**Chapter 1**

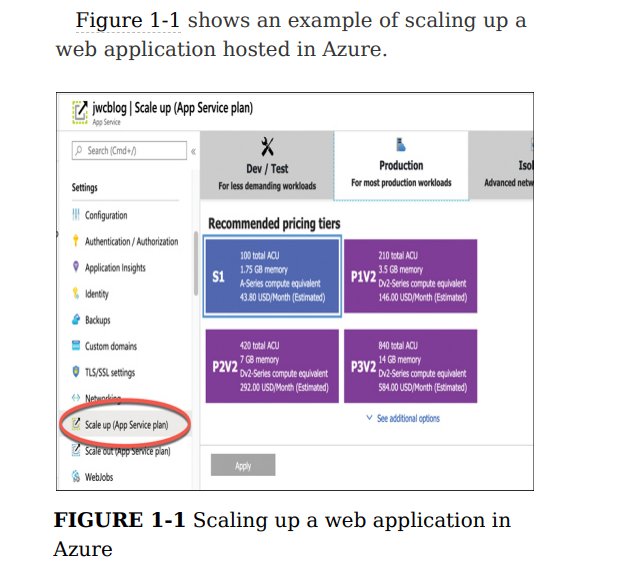
**DESCRIBE CLOUD CONCEPTS**  
This chapter covers the benefits of using the cloud, the different cloud services that are available, and cloud models that enable a variety of cloud configurations.

* High availability
* Scalability
* Elasticity
* Agility Fault tolerance and disaster recovery
* Economic benefits of the cloud

Cloud providers offer a service-level agreement **(SLA)** that guarantees a certain level of availability as a percentage. An SLA will usually guarantee an uptime of close to 100 percent, **but it only covers systems that are controlled by the cloud provider**

**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**  
Allow you to easily deal with these kinds of scenarios. 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) and vertical scaling (often referred to as scaling up). When you scale out, you add additional VMs for your application. Each VM you add is identical to other VMs servicing your application. Scaling out provides additional resources to handle additional load.

When you scale up, you move to a new VM with additional resources. 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.**

**This kind of speed and flexibility in the cloud is often called cloud agility.**If you determine that you need two more VMs for your application, you can scale out to three VMs in seconds. Azure takes care of allocating the resources for you. All you have to do is tell Azure how many VMs you want and you’re up and running  
  
**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

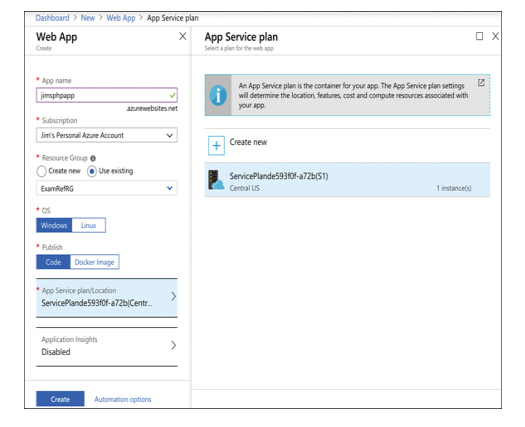
**SKILL 1.2: DESCRIBE THE DIFFERENCES BETWEEN INFRASTRUCTURE-AS-ASERVICE (IAAS), PLATFORMAS-A-SERVICE (PAAS), AND SOFTWARE-AS-A-SERVICE (SAAS)**

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.

* Azure CDN
* Azure Cosmos DB
* Azure SQL Database
* Azure Database for MySQL
* Azure Storage
* Azure Synapse Analytics

Your application code works without you having to do any kind of complex configuration. In fact, this is one of the main benefits of using a PaaS service; you can often move your application from on-premises to a cloud environment by simply deploying it to the cloud. This concept is often referred to as lift-and-shift  
  
A PaaS service also benefits from all of the other enhancements offered by the cloud; you get fault tolerance, elasticity, easy and quick scaling, backup and disaster recovery features, and more

SAAS  
SaaS service is software provided by a cloud provider that’s installed on infrastructure completely controlled by the hosting provider.

* 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**

This section covers:

* Azure regions
* Availability zones
* Resource groups
* Azure subscriptions
* Management groups
* Azure Resource Manager (ARM)

**Azure regions**   
As an example, 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? Each 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, and it’s likely this concept will be included on the exam. We’ll cover more about this later in this chapter.

*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.*

For example, if the South Central US region is hit by a devastating tornado (not out of the question in Texas), data that is also replicated to the North Central US region in Illinois is still safe and available. 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.

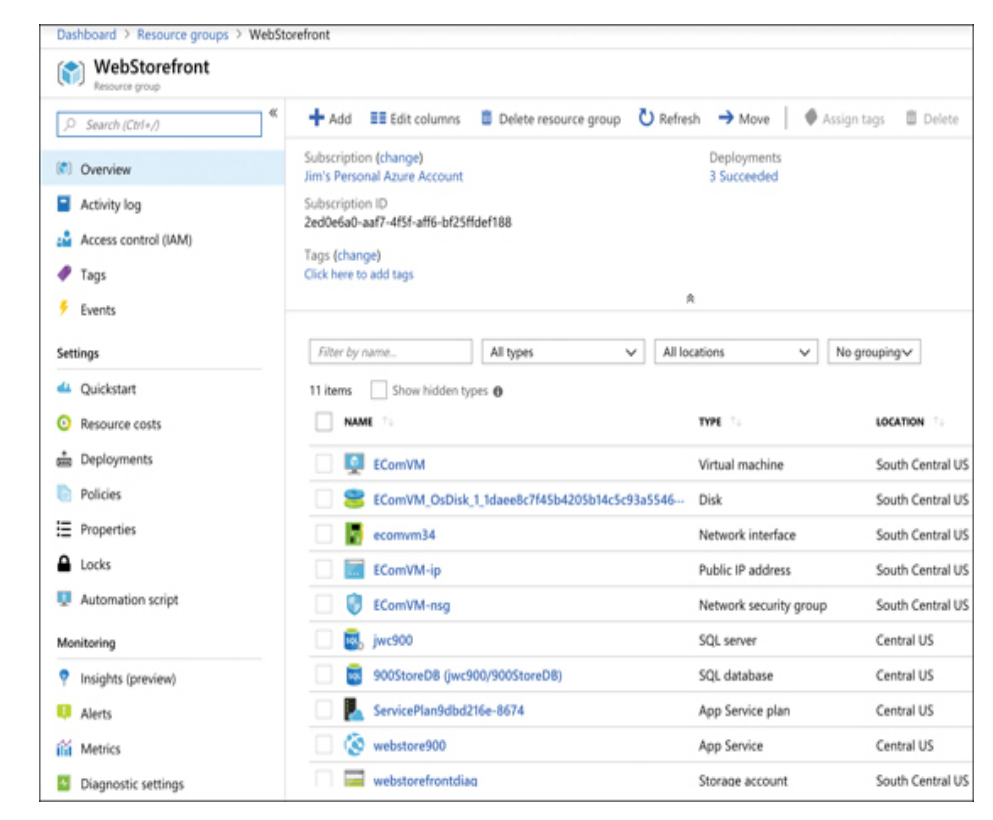
* Windows virtual machines
* Linux virtual machines
* Virtual Machine Scale Sets
* Azure Kubernetes Service
* Managed disks
* Zone-redundant storage
* Standard Load Balancer
* Standard IP address
* VPN Gateway
* ExpressRoute Gateway
* Application Gateway V2
* Azure Firewall
* Azure Data Explorer
* Azure SQL Database
* Azure Cache for Redis
* Azure Cosmos DB
* Event Hubs Service Bus (Premium tier)
* Event Grid
* Azure AD Domain Services
* App Service Environments ILB

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. An 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.

There are two categories of services that support availability zones:   
zonal services and zone redundant services.   
Zonal services are services such as virtual machines, managed disks used in a virtual machine, and public IP addresses used in virtual machines. In order to achieve high availability, you must explicitly deploy zonal services into two or more zones.   
  
Note Managed Disks and Public IP Addresses When you create a virtual machine in Azure and you deploy it to an availability zone, Azure will automatically deploy the managed disk(s) and public IP address (if one is configured) to the same availability zone.   
  
Zone redundant services are services such as zone redundant storage and SQL Databases. To use availability zones with these services, you specify the option to make them zone redundant when you create them. (For storage, the feature is called ZRS or zone redundant storage. For SQL Database, there is an option to make the database zone redundant.) Azure takes care of the rest for you by replicating data automatically to multiple availability zones.

**Resource group.**

Notice in Figure 2-3 that you see resources in several different Azure regions (Regions are in the Location column). 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. Only one free trial subscription is available per account, and you cannot create a new free trial if a previous one has expired.

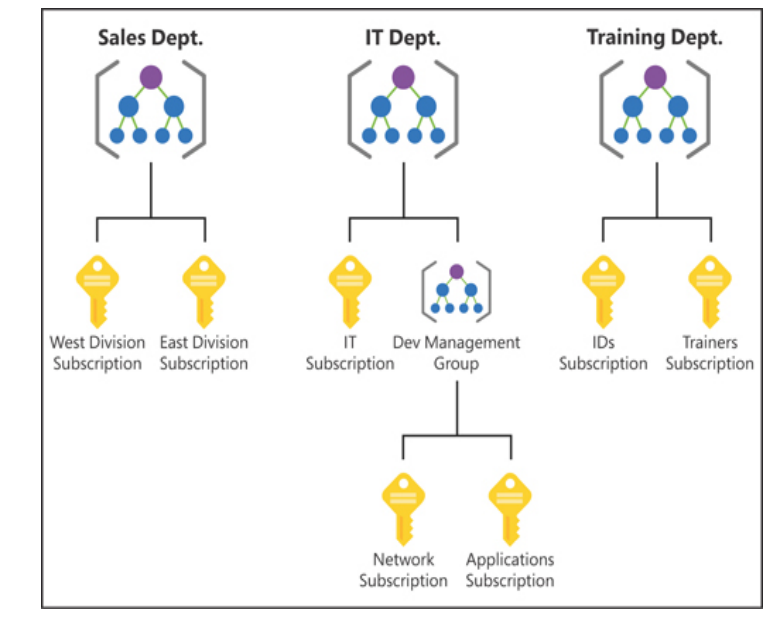
**Pay-As-You-Go** You pay only for those resources you use in Azure. There’s no up-front cost, and you can cancel the subscription at any time.

**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**

Management groups are 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.

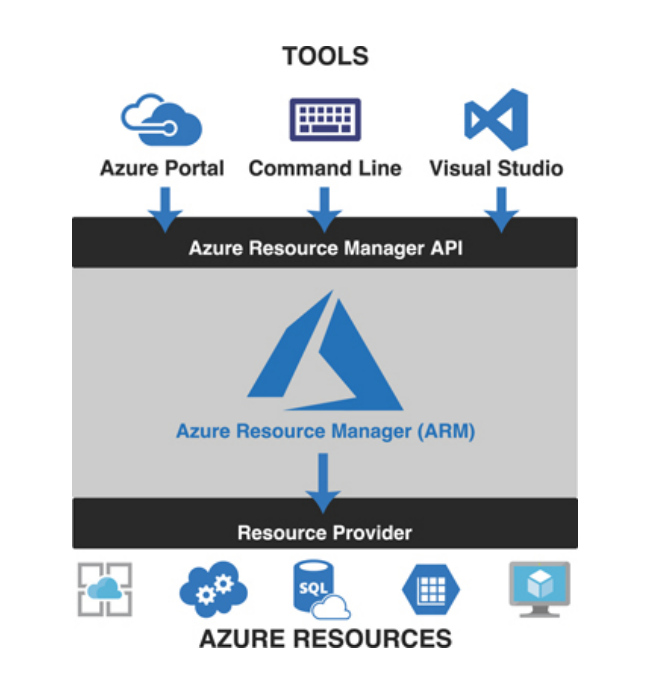


By organizing the subscriptions using management groups, you can have more precise control over who has access to which resources. You can also control the configuration of resources created within those subscriptions.

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.

For example, think of a situation where you’re deploying a certificate to be used with a web app. One of the properties you need to set on the web app is the certificate that you want to use, but if that certificate hasn’t been deployed yet, your deployment will fail. 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**

This section covers:

* Azure virtual machines
* Azure App Service
* Azure Container Instances (ACI)
* Azure Kubernetes Service (AKS)
* Windows Virtual Desktop
* Virtual networks
* ExpressRoute
* Container (Blob) Storage
* Disk Storage
* Azure Files Storage tiers
* Cosmos DB
* Azure SQL Database
* Azure Database for MySQL
* Azure Database for PostgreSQL
* The Azure Marketplace and its usage scenarios

**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.*

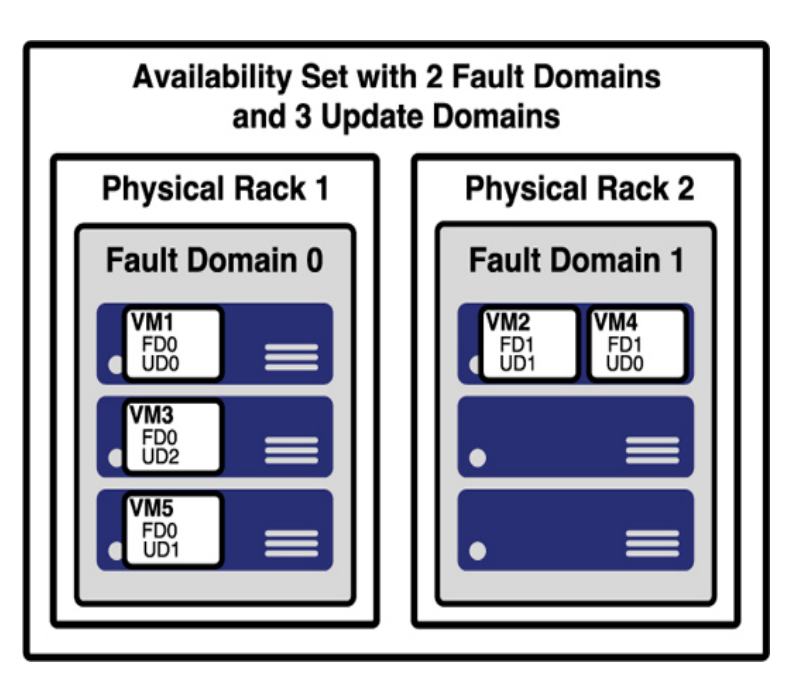
**Planned maintenance** includes things like operating system updates, driver updates, and so on.

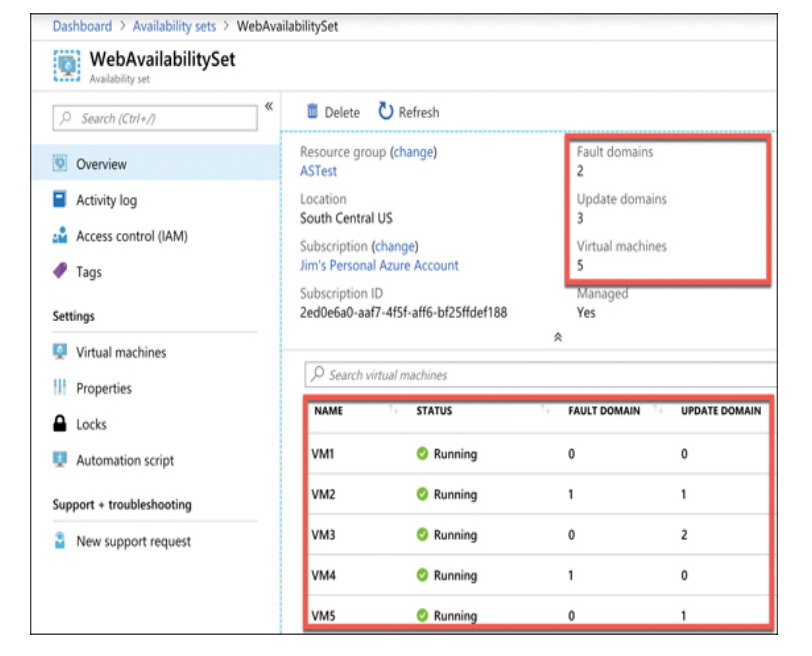
Azure has underlying systems that constantly monitor the health of computer components. If one of these underlying systems detects that a component within the host computer might fail soon, Azure will flag the computer for unplanned maintenance.   
In an **unplanned maintenance** event, Azure will attempt 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** are 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** are 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.*

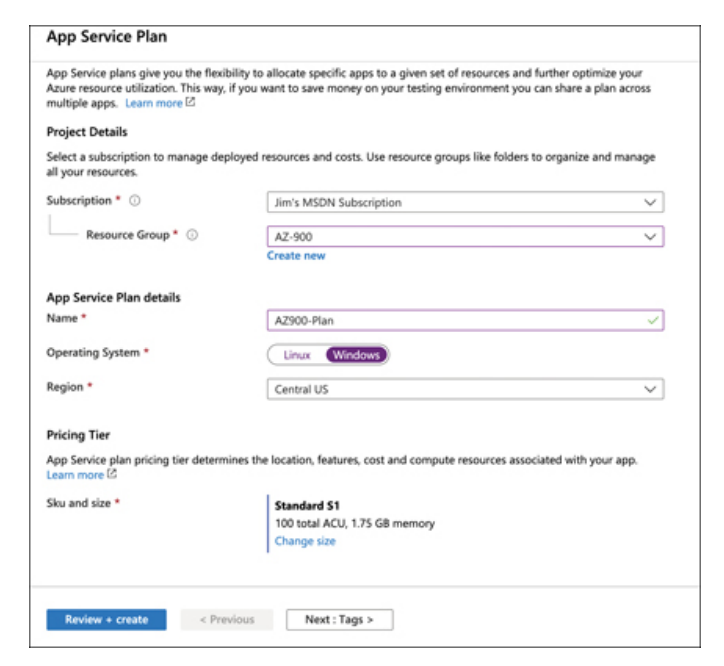
**Scale set:** When you create a scale set, you tell Azure what operating system you want to run and then you tell Azure how many VMs you want in your scale set. You have many other options such as creating a load balancer or gateway and so forth. Azure will create as many VMs as you specify (up to 1,000)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

*VMs in a scale set are also compatible with availability zones, so you are protected from problems in an Azure datacenter.*

*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*

**Azure App Service**Azure App Service is a PaaS offering in Azure for hosting websites.  
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.*



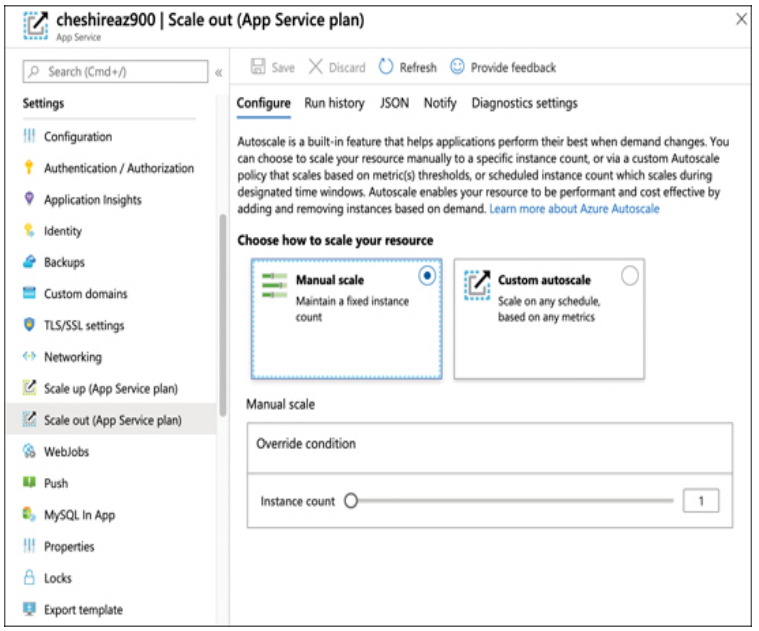
* **Free** A no-cost tier for testing only that runs on VMs shared with other App Service customers.
* **Shared** A low-cost tier for testing only with some additional features not offered in the Free tier. Runs on VMs shared with other App Service customers.
* **Basic, Standard, Premium, and PremiumV2**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

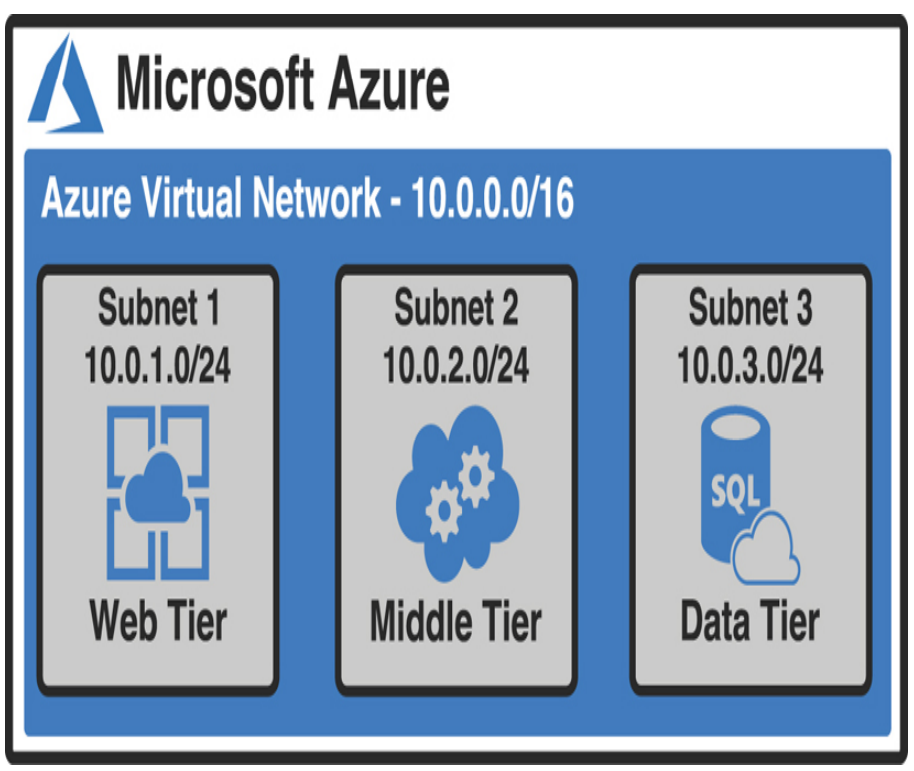
Once you’ve set up the tenant, you can add users from your **Azure Active Directory** so that they can access the OSes and apps in your tenant and assign permissions to them. Those users can then access WVD using the following methods.

* 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 -** Azure virtual network (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.



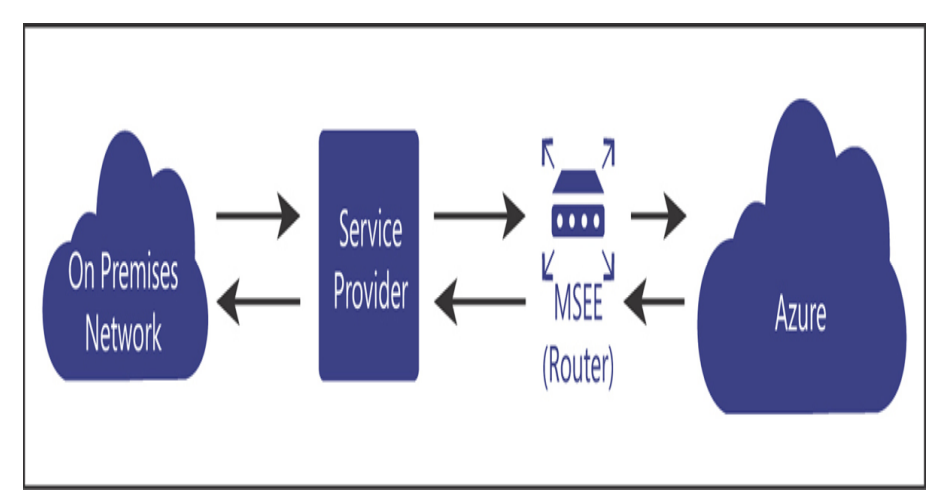
The IP addresses within the VNet at this point are all private IP addresses. They allow resources within the VNet to talk to each other, but you can’t use a private IP address on the Internet. You need a public IP address in order to give the Internet access to your web tier.

**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.