
  
***From Cloud Shell, you can run any of the commands you can run in the Azure CLI.*** *If you’re in PowerShell, you can also use commands from the Az PowerShell module.  
  
Any files that you upload will be available to you in Cloud Shell on any of your devices.*

The Open Editor button on the toolbar will open an instance of the Monaco Editor, a code editor that makes it easy to edit scripts and other files.  


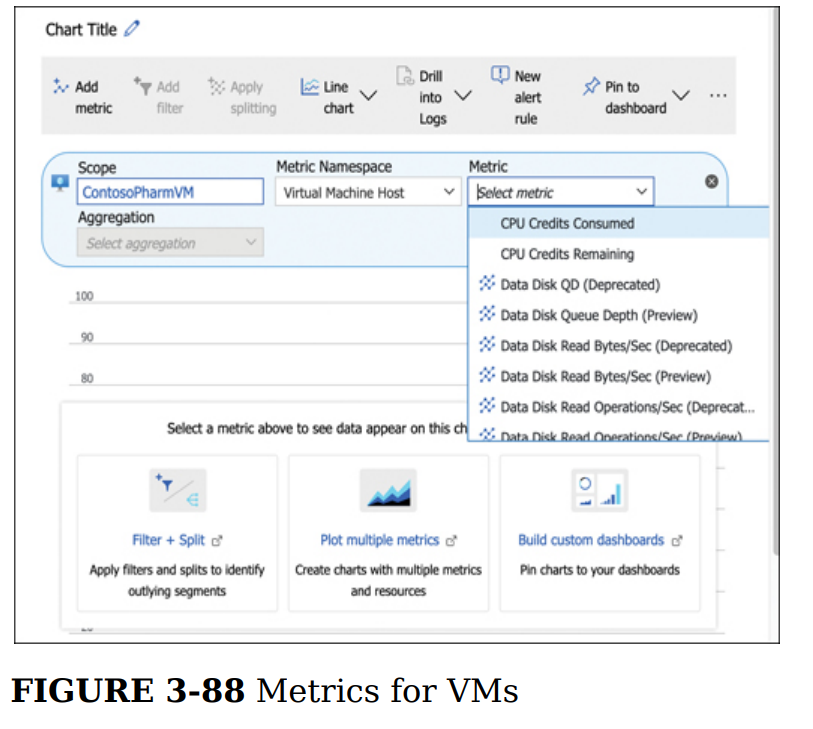
**Azure mobile app**If you own **an Android or iOS device**, you can download the Azure mobile app to manage your Azure resources from your device. You can always browse to the Azure portal on your device, and you’ll get an experience customized for smaller screens. However, just as with other websites you might use, an app provides a better first-class experience on a mobile device.

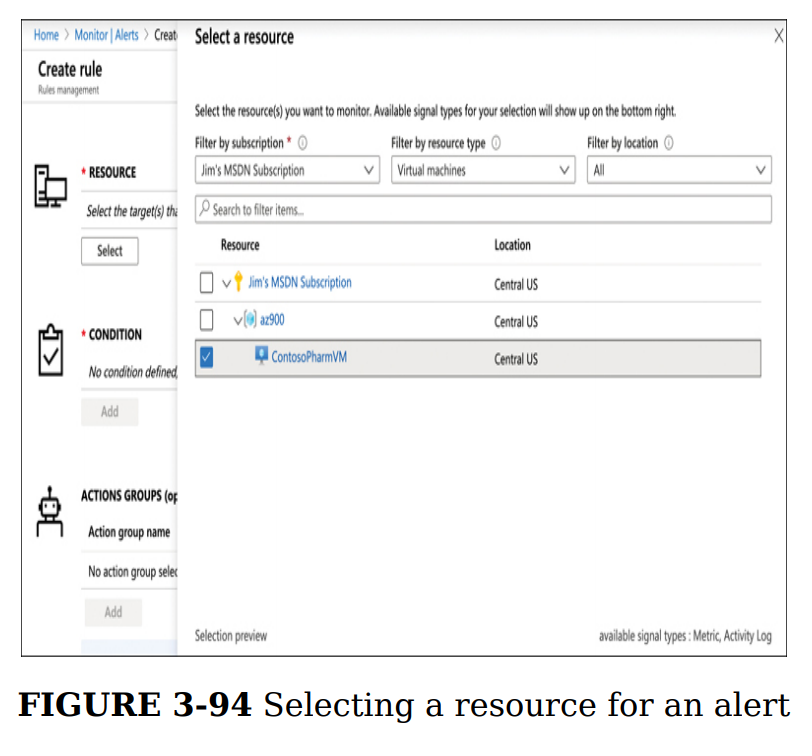
*You won’t have the full functionality of the Azure portal, but you will be able to see details of the resource and perform basic functions against it.  
Connecting to a VM requires that you have the* ***Microsoft Remote Desktop app installed****. You can download it free from the Apple Store or the Google Play store.*

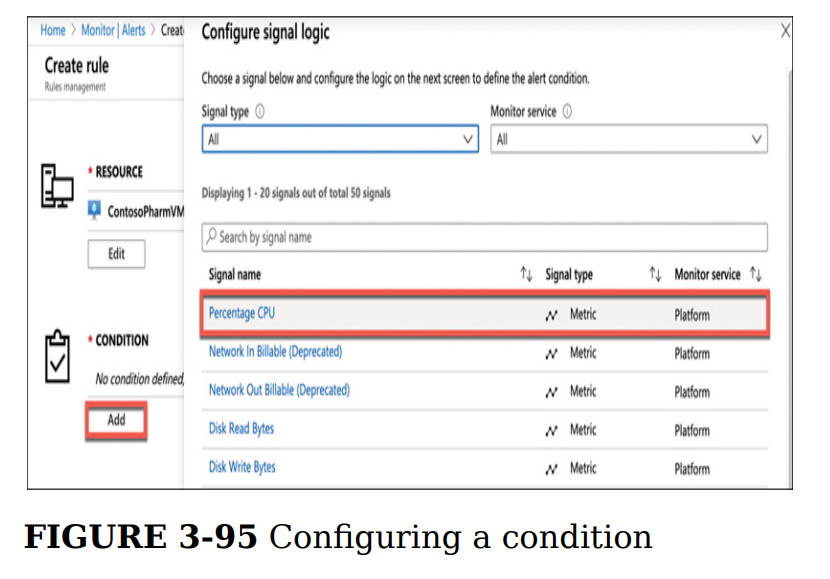
**Azure Advisor  
Can offer advice about high availability, security, performance, and cost.**

******

**Azure Monitor  
Aggregates metrics for Azure services and exposes them in a single interface. You can also create alerts that will notify you or someone else when there are concerns you might want to address.**

**Azure Monitor Alerts can notify you or others with email or SMS text message, run a Logic App flow, call a Function App, make a request to a webhook, and more, when a certain condition is met.**Alerts are based on rules that you define, and when a rule’s condition is met, an alert performs the action you specify.

******

******

**An alert rule can consist of multiple conditions. For example, you can have a rule that only triggers if CPU averages above 70 percent and disk usage is also high. The choice is yours.**

**Azure status  
View other issues that might be impacting your services**[**https://status.azure.com/en-us/status**](https://status.azure.com/en-us/status)

**Azure Service Health**Azure Status is a web page where you can view the current status of Azure services in all regions where Azure operates. While it is a helpful view of overall Azure health, the enormous scope of the web page doesn’t make it the most effective way to get an overview of the health of your specific services. **Azure Service Health can provide you with a view specific to your resources.**

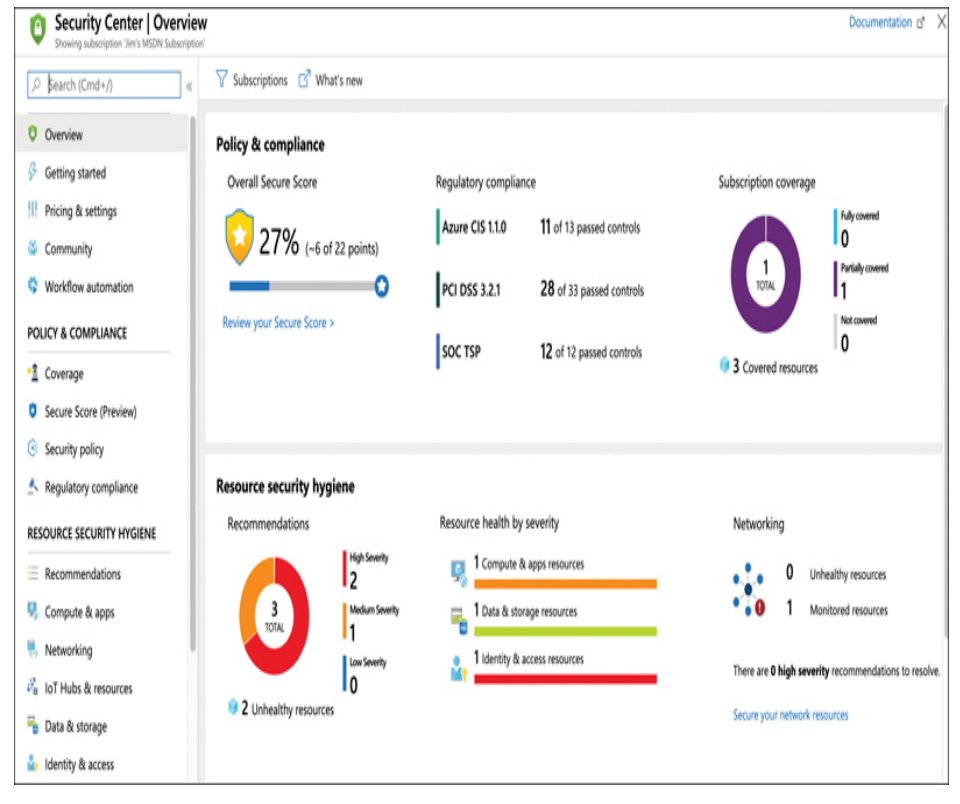
*Both Azure Monitor and Azure Service Health are critical to the overall view of your Azure resources.* **Azure Monitor is geared toward monitoring the cost and performance of your resources and alerting you and others when conditions warrant. Azure Service Health, on the other hand, is the single-point-of-truth for information on the health of Azure itself and how Azure incidents are affecting your resources. The combination of these two services provides you with all the tools you need to keep up with your Azure resources and how well they’re performing.**

**Chapter 4 DESCRIBE GENERAL SECURITY AND NETWORK SECURITY FEATURES**

**SKILL 4.1: DESCRIBE AZURE SECURITY FEATURES**

**Azure Security Center  
Can help you keep up with best practices, but it also can help with providing the steps you need to take to keep your resources configured in a way that makes them more secure. Security Center can even help you with keeping your on-premises resources secure.**

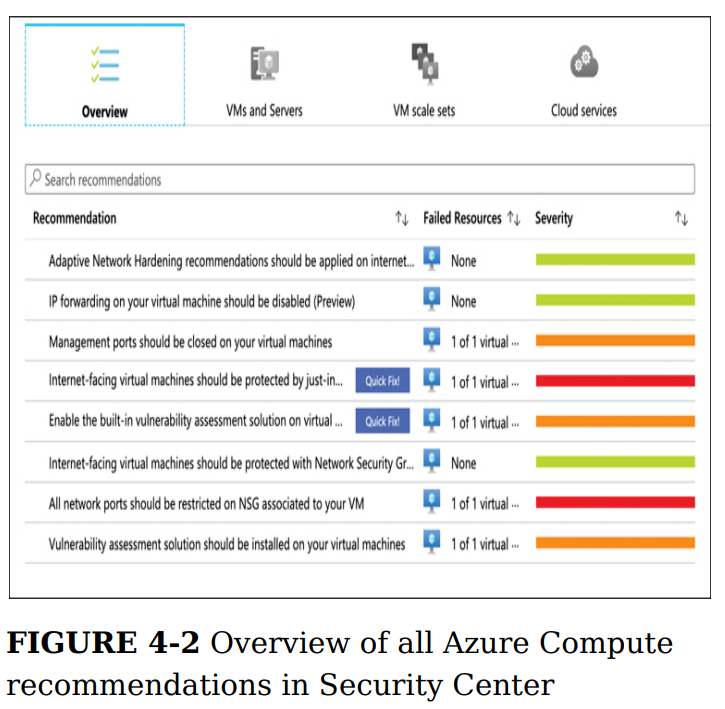
* **Free tier** The free tier provides general assessment and recommendations for securing your Azure resources and covers only Azure virtual machines and Azure App Service.
* **Standard tier** The Standard tier adds coverage of your Azure SQL Databases, MySQL databases, PostgreSQL, Azure Storage, IoT devices, AKS, Azure Container Registry, and Azure Key Vault. The Standard tier also offers additional features such as advanced threat detection, analysis from Microsoft Threat Intelligence, and the ability to manage the regulatory compliance of your Azure resources. The Standard tier is billed by the hour.

******

**3 primary areas of coverage in Security Center:**

* **Policy & Compliance** Provides a Secure Score and an Overall Score, which shows the security of your resources. This area also covers your compliance with regulatory standards.
* **Resource Security Hygiene** Provides a high-level overview of the health of your resources from a security perspective. Security issues are categorized as High Severity, Medium Severity, or Low Severity.
* **Threat Protection** Shows you any active or past attacks or threats on your resources.

***Information for the Policy & Compliance and Resource Security Hygiene areas is provided by the service being protected. This information is often related to best practices. The information in the Threat Protection area, on the other hand, is specifically targeted at analyzing both the network traffic and the behavior of users of your resources. If anything looks suspicious, it’s reported by Security Center (*For example, if a user elevates his privileges on a VM and runs an unknown process, these activities would likely be flagged as an incident that should be investigated.)**

******

*Clicking one of the recommendations will provide additional information. In most cases, you’ll see a link to instructions on how you can address the recommendation, but* **Security Center can automatically take care of some recommendations***. Recommendations that can be fixed automatically will display a Quick Fix badge*

Security Center provides a feature **called just-in-time (JIT) access** that helps to protect your VMs from attacks on management ports. **When JIT access is enabled**, users must request access to a VM in order to remote into it. Until someone is given JIT access, management ports on the VM are closed so they can’t be accessed. Once JIT access is given to a user, the ports are open for ***a specific period of time*** as requested by the user. Once that time period has elapsed, the management ports are closed again.

**In addition to specifying the port, you can also control which protocols are allowed over the port and which IP addresses are allowed**. If the allowed IPs are set to Per Request, the user who requests access will have the option of specifying an IP address or a CIDR block. Otherwise, you can specify a **CIDR** block yourself in order to allow access only from a specific IP address range.

***The maximum request time can be configured from 1 to 24 hours, but it defaults to 3 hours.***

**Key Vault  
Provides a secure way to store secrets, keys, and certificates**

*Once an item is stored in Key Vault, you can apply security policies that define which users and applications can access it. Key Vault is encrypted using encryption keys, but Microsoft has no visibility into the encryption keys or the encrypted data.*

There are two pricing tiers available in Key Vault:   
**Standard and Premium -** The only difference between the two is that keys are stored in hardware security modules (**HSMs**) in the Premium tier*.****HSM:*** *is a separate piece of hardware that is designed for securely storing encrypted content, and it’s also specialized for processing cryptographic data.*

*(Keeping encryption keys in an HSM boundary is required for Federal Information Processing Standard (FIPS) 140-2, so companies that need to maintain compliance with FIPS 140-2 can do so by using the Premium tier of Key Vault)*

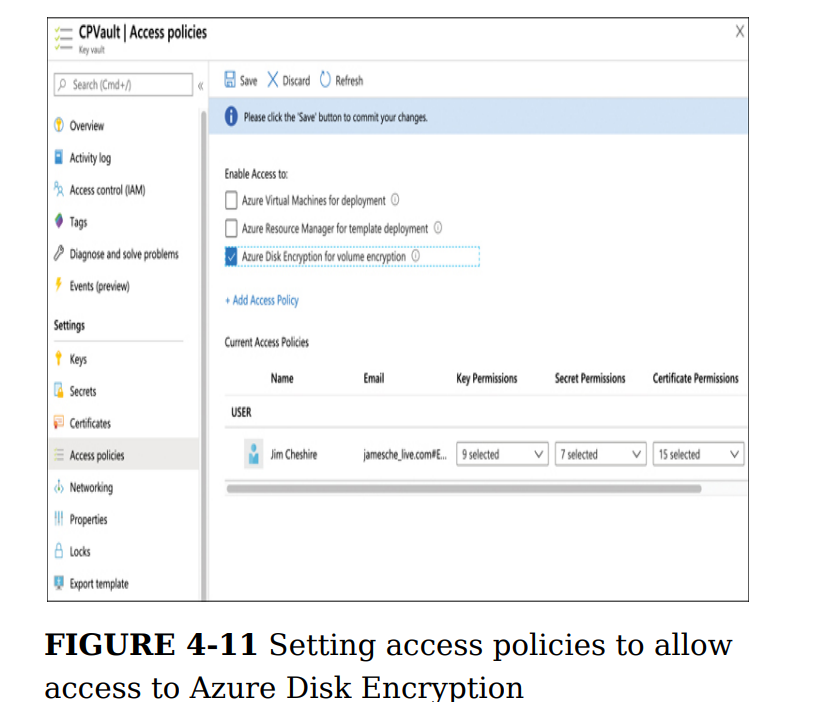
*You can import a key, secret, or certificate into Key Vault, but Key Vault can also generate security keys and certificates for you.*

For example, you might want to generate a security key that your company can use to sign certificates. If you want to generate a 4,096-bit security key for this purpose and store it in Key Vault, click Keys and then click Generate/Import.

*Once the key has been stored, you can view the entry to get the key identifier, which is a URL that can be used by authorized users or applications to retrieve the key. However, you cannot view the key because it’s encrypted and not available except through the key identifier.*

*Another common use scenario for Key Vault is to store encryption keys for Azure VMs.* ***One of the security recommendations offered by Security Center is to encrypt VM disks.*** *A VM disk is stored as a VHD file, and when it’s encrypted, the host operating system that runs the VM must be able to access the security key in order to decrypt the VHD and run the VM. Key Vault offers capabilities that are specifically targeted for this kind of scenario.*

In order to use Key Vault for disk encryption keys, the access policies must be configured to allow the vault for disk encryption. If this wasn’t done when the vault was created, you can change it by clicking Access Policies, and checking the **Azure Disk Encryption** For Volume Encryption option

**

**In order to enable encryption and store the keys in Key Vault, your VMs and Key Vault must be in the same Azure subscription, and they must be in the same Azure region. For more details on disk encryption requirements and steps to enable encryption.**

**Azure Dedicated Host  
Provides physical server that host one more Azure virtual machines that is dedicated to a single organization`s workland.**

* Hardware isolation at the server level
* Control over maintence event timing
* Aligned with Azure Hybrid Use Benefits

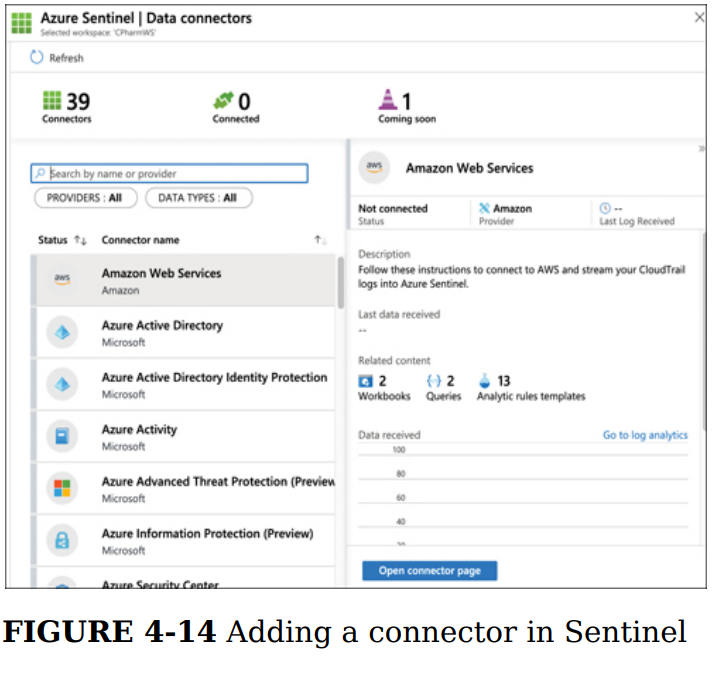
***Azure Dedicated Host*** *is your very own* ***private cloud in AzureWith*** *Azure Dedicated Host, you can control the maintenance window, gain visibility over the underlying infrastructure, and place your Azure VMs on a single tenant server to satisfy specific compliance or regulatory requirements.*

**Azure Sentinel  
Is a scalable, cloud-native SIEM e SOAR solution.** Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

* SOAR (Security Orchestration, Automation, and Response)
* SIEM (Security Information and Event Management). Many companies, in fact, use SOAR and SIEM in combination.
* **Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.**
* **Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.**
* **Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.**
* **Respond to incidents rapidly with built-in orchestration and automation of common tasks.**

*Azure Sentinel isn’t only for Azure. It can also provide threat reporting and analysis for on-premises resources and for resources on other clouds.*

Microsoft provides connectors for Azure and other Microsoft products, but there are also connectors for third parties.

******

**When Sentinel finds a problem, you can have it respond using a Playbook. A Playbook is a workflow that runs in response to an alert in Sentinel.** To create a Playbook, click Playbooks and then click Add Playbook.

**When you add a new Playbook, Sentinel will ask you to create a new Logic App. That’s because Playbooks use Logic Apps for their workflows.**

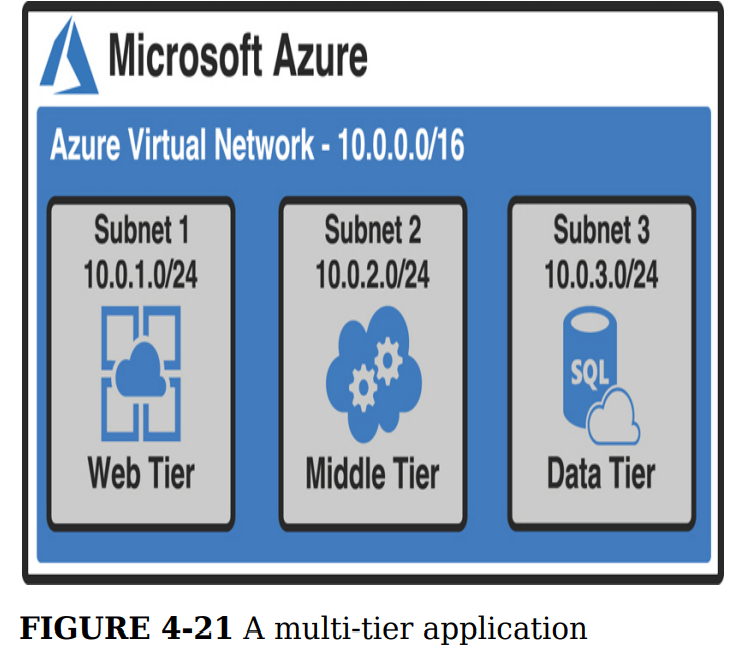
**SKILL 4.2: DESCRIBE AZURE NETWORK SECURITY**

**Defense in depth**Medieval folks had a pretty good idea when it came to security. They realized that a single opposing force wouldn’t be enough to keep them secure. They needed layered opposition so that anyone defeating one method of security would be met with several more down the line.  
  
This is a perfect example of defense in depth, and it’s why defense in depth is often referred to as the **“castle approach.”**

* **Azure Firewall** can help prevent a malicious user from making it into your network
* **Network Security Groups** can help you control network traffic inside your network
* **Azure DDoS Protection** can help to identify and mitigate malicious traffic that might otherwise seem normal.

**Shared Security**

**Network Security Groups (NSGs)  
Allows you to filter traffic on your network and apply rules on that traffic**. An NSG contains several built-in rules provided by Azure that are designed to **allow your resources in the virtual network to communicate with each other**. You can then add your own rules to the NSG to control traffic into and out of the network, and also between resources in the network.

****

Here’s the traffic flow of this application

* Subnet 1 receives data from another virtual network running Azure Firewall.
* Subnet 1 communicates with Subnet 2 to process requests.
* Subnet 2 communicates with a database server in Subnet 3 in order to access data.

**If you want to ensure a secure environment, Subnet 1 should not be able to directly communicate with resources in Subnet 3. Likewise, Subnet 3 should not be able to directly communicate with resources in Subnet 1. Finally, only Subnet 1 should be able to communicate with the other virtual network running Azure Firewall. You can use NSGs to implement rules that will enforce these policies.**

**An NSG that’s associated with a subnet affects all VMs inside that subnet, as well as traffic to and from the subnet. For example, let’s say you configure an NSG to prevent all traffic except traffic from the Internet and you then associate that NSG with a subnet containing two VMs. In that event, those two VMs will no longer be able to communicate with each other because only traffic from the Internet is allowed by the NSG.**

To prevent rules from interfering with each other, each rule you create in an NSG has a priority between 100 and 4,096. Rules with a lower priority take precedence over rules with a higher priority.

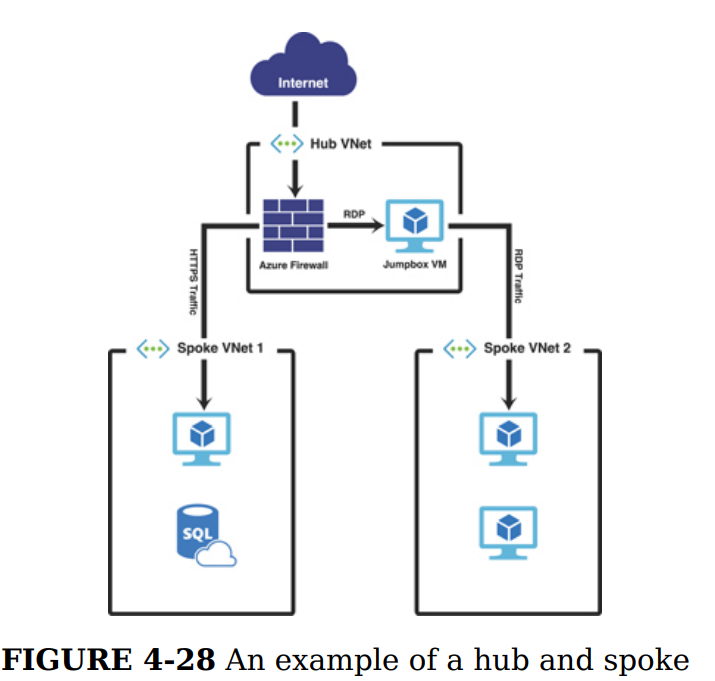
**Service Tag**   
is a special identifier created by Microsoft that applies to the Internet or to a specific service type within Azure. **For example, if you have some web apps running in Azure App Service, and you want to allow them to communicate with your subnet, you can use the AppService service tag in your inbound rule to allow that.**

**Azure Firewall**Is a PaaS offering in Azure, and it’s easily managed and offers a **99.95 percent uptime guarantee.** Azure Firewall scales according to your networking needs, so you don’t have to worry about traffic spikes causing latency or downtime for your applications.  
  
**Azure Firewall is a stateful firewall. That means that it stores data in its memory about the state of network connections that flow through it.** When new network packets for an existing connection hit the firewall, it can tell if the **state of that connection represents a security threat.** For example, i**f someone spoofs your IP address and attempts to gain access to your virtual network in Azure, the firewall would recognize that the hardware address of the computer being used has changed and reject the connection.**

A typical setup for Azure Firewall consists of the following

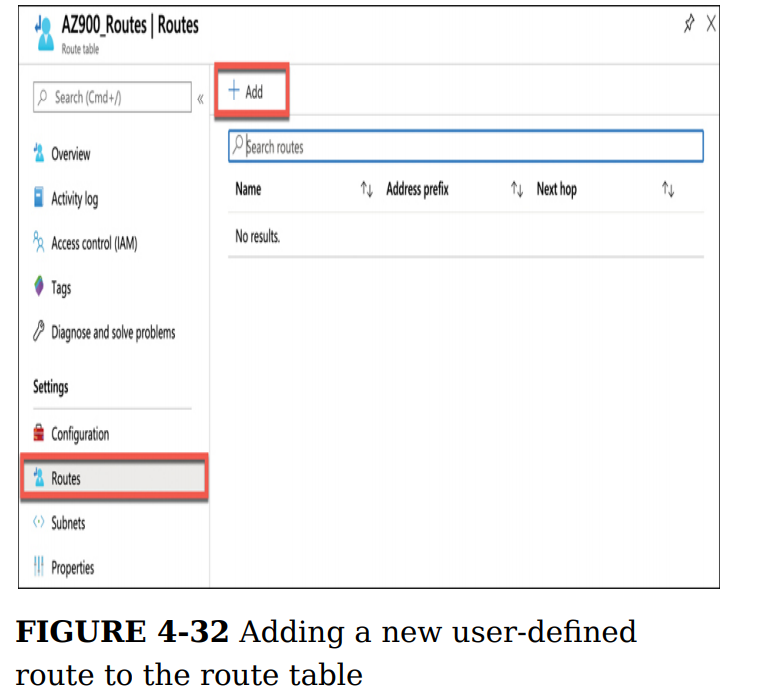
* **A centralized hub network that contains the Azure Firewall and a VM that operates as a jumpbox. The firewall exposes a public IP address, but the jumpbox VM does not.**
* **One or more additional networks (called spoke networks) that don’t expose a public IP address. These networks contain your various Azure resources.**

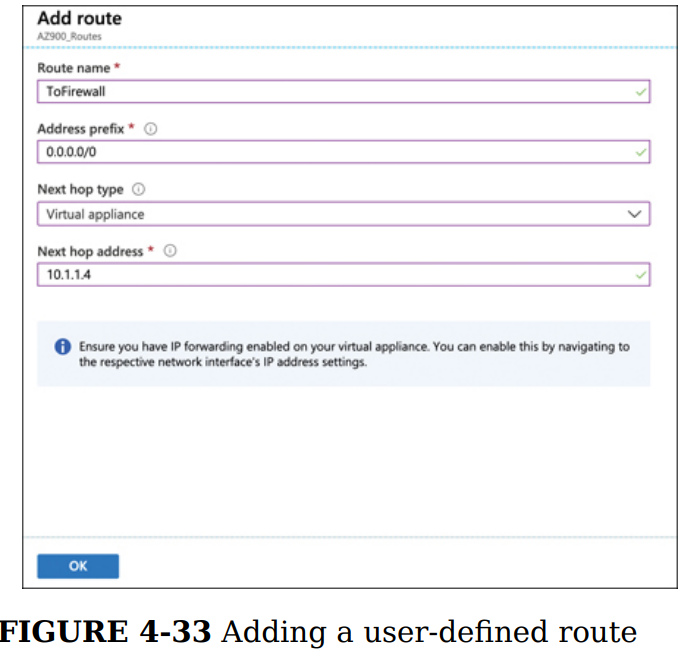
**The jumpbox is a VM that you can remote into in order to manage other VMs in your networks. All other VMs are configured to only allow remote access from the jumpbox VM’s IP address.**

******

To send traffic to your firewall, you need to create a route table.   
  
**Route Table   
Is an Azure resource that is associated with a subnet and it contains rules (called routes) that define how network traffic in the subnet is handled.**A route table is created using the Route Table item in the Azure Marketplace. Once you create a new route table, you must associate it with one or more subnets. To do that, click Subnets and then click Associate, as shown in Figure  
******  
 *It’s important to understand that a firewall can (and should) be used to filter traffic flowing into and out of a network. For example, you want the firewall to handle traffic into your jumpbox, but you also want to ensure that traffic flowing from the subnet where other servers are located is secure and not inappropriately sending data out of your network.*

Once we’ve associated the route table with the subnets, we create a user-defined route so that traffic is directed through Azure Firewall





**There are three types of rule collections available in Azure Firewall.**

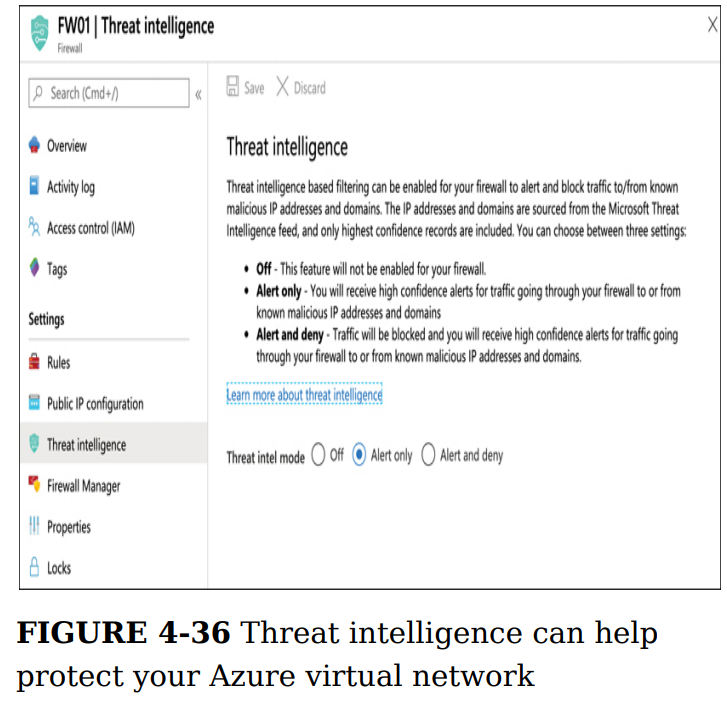
* NAT Rule Collection Network address translation (NAT) rules are used to forward traffic from the firewall to another device on the network.
* Network Rule Collection These are rules that allow traffic on specific IP address ranges and ports that you specify.
* Application Rules Collection Application rules are used to allow applications, such as

Windows Update, to communicate across your network. Also, they can be used to allow particular domain names such as azure.com and microsoft.com.

*If there isn’t a NAT rule that matches the traffic, network rules are applied. If a network rule matches the traffic, all further rule processing is stopped. If there isn’t a network rule that applies to the traffic, the application rules are applied. If none of the application rules match the traffic, the traffic is rejected by the firewall.*

In addition to rules that you configure, the threat intelligence feature in **Azure Firewall can protect you from known-malicious IP addresses and domain names.  
Microsoft constantly updates its list of known-bad actors, and the data collected is provided in the Microsoft Threat Intelligence feed.**

When **you enable threat intelligence,** you can choose to have Azure alert you if traffic from a known-malicious IP address or domain name attempts to enter your network. Also, you can choose to have the traffic denied by the firewall automatically.

******

**Azure DDoS ProtectionProtection to help protect against DDoS attacks. DDoS Protection is a feature of Azure Virtual Networks. There are two tiers of DDoS Protection: Basic and Standard.**

**Basic** protects you from volume-based DDoS attacks by distributing large amounts of volume across Azure’s entire network infrastructure. Basic DDoS Protection applies to both IPv4 and IPv6 public IP addresses. With the Basic tier, you have no logging or reporting of any DDoS mitigation, and there’s no way to configure alerts so that you’re notified if a problem is detected. However, the Basic tier is free and provides basic protection.

**Standard** offers protection from volume-based DDoS attacks, and when it’s used in combination with Azure Application Gateway, it also provides protection from attacks designed to target the security of your applications. It offers logging and alerting of DDoS events and mitigations, and if you need help during a DDoS attack, Microsoft provides access to experts who can help you. The DDoS Standard tier applies only to IPv6 public IP addresses. The Standard tier is targeted at enterprise customers and is billed at $2,994 per month, plus a small fee per gigabyte for data that is processed. The fixed monthly price covers up to 100 resources. If you need to cover additional resources, you pay an additional $30 per resource, per month.

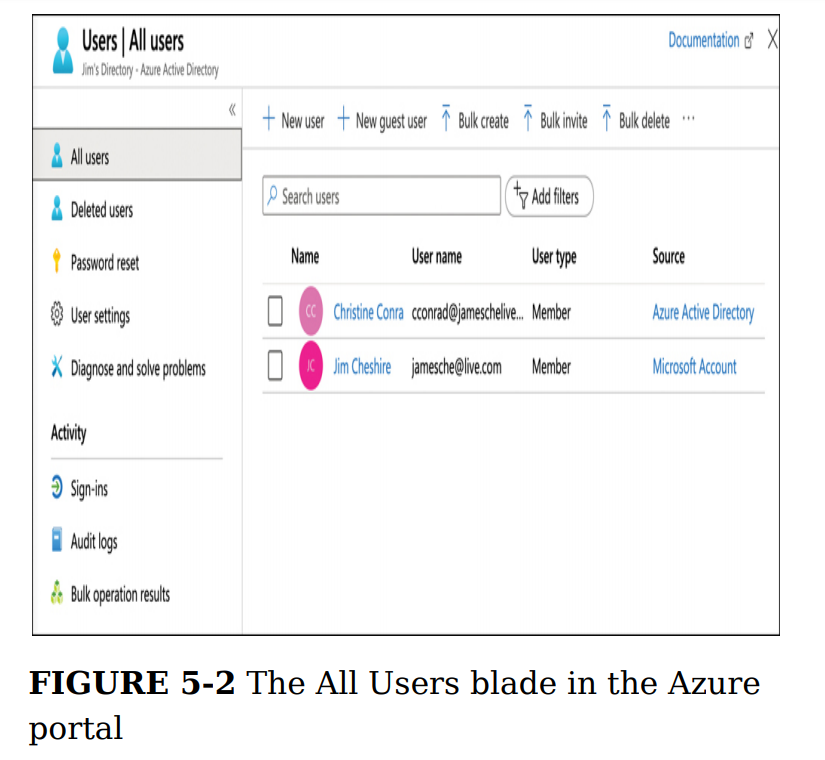
*To enable Standard tier, you’ll need a DDoS Protection plan. If you don’t currently have one, click Create A DDoS Protection Plan to create one in the Azure portal.*

**Chapter 5 DESCRIBE IDENTITY, GOVERNANCE, PRIVACY, AND COMPLIANCE FEATURES**

**SKILL 5.1: DESCRIBE CORE AZURE IDENTITY SERVICES**

**Azure Active Directory**Azure AD is a cloud-based identity service in Azure that can help you authenticate and authorize users

**When you sign up for an Azure subscription, an Azure AD resource is automatically created for you.**

**** *The Azure AD shown in the Figure contains two users. The first user’s source is Azure Active Directory, and this user was manually added to the directory. The other user is using a Microsoft Account to log in to the directory.*

**Azure AD B2B** (business-to-business)   
**Collaboration that allows you to add users who don’t belong to your company**. So, you can invite other users from outside of your company to be members of your Azure AD. **Those users can then be given access to your resources. Users who are not part of your company are called guest users.**

*User can be given access to the corporate social media accounts by adding those applications to Azure AD. Thousands of applications can be added, including social media apps such as Facebook and Twitter.*

After you add an application, **you can configure Azure AD so that users with access to that application can authenticate to it using the same credentials they use to log in to Azure AD.** This kind of authentication is known as **single sign-on** (or **SSO**), and it’s one of the key benefits to using Azure AD.

*Azure AD B2B allows you to invite guest users to your Azure AD from other businesses. Another AD feature called* ***Azure AD B2C*** *allows you to give users access to Azure AD applications by signing in with existing accounts, such as a Facebook or Google account.***Azure Active Directory B2C** provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.



**Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM)** solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring and automatically handling threats like denial-of-service, password spray, or brute force attacks.

**Conditional Access and multifactor authentication (MFA)**Azure Conditional Access **allows you to create policies that are applied against users. These policies use assignments and access controls to configure access to your resources.**

*Conditional Access is only available in the Premium tiers of Azure AD. Because the free version of Azure AD is being used in these examples, the New Policy button is disabled*

* **Something you know, such as a username and password**
* **Something you have, such as a phone or mobile device**
* **Something you are, such as facial recognition or a fingerprint**
* **IP Location**

If multifactor authentication requires all three of these, it’s referred to as three-factor authentication, or sometimes **3FA**. If only the first two are required, it’s referred to as two factor authentication, or sometimes **2FA**.

**Device Management**Azure AD provides you with a central place to manage device identities



The All devices page enables you to:

Identify devices, including:

* Devices that have been joined or registered in Azure AD.
* Devices deployed using Windows Autopilot.
* Printers using Universal Print
* Perform device identity management tasks like enable, disable, delete, or manage.
* Printers and Windows Autopilot devices have limited management options in Azure AD. They must be managed from their respective admin interfaces.
* Configure your device identity settings.
* Enable or disable Enterprise State Roaming.
* Review device-related audit logs

**Role-based access control (RBAC)**Is a generic term that refers to the concept of authorizing users to a system that is based on defined roles to which the user belongs. **Azure implements RBAC across all Azure resources, so you can control how users and applications can interact with your Azure resources.**

* **Security principal** represents an identity. It can be a user, a group, an application (which is called a service principal), or a special AAD entity called a managed identity. A managed identity is how you authorize another Azure service to access your Azure resource.
* **Role** is what defines how the security principal can interact with an Azure resource. For example, a role might define that a security principal can read the properties of a resource but cannot create new resources or delete existing resources.
* **Scope** defines the level at which the role is applied, and it specifies how much control the security principal has. For example, if the scope is a resource group, the role defines activities that can be performed on all resources in the resource group.
* **Role assignments** Roles are assigned to a security principal at a particular scope, and that’s what ultimately defines the level of access for the security principal.

RBAC includes many built-in roles. Three of these built-in roles apply to all Azure resources.

* **Owner** Members of this role have **full access** to the resources.
* **Contributor** Members of this role can **create resources and manage resources, but they cannot delegate that right to anyone else.**
* **Reader** Members of this role **can see Azure resources, but they cannot create, delete, or manage those resources.**

**RBAC roles can be scoped to the management group, subscription, resource group, or resource level.**

*It’s important to understand that role assignments are additive. Your RBAC abilities at any particular scope are the result of all role assignments up to that level. In other words, if I have the Owner role on a resource group and you assign me the Website Contributor role on a web app within that resource group, the Website Contributor assignment will have no effect because I already have the Owner role on the entire resource group.*

**SKILL 5.2: DESCRIBE AZURE GOVERNANCE FEATURES**

**Azure Policy  
Allows you to define rules that are applied when Azure resources are created and managed.** For example, **you can create a policy that specifies that only a certain size VM can be created and that the VMs must be created in the South-Central US region**. Azure will take care of enforcing this policy so that you remain in accordance with your corporate policies.  
 **Six effects are supported in Azure Policy**. However, not all effects are available for built-in policies. The effects are:

* **Append** Adds additional properties to a resource**. It can be used to add a tag with a specific value to resources.**
* **Logs** a warning if the policy is not complied with.
* **AuditIfNotExists** Allows you to specify an additional resource type that must exist along with the resource being created or updated. If that resource type does not exist, a warning is logged.
* **Deny** Denies the create or update operation.
* **DeployIfNotExists** Allows you to specify an additional resource type you want deployed with the resource being created or updated. If that resource type is not included, it is automatically deployed.
* **Disabled** The policy is not in effect.

**Resource locks**RBAC is a great way to control access to an Azure resource,but **in cases where you just want to prevent changes to a resource, or prevent that resource from being deleted, resource locks (or locks) are a simpler solution. Unlike RBAC, locks apply to everyone with access to the resource.**

In order to create a lock, you must either be in the **Owner** or the **User Access Administrator** role in RBAC. Alternatively, an administrator can create a custom role that grants the right to create a lock.

**Locks can be applied at the resource level, the resource group level, or at the subscription level.**

**Locks only apply to operations that are handled by ARM, and some operations specific to a resource are handled**, *if you set a read-only lock on an instance of Azure Key Vault, it will prevent a user from changing access policies on the vault, but users can still add and delete keys, secrets, and certificates because those operations are handled internally by Key Vault.*

**If a lock is applied to a resource group, all resources in that resource group inherit the lock.** **Similarly, if a lock is applied at the subscription level, all resources in the subscription inherit the lock.   
  
It is possible to nest locks, and in such situations, the most restrictive lock is the effective lock.** For example, **if you have a read-only lock on a resource group and a delete lock on a resource in that resource group, the resource will actually have a read-only lock applied to it because a read-only lock is more restrictive.** The explicit delete lock will be ineffective**.**

**Tags**A tag consists of a name and a value.

You can apply a tag to most Azure resources, not just resource groups. **It’s also important to understand that by adding a tag to a resource group, you are not adding that tag to the resources within the resource group.**

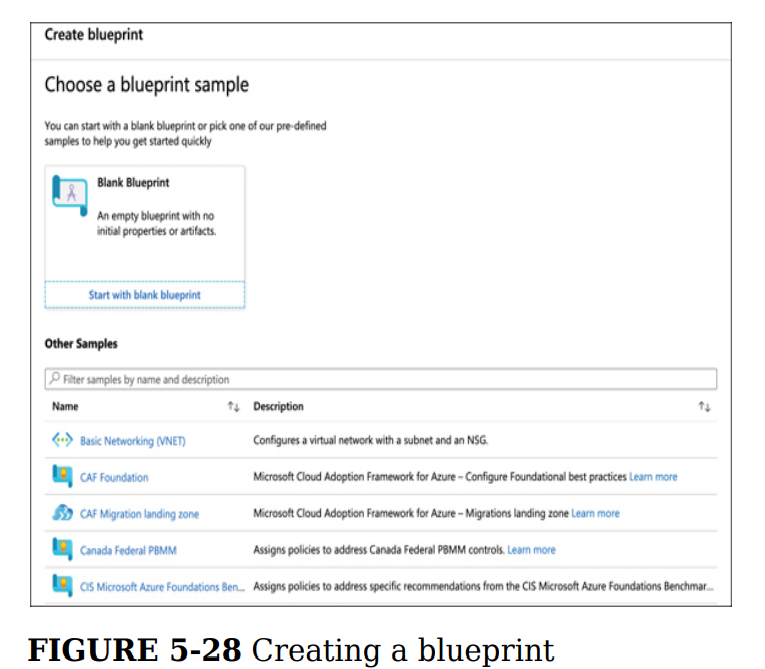
***Tags can also help you organize your Azure billing expenses. When you download your Azure invoice, resource tags will appear in one of the columns.*** *Because Azure invoices can be downloaded as comma-separated values, you can use tools like Microsoft Excel to filter based on tags.*

**Azure Blueprints  
Is a service that can make the process of deploying to the cloud easier.  
Blueprints allows you configure an environment just as you need it to be, along with all the policies and other governance aspects in place. That configuration can then be saved so it can be duplicated at any time in other deployments.**

Items that you add to a blueprint are called artifacts. An artifact can be a resource group, an ARM template, a policy assignment, or a role assignment.

You might be wondering how blueprints differ from ARM templates. After all, we did say that ARM templates are used to facilitate predictable and reproducible deployments. **Blueprints offer numerous benefits over ARM templates.** Because blueprints are actual Azure resources and not simply files designed to define a deployment, Azure maintains a connection between the blueprint and the resources that use the blueprint. That allows companies to iterate on blueprints and improve them. It also makes it much easier for a blueprint to evolve with a company’s needs. Also, blueprints are versioned and can be stored in a source-control system, so tracking of blueprints is easy and effective. With that said, it’s important to understand that blueprints aren’t a replacement for ARM templates. In fact, most blueprints make extensive use of ARM templates as artifacts.

Microsoft provides many sample templates that you can use as a foundation for your blueprint, but you can also start with a blank blueprint.



*You cannot change the name or the definition location of a blueprint after it’s created*

**SKILL 5.3: DESCRIBE PRIVACY AND COMPLIANCE RESOURCES**

**Microsoft privacy statement**

**Cloud Adoption Framework for Azure**Is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey.The Cloud Adoption Framework brings together all the best practices from Microsoft employees, Microsoft partners, and lessons learned from Microsoft customers. All this information is made available in a comprehensive website. All the information from the framework is neatly organized, and you can even download assets such as an infographic to help you visualize the Cloud Adoption Framework.

**Trust Center**The Trust Center is a web portal where you can learn all about Microsoft’s approach to security, privacy, and compliance. You can access Trust Center by browsing to <https://aka.ms/microsofttrustcenter>

**Service Trust Portal**Is a portal that provides access to various compliance tools Microsoft provides for you to track compliance in your applications running on Microsoft’s various platforms.  
<https://aka.ms/STP>  
The STP is a launching point for Compliance Manager, which is a tool for managing your regulatory compliance in the cloud. Compliance Manager makes it easy to visualize your compliance with industry standards. It also provides details on how you can improve compliance, and for those areas where compliance is Microsoft’s responsibility, it provides full details on how Microsoft maintains compliance. **Azure sovereign regions**Some US government compliance scenarios require that data stays within the United States of America and that only citizens of the United States have any access to systems used to store that data. You can’t meet this requirement with policies. In fact, you can’t meet that requirement at all in the public cloud **to address this type of issue, Microsoft developed completely isolated Azure data centers that make up the Azure Government cloud.**

Azure Government data centers are separate from public data centers. All employees working in Azure Government are screened and are citizens of the US. Even Microsoft employees who provide technical support to Azure Government customers are required to be US citizens.

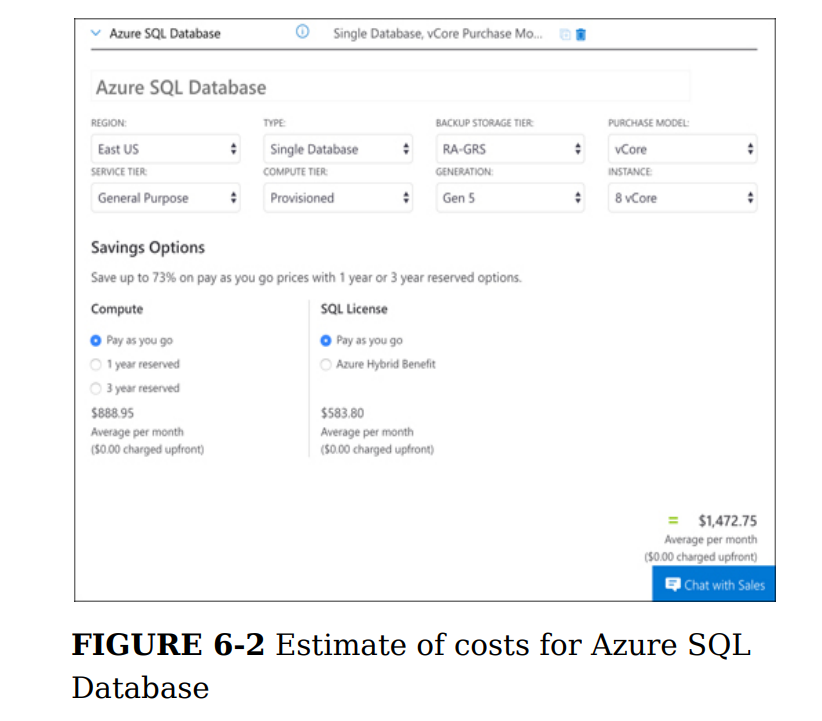
**Chapter 6 DESCRIBE AZURE PRICING, SLAS, AND LIFECYCLES**

**SKILL 6.1: DESCRIBE METHODS FOR PLANNING AND MANAGEMENT OF COSTS**

**Factors affecting costs**Choosing the least-expensive region for each of your Azure resources usually isn’t a good way to control costs. You might end up having to pay for network traffic across regions, and that could increase your costs above the amount you’re saving. ***Many Azure resources do not charge for network traffic within the same region, but they will charge for traffic across regions.***

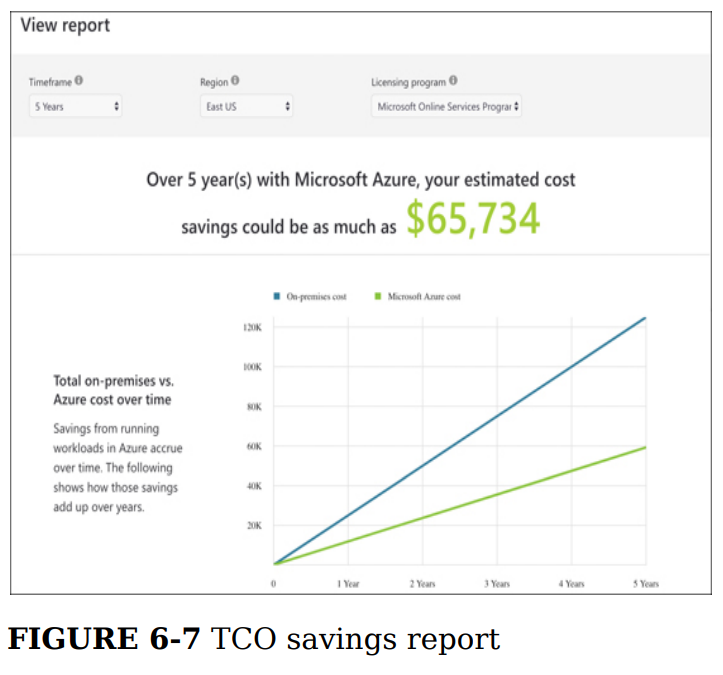
**It’s also important to keep in mind that you’re not charged for network traffic into an Azure datacenter**, **but you are charged for network traffic out of a datacenter**. However, your first 5GB of outbound data is free. After that point, you are charged a set amount on a tiered model.

**Pricing calculator**After you add the products you want to use, scroll down to configure the specific details of each service. These details vary based upon how Microsoft charges for the product. Figure 6-2 shows the options for Azure SQL Database.



**Total cost of ownership calculator**The pricing calculator is helpful for estimating your expenses for new applications in Azure, but **if you have on-premises applications you want to migrate to Azure and you want an estimate of how much you can save in Azure, the TCO calculator is a better choice.**

When using the **TCO** calculator, the first step is to add details about your on-premises servers, databases, storage, and network usage. In Figure 6-4, an on-premises server has been configured for a web app. You can configure all the details about the server, including the OS, whether it’s a VM or a physical server, and more.

****

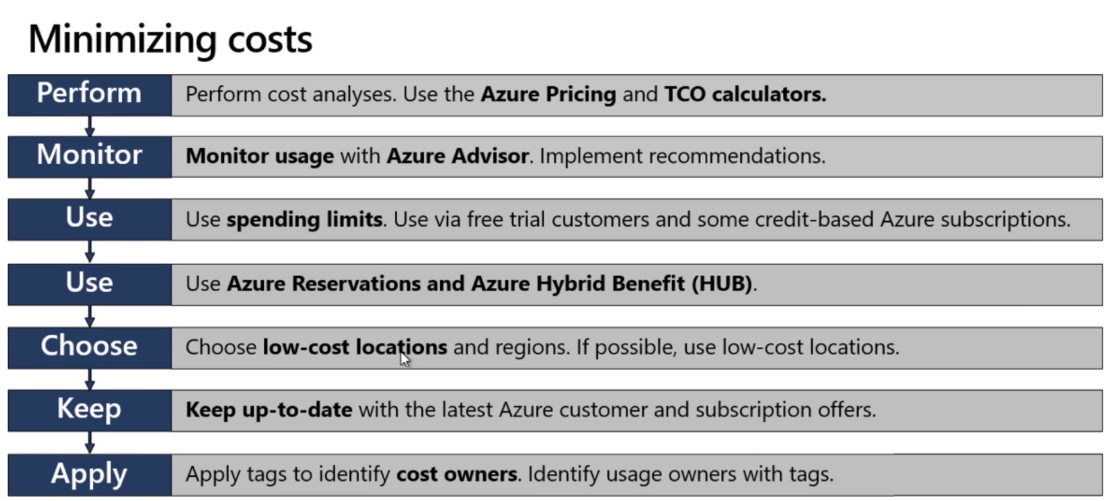
**Azure Cost Management**Is a tool in Azure that makes it easy to analyze your costs at a granular level. Cost Management **allows you to create a budget for your Azure expenses, set configurable alerts so you’ll know if you are approaching a budgeted limit, and analyze your costs in detail**

To effectively monitor your costs, you should create a budget in Cost Management. Creating a budget isn’t required, but it will allow you to visualize your spending compared to your planned expenses.

**Factors Affecting Costs  
  
Resource type -** Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource depend on the resource type.

**Services -** Azure usage rates and billing periods can differ between **Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers**. Some subscription types also include usage allowances, which affect costs.  
 **Location -** Azure has datacenters all over the world. Usage costs vary between locations that offer particular Azure products, services, and resources based on popularity, demand, and local infrastructure costs.  
 **Bandwidth -** Refers to data moving in and out of Azure data centers, as well as data moving between Azure data centers; other transfers are explicitly covered by the Content Delivery Network, ExpressRoute pricing, or Peering.

**Reserved Instances -** Save money when you reserve resources in advance. Plus, enjoy monthly payment options at no extra cost.  
Azure Reservations help you save money by committing to one-year or three-years plans for many Azure resources. Before you enter a commitment to buy a reservation, be sure to review the following sections to prepare for your purchase. **Azure Hybrid Benefit   
*Is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure. And now, this benefit applies to RedHat and SUSE Linux subscriptions, too****.*

  
 **SKILL 6.2: DESCRIBE AZURE SERVICE LEVEL AGREEMENTS (SLAS) AND SERVICE LIFECYCLES**

Many of the services you use today include a **service level agreement (SLA) that serves as a contract between you and the service provider for a certain level of service.** Microsoft provides SLAs in Azure, and they also provide comprehensive documentation on how the SLA is computed for a service. **However, not all services come with an SLA.**   
**Microsoft will often make services available in preview prior to releasing them for production use. These preview services often don’t come with an SLA.**

**Azure service level agreement (SLA)  
An important concept in cloud service SLAs is that the cloud provider considers an application to be outside of SLA only when the availability percentage is not met because of an issue that the cloud provider can control.** In other words, if you deploy new code to your application, and it causes your application to crash, the cloud provider is not going to consider that a breach of SLA.

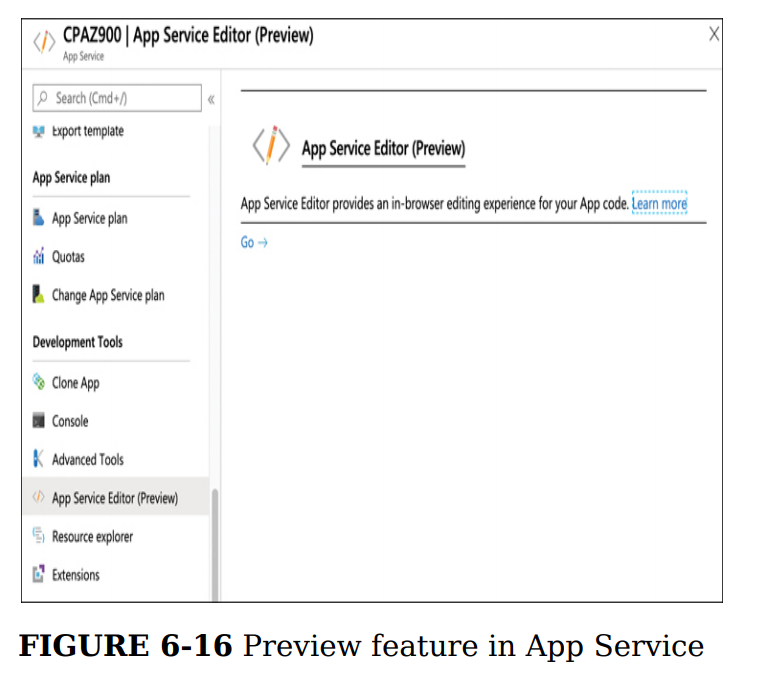
**Interpret the terms of an SLA**Microsoft provides details on the SLA for every Azure service at https://bit.ly/az900-azuresla.

**The SLA for App Service is 99.95 percent, and the SLA for a single VM running Premium storage is 99.9 percent. Therefore, your overall SLA for your application is 99.95 percent x 99.9 percent, or 99.85 percent. By deploying two VMs into two availability zones in the same region, you can obtain a 99.99 percent SLA for your VMs, and that increases your overall SLA to 99.94 percent.**

**Service lifecycle in Azure**As Azure product teams develop new services and features, it’s important for them to get feedback from customers using those services and features in a real-world environment. For that reason, **Microsoft will often offer new services and features to customers as preview offerings.** While the Microsoft official term is preview, you will often see people refer to these services and features as being a beta offering. **Once a feature has reached a certain level of completeness and reliability, it moves to a stage called general availability**. *This is the point where a service is fully supported and has an SLA associated with it.*

**Services and features that are in preview do not offer an SLA, and they are not meant to be used in production applications.** Preview features are also usually **not offered in all Azure regions.** Microsoft will provide documentation on which regions are available for a specific preview.

**Features and services that are in public preview are provided at a discounted rate**, but like private preview features and services, they typically don’t offer an SLA and are provided asis.

******

**General availability**Once a preview service or feature reaches a quality and availability bar suitable to the engineering team, they will declare general availability or GA. At this point, the service or feature is fully supported. **Once a service or feature reaches GA, it falls under the SLA Microsoft provides.** If it’s a new service, a new SLA will be published on the SLA web page. For new features of existing services, once GA is reached, the feature will inherit the SLA of the service it’s a feature of.

**When a service or feature reaches GA, it may not be GA in all Azure geographies.** In those cases, other geographies will usually GA later in the lifecycle of the service or feature. Preview pricing might also remain in effect for some period after GA. Details like this are published on the official GA announcement on the Azure website.  
  
**Azure Preview Program**User can test beta and other pre-release features, products, services, software, and regions to provide feedback.  
**Public Preview:** All Azure customers can evalute the new features  
**Generally available (GA):** After public preview is completed, all customers can use the features, and region availability will vary.

**Content Delivery Network**Secure and reliable global content delivery and acceleration  
A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs' store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

**Batch**Cloud-scale job scheduling and compute management

**Azure Information Protection**  
Azure Information Protection (AIP) is a cloud-based solution that enables organizations to discover, classify, and protect documents and emails by applying labels to content.

**Compare support plans  
<https://azure.microsoft.com/en-us/support/plans/>**

**Azure Queue Storage**Is a service for storing large numbers of messages. You access messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue message can be up to 64 KB in size. A queue may contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously.