<https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing>

Cloud computing =>What is CC?

On demand computing resources delivered to you over internet.

A computing service you traditionally did local(on-premised), now performed remotely,across the internet(off-premises)

Is an apporach to computing that leverages the efficient pooling of an on demand, self managed, Virtual infrastructure.

Cloud Computing can be defined as delivering computing power( CPU, RAM, Network Speeds, Storage OS software) a service over a network (usually on the internet) rather than physically having the computing resources at the customer location.

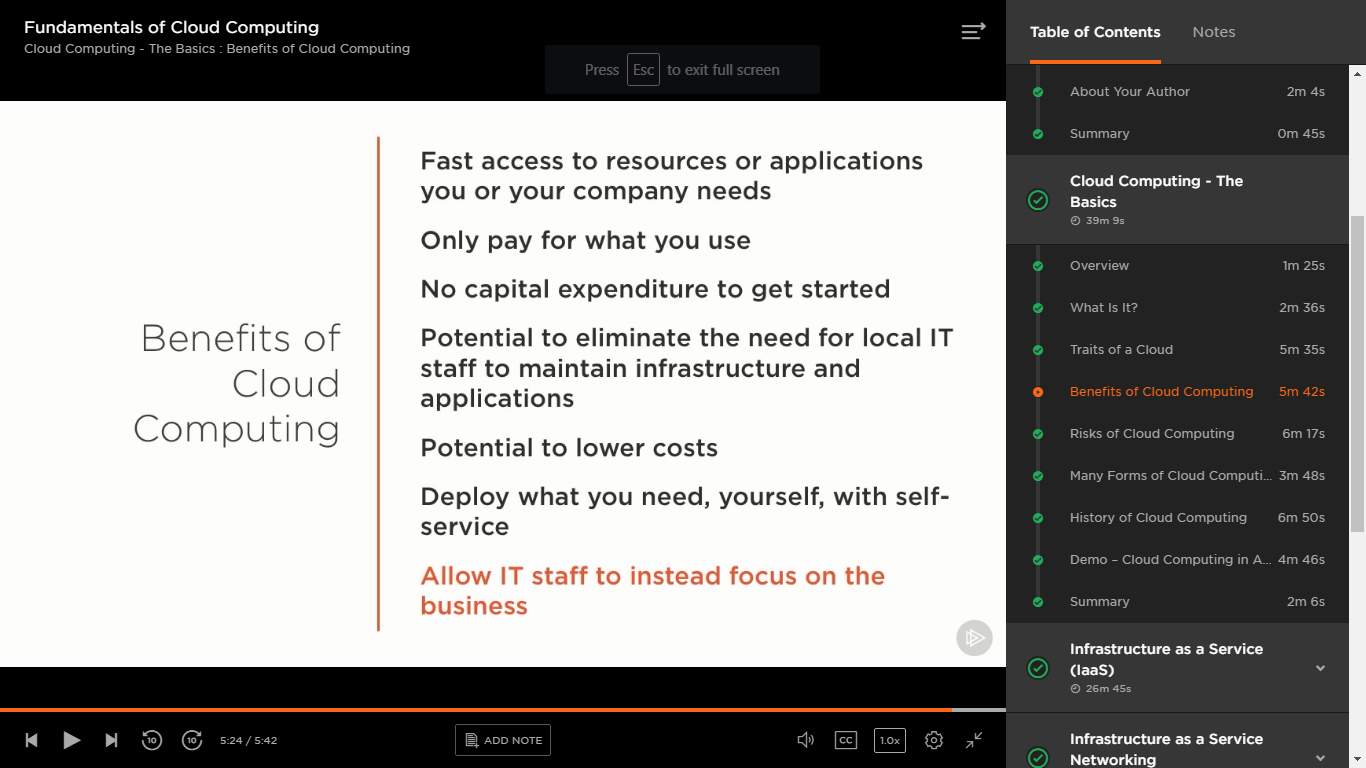
Example: AWS, Azure, Google Cloud

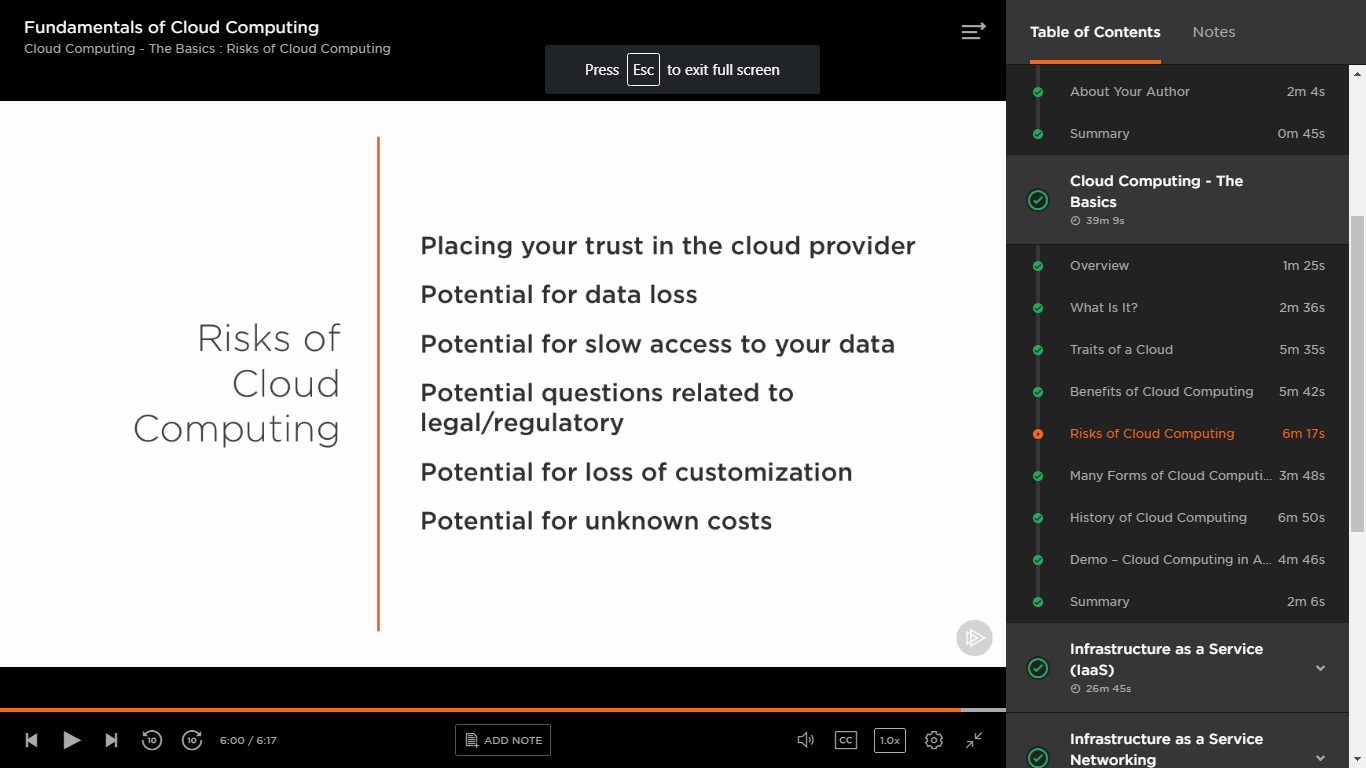
Traits:

1. Elastic : Scales up and down
2. Meterd : Pay only for wat u use
3. Self Service: No need for IT experts

Benefits:

It’s cost-effective, scalable, elastic, current, reliable, and secure. This means you’re able to spend more time on what matters and less time managing the underlying details.





Types of cloud

SAAS: Accessing application in cloud .Pay for wat u use

Gmail, DropBOX, O365, SalesForce.com

IAAS : Accesssing VM that is instance of physical machine.

PAAS: Developers need platform to develop and deploy the code. No need to maintain the underline software and hardware.

Types of 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 (IT infrastructure servers and virtual machines (VMs), storage, networks, and operating systems). Instead of buying hardware, with IaaS, you rent it. It's an instant computing infrastructure, provisioned and managed over the internet.

PAAS:

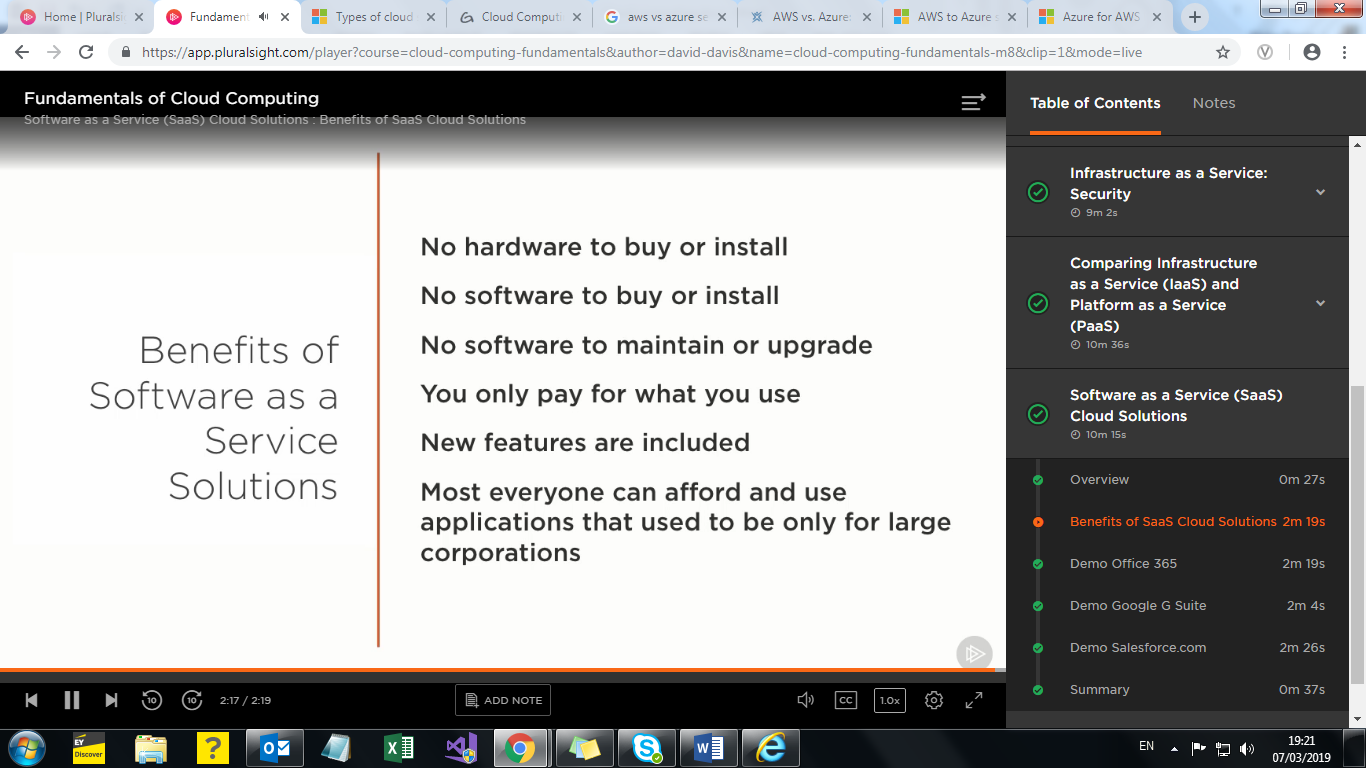
The cloud provider is responsible for operating system management, and network and service configuration. Cloud providers are typically responsible for everything apart from the application that a user wants to run. They provide a complete managed platform on which to run an application.

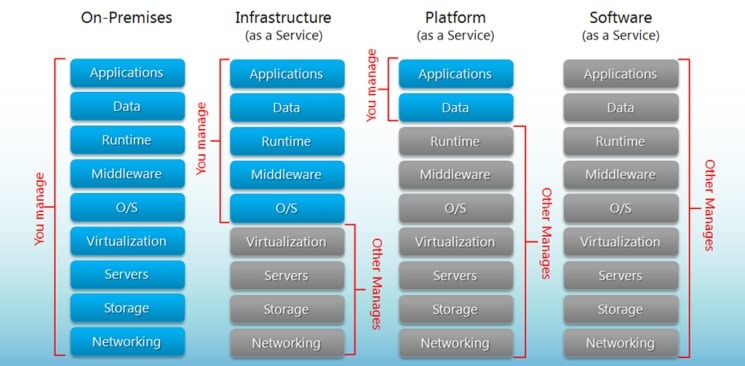
SAAS

The cloud provider is responsible for the provision, management, and maintenance of the application software.

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. Office 365, Skype, and Dynamics CRM Online are perfect examples of SaaS software.

**Benefits of SAAS**





IAAS

**IaaS (Infrastructure as a Service).**

IaaS businesses offer services such as pay-as-you-go storage, networking, and virtualization.

IaaS gives users cloud-based alternatives to on-premise infrastructure, so businesses can avoid investing in expensive on-site resources.

***IaaS Delivery:***

Over the internet.

***IaaS Advantages:***

Maintaining on-premise IT infrastructure is costly and labor-intensive.

It often requires a significant initial investment in physical hardware, and then you will probably need to engage external IT contractors to maintain the hardware and keep everything working and up-to-date.

IaaS solutions are highly flexible and highly scalable, and you can replace it whenever you need without losing money on your initial investment.

Another advantage of IaaS is it puts control over the infrastructure back in your hands.

You no longer need to place faith in an external IT contractor; you can access and oversee IaaS platforms yourself if you wish (without being an IT whizz).

***IaaS Characteristics:***

IaaS platforms are:

* Highly flexible and highly scalable.
* Accessible by multiple users.
* Cost-effective.

***When to Use IaaS:***

IaaS is beneficial to businesses of all shapes and sizes, as it allows complete control over your infrastructure, and operates on a pay-as-you-use model, so it fits into most budgets.

As it becomes less common to invest in physical hardware and IT infrastructure, choosing IaaS alternatives is a safer, more reliable option

A good example of IaaS is [AWS EC2](https://aws.amazon.com/ec2/).

EC2 provides scalable infrastructure for companies who want to host cloud-based applications.

EC2 users do not own the physical servers; AWS provides virtual servers.

So users only pay for the usage of the servers, saving them the cost (and associated ongoing maintenance) of investing in physical hardware



IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More

GET THE PRINT VERSION

Tired of scrolling? Download a PDF version for easier offline reading and sharing with coworkers.   
DOWNLOAD PDF

If you’re considering moving your [ecommerce business](https://www.bigcommerce.com/blog/ecommerce-business-ideas/) to the Cloud, here are three important acronyms to wrap your head around:

* IaaS.
* PaaS.
* SaaS.

These are the [three main types of cloud computing](https://www.bigcommerce.com/ecommerce-answers/what-is-cloud-computing/).

You’ve probably heard of them before; they’re all experiencing a surge in popularity as more businesses move to the Cloud.

* SaaS accounts for approximately [24% of all enterprise workloads](https://451research.com/blog/764-enterprise-it-executives-expect-60-of-workloads-will-run-in-the-cloud-by-2018) (up from 14% in 2016)
* IaaS is hovering around 12% (up from 6%).
* PaaS is currently the most popular model, hovering around 32% and [expected to grow in 2020](https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/the-creative-cios-agenda-journey-to-cloud.PDF).

With uptake rates like these, cloud computing is becoming the norm, and many businesses are phasing out on-premise software altogether.

The Key Differences Between On-Premise, SaaS, PaaS, IaaS

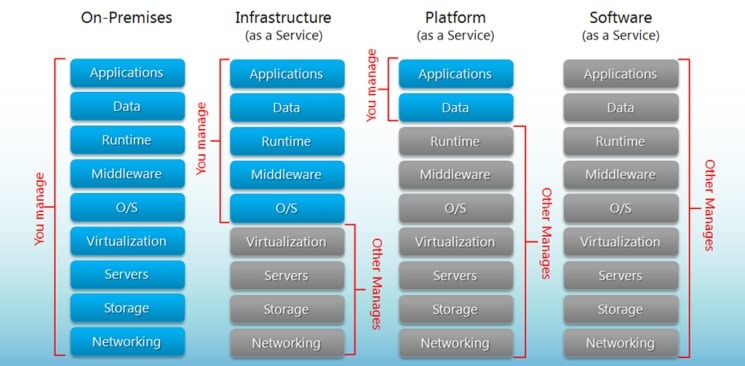
Not so long ago, all of a company’s IT systems were on-premise, and clouds were just white fluffy things in the sky.

Now, you can utilize the Cloud platform for nearly all your systems and processes.

SaaS, PaaS, and IaaS are simply three ways to describe how you can use the cloud for your business.

* IaaS: cloud-based services, pay-as-you-go for services such as storage, networking, and virtualization.
* PaaS: hardware and software tools available over the internet.
* SaaS: software that’s available via a third-party over the internet.
* On-premise: software that’s installed in the same building as your business.

Here’s a great visual breakdown from [Hosting Advice](https://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/):



Examples of SaaS, PaaS, and IaaS

Most businesses use a combination of SaaS and IaaS cloud computing service models, and many engage developers to create applications using PaaS, too.

SaaS examples: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot.

PaaS examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.

IaaS examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition\*.

*\*Note that Magento 1 Enterprise can be either on prem or IaaS, but it is generally IaaS.*

The Three Types of Cloud Computing Service Models Explained

**1. IaaS (Infrastructure as a Service).**

IaaS businesses offer services such as pay-as-you-go storage, networking, and virtualization.

IaaS gives users cloud-based alternatives to on-premise infrastructure, so businesses can avoid investing in expensive on-site resources.

***IaaS Delivery:***

Over the internet.

***IaaS Advantages:***

Maintaining on-premise IT infrastructure is costly and labor-intensive.

It often requires a significant initial investment in physical hardware, and then you will probably need to engage external IT contractors to maintain the hardware and keep everything working and up-to-date.

With IaaS, you can buy what you need, as you need it, and purchase more as your business grows.

IaaS solutions are highly flexible and highly scalable, and you can replace it whenever you need without losing money on your initial investment.

Another advantage of IaaS is it puts control over the infrastructure back in your hands.

You no longer need to place faith in an external IT contractor; you can access and oversee IaaS platforms yourself if you wish (without being an IT whizz).

***IaaS Characteristics:***

IaaS platforms are:

* Highly flexible and highly scalable.
* Accessible by multiple users.
* Cost-effective.

***When to Use IaaS:***

IaaS is beneficial to businesses of all shapes and sizes, as it allows complete control over your infrastructure, and operates on a pay-as-you-use model, so it fits into most budgets.

As it becomes less common to invest in physical hardware and IT infrastructure, choosing IaaS alternatives is a safer, more reliable option.

With most IaaS platforms, you get access to ongoing support and have the option of scaling up your requirements at any time.

Utilizing IaaS is a great way to future-proof your business.

***IaaS Non-Ecommerce Example:***

A good example of IaaS is [AWS EC2](https://aws.amazon.com/ec2/).

EC2 provides scalable infrastructure for companies who want to host cloud-based applications.

EC2 users do not own the physical servers; AWS provides virtual servers.

So users only pay for the usage of the servers, saving them the cost (and associated ongoing maintenance) of investing in physical hardware.

***IaaS Ecommerce Example:***

Magento 1 Enterprise Edition can be either on-premise or IaaS depending on how the merchant chooses to host their store.

In the case of IaaS, the merchant is paying Magento for the licensing of the software and then using a [third party vendor for hosting](https://www.adamenfroy.com/best-web-hosting-services) such as Rackspace.

Merchants are able to pay for a hosting plan that meets their own needs without the cost of maintaining their own physical servers.

The merchant is still responsible for installing and managing updates to their Magento software.

Want more insights like this?

We’re on a mission to provide businesses like yours marketing and sales tips, tricks and industry leading knowledge to build the next house-hold name brand. Don’t miss a post. Sign up for our weekly newsletter.

Top of Form

SUBSCRIBE

Bottom of Form

**2. PaaS (Platform as a Service).**

A PaaS vendor provides hardware and software tools over the internet, and people use these tools to develop applications. PaaS users tend to be developers.

***PaaS Delivery:***

Over the internet.

***PaaS Advantages:***

PaaS is primarily used by developers who are building software or applications.

A PaaS solution provides the platform for developers to create unique, customizable software.

This means developers don’t need to start from scratch when creating applications, saving them a lot of time (and money) on writing extensive code.

PaaS is a popular choice for businesses who want to create unique applications without spending a fortune or taking on all the responsibility.

It’s kind of like the difference between hiring a venue to put on a show vs. building a venue to put on a show.

The venue stays the same, but what you create in that space is unique.

***PaaS Characteristics:***

PaaS platforms are:

* Accessible by multiple users.
* Scalable – you can choose from various tiers of resources to suit the size of your business.
* Built on virtualization technology.
* Easy to run without extensive system administration knowledge.

***When to Use PaaS:***

PaaS is often the most cost-effective and time-effective way for a developer to create a unique application.

PaaS allows the developer to focus on the creative side of app development, as opposed to menial tasks such as managing software updates or security patches. All of their time and brainpower will go into creating, testing, and deploying the app.

***PaaS Non-Ecommerce Example:***

A good example of PaaS is [AWS Elastic Beanstalk](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html).

Amazon Web Services (AWS) offers over 100 cloud computing services such as EC2, RDS, and S3.

Most of these services can be used as IaaS, and most companies who use AWS will pick and choose the services they need.

However, managing multiple different services can quickly become difficult and time-consuming for users.



IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More

GET THE PRINT VERSION

Tired of scrolling? Download a PDF version for easier offline reading and sharing with coworkers.   
DOWNLOAD PDF

If you’re considering moving your [ecommerce business](https://www.bigcommerce.com/blog/ecommerce-business-ideas/) to the Cloud, here are three important acronyms to wrap your head around:

* IaaS.
* PaaS.
* SaaS.

These are the [three main types of cloud computing](https://www.bigcommerce.com/ecommerce-answers/what-is-cloud-computing/).

You’ve probably heard of them before; they’re all experiencing a surge in popularity as more businesses move to the Cloud.

* SaaS accounts for approximately [24% of all enterprise workloads](https://451research.com/blog/764-enterprise-it-executives-expect-60-of-workloads-will-run-in-the-cloud-by-2018) (up from 14% in 2016)
* IaaS is hovering around 12% (up from 6%).
* PaaS is currently the most popular model, hovering around 32% and [expected to grow in 2020](https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/the-creative-cios-agenda-journey-to-cloud.PDF).

With uptake rates like these, cloud computing is becoming the norm, and many businesses are phasing out on-premise software altogether.

The Key Differences Between On-Premise, SaaS, PaaS, IaaS

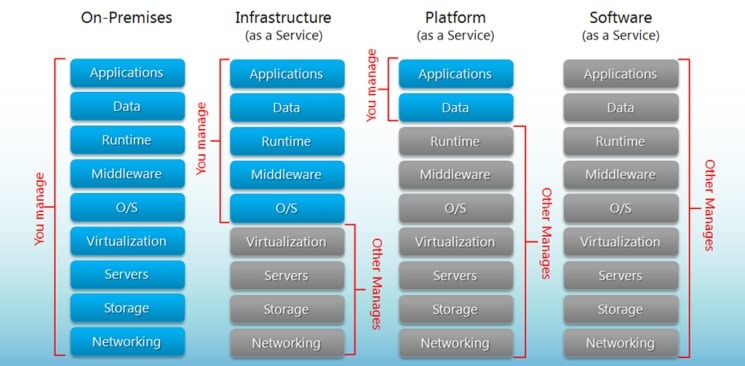
Not so long ago, all of a company’s IT systems were on-premise, and clouds were just white fluffy things in the sky.

Now, you can utilize the Cloud platform for nearly all your systems and processes.

SaaS, PaaS, and IaaS are simply three ways to describe how you can use the cloud for your business.

* IaaS: cloud-based services, pay-as-you-go for services such as storage, networking, and virtualization.
* PaaS: hardware and software tools available over the internet.
* SaaS: software that’s available via a third-party over the internet.
* On-premise: software that’s installed in the same building as your business.

Here’s a great visual breakdown from [Hosting Advice](https://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/):



Examples of SaaS, PaaS, and IaaS

Most businesses use a combination of SaaS and IaaS cloud computing service models, and many engage developers to create applications using PaaS, too.

SaaS examples: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot.

PaaS examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.

IaaS examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition\*.

*\*Note that Magento 1 Enterprise can be either on prem or IaaS, but it is generally IaaS.*

The Three Types of Cloud Computing Service Models Explained

**1. IaaS (Infrastructure as a Service).**

IaaS businesses offer services such as pay-as-you-go storage, networking, and virtualization.

IaaS gives users cloud-based alternatives to on-premise infrastructure, so businesses can avoid investing in expensive on-site resources.

***IaaS Delivery:***

Over the internet.

***IaaS Advantages:***

Maintaining on-premise IT infrastructure is costly and labor-intensive.

It often requires a significant initial investment in physical hardware, and then you will probably need to engage external IT contractors to maintain the hardware and keep everything working and up-to-date.

With IaaS, you can buy what you need, as you need it, and purchase more as your business grows.

IaaS solutions are highly flexible and highly scalable, and you can replace it whenever you need without losing money on your initial investment.

Another advantage of IaaS is it puts control over the infrastructure back in your hands.

You no longer need to place faith in an external IT contractor; you can access and oversee IaaS platforms yourself if you wish (without being an IT whizz).

***IaaS Characteristics:***

IaaS platforms are:

* Highly flexible and highly scalable.
* Accessible by multiple users.
* Cost-effective.

***When to Use IaaS:***

IaaS is beneficial to businesses of all shapes and sizes, as it allows complete control over your infrastructure, and operates on a pay-as-you-use model, so it fits into most budgets.

As it becomes less common to invest in physical hardware and IT infrastructure, choosing IaaS alternatives is a safer, more reliable option.

With most IaaS platforms, you get access to ongoing support and have the option of scaling up your requirements at any time.

Utilizing IaaS is a great way to future-proof your business.

***IaaS Non-Ecommerce Example:***

A good example of IaaS is [AWS EC2](https://aws.amazon.com/ec2/).

EC2 provides scalable infrastructure for companies who want to host cloud-based applications.

EC2 users do not own the physical servers; AWS provides virtual servers.

So users only pay for the usage of the servers, saving them the cost (and associated ongoing maintenance) of investing in physical hardware.

***IaaS Ecommerce Example:***

Magento 1 Enterprise Edition can be either on-premise or IaaS depending on how the merchant chooses to host their store.

In the case of IaaS, the merchant is paying Magento for the licensing of the software and then using a [third party vendor for hosting](https://www.adamenfroy.com/best-web-hosting-services) such as Rackspace.

Merchants are able to pay for a hosting plan that meets their own needs without the cost of maintaining their own physical servers.

The merchant is still responsible for installing and managing updates to their Magento software.

Want more insights like this?

We’re on a mission to provide businesses like yours marketing and sales tips, tricks and industry leading knowledge to build the next house-hold name brand. Don’t miss a post. Sign up for our weekly newsletter.

Top of Form

SUBSCRIBE

Bottom of Form

**2. PaaS (Platform as a Service).**

A PaaS vendor provides hardware and software tools over the internet, and people use these tools to develop applications. PaaS users tend to be developers.

***PaaS Delivery:***

Over the internet.

***PaaS Advantages:***

PaaS is primarily used by developers who are building software or applications.

A PaaS solution provides the platform for developers to create unique, customizable software.

This means developers don’t need to start from scratch when creating applications, saving them a lot of time (and money) on writing extensive code.

PaaS is a popular choice for businesses who want to create unique applications without spending a fortune or taking on all the responsibility.

It’s kind of like the difference between hiring a venue to put on a show vs. building a venue to put on a show.

The venue stays the same, but what you create in that space is unique.

***PaaS Characteristics:***

PaaS platforms are:

* Accessible by multiple users.
* Scalable – you can choose from various tiers of resources to suit the size of your business.
* Built on virtualization technology.
* Easy to run without extensive system administration knowledge.

***When to Use PaaS:***

PaaS is often the most cost-effective and time-effective way for a developer to create a unique application.

PaaS allows the developer to focus on the creative side of app development, as opposed to menial tasks such as managing software updates or security patches. All of their time and brainpower will go into creating, testing, and deploying the app.

***PaaS Non-Ecommerce Example:***

A good example of PaaS is [AWS Elastic Beanstalk](https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html).

Amazon Web Services (AWS) offers over 100 cloud computing services such as EC2, RDS, and S3.

Most of these services can be used as IaaS, and most companies who use AWS will pick and choose the services they need.

However, managing multiple different services can quickly become difficult and time-consuming for users.

That’s where AWS Elastic Beanstalk comes in: it works as another layer on top of the infrastructure services and automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

All you need to do is upload and maintain your application.

***PaaS Ecommerce Example:***

Magento Commerce Cloud (also known as Magento Enterprise Cloud Edition) is the most common example of PaaS for ecommerce.

This enables the merchant to bundle their hosting as part of their package with Magento.

Merchants evaluating Magento go through a scoping process to determine their hosting needs which is then bundled into their monthly plan.

Merchants still have full access to edit the source code of their Magento store and can fully customize the application.

Any platform updates, security patches and general maintenance to their store would be the responsibility of the merchant.

**3. SaaS (Software as a Service).**

SaaS platforms make software available to users over the internet, usually for a monthly subscription fee.

***SaaS Delivery:***

Over the internet.

***SaaS Advantages:***

With [SaaS](https://learn.g2crowd.com/what-is-saas), you don’t need to install and run software applications on your computer (or any computer).

Everything is available over the internet when you log in to your account online.

You can usually access the software from any device, anytime (as long as there is an internet connection).

The same goes for anyone else using the software. All your staff will have personalized logins, suitable to their access level.

You no longer need to engage an IT specialist to download the software onto multiple computers throughout your office or worry about keeping the software on every computer up-to-date.

It’s all taken care of in the Cloud.

Another key advantage is the payment structure.

Most SaaS providers operate a subscription model with a fixed, inclusive monthly account fee.

You know exactly how much the software will cost and can budget accordingly, without worrying about hidden surprises.

Most subscriptions include maintenance, compliance, and security services, which can be time-consuming and costly when using on-premise software.

SaaS providers also offer out-of-the-box solutions that are simple to set up (if you need a basic package), with more complex solutions for larger organizations.

You could have the basic software up and running within a matter of hours – and you’ll have access to customer service and support along the way.

***SaaS Characteristics:***

SaaS platforms are:

* Available over the internet.
* Hosted on a remote server by a third-party provider.
* Scalable, with different tiers for small, medium, and enterprise-level businesses.
* Inclusive, offering security, compliance, and maintenance as part of the cost.

***When to Use SaaS:***

SaaS platforms are ideal for when you want an application to run smoothly and reliably with minimal input from you.

Take your email server, for example.

You want to know that you’ll continue to send and receive emails without needing to fiddle with your email settings or worry about updates.

Imagine if your email server went under because you forgot to update it and you went days without email? That’s simply not an option in today’s marketplace.

If you use a SaaS platform to run your email inbox, the chances of something going wrong are very small.

And if something did go wrong, it would be up to the SaaS provider to find a solution.

You’re not only paying for the SaaS applications/products: you’re paying for peace of mind.

***SaaS Ecommerce Example:***

BigCommerce is an example of a [SaaS ecommerce platform](https://www.bigcommerce.com/blog/ecommerce-platforms/).

BigCommerce provides complete shopping cart software, as well as hosting infrastructure to the user, allowing businesses to create an online shop within minutes without worrying about coding, hosting, or software.

The BigCommerce platform also has regular updates that automatically roll out for users, and all the software licenses, upgrades, and hosting costs are covered in the monthly subscription fee.

What are the differences between IaaS, PaaS, and SaaS?

* IaaS is there to provide you with maximum flexibility when it comes to hosting custom-built apps, as well as a providing a general data center for data storage.
* PaaS is most often built on top of an IaaS platform to reduce the need for system administration. It allows you to focus on app development instead of infrastructure management.
* SaaS offers ready-to-use, out-of-the-box solutions that meet a particular business need (such as website or email). Most modern SaaS platforms are built on IaaS or PaaS platforms.

You might choose to start with one cloud computing service model or find a need for all three: that depends on the size and complexity of your business.

**Three different models**

Nearly everyone uses the cloud, but not everyone uses the same type of cloud. There are in fact three different cloud models, including public, private and hybrid clouds. To help determine which cloud best suits your company’s needs, the following explores how these three models compare and contrast.

**Public cloud**

Public clouds are what most people refer to when thinking about “the cloud.” What makes a public cloud “public” is it is hosted by a service provider like Amazon, Google, IBM or Microsoft, which enables customers to access and share basic computer infrastructure, including hardware, storage and bandwidth.

A public cloud has several benefits. In addition to delivering services over the web, customers only pay for the resources they use like a utility bill. Moreover, since organizations have access to the service provider’s cloud infrastructure, they don’t have to worry about personally installing and maintaining it.

One drawback of a public cloud pertains to security. Public clouds often cannot meet many security regulatory compliance requirements since different servers reside in multiple countries with various security regulations. Moreover, network issues can occur during peaks in online traffic. And while a public cloud model is generally cost-effective by offering pay-as-you go pricing, expenses can accrue quickly when moving large amounts of data.

**Private cloud**

A private cloud is one in which a business has sole access to infrastructure resources. Customers can choose to have the private cloud located at an on-site data center or hosted by a third-party service provider.

A benefit of a private cloud model is it provides greater security compared to a public cloud model since a single company is the only designated entity that has access to it. This also makes it easier for organizations to customize their resources to meet specific IT requirements.

A disadvantage of a private cloud is it can be expensive to install. Moreover, businesses are restricted to cloud infrastructure resources as specified in a contract. The heightened security of a private cloud can make it difficult to access from remote locations too.

**Hybrid cloud**

A hybrid cloud model provides multiple options from different service providers. With a hybrid cloud, data and applications move between both a private and public cloud. For example, customers can choose to store data in a private cloud, while running an application in a public cloud.

A benefit of a hybrid cloud approach is it allow users to take advantage of both public and private clouds. It also provides a great deal of flexibility as applications drift across multi-cloud environments. Additionally, a hybrid cloud model is cost-effective since companies can decide to use more expensive cloud resources only as needed.

A difficulty with a hybrid cloud is it can be hard to maintain and secure on account of being more complex. Additionally, integration can be a challenge since a hybrid cloud is a combination of different clouds, data and applications. Major compatibility issues can arise across the infrastructure when developing a hybrid cloud as well.

Resource group

A resource group contains the resources required to successfully deploy a vSRX VM in Azure. It is a container that holds related resources for an Azure solution. In Azure, you logically group related resources such as storage accounts, virtual networks, and virtual machines (VMs) to deploy, manage, and maintain them as a single entity.

It is a container that holds related **resources** for an **Azure** solution. In **Azure**, you logically **group** related **resources** such as storage accounts, virtual networks, and virtual machines (VMs) to deploy, manage, and maintain them as a single entity. ... click Add (+) to create a new **resource group**.

| Parameter | Description |
| --- | --- |
| Resource Group Name | Enter a unique name for your new resource group. A resource group name can include alphanumeric characters, periods (.), underscores (\_), hyphens (-), and parenthesis (), but the name cannot end with a period. |
| Subscription | Select your Microsoft Azure subscription. |
| Resource Group Location | Select the location of the Microsoft Azure data center from which you intend to deploy the vSRX VM. Specify a location where the majority of your resources will reside. Typically, select the location that is closest to your physical location. |

Virtual Network:

Build a hybrid infrastructure that you control

Bring your own IP addresses and DNS servers

Secure your connections with an IPsec VPN or ExpressRoute

Get granular control over traffic between subnetss

Create sophisticated network topologies using virtual appliances

Get an isolated and highly-secure environment for your applications

A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

Azure resources can be deployed into a virtual network and have network security groups associated to them.

<https://app.pluralsight.com/library/courses/microsoft-azure-configuring-virtual-machines/table-of-contents>

<https://app.pluralsight.com/player?course=azure-vms-getting-started&author=tim-warner&name=azure-vms-getting-started-m0&clip=0&mode=live>

<https://app.pluralsight.com/library/courses/azure-vms-getting-started/table-of-contents>

<https://app.pluralsight.com/library/courses/microsoft-azure-connecting-virtual-networks/table-of-contents>

<https://app.pluralsight.com/library/courses/microsoft-azure-implement-manage-virtual-networks/table-of-contents>

Learn how to create a virtual network, deploy virtual machines into it, and then communicate between the virtual machines, and the internet

Learn how to create and connect virtual networks and control routing and filtering.

Filter network traffic

Route network traffic

Restrict network access to resources

Connect virtual networks

Networking

Virtaul network is isolated container secured network in which we can populate one or more windows server or linux virtual machine. To communicate between 2 virtual network we have vNet to vNet connection or vPN(Virtual private network).

Think of your onprem IP ranges,In VN we have subnet in which ip range is subdivided into subnet.

DNS for resolving ip conflict in vNet to vNet.

NSG is the software firewall bind to subnet. We have separate traffic rule.

Quickstart: Create a virtual network using the Azure portal

11/30/2018

5 minutes to read

Contributors

Jim Dial Kumud Dwivedi John Parente Peter Semkin

A virtual network enables Azure resources, like virtual machines (VMs), to communicate privately with each other, and with the internet. In this quickstart, you learn how to create a virtual network. After creating a virtual network, you deploy two VMs into the virtual network. You then connect to the VMs from the internet, and communicate privately between the two VMs.

If you don't have an Azure subscription, create a free account now.

Sign in to Azure

Sign in to the Azure portal.

Create a virtual network

On the upper-left side of the screen, select Create a resource > Networking > Virtual network.

In Create virtual network, enter or select this information:

Setting Value

Name Enter myVirtualNetwork.

Address space Enter 10.1.0.0/16.

Subscription Select your subscription.

Resource group Select Create new, enter myResourceGroup, then select OK.

Location Select East US.

Subnet - Name Enter myVirtualSubnet.

Subnet - Address range Enter 10.1.0.0/24.

Leave the rest of the defaults and select Create.

Create virtual machines

Create two VMs in the virtual network:

Create the first VM

On the upper-left side of the screen, select Create a resource > Compute > Windows Server 2016 Datacenter.

In Create a virtual machine - Basics, enter or select this information:

Setting Value

PROJECT DETAILS

Subscription Select your subscription.

Resource group Select MyResourceGroup. You created it in the last section.

INSTANCE DETAILS

Virtual machine name Enter myVm1.

Region Select East US.

Availability options Leave the default No infrastructure redundancy required.

Image Leave the default Windows Server 2016 Datacenter.

Size Leave the default Standard DS1 v2.

ADMINISTRATOR ACCOUNT

Username Enter a user name of your choosing.

Password Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements.

Confirm Password Reenter password.

INBOUND PORT RULES

Public inbound ports Leave the default None.

SAVE MONEY

Already have a Windows license? Leave the default No.

Select Next : Disks.

In Create a virtual machine - Disks, leave the defaults and select Next : Networking.

In Create a virtual machine - Networking, select this information:

Setting Value

Virtual network Leave the default myVirtualNetwork.

Subnet Leave the default myVirtualSubnet (10.1.0.0/24).

Public IP Leave the default (new) myVm-ip.

Network security ports Select Allow selected ports.

Select inbound ports Select HTTP and RDP.

Select Next : Management.

In Create a virtual machine - Management, for Diagnostics storage account, select Create New.

In Create storage account, enter or select this information:

Setting Value

Name Enter myvmstorageaccount.

Account kind Leave the default Storage (general purpose v1).

Performance Leave the default Standard.

Replication Leave the default Locally-redundant storage (LRS).

Select OK

Select Review + create. You're taken to the Review + create page and Azure validates your configuration.

When you see that Validation passed, select Create.

Create the second VM

Complete steps 1 and 9 from above.

Note

In step 2, for the Virtual machine name, enter myVm2.

In step 7, for Diagnosis storage account, make sure you select myvmstorageaccount.

Select Review + create. You're taken to the Review + create page and Azure validates your configuration.

When you see that Validation passed, select Create.

Connect to a VM from the internet

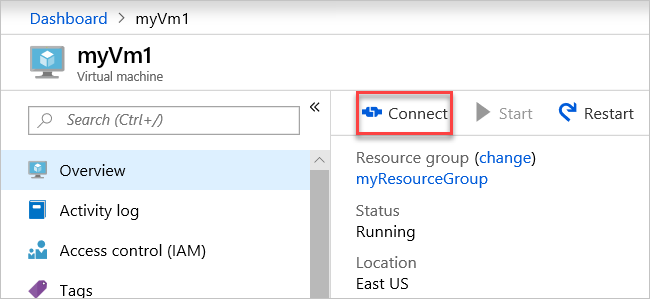
After you've created myVm1, connect to it over the internet.

In the portal's search bar, enter myVm1.

Select the Connect button.

Connect to a virtual machine

After selecting the Connect button, Connect to virtual machine opens.



Select Download RDP File. Azure creates a Remote Desktop Protocol (.rdp) file and downloads it to your computer.

Open the downloaded .rdp file.

If prompted, select Connect.

Enter the user name and password you specified when creating the VM.

Note

You may need to select More choices > Use a different account, to specify the credentials you entered when you created the VM.

Select OK.

You may receive a certificate warning during the sign in process. If you receive a certificate warning, select Yes or Continue.

Once the VM desktop appears, minimize it to go back to your local desktop.

Communicate between VMs

In the Remote Desktop of myVm1, open PowerShell.

Enter ping myVm2.

You'll get back something like this message:

PowerShell

Copy

Pinging myVm2.0v0zze1s0uiedpvtxz5z0r0cxg.bx.internal.clouda

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 10.1.0.5:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

The ping fails, because ping uses the Internet Control Message Protocol (ICMP). By default, ICMP isn't allowed through the Windows firewall.

To allow myVm2 to ping myVm1 in a later step, enter this command:

PowerShell

Copy

New-NetFirewallRule –DisplayName “Allow ICMPv4-In” –Protocol ICMPv4

That command allows ICMP inbound through the Windows firewall:

Close the remote desktop connection to myVm1.

Complete the steps in Connect to a VM from the internet again, but connect to myVm2.

From a command prompt, enter ping myvm1.

You'll get back something like this message:

PowerShell

Copy

Pinging myVm1.0v0zze1s0uiedpvtxz5z0r0cxg.bx.internal.cloudapp.net [10.1.0.4] with 32 bytes of data:

Reply from 10.1.0.4: bytes=32 time=1ms TTL=128

Reply from 10.1.0.4: bytes=32 time<1ms TTL=128

Reply from 10.1.0.4: bytes=32 time<1ms TTL=128

Reply from 10.1.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.4:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

You receive replies from myVm1, because you allowed ICMP through the Windows firewall on the myVm1 VM in a previous step.

Close the remote desktop connection to myVm2.

Clean up resources

When you're done with the virtual network, and the VMs, delete the resource group and all of the resources it contains:

Enter myResourceGroup in the Search box at the top of the portal.

When you see myResourceGroup in the search results, select it.

Select Delete resource group.

Enter myResourceGroup for TYPE THE RESOURCE GROUP NAME and select Delete.

Next steps

In this quickstart, you created a default virtual network and two VMs. You connected to one VM from the internet, and communicated privately between the two VMs. To learn more about virtual network settings, see Manage a virtual network.

By default, Azure allows unrestricted private communication between VMs. Conversely, it only allows inbound remote desktop connections to Windows VMs from the internet. To learn more about configuring different types of VM network communications, go to the Filter network traffic tutorial.

Manage VN:

<https://docs.microsoft.com/en-us/azure/virtual-network/manage-virtual-network>

Create, change, or delete a virtual network

01/10/2019

13 minutes to read

Contributors

Jim Dial MSshujia Kent Sharkey Jonathan Gao Alma Jenks all

Note

This article has been updated to use the new Azure PowerShell Az module. To learn more about the new Az module and AzureRM compatibility, see Introducing the new Azure PowerShell Az module. For installation instructions, see Install Azure PowerShell.

Learn how to create and delete a virtual network and change settings, like DNS servers and IP address spaces, for an existing virtual network. If you're new to virtual networks, you can learn more about them in the Virtual network overview or by completing a tutorial. A virtual network contains subnets. To learn how to create, change, and delete subnets, see Manage subnets.

Before you begin

Complete the following tasks before completing steps in any section of this article:

If you don't already have an Azure account, sign up for a free trial account.

If using the portal, open https://portal.azure.com, and log in with your Azure account.

If using PowerShell commands to complete tasks in this article, either run the commands in the Azure Cloud Shell, or by running PowerShell from your computer. The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account. This tutorial requires the Azure PowerShell module version 1.0.0 or later. Run Get-Module -ListAvailable Az to find the installed version. If you need to upgrade, see Install Azure PowerShell module. If you are running PowerShell locally, you also need to run Connect-AzAccount to create a connection with Azure.

If using Azure Command-line interface (CLI) commands to complete tasks in this article, either run the commands in the Azure Cloud Shell, or by running the CLI from your computer. This tutorial requires the Azure CLI version 2.0.31 or later. Run az --version to find the installed version. If you need to install or upgrade, see Install Azure CLI. If you are running the Azure CLI locally, you also need to run az login to create a connection with Azure.

The account you log into, or connect to Azure with, must be assigned to the network contributor role or to a custom role that is assigned the appropriate actions listed in Permissions.

Create a virtual network

Select + Create a resource > Networking > Virtual network.

Enter or select values for the following settings, then select Create:

Name: The name must be unique in the resource group that you select to create the virtual network in. You cannot change the name after the virtual network is created. You can create multiple virtual networks over time. For naming suggestions, see Naming conventions. Following a naming convention can help make it easier to manage multiple virtual networks.

Address space: The address space for a virtual network is composed of one or more non-overlapping address ranges that are specified in CIDR notation. The address range you define can be public or private (RFC 1918). Whether you define the address range as public or private, the address range is reachable only from within the virtual network, from interconnected virtual networks, and from any on-premises networks that you have connected to the virtual network. You cannot add the following address ranges:

224.0.0.0/4 (Multicast)

255.255.255.255/32 (Broadcast)

127.0.0.0/8 (Loopback)

169.254.0.0/16 (Link-local)

168.63.129.16/32 (Internal DNS, DHCP, and Azure Load Balancer health probe)

Although you can define only one address range when you create the virtual network, you can add more address ranges to the address space after the virtual network is created. To learn how to add an address range to an existing virtual network, see Add or remove an address range.

Warning

If a virtual network has address ranges that overlap with another virtual network or on-premises network, the two networks cannot be connected. Before you define an address range, consider whether you might want to connect the virtual network to other virtual networks or on-premises networks in the future.

Subnet name: The subnet name must be unique within the virtual network. You cannot change the subnet name after the subnet is created. The portal requires that you define one subnet when you create a virtual network, even though a virtual network isn't required to have any subnets. In the portal, you can define only one subnet when you create a virtual network. You can add more subnets to the virtual network later, after the virtual network is created. To add a subnet to a virtual network, see Manage subnets. You can create a virtual network that has multiple subnets by using Azure CLI or PowerShell.

Tip

Sometimes, administrators create different subnets to filter or control traffic routing between the subnets. Before you define subnets, consider how you might want to filter and route traffic between your subnets. To learn more about filtering traffic between subnets, see Network security groups. Azure automatically routes traffic between subnets, but you can override Azure default routes. To learn more about Azures default subnet traffic routing, see Routing overview.

Subnet address range: The range must be within the address space you entered for the virtual network. The smallest range you can specify is /29, which provides eight IP addresses for the subnet. Azure reserves the first and last address in each subnet for protocol conformance. Three additional addresses are reserved for Azure service usage. As a result, a virtual network with a subnet address range of /29 has only three usable IP addresses. If you plan to connect a virtual network to a VPN gateway, you must create a gateway subnet. Learn more about specific address range considerations for gateway subnets. You can change the address range after the subnet is created, under specific conditions. To learn how to change a subnet address range, see Manage subnets.

Subscription: Select a subscription. You cannot use the same virtual network in more than one Azure subscription. However, you can connect a virtual network in one subscription to virtual networks in other subscriptions with virtual network peering. Any Azure resource that you connect to the virtual network must be in the same subscription as the virtual network.

Resource group: Select an existing resource group or create a new one. An Azure resource that you connect to the virtual network can be in the same resource group as the virtual network or in a different resource group.

Location: Select an Azure location, also known as a region. A virtual network can be in only one Azure location. However, you can connect a virtual network in one location to a virtual network in another location by using a VPN gateway. Any Azure resource that you connect to the virtual network must be in the same location as the virtual network.

Commands

Azure CLI: az network vnet create

PowerShell: New-AzVirtualNetwork

View virtual networks and settings

In the search box at the top of the portal, enter virtual networks in the search box. When Virtual networks appear in the search results, select it.

From the list of virtual networks, select the virtual network that you want to view settings for.

The following settings are listed for the virtual network you selected:

Overview: Provides information about the virtual network, including address space and DNS servers. The following screenshot shows the overview settings for a virtual network named MyVNet:

Network interface overview

You can move a virtual network to a different subscription or resource group by selecting Change next to Resource group or Subscription name. To learn how to move a virtual network, see Move resources to a different resource group or subscription. The article lists prerequisites, and how to move resources by using the Azure portal, PowerShell, and Azure CLI. All resources that are connected to the virtual network must move with the virtual network.

Address space: The address spaces that are assigned to the virtual network are listed. To learn how to add and remove an address range to the address space, complete the steps in Add or remove an address range.

Connected devices: Any resources that are connected to the virtual network are listed. In the preceding screenshot, three network interfaces and one load balancer are connected to the virtual network. Any new resources that you create and connect to the virtual network are listed. If you delete a resource that was connected to the virtual network, it no longer appear in the list.

Subnets: A list of subnets that exist within the virtual network is shown. To learn how to add and remove a subnet, see Manage subnets.

DNS servers: You can specify whether the Azure internal DNS server or a custom DNS server provides name resolution for devices that are connected to the virtual network. When you create a virtual network by using the Azure portal, Azure's DNS servers are used for name resolution within a virtual network, by default. To modify the DNS servers, complete the steps in Change DNS servers in this article.

Peerings: If there are existing peerings in the subscription, they are listed here. You can view settings for existing peerings, or create, change, or delete peerings. To learn more about peerings, see Virtual network peering.

Properties: Displays settings about the virtual network, including the virtual network's resource ID and the Azure subscription it is in.

Diagram: The diagram provides a visual representation of all devices that are connected to the virtual network. The diagram has some key information about the devices. To manage a device in this view, in the diagram, select the device.

Common Azure settings: To learn more about common Azure settings, see the following information:

Activity log

Access control (IAM)

Tags

Locks

Automation script

Commands

Azure CLI: az network vnet show

PowerShell: Get-AzVirtualNetwork

Add or remove an address range

You can add and remove address ranges for a virtual network. An address range must be specified in CIDR notation, and cannot overlap with other address ranges within the same virtual network. The address ranges you define can be public or private (RFC 1918). Whether you define the address range as public or private, the address range is reachable only from within the virtual network, from interconnected virtual networks, and from any on-premises networks that you have connected to the virtual network.

You can decrease the address range for a virtual network if you don't have any subnets associated with it. Otherwise, you can only extend the address range, for example, changing a /16 to /8. You could begin with a small address range, and then extend it later or add additional ranges.

You cannot add the following address ranges:

224.0.0.0/4 (Multicast)

255.255.255.255/32 (Broadcast)

127.0.0.0/8 (Loopback)

169.254.0.0/16 (Link-local)

168.63.129.16/32 (Internal DNS, DHCP, and Azure Load Balancer health probe)

To add or remove an address range:

In the search box at the top of the portal, enter virtual networks in the search box. When Virtual networks appear in the search results, select it.

From the list of virtual networks, select the virtual network for which you want to add or remove an address range.

Select Address space, under SETTINGS.

Complete one of the following options:

Add an address range: Enter the new address range. The address range cannot overlap with an existing address range that is defined for the virtual network.

Remove an address range: On the right of the address range you want to remove, select ..., then select Remove. If a subnet exists in the address range, you cannot remove the address range. To remove an address range, you must first delete any subnets (and any resources in the subnets) that exist in the address range.

Select Save.

Commands

Azure CLI: az network vnet update

PowerShell: Set-AzVirtualNetwork

Change DNS servers

All VMs that are connected to the virtual network register with the DNS servers that you specify for the virtual network. They also use the specified DNS server for name resolution. Each network interface (NIC) in a VM can have its own DNS server settings. If a NIC has its own DNS server settings, they override the DNS server settings for the virtual network. To learn more about NIC DNS settings, see Network interface tasks and settings. To learn more about name resolution for VMs and role instances in Azure Cloud Services, see Name resolution for VMs and role instances. To add, change, or remove a DNS server:

In the search box at the top of the portal, enter virtual networks in the search box. When Virtual networks appear in the search results, select it.

From the list of virtual networks, select the virtual network for which you want to change DNS servers for.

Select DNS servers, under SETTINGS.

Select one of the following options:

Default (Azure-provided): All resource names and private IP addresses are automatically registered to the Azure DNS servers. You can resolve names between any resources that are connected to the same virtual network. You cannot use this option to resolve names across virtual networks. To resolve names across virtual networks, you must use a custom DNS server.

Custom: You can add one or more servers, up to the Azure limit for a virtual network. To learn more about DNS server limits, see Azure limits. You have the following options:

Add an address: Adds the server to your virtual network DNS servers list. This option also registers the DNS server with Azure. If you've already registered a DNS server with Azure, you can select that DNS server in the list.

Remove an address: Next to the server that you want to remove, select ..., then Remove. Deleting the server removes the server only from this virtual network list. The DNS server remains registered in Azure for your other virtual networks to use.

Reorder DNS server addresses: It's important to verify that you list your DNS servers in the correct order for your environment. DNS server lists are used in the order that they are specified. They do not work as a round-robin setup. If the first DNS server in the list can be reached, the client uses that DNS server, regardless of whether the DNS server is functioning properly. Remove all the DNS servers that are listed, and then add them back in the order that you want.

Change an address: Highlight the DNS server in the list, and then enter the new address.

Select Save.

Restart the VMs that are connected to the virtual network, so they are assigned the new DNS server settings. VMs continue to use their current DNS settings until they are restarted.

Commands

Azure CLI: az network vnet update

PowerShell: Set-AzVirtualNetwork

Delete a virtual network

You can delete a virtual network only if there are no resources connected to it. If there are resources connected to any subnet within the virtual network, you must first delete the resources that are connected to all subnets within the virtual network. The steps you take to delete a resource vary depending on the resource. To learn how to delete resources that are connected to subnets, read the documentation for each resource type you want to delete. To delete a virtual network:

In the search box at the top of the portal, enter virtual networks in the search box. When Virtual networks appear in the search results, select it.

From the list of virtual networks, select the virtual network you want to delete.

Confirm that there are no devices connected to the virtual network by selecting Connected devices, under SETTINGS. If there are connected devices, you must delete them before you can delete the virtual network. If there are no connected devices, select Overview.

Select Delete.

To confirm the deletion of the virtual network, select Yes.

Commands

Azure CLI: azure network vnet delete

PowerShell: Remove-AzVirtualNetwork

Permissions

To perform tasks on virtual networks, your account must be assigned to the network contributor role or to a custom role that is assigned the appropriate actions listed in the following table:

Action Name

Microsoft.Network/virtualNetworks/read Read a virtual Network

Microsoft.Network/virtualNetworks/write Create or update a virtual network

Microsoft.Network/virtualNetworks/delete Delete a virtual network

Tutorial: Filter network traffic with a network security group using the Azure Portal

<https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic>

You can filter network traffic inbound to and outbound from a virtual network subnet with a network security group. Network security groups contain security rules that filter network traffic by IP address, port, and protocol. Security rules are applied to resources deployed in a subnet. In this tutorial, you learn how to:

Create a network security group and security rules

Create a virtual network and associate a network security group to a subnet

Deploy virtual machines (VM) into a subnet

Test traffic filters

If you prefer, you can complete this tutorial using the Azure CLI or PowerShell.

If you don't have an Azure subscription, create a free account before you begin.

Sign in to Azure

Sign in to the Azure portal at https://portal.azure.com.

Create a virtual network

Select + Create a resource on the upper, left corner of the Azure portal.

Select Networking, and then select Virtual network.

Enter, or select, the following information, accept the defaults for the remaining settings, and then select Create:

Setting Value

Name myVirtualNetwork

Address space 10.0.0.0/16

Subscription Select your subscription.

Resource group Select Create new and enter myResourceGroup.

Location Select East US.

Subnet- Name mySubnet

Subnet - Address range 10.0.0.0/24

Create application security groups

An application security group enables you to group together servers with similar functions, such as web servers.

Select + Create a resource on the upper, left corner of the Azure portal.

In the Search the Marketplace box, enter Application security group. When Application security group appears in the search results, select it, select Application security group again under Everything, and then select Create.

Enter, or select, the following information, and then select Create:

Setting Value

Name myAsgWebServers

Subscription Select your subscription.

Resource group Select Use existing and then select myResourceGroup.

Location East US

Complete step 3 again, specifying the following values:

Setting Value

Name myAsgMgmtServers

Subscription Select your subscription.

Resource group Select Use existing and then select myResourceGroup.

Location East US

Create a network security group

Select + Create a resource on the upper, left corner of the Azure portal.

Select Networking, and then select Network security group.

Enter, or select, the following information, and then select Create:

Setting Value

Name myNsg

Subscription Select your subscription.

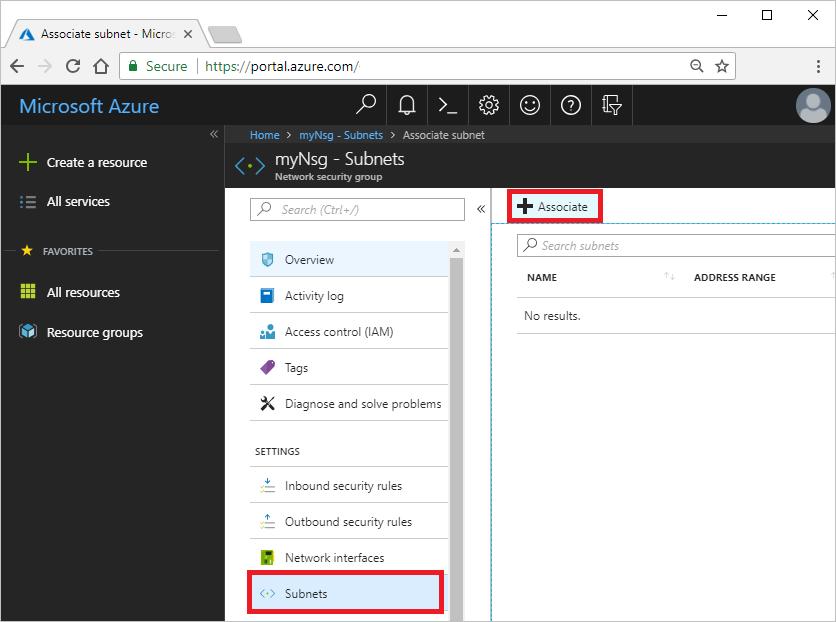
Resource group Select Use existing and then select myResourceGroup.

Location East US

Associate network security group to subnet

In the Search resources, services, and docs box at the top of the portal, begin typing myNsg. When myNsg appears in the search results, select it.

Under SETTINGS, select Subnets and then select + Associate, as shown in the following picture:



Associate NSG to subnet

Under Associate subnet, select Virtual network and then select myVirtualNetwork. Select Subnet, select mySubnet, and then select OK.

Create security rules

Under SETTINGS, select Inbound security rules and then select + Add, as shown in the following picture:

Add an inbound security rule

Create a security rule that allows ports 80 and 443 to the myAsgWebServers application security group. Under Add inbound security rule, enter, or select the following values, accept the remaining defaults, and then select Add:

Setting Value

Destination Select Application security group, and then select myAsgWebServers for Application security group.

Destination port ranges Enter 80,443

Protocol Select TCP

Name Allow-Web-All

Complete step 2 again, using the following values:

Setting Value

Destination Select Application security group, and then select myAsgMgmtServers for Application security group.

Destination port ranges Enter 3389

Protocol Select TCP

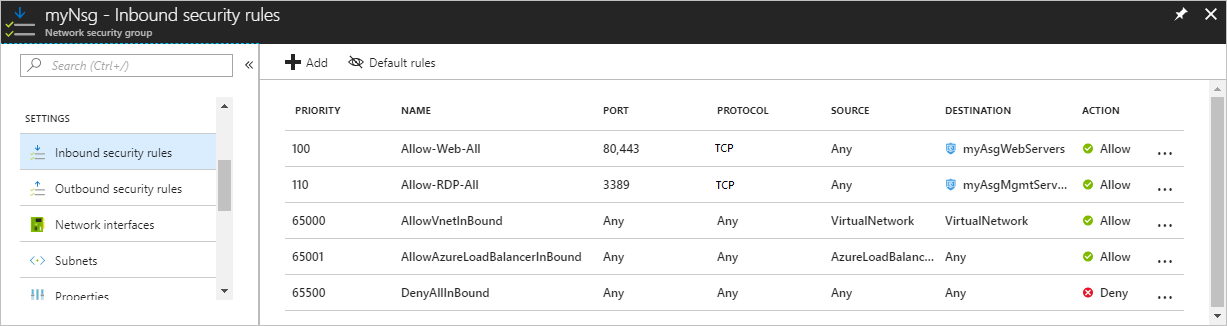
Priority Enter 110

Name Allow-RDP-All

In this tutorial, RDP (port 3389) is exposed to the internet for the VM that is assigned to the myAsgMgmtServers application security group. For production environments, instead of exposing port 3389 to the internet, it's recommended that you connect to Azure resources that you want to manage using a VPN or private network connection.

Once you've completed steps 1-3, review the rules you created. Your list should look like the list in the following picture:

Security rules



Create virtual machines

Create two VMs in the virtual network.

Create the first VM

Select + Create a resource found on the upper, left corner of the Azure portal.

Select Compute, and then select Windows Server 2016 Datacenter.

Enter, or select, the following information, accept the defaults for the remaining settings, and then select OK:

Setting Value

Name myVmWeb

User name Enter a user name of your choosing.

Password Enter a password of your choosing. The password must be at least 12 characters long and meet the defined complexity requirements.

Subscription Select your subscription.

Resource group Select Use existing and select myResourceGroup.

Location Select East US

Select a size for the VM and then select Select.

Under Settings, select the following values, accept the remaining defaults, and then select OK:

Setting Value

Virtual network Select myVirtualNetwork

Network Security Group Select Advanced.

Network security group (firewall) Select (new) myVmWeb-nsg, and then under Choose network security group, select None.

Under Create of the Summary, select Create to start VM deployment.

Create the second VM

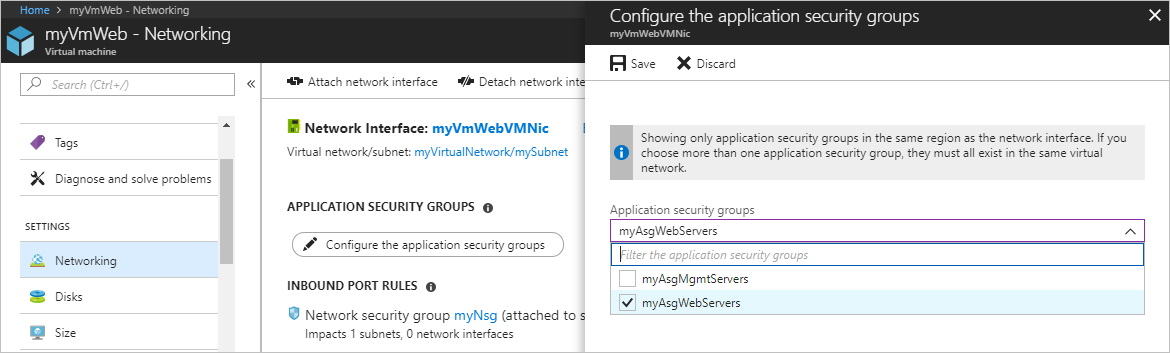
Complete steps 1-6 again, but in step 3, name the VM myVmMgmt. The VM takes a few minutes to deploy. Do not continue to the next step until the VM is deployed.

Associate network interfaces to an ASG

When the portal created the VMs, it created a network interface for each VM, and attached the network interface to the VM. Add the network interface for each VM to one of the application security groups you created previously:

In the Search resources, services, and docs box at the top of the portal, begin typing myVmWeb. When the myVmWeb VM appears in the search results, select it.

Under SETTINGS, select Networking. Select Configure the application security groups, select myAsgWebServers for Application security groups, and then select Save, as shown in the following picture:



Associate to ASG

Complete steps 1 and 2 again, searching for the myVmMgmt VM and selecting the myAsgMgmtServers ASG.

Test traffic filters

Connect to the myVmMgmt VM. Enter myVmMgmt in the search box at the top of the portal. When myVmMgmt appears in the search results, select it. Select the Connect button.

Select Download RDP file.

Open the downloaded rdp file and select Connect. Enter the user name and password you specified when creating the VM. You may need to select More choices, then Use a different account, to specify the credentials you entered when you created the VM.

Select OK.

You may receive a certificate warning during the sign-in process. If you receive the warning, select Yes or Continue, to proceed with the connection.

The connection succeeds, because port 3389 is allowed inbound from the internet to the myAsgMgmtServers application security group that the network interface attached to the myVmMgmt VM is in.

Connect to the myVmWeb VM from the myVmMgmt VM by entering the following command in a PowerShell session:

Copy

mstsc /v:myVmWeb

You are able to connect to the myVmWeb VM from the myVmMgmt VM because VMs in the same virtual network can communicate with each other over any port, by default. You can't however, create a remote desktop connection to the myVmWeb VM from the internet, because the security rule for the myAsgWebServers doesn't allow port 3389 inbound from the internet and inbound traffic from the Internet is denied to all resources, by default.

To install Microsoft IIS on the myVmWeb VM, enter the following command from a PowerShell session on the myVmWeb VM:

PowerShell

Copy

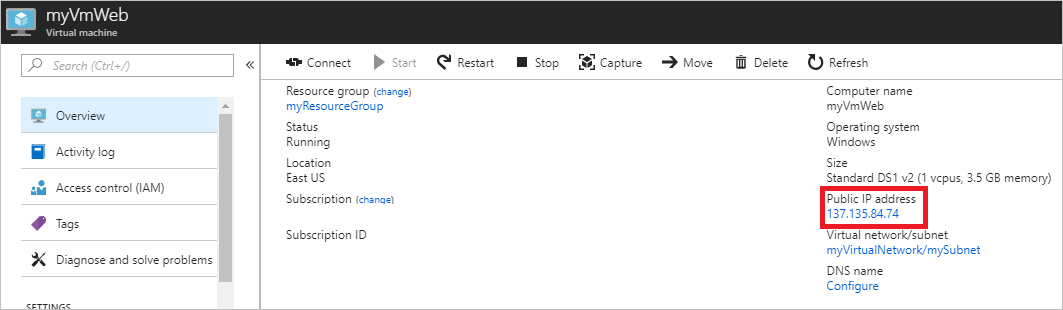
Install-WindowsFeature -name Web-Server -IncludeManagementTools

After the IIS installation is complete, disconnect from the myVmWeb VM, which leaves you in the myVmMgmt VM remote desktop connection.

Disconnect from the myVmMgmt VM.

In the Search resources, services, and docs box at the top of the Azure portal, begin typing myVmWeb from your computer. When myVmWeb appears in the search results, select it. Note the Public IP address for your VM. The address shown in the following picture is 137.135.84.74, but your address is different:

Public IP address



To confirm that you can access the myVmWeb web server from the internet, open an internet browser on your computer and browse to http://<public-ip-address-from-previous-step>. You see the IIS welcome screen, because port 80 is allowed inbound from the internet to the myAsgWebServers application security group that the network interface attached to the myVmWeb VM is in.

Clean up resources

When no longer needed, delete the resource group and all of the resources it contains:

Enter myResourceGroup in the Search box at the top of the portal. When you see myResourceGroup in the search results, select it.

Select Delete resource group.

Enter myResourceGroup for TYPE THE RESOURCE GROUP NAME: and select Delete.

Next steps

In this tutorial, you created a network security group and associated it to a virtual network subnet. To learn more about network security groups, see Network security group overview and Manage a network security group.

Azure routes traffic between subnets by default. You may instead, choose to route traffic between subnets through a VM, serving as a firewall, for example. To learn how to create a route table, advance to the next tutorial.