AZ – 900

Microsoft Azure Fundamental

**Learning Objectives**

After completing this module, you will be able to:

* Describe and understand cloud services and their benefits.
* Understand key terms you will encounter when working with cloud services.
* Understand public, private, and hybrid cloud models.
* Understand infrastructure as a service (IaaS).
* Understand platform as a service (PaaS).
* Understand software as a service (SaaS).

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/c2df5c21-cfce-e32d-b792-25e628f1045f/cb86f40d-12fd-f373-7591-27c20d7962e7/?child=first>

# ****Key concepts and terms****

**What is cloud computing?**

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the internet (the cloud), enabling faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change.

Cloud services is a big shift from the traditional way businesses think about IT resources. Cloud services have particular characteristics and considerations, some of which are outlined and explained below:

* **High availability**. The ability to keep services up and running for long periods of time, with very little downtime, depending on the service in question.
* **Scalability**. The ability to increase or decrease resources for any given workload. You can add additional resources to service a workload (known as scaling out), or add additional capabilities to manage an increase in demand to the existing resource (known as scaling up). Scalability doesn't have to be done automatically
* **Elasticity**. The ability to automatically or dynamically increase or decrease resources as needed. Elastic resources match the current needs, and resources are added or removed automatically to meet future needs when it’s needed, and from the most advantageous geographic location. A distinction between scalability and elasticity is that elasticity is done automatically
* **Agility**. The ability to react quickly. Cloud services can allocate and deallocate resources quickly. They are provided on-demand via self-service, so vast amounts of computing resources can be provisioned in minutes. There is no manual intervention in provisioning or deprovisioning services.
* **Fault tolerance**. The ability to remain up and running even in the event of a component or service no longer functioning. Typically, redundancy is built into cloud services architecture so if one component fails, a backup component takes its place. The type of service is said to be tolerant of faults.
* **Disaster recovery**. The ability to recover from an event which has taken down a cloud service. Cloud services disaster recovery can happen very quickly with automation and services being readily available to use.
* **Global reach**. The ability reach audiences around the globe. Cloud services can have presence in various regions across the globe which you can access, giving you a presence in those regions even though you may not have any infrastructure in that region.
* **Customer latency capabilities**. If customers are experiencing slowness with a particular cloud service, they are said to be experiencing some latency. Even though modern fiber optics are fast, it can still take time for services to react to customer actions if the service is not local to the customer. Cloud services have the ability deploy resources in datacenters around the globe, thus addressing customer latency issues.
* **Predictive cost considerations**. The ability for users to predict what costs they will incur for a particular cloud service. Costs for individual services are made available, and tools are provided to allow you predict what costs a service will incur. You can also perform analysis based on future growth.
* **Technical skill requirements and considerations**. Cloud services can provide and manage hardware and software for workloads. Therefore, getting a workload up and running with cloud services demands less technical resources than having IT teams build and maintain physical infrastructure for handling the same workload. A user can be expert in the application they want to run without having to need skills to build and maintain the underlying hardware and software infrastructure.
* **Increased productivity**. On-site datacenters typically require a lot of hardware setup (otherwise known as racking and stacking), software patching, and other time-consuming IT management chores. Cloud computing eliminates the need for many of these tasks, so IT teams can spend time on achieving more important business goals.
* **Security**. Cloud providers offer a broad set of policies, technologies, controls, and expert technology skills that can provide better security than most organizations can otherwise achieve. The result is strengthened security, which helps to protect data, apps, and infrastructure from potential threats.

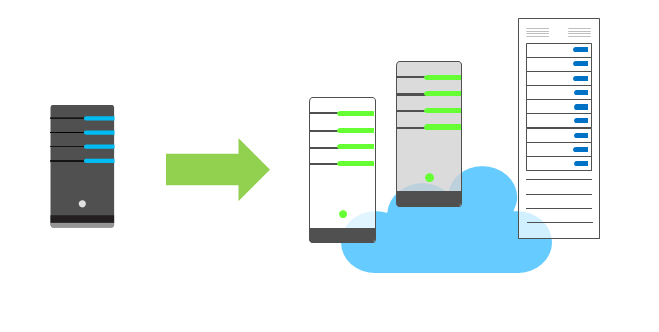
**Note**: You can read more conceptual detail about cloud computing on the page [What is cloud computing?](https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/) and there is also a term reference guide available on the page [Cloud computing Terms](https://azure.microsoft.com/en-us/overview/cloud-computing-dictionary/), which may be of some use.

# ****Economies of scale****

The concept of economies of scale is the ability to do things more cheaply and more efficiently when operating at a larger scale in comparison to operating at a smaller scale.

Cloud providers such as Microsoft, Google, and AWS are very large businesses, and are able to leverage the benefits of economies of scale, and then pass those benefits on to their customers.

This is apparent to end users in a number of ways, one of which is the ability to acquire hardware at a lower cost than if a single user or smaller business were purchasing it.



Storage costs, for example, have decreased significantly over the last decade due in part to cloud providers' ability to purchase larger amounts of storage at significant discounts. They are then able to use that storage more efficiently, and pass on those benefits to end users in the form of lower prices.

There are limits to the benefits large organizations can realize through economies of scale. A product will inevitably have an underlying core cost, as it becomes more of a commodity, based on what it costs to produce . Competition is also another factor which has an effect on costs of cloud services.

# ****Capital expenditure (CapEx) versus operational expenditure (OpEx)****

In previous years, startup companies needed to acquire a physical premises and infrastructure to start their business and begin trading. Large amounts of money were need to get a new business up and running, or to grow an existing company. They would have to buy new datacenters or new servers to allow them build out new services, which they could then deliver to their customers. That is no longer the case.

Today, organizations can sign up for a service from a cloud provider to get up and running. This enables them to begin selling or providing services to their customers more quickly, without the need for significant upfront costs.

These two approaches to investment are referred to as:

* **Capital Expenditure (CapEx)**: This is the spending of money on physical infrastructure up front, and then deducting that expense from your tax bill over time. CapEx is an upfront cost which has a value that reduces over time.
* **Operational Expenditure (OpEx)**: This is spending money on services or products now and being billed for them now. You can deduct this expense from your tax bill in the same year. There is no upfront cost, you pay for a service or product as you use it.

Companies wanting to start a new business or grow their business do not have to incur upfront costs to try out a new product or service for customers. Instead, they can get into a market immediately and pay as much or as little for the infrastructure as the business requires. They also can terminate that cost if and when they need to.

If your service is busy and you consume a lot of resources in a month, then you receive a large bill. If those services are minimal and don't use a lot of resources, then you will receive a smaller bill.

A business can still use the CapEx expenditure strategy if they wish, but it is no longer a requirement that they do so.

**Consumption-based model**

Cloud service providers operate on a *consumption-based model*, which means that end users only pay for the resources that they use. Whatever they use is what they pay for.

This consumption-based model brings with it many benefits, including:

* No upfront costs
* No need to purchase and manage costly infrastructure that they may or may not use to its fullest
* The ability to pay for additional resources if and when they are needed
* The ability to stop paying for resources that are no longer needed

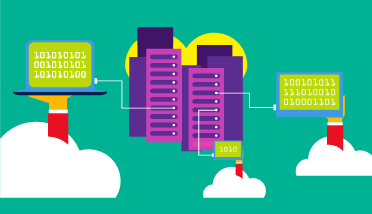
<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/c2df5c21-cfce-e32d-b792-25e628f1045f/41433040-5fa8-82a1-52fd-a11a6a05950c/?child=first>

**Public cloud**

A public cloud is owned by the cloud services provider (also known as a *hosting provider*). It provides resources and services to multiple organizations and users, who connect to the cloud service via a secure network connection, typically over the internet.

Public cloud models have the following characteristics:

* **Ownership**. This is the resources that an organization or end user uses. Examples include storage and processing power. Resources do not belong to the organization that is utilizing them, but rather they are owned and operated by a third party such as the cloud service provider.
* **Multiple End Users**. Public cloud modes may make their resources available to multiple organizations.
* **Public Access**. This provides access to the public.
* **Availability**. This is the most common cloud-type deployment model.
* **Connectivity**. Users and organizations are typically connected to the public cloud over the internet using a web browser.
* **Skills**. Public clouds do not require deep technical knowledge to set up and use its resources.



With a public cloud, there is no local hardware to manage or keep up to date; everything runs on the cloud provider’s hardware. In some cases, cloud users can save additional costs by sharing computing resources with other cloud users.

A common use case scenario is deploying a web application or a blog site on hardware and resources that are owned by a cloud provider. Using a public cloud in this scenario allows cloud users to get their website or blog up quickly, and then focus on maintaining the site without having to worry about purchasing, managing or maintaining the hardware on which it runs.

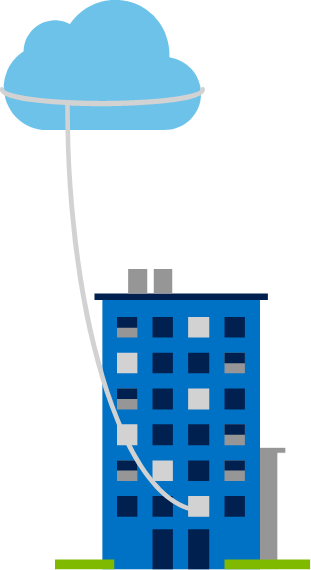
Businesses can use multiple public cloud service provider companies of varying scale. Microsoft Azure is an example of a public cloud provider.

**Private cloud**

A private cloud is owned and operated by the organization that uses the resources from that cloud. They create a cloud environment in their own datacenter, and provide self-service access to compute resources to users within their organization. The organization remains the owner, entirely responsible for the operation of the services they provide.

Private cloud models have the following characteristics:

* **Ownership**. The owner and user of the cloud services are the same.
* **Hardware**. The owner is entirely responsible for the purchase, maintenance, and management of the cloud hardware.
* **Users**. A private cloud operates only within one organization and cloud computing resources are used exclusively by a single business or organization.
* **Connectivity**. A connection to a private cloud is typically made over a private network that is highly secure.
* **Public access**. Does not provide access to the public.
* **Skills**. Requires deep technical knowledge to set up, manage, and maintain.



A use case scenario for a private cloud would be when an organization has data that cannot be put in the public cloud, perhaps for legal reasons. For example, they may have medical data that cannot be exposed publicly.

Another scenario may be where government policy requires specific data to be kept in-country or privately.

A private cloud can provide cloud functionality to external customers as well, or to specific internal departments such as Accounting or Human Resources.

**Hybrid cloud**

A hybrid cloud combines both public and private clouds, allowing you to run your applications in the most appropriate location.

Hybrid cloud models have the following characteristics:

* **Resource location**. Specific resources run or are used in a public cloud, and others run or are used in a private cloud.
* **Cost and efficiency**. Hybrid cloud models allow an organization to leverage some of the benefits of cost, efficiency, and scale that are available with a public cloud model.
* **Control**. Organizations retain management control in private clouds.
* **Skills**. Technical skills are still required to maintain the private cloud and ensure both cloud models can operate together.



An example of a hybrid cloud usage scenario would be hosting a website in the public cloud and linking it to a highly secure database hosted in a private cloud.

Hybrid cloud scenarios can be useful when organizations have some things that cannot be put in a public cloud, possibly for legal reasons. For example, you may have medical data that cannot be exposed publicly.

Another example is one or more applications that run on old hardware that can’t be updated. In this case, you can keep the old system running locally in your private cloud, and connect it to the public cloud for authorization or storage.

**Note**: You can read more about Microsoft Azure Hybrid cloud options from the page [The only consistent and comprehensive hybrid cloud](https://azure.microsoft.com/en-us/overview/hybrid-cloud/)

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/c2df5c21-cfce-e32d-b792-25e628f1045f/41433040-5fa8-82a1-52fd-a11a6a05950c/?child=first>

# ****Cloud model comparison****

Below is an outline of some of the advantages and disadvantages for public, private, and hybrid clouds.

### Public cloud

* **Advantages**:
  + **No CapEx**. You don’t have to buy a new server in order to scale.
  + **Agility**. Applications can be made accessible quickly, and deprovisioned whenever needed.
  + **Consumption-based model**. Organizations pay only for what they use, and operate under an OpEx model.
  + **Maintenance**. Organizations have no responsibility for hardware maintenance or updates.
  + **Skills**. No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.
* **Disadvantages**:
  + **Security**. There may be specific security requirements that cannot be met by using public cloud.
  + **Compliance**. There may be government policies, industry standards, or legal requirements which public clouds cannot meet.
  + **Ownership**. Organizations don't own the hardware or services and cannot manage them as they may wish.
  + **Specific scenarios**. If organizations have a unique business requirement, such as having to maintain a legacy application, it may be hard to meet that requirement with public cloud services.

### Private cloud

* **Advantages**:
  + **Control**. Organizations have complete control over the resources.
  + **Security**. Organizations have complete control over security.
  + **Compliance**. If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.
  + **Specific scenarios**. If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.
* **Disadvantages**:
  + **Upfront CapEx**. Hardware must be purchased for start-up and maintenance.
  + **Agility**. Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.
  + **Maintenance**. Organizations have the responsibility for hardware maintenance and updates.
  + **Skills**. Private clouds requires in-house IT skills and expertise that may be hard to get or be costly.

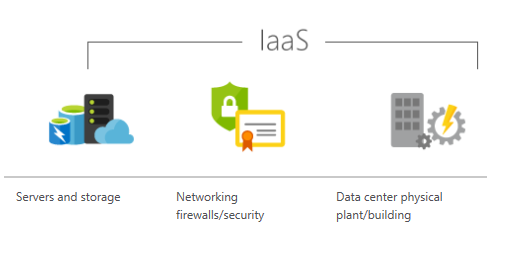
### Hybrid cloud

* **Advantages**:
  + **Flexibility**. The most flexible scenario; with a hybrid cloud setup, an organization can decide to run their applications either in a private cloud or in a public cloud.
  + **Costs**. Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.
  + **Control**. Organizations can still access resources over which they have total control.
  + **Security**. Organizations can still access resources for which they are responsible for security.
  + **Compliance**. Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.
  + **Specific scenarios**. Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications. In this case, they can keep the old system running locally, and connect it to the public cloud for authorization or storage. Additionally, they could host a website in the public cloud, and link it to a highly secure database hosted in their private cloud.
* **Disadvantages**:
  + **Upfront CapEx**. Upfront CapEx is still required before organizations can leverage a private cloud.
  + **Costs**. Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.
  + **Skills**. Deep technical skills are still required to be able to set up a private cloud.
  + **Ease of management**. Organizations need to ensure there are clear guidelines to avoid confusion, complications or misuse.

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/c2df5c21-cfce-e32d-b792-25e628f1045f/c52f4a1e-ab4a-7199-f386-73b95ee29ad0/?child=first>

# ****Infrastructure as a service (IaaS)****

IaaS is the most basic category of cloud computing services. With IaaS, you rent IT infrastructure servers and virtual machines (VMs), storage, networks, and operating systems from a cloud provider on a pay-as-you-go basis. It's an instant computing infrastructure, provisioned and managed over the internet.



IaaS has the following characteristics:

* **Upfront costs**. IaaS has no upfront costs. Users pay only for what they consume.
* **User ownership**. The user is responsible for the purchase, installation, configuration, and management of their own software operating systems, middleware, and applications.
* **Cloud provider ownership**. The cloud provider is responsible for ensuring that the underlying cloud infrastructure (such as virtual machines, storage and networking) is available for the user.

**Note**: When using IaaS, ensuring that a service is up and running is a shared responsibility: the cloud provider is responsible for ensuring the cloud infrastructure is functioning correctly; the cloud customer is responsible for ensuring the service they are using is configured correctly, is up to date, and is available to their customers. This is referred to as the **shared responsibility model**.

#### Common usage scenarios:

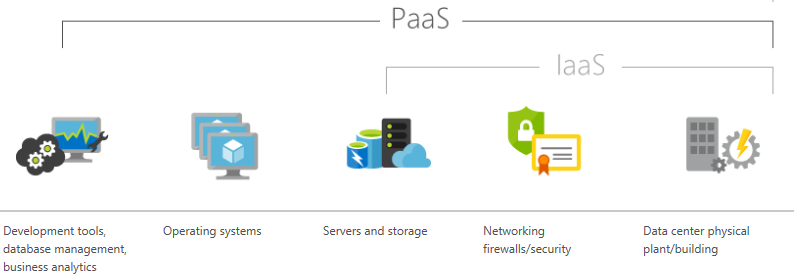
* **Migrating workloads**. Typically, IaaS facilities are managed in a similar way as on-premises infrastructure, and provide an easy migration path for moving existing applications to the cloud.
* **Test and development**. Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS makes scaling development testing environments up and down fast and economical.
* **Website hosting**. Running websites using IaaS can be less expensive than traditional web hosting.
* **Storage, backup, and recovery**. Organizations avoid the capital outlay and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for managing unpredictable demand and steadily growing storage needs. It can also simplify the planning and management of backup and recovery systems.

**Note**: For more information on IaaS see the page [What is IaaS?](https://azure.microsoft.com/en-us/overview/what-is-iaas/)

# ****Platform as a Service (PaaS)****

PaaS provides an environment for building, testing, and deploying software applications. The goal of PaaS is to help create an application as quickly as possible without having to worry about managing the underlying infrastructure. For example, when deploying a web application using PaaS, you don't have to install an operating system, web server, or even system updates. PaaS is a complete development and deployment environment in the cloud, with resources that enable organizations to deliver everything from simple cloud-based apps to sophisticated cloud-enabled enterprise applications.

Resources are purchased from a cloud service provider on a pay-as-you-go basis and accessed over a secure Internet connection.



PaaS has the following characteristics:

* **Upfront costs**. There are no upfront costs, and users pay only for what they consume.
* **User ownership**. The user is responsible for the development of their own applications. However, they are not responsible for managing the server or infrastructure. This allows the user to focus on the application or workload they want to run.
* **Cloud provider ownership**. The cloud provider is responsible for operating system management, and network and service configuration. Cloud providers are typically responsible for everything apart from the application that a user wants to run. They provide a complete managed platform on which to run an application.

#### Common usage scenarios:

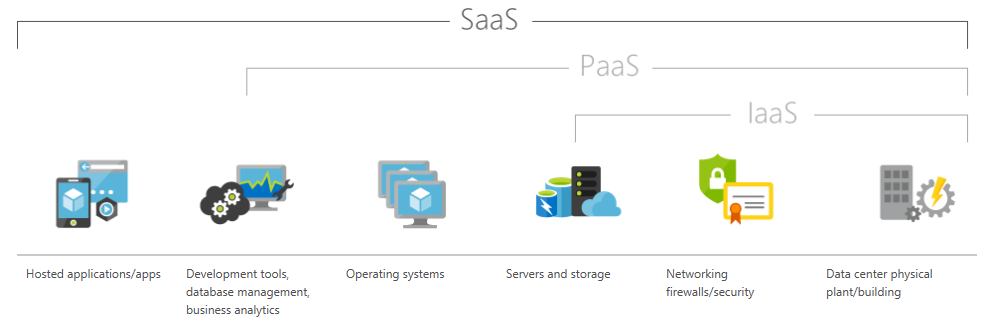
* **Development framework**. PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create a Microsoft Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
* **Analytics or business intelligence**. Tools provided as a service with PaaS allow organizations to analyze and mine their data. They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

**Note**: For more information on PaaS see the page [What is PaaS?](https://azure.microsoft.com/en-us/overview/what-is-paas/)

# ****Software as a Service (SaaS)****

SaaS is software that is centrally hosted and managed for the end customer. It allows users to connect to and use cloud-based apps over the internet. Common examples are email, calendars, and office tools such as Microsoft Office 365.

SaaS is typically licensed through a monthly or annual subscription, and Office 365 is an example of SaaS software.



SaaS has the following characteristics:

* **Upfront costs**. Users have no upfront costs; they pay a subscription, typically on a monthly or annual basis.
* **User ownership**. Users just use the application software; they are not responsible for any maintenance or management of that software.
* **Cloud provider ownership**. The cloud provider is responsible for the provision, management, and maintenance of the application software.

#### Common usage scenarios:

* Examples of Microsoft SaaS services include Office 365, Skype, and Microsoft Dynamics CRM Online.

**Note**: For more information on SaaS see the page [What is SaaS?](https://azure.microsoft.com/en-us/overview/what-is-saas/)

# ****Cloud service comparison****

There are both advantages and disadvantages for IaaS, PaaS, and SaaS cloud services.

### IaaS

Infrastructure as a Service is the most flexible category of cloud services. It aims to give you complete control over the hardware that runs your application. Instead of buying hardware, with IaaS, you rent it.

* **Advantages**:
  + **No CapEx**. Users have no upfront costs.
  + **Agility**. Applications can be made accessible quickly, and deprovisioned whenever needed.
  + **Consumption-based model**. Organizations pay only for what they use, and operate under an OpEx model.
  + **Skills**. No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.
  + **Cloud benefits**. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are made secure and highly available.
  + **Flexibility**: IaaS is the most flexible cloud service as you have control to configure and manage the hardware running your application.
* **Disadvantages**:
  + **Management**. The shared responsibility model applies; the user manages and maintains the services they have provisioned, and the cloud provider manages and maintains the cloud infrastructure.

### PaaS

PaaS provides the same benefits and considerations as IaaS, but there some additional benefits.

* **Advantages**:
  + **No CapEx**. Users have no upfront costs.
  + **Agility**. PaaS is more agile than IaaS, and users do not need to configure servers for running applications.
  + **Consumption-based model**. Users pay only for what they use, and operate on an OpEx model.
  + **Skills**. No deep technical skills are required to deploy, use, and gain the benefits of PaaS.
  + **Cloud benefits**. Users can leverage the skills and expertise of the cloud provider to ensure their workloads are made secure and highly available. In addition, users can gain access to more cutting-edge development tools and toolsets. They then can apply these tools and toolsets across an application's lifecycle.
  + **Productivity**. Users can focus on application development only, as all platform management is handled by the cloud provider. Working with distributed teams as services is easier, as the platform is accessed over the internet and can be made globally available more easily.
* **Disadvantages**:
  + **Platform limitations**. There may be some limitations to a particular cloud platform that could affect how an application runs. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a particular workload.

### SaaS

SaaS is software that is centrally hosted and managed for the end customer. It is usually based on an architecture where one version of the application is used for all customers, and licensed through a monthly or annual subscription

SaaS provides the same benefits as IaaS, but again there some additional benefits.

* **Advantages**:
  + **No CapEx**. Users don’t have any upfront costs.
  + **Agility**. Users can provide staff with access to the latest software quickly and easily.
  + **Pay-as-you-go pricing model**: Users pay for the software they use on a subscription model, typically monthly or yearly, regardless of how much they use the software.
  + **Flexibililty**. Users can access the same application data from anywhere.
* **Disadvantages**
  + **Software limitations**. There may be some limitations to a particular software application that might affect how users work. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a particular workload.

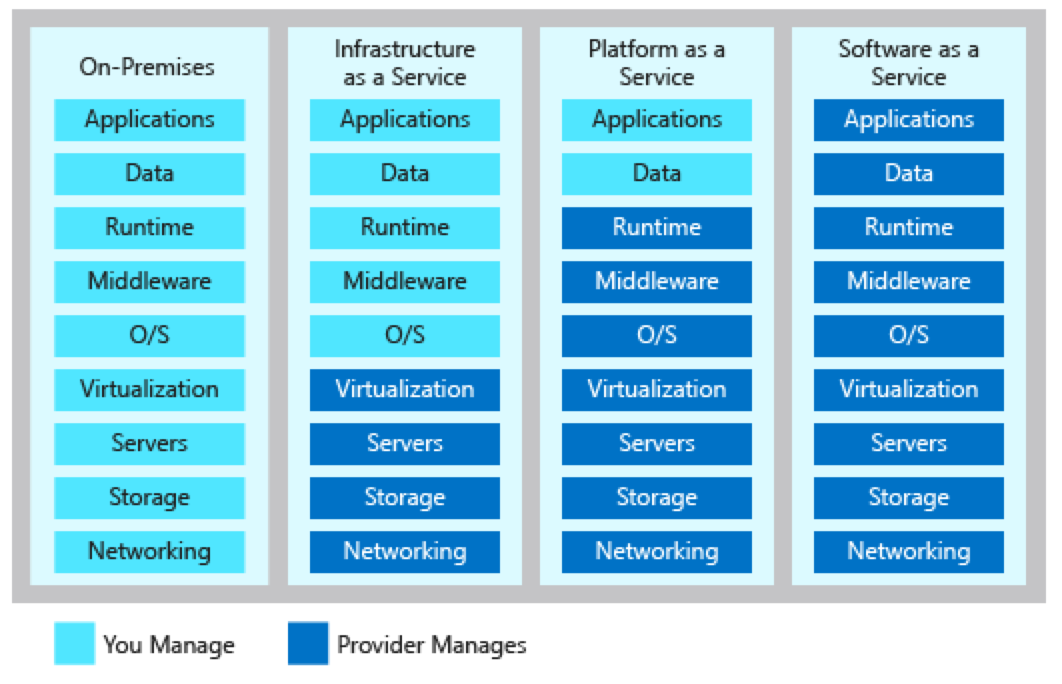
### Summary

IaaS, PaaS, and SaaS each contain different levels of managed services. You may easily use a combination of these types of infrastructure. You could use Office 365 on your company’s computers (SaaS), and in Azure you could host your VMs (IaaS) and use Azure SQL Database (PaaS) to store your data. With the cloud’s flexibility, you can use any combination that provides you with the maximum result.

**Management responsibilities**

The following list of cloud service types describes the management responsibilities for the user and the cloud provider as compared to on-premises systems:

* IaaS requires the most user management of all the cloud services. The user is responsible for managing the operating systems, data, and applications.
* PaaS requires less user management. The cloud provider manages the operating systems, and the user is responsible for the applications and data they run and store.
* SaaS requires the least amount of management. The cloud provider is responsible for managing everything, and the end user just uses the software.



**Note**: It is important that users understand what they are responsible for, when using cloud services, to ensure their workloads are managed correctly and don't suffer any down time. There is a **shared responsibility model** for ensuring cloud workloads are run securely and in a well-managed way. Depending on the service you are using: the cloud provider is responsible for some aspects of the workload management, and the end user is responsible for other aspects of the workload management.

### **Review Question 1**

What terms from the list below would be viewed as benefits of using cloud services?

Elasticity

Un-predictable costs

Local reach only

Agility

Economies of scale

### **Review Question 2**

When looking at using a cloud service, what expenditure type are cloud services based on?

Capital Expenditure (CapEx)

Friendly expenditure

Maximum expense

Operational Expenditure (OpEx)

### **Review Question 3**

0.0/1.0 point (ungraded)

Which of the following terms relate to making a service available with no downtime for an extended period of time?  
                                                 

### **Review Question 4**

0.0/1.0 point (ungraded)

(choose two)

Which cloud models provide services that can be accessed by the public?

Public

Private

Hybrid

Global

### **Review Question 5**

0.0/1.0 point (ungraded)

Which cloud model provides the greatest degree of ownership and control?

Public

Private

Hybrid

### **Review Question 6**

0.0/1.0 point (ungraded)

Which cloud model provides the greatest degree of flexibility?

Public

Private

Hybrid

**Explanation**

Hybrid cloud model provides the greatest degree of flexibility, as you have the option to choose either public or private depending on your requirements.  
Public cloud means you will not have full ownership over all aspects of the service.  
Private cloud means there is upfront costs associated with creating, managing and maintaining your private cloud.

### **Review Question 7**

0.0/1.0 point (ungraded)

You are running a virtual machine in a public cloud using IaaS. Which model correctly reflects how that resource is managed?

user management model

cloud user management model

no responsibility management model

shared responsibility model

### **Review Question 8**

0.0/1.0 point (ungraded)

Which term best describes PaaS?

Users can create and deploy an application as quickly as possible without having to worry about managing the underlying infrastructure

Users are responsible for purchasing, installing, configuring, and managing their own software—operating systems, middleware, and applications

Users pay an annual or monthly subscription

### **Review Question 9**

0.0/1.0 point (ungraded)

You have two types of applications which you need to run: legacy applications that require specialized mainframe hardware and newer applications that can run on commodity hardware. Which cloud deployment model would be best for you?"

Public cloud

Private cloud

Hybrid cloud

On-Premises

**Explanation**

Hybrid cloud is the correct answer.  
A hybrid cloud is a public and private cloud combined. You can run your new applications on commodity hardware you rent from the public cloud and maintain your specialized mainframe hardware on-premises

# ****Module 1 summary****

In this module you've learned about cloud computing, what it is and what its key characteristics are. You learned about the different types of cloud models that are available and the considerations of using those different models. You also learned about the different cloud services available, the benefits of using the different types, and the management responsibilities under each service type.

### Why cloud services?

In this lesson you have learned about what cloud computing is, and why you should consider using cloud services. You've learned what some of the key terms and concepts are, such as high availability, agility, elasticity, fault tolerance, global reach, CapEx versus OpEX in the context of cloud computing, economies of scale, and the consumption-based cost model.

### Types of cloud models

In this lesson you have learned about public cloud, private cloud, and hybrid cloud models, and what the key characteristics of each model are. You've also learned how they compare, what considerations you need to take into account when using them, and when you might use them.

### Types of cloud services

In this lesson you have learned about the different types of cloud service available, IaaS, PaaS, and SaaS. You've learned what the key characteristics of each service are, how they compare, what considerations you need to take into account when using them, and when you might use them.

**Learning objectives**

After completing this module, you will be able to:

* Understand and describe core Azure architectural components.
* Understand and describe core Azure services and products.
* Understand and describe Azure solutions.
* Understand and describe Azure management tools.

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

# ****Regions****

Microsoft Azure is made up of datacenters located around the globe. These datacenters are organized and made available to end users by region.

A region is a geographical area on the planet containing at least one, but potentially multiple datacenters that are in close proximity and networked together with a low-latency network.

For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be deployed. A few examples of regions are West US, Canada Central, West Europe, Australia East, and Japan West.

Azure has more global regions than any other cloud provider. This provides customers the flexibility and scale needed to bring applications closer to users around the world, preserving data residency and offering comprehensive compliance and resiliency options for customer. At the time of writing this, Azure is generally available in 42 regions around the world, with plans announced for 12 additional regions.



**Note**: A list of regions and their locations is available on the page[Azure Regions](https://azure.microsoft.com/en-us/global-infrastructure/regions/)

### Special Azure regions

Azure also has some special regions that you might want to use when building out your applications for compliance or legal purposes. These special regions include:

* US DoD Central, US Gov Virginia, US Gov Iowa and more: These are physical and logical network-isolated instances of Azure for US government agencies and partners. They are operated by screened US persons. Includes additional compliance certifications.
* China East, China North and more: These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft does not directly maintain the datacenters.
* Germany Central and Germany Northeast: These regions are available through a data trustee model whereby customer data remains in Germany under control of T-Systems, a Deutsche Telekom company, acting as the German data trustee. Any user or enterprise who needs their data to reside in Germany can use this service.

### Region pairs

Each Azure region is paired with another region within the same geography (such as US, Europe, or Asia). This approach allows for the replication of resources (such as virtual machine storage) across a geography that helps reduce the likelihood of interruptions due to events such as natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once. Additional advantages of region pairs include:

* In the event of a wider Azure outage, one region out of every pair is prioritized to help reduce the time it takes to restore them for applications.
* Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
* Data continues to reside within the same geography as its pair (except for Brazil South) for tax and law enforcement jurisdiction purposes.

Examples of region pairs would be West US paired with East US, and SouthEast Asia paired with East Asia.

**Note**: A full list of region pairs is avalable [here](https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions#what-are-paired-regions).

### Feature availability

Finally, some services or virtual machine features are only available in certain regions, such as specific virtual machine sizes or storage types. There are also some global Azure services that do not require you to select a particular region, such as Microsoft Azure Active Directory, Microsoft Azure Traffic Manager, or Azure DNS.

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

# ****Geographies****

A geography is a discrete market typically containing two or more regions that preserves data residency and compliance boundaries.

Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries. Geographies are fault-tolerant to withstand complete region failure through their connection to dedicated high-capacity networking infrastructure.

Geographies are broken up into Americas, Europe, Asia Pacific, Middle East and Africa.

**Note**: See the page [Azure Grographies for more details](https://azure.microsoft.com/en-us/global-infrastructure/geographies/).

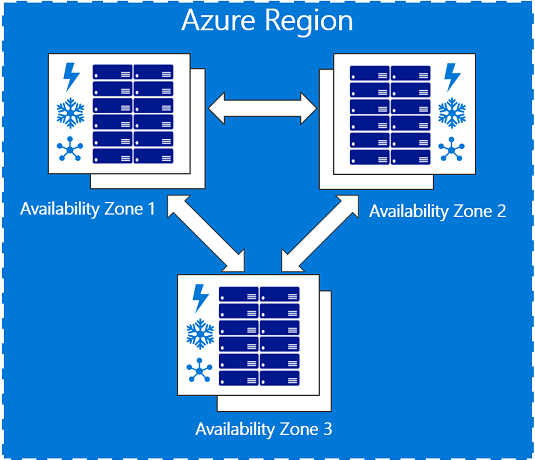
<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

# ****Availability Zones****

Availability zones are physically separate locations within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. It is set up to be an isolation boundary. If one availability zone goes down, the other continues working. The availability zones are typically connected to each other through very fast, private fiber-optic networks.

Availability zones allow customers to run mission-critical applications with high availability and low-latency replication.

Availability zones are offered as a service within Azure, and to ensure resiliency, there’s a minimum of three separate zones in all enabled regions.



Regions that support Availability Zones include Central US, North Europe, SouthEast Asia, and more.

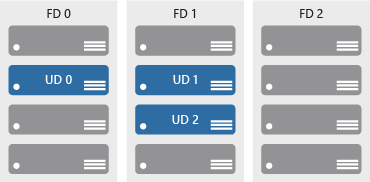
**Note**: See the page [What are Availability Zones in Azure?](https://docs.microsoft.com/en-us/azure/availability-zones/az-overview) for more details.

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

# ****Availability sets****

Availability sets are a way for you to ensure your application remains online if a high-impact maintenance event is required, or a hardware a failure occurs. Availability sets are made up of update domains and fault domains.

* Update domains (UD). When a maintenance event occurs (such as a performance update or critical security patch applied to the host), the update is sequenced through update domains. Sequencing updates using update domains ensures that the entire datacenter isn't unavailable during platform updates and patching. Update domains are a logical section of the datacenter, and they are implemented with software and logic.
* Fault domains (FD). Fault domains provide for the physical separation of your workload across different hardware in the datacenter. This includes power, cooling, and network hardware that supports the physical servers located in server racks. In the event the hardware that supports a server rack becomes unavailable, only that rack of servers would be affected by the outage.



<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

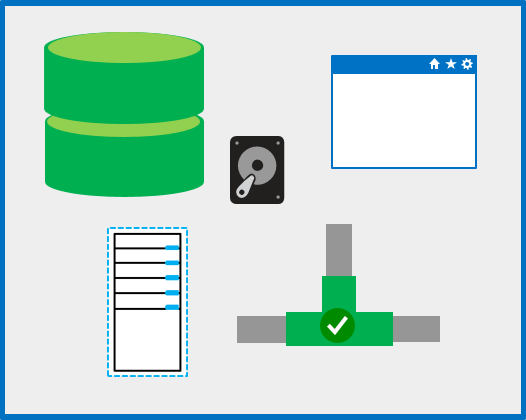
# ****Resource groups****

A resource group is a unit of management for your resources in Azure. You can think of your resource group as a container that allows you to aggregate and manage all the resources required for your application in a single manageable unit. This allows you to manage the application collectively over its life cycle, rather than manage components individually.

You can manage and apply the following resources at resource group level:

* Metering and billing
* Policies
* Monitoring and alerts
* Quotas
* Access control

Remember that when you delete a resource group you delete all resources contained within it.



### Considerations

When creating and placing resources within resource groups there are a few considerations to take into account:

* Each resource must exist in one, and only one, resource group.
* A resource group can contain resources that reside in different regions.
* You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.
* You can add or remove a resource to a resource group at any time.
* You can move a resource from one resource group to another.
* Resources for an application do not need to exist in the same resource group. However, it is recommended that you keep them in the same resource group for ease of management.

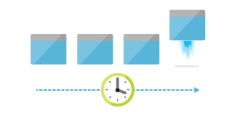
<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/21b33c86-c7aa-54aa-ea37-7fcf946e8af0/?child=first>

# ****Azure Resource Manager****

Azure Resource Manager is a management layer in which resource groups and all the resources within it are created, configured, managed, and deleted. It provides a consistent management layer which allows you automate the deployment and configuration of resources using different automation and scripting tools, such as Microsoft Azure PowerShell, Azure Command-Line Interface (Azure CLI), Azure portal, REST API, and client SDKs.

With Azure Resource Manager, you can:

* Deploy Application resources. Update, manage, and delete all the resources for your solution in a single, coordinated operation.



* Organize resources. Manage your infrastructure through declarative templates rather than scripts. You can see which resources are linked by a dependency, and you can apply tags to resources to categorize them for management tasks, such as billing.



* Control access and resources. You can control who in your organization can perform actions on the resources. You manage permissions by defining roles, adding users or groups to the roles, and applying policies at resource group level. Examples of elements you may wish to control are: enforcing naming convention on resources, limiting which types and instances of resources can be deployed, or limiting which regions can host a type of resource.



**Note**: See the page [Azure Resource Manager](https://azure.microsoft.com/en-us/features/resource-manager/) for more details.

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/067035b1-214a-8172-2c4d-7135e6a5ba75/?child=first>

# ****Azure Compute Services****

Azure compute is an on-demand computing service for running cloud-based applications. It provides computing resources such as disks, processors, memory, networking and operating systems. The resources are available on-demand and can typically be made available in minutes or even seconds. You pay only for the resources you use and only for as long as you're using them.

There are two common service types for performing compute in Azure: virtual machines, and containers.

## What are virtual machines?

Virtual machines, (VMs), are software emulations of physical computers. They include a virtual processor, memory, storage, and networking resources. They host an operating system, and you're able to install and run software just like a physical computer. When using a remote desktop client, you can use and control the virtual machine as if you were sitting in front it.

Azure supports a wide range of computing solutions for development and testing, running applications, and extending your datacenter, including Linux, Windows Server, Microsoft SQL Server, Oracle, IBM, and SAP.

Azure also has many services that can run virtual machines, each providing different options depending on your requirements. Some of the most prominent services are VM Scale Sets, App Services, and Azure Functions.

### **Azure VMs**

Azure virtual machine icon.

Azure VMs lets you create and use virtual machines in the cloud. It provides infrastructure as a service (IaaS) and can be used in a variety of different ways. When you need total control over an operating system and environment, Azure VMs are an ideal choice. Just like a physical computer, you're able to customize all of the software running on the VM. This is particularly helpful when you are running custom software or custom hosting configurations. See [Virtual Machines](https://azure.microsoft.com/en-us/services/virtual-machines/) for more details.

### **VM scale sets**



Virtual machine scale sets are an Azure compute resource that you can use to deploy and manage a set of identical VMs. With all VMs configured the same, VM scale sets are designed to support true auto-scale—no pre-provisioning of VMs is required—and as such makes it easier to build large-scale services targeting big compute, big data, and containerized workloads. So, as demand goes up more virtual machine instances can be added, and as demand goes down virtual machines instances can be removed. The process can be manual, automated, or a combination of both. See [Virtual Machine Scale Sets](https://azure.microsoft.com/en-us/services/virtual-machine-scale-sets/) for more details.

### **App services**



With App services, you can quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. You can meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. App Services is a platform as a service (PaaS) offering. See [App Service](https://azure.microsoft.com/en-us/services/app-service/) for more details.

### **Functions**



When you're concerned only about the code running your service and not the underlying platform or infrastructure, Azure Functions are ideal. They're commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less. See [Functions](https://azure.microsoft.com/en-us/services/functions/) for more details.

## What are containers?

Containers are a virtualization environment. However, unlike virtual machines they do not include an operating system. Instead, they reference the operating system of the host environment that runs the container.

Containers are meant to be lightweight and are designed to be created, scaled out, and stopped dynamically. This allows you to respond to changes on demand and quickly restart in case of a crash or hardware interruption.

Azure supports Docker containers, and there several ways to manage both Docker and Microsoft-based containers in Azure.

### **Azure Container Instances**



Azure Container Instances offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services. It is a PaaS offering that allows you to upload your containers, which it will run for you. See [Container Instances](https://azure.microsoft.com/en-us/services/container-instances/) for more details.

### **Azure Kubernetes Service**



The task of automating and managing a large number of containers and how they interact is known as orchestration. Azure Kubernetes Service (AKS) is a complete orchestration service for containers with distributed architectures and large volumes of containers. See [Azure Kubernetes Service (AKS)](https://azure.microsoft.com/en-us/services/kubernetes-service/) for more details.

**Note**: For a full list of compute services available with Azure and the context on when to use them, see [Compute](https://azure.microsoft.com/en-us/product-categories/compute/).

<https://training.azure-academy.com/courses/course-v1:FP+AZ-900+2019_T1/courseware/881ee5c0-b525-fe76-210c-7c479b6db568/067035b1-214a-8172-2c4d-7135e6a5ba75/?child=first>

To Create VM using Azure Portal

## Walkthrough-Create a Virtual machine using Azure Portal

In this walkthrough task we will create a virtual machine in Azure via the Azure Portal, configure it as a web server and connect to the web server over the internet.

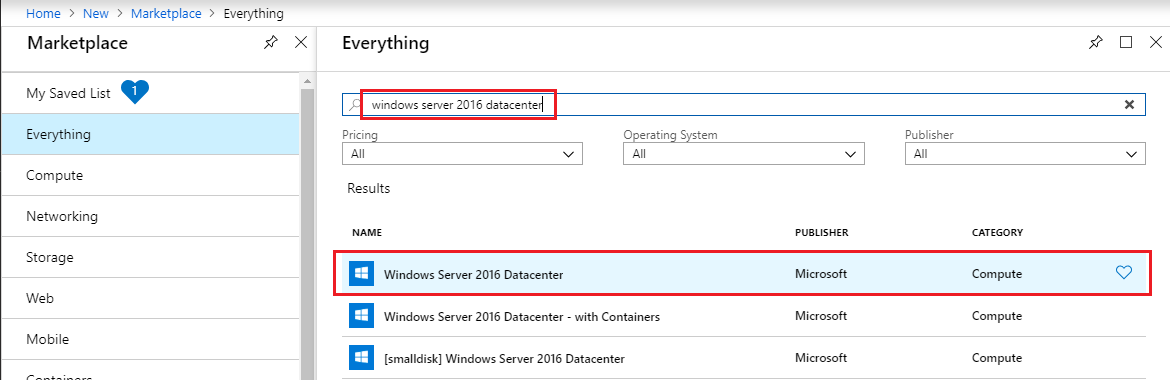
You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time.

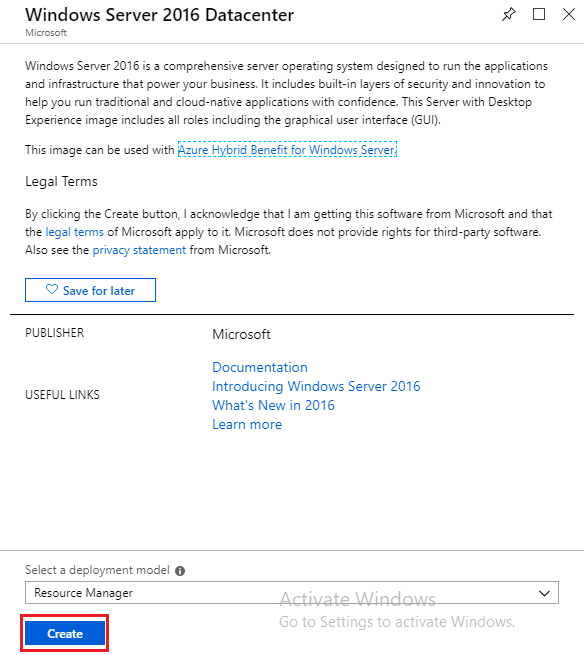
### Prerequisites

* You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today](https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio) webpage.

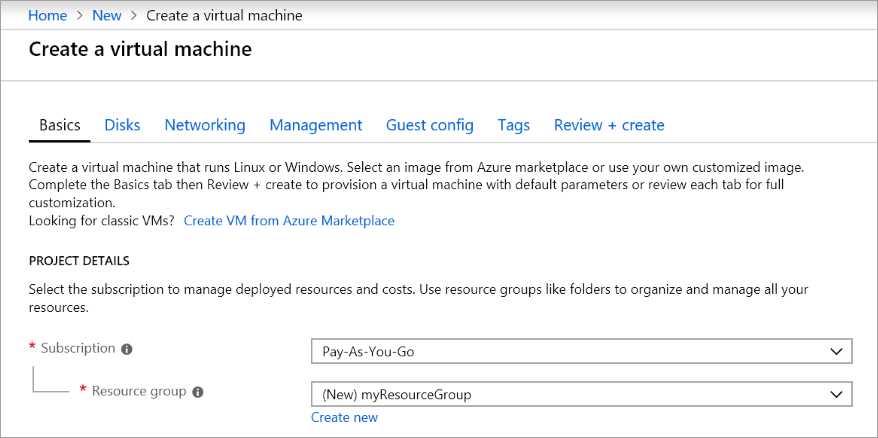
### Steps

1. Sign in to the Azure portal at [https://portal.azure.com](https://portal.azure.com/)
2. Choose **Create a resource** in the upper left-hand corner of the Azure portal.
3. In the search box above the list of Azure Marketplace resources, search for and select **Windows Server 2016 Datacenter**, then choose **Create**.

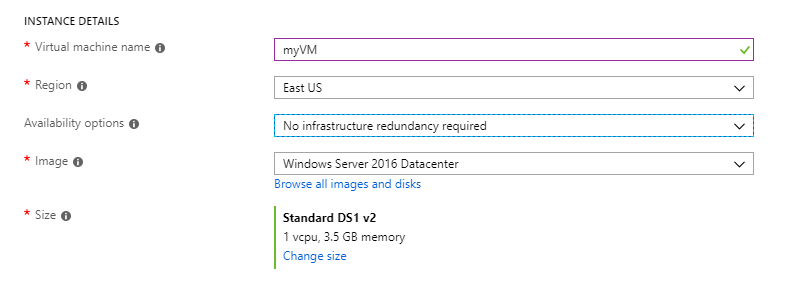




1. In the **Basics** tab, under Project details, make sure the correct subscription is selected and then choose to **Create new resource group**. Type myResourceGroup for the name.



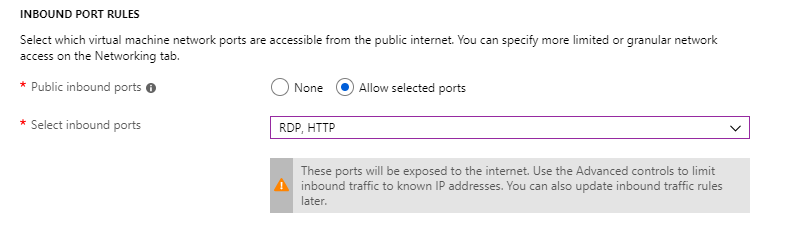
1. Under **Instance details**, type **myVM** for the Virtual machine name and choose **East US** for your Location. Leave the other defaults.



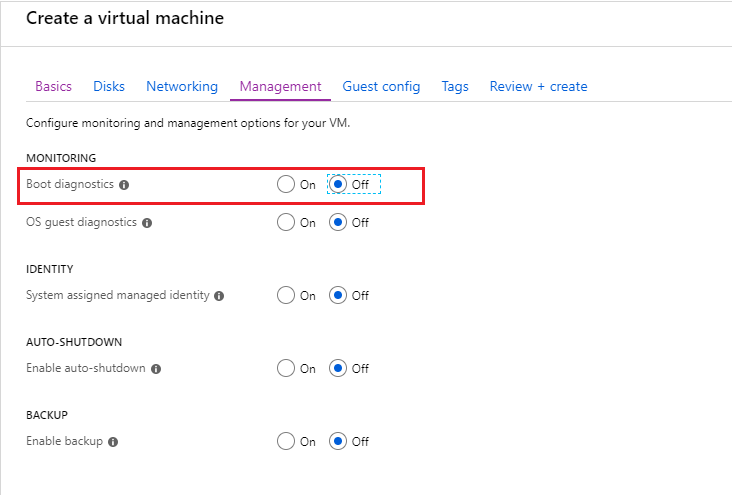
1. Under the **Administrator account** section, provide a username, such as **azureuser** and a password. The password must be at least 12 characters long and meet the defined complexity requirements.



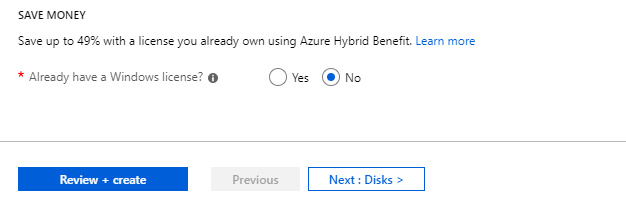
1. Under **Inbound port** rules, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP (80)** from the drop-down. These are to allow us to connect to the virtual machine using RDP over port 3389 and then to see a web page display over HTTP on port 80.



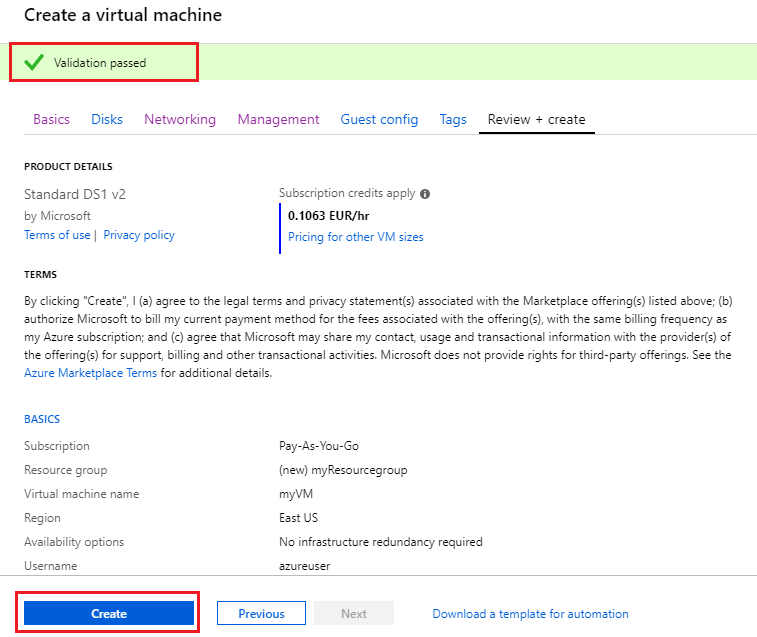
1. Go to the Management tab and under the **Monitoring** section under **Boot diagnostics** select **Off**



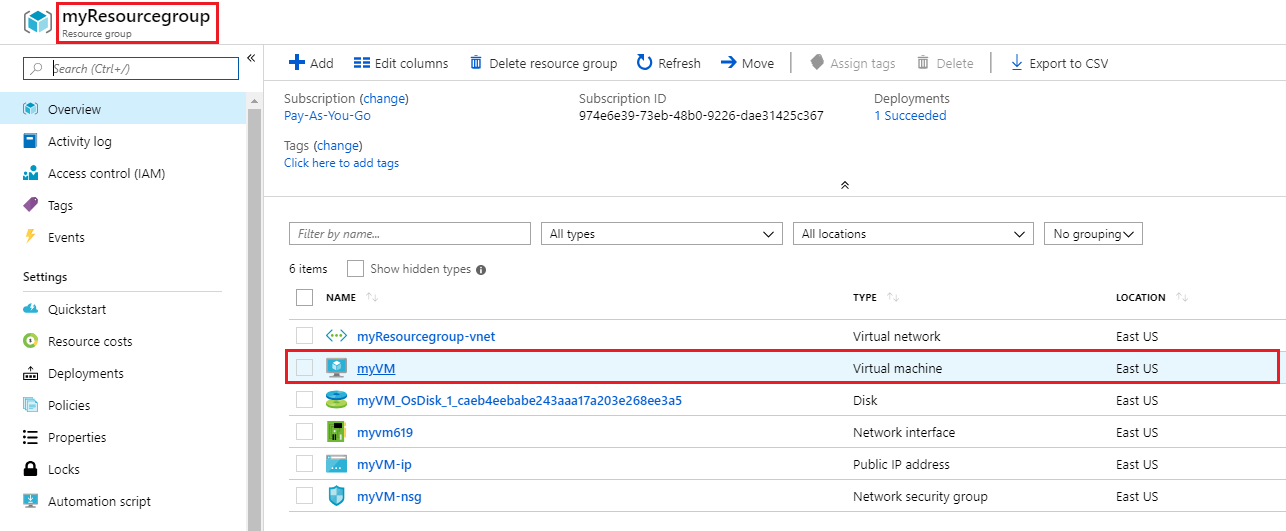
1. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.

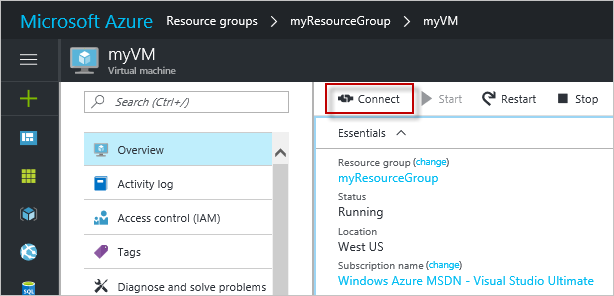


1. Once Validation is passed click the **Create** button. It can take approx three to five minutes to deploy the virtual machine.



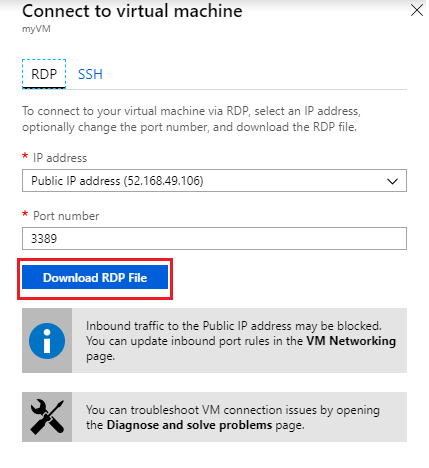
1. Once the virtual machine is created, go to the resource group you placed the virtual machine in, and open up the virtual machine, then click the **Connect** button on the virtual machine properties page.



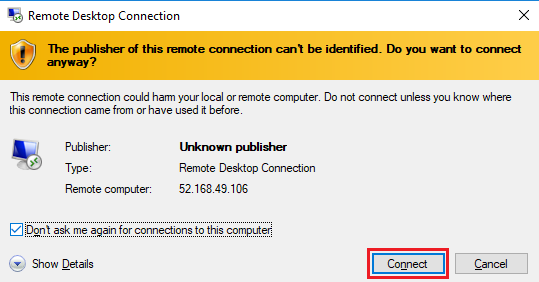


**Note**: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on Linux virtual machine you could connect directly from a bash shell using ssh.

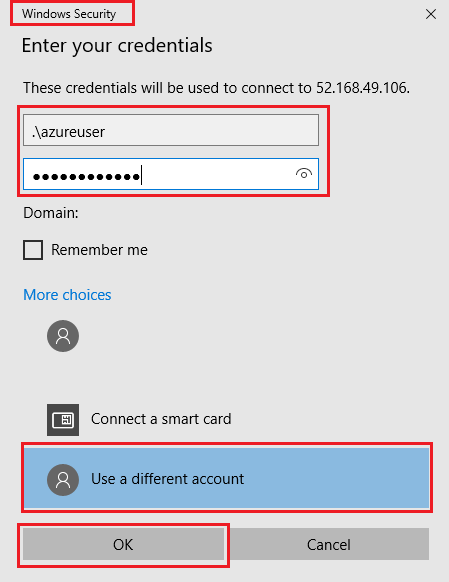
1. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP File**.



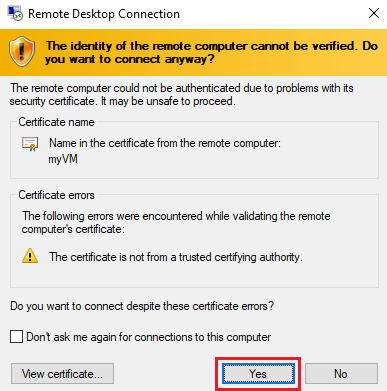
1. Open the downloaded RDP file and click **Connect** when prompted.



1. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as localhost\username, (you could also type **.\azureuser**) enter password you created for the virtual machine, and then click **OK**.



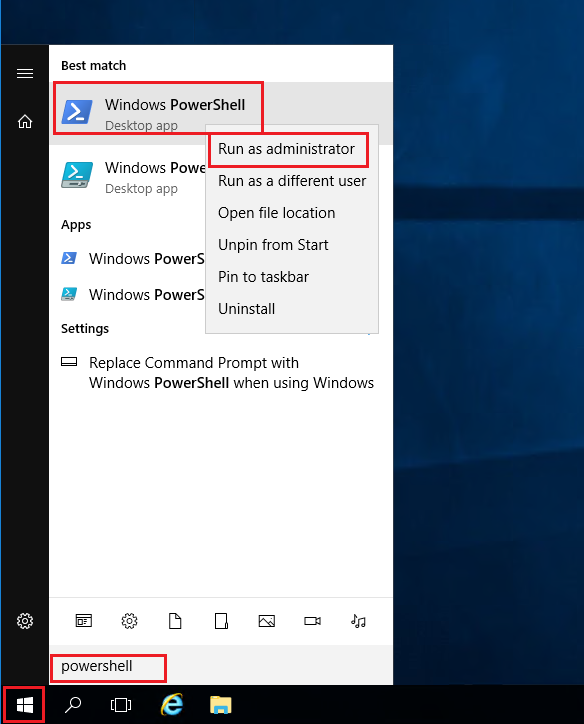
1. You may receive a certificate warning during the sign-in process. Click **Yes** or to create the connection and connect to your deployed VM. You should connect successfully.



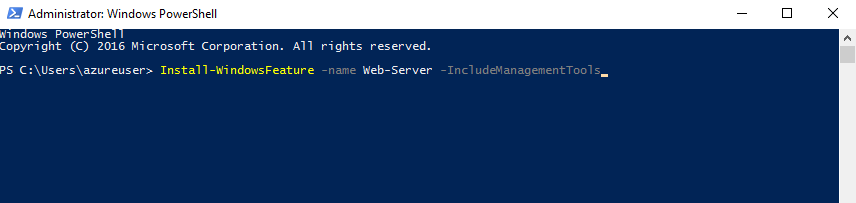
Congratulations! You have deployed and connected to a Windows Server virtual machine in Azure

If you wish and have time you could also make the deployed server a functioning web server and make a web page available publicly, by continuing with the following steps

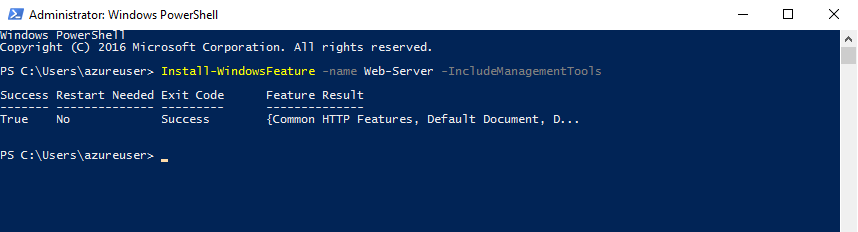
1. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell** right clicking **Windows PowerShell** in the menu and selecting **Run as administrator**



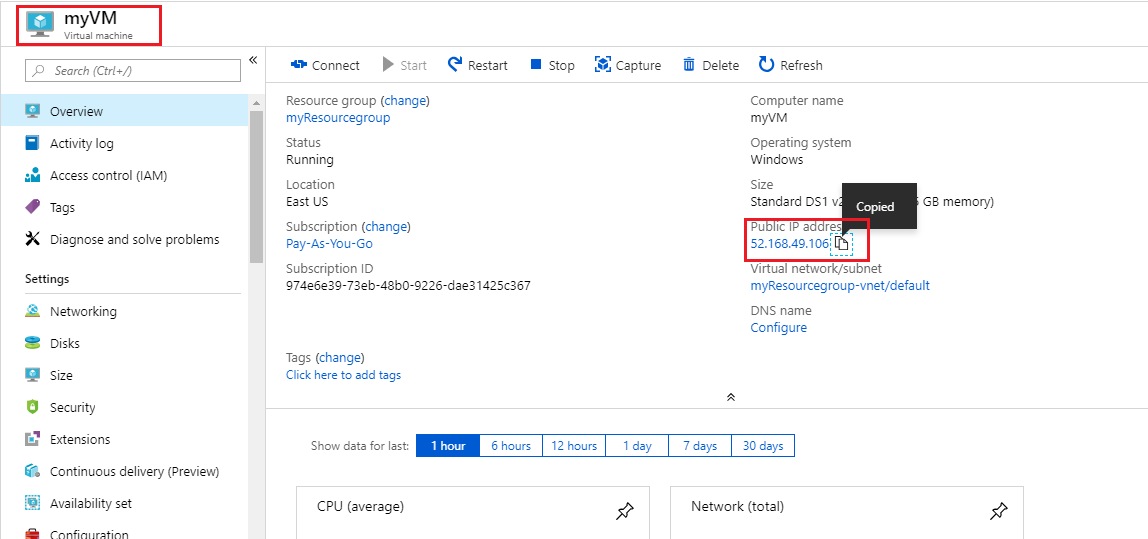
1. Install the **Web-Server** feature in the virtual machine by running the following command in the PowerShell command prompt: PowerShell
2. Install-WindowsFeature -name Web-Server -IncludeManagementTools



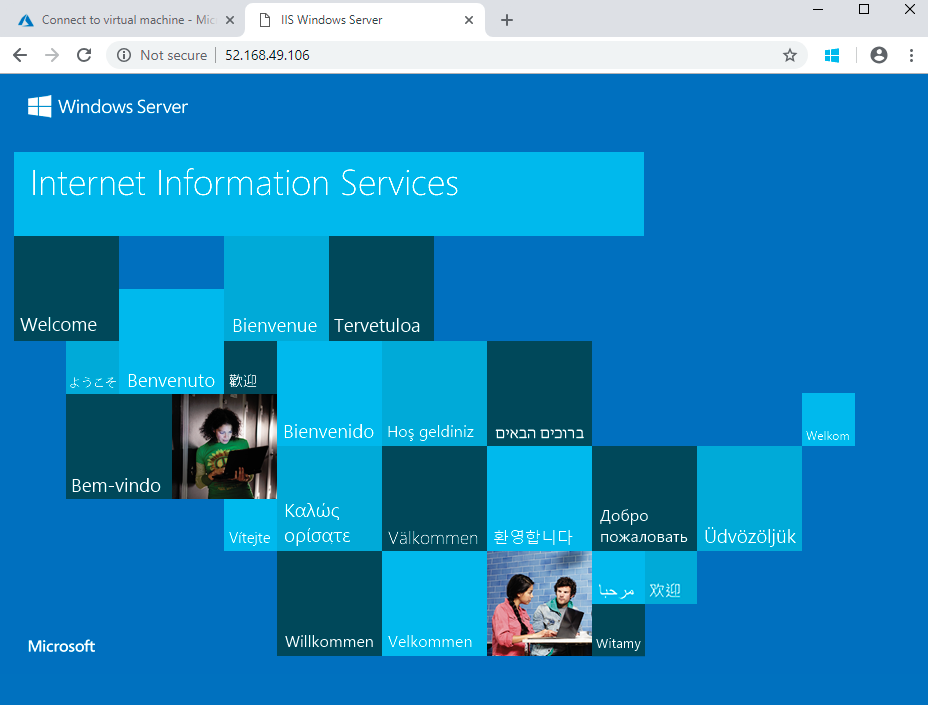
1. When completed you should see a prompt stating **Success** with a value **True**, among other items in the output. You do not need to restart the virtual machine to complete the installation. Close the RDP connection to the VM.



1. Back in the portal, select the VM and in the overview pane of the VM, use the **Click to copy** button to the right of the IP address to copy it and paste it into a browser tab.



1. The default IIS Web Server welcome page will open, and is available to connect to publicly via this IP address, or via the fully qualified domain name.



Congratulations! You have created a web server that can be connected to publicly via this IP address, or via the fully qualified domain name. If you had a web page to host you could deploy those source files to the virtual machine and host them for public access on the deployed virtual machine.

**Note**: Remember to delete the resources you have just deployed if you are no longer using them to ensure you do not incur costs for running resources. You can delete all deployed resources by deleting the resource group in which they all reside.