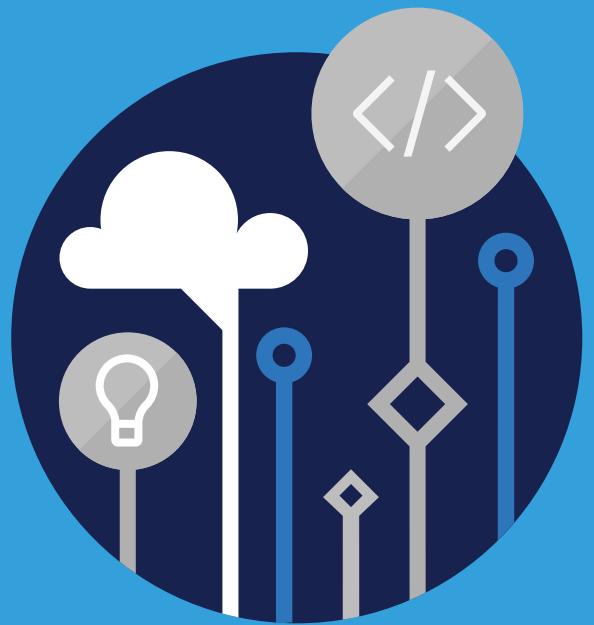


Microsoft
Official
Course



AZ-900T01

Microsoft Azure
Fundamentals

AZ-900T01

Microsoft Azure Fundamentals

MCT USE ONLY. STUDENT USE PROHIBITED

MCT USE ONLY. STUDENT USE PROHIBITED



Contents

■	Module 0 Course Introduction	1
	Course overview	1
■	Module 1 Cloud Concepts	3
	Learning Objectives	3
	Why Cloud Services	4
	Types of Cloud models	8
	Types of Cloud Services	13
	Module 1 Review Questions	19
	Module 1 Summary	22
■	Module 2 Core Azure Services	27
	Learning Objectives	27
	Core Azure Architectural components	28
	Core Azure Services and Products	36
	Azure Solutions	86
	Azure Management Tools	105
	Module 2 Review Questions	138
	Module 2 Summary	141
■	Module 3 Security, Privacy, Compliance and Trust	145
	Learning Objectives	145
	Securing network connectivity in Azure	146
	Core Azure Identity services	191
	Security Tools and Features	194
	Azure Governance methodologies	219
	Monitoring and Reporting in Azure	250
	Privacy, Compliance and Data Protection standards in Azure	282
	Module 3 Review Questions	296
	Module 3 Summary	299
■	Module 4 Azure Pricing and Support	305
	Learning Objectives	305
	Azure Subscriptions	306
	Planning and Managing costs	329
	Support Options Available with Azure	351
	Azure Service Level Agreements (SLAs)	365

Service Lifecycle in Azure	375
Module 4 Review Questions	389
Module 4 Summary	392

Module 0 Course Introduction

Course overview

Video: About this Course



<https://www.youtube.com/watch?v=VseQkSTtUPQ>

References

Core sources of reference which are used in this course and which may be of use to you are:

- [Microsoft Azure Homepage¹](https://azure.microsoft.com/en-us/)
- [Microsoft Azure Documentation site²](https://docs.microsoft.com/en-us/azure/)

Demo: Create Free Azure Account



https://www.youtube.com/watch?v=H53yVpKB3_c

¹ <https://azure.microsoft.com/en-us/>

² <https://docs.microsoft.com/en-us/azure/>

MCT USE ONLY. STUDENT USE PROHIBITED

Module 1 Cloud Concepts

Learning Objectives

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).

Why Cloud Services

Video: Cloud Services



<https://www.youtube.com/watch?v=bVoREzbC7rk>

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 to 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 to 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 expertise 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?](#)¹ and there is also a term reference guide available on the page [Cloud computing Terms](#)², 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.



¹ <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/>

² <https://azure.microsoft.com/en-us/overview/cloud-computing-dictionary/>

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.

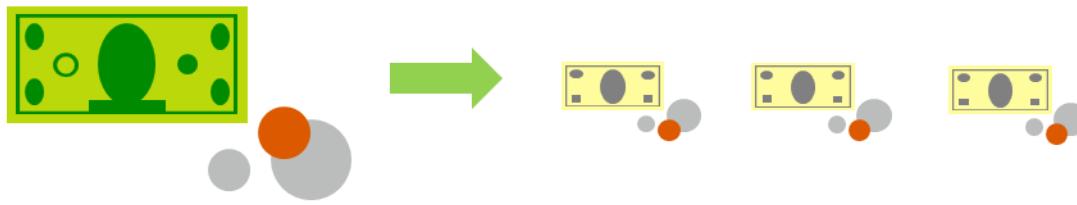
CapEx Vs OpEx

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.

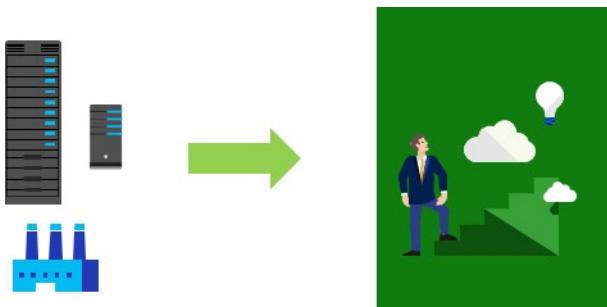
A business can still use the CapEx expenditure strategy if they wish, but it is no longer a requirement that they do so.

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



Types of Cloud models

Video: Cloud Models



https://www.youtube.com/watch?v=Nnn_Un2F8EI

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.

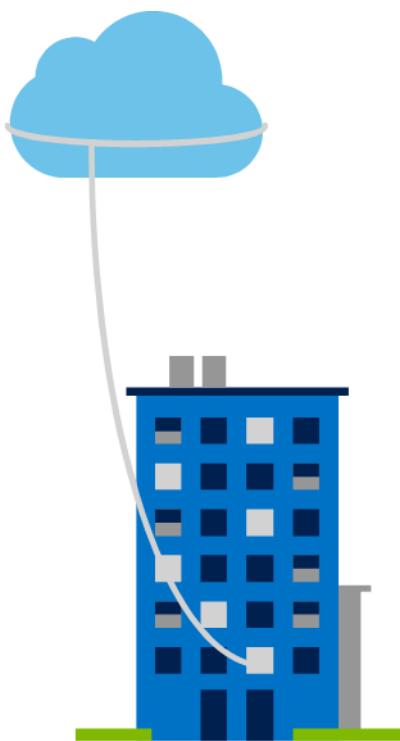
Businesses can use multiple public cloud service provider companies of varying scale. Microsoft Azure is an example of a public cloud provider.

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 cloud³](#)

³ <https://azure.microsoft.com/en-us/overview/hybrid-cloud/>

Video: Cloud Model Comparison



https://www.youtube.com/watch?v=4v_7sJnS3LU

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 require 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.

Types of Cloud Services

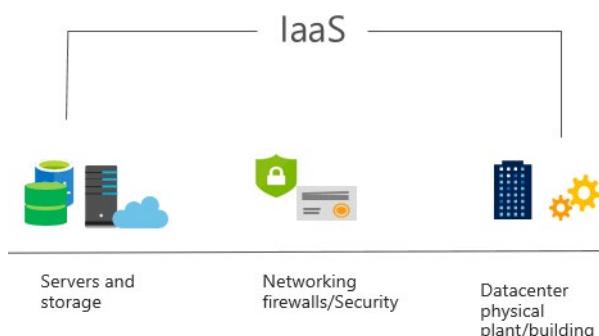
Video: Types of Cloud Services



<https://www.youtube.com/watch?v=JQ2RHPeJYSA>

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.

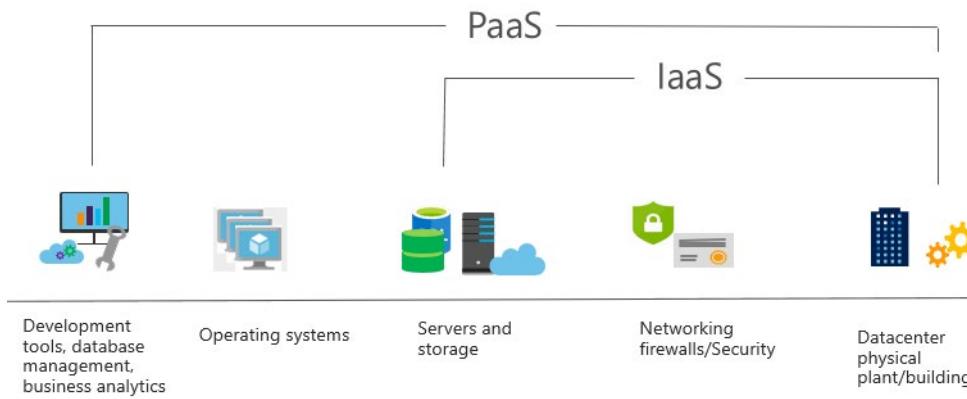
- **Website hosting.** Running websites using IaaS can be less expensive than traditional web hosting.
- **Storage, backup, and recovery.** Organizations avoid the capital outlay and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance 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?](#)⁴

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,

⁴ <https://azure.microsoft.com/en-us/overview/what-is-iaas/>

high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.

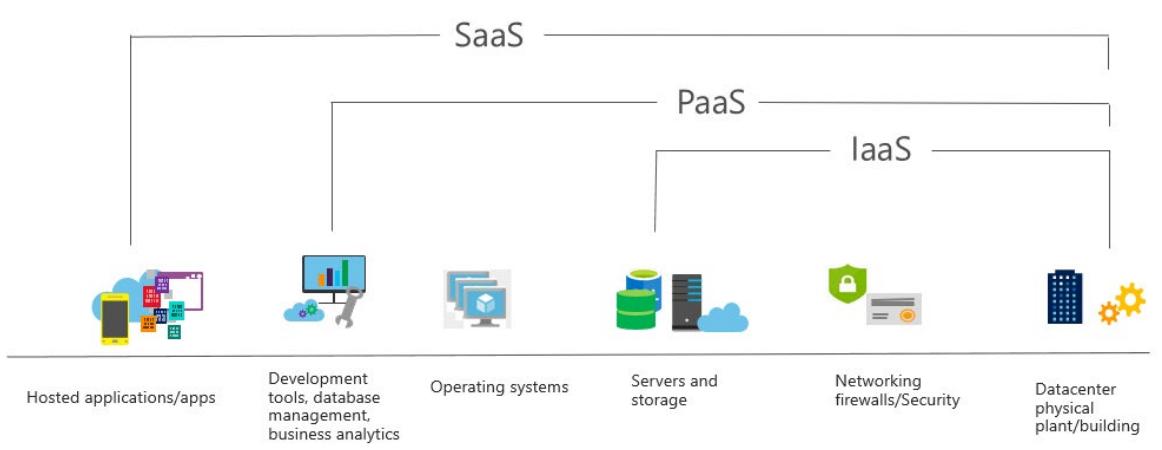
- **Analytics or business intelligence.** Tools provided as a service with PaaS allow organizations to analyze and mine their data. They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

Note: For more information on PaaS see the page [What is PaaS?](#)⁵

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?](#)⁶

Cloud Service Comparison

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

⁵ <https://azure.microsoft.com/en-us/overview/what-is-paas/>

⁶ <https://azure.microsoft.com/en-us/overview/what-is-saas/>

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 are 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 are 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.
- **Flexibility.** 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.

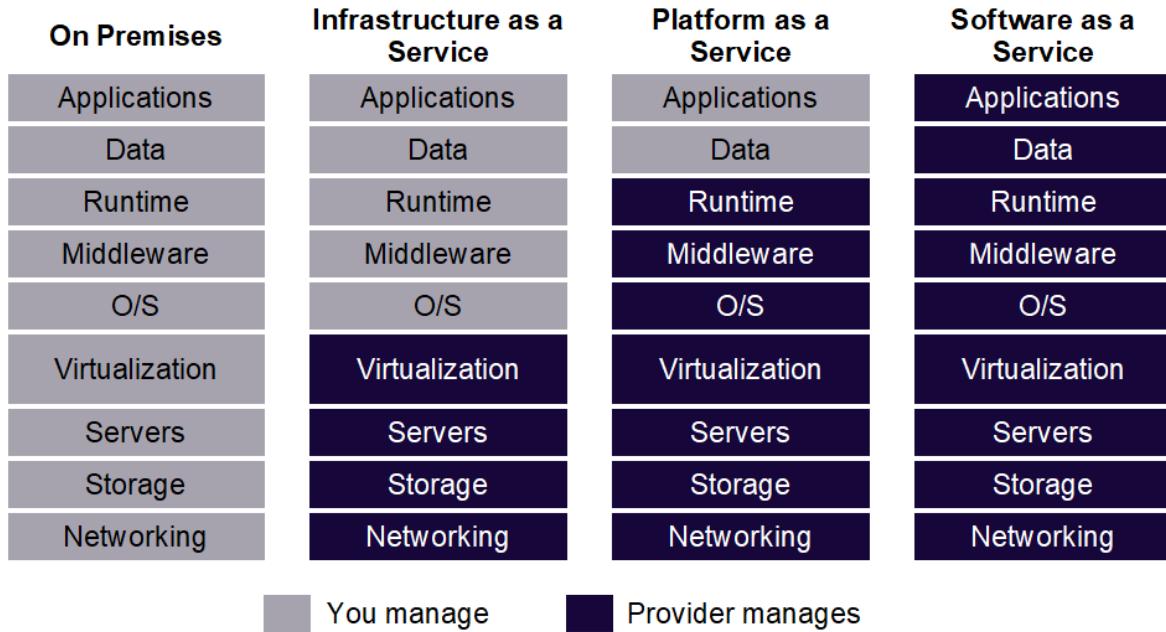
Summary

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.

Module 1 Review Questions

Cloud Concepts Review Questions

About review questions

End-of-module review questions are for practice only and are not included in your grade for the course. The final assessment at the end of the course is graded.

Review Question 1

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

(Choose three)

- 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

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

- Performance
- High Availability
- Fault Tolerance
- Agility

Review Question 4

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

(choose two)

- Public
- Private
- Hybrid
- Global

Review Question 5

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

- Public
- Private
- Hybrid

Review Question 6

Which cloud model provides the greatest degree of flexibility?

- Public
- Private
- Hybrid

Review Question 7

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

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

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

Module 1 Summary

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.

Answers

Review Question 1

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

(Choose three)

- Elasticity
- Un-predictable costs
- Local reach only
- Agility
- Economies of scale

Explanation

Elasticity, Agility and Economies of scale are the correct answers, and would be seen as benefits that you can gain from using cloud services.

All other answers are incorrect.

Un-predictable costs and local reach only would not be benefits of using cloud services because cloud services does provide predictable costs and global reach.

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)

Explanation

Operational Expenditure (OpEx) is the correct answer. Cloud services operate on an Operational Expenditure model. It is regular, repeated expenditure that you pay for using cloud services.

Capital Expenditure (CapEx) is not the correct answer. Capital Expenditure (CapEx) is not required to be paid upfront when looking to start using a cloud services. There are no up front costs to use cloud services. You pay for what you consume, under a consumption based model.

Friendly expenditure and Maximum expense are not defined expenditure types.

Review Question 3

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

- Performance
- High Availability
- Fault Tolerance
- Agility

Explanation

High Availability is the correct answer. The other answers, while they may be related, are not correct.

Performance is the ability to provide quick and efficient response times to requests.

Fault Tolerance is the ability to survive a failure of a component.

Agility is the ability to react quickly.

Review Question 4

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

(choose two)

- Public
- Private
- Hybrid
- Global

Explanation

Public and Hybrid cloud models use services that can be accessed by the public.

Hybrid cloud has a public and private element, hence the public part is accessible by the public.

Private cloud models is run and owned by an organization for use exclusively for that organization and access is not provided to the public. It may be made available to other 3rd parties depending on the business requirements.

Global is not a valid cloud model.

Review Question 5

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

- Public
- Private
- Hybrid

Explanation

Private cloud models is the correct answer.

Both public and hybrid clouds have an infrastructure that is managed by another party. As such, there is less control over the infrastructure.

Review Question 6

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

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

Explanation

The shared responsibility model is the correct answer. Under the shared responsibility model, management of the resource is shared between the cloud provider and the end user. The cloud provider being responsible for the cloud services infrastructure and the end user being responsible for the service being configured and managed correctly.

The user management model, cloud user management model and no responsibility management model are not valid defined management models.

Review Question 8

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

Explanation

The correct answer is that the 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 applies to IaaS.

Users pay an annual or monthly subscription is applicable to SaaS services.

Review Question 9

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 2 Core Azure Services

Learning Objectives

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.

Core Azure Architectural components

Video: Regions



<https://www.youtube.com/watch?v=dg2Vf1LhhZY>

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 Regions¹](#)

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 available [here²](#).

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.

¹ <https://azure.microsoft.com/en-us/global-infrastructure/regions/>

² <https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions#what-are-paired-regions>

Video: Geographies



<https://www.youtube.com/watch?v=qhpI5lALNig>

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 Geographies for more details³](#).

Video: Availability Zones



<https://www.youtube.com/watch?v=19F5hSdTC8c>

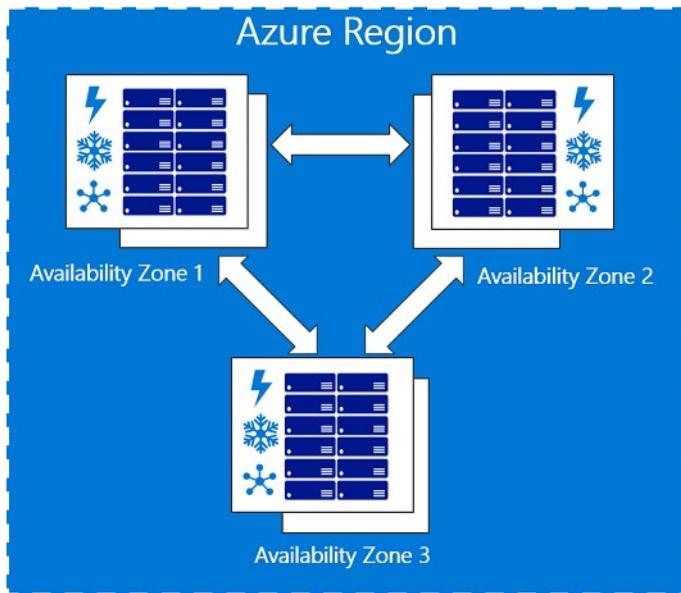
Availability Zones

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.

³ <https://azure.microsoft.com/en-us/global-infrastructure/geographies/>



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

Note: See the page [What are Availability Zones in Azure?](#)⁴ for more details.

Video: Availability Sets



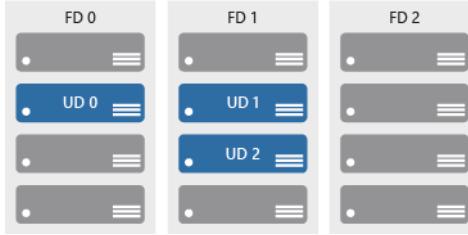
<https://www.youtube.com/watch?v=xV7SRPjLZ0>

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 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.

⁴ <https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>



Video : Resource Groups



<https://www.youtube.com/watch?v=EvJlk4S1Gw>

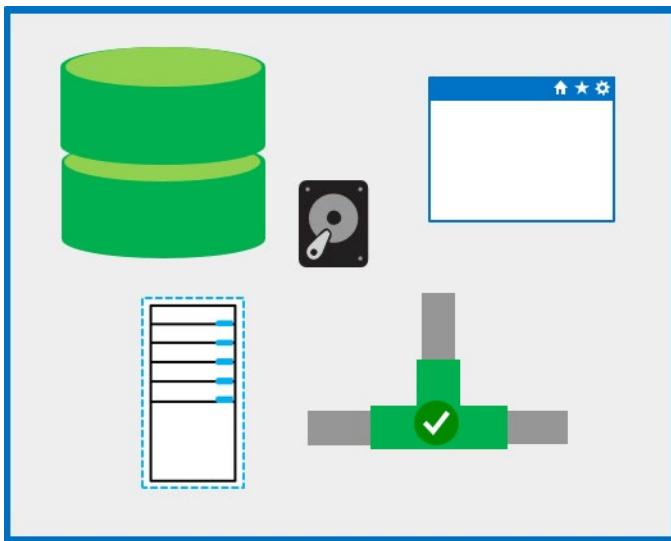
Resource Groups

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.

Video: Azure Resource Manager



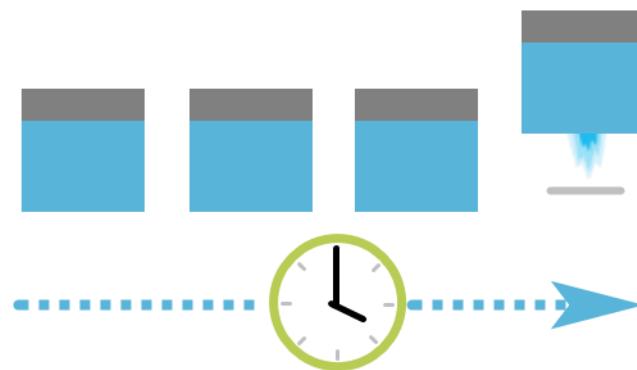
<https://www.youtube.com/watch?v=ygotn3oLnGI>

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:

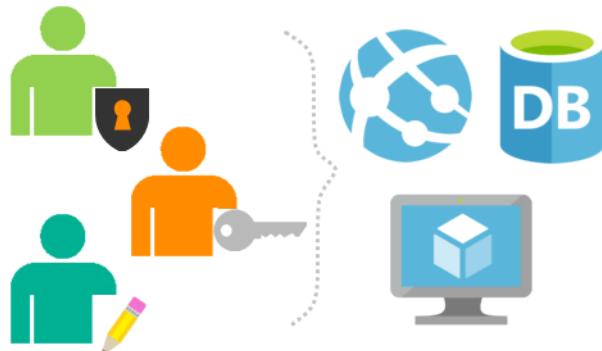
- Deploy Application resources. Update, manage, and delete all the resources for your solution in a single, coordinated operation.



- 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 Manager⁵](#) for more details.

MCT USE ONLY. STUDENT USE PROHIBITED

⁵ <https://azure.microsoft.com/en-us/features/resource-manager/>

Core Azure Services and Products

Video: Azure Compute Services



<https://www.youtube.com/watch?v=8B-HW6wPCPg>

Azure Compute Service

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 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**⁶ for more details.

⁶ <https://azure.microsoft.com/en-us/services/virtual-machines/>

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**⁷ 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**⁸ 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**⁹ 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.

⁷ <https://azure.microsoft.com/en-us/services/virtual-machine-scale-sets/>

⁸ <https://azure.microsoft.com/en-us/services/app-service/>

⁹ <https://azure.microsoft.com/en-us/services/functions/>

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 Instances¹⁰](#) 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 \(AKS\)¹¹](#) for more details.

Note: For a full list of compute services available with Azure and the context on when to use them, see [Compute¹²](#).

Demo: Create Azure Virtual machine



<https://www.youtube.com/watch?v=rGGfRogOCJQ>

¹⁰ <https://azure.microsoft.com/en-us/services/container-instances/>

¹¹ <https://azure.microsoft.com/en-us/services/kubernetes-service/>

¹² <https://azure.microsoft.com/en-us/product-categories/compute/>

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 today¹³](#) webpage.

Steps

1. Sign in to the Azure portal at [¹⁴](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**.

The screenshot shows the Azure Marketplace search interface. On the left is a sidebar with categories: My Saved List, Everything, Compute, Networking, Storage, Web, Mobile, and Containers. The main area has a search bar containing 'windows server 2016 datacenter'. Below the search bar are filters for Pricing (All), Operating System (All), and Publisher (All). The results section shows three items:

NAME	PUBLISHER	CATEGORY
Windows Server 2016 Datacenter	Microsoft	Compute
Windows Server 2016 Datacenter - with Containers	Microsoft	Compute
[smalldisk] Windows Server 2016 Datacenter	Microsoft	Compute

The first item in the list is highlighted with a red box.

¹³ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

¹⁴ <https://portal.azure.com>

The screenshot shows the Windows Server 2016 Datacenter product page. At the top, it says "Windows Server 2016 Datacenter" and "Microsoft". Below that is a description: "Windows Server 2016 is a comprehensive server operating system designed to run the applications and infrastructure that power your business. It includes built-in layers of security and innovation to help you run traditional and cloud-native applications with confidence. This Server with Desktop Experience image includes all roles including the graphical user interface (GUI)." A note below says "This image can be used with [Azure Hybrid Benefit for Windows Server](#)". There's a "Legal Terms" section with a note about acknowledging Microsoft's terms and privacy statement. A "Save for later" button is visible. At the bottom, there's information about the publisher (Microsoft), useful links (Documentation, Introducing Windows Server 2016, What's New in 2016, Learn more), and a deployment model section with "Resource Manager" selected, "Activate Windows" dropdown, and a "Create" button.

4. 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.

The screenshot shows the "Create a virtual machine" wizard in the Azure portal. The "Basics" tab is selected. The "PROJECT DETAILS" section asks for a subscription ("Pay-As-You-Go") and a resource group ("(New) myResourceGroup"). The "Basics" tab also contains a description of what a virtual machine is and a link to classic VMs.

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

INSTANCE DETAILS

* Virtual machine name ✓

* Region ✓

Availability options ✓

* Image ✓
Browse all images and disks

* Size
1 vcpu, 3.5 GB memory
[Change size](#)

6. 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.

ADMINISTRATOR ACCOUNT

* Username ✓

* Password ✓

* Confirm password ✓ Password and confirm password must match.

7. 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.

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports None Allow selected ports

* Select inbound ports ✓

⚠ These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

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

Create a virtual machine

Basics Disks Networking Management Guest config Tags Review + create

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics i On Off

OS guest diagnostics i On Off

IDENTITY

System assigned managed identity i On Off

AUTO-SHUTDOWN

Enable auto-shutdown i On Off

BACKUP

Enable backup i On Off

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

SAVE MONEY

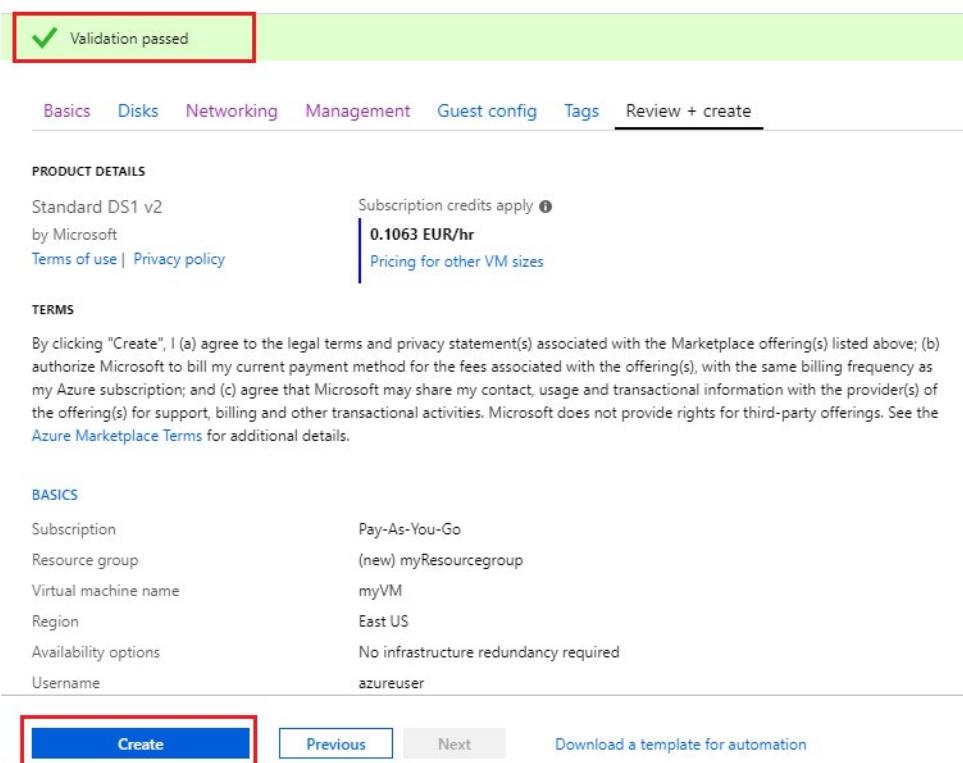
Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

* Already have a Windows license? i Yes No

Review + create Previous Next : Disks >

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

Create a virtual machine



Validation passed

Basics Disks Networking Management Guest config Tags Review + create

PRODUCT DETAILS

Standard DS1 v2 by Microsoft **0.1063 EUR/hr** Subscription credits apply (1) **Pricing for other VM sizes**

TERMS

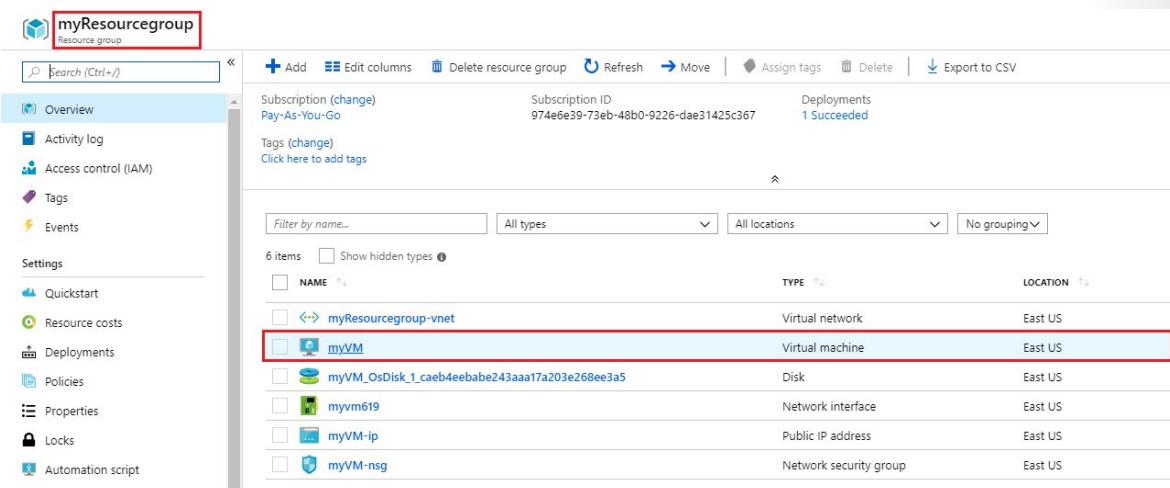
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription	Pay-As-You-Go
Resource group	(new) myResourcegroup
Virtual machine name	myVM
Region	East US
Availability options	No infrastructure redundancy required
Username	azureuser

Create Previous Next Download a template for automation

11. 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.



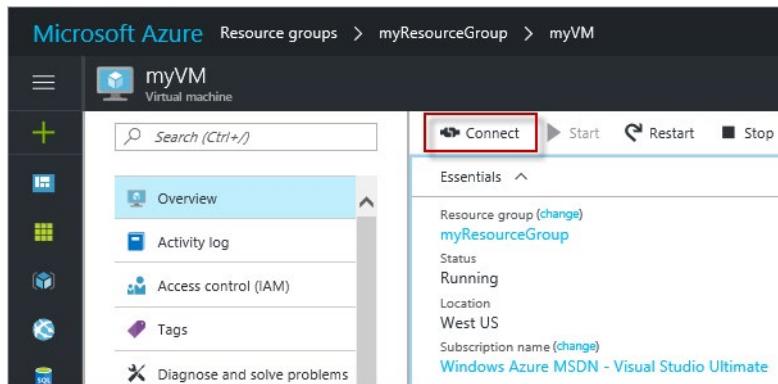
myResourcegroup Resource group

Subscription (change) Pay-As-You-Go Deployment ID 974e6e39-73eb-48b0-9226-dae31425c367 Deployments 1 Succeeded

Tags (change) Click here to add tags

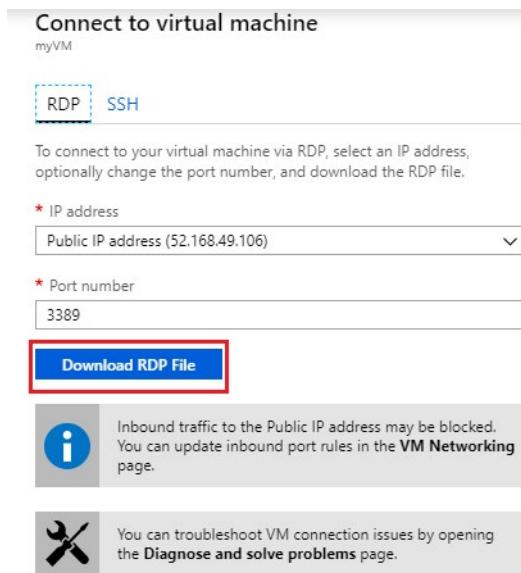
Filter by name... All types All locations No grouping

NAME	TYPE	LOCATION
myResourcegroup-vnet	Virtual network	East US
myVM	Virtual machine	East US
myVM_OsDisk_1_caeb4eebabe243aaa17a203e268ee3a5	Disk	East US
myvm619	Network interface	East US
myVM-ip	Public IP address	East US
myVM-nsg	Network security group	East US

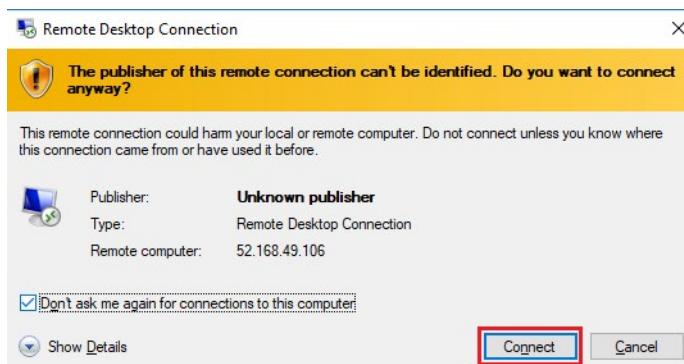


Note: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on Linux virtual machine you could connect directly from a bash shell using `ssh`.

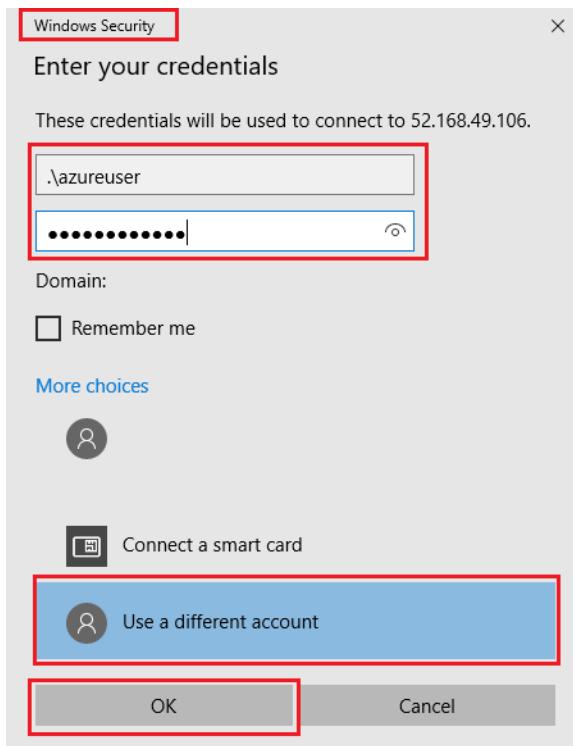
12. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP File**.



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



14. 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**.

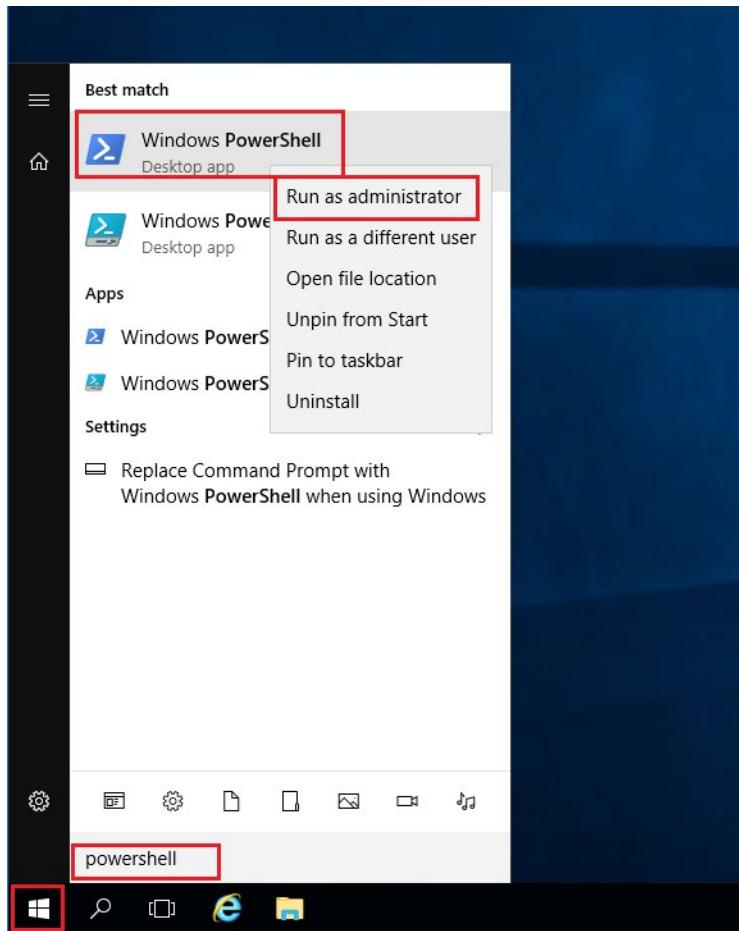


15. You may receive a certificate warning during the sign-in process. Click **Yes** or to create the connection and connect to your deployed VM. You should connect successfully.



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

16. 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**



17. Install the **Web-Server** feature in the virtual machine by running the following command in the PowerShell command prompt:

PowerShell

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

18. 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.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> Install-WindowsFeature -name Web-Server -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- ----- ----- {Common HTTP Features, Default Document, D...
True   No       Success           {Common HTTP Features, Default Document, D...
PS C:\Users\azureuser>

```

19. 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.

myVM

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Networking

Disks

Size

Security

Extensions

Continuous delivery (Preview)

Availability set

Configuration

Resource group (change)
myResourcegroup

Status
Running

Location
East US

Subscription (change)
Pay-As-You-Go

Subscription ID
974e6e39-73eb-48b0-9226-dae31425c367

Computer name
myVM

Operating system
Windows

Size
Standard DS1 v2 8 GB memory

Public IP address
52.168.49.106

Virtual network/subnet
myResourcegroup-vnet/default

DNS name
Configure

Tags (change)
Click here to add tags

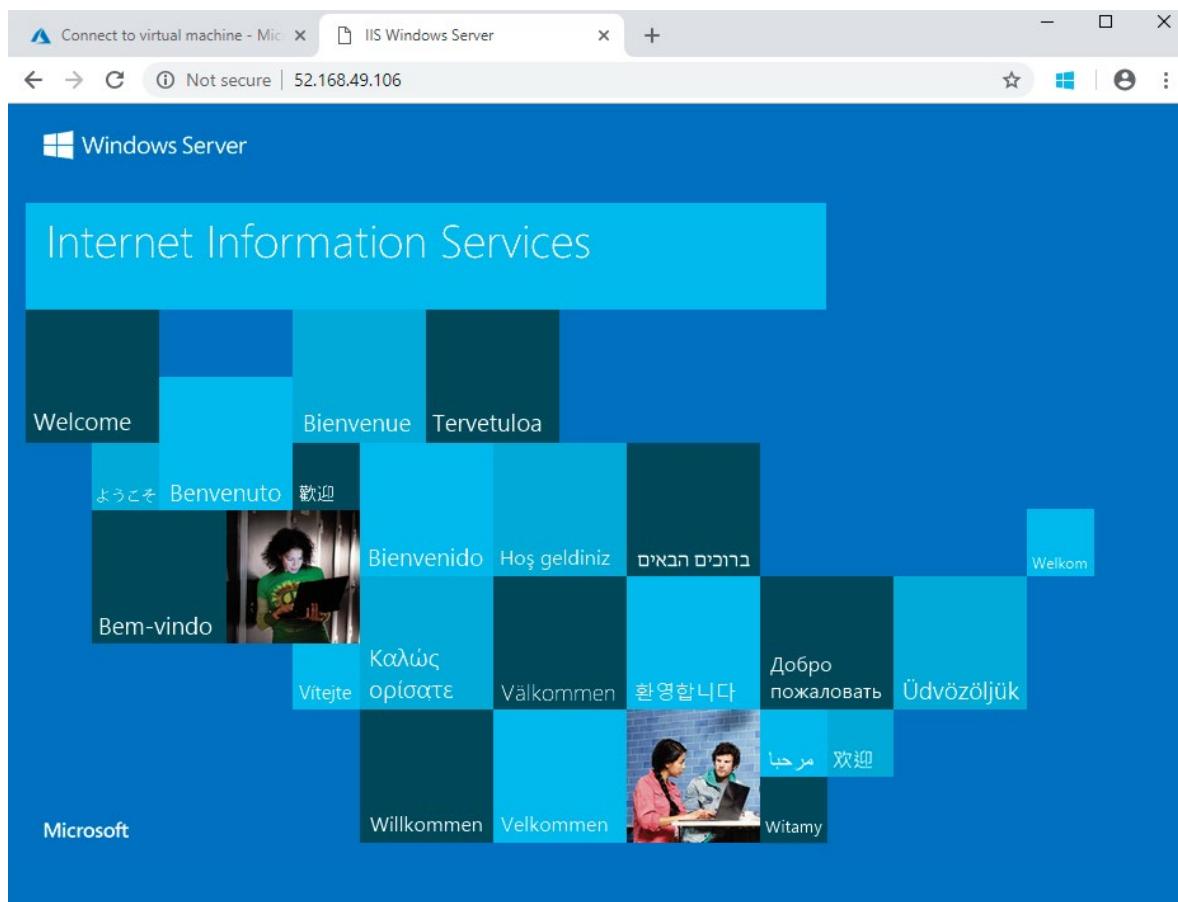
Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

CPU (average)

Network (total)

20. 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.

MCT USE ONLY. STUDENT USE PROHIBITED



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 remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Demo: Deploy Azure Container Instances (ACI) in Azure Portal



<https://www.youtube.com/watch?v=qqTRm3tC2Rw>

Walkthrough-Deploy Azure Container Instances (ACI) in Azure Portal

In this walkthrough, you create, configure, and deploy a Docker container to *Azure Container Instances* (ACI) in Azure Portal. The container is created from an image template called `microsoft/aci-helloworld`. The image packages a small web application, written in Node.js, and serves a static HTML page.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Prerequisites

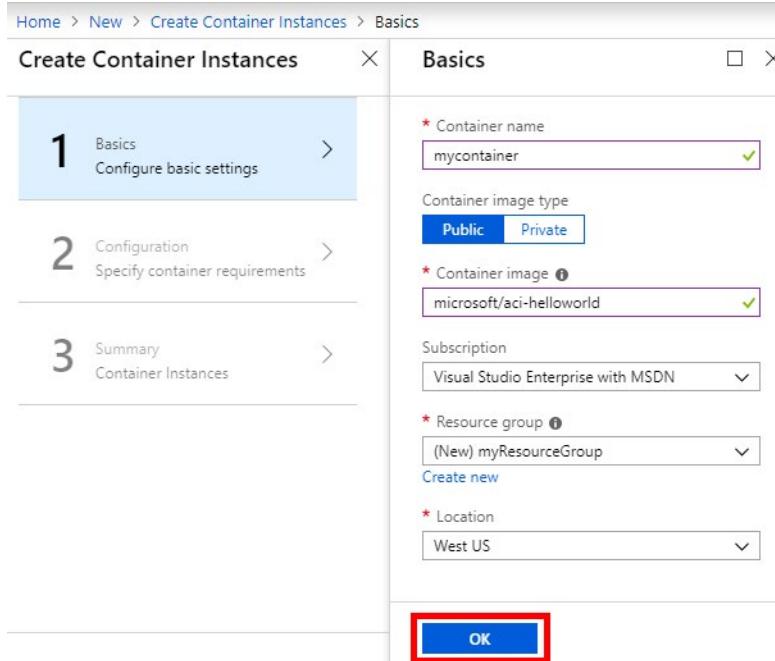
An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**¹⁵ before you begin.

Steps

1. To create a new Azure Container Instance, sign in to the Azure Portal and locate the *Azure Container Instance* service, then select **Create**, or alternatively, click on this **Create Container Instance**¹⁶ link and when prompted, sign into Azure Portal.
2. Provide the following basic details for the new container instance. The UI you encounter may be slightly different compared to the screenshots in this walkthrough, depending on if you accessed the Create New Container Instance via the *Azure portal* or via the *Deploy to Azure* button above, however the details provided will be the same.
 - **Container name:** mycontainer
 - **Container image type:** Public
 - **Container image:** microsoft/aci-helloworld
 - **Subscription:** Choose your subscription.
 - **Resource group:** Select **Create new**, then type myResourceGroup, and select **OK**.
 - **Location:** Use the dropdown to choose the Azure region that is closest to you.
 - Press the **OK** button.

¹⁵ <https://azure.microsoft.com/free/>

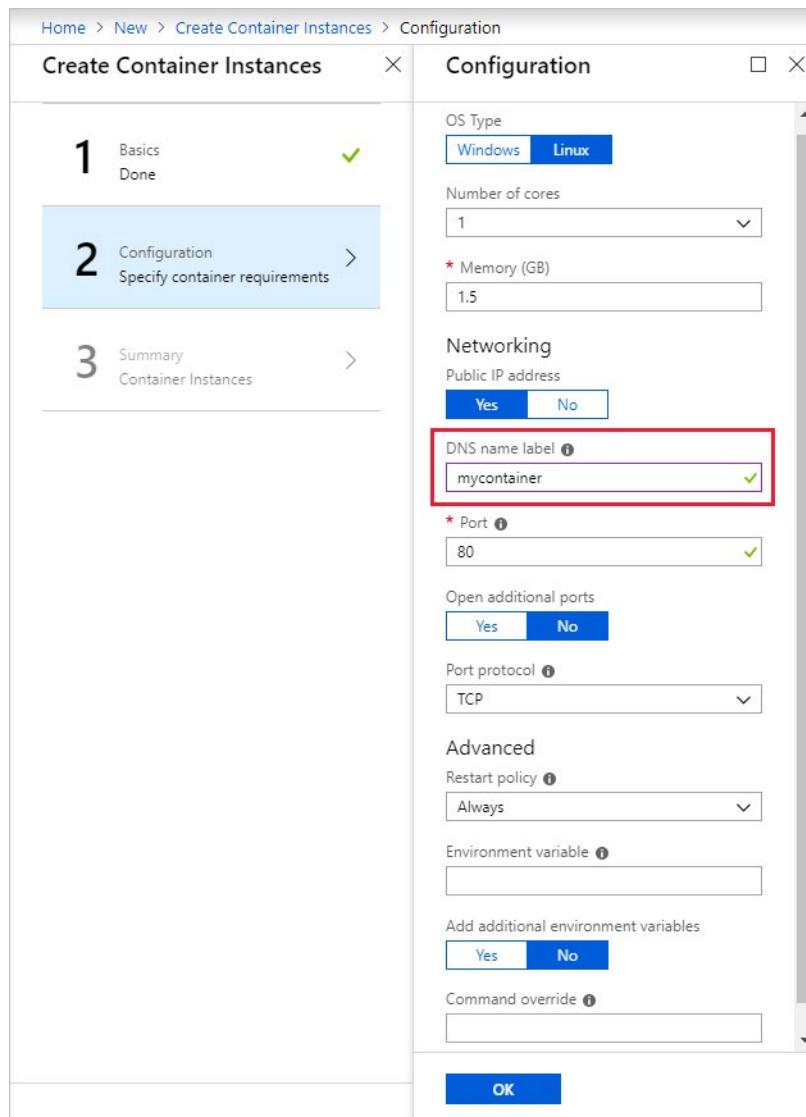
¹⁶ <https://portal.azure.com/#create/microsoft.containerinstances>



3. Configure the new container instance as follows.

- **DNS name label:** Specify a DNS name label for your container. The DNS name label you specify must be unique within the Azure region where you create the container instance. Your container will be publicly reachable at `http://<dns-name-label>.<region>.azurecontainer.io`. If you receive a **DNS name label not available** error message, specify a different DNS name label.
- Leave all other settings in the **Configuration** pane at their default values.
- Select **OK** to start the automatic validation process.

MCT USE ONLY. STUDENT USE PROHIBITED



- When the validation process has passed, review the configuration summary, and select the **OK** button to begin deploying the container.

Create Container Instances

Summary

Validation passed

Basics	Subscription	Visual Studio Enterprise with MSDN
Resource group	myResourceGroup	
Location	East US	
Container name	mycontainer	
Container image type	Public	
Container image	microsoft/aci-helloworld	
Configuration		
OS Type	Linux	
Number of cores	1	
Memory (GB)	1.5	
Public IP address	Yes	
DNS name label	mycontainer	
Port	80	
Open additional ports	No	
Port protocol	TCP	
Restart policy	Always	
Environment variable	-	
Add additional environment va...	No	
Command override	-	

OK Download template and parameters

5. When the deployment starts, a notification appears in Azure Portal indicating the deployment is in progress. Another notification is displayed when the container deployment has completed successfully. Wait for the deployment succeeded notification *before* going to Step 6.



6. Obtain the Fully Qualified Domain Name (FQDN), in Azure Portal, by opening the **Overview** pane for the container group and navigating to **Resource Groups > myResourceGroup > mycontainer**. Make a note of the **FQDN** of the container instance, as well it's **Status**.

mycontainer

Overview

Status: Running

FQDN: mycontainer.eastus.azurecontainer.io

7. When the **Status** value of the container instance is **Running**, navigate to the container's FQDN in a web browser.



Note: You can also navigate to the container's IP address in your browser. You can obtain the IP address by following Step 6, and making a note of the **IP address** instead of the **FQDN**.

Congratulations! You have used Azure Portal to deploy an application to a container in Azure Container Instances successfully.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: Azure Networking Services



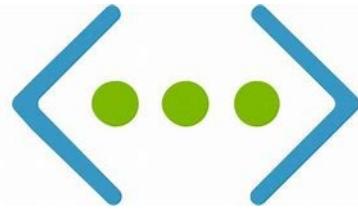
<https://www.youtube.com/watch?v=lWsb-0HAuHw>

Azure Network Services

Networking on Azure allows you to connect cloud and on-premises infrastructure and services to provide your customers and users the best possible experience. Once the resources move to Azure, they require the same networking functionality as an on-premises deployment. In specific scenarios, they may require some level of network isolation. Azure networking components offer a range of functionality and services that can help organizations design and build cloud infrastructure services that meet their requirements.

Some of the most common networking service types in Azure are discussed in the following sections.

Azure Virtual Network



Azure Virtual Network enables many types of Azure resources such as Azure VMs to securely communicate with each other, the internet, and on-premises networks. A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected together using virtual network peering. With Azure Virtual Network you can provide isolation, segmentation, communication with on-premises and cloud resources, routing and filtering of network traffic. See [Virtual Network¹⁷](#) for more details.

Azure Load Balancer



Azure Load Balancer can provide scale for your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) applications. You can use Load Balancer with incoming internet traffic, internal traffic across Azure services, port forwarding for specific traffic, or outbound connectivity for VMs in your virtual network. See [Load Balancer¹⁸](#) for more details.

VPN gateway



A *VPN gateway*, can also be referred to as a **virtual network gateway**, but a VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure Virtual Network and an on-premises location over the public internet. It provides a more secure connection from on-premises to Azure over the internet. See [VPN Gateway¹⁹](#) for more details.

¹⁷ <https://docs.microsoft.com/en-us/azure/virtual-network/>

¹⁸ <https://azure.microsoft.com/en-us/services/load-balancer/>

¹⁹ <https://azure.microsoft.com/en-us/services/vpn-gateway/>

Azure Application Gateway



Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It is the connection through which users connect to your application. With Application Gateway you can route traffic based on source IP address and port to a destination IP address and port. You also can help protect a web application with a web application firewall, redirection, session affinity to keep a user on the same server, and many more configuration options. See **Application Gateway** ²⁰ for more details.

Content Delivery Network



A *content delivery network* (CDN) is a distributed network of servers that can efficiently deliver web content to users. It is a way to get content to users in their local region to minimize latency. CDN can be hosted in Azure or any other location. You can cache content at strategically placed physical nodes across the world and provide better performance to end users. Typical usage scenarios include web applications containing multimedia content, a product launch event in a particular region, or any event where you expect a high bandwidth requirement in a region. See **Content Delivery Network** ²¹ for more details.

Note: For a full list of networking services available with Azure, and context on when you use them, see the page **Networking**²².

Walkthrough-Create a virtual network via the Azure Portal

In this walkthrough task we will create a virtual network, deploy two virtual machines onto that virtual network and then configure them to allow one virtual machine to ping the other over that virtual network.

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

²⁰ <https://azure.microsoft.com/en-us/services/application-gateway/>

²¹ <https://azure.microsoft.com/en-us/services/cdn/>

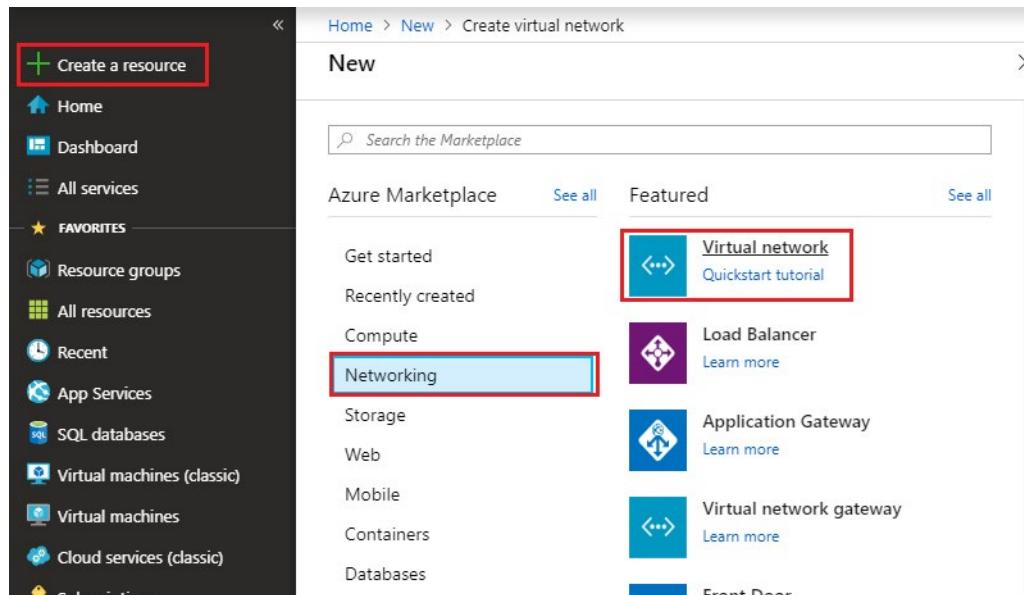
²² <https://azure.microsoft.com/en-us/product-categories/networking/>

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 today²³](#) webpage.

Steps

- Sign in to the Azure portal at [²⁴](https://portal.azure.com)
- Choose **Create a resource** in the upper left-hand corner of the Azure portal, then select **Networking > Virtual network**



- In the **Create virtual network** pane above the list of Azure Marketplace resources, search for and select **Windows Server 2016 Datacenter**, then choose **Create**.

Setting	Value
Name	vnet1
Address space	10.1.0.0/16
Subscription	< Select your subscription >
Resource group	Select Create new , enter vnet1-rg1 , then select OK .
Location	East US
Subnet - Name	subnet1
Subnet Address range	10.1.0.0/24

Leave the rest of the settings at their default values and select **Create**.

²³ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

²⁴ <https://portal.azure.com>

MCT USE ONLY. STUDENT USE PROHIBITED

Create virtual network □ X

* Name ✓

* Address space ✓
10.1.0.0/16
10.1.0.0 - 10.1.255.255 (65536 addresses)

* Subscription

* Resource group Create new

* Location

Subnet

* Name ✓

* Address range ✓
10.1.0.0/24
10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection Basic Standard

Service endpoints ✓
 Disabled Enabled

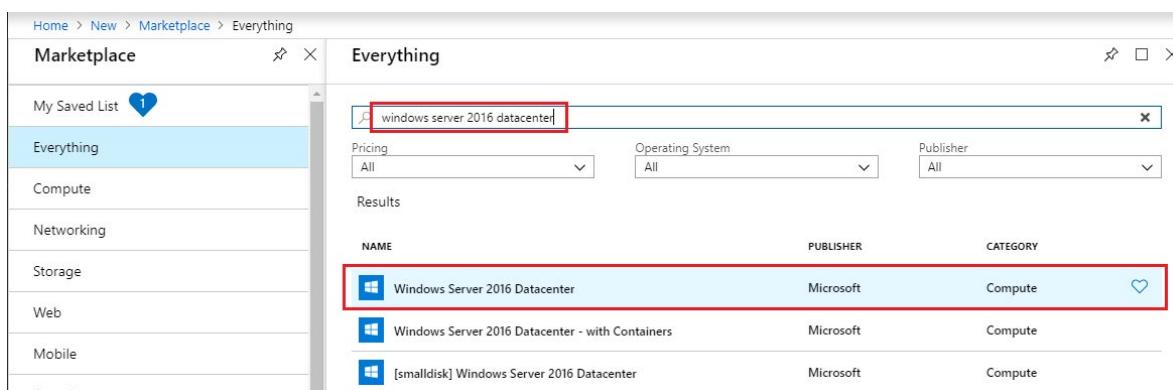
Firewall ✓
 Disabled Enabled

Create Automation options

4. Verify the creation of the virtual network by going to the newly created resource group and viewing the virtual network is present, you can click on the virtual network and view its properties if you wish.

Subscription (change) Pay-As-You-Go			Subscription ID 974e6e39-73eb-48b0-9226-dae31425c367	Deployments 1 Succeeded
Tags (change) Click here to add tags				
<input type="checkbox"/> NAME			TYPE	LOCATION
<input checked="" type="checkbox"/> vnet1			Virtual network	East US

5. Create a virtual machine by going to the upper-left side of the Azure Portal and selecting **Create a resource > Compute > Windows Server 2016 Datacenter**



Windows Server 2016 Datacenter

Microsoft

Windows Server 2016 is a comprehensive server operating system designed to run the applications and infrastructure that power your business. It includes built-in layers of security and innovation to help you run traditional and cloud-native applications with confidence. This Server with Desktop Experience image includes all roles including the graphical user interface (GUI).

This image can be used with [Azure Hybrid Benefit for Windows Server](#).

Legal Terms

By clicking the Create button, I acknowledge that I am getting this software from Microsoft and that the [legal terms](#) of Microsoft apply to it. Microsoft does not provide rights for third-party software. Also see the [privacy statement](#) from Microsoft.

[Save for later](#)

PUBLISHER	Microsoft
USEFUL LINKS	Documentation Introducing Windows Server 2016 What's New in 2016 Learn more

Select a deployment model ?

Resource Manager [Activate Windows](#) Go to Settings to activate Windows.

[Create](#)

6. In Create a **virtual machine - Basics** tab, enter or select this information:

Setting	Value
Subscription	< Select your subscription >
Resource group	The resource group you created it in the last section, i.e. vnet1-rg1
Virtual machine name	vm1
Region	East US
Availability options	Leave the default No infrastructure redundancy required

Setting	Value
Image	Leave the default Windows Server 2016 Data-center
Size	Leave the default Standard DS1 v2
Username	azureuser
Password	enter a password that meets the complexity requirements.
Public inbound ports	Select Allow selected ports
Selected inbound ports	Select HTTP, HTTPS, SSH and RDP

7. Select **Next : Disks**, leave the default values.
8. Select **Next : Networking**, complete the following details

Setting	Value
Virtual network	Leave the default vnet1
Subnet	Leave the default subnet1 (10.1.0.0/24)
Public IP	Leave the default (new) vm1-ip
NIC network security group	accept the default Basic
Public inbound ports	Select Allow selected ports
Selected inbound ports	Select HTTP, HTTPS, SSH and RDP

Create a virtual machine

NETWORK INTERFACE
When creating a virtual machine, a network interface will be created for you.

CONFIGURE VIRTUAL NETWORKS

* Virtual network

* Subnet

Public IP

NIC network security group Basic Advanced

* Public inbound ports Allow selected ports

* Select inbound ports

! These ports will be exposed to the internet. Use the Advanced controls to limit inbound traffic to known IP addresses. You can also update inbound traffic rules later.

9. Select **Next : Management**, accept all the default values except for the below settings:

Setting	Value
Boot diagnostics	accept the default value i.e. On
Diagnostic storage account	accept the default value i.e. vnet1rgdiag

Create a virtual machine

The screenshot shows the 'Management' tab of the Azure VM creation interface. It includes sections for MONITORING, IDENTITY, AUTO-SHUTDOWN, and BACKUP, each with various configuration options.

- MONITORING:**
 - Boot diagnostics: On (radio button selected)
 - OS guest diagnostics: Off (radio button selected)
 - Diagnostics storage account: (new) vnet1rg1diag (dropdown menu)
 - Create new (button)
- IDENTITY:**
 - System assigned managed identity: Off (radio button selected)
- AUTO-SHUTDOWN:**
 - Enable auto-shutdown: Off (radio button selected)
- BACKUP:**
 - Enable backup: Off (radio button selected)

10. Select **Review + create**. Azure will validate the configuration. When you see that Validation passed, select **Create**. Deployment times can vary but it can generally take between three to six minutes to deploy.

Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Guest config Tags Review + create

PRODUCT DETAILS

Standard DS1 v2
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.1063 EUR/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription	Pay-As-You-Go
Resource group	vnet1-rg1
Virtual machine name	vm1
Region	East US
Availability options	No infrastructure redundancy required
Username	azureuser
Public inbound ports	HTTP, HTTPS, SSH, RDP
Already have a Windows license?	No

Create Previous Next Download a template for automation

11. Create a second Virtual machine by repeating steps **5 to 9** above, using the same values above ensuring the below settings are set:

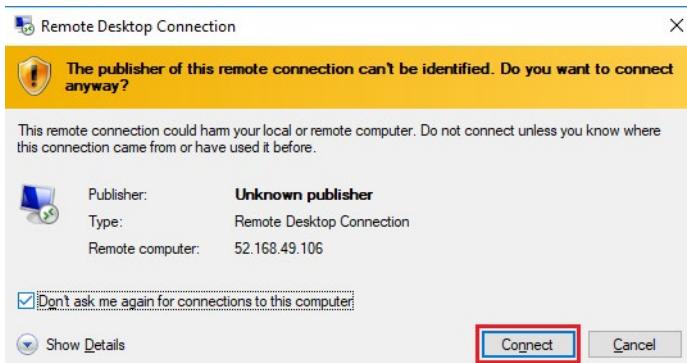
Setting	Value
Virtual machine name	vm2
Public IP	Leave the default (new) vm2-ip
Diagnostic storage account	Leave the default value i.e. vnet1rg1diag

12. When finished filling in the details, validate the configuration by clicking **Review + create** and once successfully validated click **Create**
13. When both virtual machine have completed deployment connect to the first virtual machine, **vm1**, by going to the resource group you placed the virtual machine in, **vnet-rg1** and open up the virtual machine, then click the **Connect** button on the virtual machine properties page.

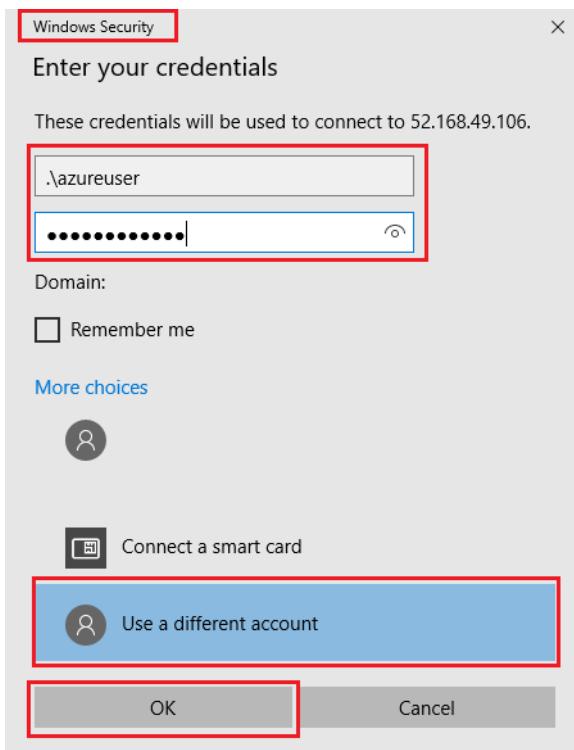
Note: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on Linux virtual machine you could connect directly from a bash shell using `ssh`.

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

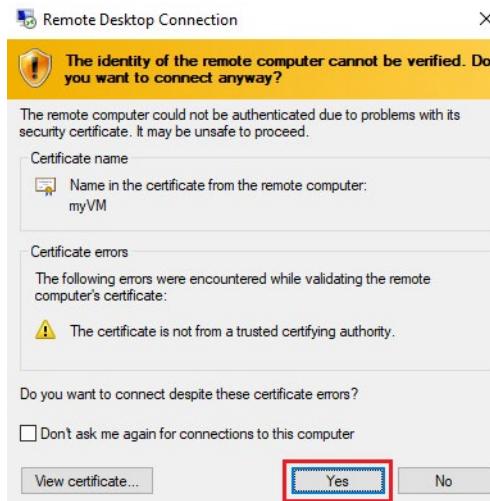
15. Open the downloaded RDP file and click **Connect** when prompted.



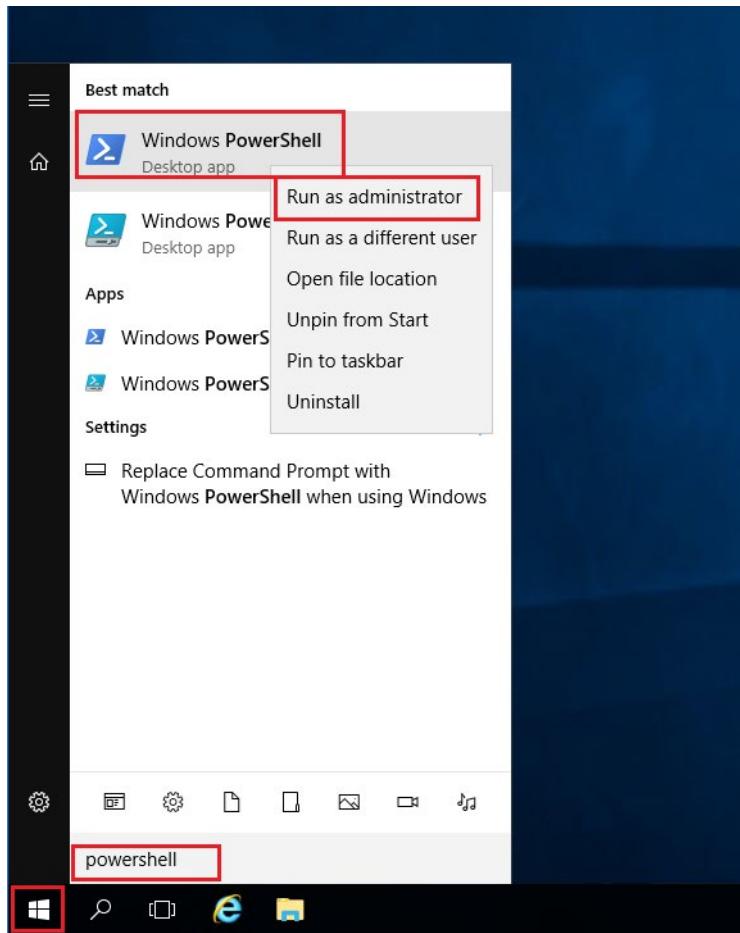
16. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as localhost\username, (you could also type .\azureuser) enter password you created for the virtual machine, and then click **OK**.



17. 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.



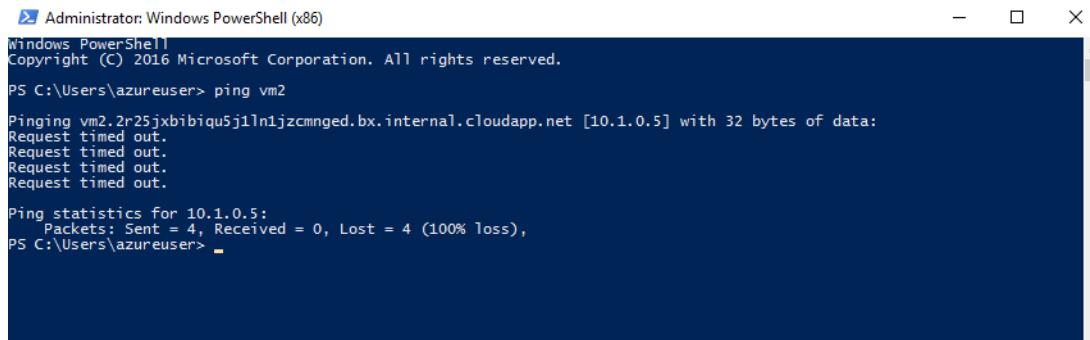
18. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell** right clicking **Windows PowerShell** in the menu and selecting **Run as administrator**



19. Run the command

```
ping vm2
```

You receive an error, saying request timed out. The ping fails, because ping uses the **Internet Control Message Protocol (ICMP)**. By default, ICMP isn't allowed through the Windows firewall.



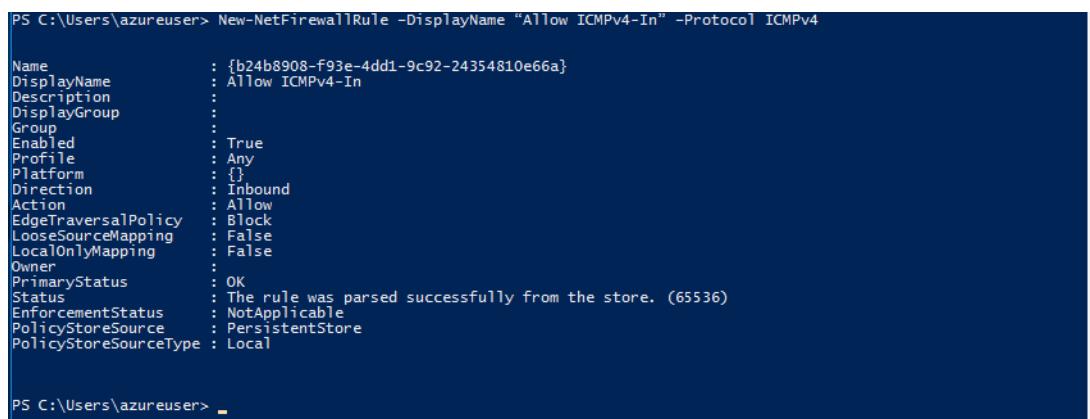
```
Administrator: Windows PowerShell (x86)
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> ping vm2
Pinging vm2.2r25jxbibiqu5j1ln1jzcmnged.bx.internal.cloudapp.net [10.1.0.5] with 32 bytes of data:
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),
PS C:\Users\azureuser>
```

20. To allow *vm2* to ping *vm1* enter the below command. This command allows ICMP inbound through the Windows firewall:

```
New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4
```

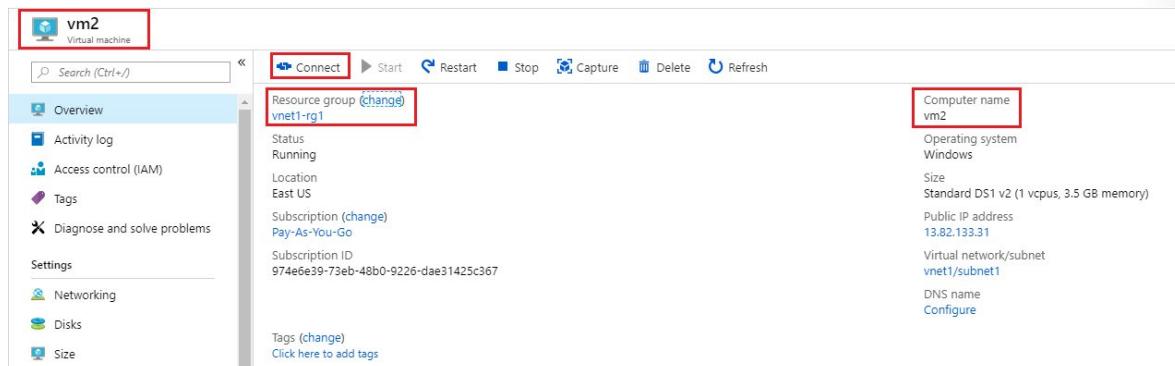


```
PS C:\Users\azureuser> New-NetFirewallRule -DisplayName "Allow ICMPv4-In" -Protocol ICMPv4

Name : {b24b8908-f93e-4dd1-9c92-24354810e66a}
DisplayName : Allow ICMPv4-In
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform :
Direction : Inbound
Action : Allow
EdgeTraversalPolicy :
LooseSourceMapping :
LocalOnlyMapping :
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

PS C:\Users\azureuser>
```

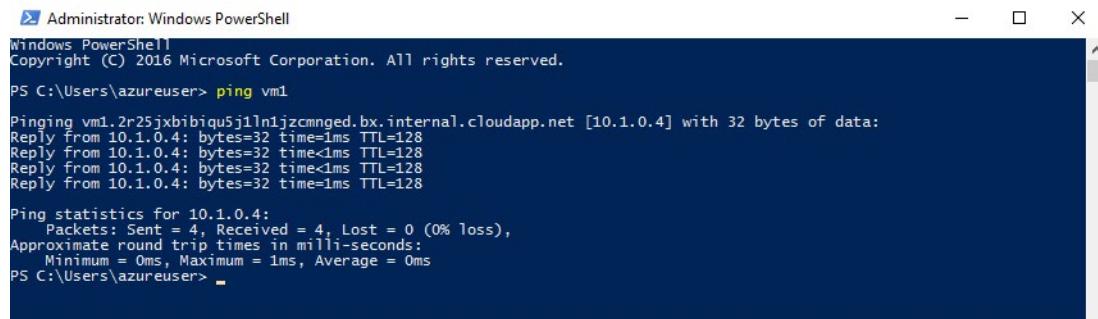
21. Connect to *VM2* as has been done for *VM1*, using rdp. i.e. open **vm2** properties and click the **Connect** button to download and then connect via RDP



22. Open up a PowerShell command prompt on the virtual machine, VM2, and run the command:

```
ping vm1
```

You should now be able to ping the *vm1* virtual machine successfully, because ICMP has been configured to be allowed through the Windows firewall on the *vm1* virtual machine in an earlier step.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> ping vm1

Pinging vm1.2r25jxbibiqu5j1ln1jzcmnged.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

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

PS C:\Users\azureuser>
```

Congratulations! This ping is being done using the *virtual network* you created and deployed the two virtual machines into. The two virtual machines are communicating over this *virtual network* that was created.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: Azure Storage Services



<https://www.youtube.com/watch?v=gf7YLqhLiMo>

Azure Storage Services

Azure Storage is a service that you can use to store files, messages, tables, and other types of information. You can use Azure Storage on its own (for example as a file share), but developers also often use it as a store for working data. Such stores can be used by websites, mobile apps, desktop applications, and many other types of custom solutions. Azure Storage is also used by IaaS virtual machines, and PaaS cloud services.

You can generally think of Azure Storage in categories.

Structured data

Structured data is data that adheres to a schema, so all of the data has the same fields or properties. Structured data can be stored in a database table with rows and columns. Structured data relies on keys to indicate how one row in a table relates to data in another row of another table. Structured data is also referred to as *relational data*, as the data's schema defines the table of data, the fields in the table, and the clear relationship between the two. Structured data is straightforward in that it's easy to enter, query,

and analyze. All of the data follows the same format. Examples of structured data include, sensor data or financial data.

Semi-structured data

Semi-structured data is less organized than structured data, and is not stored in a relational format, meaning the fields do not neatly fit into tables, rows, and columns. Semi-structured data contains tags that make the organization and hierarchy of the data apparent. Semi-structured data is also referred to as *non-relational* or *NoSQL* data.

Unstructured data

Unstructured data encompasses data that has no designated structure to it. This also means that there are no restrictions on the kinds of data it can hold. For example, a blob can hold a PDF document, a JPG image, a JSON file, video content, etc. As such, unstructured data is becoming more prominent as businesses try to tap into new data sources.

Some of the most common storage service types in Azure are blob, disk, file, and archive.

Blob Storage



Azure Blob Storage is *unstructured*, meaning that there are no restrictions on the kinds of data it can hold. Blobs are highly scalable and apps work with blobs in much the same way as they would work with files on a disk, such as reading and writing data. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.

Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing. See **Blob Storage** ²⁵ for more details.

Disk storage



Disk storage provides disks for virtual machines, applications, and other services to access and use as they need, similar to how they would in on-premises scenarios. Disk storage allows data to be persistently stored and accessed from an attached virtual hard disk. The disks can be managed or unmanaged by Azure, and therefore managed and configured by the user. Typical scenarios for using disk storage are if you want to lift and shift applications that read and write data to persistent disks, or if you are storing data that is not required to be accessed from outside the virtual machine to which the disk is attached.

²⁵ <https://azure.microsoft.com/en-us/services/storage/blobs/>

Disks come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance abilities. Details on pricing are available on the Managed Disks pricing page.

Managed Disks pricing²⁶ page. Also, see **Disk Storage²⁷** for more general details.

File storage



Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and MacOS. Applications running in Azure virtual machines or cloud services can mount a file storage share to access file data, just as a desktop application would mount a typical SMB share. Any number of Azure virtual machines or roles can mount and access the file storage share simultaneously. Typical usage scenarios would be to share files anywhere in the world, diagnostic data, or application data sharing. See **Azure Files²⁸** for more details.

Archive storage



Archive storage provides a storage facility for data that is rarely accessed. It allows you to archive legacy data at low cost to what it would traditionally have cost to create and maintain archives. Archive storage is available as a tier of Blob Storage, object data in the most cost-effective manner. It is stored offline and offers the lowest storage costs. However, it also has the highest access cost, hence it is suited for archival data that is rarely accessed. Archive storage is intended for data that can tolerate several hours of retrieval latency and will remain archived for at least 180 days. See **Azure Archive Storage²⁹** for more details.

Note: For a full list of storage services available with Azure, and context on when you use them, see the page **Storage³⁰**.

²⁶ <https://azure.microsoft.com/en-us/pricing/details/managed-disks/>

²⁷ <https://azure.microsoft.com/en-us/services/storage/disks/>

²⁸ <https://azure.microsoft.com/en-us/services/storage/files/>

²⁹ <https://azure.microsoft.com/en-us/services/storage/archive/>

³⁰ <https://azure.microsoft.com/en-us/product-categories/storage/>

Demo: Create Blob Storage



<https://www.youtube.com/watch?v=Y8hz0oluWDs>

Walkthrough-Create Blob storage

In this walkthrough task we will create a storage account, then create a blob storage container within that storage account, then upload a block blob, view and edit the blob file within the blob container in Azure, and then download the block blob file.

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 today³¹](#) webpage.

Steps

1. Sign in to the Azure portal at [³²](https://portal.azure.com)
2. Select **All services** on the upper left hand side of the Azure Portal. In the **All services** filter box, type **Storage Accounts**. As you begin typing, the list filters based on your input. Select **Storage Accounts**.

3. On the **Storage Accounts** window that appears, if there are no storage accounts present you can select **Create storage account**, or if there are already storage accounts present, this option will not be present and you can choose the option + **Add**.

³¹ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

³² <https://portal.azure.com>

The screenshot shows the 'Storage accounts' blade in the Azure portal. At the top, there's a header with 'Home > Storage accounts'. Below it, a section titled 'Storage accounts' shows '0 items'. A red box highlights the '+ Add' button. There are also buttons for 'Edit columns', 'Refresh', and 'Assign tags'. A message at the top says 'Subscriptions: All 2 selected - Don't see a subscription? Open Directory + Subscription settings'. Below this are filters for 'Filter by name...', 'All subscriptions', 'All resource groups', 'All types', 'All locations', 'All tags', and 'No grouping'. The main area has columns for 'NAME', 'TYPE', 'KIND', 'RESOURCE GROUP', 'LOCATION', and 'SUBSCRIPTION'. A large, empty placeholder icon is shown. At the bottom, a message reads: 'Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed. Learn more' with a 'Create storage account' button.

4. Complete the Create storage account blade with the following details

Setting	Value
Subscription	< Select your subscription >
Resource group	Select Create new , enter strac-rg1 , then select OK .
Storage account name	< this must be between 3-24 characters in length, can be numbers and lowercase only, and must be unique across Azure >
Location	East US
Performance	Standard
Account kind	Leave the default value StorageV2 (general purpose v2)*
Replication	Locally redundant storage (LRS)
Access tier (default)	Hot

Create storage account

Basics Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

Pay-As-You-Go

* Resource group

(New) strac-rg1

[Create new](#)

INSTANCE DETAILS

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name [i](#)

* Location

West Europe

Performance [i](#)

Standard Premium

Account kind [i](#)

StorageV2 (general purpose v2)

Replication [i](#)

Read-access geo-redundant storage (RA-GRS)

Access tier (default) [i](#)

Cool Hot

[Review + create](#)

[Previous](#)

[Next : Advanced >](#)

5. Select **Review + Create** to review your storage account settings and allow Azure to validate the configuration. Once validated select **Create**.

Create storage account

✓ Validation passed

Basics Advanced Tags Review + create

BASICS

Subscription	Pay-As-You-Go
Resource group	(new) strac-rg1
Location	East US
Storage account name	strac1
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Performance	Standard
Access tier (default)	Hot

ADVANCED

Secure transfer required	Enabled
Allow access from	All networks
Hierarchical namespace	Disabled

Actions

Create Previous Next Download a template for automation

- Verify its successful creation by going to the resource group just created and locate the storage account.

strac-rg1
Resource group

Subscription (change)
Pay-As-You-Go

Subscription ID
974e6e39-73eb-48b0-9226-dae31425c367

Tags (change)
Click here to add tags

Deployments
1 Succeeded

Filter by name... All types All locations No grouping

1 items Show hidden types

NAME	TYPE	LOCATION	...
strac1	Storage account	East US	...

- Open the storage account and scroll in the left menu for the storage account, scroll to the **Blob** service section, select **Blobs** and then select the **+ Container** button.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Azure Storage account interface for 'strac1'. On the left, a sidebar lists options: Shared access signature, Firewalls and virtual networks, Advanced Threat Protection (pr...), Static website, Properties, Locks, Automation script, Blob service, Blobs (which is selected and highlighted in blue), and Custom domain. At the top, there's a search bar labeled 'Search (Ctrl+J)' and a '+ Container' button. The main area shows a table with columns: NAME, LAST MODIFIED, PUBLIC ACCESS L..., and LEASE STATE. A message at the top of the table says, 'You don't have any containers yet. Click '+ Container' to get started.'

8. Configure the blob container as below and select **OK** when complete to create the blob container.

Setting	Value
Name	i.e. blob1 The container name must be lowercase, must start with a letter or number, and can include only letters, numbers, and the dash (-) character.
public access level	leave the default value i.e. The default level is Private (no anonymous access)

New container

* Name
blob1

Public access level
Private (no anonymous access)

OK **Cancel**

9. The container should be created and available

The screenshot shows the same Azure Storage account interface as before, but now it lists a single container named 'blob1' in the main table. The table has columns: NAME, LAST MODIFIED, PUBLIC ACCESS L..., and LEASE STATE. The 'blob1' entry shows a last modified date of 1/24/2019, 10:25:05 PM, a public access level of Private, and a lease state of Available.

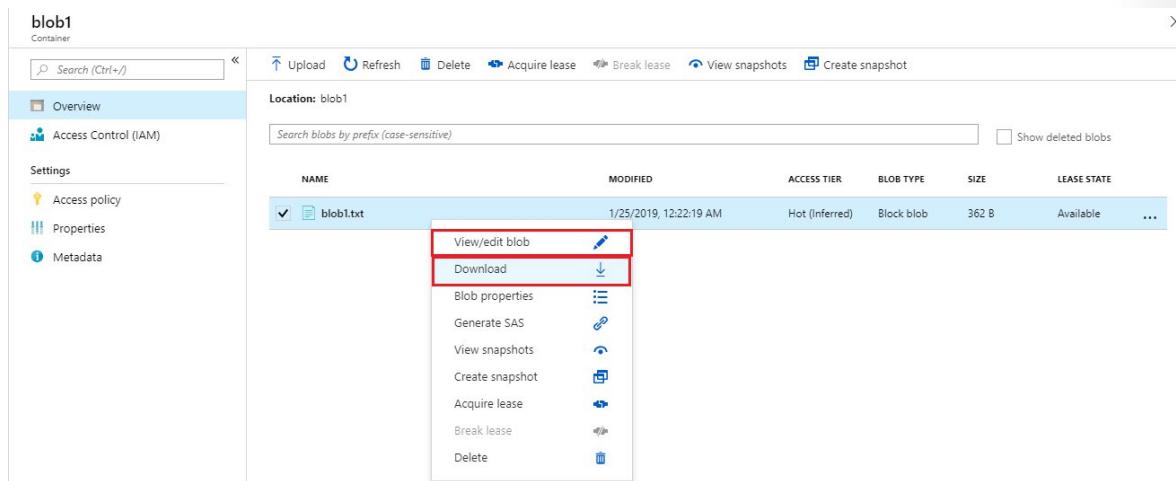
10. We will upload a block blob to your new container. Select the container to show a list of blobs it contains. Since this container is new, it won't yet contain any blobs

Note: Block blobs consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos.

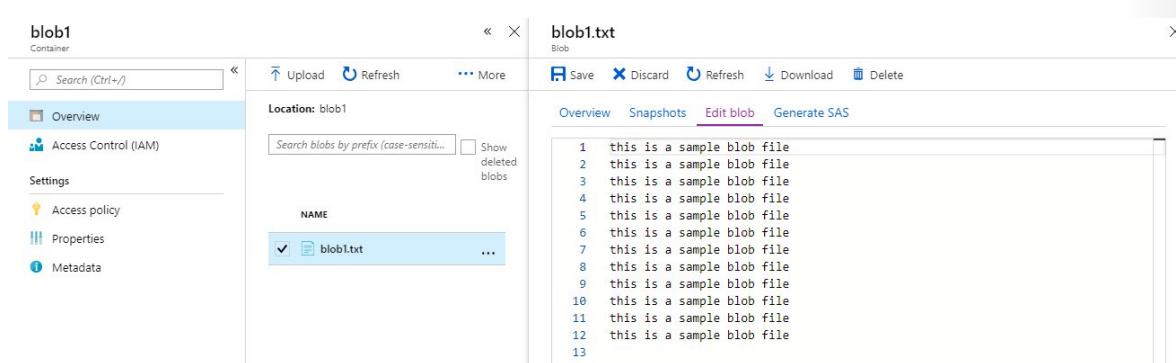
11. Create a .txt file on your local machine, named **blob1.txt**, and enter some text into it, such as this is a blob file or something like that.
12. Select the **Upload** button to upload a blob to the container. Browse your local file system to find the file you created in the previous steps to upload as a block blob. Click on the **Advanced** arrow, leave the default values as they are, just note them, and then select **Upload**.

Note: You can upload as many blobs as you like in this way. You'll see that the new blobs are now listed within the container.

13. View the uploaded block blob by right clicking on the blob file that was uploaded and selecting **View/edit blob**

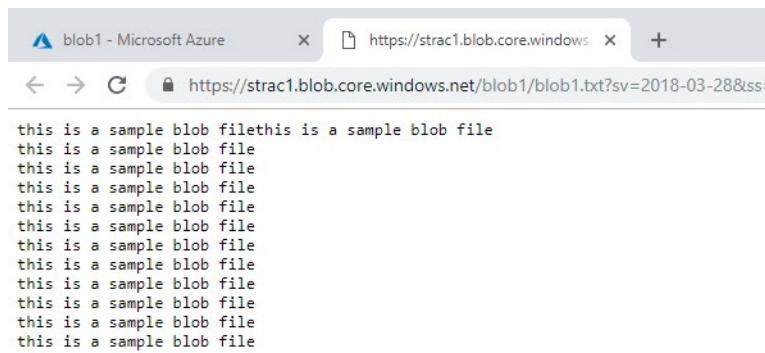


The screenshot shows the Azure Storage Blob Container 'blob1'. On the left, there's a sidebar with 'Overview', 'Access Control (IAM)', 'Settings' (which includes 'Access policy', 'Properties', and 'Metadata'), and a search bar. The main area shows a table of blobs. One row for 'blob1.txt' is selected, and a context menu is open over it. The 'Download' option in the menu is highlighted with a red box.



The screenshot shows the same 'blob1' container. The right pane displays the contents of 'blob1.txt', which consists of a list of numbers from 1 to 13, each followed by the text 'this is a sample blob file'.

14. You can download a block blob by right clicking on the block blob and selecting **Download**. The blob file opens in a browser and is then downloadable by right clicking on the file and selecting save as



The screenshot shows a web browser window with the URL <https://strac1.blob.core.windows.net/blob1/blob1.txt?sv=2018-03-28&ss=0&sr=c&si=&st=2018-03-28T12%3A45%3A00Z&se=2018-03-28T12%3A55%3A00Z&sp=r>. The page content is a repeating string of 'this is a sample blob file'.

Congratulations! You have created a storage account, created a blob storage container within that storage account, then uploaded a block blob, viewed and edited the block blob in the blob container and then downloaded the block blob.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: Azure Data Services



<https://www.youtube.com/watch?v=-gNLs-ky4nc>

Azure Database Services

Azure database services are fully-managed PaaS database services that free up valuable time you'd otherwise spend managing your database. Enterprise-grade performance with built-in high availability means you can scale quickly and reach global distribution without worrying about costly downtime. Developers can take advantage of industry-leading innovations such as built-in security with automatic monitoring and threat detection, automatic tuning for improved performance, and turnkey global distribution.

Some of the most common data service types in Azure as follows:

Azure Cosmos DB



Microsoft Azure Cosmos DB is a globally distributed database service that enables you to elastically and independently scale throughput and storage across any number of Azure's geographic regions. It supports schema-less data that lets you build highly responsive and Always On applications to support constantly changing data. You can use Cosmos DB to store data that is updated and maintained by users around the world. It makes it easy to build scalable, highly responsive applications at global scale. See [Azure Cosmos DB³³](#) for more details.

³³ <https://azure.microsoft.com/en-us/services/cosmos-db/>

Azure SQL Database



Azure SQL Database is a relational database as a service (DaaS) based on the latest stable version of Microsoft SQL Server database engine. SQL Database is a high-performance, reliable, fully managed and secure database that you can use to build data-driven applications and websites in the programming language of your choice without needing to manage infrastructure. See [SQL Database³⁴](#) for more general details.

³⁴ <https://azure.microsoft.com/en-us/services/sql-database/>

Azure Database Migration



The Azure Database Migration Service is a fully-managed service designed to enable seamless migrations from multiple database sources to Azure data platforms with minimal downtime (online migrations). The service uses the Microsoft Data Migration Assistant to generate assessment reports that provide recommendations to help guide you through required changes prior to performing a migration. Once you assess and perform any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps. See [Azure Database Migration Service³⁵](#) for more details.

Note: For a full list of data services available with Azure, and context on when you use them, see the page [Databases³⁶](#).

Walkthrough-Create a SQL database

In this walkthrough task we will create a SQL database in Azure and then query the data in that database.

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 today³⁷](#) webpage.

Steps

1. Sign in to the Azure portal at [| Setting | Value |
|----------------|--|
| Database name | db1 |
| Subscription | < Select your subscription > |
| Resource group | Select Create new , enter sqldb1-rg1 , then select OK . |
| Select source | Select Sample AdventureWorksLT |](https://portal.azure.com³⁸2. Select Create a resource on the upper left hand side of the Azure Portal. Select Databases > SQL Databases and in the SQL Database pane fill in the fields as per the below table, and then click Server</div><div data-bbox=)

³⁵ <https://azure.microsoft.com/en-us/services/database-migration/>

³⁶ <https://azure.microsoft.com/en-us/product-categories/databases/>

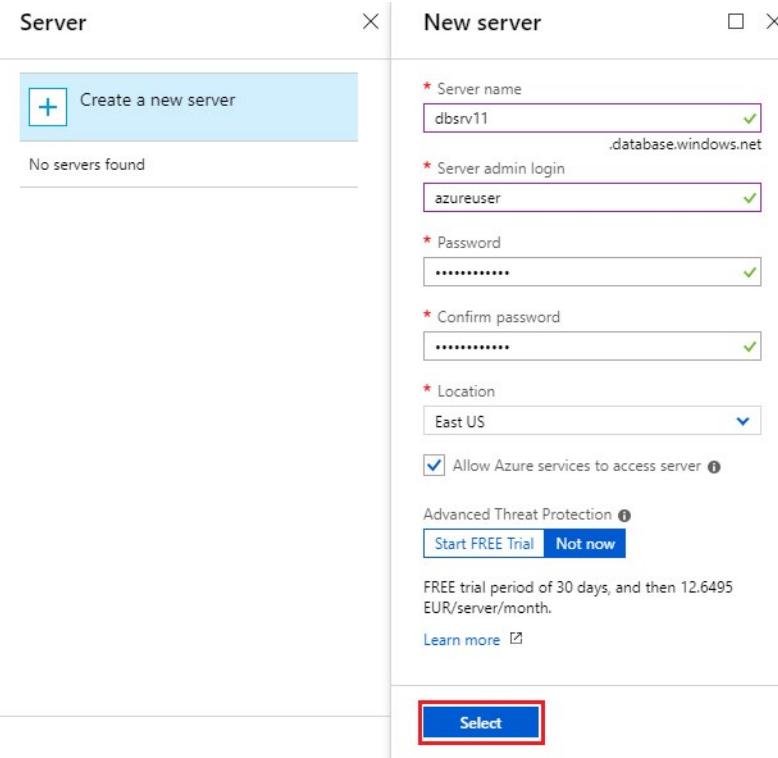
³⁷ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

³⁸ <https://portal.azure.com>

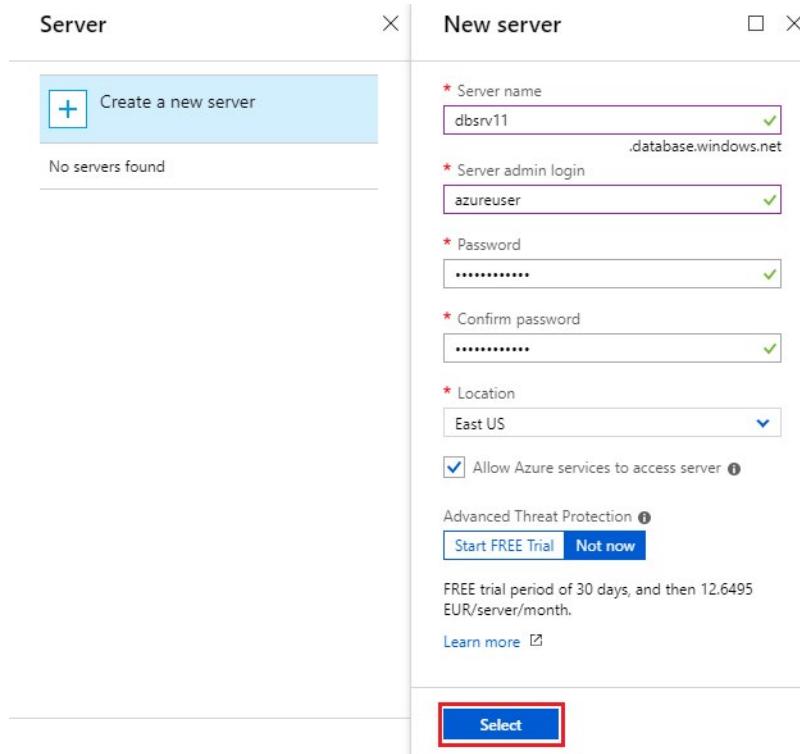
MCT USE ONLY. STUDENT USE PROHIBITED

3. In the **Server** pane, choose **Create a new server** and complete the New server pane using below details and click **Select** when finished.

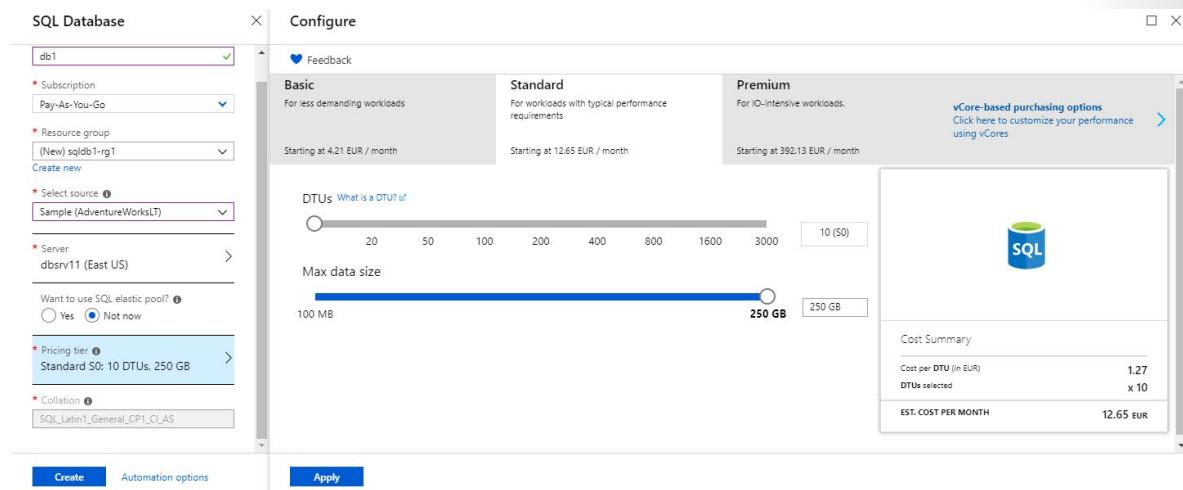
Setting	Value
Server name	< this needs to be a unique name >
Server admin login	azureuser
Password	Enter a password that meets the complexity requirements.
Location	East US



- On the **Storage Accounts** window that appears, if there are no storage accounts present you can select **Create storage account**, or if there are already storage accounts present, this option will not be present and you can choose the option **+ Add**.

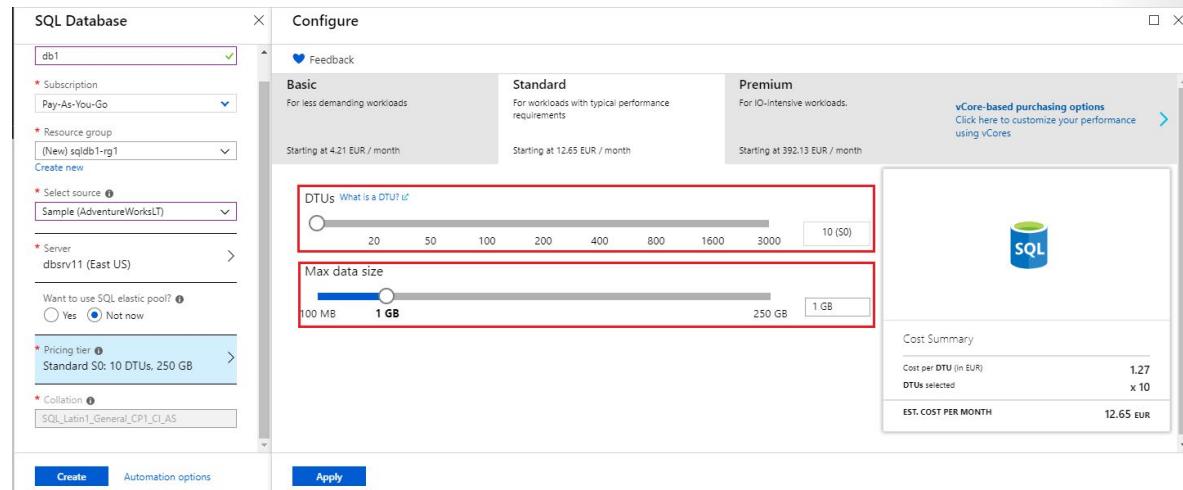


5. On the **SQL Database** pane , select **Pricing tier**. Explore the amount of *DTUs* and *storage* available for each service tier.



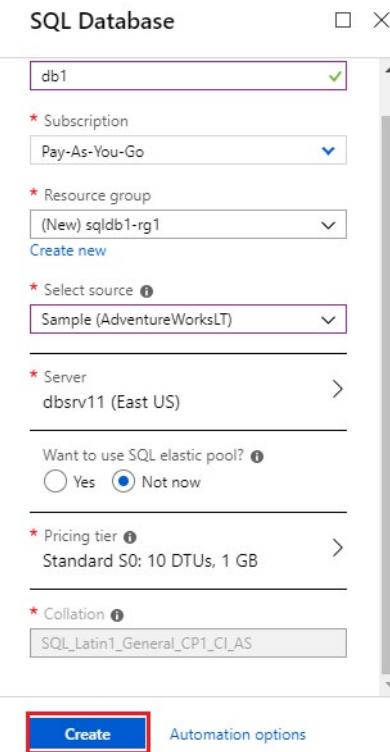
Note: This database uses the DTU-based purchasing model, but there is another, the vCore-based purchasing model, which is also available.

6. Select the **Standard** service tier, and then use the slider to select **10 DTUs** (S0) and **1 GB** of storage and select **Apply**.



7. Click **Create** to deploy and provision the resource group, server, and database. It can take approx. 2 to 5 minutes to deploy.

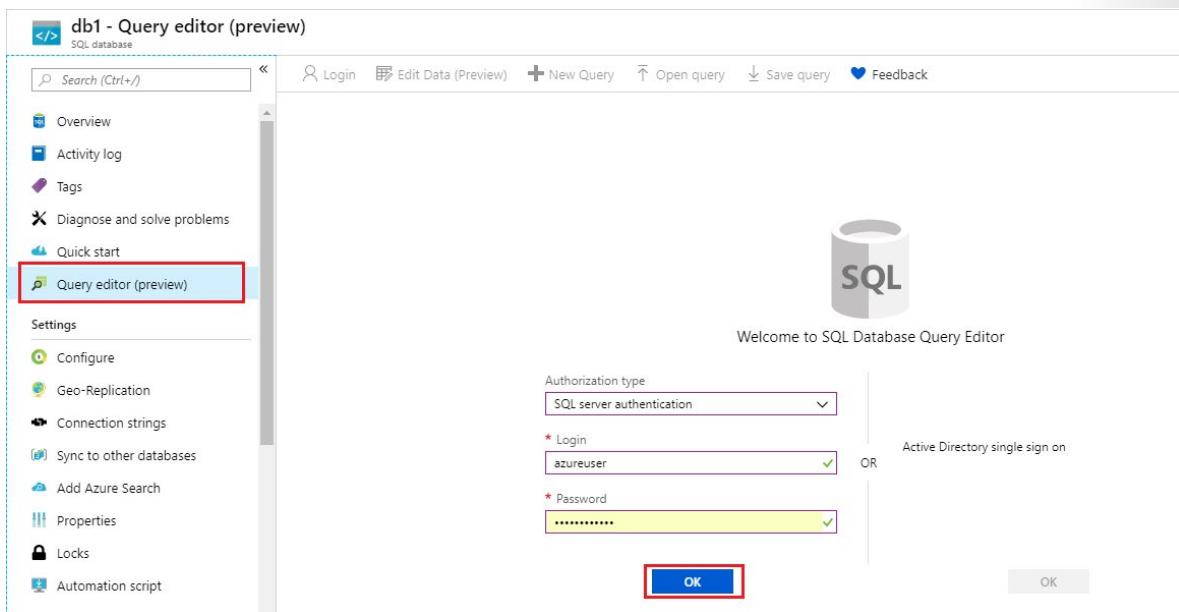
MCT USE ONLY. STUDENT USE PROHIBITED



- Once complete verify the successful deployment by going to the resource group you just created in the Azure Portal and verifying the presence of the server and database.

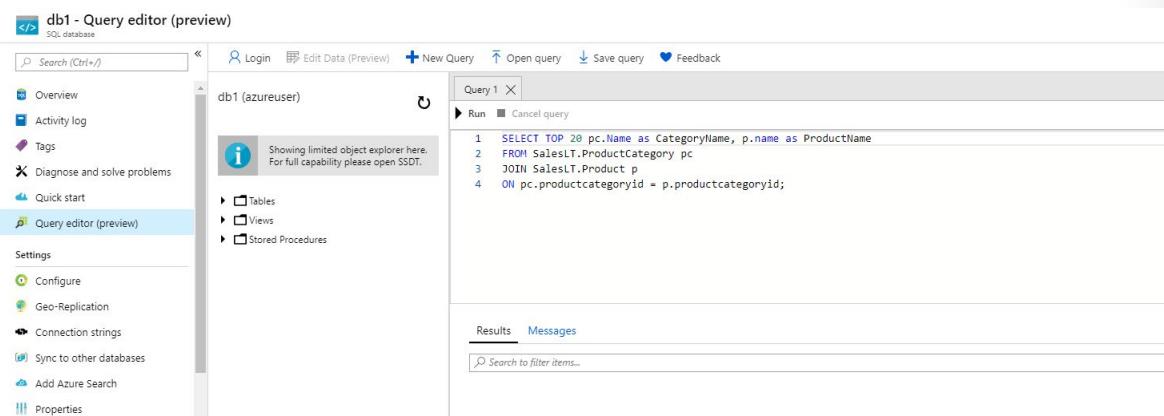
Subscription (change)			Deployment												
Pay-As-You-Go	Subscription ID 974e6e39-73eb-48b0-9226-dae31425c367	1 Succeeded													
Tags (change) Click here to add tags															
Filter by name... All types All locations No grouping															
2 items Show hidden types <table border="1"> <thead> <tr> <th>NAME</th> <th>TYPE</th> <th>LOCATION</th> <th>...</th> </tr> </thead> <tbody> <tr> <td>dbsrv11</td> <td>SQL server</td> <td>East US</td> <td>...</td> </tr> <tr> <td>db1 (dbsrv11/db1)</td> <td>SQL database</td> <td>East US</td> <td>...</td> </tr> </tbody> </table>				NAME	TYPE	LOCATION	...	dbsrv11	SQL server	East US	...	db1 (dbsrv11/db1)	SQL database	East US	...
NAME	TYPE	LOCATION	...												
dbsrv11	SQL server	East US	...												
db1 (dbsrv11/db1)	SQL database	East US	...												

- Open the SQL database you crated **db1**, go to the **Query Editor (preview)** in the left hand pane, and enter the login details and password. then click **OK**



10. Once you log in successfully the query pane appears, enter the following query into the editor pane

```
SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
FROM SalesLT.ProductCategory pc
JOIN SalesLT.Product p
ON pc.productcategoryid = p.productcategoryid;
```



11. Select **Run**, and then review the query results in the **Results** pane. The query should run successfully.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows a SQL query interface with the following details:

- Query 1:** A SQL query is displayed:

```
1 SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
2 FROM SalesLT.ProductCategory pc
3 JOIN SalesLT.Product p
4 ON pc.productcategoryid = p.productcategoryid;
```
- Run:** A button labeled "Run" is highlighted with a dashed blue border.
- Results:** The tab is selected, showing a table with two columns: "CATEGORYNAME" and "PRODUCTNAME".

CATEGORYNAME	PRODUCTNAME
Road Frames	HL Road Frame - Black, 58
Road Frames	HL Road Frame - Red, 58
Helmets	Sport-100 Helmet, Red
Helmets	Sport-100 Helmet, Black
Socks	Mountain Bike Socks, M
- Messages:** This tab is shown below the Results tab.
- Status Bar:** A message "Query succeeded | 1s" is displayed at the bottom left of the results area.

Congratulations! You have created a SQL database in Azure and successfully queried the data in that database.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

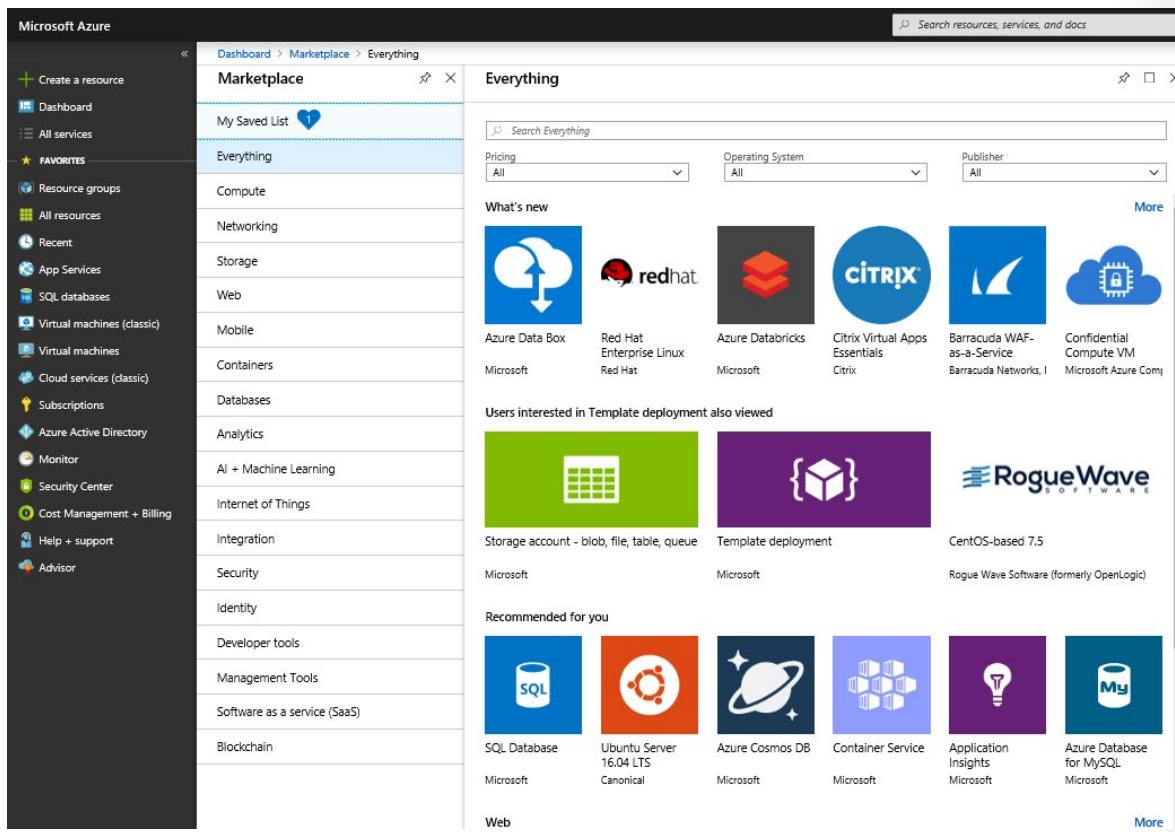
Video: Azure Marketplace



<https://www.youtube.com/watch?v=5AeJIL2gtBg>

Azure Marketplace

Azure Marketplace is a service on Azure that helps connect end users with Microsoft partners, independent software vendors (ISVs), and start-ups that are offering their solutions and services, which are optimized to run on Azure. Azure Marketplace allows customers—mostly IT professionals and cloud developers—to find, try, purchase, and provision applications and services from hundreds of leading service providers, all certified to run on Azure.



The solution catalog spans several industry categories, including but not limited to: open-source container platforms, virtual machine images, databases, application build and deployment software, developer tools, threat detection, and blockchain. Using Azure Marketplace, you can provision end-to-end solutions quickly and reliably, hosted in your own Azure environment. At the time of writing, this includes over 8,000 listings.

While Azure Marketplace is designed for IT professionals and cloud developers interested in commercial and IT software, Microsoft Partners also use it as a launch point for all joint Go-To-Market activities.

Note: You can read more about Azure Marketplace at <https://azuremarketplace.microsoft.com/en-us/>³⁹ and there is also a **Marketplace FAQ**⁴⁰ available.

³⁹ [https://azuremarkplace.microsoft.com/en-us/](https://azuremarketplace.microsoft.com/en-us/)

⁴⁰ <https://azure.microsoft.com/en-us/marketplace/faq/>

Azure Solutions

Video: Internet of Things



https://www.youtube.com/watch?v=at_qsDBMHMY

Internet of Things

People are able to access more information than ever before. It began with personal digital assistants (PDAs), then morphed into smartphones. Now there are smart watches, smart thermostats, even smart refrigerators. Personal computers used to be the norm. Now the internet allows any item that's online-capable to access valuable information. This ability for devices to gather and then relay information for data analysis is referred to as the *Internet of Things* (IoT).

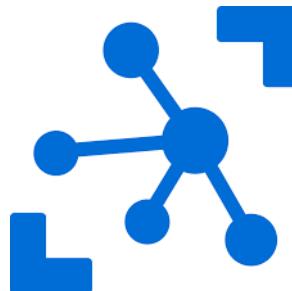
There are a number of services that can assist and drive end-to-end solutions for IoT on Azure. Two of the core Azure IoT service types are IoT Central, and Azure IoT Hub.

IoT Central



IoT Central is a fully-managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale. No cloud expertise is required to use IoT Central. As a result, you can bring your connected products to market faster while staying focused on your customers. See [Azure IoT Central⁴¹](#) for more details.

Azure IoT Hub



⁴¹ <https://azure.microsoft.com/en-us/services/iot-central/>

Azure IoT Hub is a managed service hosted in the cloud that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages. You can use Azure IoT Hub to build IoT solutions with reliable and secure communications between millions of IoT devices and a cloud-hosted solution backend. You can connect virtually any device to your IoT Hub.

IoT Hub supports communications both from the device to the cloud and from the cloud to the device. It also supports multiple messaging patterns such as device-to-cloud telemetry, file upload from devices, and request-reply methods to control your devices from the cloud. IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

IoT Hub's capabilities help you build scalable, full-featured IoT solutions such as managing industrial equipment used in manufacturing, tracking valuable assets in healthcare, and monitoring office building usage. See **Azure IoT Hub**⁴² for more general details.

Note: For a full list of IoT-related services available with Azure, and for context on when you use them, see the page **Find the Internet of Things product you need**⁴³.

Demo: Add IoT device to Azure IoT Hub



<https://www.youtube.com/watch?v=bCNBzsiA3MQ>

Walkthrough-Add IoT device to Azure IoT Hub

In this walkthrough you set up a new Azure IoT Hub in Azure Portal, and configure the hub to authenticate a connection to an IoT device using the **online Raspberry Pi device simulator**⁴⁴. Sensor data and messages are passed from the Raspberry Pi simulator to your Azure IoT Hub, and you view metrics for the messaging activity in Azure Portal.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Prerequisites

An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**⁴⁵ before you begin.

Steps

- To create a new IoT Hub, sign in to the Azure Portal and locate the *IoT Hub* service, then select **Create IoT Hub**, or alternatively, click on this **Create IoT Hub**⁴⁶ link and when prompted, sign into Azure Portal.

⁴² <https://azure.microsoft.com/en-us/services/iot-hub/>

⁴³ <https://azure.microsoft.com/en-us/product-categories/iot/>

⁴⁴ <https://azure-samples.github.io/raspberry-pi-web-simulator/#Getstarted>

⁴⁵ <https://azure.microsoft.com/free/>

⁴⁶ <https://portal.azure.com/#create/microsoft.iothub>

2. Fill in the fields with the following details.

- **Subscription:** Select the subscription to use for your new Azure IoT Hub.
- **Resource Group:** Choose **Create new** and provide a name for the resource group.
- **Region:** Select the Azure region that is closest to your location from the dropdown list.
- **IoT Hub Name:** Put in a name for your Azure IoT Hub. This name must be unique to your chosen region. If the name you enter is available, a green check mark appears.
- Select the **Next: Size and scale** button to continue.

The screenshot shows the 'Basics' tab of the Azure IoT hub creation wizard. It includes the following fields:

- Subscription:** Microsoft Azure Internal Consumption
- Resource Group:** Create new (selected), contoso-hub-rgrp
- Region:** West US
- IoT Hub Name:** contoso-test-hub

The 'Next: Size and scale' button at the bottom is also highlighted with a red box.

3. On the **Size and scale** tab, use the dropdown list to set the **Pricing and scale tier** to F1 – Free tier.

- Leave all other options set to their defaults.
- Select the **Review + create** button at the bottom.

MCT USE ONLY. STUDENT USE PROHIBITED

IoT hub
Microsoft

Basics Size and scale Review + create

Each IoT Hub is provisioned with a certain number of units in a specific tier. The tier and number of units determine the maximum daily quota of messages that you can send. [Learn more](#)

SCALE TIER AND UNITS

* Pricing and scale tier [F1: Free tier](#) [Learn how to choose the right IoT Hub tier for your solution](#)

Number of F1 IoT Hub units [1](#) This determines your IoT Hub scale capability and can be changed as your need increases.

Pricing and scale tier F1	Device-to-cloud-messages Enabled
Messages per day 8,000	Message routing Enabled
Cost per month 0.00 EUR	Cloud-to-device commands Enabled
	IoT Edge Enabled
	Device management Enabled

Advanced Settings

[Review + create](#) [« Previous: Basics](#) [Automation options](#)

4. Review your choices on the **Review + create** tab, then select the **Create** button to begin creating your new Azure IoT Hub.

Home > New > IoT hub

IoT hub
Microsoft

Basics Size and scale **Review + create**

BASICS

Subscription Microsoft Azure Internal Consumption	Resource Group contoso-hub-rgrp
Region West US	IoT Hub Name contoso-test-hub

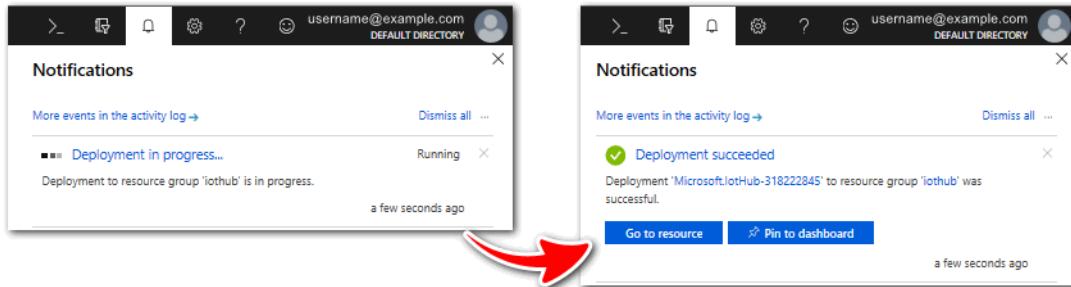
SIZE AND SCALE

Pricing and scale tier \$1	Number of S1 IoT Hub units 1
Messages per day 400,000	Cost per month 25.00 USD

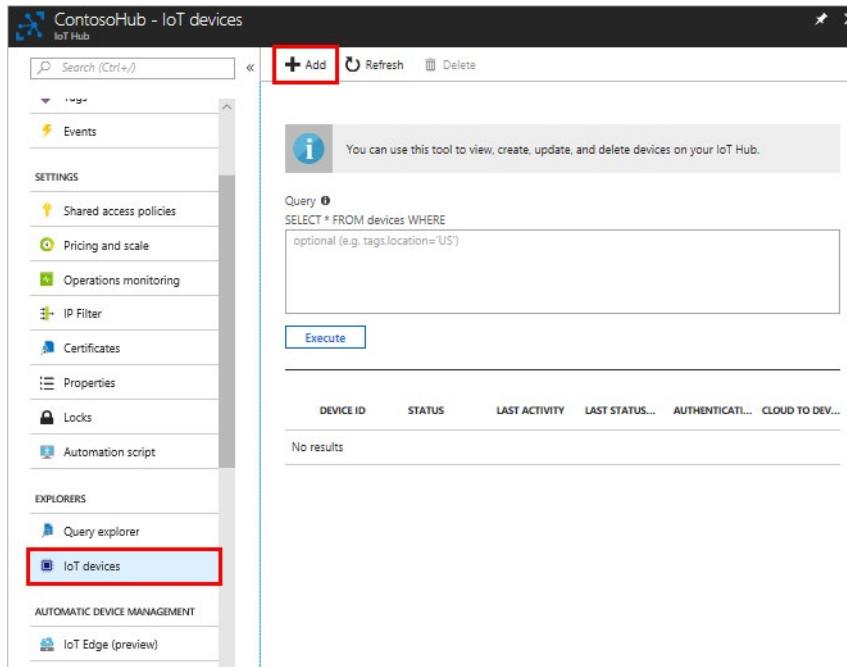
[Create](#) [« Previous: Size and scale](#) [Automation options](#)

Note: When the deployment starts, a notification appears in Azure Portal indicating the deployment is in progress. Another notification is displayed when the deployment has completed successfully.

- When the deployment has completed, choose **Go to resource** from the notification area to open the Azure IoT Hub **Overview** blade. You can also select **All resources** from the main menu, then choose your Azure IoT Hub from the list of resources.



- To add a new IoT device, select **Explorers > IoT Devices** from the **IoT Hub navigation** blade. Then, choose the **+ Add** button.



- Provide a name for your new IoT device, for example `myDeviceId`, and select the **Save** button. This will create a new IoT device identity in your Azure IoT Hub.

MCT USE ONLY. STUDENT USE PROHIBITED

Create a device

Learn more about creating devices

* Device ID ✓

Authentication type Symmetric key X.509 Self-Signed X.509 CA Signed

* Primary key

* Secondary key

Auto-generate keys

Connect this device to an IoT hub Enable Disable

Parent device (Preview) No parent device

- After the new device is created, select the new device from the list of IoT devices in the **IoT devices** pane. Copy the **Connection string—primary key** value. You will use this key in Step 10 to authenticate a connection to a Raspberry Pi device.

Device details
myDeviceId

Save Message to device Direct method Device twin More

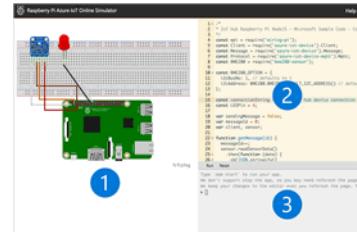
Device Id	<input type="text" value="myDeviceId"/>
Primary key	<input type="text" value="<primary key>"/>
Secondary key	<input type="text" value="<secondary key>"/>
Connection string (primary key)	<input type="text" value="HostName=iothub.azure-devices.net;DeviceId="/>
Connection string (secondary key)	<input type="text" value="<connection string secondary key>"/>

9. In a web browser, open the **online Raspberry Pi simulator**⁴⁷. Select “X” to close the **Overview of Raspberry Pi Simulator** window or choose **Next** to step through the guide.



Overview of Raspberry Pi Simulator

- 2. Coding Area. An online code editor for you to make an app on Raspberry Pi with Node.js
- 3. Integrated console window. You can see the output of your app.

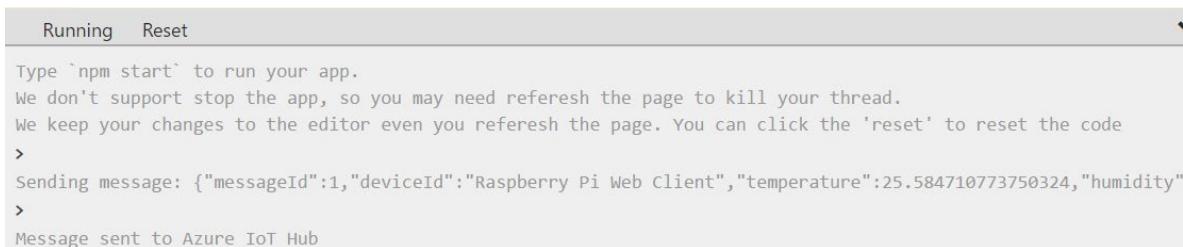


Next

10. In the coding area, make sure that you are working on the default, Microsoft sample code. Replace the placeholder code on Line 15 with the Azure IoT Hub connection string value that you copied from Step 8. Copy over the text that is present, including the brackets.

```
14
15 const connectionString = '[Your IoT hub device connection string]';
16 const LEDPin = 4;
17
```

11. Select **Run** or type `npm start` to run the application. The console output should show the sensor data and messages that are sent from the Raspberry Pi simulator to your Azure IoT Hub. Data and messages are sent each time the Raspberry Pi simulator LED flashes. Select **Stop** to stop sending data.



12. To view metrics for the messaging activity in Azure Portal, select **All resources** from the main menu. Choose your Azure IoT Hub from the list of resources. Scroll down to the **IoT Hub Usage** pane of the **IoT Hub Overview** blade. To access these metrics from the **IoT Hub navigation** blade, select **Metrics** from the **Monitoring** section.

⁴⁷ <https://azure-samples.github.io/raspberry-pi-web-simulator/#Getstarted>

The screenshot shows the Azure portal interface for managing IoT resources. On the left, the 'All resources' section is highlighted. In the center, the 'iothubmk19' IoT Hub is selected. The 'Metrics' section under the 'Monitoring' tab is highlighted with a red box. To the right, a chart titled 'IoT Hub Usage' shows a daily breakdown of messages and IoT devices. A large red box highlights the chart area, specifically the bar for 'Successful twin reads from back end (Count)' on March 19, 2024, which has a value of 7.

Congratulations! You have set up Azure IoT Hub to collect sensor data from an IoT device.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: Big Data and Analytics



<https://www.youtube.com/watch?v=UwPnPv7R1Uk>

Big Data and Analytics

Data comes in all types of forms and formats. When we talk about Big Data, we're referring to large volumes of data. Data from weather systems, communications systems, imaging platforms, and many other scenarios generate large amounts of data. This amount of data becomes increasingly hard to make sense of, and make decisions around. The volumes are so large that traditional forms of processing and analysis are no longer appropriate.

Open source cluster technologies have been developed, over time, to try to deal with these large data sets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions. Some of the most common big data and analytic service types in Azure are Azure SQL Data Warehouse, HDInsight, and Data Lake Analytics.

Azure SQL Data Warehouse



Azure SQL Data Warehouse is a cloud-based Enterprise Data Warehouse (EDW) that leverages MPP to run complex queries quickly across petabytes of data. You can use SQL Data Warehouse as a key component of a big data solution by importing big data into SQL Data Warehouse with simple PolyBase Transact-SQL (T-SQL) queries, and then use the power of MPP to run high-performance analytics. Once data is stored in SQL Data Warehouse, you can run analytics at massive scale. Compared to traditional database systems, analysis queries finish in seconds instead of minutes, or hours instead of days. See **SQL Data Warehouse**⁴⁸ for more details.

Azure HDInsight



Azure HDInsight is a fully managed, open-source analytics service for enterprises. It is a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. HDInsight allows you run popular open-source frameworks and create cluster types such as **Apache Spark**⁴⁹, **Apache Hadoop**⁵⁰, **Apache Kafka**⁵¹, **Apache HBase**⁵², **Apache Storm**⁵³, **Machine Learning Services**⁵⁴. HDInsight also supports a broad range of scenarios such as extraction, transformation, and loading (ETL); data warehousing; machine learning; and IoT. See **HDInsight**⁵⁵ for more general details.

⁴⁸ <https://azure.microsoft.com/en-us/services/sql-data-warehouse/>

⁴⁹ <https://docs.microsoft.com/en-us/azure/hdinsight/spark/apache-spark-overview>

⁵⁰ <https://docs.microsoft.com/en-us/azure/hdinsight/hadoop/apache-hadoop-introduction>

⁵¹ <https://docs.microsoft.com/en-us/azure/hdinsight/kafka/apache-kafka-introduction>

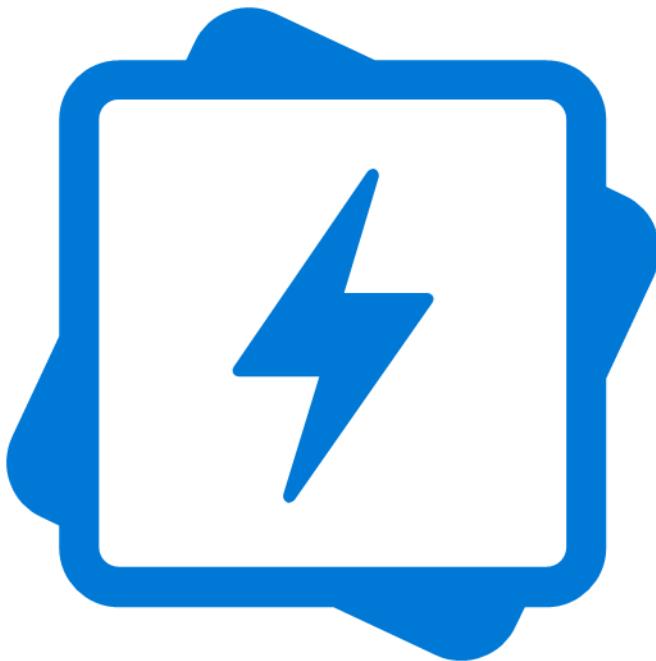
⁵² <https://docs.microsoft.com/en-us/azure/hdinsight/hbase/apache-hbase-overview>

⁵³ <https://docs.microsoft.com/en-us/azure/hdinsight/storm/apache-storm-overview>

⁵⁴ <https://docs.microsoft.com/en-us/azure/hdinsight/r-server/r-server-overview>

⁵⁵ <https://azure.microsoft.com/en-us/services/hdinsight/>

Azure Data Lake Analytics



Azure Data Lake Analytics is an on-demand analytics job service that simplifies big data. Instead of deploying, configuring, and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by setting the dial for how much power you need. You only pay for your job when it is running, making it more cost-effective. See **Data Lake Analytics**⁵⁶for more details.

Note: For a full list of big data and analytics services available with Azure, see the page **Analytics**⁵⁷.

Video: Artificial Intelligence



https://www.youtube.com/watch?v=m3_QmvDX1q8

Artifical Intelligence

Artificial Intelligence, in the context of cloud computing, is based around a broad range of services, the core of which is *Machine Learning*. Machine Learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes, and trends. Using machine learning, computers learn without being explicitly programmed.

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning helps recommend other products you might like based on what

⁵⁶ <https://azure.microsoft.com/en-us/services/data-lake-analytics/>

⁵⁷ <https://azure.microsoft.com/en-us/product-categories/analytics/>

you've purchased. Or when your credit card is swiped, machine learning compares the transaction to a database of transactions and helps detect fraud. And when your robot vacuum cleaner vacuums a room, machine learning helps it decide whether the job is done.

Some of the most common Artificial Intelligence and Machine Learning service types in Azure are:

Azure Machine Learning Service



The *Azure Machine Learning* service provides a cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It fully supports open-source technologies, so you can use tens of thousands of open-source Python packages with machine learning components such as *TensorFlow* and *scikit-learn*. Rich tools, such as *Jupyter notebooks* or the *Visual Studio Code Tools for AI*, make it easy to interactively explore data, transform it, and then develop, and test models. Azure Machine Learning service also includes features that automate model generation and tuning to help you create models with ease, efficiency, and accuracy.

The Azure Machine Learning service can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud. When you have the right model, you can easily deploy it in a container such as Docker in Azure. Use Machine Learning service if you work in a Python environment, you want more control over your machine learning algorithms, or you want to use open-source machine learning libraries.

See [Azure Machine Learning service⁵⁸](#) for more details.

Azure Machine Learning Studio



Azure Machine Learning Studio is a collaborative, drag-and-drop visual workspace where you can build, test, and deploy machine learning solutions without needing to write code. It uses pre-built and pre-configured machine learning algorithms and data-handling modules. Use Machine Learning Studio when you want to experiment with machine learning models quickly and easily, and the built-in machine learning algorithms are sufficient for your solutions. It does not provide as much control over machine learning algorithms as the Machine Learning Service we discussed earlier. See [Azure Machine Learning Studio⁵⁹](#) for more general details.

⁵⁸ <https://azure.microsoft.com/en-us/services/machine-learning-service/>

⁵⁹ <https://azure.microsoft.com/en-us/services/machine-learning-studio/>

Note: For a full list of Artificial Intelligence and Machine Learning services available with Azure, see the page [AI + Machine Learning](#)⁶⁰.

Video: Serverless Computing



https://www.youtube.com/watch?v=IU_KW00fdHU

Serverless Computing

Serverless computing is a cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment. You create an instance of the service and you add your code. No infrastructure configuration or maintenance is required, or even allowed.

You configure your serverless apps to respond to events. An event could be a REST endpoint, a periodic timer, or even a message received from another Azure service. The serverless app runs only when it's triggered by an event.

Scaling and performance are handled automatically, and you are billed only for the exact resources you use. You don't even need to reserve resources.

Some of the most common serverless service types in Azure are Azure Functions, Azure Logic Apps, and Azure Event Grid.

Azure Functions



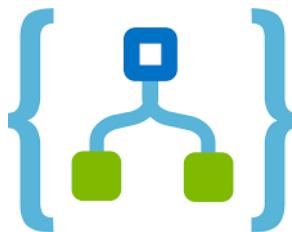
Azure Functions are ideal when you're only concerned with the code running your service and not the underlying platform or infrastructure. Azure Functions are commonly used when you need to perform work in response to an event—often via a REST request, timer, or message from another Azure service—and when that work can be completed quickly, within seconds or less.

Azure Functions scale automatically and charges accrue only when a function is triggered, so they're a solid choice when demand is variable. For example, you may be receiving messages from an IoT solution that monitors a fleet of delivery vehicles. You'll likely have more data arriving during business hours. Azure Functions can scale out to accommodate these busier times.

⁶⁰ <https://azure.microsoft.com/en-us/services/>

Furthermore, Azure Functions are stateless; they behave as if they're restarted every time they respond to an event. This is ideal for processing incoming data. And if state is required, they can be connected to an Azure storage service. See **Functions⁶¹** for more details.

Azure Logic Apps



Azure Logic Apps is a cloud service that helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. Logic Apps simplifies how you design and build scalable solutions—whether in the cloud, on premises, or both—for app integration, data integration, system integration, enterprise application integration (EAI), and business-to-business (B2B) integration.

Logic Apps are designed in a web-based designer and can execute logic triggered by Azure services without writing any code. To build enterprise integration solutions with Azure Logic Apps, you can choose from a growing gallery of over 200 connectors. These include services such as Salesforce, SAP, Oracle DB, and file shares. See **Logic Apps⁶²** for more details.

Azure Event Grid



Azure Event Grid allows you to easily build applications with event-based architectures. It's a fully-managed, intelligent event routing service that uses a publish-subscribe model for uniform event consumption. Event Grid has built-in support for events coming from Azure services, such as storage blobs and resource groups.

You can use Event Grid to support your own non-Azure-based events in near-real time, using custom topics. You can use filters to route specific events to different endpoints, and ensure your events are reliably delivered. See **Event Grid⁶³** for more details.

Note: For more details about serverless services available with Azure, see the page **Serverless in Azure⁶⁴**.

61 <https://azure.microsoft.com/en-us/services/functions/>

62 <https://azure.microsoft.com/en-us/services/logic-apps/>

63 <https://azure.microsoft.com/en-us/services/event-grid/>

64 <https://azure.microsoft.com/en-us/solutions/serverless/>

Demo: Run serverless code with Azure Functions in Azure portal



<https://www.youtube.com/watch?v=1H7alJ57BfU>

Walkthrough-Run serverless code with Azure Functions in Azure portal

In this walkthrough you write and run serverless code inside an *Azure Function App* in Azure portal.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Prerequisites

An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**⁶⁵ before you begin.

Steps

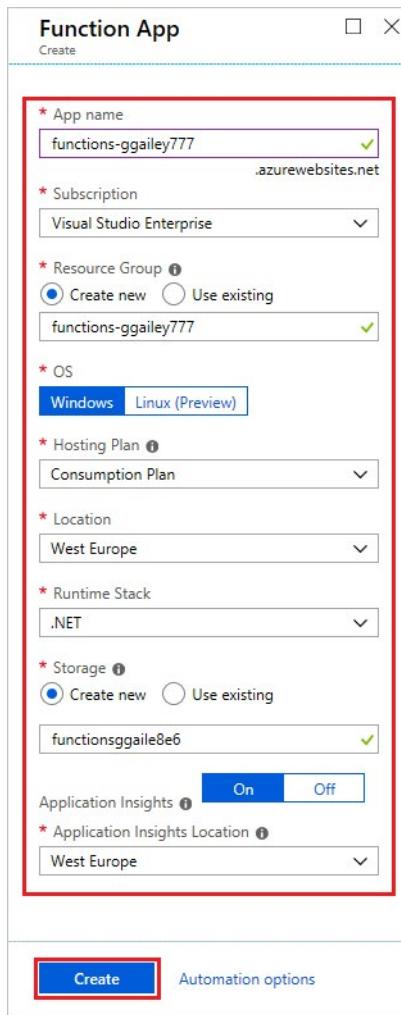
1. To create a new Azure Function App, sign in to the Azure Portal and locate the *Function App* service, then select **Create Function App**, or alternatively, click on this [Create Function App](#)⁶⁶ link and when prompted, sign into Azure Portal.
2. Fill in the Azure Function App settings fields with the following details.
 - **App name:** Provide a unique name that identifies your new Function App.
 - **Subscription:** Select an Azure subscription for your Function App.
 - **Resource Group:** Choose **Create new**. Provide a unique name for your new Resource Group, if Azure has not provided a name automatically.
 - **OS:** Select Windows. For Linux hosting, see [Create your first function running on Linux using the Azure CLI](#)⁶⁷.
 - **Hosting plan:** Choose Consumption plan. With Azure serverless hosting, you only pay for the time that your functions run. Using the default **Consumption Plan** means that resources are added dynamically as required by your functions.
 - **Location:** Choose the Azure region that is closest to your location.
 - **Runtime stack:** Select .NET (this is suitable for running C# and F# functions).
 - **Storage:** Choose **Create new**. Provide a unique name for your new storage account, if Azure has not provided a name automatically.

⁶⁵ <https://azure.microsoft.com/free/>

⁶⁶ <https://portal.azure.com/#create/Microsoft.FunctionApp>

⁶⁷ <https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-azure-function-azure-cli-linux>

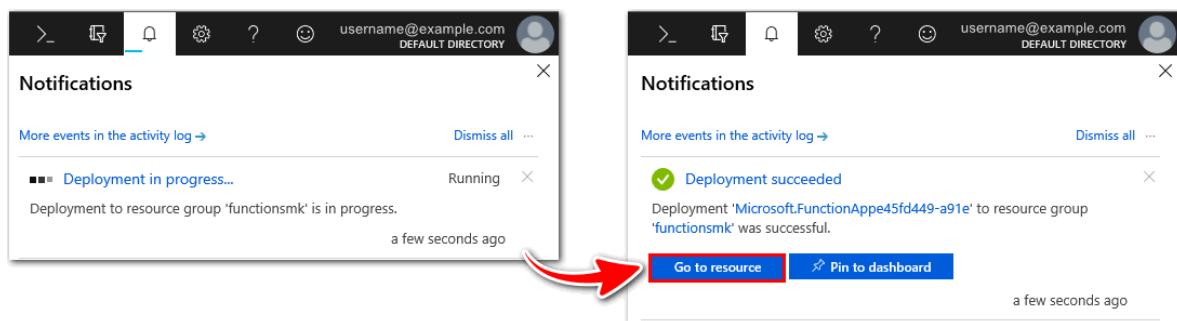
- **Application Insights:** Leave this set to the default value, provided by Azure automatically.



3. Select the **Create** button to begin provisioning and deploying your new Azure Function App.

Note: When the deployment starts, a notification appears in Azure Portal indicating the deployment is in progress. Another notification is displayed when the deployment has completed successfully.

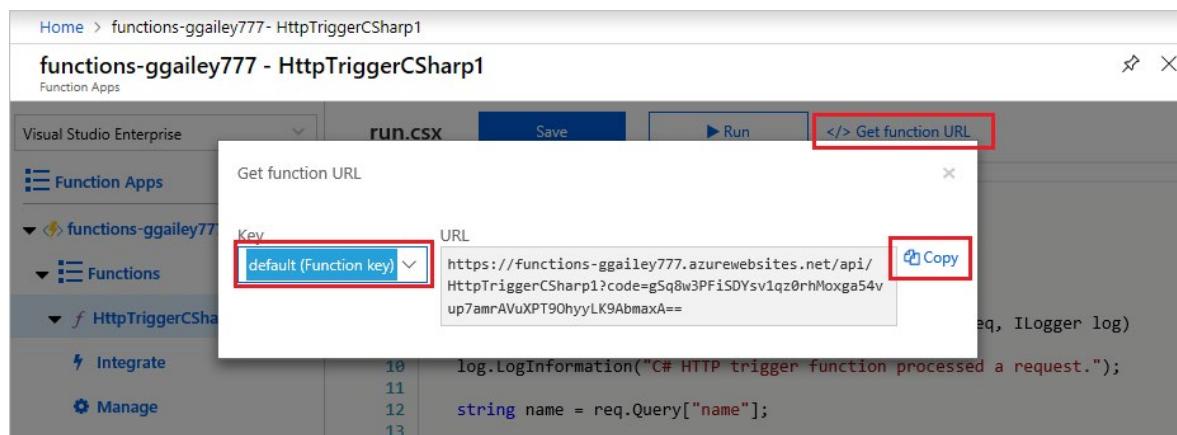
4. When the deployment has completed, choose **Go to resource** from the notification area to view your new Azure Function App. You can also select **All resources** from the main Azure menu, then choose your Azure Function App from the list of resources.



5. To create an *HTTP Triggered Function*, use the down arrow icon to expand your Azure Function App. Select the "+" button next to **Functions**. Choose **In-portal**, and select **Continue**.

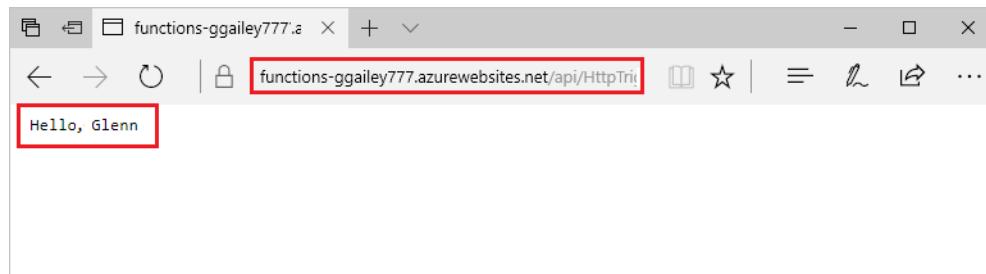
6. Choose **WebHook + API**, and then select **Create**.

7. Select **</> Get function URL** from the within the function editor. Set the **Key** value to **default** (Function key) using the dropdown. Then, select **Copy** to copy the function URL.



- Paste the copied function URL into your web browser's address bar. Append &name=<yourname> to the end of the URL.

Note: Here, <yourname> refers to your given first name. Navigate to the URL to see the "Hello" message, followed by the name you provided, displayed in your browser. The URL should be similar to <https://azfuncck01.azurewebsites.net/api/HttpTrigger1?code=X9xx9999xXXXXX9x9xxxXX==&name=glen>



- When your function runs, trace information is written to log files in Azure. To view the logs in Azure portal, return to the function editor, and select the **Logs** button.



Congratulations! You have written and run serverless code inside an Azure Function App, in Azure portal, successfully.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: DevOps



<https://www.youtube.com/watch?v=eoQqnVmSAog>

DevOps

DevOps (Deployment and Operations) brings together people, processes, and technology, automating software delivery to provide continuous value to your users. Azure DevOps Services allows you to create, build, and release pipelines that provide continuous integration, delivery, and deployment for your applications. You can integrate repositories and application tests, perform application monitoring, and work with build artifacts. You can also work with and backlog items for tracking, automate infrastructure deployment, and integrate a range of third-party tools and services such as Jenkins and Chef. All of these functions and many more are closely integrated with Azure to allow for consistent, repeatable deployments for your applications to provide streamlined build and release processes.

Some of the main DevOps services available with Azure are Azure DevOps Services, and Azure DevTest Labs.

Azure DevOps Services



Azure DevOps Services (formerly known as *Visual Studio Team Services (VSTS)*), provides development collaboration tools including high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. See [Azure DevOps⁶⁸](#) for more details.

Azure DevTest Labs



⁶⁸ <https://azure.microsoft.com/en-us/services/devops>

Azure DevTest Labs is a service that helps developers and testers quickly create environments in Azure, while minimizing waste and controlling cost. Users can test their latest application versions by quickly provisioning Windows and Linux environments using reusable templates and artifacts. You can easily integrate your deployment pipeline with DevTest Labs to provision on-demand environments. With DevTest Labs you can scale up your load testing by provisioning multiple test agents, and create pre-provisioned environments for training and demos. See **Azure DevTest Labs**⁶⁹ for more general details.

Note: For more general details on DevOps services available with Azure, see the page **DevOps**⁷⁰.

⁶⁹ <https://azure.microsoft.com/en-us/services/devtest-lab/>

⁷⁰ <https://azure.microsoft.com/en-us/solutions/devops>

Azure Management Tools

Video: Azure Management Tools



<https://www.youtube.com/watch?v=oTiDdp8RICU>

Azure Management Tools

You can configure and manage Azure using a broad range of tools and platforms. There are tools available for the command line, language-specific Software Development Kits (SDKs), developer tools, tools for migration, and many others. Tools that are commonly used for day-to-day management and interaction include: *Azure Portal*, for interacting with Azure via a Graphical User Interface (GUI); *Azure PowerShell*, *Azure Command-Line Interface* (CLI), and *Azure Cloud Shell*, for command line and automation-based interactions with Azure.

Creating administration scripts and using automation tools is a powerful way to optimize your work flow. You can automate common repetitive tasks, and once a script has been verified it will run consistently, thereby reducing errors.

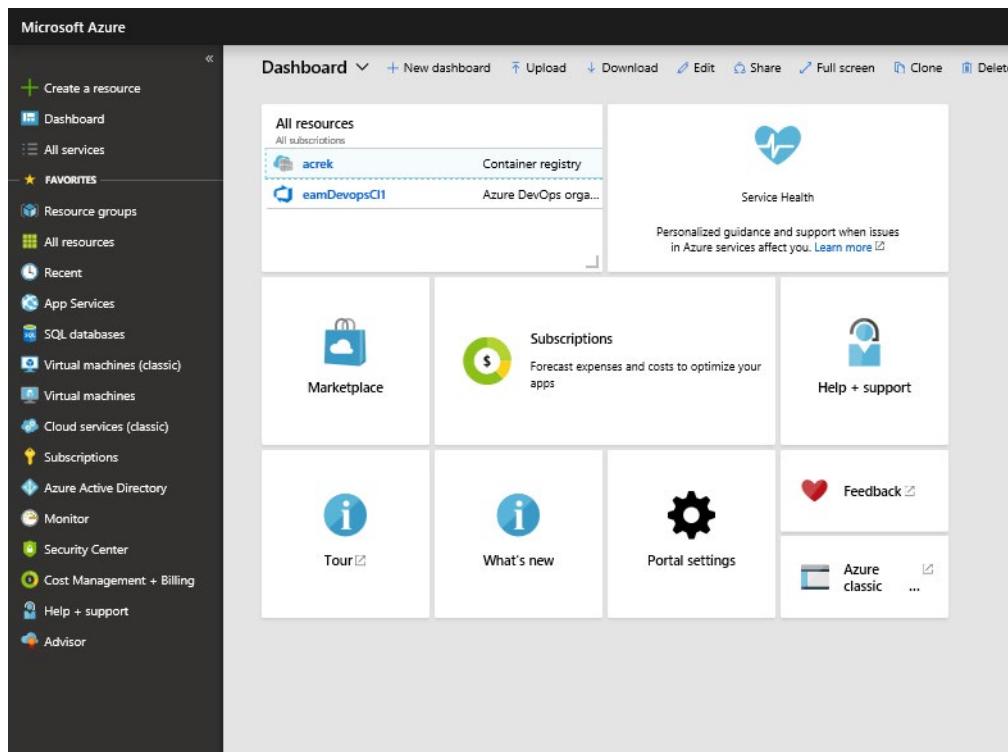
Azure Portal

Azure Portal is a website that you can access with a web browser, by going to the URL <https://portal.azure.com>⁷¹. From here you can interact manually with all the Azure services. You can identify a service you are looking for, obtain links for help and more learning on particular topics, and deploy, manage and delete resources. It also guides you through complex administrative tasks by providing wizards and tooltips.

The dashboard view provides high-level details about your Azure environment. You can customize the portal view as you need by moving and resizing tiles, displaying just particular services of interest, accessing links for help and support, and providing feedback.

The portal does not provide any way to automate repetitive tasks. For example, to set up multiple VMs, you would need to create them one at a time by completing the wizard for each VM. This can be time-consuming and error-prone for complex tasks.

⁷¹ <https://portal.azure.com>



Azure PowerShell

Azure PowerShell is a module that you add to Windows PowerShell or PowerShell Core that enables you to connect to your Azure subscription and manage resources. Azure PowerShell requires Windows PowerShell to function. PowerShell provides services such as the shell window and command parsing. Azure PowerShell then adds the Azure-specific commands.

For example, Azure PowerShell provides the **New-AzureRmVm** command that creates a virtual machine for you inside your Azure subscription. To use it, you would launch PowerShell, sign in to your Azure account using the command `Connect-AzureRMAccount`, and then issue a command such as:

```
New-AzureRmVm  
  -ResourceGroupName "TesResourceGroup"  
  -Name "Testvm"  
  -Image "UbuntuLTS"  
  ...
```

```

PS C:\WINDOWS\system32> New-AzureRmVm
>> -ResourceGroupName "CrmTestingResourceGroup"
>> -Name "CrmUnitTests"
>> -Image "UbuntuLTS"

cmdlet New-AzureRmVm at command pipeline position 1
Supply values for the following parameters:
Credential

ResourceGroupName      : CrmTestingResourceGroup
Id                    : /subscriptions/974e6e39-73eb-48b0-9226-dae31425c367/resourceGroups/CrmTestingResourceGroup/providers/Microsoft.Compute/virtualMachines/CrmUnitTests
VmId                 : 9cc7f63a-1ad5-495b-8ccd-f32652bccb9
Name                  : CrmUnitTests
Type                  : Microsoft.Compute/virtualMachines
Location              : eastus
Tags                  :
HardwareProfile       : {VmSize}
NetworkProfile        : {NetworkInterfaces}
OsProfile              : {ComputerName, AdminUsername, LinuxConfiguration, Secrets}
ProvisioningState     : Succeeded
StorageProfile         : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName : crmunittests-d01add.eastus.cloudapp.azure.com

```

Note: *PowerShell Core* is a cross-platform version of PowerShell that runs on Windows Linux or macOS. Details are available from the page [What's New in PowerShell Core 6.1⁷²](#) which is now also available.

Azure CLI

Azure CLI is a cross-platform command-line program that connects to Azure and executes administrative commands on Azure resources. *Cross platform* means that it can be run on Windows, Linux, or macOS. For example, to create a VM, you would open a command prompt window, sign in to Azure using the command `az login`, create a resource group, then use a command such as:

```

az vm create \
--resource-group Testrg1 \
--name Testvm \
--image UbuntuLTS
--generate-ssh-keys
...

```

```

C:\WINDOWS\system32>az vm create --resource-group testrg1 --name testvm1 --image UbuntuLTS
{/ Finished ..
{
  "fqdns": "",
  "id": "/subscriptions/999x99-99-99x9-99x9-99990-9x9x/resourceGroups/testrg1/providers/Microsoft.Compute/virtualMachines/testvm1",
  "location": "westeurope",
  "macAddress": "00-00-0A-21-5D-4F",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "40.113.108.152",
  "resourceGroup": "testrg1"
}

```

Azure Cloud Shell

Azure Cloud Shell is a browser-based scripting environment in your portal. It provides the flexibility of choosing the shell experience that best suits the way you work. Linux users can opt for a Bash experience, while Windows users can opt for PowerShell.

⁷² <https://docs.microsoft.com/en-us/powershell/scripting/whats-new/what-s-new-in-powershell-core-60?view=powershell-6>

A storage account is required to use the cloud shell and you will be prompted to create one when accessing the Azure cloud shell.

Note: You can access Azure Cloud Shell by going to <https://shell.azure.com/>⁷³.

Note: There are also **Azure SDKs** in a range of languages, as well as **REST APIs** through which you can configure Azure. For a full list of tools available, see the [Downloads](#)⁷⁴ page.

Demo: Customize the Azure Portal



https://www.youtube.com/watch?v=9XgJG_vUaXk

Walkthrough-Working with the Azure CLI

In this walkthrough task we will install the Azure CLI on our local machine, then create a virtual machine using the Azure CLI and an Azure Resource Manager template, then verified that deployment using the Azure CLI in the Azure Cloud Shell.

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](#)⁷⁵ webpage.
- A local environment is also needed such as a Windows, Linux or MacOS

Note: The following steps are based on a Windows installation, however they could equally be applicable to a Mac or Linux environment. However there are specific installation steps for each environment. To see the installation steps for your particular environment see the

[Install the Azure CLI](#)⁷⁶ page.

Steps

We will install Azure CLI on the Windows operating system using the MSI installer:

1. To download the Azure CLI msi, click on the URL <https://aka.ms/installazurecliwindows>⁷⁷, and in the browser, select to **Run**.

⁷³ <https://shell.azure.com/>

⁷⁴ <https://azure.microsoft.com/en-us/downloads/>

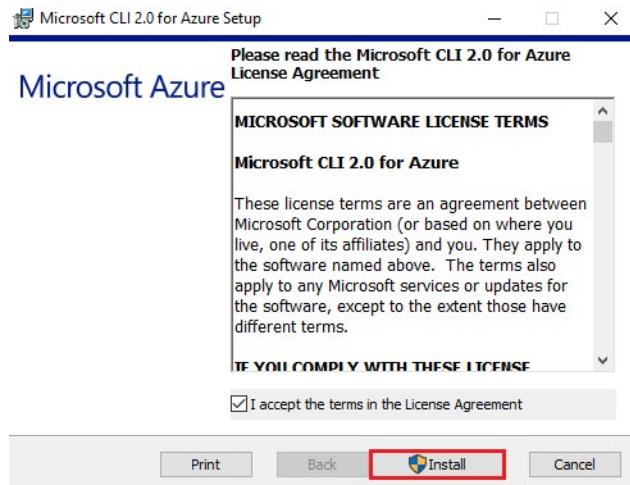
⁷⁵ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

⁷⁶ <https://docs.microsoft.com/cli/azure/install-azure-cli>

⁷⁷ <https://aka.ms/installazurecliwindows>



- In the installation wizard, accept the license terms, and then click **Install**.

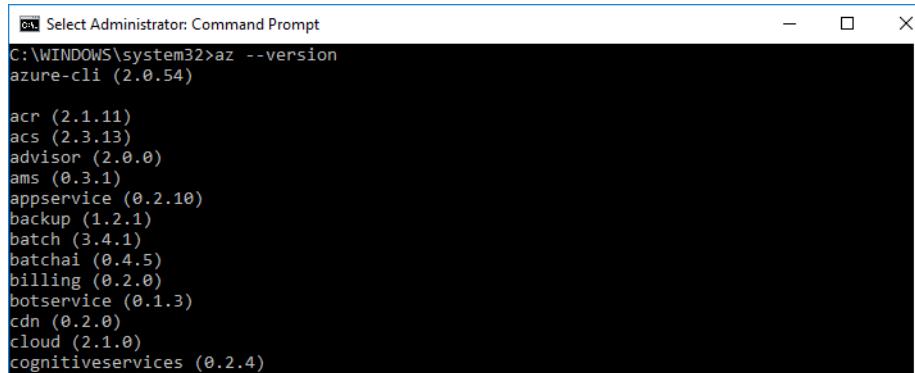


- In the **User Account Control** dialog, select **Yes**.
- Once successfully installed, the Azure CLI is run by opening a Bash shell for Linux or macOS, or from the command prompt or PowerShell for Windows. Open a command prompt as administrator.
- Login to your Azure subscription by running the below command and following the prompts

```
az login
```

- Verify your installation by running the version check command and ensuring it runs successfully:

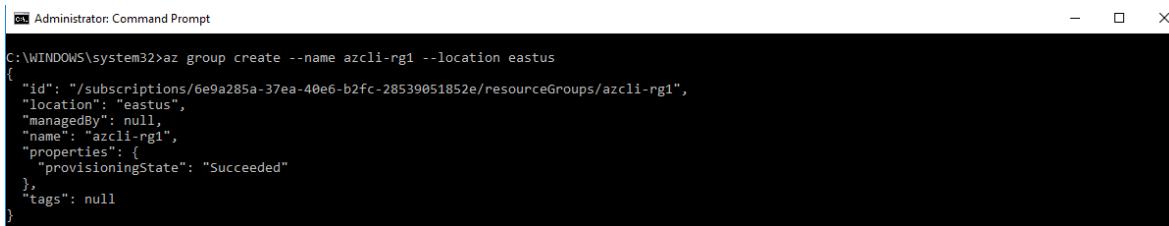
```
az --version
```



Note: Running Azure CLI from PowerShell has some advantages over running Azure CLI from the Windows command prompt. PowerShell provides more tab completion features than the command prompt.

- Create a resource group to deploy your resources to, by running the following command:

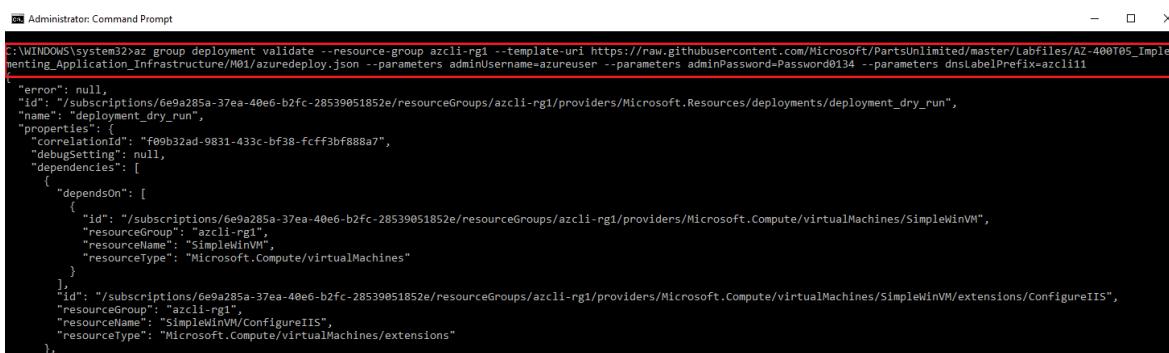
```
az group create --name < resource group name > --location < your nearest  
datacenter >
```



```
C:\WINDOWS\system32>az group create --name azcli-rg1 --location eastus  
{  
  "id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/azcli-rg1",  
  "location": "eastus",  
  "managedBy": null,  
  "name": "azcli-rg1",  
  "properties": {  
    "provisioningState": "Succeeded"  
  },  
  "tags": null  
}
```

8. We will now deploy a virtual machine and configure it using an Azure Resource Manager template. The template is available on GitHub at the location <https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json>⁷⁸, and we will call the script using an Azure CLI command and some other parameters.
9. Before deploying we will validate the template and command by running the following Azure CLI command, substituting the values with your own, specifying a username and password and a unique name for the virtual machine DNS label prefix value. The command should run successfully without error, identify what is causing the error, modify it and run the command again until it does validate successfully.

```
az group deployment validate `  
  --resource-group < resource group created earlier > `  
  --template-uri https://raw.githubusercontent.com/Azure/azure-quick-  
  start-templates/master/101-vm-simple-windows/azuredeploy.json `  
  --parameters adminUsername=$USERNAME `  
  --parameters adminPassword=$PASSWORD `  
  --parameters dnsLabelPrefix=$DNS_LABEL_PREFIX
```



```
C:\WINDOWS\system32>az group deployment validate --resource-group azcli-rg1 --template-uri https://raw.githubusercontent.com/Microsoft/PartsUnlimited/master/Labfiles/AZ-400T05_Implementing_Application_Infrastructure/M01/azuredeploy.json --parameters adminUsername=azureuser --parameters adminPassword=Password0134 --parameters dnsLabelPrefix=azcli11  
  
{"error": null,  
 "id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/azcli-rg1/providers/Microsoft.Resources/deployments/deployment_dry_run",  
 "name": "deployment_dry_run",  
 "properties": {  
   "correlationId": "f0eb32ad-9831-433c-bf38-fcff3bf888a7",  
   "debugSetting": null,  
   "dependencies": [  
     {  
       "dependsOn": [  
         {  
           "id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/azcli-rg1/providers/Microsoft.Compute/virtualMachines/SimpleWinVM",  
           "resourceGroup": "azcli-rg1",  
           "resourceName": "SimpleWinVM",  
           "resourceType": "Microsoft.Compute/virtualMachines"  
         },  
         {"id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/azcli-rg1/providers/Microsoft.Compute/virtualMachines/SimpleWinVM/extensions/ConfigureIIS",  
          "resourceGroup": "azcli-rg1",  
          "resourceName": "SimpleWinVM/ConfigureIIS",  
          "resourceType": "Microsoft.Compute/virtualMachines/extensions"  
        }  
      ]  
    }  
  }  
}
```

10. Deploy the resource by running the following command, substituting the same values as earlier:

```
az group deployment create `  
  --name MyDeployment `  
  --resource-group <rgn>[sandbox resource group name]</rgn> `  
  --template-uri https://raw.githubusercontent.com/Azure/azure-quick-  
  start-templates/master/101-vm-simple-windows/azuredeploy.json `  
  --parameters adminUsername=$USERNAME `  
  --parameters adminPassword=$PASSWORD `
```

⁷⁸ <https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json>

```
--parameters dnsLabelPrefix=$DNS_LABEL_PREFIX
```

```
C:\WINDOWS\system32>az group deployment create --name MyDeployment --resource-group azcli-rg1 --template-uri https://raw.githubusercontent.com/Microsoft/PartsUnlimited/master/Labfiles/AZ-400T05_Implementing_Application_Infrastructure/M01/azuredeploy.json --parameters adminUsername=azureuser --parameters adminPassword=Password0134 --parameters dnsLabelPrefix=azcli11
-- Running ..
```

11. Verify the deployment by signing into the Azure portal at <https://portal.azure.com>⁷⁹

12. Go to the resource group you created and verify the virtual machine and resources are present, note the name of the virtual machine is *SimpleWinVM*

The screenshot shows the Azure Resource Group 'azcli-rg1' details and a list of deployed resources:

NAME	TYPE	LOCATION
3kuomarwq4djisawinvm	Storage account	East US
myPublicIP	Public IP address	East US
myVMNIC	Network interface	East US
MyVNET	Virtual network	East US
SimpleWinVM	Virtual machine	East US
SimpleWinVM_disk2_fbd77db70b6642acb003b5fb62e8e531	Disk	East US
SimpleWinVM_OsDisk_1_4831a665d89447fcff1ff2834896e4e	Disk	East US

13. It is also possible to use the Azure CLI with the **Azure Cloud Shell**. The **Azure Cloud Shell** has the Azure CLI already installed. Open the **Azure Cloud Shell** by clicking on the *Azure Cloud Shell icon* in the top right of the Azure Portal.



14. The browser becomes split and the Azure cloud Shell opens in the bottom half of your existing browser and you are prompted to select between **Bash** or **PowerShell**, select **Bash**



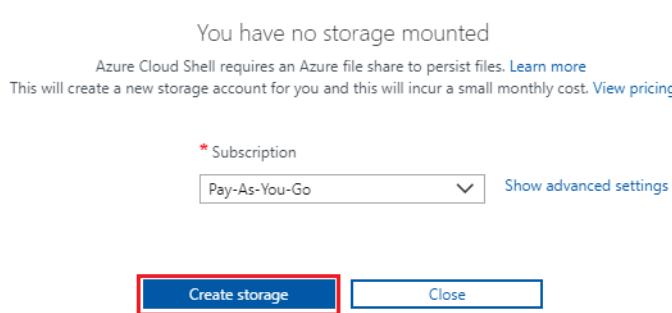
Welcome to Azure Cloud Shell

Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session.

Bash | PowerShell

15. You are prompted to create storage, select **Create storage**, and allow the Azure Cloud Shell to initialize. You do not need to sign into the Azure Cloud Shell, it does this automatically for you.

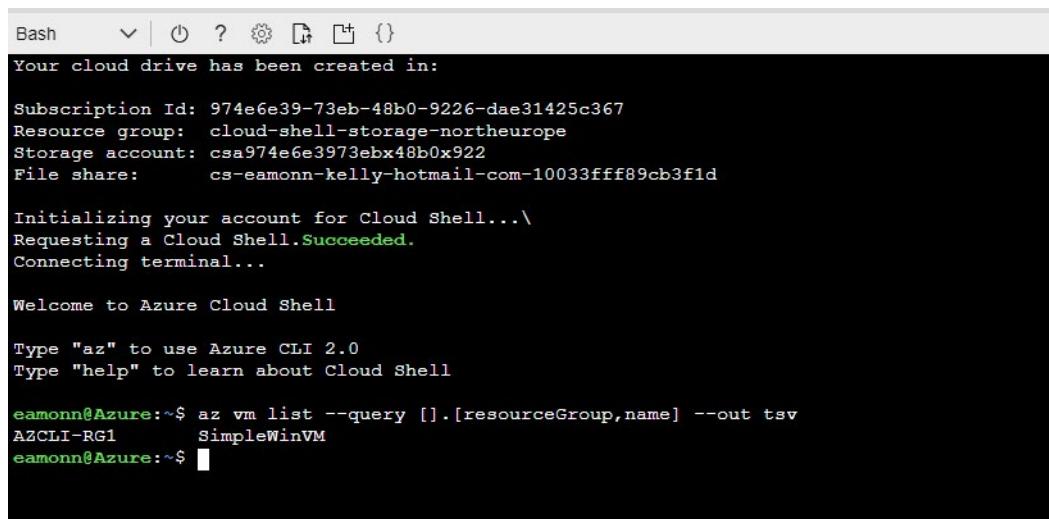
⁷⁹ <https://portal.azure.com>



The screenshot shows a dialog box from the Azure Cloud Shell. At the top, it says "You have no storage mounted" with a close button "X" on the right. Below that, it states "Azure Cloud Shell requires an Azure file share to persist files. [Learn more](#)" and "This will create a new storage account for you and this will incur a small monthly cost. [View pricing](#)". There is a dropdown menu labeled "Subscription" with "Pay-As-You-Go" selected, and a link "Show advanced settings". At the bottom, there are two buttons: "Create storage" (highlighted with a red border) and "Close".

16. Obtain a list of the virtual machines present in your subscription, and display only the resource group and virtual machine name by running the command:

```
az vm list --query [].[resourceGroup,name] --out tsv
```



The screenshot shows the Azure Cloud Shell terminal. It starts with "Bash" and various icons. It then displays the message "Your cloud drive has been created in:" followed by the details of the storage account: Subscription Id: 974e6e39-73eb-48b0-9226-dae31425c367, Resource group: cloud-shell-storage-northeurope, Storage account: csa974e6e3973ebx48b0x922, File share: cs-eamonn-kelly-hotmail-com-10033fff89cb3f1d. It then shows the process of initializing the account, requesting a Cloud Shell, and connecting to the terminal. Finally, it shows the command being run: "az vm list --query [].[resourceGroup,name] --out tsv", which returns the output: AZCLI-RG1 SimpleWinVM.

Congratulations! You have installed the Azure CLI on your local machine, created a virtual machine using the Azure CLI and an Azure Resource Manager template, then verified that deployment using the Azure CLI in the Azure Cloud Shell.

Note: Don't forget to delete any resources you deployed to avoid incurring additional costs from them.

Demo: Create VMs from a script with Azure PowerShell



<https://www.youtube.com/watch?v=YITj45mtYjA>

Walkthrough—Create VMs from a script with Azure PowerShell

In this walkthrough you write and run a local PowerShell script. The PowerShell script uses the *Azure PowerShell* module to create three virtual machines (VMs) in Azure from a Linux Ubuntu image.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Note: The screenshots throughout this walkthrough are Windows specific, but the PowerShell commands will run on any suitable Operating System platform with Azure PowerShell.

Prerequisites

- An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**⁸⁰ before you begin.
- Installing the Azure PowerShell module requires *Windows PowerShell* 5.1 or higher on Windows, or *PowerShell Core* 6.0 on Windows, Linux, macOS and ARM. Follow these instructions for **Installing various versions of PowerShell**⁸¹ on your local machine.
- You must have a text editor installed to write a new PowerShell script. You could use the **PowerShell Integrated Scripting Environment (ISE)**⁸² or another option could be to use **Visual Studio Code**⁸³.

Steps

1. Open a text editor. Make a new file, and add the following code into the new file. The comments explain each of the commands within the script file.

```
# capture the input parameter in a variable
param([string]$resourceGroup)

# prompt for a username and password for the VMs admin account
# and capture the result in a variable
$adminCredential = Get-Credential -Message "Enter a username and password
for the VM administrator."

# Add a loop that executes three times to create a new VM for each loop
iteration
For ($i = 1; $i -le 3; $i++)
{
    # create a name for each VM, store it in a variable and output it to
    the console
    $vmName = "AzDemo" + $i
    Write-Host "Creating VM: " $vmName

    # create a VM using the $vmName variable
    New-AzVm -ResourceGroupName $resourceGroup -Name $vmName -Credential
    $adminCredential -Image UbuntuLTS
```

⁸⁰ <https://azure.microsoft.com/free/>

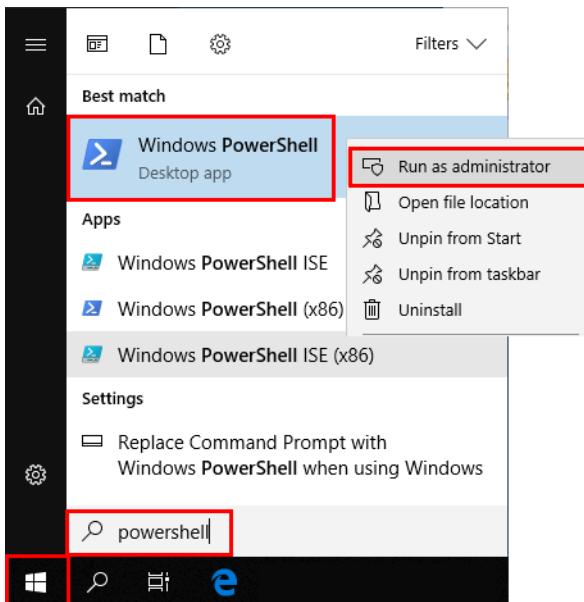
⁸¹ <https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell?view=powershell-6>

⁸² <https://docs.microsoft.com/en-us/powershell/scripting/components/ise/windows-powershell-integrated-scripting-environment-ise?view=powershell-6>

⁸³ <https://visualstudio.microsoft.com/>

```
}
```

2. Save the new file as `azdemo.ps1`. Make a note of the directory location where you save the script file, you will be required to recall the directory location in Step 6.
3. Open a new PowerShell session with *elevated* privileges.
 - **Windows:** Select the **Start** icon from the task bar. Type **Powershell**. Right select the **Windows PowerShell Desktop App** icon. Choose **Run as administrator**.



- **Linux and macOS:** In a terminal, launch PowerShell Core with elevated privileges using the following command.

```
sudo pwsh
```

4. At the PowerShell prompt, install the Azure PowerShell module (`Az`) by running the following command.

```
Install-Module Az -AllowClobber
```

Answer **Yes** or **Yes to All**, if prompted, to trust the `Az` module.

```
[+] Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Install-Module Az -AllowClobber

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\WINDOWS\system32>
```

Note: Windows users should agree to install the *NuGet* provider, and agree to install modules from the *PowerShell Gallery* (PSGallery), if prompted. If you receive script execution failures, run `Set-Execution-`

Policy RemoteSigned in an elevated PowerShell session. Running the command will unrestricted your execution policy, and allow you to install and run modules from the PSGallery.

5. Update the Az module by running the following command.

```
Update-Module -Name Az
```

Answer **Yes** or **Yes to All**, if prompted, to trust updates to the Az module. If you already have the latest version of the Az module installed, the prompt will be returned automatically.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Update-Module -Name Az
PS C:\WINDOWS\system32>
```

6. Use the `cd` command to change into the directory that contains the PowerShell script file `azdemo.ps1` that you created in Step 1. Replace `scriptsdir` with the actual directory where you saved the script file.

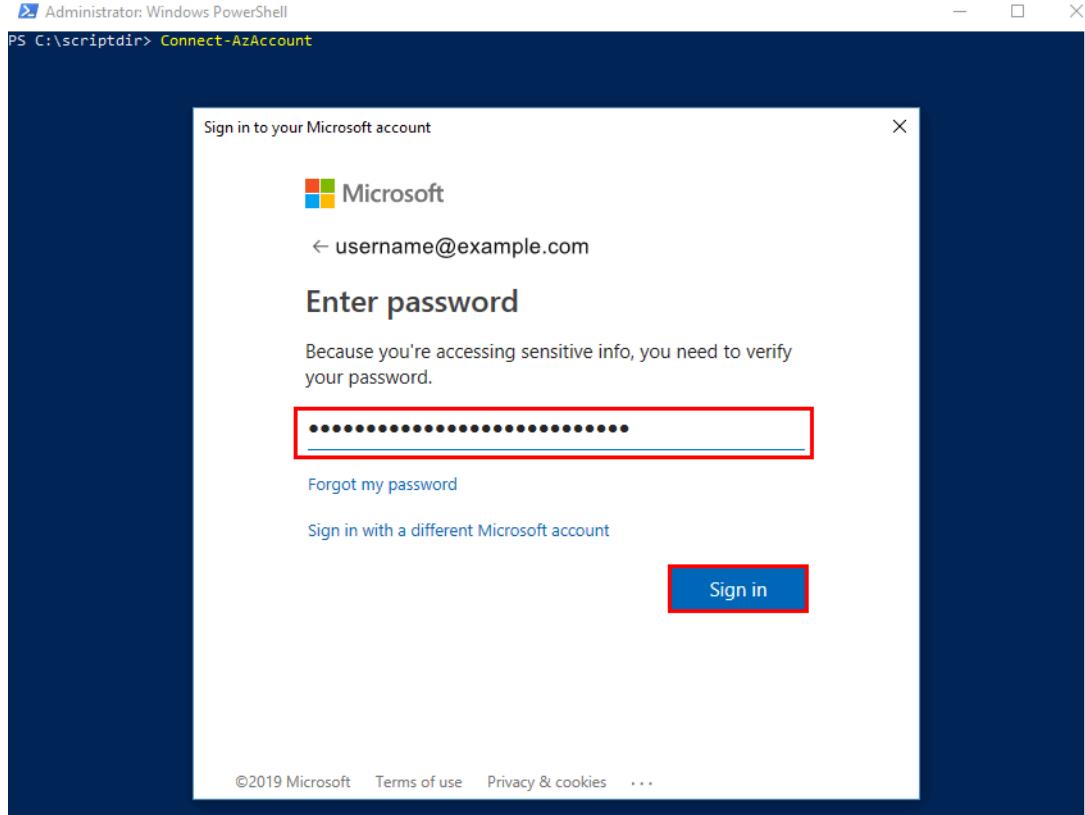
```
cd C:\scriptsdir
```



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> cd C:\scriptdir\
PS C:\scriptdir>
```

7. Sign into Azure by running the following command. When prompted, provide your Azure login credentials and select the **sign in** button.

```
Connect-AzAccount
```

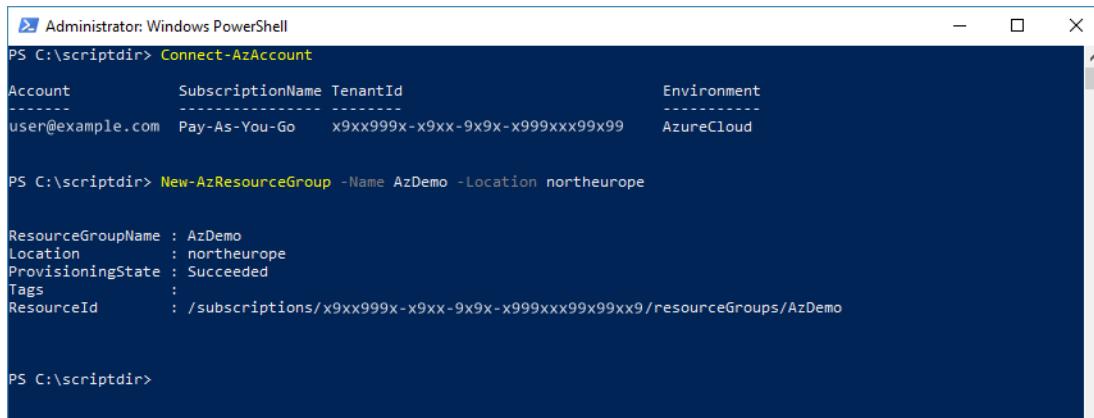


Note: The following Step 8 assumes that you have a single Azure subscription associated with your Azure account. If you have multiple subscriptions, you can get a list of your subscriptions using the command `Get-AzSubscription`. Specify which subscription to use with the command `Select-AzSubscription -Subscription "Name of your subscription"`. Substitute the actual name of the subscription you want to use for "Name of your subscription".

8. Create a new resource group using the following command.

```
New-AzResourceGroup -Name "name" -Location "location"
```

Replace `name` with a suitable name for the new resource group. For example, `AzDemo`. Add a value for `location` that corresponds to the Azure region closest to you. For example, `northeurope`.



```

Administrator: Windows PowerShell
PS C:\scriptdir> Connect-AzAccount
Account          SubscriptionName TenantId           Environment
-----          -----
user@example.com Pay-As-You-Go  x9xx999x-x9xx-9x9x-x999xxx99x99  AzureCloud

PS C:\scriptdir> New-AzResourceGroup -Name AzDemo -Location northeurope

ResourceGroupName : AzDemo
Location         : northeurope
ProvisioningState: Succeeded
Tags             :
ResourceId       : /subscriptions/x9xx999x-x9xx-9x9x-x999xxx99x99/resourceGroups/AzDemo

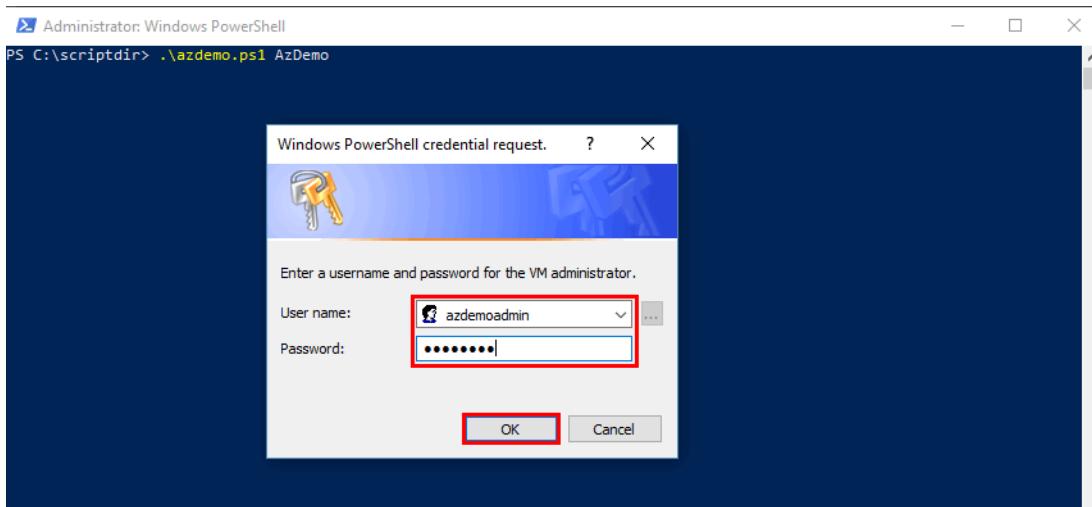
PS C:\scriptdir>

```

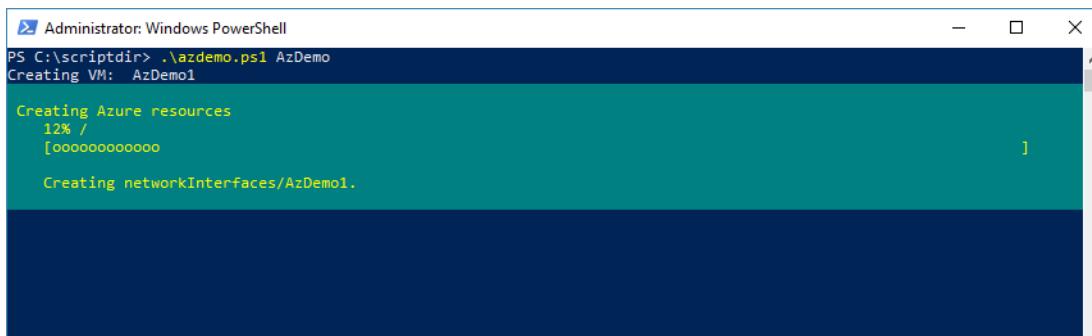
9. Execute the azdemo.ps1 script by running the following command. Substitute the name of the resource group that you created in the previous Step 8 for resource group name.

```
.\azdemo.ps1 "resource group name"
```

10. When prompted, provide a username and password for the VM administrator, and select **ok**. For example, for the **User name** enter azdemoadmin and for the **Password** enter pa\$\$W0rd101.



11. The script will begin creating the Azure resources required by each VM, and may take several minutes to complete. Wait for the script to finish before you go to Step 12.



```
PS C:\scriptdir> .\azdemo.ps1 AzDemo
Creating VM: AzDemo1

ResourceGroupName : AzDemo
Id              : /subscriptions/x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compute/virtualMachines/AzDemo1
VmId            : x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9
Name             : AzDemo1
Type             : Microsoft.Compute/virtualMachines
Location         : northeurope
Tags             : {}
HardwareProfile : {VmSize}
NetworkProfile  : {NetworkInterfaces}
OSProfile        : {ComputerName, AdminUsername, LinuxConfiguration, Secrets, AllowExtensionOperations}
ProvisioningState : Succeeded
StorageProfile   : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName : azdemo1- 9x9xx .northeurope.cloudapp.azure.com

Creating VM: AzDemo2

ResourceGroupName : AzDemo
Id              : /subscriptions/x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compute/virtualMachines/AzDemo2
VmId            : x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9
Name             : AzDemo2
Type             : Microsoft.Compute/virtualMachines
Location         : northeurope
Tags             : {}
HardwareProfile : {VmSize}
NetworkProfile  : {NetworkInterfaces}
OSProfile        : {ComputerName, AdminUsername, LinuxConfiguration, Secrets, AllowExtensionOperations}
ProvisioningState : Succeeded
StorageProfile   : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName : azdemo2- 9x9xx .northeurope.cloudapp.azure.com

Creating VM: AzDemo3

ResourceGroupName : AzDemo
Id              : /subscriptions/x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compute/virtualMachines/AzDemo3
VmId            : x9xxxx9x-9xxx-9x99-x9x9-9x9999x9x9
Name             : AzDemo3
Type             : Microsoft.Compute/virtualMachines
Location         : northeurope
Tags             : {}
HardwareProfile : {VmSize}
NetworkProfile  : {NetworkInterfaces}
OSProfile        : {ComputerName, AdminUsername, LinuxConfiguration, Secrets, AllowExtensionOperations}
ProvisioningState : Succeeded
StorageProfile   : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName : azdemo3- 9x9xx .northeurope.cloudapp.azure.com

PS C:\scriptdir>
```

12. When the script is finished, verify that it ran successfully by looking at the resources listed in the resource group that you created in Step 8. When you run the following command you should see three VMs, each with a unique name.

```
Get-AzResource -ResourceType Microsoft.Compute/virtualMachines
```

```

Administrator: Windows PowerShell
PS C:\scriptdir> Get-AzResource -ResourceType Microsoft.Compute/virtualMachines

Name          : AzDemo1
ResourceGroupName : AzDemo
 ResourceType    : Microsoft.Compute/virtualMachines
 Location       : northeurope
 ResourceId     : /subscriptions/x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compu
                  te/virtualMachines/AzDemo1

Name          : AzDemo2
ResourceGroupName : AzDemo
 ResourceType    : Microsoft.Compute/virtualMachines
 Location       : northeurope
 ResourceId     : /subscriptions/x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compu
                  te/virtualMachines/AzDemo2

Name          : AzDemo3
ResourceGroupName : AzDemo
 ResourceType    : Microsoft.Compute/virtualMachines
 Location       : northeurope
 ResourceId     : /subscriptions/x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9/resourceGroups/AzDemo/providers/Microsoft.Compu
                  te/virtualMachines/AzDemo3

PS C:\scriptdir>

```

13. The suffix `AzVM` is specific to VM-based commands in Azure PowerShell. The following are examples of other Azure PowerShell commands you can try with `AzVM`.

Stop a running VM named `xyz` in the resource group named `abc`

```
Stop-AzVM -ResourceGroupName abc -Name xyz
```

Start a stopped VM named `xyz` in the resource group named `abc`

```
Start-AzVM -ResourceGroupName abc -Name xyz
```

Restart the VM named `xyz` in the resource group named `abc`

```
Restart-AzVM -ResourceGroupName abc -Name xyz
```

Update the configuration for the VM named `xyz` in the resource group named `abc`

```
Update-AzVM -ResourceGroupName abc -Name xyz
```

Delete the VM named `xyz` from the resource group named `abc`

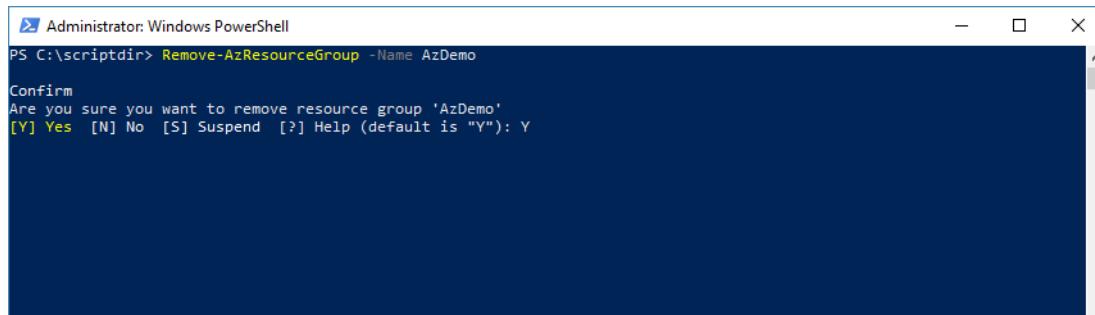
```
Remove-AzVM -ResourceGroupName abc -Name xyz
```

Substitute the name of the resource group that you created in Step 8 for `abc`. Replace `xyz` with the name of a VM you listed in Step 12. If you wish you can also have a look in the Azure Portal to verify the virtual machines are present in the GUI.

14. When you are finished, use the following Azure PowerShell command to delete the resource group and all the resources within it.

```
Remove-AzResourceGroup -Name "Resource group name"
```

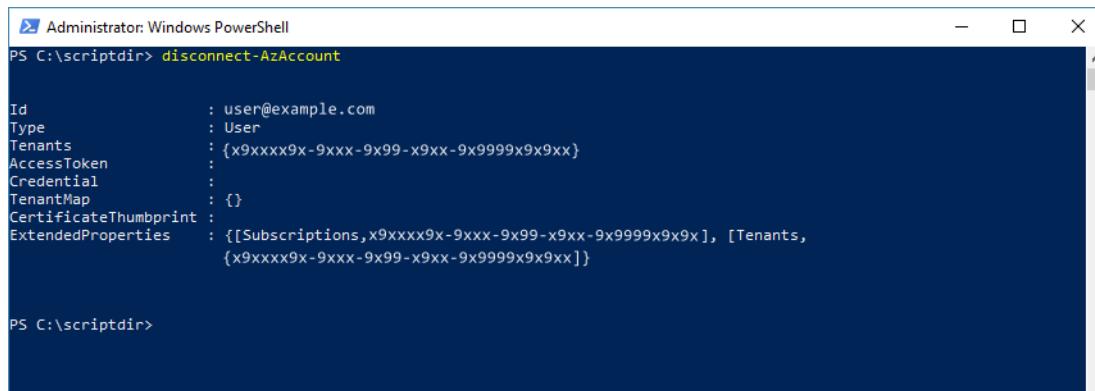
Substitute the name of the resource group you created in Step 8 for `resource group name`. When asked to confirm the deletion, answer **Yes**. The command may take several minutes to complete, and will return **True** when the resource group is deleted successfully.



```
Administrator: Windows PowerShell
PS C:\scriptdir> Remove-AzResourceGroup -Name AzDemo
Confirm
Are you sure you want to remove resource group 'AzDemo'
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

15. Run the following command to disconnect the PowerShell session from your Azure account. Then, exit or close the PowerShell terminal window.

```
disconnect-AzAccount
```



```
Administrator: Windows PowerShell
PS C:\scriptdir> disconnect-AzAccount

Id          : user@example.com
Type        : User
Tenants     : {x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9xx}
AccessToken :
Credential  :
TenantMap   : {}
CertificateThumbprint :
ExtendedProperties : {[Subscriptions,x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9x], [Tenants,
(x9xxxx9x-9xxx-9x99-x9xx-9x9999x9x9xx)]}

PS C:\scriptdir>
```

Congratulations! You wrote and ran a local PowerShell script. The PowerShell script used the Azure PowerShell module to create three VMs in Azure from a Linux Ubuntu image.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Demo: Install IIS webserver on a VM with Azure Cloud Shell



<https://www.youtube.com/watch?v=MeOeGp7gS3Y>

Walkthrough-Install IIS webserver on a VM with Azure Cloud Shell

In this walkthrough, you use *Azure Cloud Shell* to automate the installation of the Windows *Internet Information Services* webserver (IIS) on a new virtual machine (VM). Azure Cloud Shell creates a VM and uses the *Custom Script Extension* to install IIS.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Prerequisites

An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**⁸⁴ before you begin.

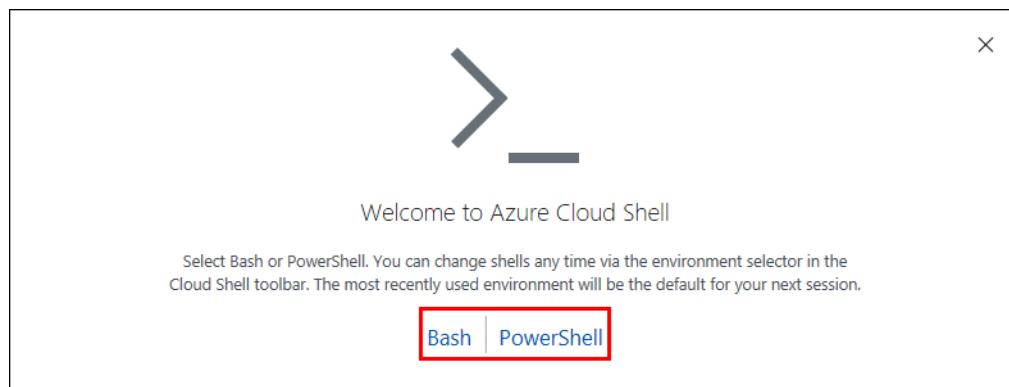
Steps

1. To access **Azure Cloud Shell** go to the location <https://shell.azure.com>⁸⁵ and sign in with your Azure user login credentials.

You can also run Azure Cloud Shell from within Azure Portal by using the Cloud Shell icon.



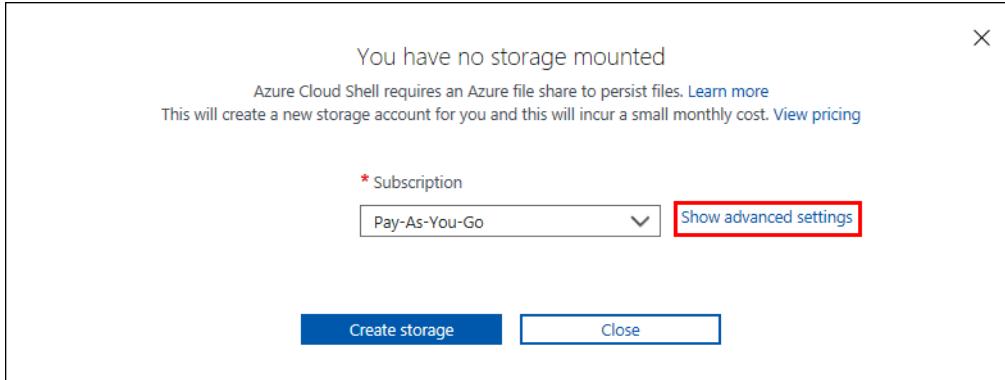
2. If prompted, choose a **Bash** or **PowerShell** environment. This walkthrough uses **PowerShell**.



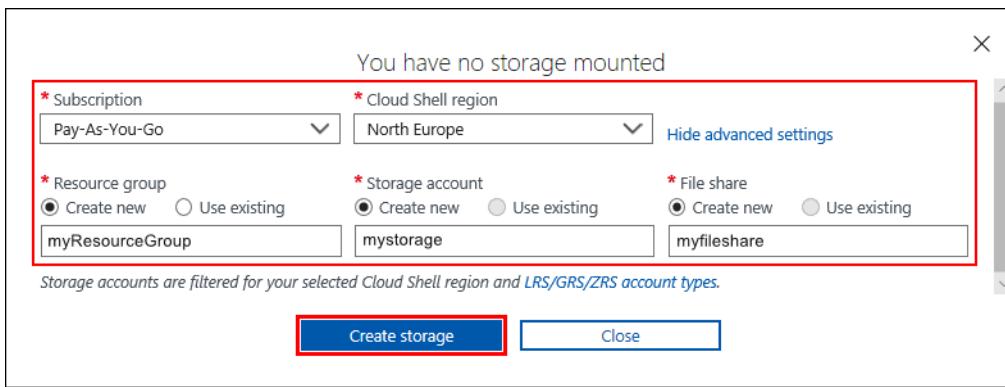
3. First time Azure Cloud Shell users must create and configure Cloud Drive storage, to allow Azure Cloud Shell files to persist. To create and configure storage, select **Show advanced settings**. If you have created and configured storage already, go to Step 5.

⁸⁴ <https://azure.microsoft.com/free/>

⁸⁵ <https://shell.azure.com>



4. Provide the following details to create and configure storage.
 - **Subscription:** Choose your subscription.
 - **Cloud Shell region:** Select the location closest to you. For example, North Europe
 - **Resource group:** Choose **Create new**, then provide a unique name for your new resource group.
 - **Storage account:** Select **Create new**, and provide a unique name for your storage account.
 - **File share:** Choose **Create new**, then enter a unique file share name.
 - Select the **Create storage** button



Wait for the storage setup to complete. When the storage setup is complete, the **Welcome to Azure Cloud Shell** message is shown in the terminal window.

The screenshot shows the Azure Cloud Shell interface. At the top, it says "Azure Cloud Shell" and "PowerShell". On the right, it shows "user@example.com" and "DEFAULT DIRECTORY". The main area displays the following text:

```
Your cloud drive has been created in:  
Subscription Id: x9xxxxx9x-9xxx-9x99-x9x9-9x999x9x9xx  
Resource group: myResourceGroup  
Storage account: mystorage  
File share: myfileshare  
  
Initializing your account for Cloud Shell...  
Requesting a Cloud Shell.Succeeded.  
Connecting terminal...  
  
Welcome to Azure Cloud Shell  
  
Type "az" to use Azure CLI 2.0  
Type "help" to learn about Cloud Shell  
  
MOTD: Switch to PowerShell from Bash: pwsh  
  
VERBOSE: Authenticating to Azure ...  
VERBOSE: Building your Azure drive ...  
Azure:/  
PS Azure:\> []
```

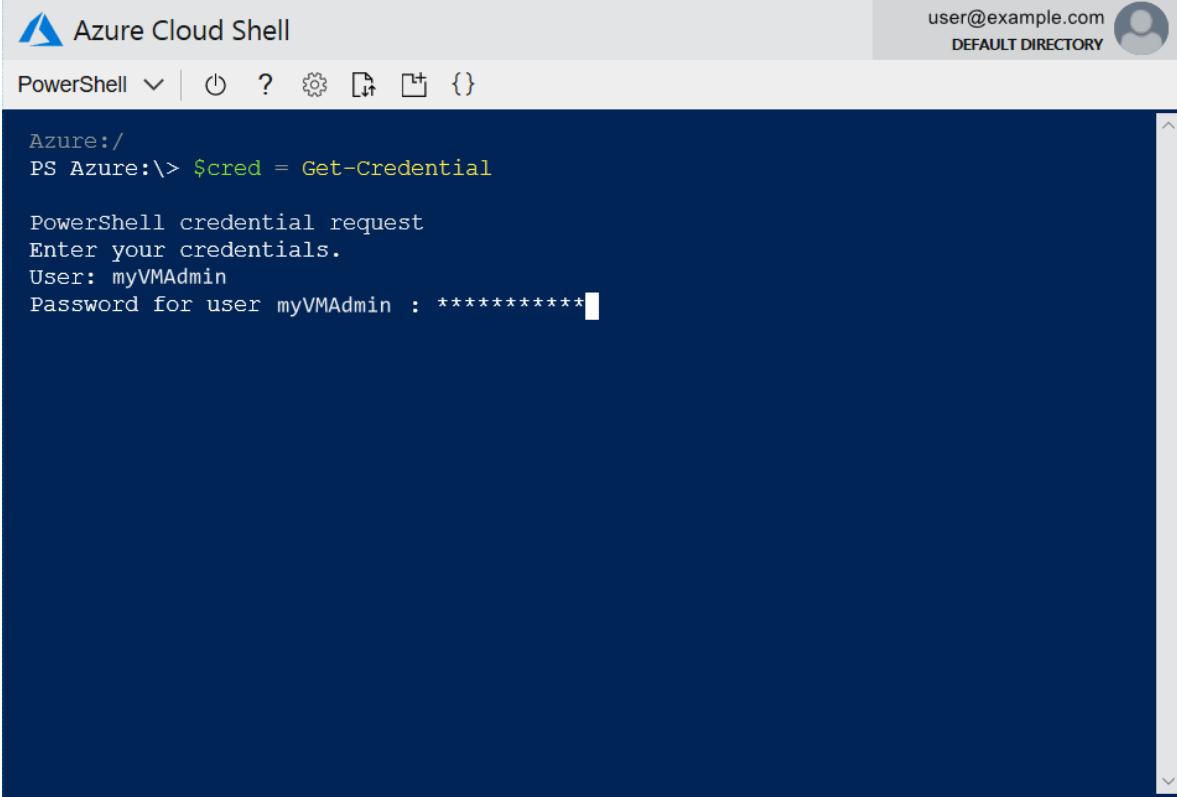
- At the Azure Cloud Shell prompt, set a VM administrator username and password with the Get-Credential command. The credentials are assigned to the variable \$cred. The variable is recalled when the new VM is created in the next Step 6.

```
$cred = Get-Credential
```

When prompted, enter a username and password for the VM administrator. For example,

- User:** myVMAdmin
- Password:** pa\$\$W0rd101

MCT USE ONLY. STUDENT USE PROHIBITED



```
Azure Cloud Shell
PowerShell | ⚡ ? 🛡 { }

Azure:/ PS Azure:\> $cred = Get-Credential

PowerShell credential request
Enter your credentials.
User: myVMAdmin
Password for user myVMAdmin : *****
```

6. Create a VM with the `New-AzVm` command. The following example creates a VM named `myVM` in the `North Europe` location. If they do not exist, the resource group `myResourceGroup` and supporting network resources are created in Azure. To allow web traffic, the following command also opens port 80. Change these to more suitable settings, if you prefer.

Note: Ensure you are signed into your Azure subscription. If you have multiple subscriptions, you can get a list of your subscriptions using the command `Get-AzSubscription`. Specify which subscription to use with the command `Select-AzSubscription -Subscription "Name of your subscription"`. Substitute the actual name of the subscription you want to use for `Name of your subscription`.

```
New-AzVm ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Name "myVM" ` 
    -Location "North Europe" ` 
    -VirtualNetworkName "myVnet" ` 
    -SubnetName "mySubnet" ` 
    -SecurityGroupName "myNetworkSecurityGroup" ` 
    -PublicIpAddressName "myPublicIpAddress" ` 
    -OpenPorts 80 ` 
    -Credential $cred
```

```
Azure:/ PS Azure:\> New-AzVm `>>     -ResourceGroupName "myResourceGroup" `>>     -Name "myVM" `>>     -Location "North Europe" `>>     -VirtualNetworkName "myVnet" `>>     -SubnetName "mySubnet" `>>     -SecurityGroupName "myNetworkSecurityGroup" `>>     -PublicIpAddressName "myPublicIpAddress" `>>     -OpenPorts 80 `>>     -Credential $cred
[Creating Azure resources
 68% - [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Creating virtualMachines/myVM.
```

When the newly created resources and VM are ready, details about the resources and VM will be displayed in the Azure Cloud Shell window. Wait for the resources and VM to be created.

```
ResourceGroupName : myResourceGroup
Id             : /subscriptions/x9xxxx9x-xxxx-9x99-x9x9-9x9999x9x9xx/resourceGroups/myResource/providers/Microsoft.Compute/virtualMachines/myVM
VmId           : x9xxxx9x-xxxx-9x99-x9x9-9x9999x9x9xx
Name           : myVM
Type           : Microsoft.Compute/virtualMachines
Location       : northeurope
Tags           : {}
HardwareProfile: {VmSize}
NetworkProfile: {NetworkInterfaces}
OsProfile      : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations}
ProvisioningState: Succeeded
StorageProfile : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName: myvm-x9xxxx9.North Europe.cloudapp.azure.com

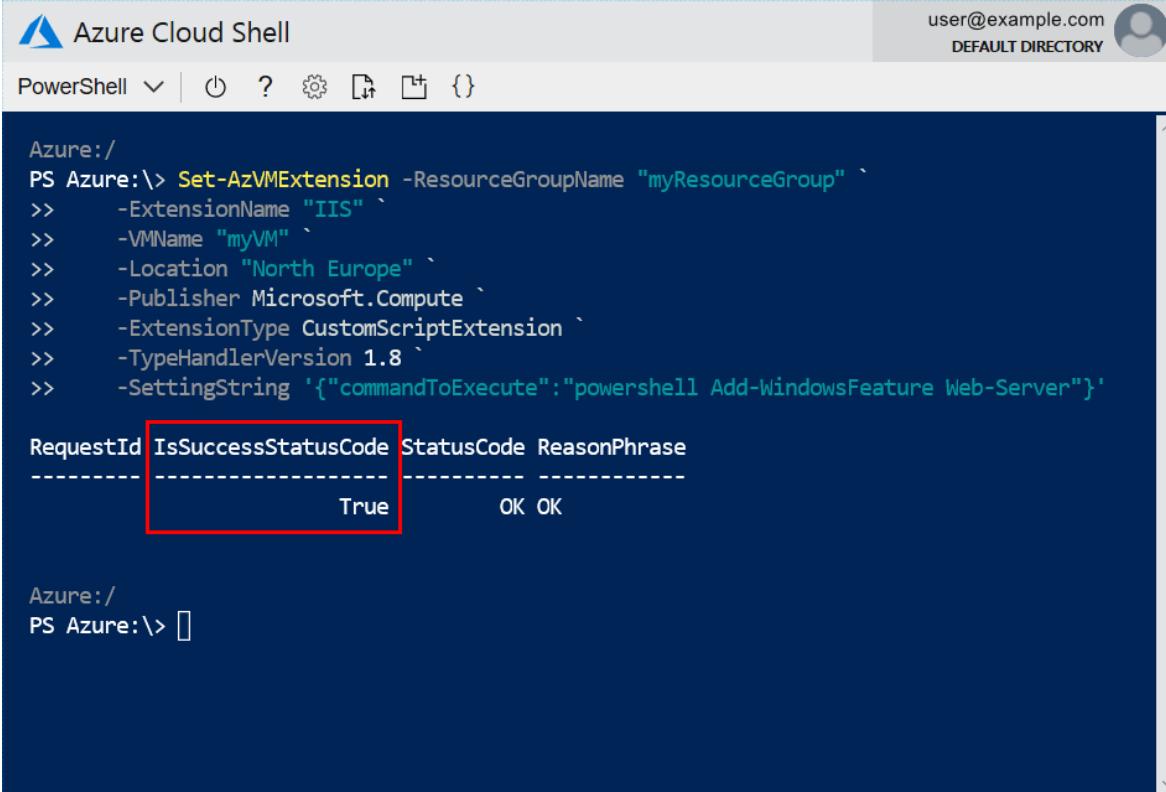
Azure:/ PS Azure:\> []
```

7. Use the `Set-AzVMExtension` command to install the Custom Script Extension. The Custom Script Extension runs the command `powershell Add-WindowsFeature Web-Server` to install IIS to your new VM.

```
Set-AzVMExtension -ResourceGroupName "myResourceGroup" `>>     -ExtensionName "IIS"
```

```
-VMName "myVM" ` 
-Location "North Europe" ` 
-Publisher Microsoft.Compute ` 
-ExtensionType CustomScriptExtension ` 
-TypeHandlerVersion 1.8 ` 
-SettingString '{"commandToExecute":"powershell Add-WindowsFeature Web-Server"}'
```

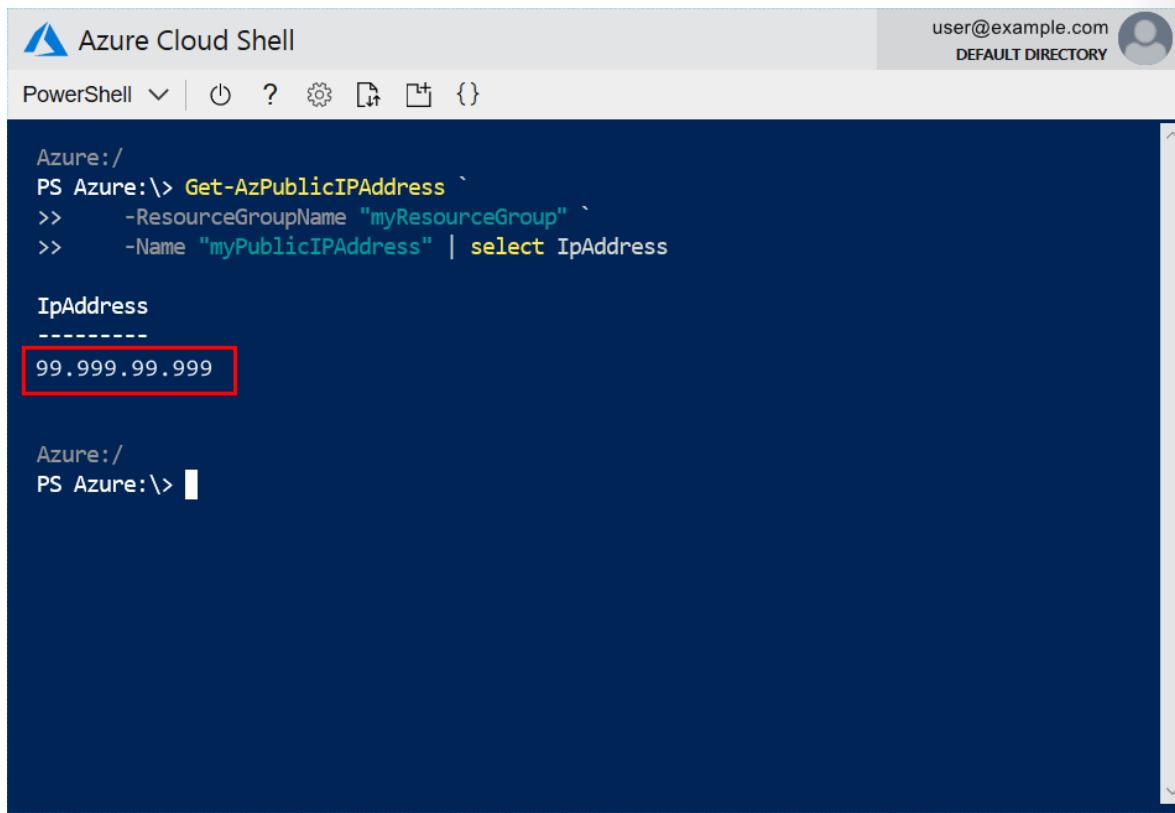
Wait for the Custom Script Extension and IIS to install. When the Custom Script Extension installs IIS successfully, `.IsSuccessStatusCode` will return `True` in the Azure Cloud Shell window.



RequestId	.IsSuccessStatusCode	StatusCode	ReasonPhrase
	True	OK	OK

8. Obtain the public IP address of your load balancer with the `Get-AzPublicIPAddress` command. The following example obtains the IP address for `myPublicIPAddress` created in Step 4.

```
Get-AzPublicIPAddress ` 
-ResourceGroupName "myResourceGroup" ` 
-Name "myPublicIPAddress" | select IPAddress
```



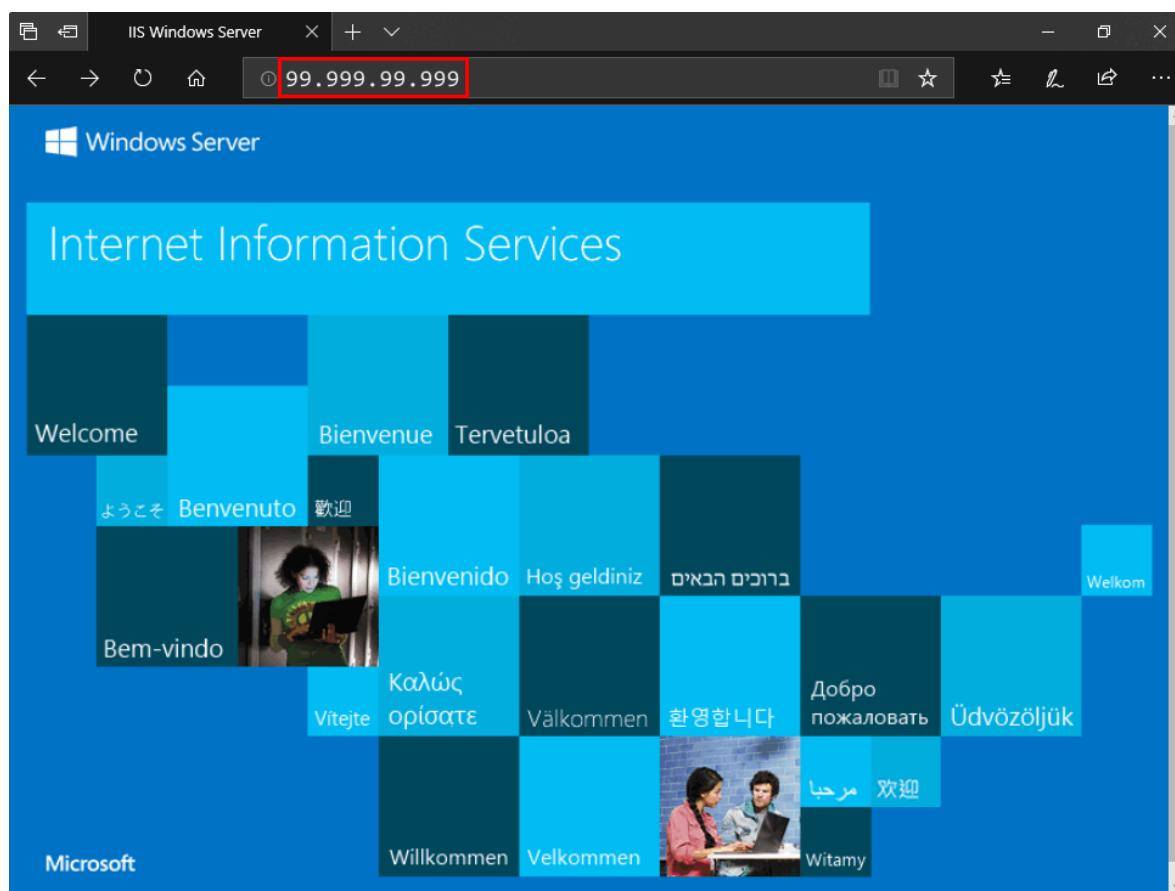
The screenshot shows the Azure Cloud Shell interface. At the top, it says "Azure Cloud Shell" and "PowerShell". On the right, it shows the user "user@example.com" and "DEFAULT DIRECTORY". The main area displays a PowerShell session:

```
Azure:/  
PS Azure:\> Get-AzPublicIPAddress  
->     -ResourceGroupName "myResourceGroup"  
->     -Name "myPublicIPAddress" | select IpAddress  
  
IpAddress  
-----  
99.999.99.999
```

The IP address "99.999.99.999" is highlighted with a red box.

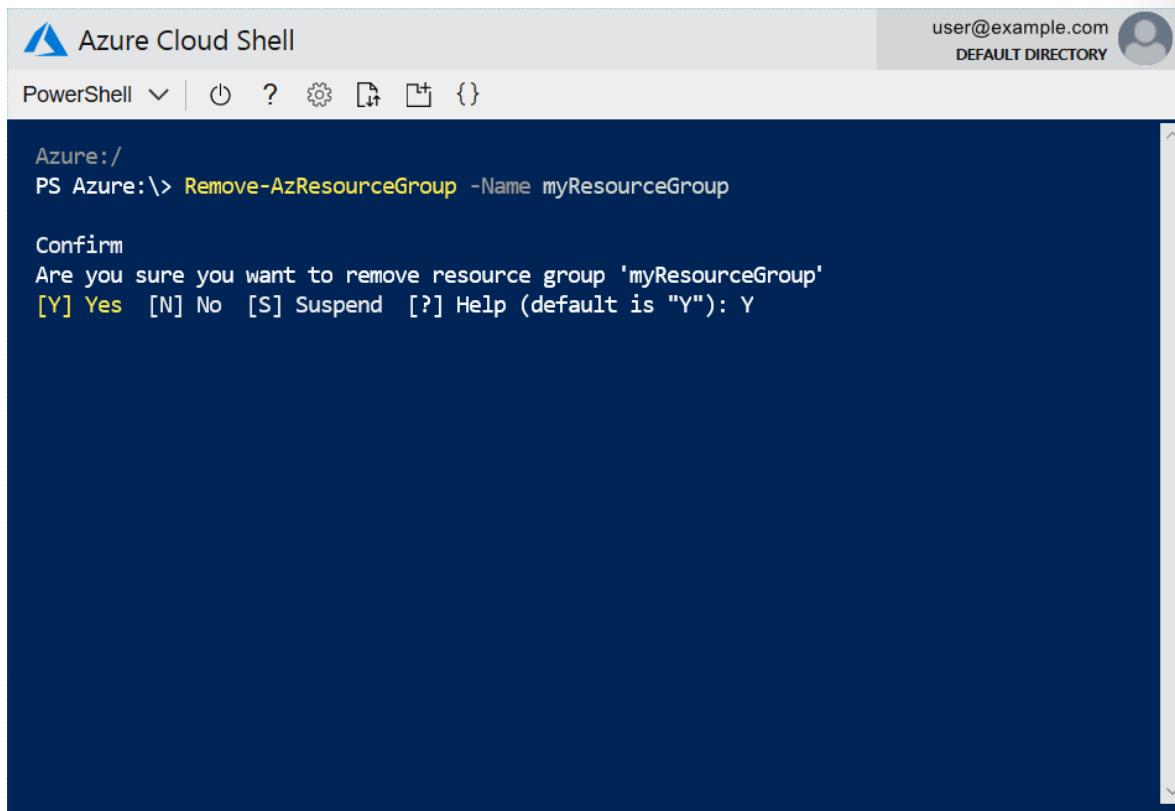
9. Use a web browser to navigate to the public IP address. The Windows server **IIS Welcome** page should be displayed in your browser.

MCT USE ONLY. STUDENT USE PROHIBITED



10. Return to Azure Cloud Shell. Run the following command to remove the resource group `myResourceGroup`, VM, and all related resources. Choose **Yes** to confirm the deletion, when prompted.

```
Remove-AzResourceGroup -Name myResourceGroup
```



```
Azure:/  
PS Azure:\> Remove-AzResourceGroup -Name myResourceGroup  
  
Confirm  
Are you sure you want to remove resource group 'myResourceGroup'  
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

Congratulations! You used Azure Cloud Shell to automate the installation of IIS on a new VM.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Video: Azure Advisor



<https://www.youtube.com/watch?v=6CmQOfc0Ueo>

Azure Advisor

Azure Advisor is a free service built into Azure that provides recommendations on high availability, security, performance, and cost. Advisor analyzes your deployed services and looks for ways to improve your environment across those four areas.

MCT USE ONLY. STUDENT USE PROHIBITED



With *Azure Advisor*, you can:

- Get proactive, actionable, and personalized best practices recommendations.
- Improve the performance, security, and high availability of your resources as you identify opportunities to reduce your overall Azure costs.
- Get recommendations with proposed actions inline.

You can access Azure Advisor through the Azure portal. After you sign in to the portal, either select **Advisor** from the navigation menu, or search for it in the *All services* menu.

You can download recommendations from Azure Advisor in PDF or CSV format, which you can then share.

Note: You can see more details about Azure Advisor on the [Azure Advisor⁸⁶](#) page.

⁸⁶ <https://azure.microsoft.com/en-us/services/advisor/>

Demo: Save a recommendations report with Azure Advisor



<https://www.youtube.com/watch?v=wWSmUSwtcCA>

Walkthrough-Save a recommendations report with Azure Advisor

In this walkthrough, you create and save a personalized recommendations report with Azure Advisor. You deploy a Virtual Machine (VM) and network resources, which Azure Advisor analyzes, to get recommendations and generate the report.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Prerequisites

An active Azure subscription is required. If you do not have an Azure subscription, create a **free Azure account**⁸⁷ before you begin.

Steps

1. To create a new VM in Azure directly from a template click on this **Create a New VM**⁸⁸ link and when prompted, sign into Azure Portal.
2. Enter the following details for the new VM.
 - **Subscription:** Select your Azure subscription.
 - **Resource group:** Choose **Create new**, and enter a name for the new resource group. Select the **ok** button.
 - **Location:** Choose the Azure location that is closest to you. For example, Australia_SouthEast.
 - **Admin Username:** Enter a name for the VM administrator.
 - **Authentication Type:** Select **password**.
 - **Admin Password Or Key:** Enter a password for the VM administrator.
 - **DNS Label Prefix:** Enter a DNS label prefix. For example, `mydnsprefix`
 - **Ubuntu OS Version:** Leave this at the default setting. For example, `16.04.0 LTS`
 - **Location:** Leave this at the default setting `[resourceGroup().location]`
 - Check the box to agree to the terms and conditions.

⁸⁷ <https://azure.microsoft.com/free/>

⁸⁸ <https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2Fazur...templates%2Fmaster%2F101-vm-simple-linux%2Fazuredeploy.json>

- Select the **Purchase** button.

Home > Deploy a simple Ubuntu Linux VM

Deploy a simple Ubuntu Linux VM

Azure quickstart template

TEMPLATE

101-vm-simple-linux
5 resources

Edit template Edit param... Learn more

BASICS

* Subscription: Pay-As-You-Go

* Resource group: (New) myResourceGroup
Create new

* Location: Australia Southeast

SETTINGS

* Admin Username: myAdministratorName

Authentication Type: password

* Admin Password Or Key: [REDACTED]

* Dns Label Prefix: mydnslabel

Ubuntu OS Version: 16.04.0-LTS

Location: [resourceGroup().location]

TERMS AND CONDITIONS

Template information | Azure Marketplace Terms | Azure Marketplace

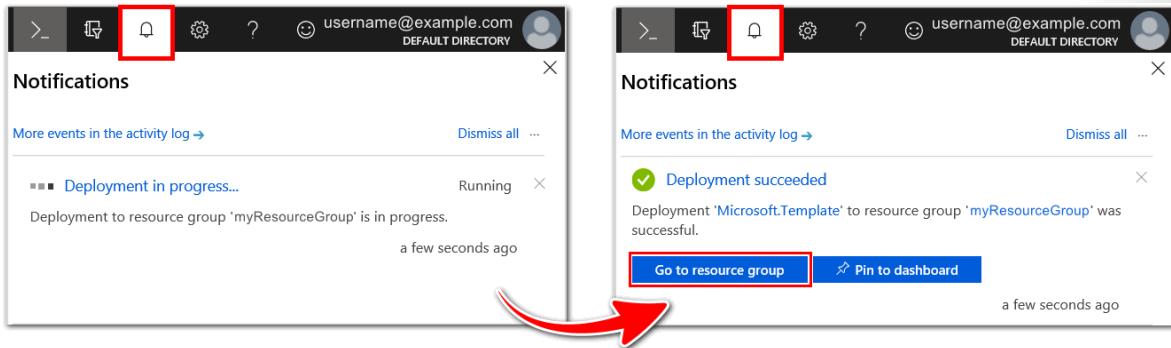
By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

I agree to the terms and conditions stated above

Purchase

Note: When the deployment starts, a notification appears in Azure Portal indicating the deployment is in progress. Another notification is displayed when the deployment has completed successfully.

- When the deployment has completed, choose **Go to resource group** from the notification area to open the Azure resource group **Overview** blade. You can also select **Resource groups** from the main Azure menu, then choose your resource group from the list.



- Verify that the new VM and associated network resources are present in the Azure resource group **Overview** pane.

NAME	TYPE	LOCATION
myPublicIP	Public IP address	Australia Southeast
MyUbuntuVM	Virtual machine	Australia Southeast
MyUbuntuVM_disk2_d883cebef2724903935e0f3dfd44bab...	Disk	Australia Southeast
MyUbuntuVM_OsDisk_1_224979907d2342ceaa8b1c633ff2feb7...	Disk	Australia Southeast
myVMNic	Network interface	Australia Southeast
MyVNET	Virtual network	Australia Southeast
x65s65mz3monwsalinuxvm	Storage account	Australia Southeast

- Open **Advisor** from the main Azure menu. The **Recommendations** tile under **Overview**, and panels, allow you to filter the recommendations identified by Azure Advisor. For example, for an overview of Security Center recommendations, select the **Security** panel.

The screenshot shows the Microsoft Azure Advisor interface. On the left, a navigation bar lists various services, with 'Advisor' highlighted by a red arrow. The main area is titled 'Advisor' and shows 'Subscriptions: Pay-As-You-Go'. It includes sections for 'High Availability', 'Security', 'Performance', and 'Cost'. A red box highlights the 'Security' section, which displays '3 Recommendations' (3 High impact, 0 Medium impact, 0 Low impact) and '4 Impacted resources'. The 'Performance' section indicates following all performance recommendations, and the 'Cost' section indicates following all cost recommendations. A 'Tips & tricks' section at the bottom right suggests customizing Advisor.

Note: Azure Advisor recommendations are unique to your Azure configuration and usage history. More or less recommendations may be available, in accordance with your Azure resource configurations and usage telemetry.

6. Choose **Follow Security Center Recommendations** to see a list of security center recommendations applicable to your subscription.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the 'Advisor - Security' dashboard. On the left, a sidebar lists categories: Overview, Recommendations, High Availability, **Security**, Performance, Cost, All recommendations, Settings, and Configuration. The 'Security' category is selected. The main area displays 'Subscriptions: Pay-As-You-Go' with a search bar and download options. A purple banner at the top right says 'Your security experience may be limited. Click here to learn more'. Below it, a summary shows 'Total recommendations: 3' with a green shield icon. A horizontal bar shows 'Recommendations by impact': 3 High impact (red), 0 Medium impact (orange), and 0 Low impact (green). A red arrow points to the 'High' impact section, which contains a button labeled 'Follow Security Center recommendations'. Other sections include 'Impacted resources: 4' with a blue cube icon, 'Security alerts' (two icons), and a 'Standard plan feature' link. At the bottom, there are 'RECOMMENDATIONS' and 'UPDATE...' buttons, and a status bar showing '3 Recommendations 26/03/20'.

- Select a recommendation from the list for more information. The following example shows how to access information about applying disk encryption to VMs. Explore the other recommendations to learn about Azure Advisor.

The screenshot shows the 'Recommendations' page under the 'Security Center' tab. It displays a summary: 'TOTAL: 4' (3 High Severity, 1 Medium Severity, 0 Low Severity) and '1 Unhealthy resources'. Below this, a chart shows resource health monitoring: 'Compute & apps' (1 resource, red bar), 'Data & storage' (1 resource, green bar), 'Networking' (0 resources, grey bar), and 'Identity & access' (0 resources, grey bar). To the right, a section titled 'Review and improve your secure score' includes a trophy icon and a link 'Learn more >'. The main table lists recommendations with columns: RECOMMENDATION, SECURE SCORE..., and FAILED RESOURCES. A red arrow points to the last recommendation in the list, 'Apply disk encryption on your virtual machines', which is highlighted with a red border. The table data is as follows:

RECOMMENDATION	SECURE SCORE...	FAILED RESOURCES
Install monitoring agent on your virtual machines	+50	1 of 1 virtual machines
Enable Network Security Groups on virtual machines	+30	1 of 1 virtual machines
Install a vulnerability assessment solution on your virtual machines	+30	1 of 1 virtual machines
Apply disk encryption on your virtual machines	+10	1 of 1 virtual machines

Dashboard > Advisor - Security > Recommendations > Apply disk encryption on your virtual machines

Apply disk encryption on your virtual machines

Description

Encrypt your virtual machine disks using Azure Disk Encryption both for Windows and Linux virtual machines. Azure Disk Encryption (ADE) leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide OS and data disk encryption to help protect and safeguard your data and help meet your organizational security and compliance commitments in customer Azure key vault. When your compliance and security requirement requires you to encrypt the data end to end using your encryption keys, including encryption of the ephemeral (locally attached temporary) disk, use Azure disk encryption. Alternatively, by default, Managed Disks are encrypted at rest by default using Azure Storage Service Encryption where the encryption keys are Microsoft managed keys in Azure. If this meets your compliance and security requirements, you can leverage the default Managed disk encryption to meet your requirements.

General Information

Recommendation score	i	0/10
Recommendation impact	+10	
User impact	Low	
Implementation cost	Low	

Threats

- Data exfiltration
- Data spillage
- Account breach

Remediation steps

To enable disk encryption on your virtual machines, follow [Encryption instructions](#).

Unhealthy resources	Healthy resources	LEARN MORE						
1	0	Learn more about recommendations ↗						
Unhealthy resources (1) Healthy resources (0) Unscanned resources (0)								
<input type="text" value="Search virtual machines"/>								
<table border="0"> <thead> <tr> <th style="text-align: left;">NAME</th> <th style="text-align: right;">↑↓</th> <th style="text-align: right;">SUBSCRIPTION</th> </tr> </thead> <tbody> <tr> <td> MyUbuntuVM</td> <td></td> <td style="text-align: right;">Pay-As-You-Go</td> </tr> </tbody> </table>			NAME	↑↓	SUBSCRIPTION	MyUbuntuVM		Pay-As-You-Go
NAME	↑↓	SUBSCRIPTION						
MyUbuntuVM		Pay-As-You-Go						

8. To download an Azure Advisor recommendations report, return to the [Azure Advisor Overview](#). Select **Download recommendations** as PDF or CSV, and save the report file.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Microsoft Azure Advisor dashboard. On the left is a navigation menu with options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (which includes 'All resources', 'Subscriptions', 'Automation Accounts', etc.), and 'Advisor'. The main content area is titled 'Advisor' and shows 'Subscriptions: Pay-As-You-Go'. It has sections for 'High Availability', 'Security', 'Performance', and 'Cost'. Each section indicates that all recommendations are followed and provides a link to see the full list. At the bottom, there are two buttons: 'Download recommendations as PDF' (with a red box around it) and 'Download recommendations as CSV'.

Congratulations! You created and saved a personalized recommendations report with Azure Advisor.

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs. Remove unused resources by deleting the Resource Group that the unused resources belong to.

Module 2 Review Questions

Core Azure Services Review Questions

About review questions

End-of-module review questions are for practice only and are not included in your grade for the course. The final assessment at the end of the course is graded.

Review Question 1

What terms from the below list are valid core architectural components of Microsoft Azure?

(choose four)

- Region
- Availability zone
- Server group
- Resource group
- Availability set

Review Question 2

Every resource created in Azure must exist in one and only one what?

- Availability set
- Availability zone
- Resource group
- Azure Resource Manager

Review Question 3

As a best practice, all resources that are part of an application and share the same life cycle exist in the same what?

- Geography
- Resource group
- Region
- Availability set

Review Question 4

You want to deploy an application in a container, and may need to run it at scale on some occasions. You want to deploy the containers directly to Azure without having to first deploy virtual machines. Which services are available for you to use to deploy containers directly to Azure?

(choose two)

- Azure Kubernetes Service (AKS)
- Azure Functions
- VMs
- Azure Container Instances

Review Question 5

You need to deploy a legacy application in Azure that has some customizations that are needed to ensure it runs successfully. The application will run on a Windows VM. Which Azure service from the below list would you recommend to run the virtual machine in?

- Azure App Service
- Azure Event Grid
- Azure Virtual Machines
- Azure Container Instances

Review Question 6

True or false: Resource Manager templates are JSON files.

- True
- False

Review Question 7

Which of the following services are part of Core Networking services in Azure?

- Azure App Services
- Azure Blob Storage
- Azure Cosmos DB
- Azure VPN Gateway

Review Question 8

Which of the following services are part of Core IoT services in Azure?

- IoT Central
- Application Gateway
- Azure DevOps
- Azure PowerShell

Review Question 9

Which of the following services are part of the Artificial Intelligence service in Azure?

- HDInsight
- Azure Machine Learning service
- Azure DevTest Labs
- Azure Advisor

Module 2 Summary

Module 2 Summary

In this module you've learned about core Microsoft Azure architectural components, core Azure services and solutions, and various management tools that are available to manage and configure Azure.

Core Azure architectural components

In this lesson we learned about how Azure datacenters and services are located and organized in regions and geographies. We also learned how availability is achieved using availability zones and availability sets. We gained an understanding of how to automate deployments and configuration of resources and services using declarative JSON templates that utilize the Azure Resource Manager layer to create and configure resources. And finally, we learned how to use resource groups for managing resources in Azure.

Core Azure services and products

In this lesson we learned about compute services, and the use of virtual machines and containers. We gained an understanding of some of the services that make up the compute service such as Azure VMs, VM scale sets, app services and functions, Azure Container Instances, and Azure Kubernetes Service. We also learned about networking services such as Virtual Network, Azure Load Balancer, VPN Gateway, Application Gateway, and Azure Content Delivery Network.

Azure solutions

In this lesson we learned about solutions such as IoT, and services that form part of the service offering such as Azure IoT Hub and Microsoft IoT Central. We discussed big data analytics services such as Azure SQL Data Warehouse, HDInsight, and Azure Data Lake Analytics. We also learned about AI and how it utilizes machine learning services such as Azure Machine Learning and Azure Machine Learning Studio. We also learned about serverless computing services such as Azure Functions, Azure Logic Apps, and Azure Event Grid. Finally we learned about DevOps services such as Azure DevOps and Azure DevTest Labs.

Azure management tools

In this lesson we learned about the management tools available for managing and configuring Azure, such as Azure Portal, Azure PowerShell, Azure CLI, and Azure Cloud Shell. It also includes Azure Advisor, which provides recommendations on high availability, security, performance, and cost.

Answers

Review Question 1

What terms from the below list are valid core architectural components of Microsoft Azure?

(choose four)

- Region
- Availability zone
- Server group
- Resource group
- Availability set

Explanation

Region, availability zone, resource group, and availability set are the correct answers, as they are all core architectural components of Azure.

Server Groups are not a core architectural component of Microsoft Azure.

Review Question 2

Every resource created in Azure must exist in one and only one what?

- Availability set
- Availability zone
- Resource group
- Azure Resource Manager

Explanation

Resource group is the correct answer. Each resource must exist in one, and only one, resource group. All other answers are incorrect, as a resource does not need to exist in an availability set or an availability zone, and Azure Resource Manager is a management layer that creates resources, but a resource cannot exist in this layer.

Review Question 3

As a best practice, all resources that are part of an application and share the same life cycle exist in the same what?

- Geography
- Resource group
- Region
- Availability set

Explanation

Resource group is the correct answer. Resources that are part of an application and share its life cycle should be placed in the same resource group for ease of management.

It is not a recommended best practice for resources to be placed in the same geography, region, or availability set.

Review Question 4

You want to deploy an application in a container, and may need to run it at scale on some occasions. You want to deploy the containers directly to Azure without having to first deploy virtual machines. Which services are available for you to use to deploy containers directly to Azure?

(choose two)

- Azure Kubernetes Service (AKS)
- Azure Functions
- VMs
- Azure Container Instances

Explanation

AKS and Azure Container Instances are the correct answers. Azure Container Instances allows you to deploy containers directly to Azure; and Azure Kubernetes Service is a container orchestrator, which allows you run containers at scale without having to manage underlying VMs.

Azure Functions is not the correct answer as Functions is involved in serverless computing and does not run containers directly.

VMs is not the correct answer either, because although you could run containers in an IaaS virtual machine, you would have to manage the virtual machine to do so.

Review Question 5

You need to deploy a legacy application in Azure that has some customizations that are needed to ensure it runs successfully. The application will run on a Windows VM. Which Azure service from the below list would you recommend to run the virtual machine in?

- Azure App Service
- Azure Event Grid
- Azure Virtual Machines
- Azure Container Instances

Explanation

Azure Virtual Machines is the correct answer, because it is an IaaS service and as such you are responsible for configuring and managing the virtual machine on which the application will run. This enables you to customize it as needed in this case.

Azure App Service is a PaaS service, and as such you will not be able to customize the underlying virtual machine in which the application runs.

Azure Event Grid is a messaging service in Azure that triggers other events. It allows you to connect serverless logic to events coming from multiple Azure services, and it connects to events from external sources, all as part of a serverless computing model. However, it does not run virtual machines.

Azure Container Instances will not run virtual machines; it will only run containers, and is a PaaS service.

Review Question 6

True or false: Resource Manager templates are JSON files.

- True
- False

Explanation

Resource Manager templates are JSON files that define the resources you need to deploy for your solution. You can then use the template to easily re-create multiple versions of your infrastructure, such as staging and production.

Review Question 7

Which of the following services are part of Core Networking services in Azure?

- Azure App Services
- Azure Blob Storage
- Azure Cosmos DB
- Azure VPN Gateway

Explanation

Azure VPN Gateway is the correct answer, because it allows you to connect securely from your on-premises environment to Azure. It is also referred to as a Virtual Network Gateway.

Azure App Services is a PaaS service for running different types of apps, such as web apps, mobile apps, and others.

Azure Blob Storage is part of storage services, and Azure Cosmos DB is part of data services.

Review Question 8

Which of the following services are part of Core IoT services in Azure?

- IoT Central
- Application Gateway
- Azure DevOps
- Azure PowerShell

Explanation

IoT Central is the correct answer, because it is an SaaS for IoT that allows you to connect, monitor, and manage your IoT assets at scale.

Application Gateway is a gateway service to allow your application connect internally or externally and is part of the Networking suite of services.

Azure DevOps is part of the DevOps suite of services and allows you build continuous integration and delivery pipelines.

Azure PowerShell is a scripting language that allows you manage and configure Azure.

Review Question 9

Which of the following services are part of the Artificial Intelligence service in Azure?

- HDInsight
- Azure Machine Learning service
- Azure DevTest Labs
- Azure Advisor

Explanation

Azure Machine Learning service is the correct answer. Machine Learning service provides a cloud-based environment that you can use to develop, train, test, deploy, manage, and track machine learning models. HDInsight is a fully managed, open-source analytics service for enterprises, and is part of the big data and analytics category of services.

Azure DevTest Labs is a service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. It is part of the DevOps suite of services.

Azure Advisor is a free service built into Azure that provides recommendations on high availability, security, performance, and cost. It is part of the management suite of tools and services.

Module 3 Security, Privacy, Compliance and Trust

Learning Objectives

Learning Objectives

After completing this module, you will be able to:

- Understand and describe how to secure network connectivity in Microsoft Azure.
- Understand and describe core Azure identity services.
- Understand and describe security tools and features.
- Understand and describe Azure governance methodologies.
- Understand and describe monitoring and reporting in Azure.
- Understand and describe privacy, compliance, and data protection standards in Azure.

Securing network connectivity in Azure

Video: Securing network connectivity



<https://www.youtube.com/watch?v=Gw8kj0UxTnk>

Azure Firewall

A *Firewall* is a service that grants server access based on the originating IP address of each request. You create firewall rules that specify ranges of IP addresses. Only clients from these granted IP addresses will be allowed to access the server. Firewall rules, generally speaking, also include specific network protocol and port information.



Azure Firewall is a managed, cloud-based, network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can create, enforce, and log, application and network connectivity policies across subscriptions, and virtual networks, centrally. Azure Firewall uses a static public IP address for your virtual network resources, which allows outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Azure Firewall provides many features, including:

- Built-in high availability.
- Unrestricted cloud scalability.
- Inbound and outbound filtering rules.
- Azure Monitor logging.

Common Usage Scenarios

You typically deploy Azure Firewall on a central virtual network to control general network access. With Azure Firewall you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.

Azure Application Gateway also provides a firewall, called the *Web Application Firewall* (WAF). However, WAF is different to Azure Firewall. WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities. While in contrast, Azure Firewall provides outbound, network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S. In addition, Azure Firewall provides inbound protection for non-HTTP/S protocols. Examples of non-HTTP/S protocols include: Remote Desktop Protocol (RDP), Secure Shell (SSH), and File Transfer Protocol (FTP). Azure Firewall's extended functionality make it suitable for different uses.

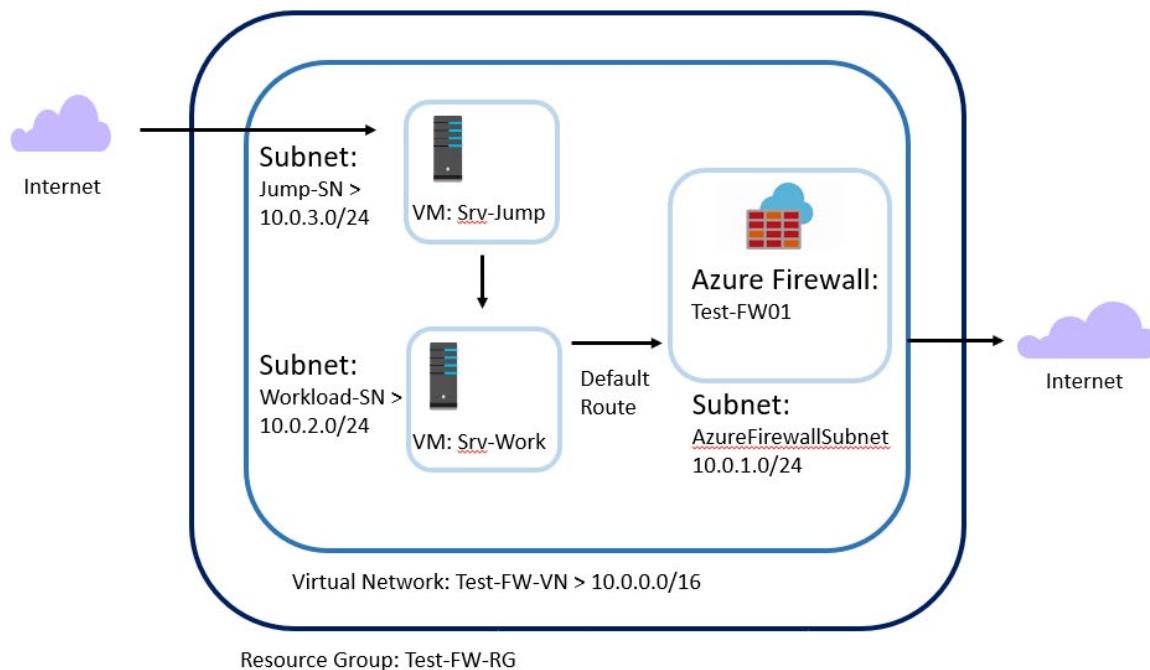
Note: For more details, see the [Azure Firewall¹](#) page.

Walkthrough-Implement an Azure Firewall using Azure Portal

In this walkthrough task we will create two virtual machines, one which will simulate running a workload, and which we will isolate, so it is running in a separated, secure network, and another which will act as a jump server, which we will use to connect to our workload server. We will also create an Azure Firewall through which all traffic from our workload server will be routed. We will create rules in Azure Firewall to *allow* access to a particular website to verify Firewall functionality. From a network architecture perspective, we will create a single Virtual Network (VNET) which will contain three subnets. The three subnets will be

- **AzureFirewallSubnet:** Contains Azure Firewall and all workload server traffic will be routed through Azure Firewall.
- **Workload-SN:** Contains the Workload server i.e. a server where a production application would run. We create a default route so that this subnet's network traffic is configured to go through the firewall. The workload server will not have a publicly accessible connection available to it and will only be accessible via a *Jump server*(*Jump box*). We will configure Azure Firewall to allow the workload server to access DNS servers over port 53 to allow it access web sites on the internet.
- **Jump-SN:** Contains a *Jump server* which has a public IP address that you can connect to using Remote Desktop. From there, you can then connect to (using another Remote Desktop) the workload server.

¹ <https://azure.microsoft.com/en-us/services/azure-firewall/>



Note: For production deployments, a **hub and spoke model**² is recommended, where the firewall is in its own VNET, and workload servers are in peered VNETs in the same region with one or more subnets.

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 today³](#) webpage.

Steps

Create Resource group

1. Sign in to the Azure portal at [⁴](https://portal.azure.com)
2. On the Azure portal home page, click **Resource groups** > **Add** and use the following details and click **Review and Create** and then **Create**.
 - **Subscription:** < select your own subscription >
 - **Resource group:** Test-FW-RG
 - **Region:** < select a Datacenter location nearest to you. Note: All subsequent resources that you create must be in the same location. >

² <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>

³ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

⁴ <https://portal.azure.com>

MCT USE ONLY. STUDENT USE PROHIBITED

Create a resource group

Basics Tags Review + Create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

PROJECT DETAILS

* Subscription

* Resource group ✓

RESOURCE DETAILS

* Region

Review + Create Next : Tags

Create a VNET

1. From the Azure portal home page, click **All services > Networking > Virtual networks**.
2. Click **Add** and use the following details, leaving any other values as their default and click **Create** when finished
 - **Name:** Test-FW-VN
 - **Address space:** 10.0.0.0/16
 - **Subscription :** < select your subscription >
 - **Resource group:** < select resource group created earlier i.e. *Test-FW-RG* >
 - **Location:** < select the same location that you used previously >
 - **Subnet>**
 - **Name:** AzureFirewallSubnet (The firewall will be in this subnet, and the subnet name must be *AzureFirewallSubnet*).
 - **Address range:** 10.0.1.0/24

The screenshot shows the 'Create virtual network' blade in the Azure portal. Key fields highlighted with red boxes are:

- Name:** Test-FW-VN
- Address space:** 10.0.0.0/16 (10.0.0.0 - 10.0.255.255 (65536 addresses))
- Resource group:** Test-FW-RG
- Address range for Subnet:** 10.0.1.0/24 (0 addresses)

Other visible settings include:

- DDoS protection:** Basic (radio button selected)
- Service endpoints:** Disabled
- Firewall:** Disabled

Buttons at the bottom include 'Create' and 'Automation options'.

Create additional subnets

Next we will create some additional subnets, into which we will subsequently place two virtual machines.

1. On the Azure portal home page, click **Resource groups** > **Test-FW-RG**.
2. Click the **Test-FW-VN** virtual network.
3. Click **Subnets** > **+ Subnet** and use the following details, leaving the remaining items at their default values and click **OK** when completed
 - **Name:** Workload-SN
 - **Address range:** 10.0.2.0/24

MCT USE ONLY. STUDENT USE PROHIBITED

Add subnet

Test-FW-VN

* Name
Workload-SN

* Address range (CIDR block) i
10.0.2.0/24
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Network security group
None

Route table
None

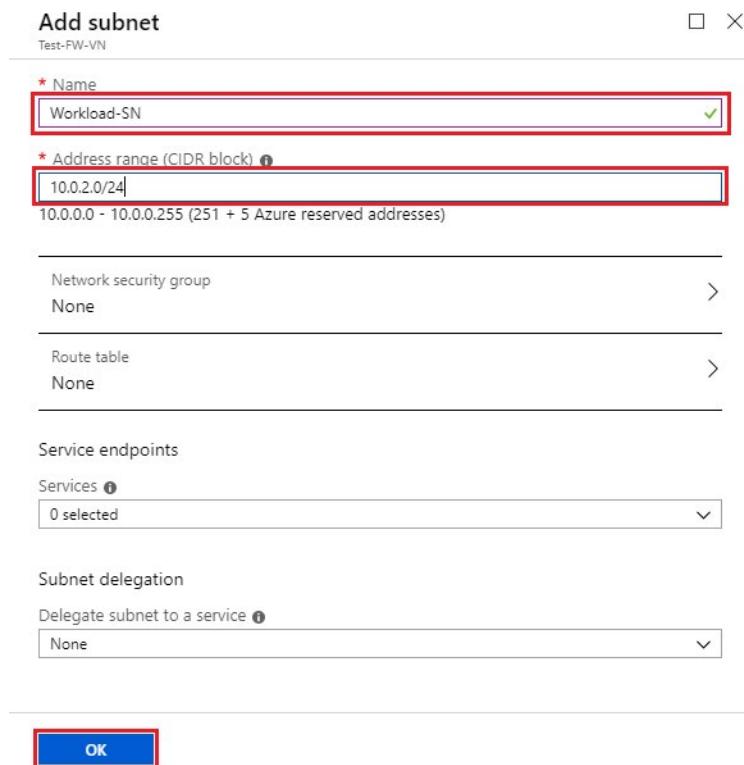
Service endpoints

Services i
0 selected

Subnet delegation

Delegate subnet to a service i
None

OK



4. Create another subnet by repeating steps 1-3 above, using the values
 - **Name:** Jump-SN
 - **Address range:** 10.0.3.0/24

Add subnet

Test-FW-VN

* Name
Jump-SN ✓

* Address range (CIDR block) ⓘ
10.0.3.0/24
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Network security group >
None

Route table >
None

Service endpoints

Services ⓘ
0 selected

Subnet delegation

Delegate subnet to a service ⓘ
None

OK

Create virtual machines to act as a Jump box and workload server

Now we will create two virtual machines and place them in the two additional subnets created in the previous section, one for the *Jump-SN* subnet, and one for the *Workload-SN* subnet.

1. On the Azure portal, click **Create a resource**.
2. Select **Windows Server 2016 Datacenter** in the Featured list.

The screenshot shows the Microsoft Azure portal's 'New' blade. On the left is a sidebar with a 'Create a resource' button highlighted by a red box. The main area shows a search bar and a 'Compute' category highlighted by a red box. Below it are other categories: Networking, Storage, Web, Mobile, Containers, Databases, Analytics, and AI + Machine Learning. To the right, there's a section for the 'Azure Marketplace' with a 'Featured' tab. One item, 'Windows Server 2016 Datacenter Quickstart tutorial', is highlighted with a red box.

- Enter these values for the virtual machine, accepting the default values for items not listed below.
When finished click **Review + Create**, then click **Create**

- Basics**

- Subscription:** < select your subscription >
- Resource group:** Test-FW-RG < the resource group you created earlier >
- Virtual machine name:** Srv-Jump
- Region:** < The region you selected earlier >
- Size:** Select **Change size** then choose **DS2_v2** (The default value is **DS1_v2**, however this is running a bit slow for our purposes, so we will increase the Vm size)
- Username:** azureuser
- Password:** Password0134!
- Public inbound ports:** RDP (3389)

- Networking**

- Virtual Network:** Test-FW-VN
- Subnet:** Jump-SN
- Public IP:** click Create new then type **Srv-Jump-PIP** for the public IP address name and click **OK**.

- Management**

- Boot diagnostics: Off

Create a virtual machine

Validation passed

Basics Disks Networking Management Guest config Tags Review + create

PRODUCT DETAILS

Standard DS1 v2 by Microsoft **0.0573 EUR/hr** Subscription credits apply (1) [Terms of use](#) | [Privacy policy](#) [Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription	Visual Studio Ultimate with MSDN
Resource group	Test-FW-RG
Virtual machine name	Srv-Jump
Region	West Europe
Availability options	No infrastructure redundancy required
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No

DISKS

OS disk type	Premium SSD
Use managed disks	Yes

NETWORKING

Virtual network	Test-FW-VN
Subnet	Jump-SN (10.0.3.0/24)
Public IP	(new) Srv-Jump-PIP
Accelerated networking	Off

4. While the virtual machine is being created, repeat steps 1-3 above to create another virtual machine with the following settings:

- **Basics**

- **Subscription:** < select your subscription >
- **Resource group:** Test-FW-RG < the resource group you created earlier >
- **Virtual machine name:** Srv-Work
- **Region:** < The region you selected earlier >
- **Size:** Select **Change size** then choose **DS2_v2** (The default value is *DS1_v2*, however this is running a bit slow for our purposes, so we will increase the Vm size)
- **Username:** azureuser
- **Password:** Password0134!
- **Public inbound ports:** None

- **Networking**

- **Virtual Network:** Test-FW-VN

- **Subnet:** Workload-SN
- **Public IP:** None
- **Management**
- **Boot diagnostics:** Off

Create a virtual machine

Validation passed

Basics **Disks** **Networking** **Management** **Guest config** **Tags** **Review + create**

PRODUCT DETAILS

Standard DS1 v2
by Microsoft

Subscription credits apply ⓘ
0.0573 EUR/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription	Visual Studio Ultimate with MSDN
Resource group	Test-FW-RG
Virtual machine name	Srv-Work
Region	West Europe
Availability options	No infrastructure redundancy required
Username	azureuser
Public inbound ports	None
Already have a Windows license?	No

DISKS

OS disk type	Premium SSD
Use managed disks	Yes

NETWORKING

Virtual network	Test-FW-VN
Subnet	Workload-SN (10.0.2.0/24)
Public IP	None
Accelerated networking	Off

Deploy the Firewall into the VNET

This will take approx. 5 mins to configure and deploy

1. From the portal home page, click **Create a resource** and in the **New** pane type **Firewall**, then click **Create**

The screenshot shows the Azure Firewall landing page. At the top, there's a red box around the 'Firewall' title and 'Microsoft' logo. Below the title, a paragraph describes Azure Firewall as a managed cloud-based network security service. A 'Save for later' button is visible. Under the publisher information, there are links for 'Learn more', 'Documentation', and 'Pricing'. At the bottom, a section titled 'Select a software plan' shows a dropdown menu with 'Firewall' selected, and a detailed description of the service. A large blue 'Create' button is at the bottom left of this section.

2. On the **Create a Firewall** page, use the following table to configure the firewall, when finished click **Review + create** then **Create**
 - **Subscription:** < your Azure subscription >
 - **Resource group:** Test-FW-RG < the resource group you created earlier >
 - **Name:** Test-FW01
 - **Region:** < Select the same location that you used previously >
 - **Choose a virtual network:** Test-FW-VN < the VNET you created earlier >
 - **Public IP address:** < select **Create new** radio button >
 - **Public IP address:** < accept the default value >
 - **Public IP address SKU:** Standard

MCT USE ONLY. STUDENT USE PROHIBITED

Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#).

PROJECT DETAILS

* Subscription: Visual Studio Ultimate with MSDN

* Resource group: Test-FW-RG [Create new](#)

INSTANCE DETAILS

* Name: Test-FW01

* Region: West Europe

Choose a virtual network Create new Use existing

Virtual network: Test-FW-VN (Test-FW-RG)

PUBLIC IP ADDRESS

* Public IP address Create new Use existing

* Public IP address name: azureFirewalls-ip

Public IP address SKU: Standard

Review + create Previous Next : Tags > Download a template for automation

3. After deployment completes, go to the **Test-FW-RG** resource group, and click the **Test-FW01** firewall.
4. Take note of the private IP address. You will use it later when you create the default route.

Resource group (change)	: Test-FW-RG	Virtual network/subnet :	Test-FW-VN/AzureFirewallSubnet
Location	: West Europe	Private IP address	10.0.1.4
Subscription (change)	: Visual Studio Ultimate with MSDN	Public IP address	: azureFirewalls-ip
Subscription ID	: 6e9a285a-37ea-40e6-b2fc-28539051852e	Provisioning state	: Succeeded
Tags (change)	: Click here to add tags		

Create a default route for our workload server to take through the Azure Firewall

For the **Workload-SN** subnet, configure the outbound default route to go through the firewall.

1. From the Azure portal home page, click **All services**. Under **Networking**, click **Route tables**.

The screenshot shows the Microsoft Azure portal's 'All services' page. The left sidebar has 'Networking' selected under the 'Networking' category. In the main pane, 'Virtual networks' is the top item, followed by 'Route tables', which is also highlighted with a red box.

2. In the Route tables pane click + **Add** and enter the following details and when finished click **Create**
 - **Name:** Firewall-route
 - **Subscription:** < select your subscription >
 - **Resource group:** Test-FW-RG < the resource group you created earlier >
 - **Location:** < select the same location that you used previously >

Create route table

You can add routes to this table after it's created.

* Name
Firewall-route

* Subscription
Visual Studio Ultimate with MSDN

* Resource group
Test-FW-RG

* Location
West Europe

Virtual network gateway route propagation
Disabled Enabled

Create Automation options

3. When it is finished click **Refresh**, and then click the **Firewall-route** route table.
4. Click **Subnets** > + **Associate**.
5. Click **Virtual network** > **Test-FW-VN**.

6. For **Subnet**, click **Workload-SN**. Make sure that you select **only** the **Workload-SN** subnet for this route, otherwise your firewall won't work correctly.
7. Click **OK**.

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP
Workload-SN	10.0.2.0/24	Test-FW-VN	-

8. Click **Routes** > **+ Add** and enter the following details and click **OK** when finished
 - **Route name:** WORKSRV-TO-FW-OUT
 - **Address prefix:** 0.0.0.0/0
 - **Next hop type:** Virtual appliance. (Azure Firewall is actually a managed service, but *virtual appliance* works in this situation.)
 - **Next hop address** < enter the private IP address for the firewall that you noted previously >

Add route

Firewall-route

* Route name
WORKSRV-TO-FW-OUT

* Address prefix
0.0.0.0/0

Next hop type
Virtual appliance

* Next hop address
10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

OK

Configure an application rule in Azure Firewall

Now we will create an *application rule* that allows outbound access to www.microsoft.com

1. Open the **Test-FW-RG**, and click the **Test-FW01** firewall.
2. On the **Test-FW01** page, under **Settings**, click **Rules**.
3. Click the **Application rule collection** tab.
4. Click **+ Add application rule collection** and enter the following values, then click **Add** when finished
 - **Name:** App-Coll01
 - **Priority:** 200

- **Action:** Allow
- **Rules**
 - **Target FQDNs**
 - **NAME:** AllowWebsite
 - **SOURCE ADDRESS:** 10.0.2.0/24
 - **PROTOCOL:PORT:** http, https
 - **TARGET FQDNs:** www.microsoft.com (You can specify part of all or a URL, including wild characters, or just a single wild character to indicate all internet sites)

NAME	SOURCE ADDRESSES	PROTOCOL:PORT	TARGET FQDNs
AllowWebsite	10.0.2.0/24	http, https	www.microsoft.com

Note: Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes. For more information, see [Infrastructure FQDNs⁵](#). You can also use [FQDN tags⁶](#) to represent a group of fully qualified domain names (FQDNs) associated with well-known Microsoft services, such as Windows Update, Azure Backup etc.

Configure a network rule

Now we will create a *network rule* that allows outbound access to two IP addresses over port 53, to allow our workload server access DNS servers.

1. Open the **Test-FW-RG**, and click the **Test-FW01** firewall.
2. On the **Test-FW01** page, under **Settings**, click **Rules**.
3. Click the **Network rule collection** tab.
4. Click **+ Add network rule collection** and enter the following details, when finished click **Add**
 - **Name:** Net-Coll01

⁵ <https://docs.microsoft.com/en-us/azure/firewall/infrastructure-fqdns>

⁶ <https://docs.microsoft.com/en-us/azure/firewall/fqdn-tags>

- **Priority:** 200
- **Action:** Allow
- **Rules:**
 - **IP Addresses:**
 - **NAME:** AllowDNS
 - **PROTOCOL:** UDP
 - **SOURCE ADDRESSES:** 10.0.2.0/24
 - **DESTINATION ADDRESSES:** 209.244.0.3,209.244.0.4
 - **DESTINATION PORTS:** 53

Add network rule collection

* Name Net-Coll01

* Priority 200

* Action Allow

Rules

NAME	PROTOCOL	SOURCE ADDRESSES	DESTINATION ADDRESSES	DESTINATION PORTS
AllowDNS	UDP	10.0.2.0/24	209.244.0.3,209.244.0.4	53
	0 selected	*, 192.168.10.1, 192.168.10.0/24,...	*, 192.168.10.1, 192.168.10.0/24,...	8080, 8080-8090, *

Service Tags

NAME	PROTOCOL	SOURCE ADDRESSES	SERVICE TAGS	DESTINATION PORTS
	0 selected	*, 192.168.10.1, 192.168.10.0/24,...	0 selected	8080, 8080-8090, *

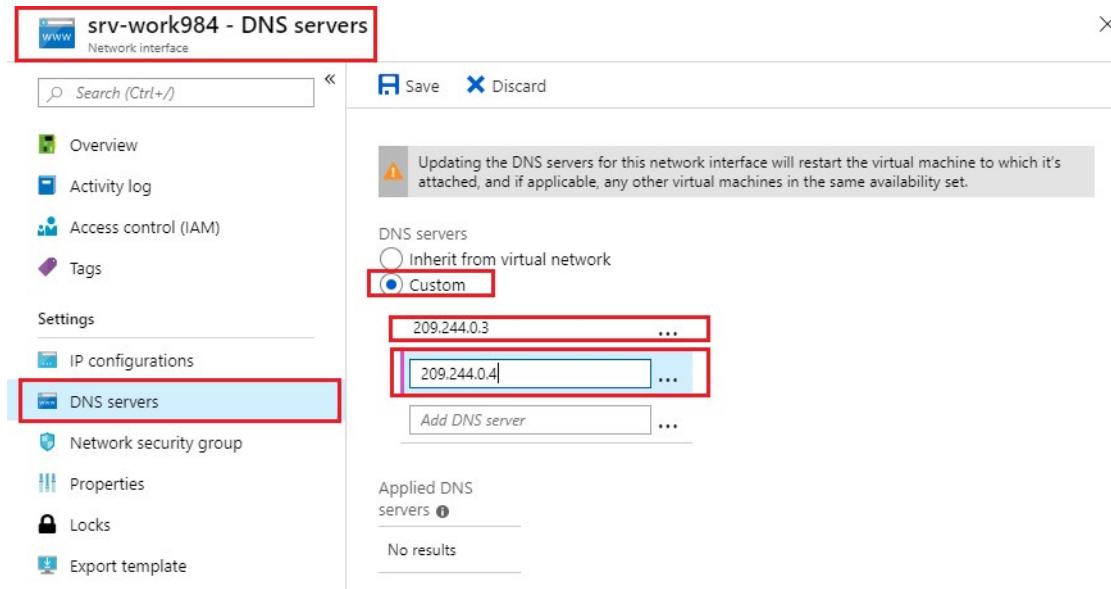
Add

Change the primary and secondary DNS address for the Srv-Work network interface

For testing purposes in this tutorial, you configure the primary and secondary DNS addresses. This isn't a general Azure Firewall requirement.

1. From the Azure portal, open the **Test-FW-RG** resource group.
2. Click the **network interface** for the **Srv-Work** virtual machine, it should be named something like **Srv-Work-xyz**.
3. Under **Settings**, click **DNS servers**.
4. Under **DNS servers**, click **Custom** and add the following details and click **Save** when finished.
 - **Box 1 - Add DNS Server:** 209.244.0.3
 - **Box 2 - Add DNS Server:** 209.244.0.4

Note: Updating the DNS records for the Network interface may automatically restart the virtual machine to which it is attached, if so you should see a message indicating such. Also the IP Addresses we are adding here are pre-existing publicly accessible DNS Server addresses. When our virtual machine looks for an external address it will refer to these DNS servers for the address details.

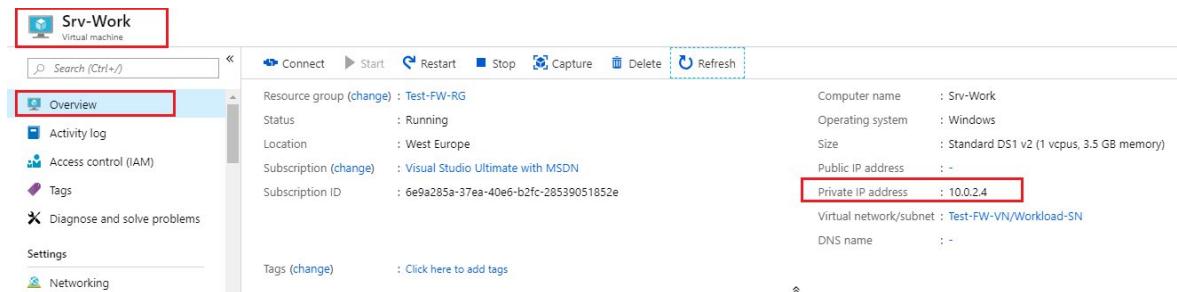


5. Go to the Srv-Work virtual machine and ensure it has a status of running, if it is de-allocated click **Start**, or if it has not re-started click **Restart**. If you do not restart the virtual machine, you may have difficulty signing into the virtual machine later.

Test the firewall

Now test the firewall to confirm that it works as expected.

1. From the Azure portal, review the network settings for the **Srv-Work** virtual machine and note the private IP address.

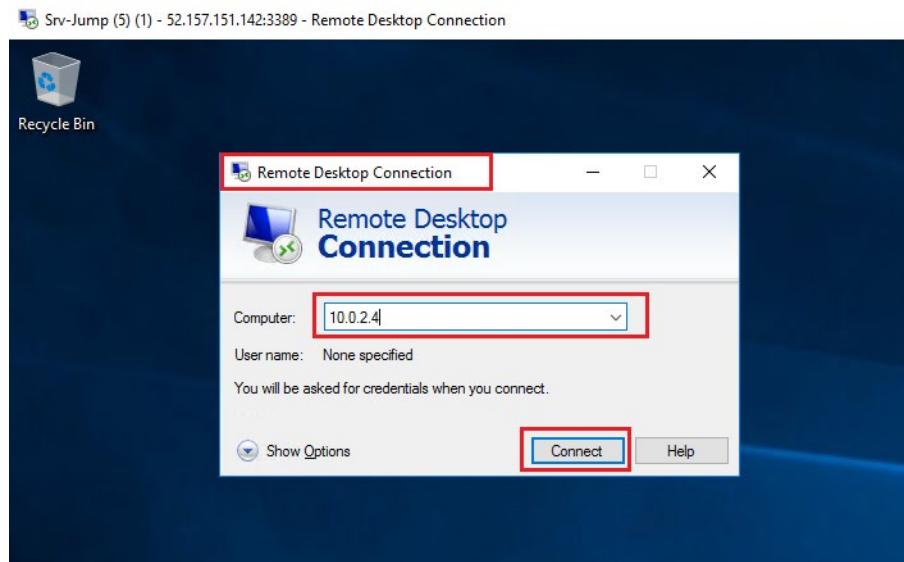


2. In the Azure Portal go to the **Srv-Jump** virtual machine and click **Connect**, followed by **Download RDP File** to open an RDP session to the **SRV-Jump** virtual machine, using the credentials you specified earlier when creating the VM.

MCT USE ONLY. STUDENT USE PROHIBITED

If you encounter any issues connecting to the virtual machine restart it.

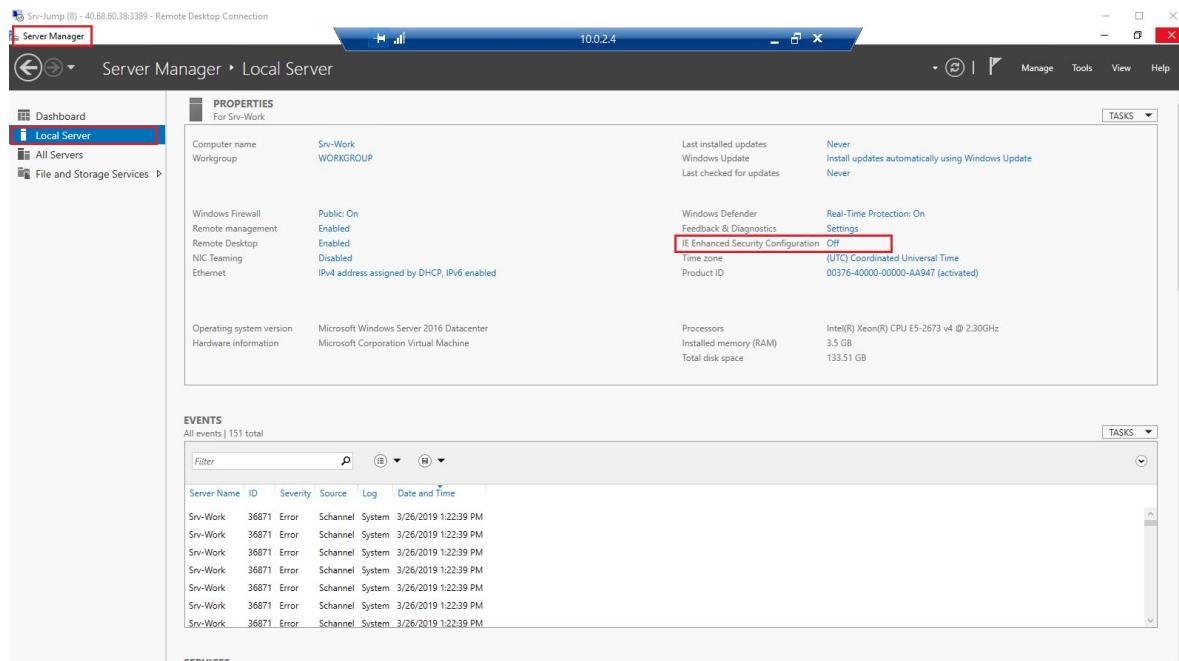
- From within the **Srv-Jump** virtual machine, click on the **Start** button, to open the start menu, then type **Remote** and click on the resultant **Remote Desktop Connection** desktop app to open it. In the **Remote Desktop Connection** dialogue, enter the private IP address that you noted earlier for the **Srv-Work** VM, then click **Connect** to open a remote desktop connection to the **Srv-Work** virtual machine. Accepting the prompts as encountered and entering the user name and password you specified earlier when creating the virtual machine i.e. **.\azureuser** and **Password0134!**



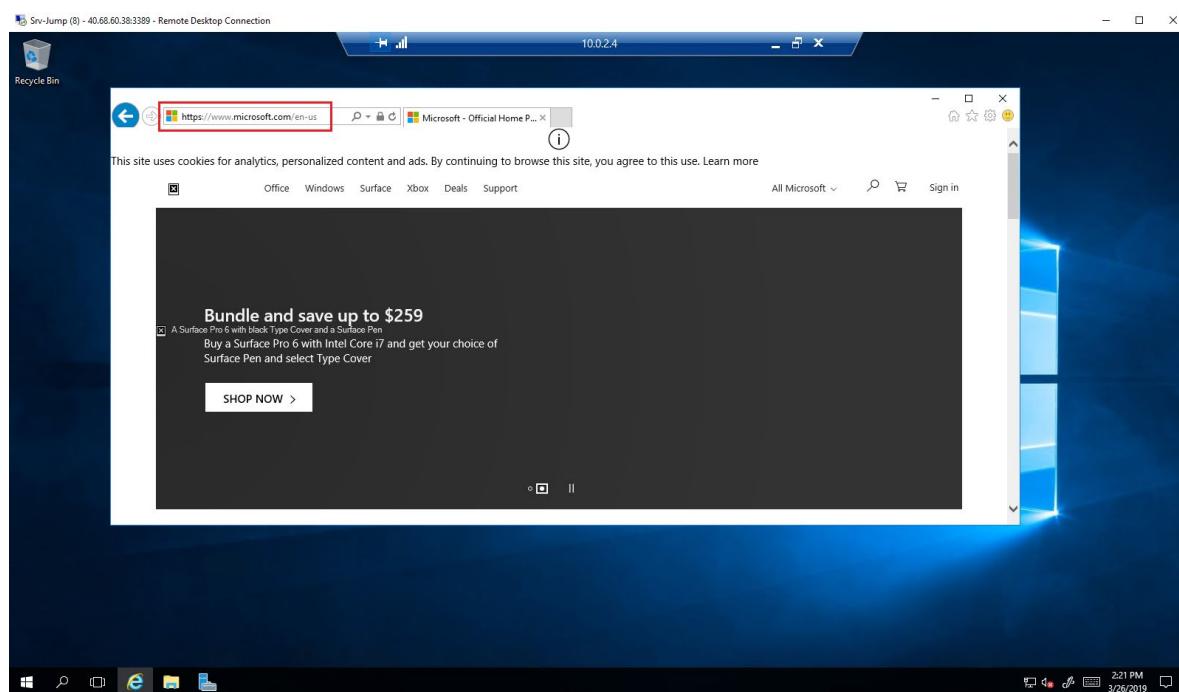
- Once logged into the **SRV-Work** virtual machine, allow **Server Manager** to open, which it will do automatically after logging in, then go to **Local server** and turn off **IE Enhanced Security Configuration** by clicking the **On** setting, and in the **Internet Explorer Enhanced Configuration** dialogue select **Off** for *administrators* and *users* and then clicking **OK**. The setting will then change to **Off** in **Server Manager**.

Note: In production environments you would not do this. This is done to reduce and prevent pop-ups in our test scenario. In a production scenario you would probably use a workload server with no GUI environment or browser applications present.

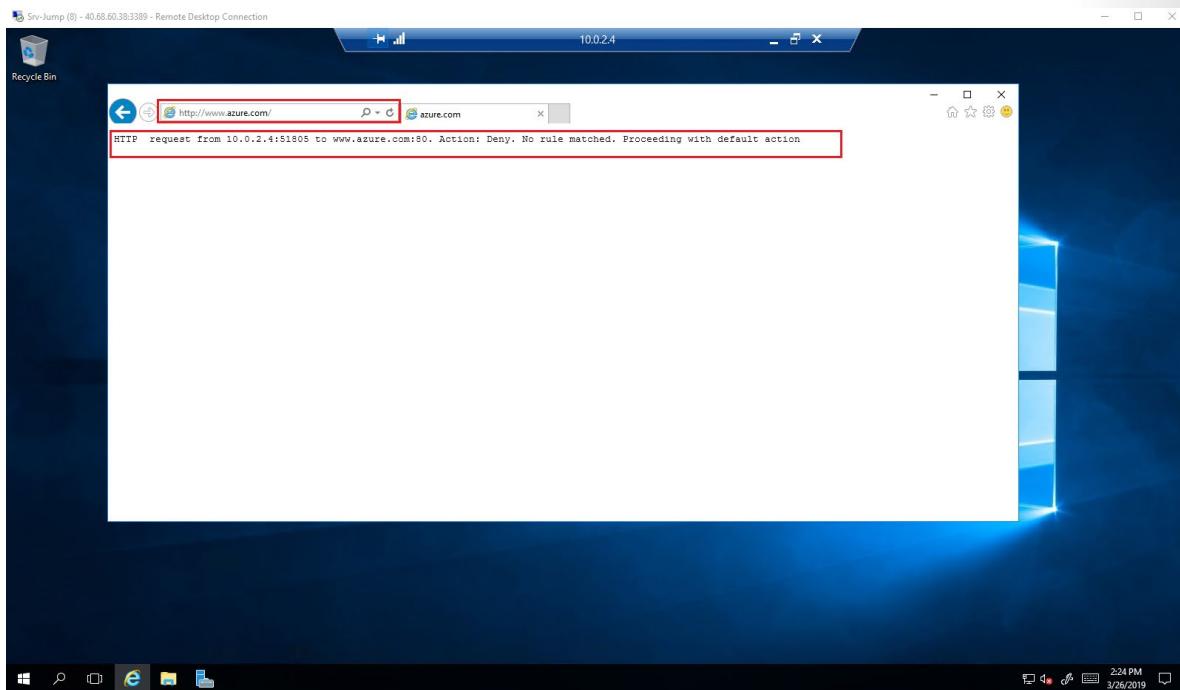
MCT USE ONLY. STUDENT USE PROHIBITED



5. Open **Internet Explorer**, accept the default or recommended settings, in any prompts you receive, and then browse to <https://www.microsoft.com>
6. Click **OK** > **Close** on the security alerts that may pop-up.
7. You should see the Microsoft.com home page.



8. Now browse to <http://www.azure.com/>. You should be blocked by the firewall and receive a message similar to that displayed in the screenshot below.



Note: If you do not receive the message as per the screenshot, this could be due to re-directs being used to account for changes to the site over time. You should try a non-Microsoft URL.

Congratulations! You have created two virtual machines, one which represented a virtual machine running a workload in Azure, and which was isolated by running it in a separate network, and another virtual machine which acted as a jump server, which was used to connect to the workload server. You configured the workload virtual machine network interface to allow it to resolve DNS names using the configured external DNS server and you created and configured Azure Firewall through which all traffic from the workload server was routed. You also created rules in Azure Firewall to *allow* access to a particular website and then verified Azure Firewall functionality by ensuring other non-specified websites were not accessible.

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.

Azure DDoS Protection

Distributed Denial of Service (DDoS) attacks attempt to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Thus, any resource exposed to the internet, such as a website, is potentially at risk from a DDoS attack.



When you combine *Azure DDoS Protection* with application design best practices, you help provide defense against DDoS attacks. DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The Azure DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.

Azure DDoS protection service tiers

Azure DDoS Protection provides the following service tiers:

- *Basic*. The Basic service tier is automatically enabled as part of the Azure platform. Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. Azure's global network is used to distribute and mitigate attack traffic across regions.
- *Standard*. The Standard service tier provides additional mitigation capabilities that are tuned specifically to Microsoft Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gateway.

DDoS standard protection

DDoS standard protection can mitigate the following types of attacks:

- *Volumetric attacks*. The attack's goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
- *Protocol attacks*. These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
- *Resource (application) layer attacks*. These attacks target web application packets to disrupt the transmission of data between hosts.

Note: You can read more about Azure DDoS Protection from the page [Azure DDoS Protection⁷](#).

Network Security Groups (NSG)

Network Security Groups (NSGs) allow you to filter network traffic to and from Azure resources in an Azure virtual network. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.



⁷ <https://azure.microsoft.com/en-us/services/ddos-protection/>

Network security rule properties

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies the following properties:

Property	Explanation
Name	Unique name of the NSG.
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	Individual IP address or IP address range, service tag, or application security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	An individual port or range of ports.
Action	Allow or Deny.

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

Note: You can read more about NSGs on the [Security groups⁸](#) page.

Application Security Groups (ASG)

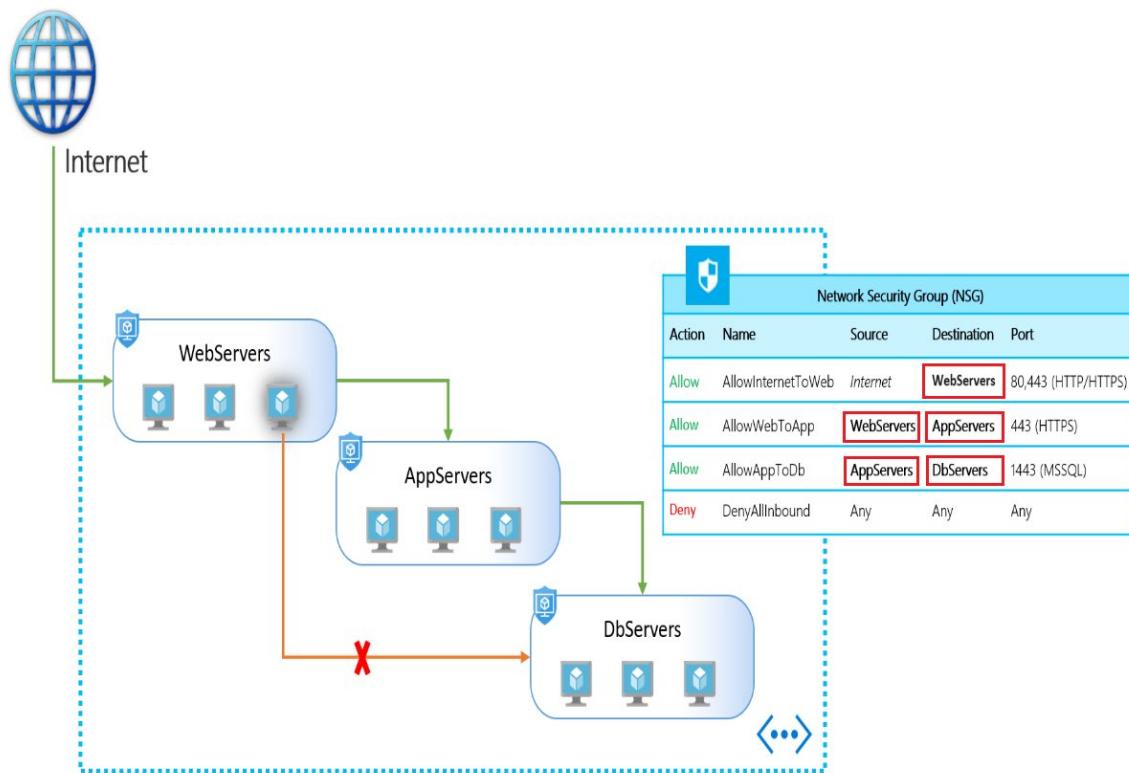
Application security groups (ASGs) enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.



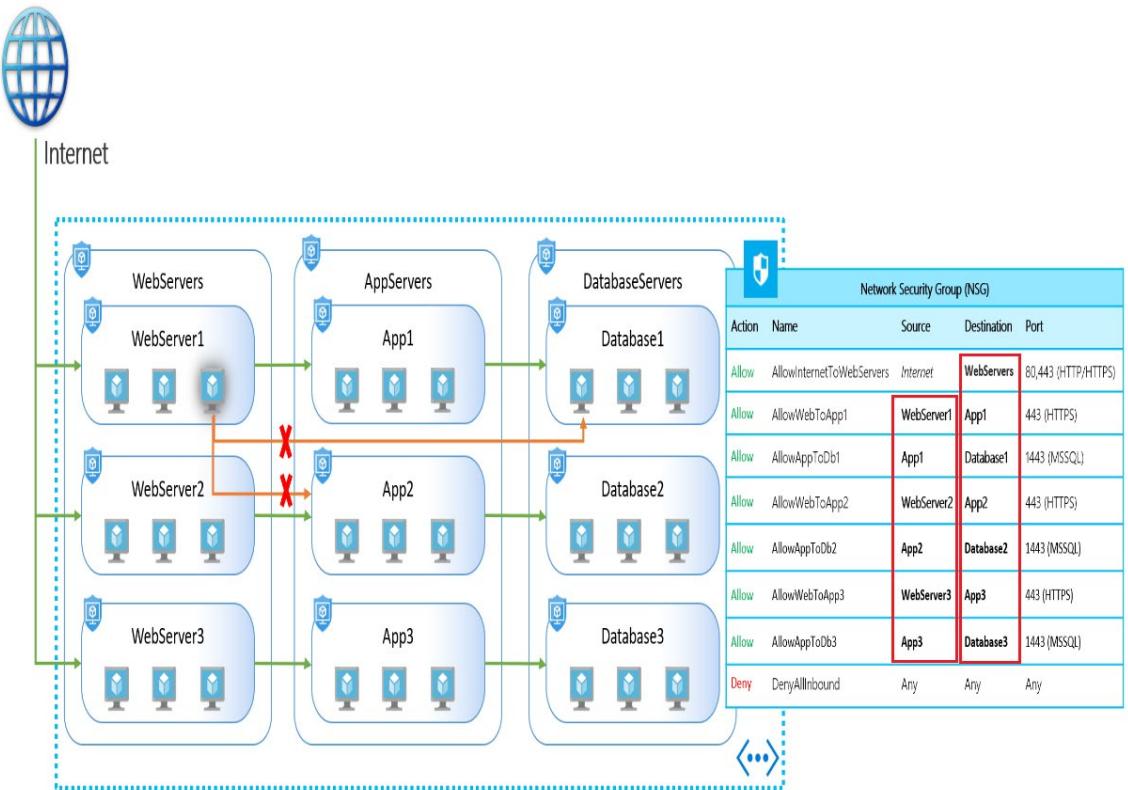
This feature allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

An ASG enables you to group servers with similar port filtering requirements, and group together servers with similar functions, such as web servers. In the below example we have ASGs defined for WebServers, AppServers and DbServers and green and red arrows indicating which network traffic paths are allowable and which are not.

⁸ <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups>



In the below example, multiple applications are deployed into the same virtual network. Based on the security rules described, workloads are isolated from each other. If a VM from one of the applications is compromised, lateral exploration is limited, minimizing the potential impact of an attacker. In this example, let's assume one of the web server VMs from application1 is compromised, the rest of the application will continue to be protected, even access to critical workloads like database servers will still be unreachable. This implementation provides multiple extra layers of security to your network, making this intrusion less harmful and easy to react on such events.



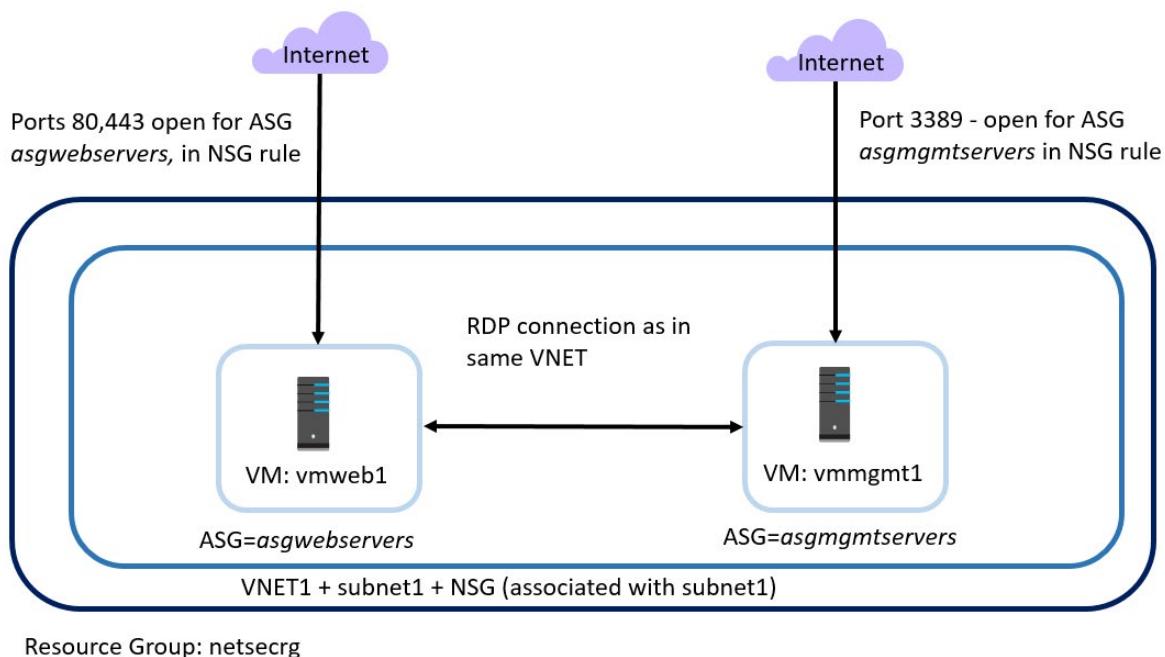
ASGs help simplify how you can filter and control network traffic coming into your organization and how that network traffic is allowed to move. They allow you to isolate multiple workloads and provide additional levels of protection for your virtual network in a more easily manageable way. See [Application security groups⁹](#) for more details.

Walkthrough-Secure Network traffic using NSGs and ASGs

In this walkthrough task we will create a virtual network and subnet, we will create two application security groups, one for management servers and one for web servers, then create a Network Security group (NSG) and associate that NSG to the subnet. We will then create two inbound network security rules, *allow-rdp-all* and *allow-web-all* traffic.

We will then create two virtual machines, one to represent a management server, and one to represent a web server, associate those virtual machines with their respective application security groups, and then with the network security group (NSG). We will then test the network security rules we have created and applied. The relationship and configuration of the resources we will create is presented in the graphic below.

⁹ <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups>



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 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 today¹⁰](#) webpage.

Steps

Create a virtual network

1. Sign into the Azure Portal
2. Select **+ Create a resource** on the upper, left corner of the Azure portal, then select **Networking**, and then select **Virtual network**.

¹⁰ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Microsoft Azure portal's 'Create a resource' interface. On the left, a sidebar lists various service categories like Home, Dashboard, All services, Favorites, Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, Azure Active Directory, Monitor, and Security Center. A red box highlights the 'Create a resource' button at the top of the sidebar. The main area is titled 'New' and shows the 'Azure Marketplace'. A search bar at the top says 'Search the Marketplace'. Below it, there are sections for 'Get started', 'Recently created', 'Compute', and 'Networking'. The 'Networking' section is highlighted with a blue box. Under 'Networking', there are several items: Storage, Web, Mobile, Containers, Databases, Analytics, AI + Machine Learning, Internet of Things, Load Balancer, Application Gateway, Front Door, Virtual network gateway, and Virtual WAN. The 'Virtual network' item is highlighted with a red box. Each item has a 'See all' link next to it.

3. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Create**:
 - **Name:** VNET1
 - **Address space:** 10.0.0.0/16
 - **Subscription :** < select your subscription >
 - **Resource group:** < Select Create new and enter **netsecrg**. >
 - **Location:** (US) East US (or a datacenter location near you)
 - **Subnet:**
 - **Name:** subnet1
 - **Address range:** 10.0.0.0/24

MCT USE ONLY. STUDENT USE PROHIBITED

Create virtual network □ X

* Name ✓

* Address space ✓
10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription

* Resource group ▼
[Create new](#)

* Location ▼

Subnet

* Name ✓

* Address range ✓
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (256 addresses)

DDoS protection ● Basic ○ Standard

Service endpoints ● Disabled ○ Enabled

Firewall ● Disabled ○ Enabled

Create Automation options

Create two application security groups

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

1. Select **+ Create a resource** on the upper, left corner of the Azure portal.
2. 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.

MCT USE ONLY. STUDENT USE PROHIBITED

3. Enter the following values then click **Review and Create** followed by **Create**

- **Subscription** : < select your subscription >
- **Resource group**: < Select existing... and then select *netsecrg* which you created earlier. >
- **Name**: asgwebservers
- **Region**: (US) East US

4. Complete steps **1 to 3** again to create another Application security group, specifying the following values:

- **Subscription** : < select your subscription >

- **Resource group:** < Select existing... and then select netsecrg which you created earlier. >
- **Name:** asgmgmtservers
- **Region:** (US) East US

Create an application security group

Basics Tags Review + create

PROJECT DETAILS

* Subscription Visual Studio Ultimate with MSDN

 * Resource group netsecrg

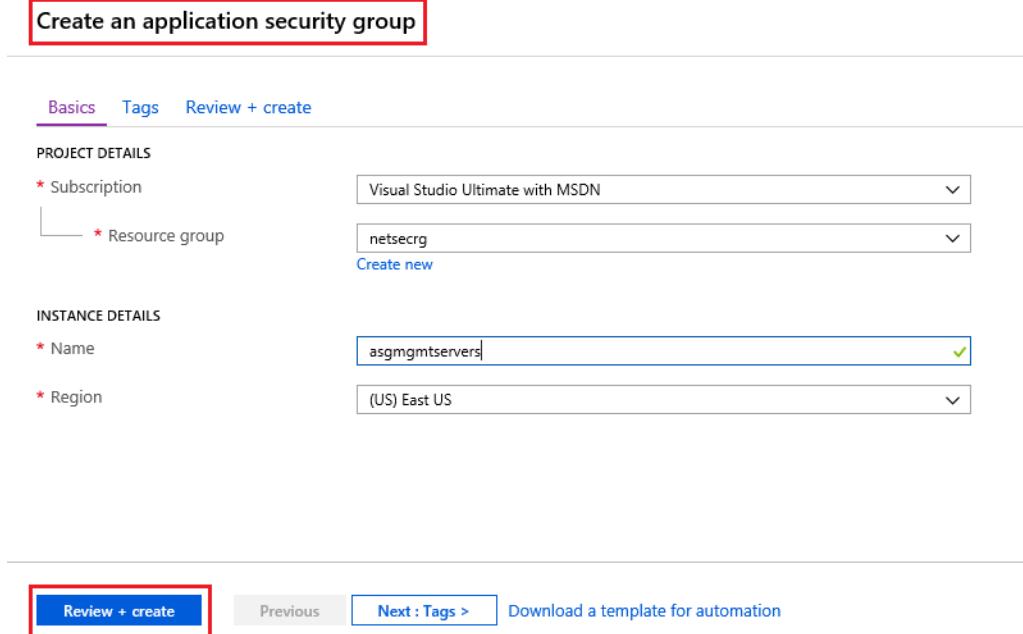
 Create new

INSTANCE DETAILS

* Name asgmgmtservers

* Region (US) East US

Review + create Previous Next : Tags > Download a template for automation



Create a network security group

1. Select + **Create a resource** on the upper, left corner of the Azure portal, then select **Networking**, and then select **Network security group**.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like Home, Dashboard, and All services. A red box highlights the 'Create a resource' button. The main area is titled 'Create network security group' and shows a 'New' section with a search bar. Below it is the 'Azure Marketplace' with tabs for 'See all' and 'Featured'. A red box highlights the 'Networking' category. Under 'Networking', a red box highlights the 'Network security group' item, which includes a 'Quickstart tutorial' link. Other items listed include Virtual network, Load Balancer, Application Gateway, Front Door, Virtual network gateway, Virtual WAN, ExpressRoute, and Developer Tools.

2. Enter, or select, the following information, and then select **Create**:

- **Name:** nsg1
- **Subscription :** < select your subscription >
- **Resource group:** < Select existing... and then select **netsecrg** which you created earlier. >
- **Location:** (US) East US

Create network security g...

* Name
nsg1

* Subscription
Visual Studio Ultimate with MSDN

* Resource group
netsecrg
Create new

* Location
(US) East US

Create Automation options

Associate the network security group to a subnet

1. Open the Network security group you just created, **nsg1**, Under **SETTINGS**, select **Subnets** and then select **+ Associate**

nsg1 - Subnets
Network security group

Search (Ctrl+ /)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces**
- Subnets** (highlighted with a red box)
- Properties
Locks
Export template

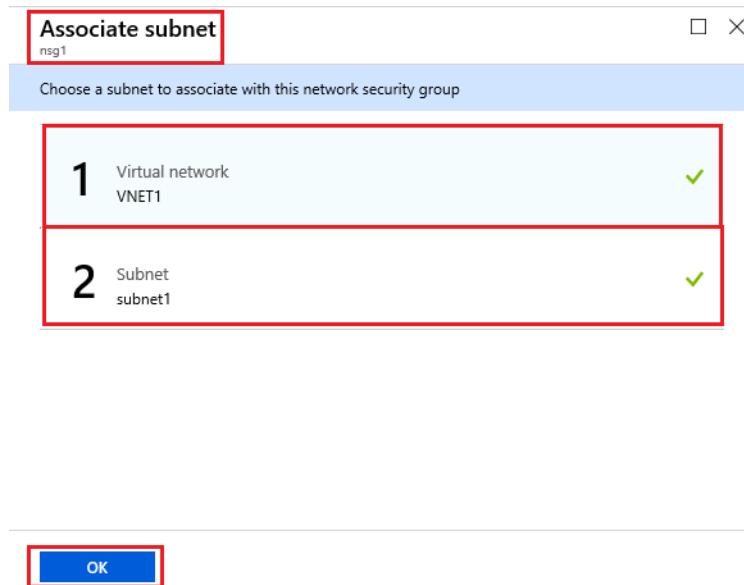
+ Associate

Search subnets

NAME
No results.

2. Under **Associate subnet**, select Virtual network and then select the virtual network you created earlier i.e. **VNET1**. Then, select Subnet and choose the subnet you created earlier i.e. select **subnet1**, and then select **OK**.

MCT USE ONLY. STUDENT USE PROHIBITED



Create security rules

1. Still in the Network Security group, Under **SETTINGS**, select **Inbound security rules** and then select **+ Add**.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetw...	VirtualNetw...	Allow
65001	AllowAzureLoadBalance...	Any	Any	AzureLoadB...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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

- **Source:** Any
- **Source port ranges:** *

- **Destination:** Application security group
- **Destination application security group:** asgwebservers
- **Destination port ranges:** 80,443
- **Protocol:** TCP
- **Action:** Allow
- **Priority:** default
- **Name:** Allow-Web-All

This allows us to connect to the web server from the internet over ports 80 and 443 only.

3. Create another inbound security rule by repeating steps **1** and **2** again, using the following values:

- **Source:** Any
- **Source port ranges:** *
- **Destination:** Application security group
- **Destination application security group:** asgmgmtservers
- **Destination port ranges:** 3389
- **Protocol:** TCP
- **Priority:** 110
- **Name:** Allow-RDP-All

Note:

- The port **3339**, the rdp port, is exposed to the internet for the VM that is assigned to the **asgmgmtservers** 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.
- Also, we designated the value **Any** for source to indicate access from the internet.

4. Review the rules you created. Your list should look like the list in the following picture:

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	Allow-Web-All	80,443	TCP	Any	asgwebservers	Allow
110	Allow-RDP-All	3389	TCP	Any	asgmgmtservers	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Create virtual machines

We will now create two VMs in the virtual network, to which we will apply our network security rules.

1. In the Azure Portal, click on the **Cloud Shell** icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.

A screenshot of the Azure Cloud Shell interface. The title bar shows "PowerShell". The main area displays a PowerShell session:

```
PowerShell | ⚡ ? 🚧 🔍 { } ⏪ ...
Requesting a Cloud Shell. Succeeded.
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: Manage Azure Active Directory: Get-Command -Module AzureAD*
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:>
```

3. Run the below Azure CLI command to create the first virtual machine, this command will run fine in either **powershell** or **bash** console. You can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
az vm create \
    --name vmmgmt1 \
    --resource-group netsecrg \
    --image Win2019Datacenter \
    --location eastus \
    --vnet-name VNET1 \
    --subnet subnet1 \
    --nsg nsg1 \
    --asg asgmgmtservers \
    --admin-username azureuser \
    --admin-password Password0134!
```

Note: The command will take two to three minutes to complete and should run successfully. Do not continue to the next step until the VM is deployed.

```
PowerShell | ⚡ ? ⚡ { } ⚡
Azure:/ PS Azure:\> az vm create `>> --name vmmgmt1 `>> --resource-group netsecrg `>> --image Win2019Datacenter `>> --location eastus `>> --vnet-name VNET1 `>> --subnet subnet1 `>> --nsg nsg1 `>> --asg asgmgmtservers `>> --admin-username azureuser `>> --admin-password Password0134!`> { "fqdns": "", "id": "/subscriptions/", "location": "eastus", "macAddress": "00-0D-3A-54-33-50", "powerState": "VM running", "privateIpAddress": "10.0.0.4", "publicIpAddress": "52.168.180.68", "resourceGroup": "netsecrg", "zones": "" } Azure:/ PS Azure:\> []
```

3. Create the second virtual machine by running the following command in the same cloud shell console in the browser window.

```
az vm create `> --name vmweb1 `> --resource-group netsecrg `> --image Win2019Datacenter `> --location eastus `> --vnet-name VNET1 `> --subnet subnet1 `> --nsg nsg1 `> --asg asgwebservers `> --admin-username azureuser `> --admin-password Password0134!
```

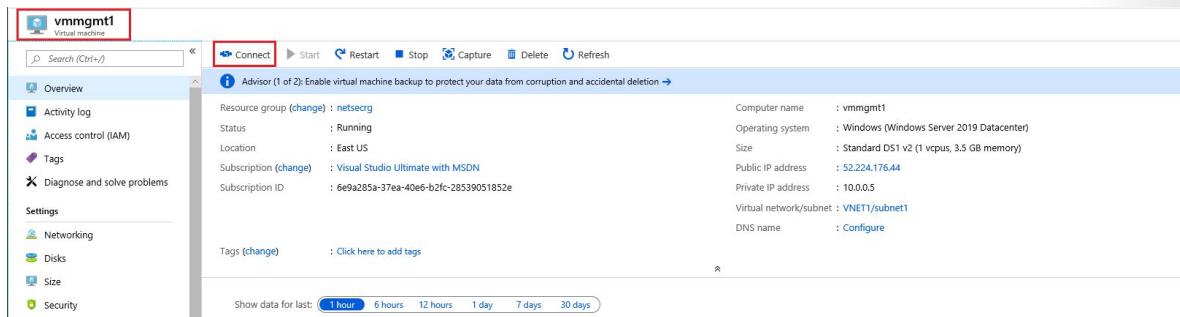
```
PowerShell | ⚡ ? ⚡ { } ⚡
Azure:/ PS Azure:\> az vm create `>> --name vmweb1 `>> --resource-group netsecrg `>> --image Win2019Datacenter `>> --location eastus `>> --vnet-name VNET1 `>> --subnet subnet1 `>> --nsg nsg1 `>> --asg asgwebservers `>> --admin-username azureuser `>> --admin-password Password0134!`> { "fqdns": "", "id": "/subscriptions/", "location": "eastus", "macAddress": "00-0D-3A-19-D0-04", "powerState": "VM running", "privateIpAddress": "10.0.0.5", "publicIpAddress": "40.117.141.231", "resourceGroup": "netsecrg", "zones": "" } Azure:/ PS Azure:\> []
```

NOTE:

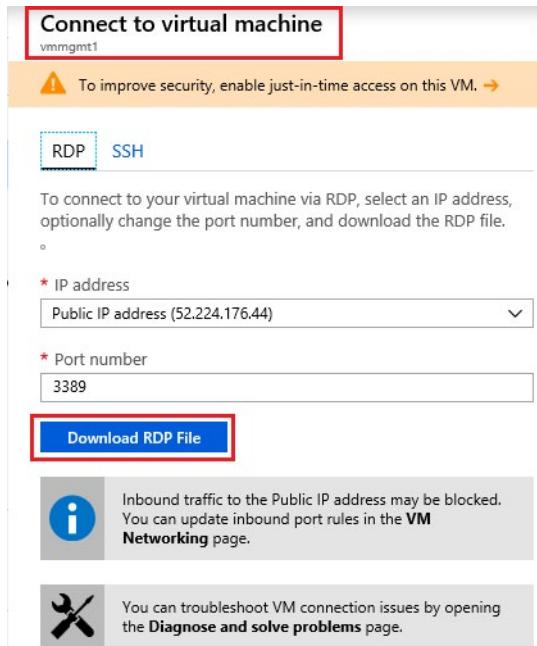
- We created a network interface for each VM, and attached the network interface to the VM.
- Both network interfaces are in Virtual network **VNET1** and its subnet **subnet1**.
- **subnet1** is part of the Network Security Group, **nsg1**, so as such the **nsg1** security rules are applied to the two virtual machines.
- **vmmgmt1** has been associated with the application security group **asgmgmtservers**
- **vmweb1** has been associated with the application security group **asgwebservers**

Test traffic filters

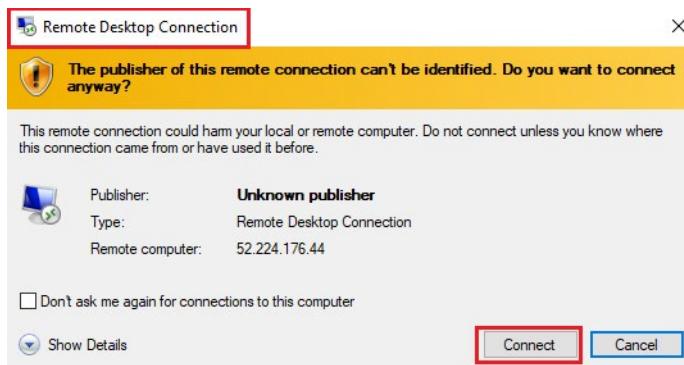
1. In the Azure Portal, go to your resource group, i.e. **netsecrg**, open the **vmmgmt1** virtual machine and connect to it by clicking on the **Connect** button.



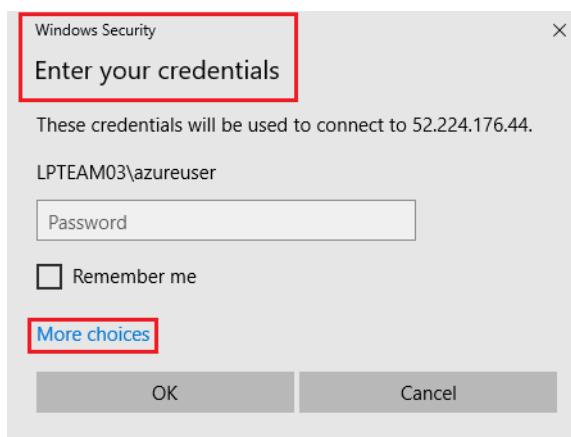
2. In the **Connect to virtual machine** blade select **Download RDP File** and click to open the rdp file when prompted to do so.



3. In the **Remote Desktop Connection** dialogue select **Connect**.



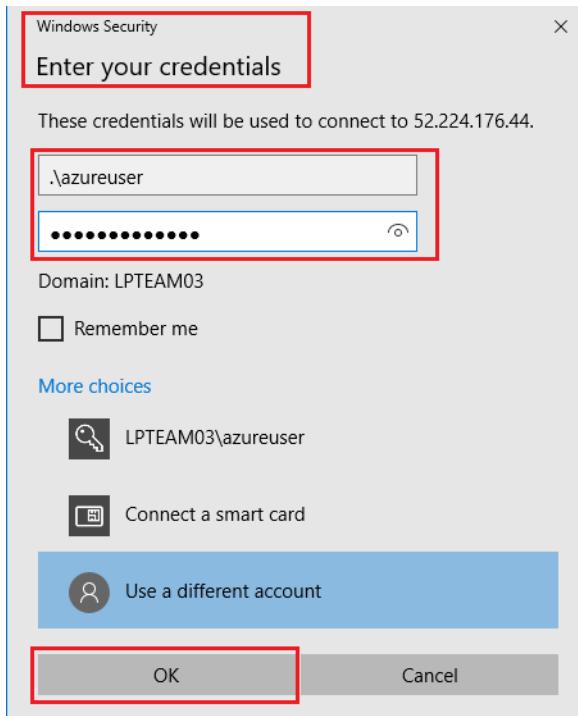
4. In the **Windows Security > Enter your credentials** dialogue select **More Choices**



5. Select use a different account and enter the user name and password you specified when creating the VM, as below, then click **OK**.

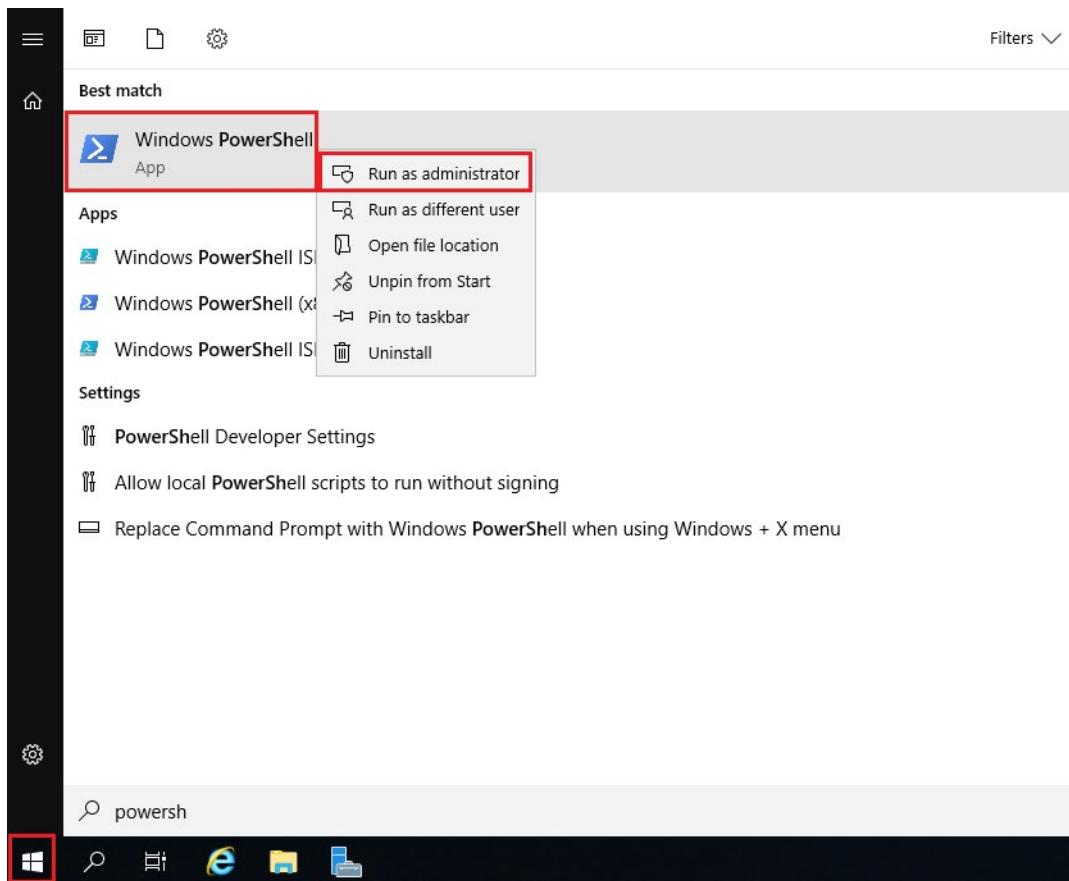
- **username**=.\azureuser (using the symbols .\ indicate for the dialogue to take the context of the local machine)
- **password** = Password0134!

Note: 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.



Note: The connection succeeds, because port 3389 is allowed inbound connections from the internet to the **asgmgmtservers** application security group, i.e. the **vmmgmt1** virtual machine is in the **VNET1** virtual network and the subnet **subnet1** which has those security rules associated with it as defined by the Network Security group **nsg1**.

6. From within the **vmmgmt1** virtual machine we will now connect via rdp to the **vmweb1** virtual machine. Still within the remote desktop connection to **vmmgmt1**, go to the start menu, type PowerShell, then locate and launch **Powershell**, by right clicking it and choosing **Run as Administrator**



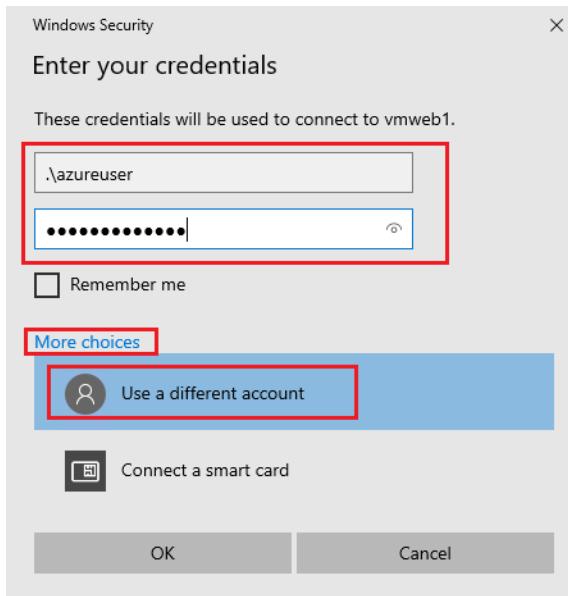
7. In that PowerShell console enter the below command to open a remote desktop connection to the other virtual machine you created, **vmweb1**.

```
mstsc /v:vmweb1
```

A screenshot of a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The window shows the command 'mstsc /v:vmweb1' being typed into the console. The background of the window is dark blue.

8. This will launch a remote desktop connection as before, and you will need to select the **More choices** option, then **Use a different account**, and then enter your credentials, as below.

- **username** = .\azureuser
- **password** = Password0134!

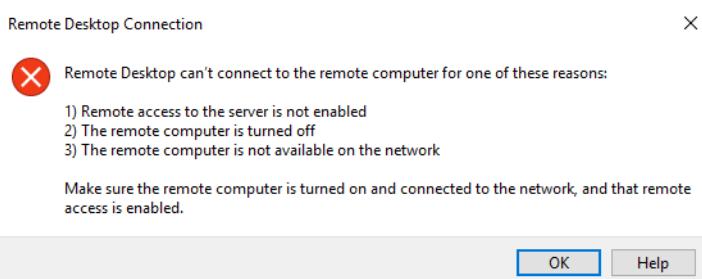


Note: You are able to connect to the **vmweb1** virtual machine from the **vmmgmt1** virtual machine because virtual machines in the same virtual network can communicate with each other over any port, by default. Leave the remote desktop connections to the **vmmgmt1** and **vmweb1** virtual machines open as we will return to them.

9. Try to connect to the **vmweb1** virtual machine from the internet by returning to the Azure Portal, then open the **vmweb1** virtual machine and connect to it by clicking on the **Connect** button.

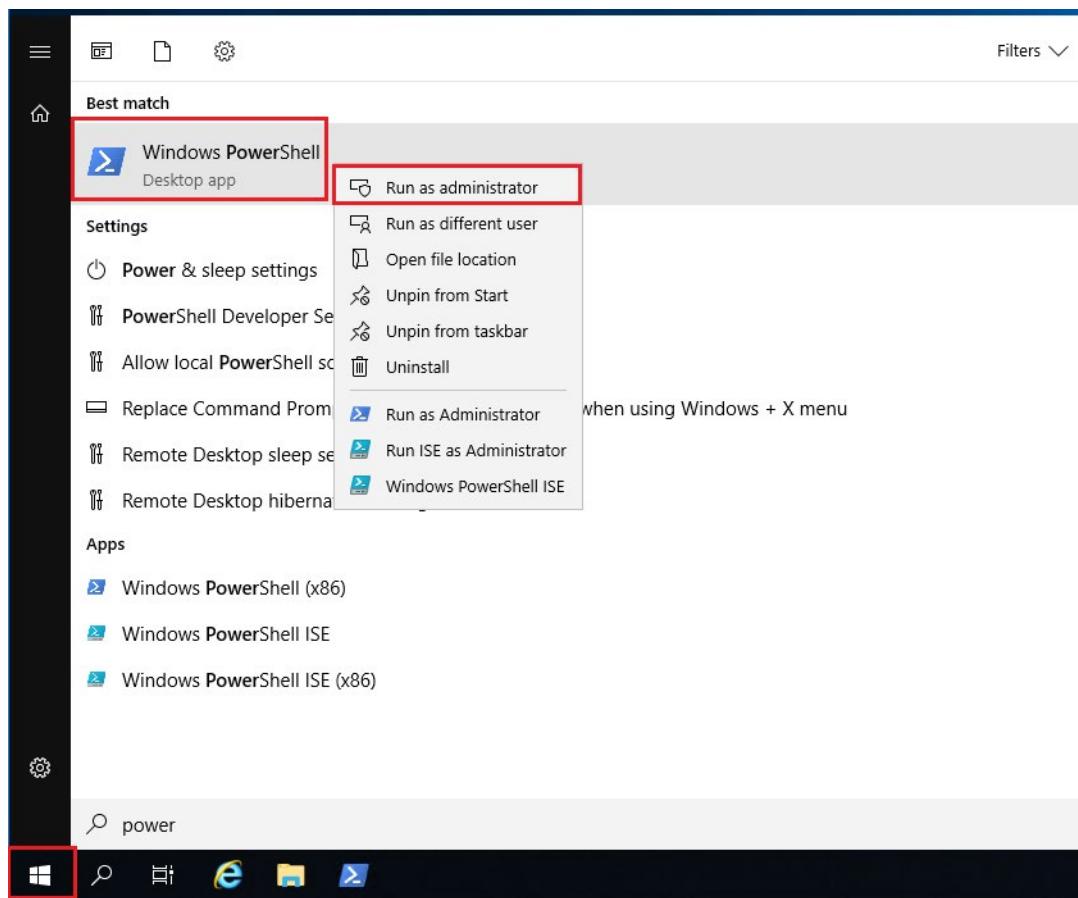
The screenshot shows the Azure portal's VM details page for 'vmweb1'. On the left, a sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (Networking, Disks, Size), and 'Search (Ctrl+F)'. The main pane shows the VM's status as 'Running', location 'East US', and subscription information. A 'Connect' button is highlighted in red at the top right of the main pane. Below it are various management actions: Start, Restart, Stop, Capture, Delete, and Refresh. On the far right, detailed configuration settings are listed.

10. Follow the prompts to **Download rdp file**, **Open** and **Connect**, as before. However, you cannot create a remote desktop connection to the **vmweb1** virtual machine from the internet, because the security rule for the **asgwebservers** doesn't allow port **3389** inbound from the internet, by default.



Note: In the case of the **vmmgmt1** virtual machine, we specifically created a rule to allow connections over port 3389, and assigned that rule to the **asgmgmtservers** ASG, that the **vmmgmt1** virtual machine is a member of, thus we are able to connect to it from the internet over port 3389.

11. We will now install **Internet Information Service (IIS)** on the **vmweb1** to allow it function as a webserver. Return to the remote desktop connection to **vmweb1** virtual machine and open a **Powershell** prompt by clicking on the start button, typing **Powershell**, the right clicking it and choosing **Run as administrator**



12. In the resultant Powershell console prompt, install Microsoft **Internet Information Service (IIS)** on the **vmweb1** virtual machine, by running the following command within the Powershell session

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

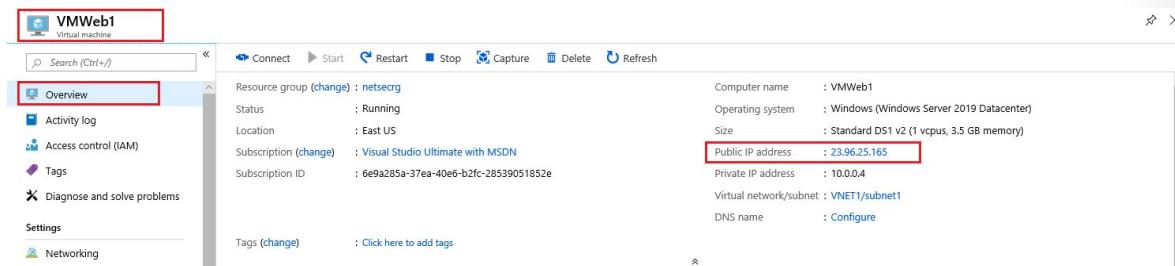
A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the command "Install-WindowsFeature -name Web-Server -IncludeManagementTools" entered at the PS C:\Users\azureuser> prompt. This command is highlighted with a red box. The window title bar also has a red box around the "Administrator" part. The background of the window is dark blue.

13. The installation should complete successfully.

```
PS C:\Users\azureuser> Install-WindowsFeature -name Web-Server -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No        Success          {Common HTTP Features, Default Document, D...
PS C:\Users\azureuser>
```

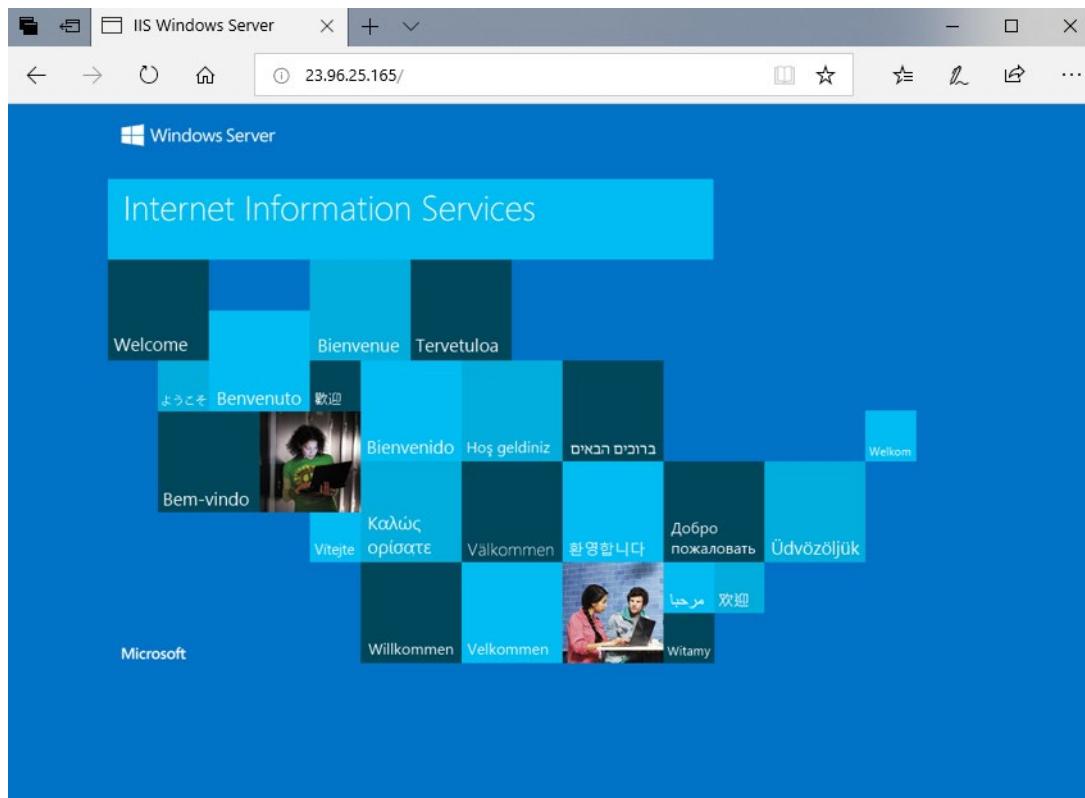
14. Disconnect from the **vmweb1** virtual machine, which leaves you in the **vmmgmt1** remote desktop connection, then also disconnect from the **vmmgmt1** virtual machine.

15. In the Azure portal open the **vmweb1**, go to **Overview** and note the **Public IP address** for the virtual machine. The address shown in the following picture is 23.96.25.165, but your address will be different:



16. From your local machine access the **vmweb1** web server from the internet by opening an internet browser on your computer and browsing to `http://<public-ip-address-from-previous-step>`. You see the IIS welcome screen,

Note: Port 80 is allowed inbound connections from the internet to the **asgwebservers** application security group, which the **vmweb1** virtual machine is a member of.



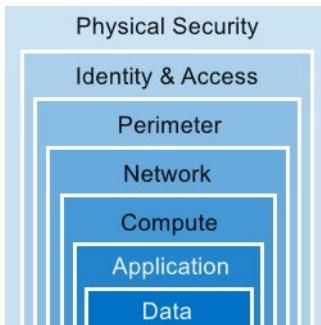
Congratulations! You have created a virtual network and subnet, and then two application security groups, one for management servers and one for web servers. You then created a Network Security group (NSG) and associated that NSG to the subnet we created earlier. You then created two inbound network security rules, to allow-rdp-all and allow-web-all traffic.

You then created two virtual machines, one to represent a management server, and one to represent a web server, and associated those virtual machines with their respective Application security groups (ASGs), and then with the network security group (NSG) containing the network security rules to control network traffic. You then tested the network security rules we have created and applied.

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.

Choosing Azure network security solutions

It's not enough to simply focus on securing the network perimeter, or on network security between services inside a network. A layered approach provides multiple levels of protection so that if an attacker gets through one layer there are further protections in place. A common security concept that is applied to computing systems is *defense in depth*, which is essentially a layered approach to providing security.



As the image illustrates, there are many layers that you need to consider. However, a broader security discussion on each layer is beyond the scope at this course. Therefore, we will primarily focus on the *Perimeter layer* and the *Networking layer*.

Perimeter layer

The network perimeter layer is about protecting organizations from network-based attacks against your resources. Identifying these attacks, alerting, and eliminating their impact is important to keep your network secure. To do this:

- Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for end users.
- Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

Networking layer

At this layer, the focus is on limiting network connectivity across all your resources to only allow what is required. Segment your resources and use network-level controls to restrict communication to only what is needed. By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack. Use NSGs to create rules about inbound and outbound communication at this layer. As best practices:

- Limit communication between resources through segmenting your network and configuring access controls.
- Deny by default.
- Restrict inbound internet access and limit outbound where appropriate.
- Implement secure connectivity to on-premises networks.

Combining services

You can also combine multiple Azure networking and security services to manage your network security and provide increased layered protection. The following are examples of combined services:

- Network security groups and Azure Firewall. Azure Firewall complements network security group functionality. Together, they provide better defense-in-depth network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall-as-a-service, which provides network and application-level protection across different subscriptions and virtual networks.

- Application Gateway WAF and Azure Firewall. *WAF* is a feature of Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities. *Azure Firewall* provides inbound protection for non-HTTP/S protocols (for example, RDP, SSH, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S. Combining both provides additional layers of protection.

Shared responsibilities

As computing environments move from customer-controlled datacenters to cloud datacenters, the responsibility for security also shifts. Security is now a concern shared by both cloud providers and customers.

Responsibility	On-premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory Infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Core Azure Identity services

Video: Core Identity Services



<https://www.youtube.com/watch?v=ZlaYK7lDaPc>

Authentication and Authorization

Two fundamental concepts that need to be understood when talking about identity and access are authentication and authorization. They underpin everything else that happens and occur sequentially in any identity and access process:

- **Authentication.** *Authentication* is the process of establishing the identity of a person or service looking to access a resource. It involves the act of challenging a party for legitimate credentials, and provides the basis for creating a security principal for identity and access control use. It establishes if they are who they say they are.
- **Authorization.** *Authorization* is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

Note: Authentication is sometimes shortened to *AuthN*, and authorization is sometimes shortened to *AuthZ*.

Azure Active Directory



Azure Active Directory (Azure AD) is a Microsoft cloud-based identity and access management service. Azure AD helps employees of an organization sign in and access resources:

- External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.
- Internal resources might include apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

Azure AD provides services such as:

- *Authentication.* This includes verifying identity to access applications and resources, and providing functionality such as self-service password reset, multi-factor authentication (MFA), a custom banned password list, and smart lockout services.
- *Single-Sign-On (SSO).* SSO enables users to remember only one ID and one password to access multiple applications. A single identity is tied to a user, simplifying the security model. As users

change roles or leave an organization, access modifications are tied to that identity, greatly reducing the effort needed to change or disable accounts.

- *Application management.* You can manage your cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as *Access panel*), and SaaS apps.
- *Business to business* (B2B) identity services. Manage your guest users and external partners while maintaining control over your own corporate data
- *Business-to-Customer* (B2C) identity services. Customize and control how users sign up, sign in, and manage their profiles when using your apps with services.
- *Device Management.* Manage how your cloud or on-premises devices access your corporate data.

Azure AD is intended for:

- *IT administrators.* Administrators can use Azure AD to control access to apps and their resources, based on your business requirements.
- *App developers.* Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that you build, such as adding Single-Sign-On functionality to an app, or allowing an app to work with a user's pre-existing credentials and other functionality.
- *Microsoft 365, Microsoft Office 365, Azure, or Microsoft Dynamics CRM Online* subscribers. These subscribers are already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant. You can immediately start to manage access to your integrated cloud apps using Azure AD.

Note: You can read more about Azure Active Directory on the [Azure Active Directory¹¹](#) webpage.

Azure Multi-Factor Authentication

Azure Multi-Factor Authentication (MFA) provides additional security for your identities by requiring two or more elements for full authentication. These elements fall into three categories:

- *Something you know* could be a password or the answer to a security question.
- *Something you possess* might be a mobile app that receives a notification, or a token-generating device.
- *Something you are* is typically some sort of biometric property, such as a fingerprint or face scan used on many mobile devices.



Using MFA increases identity security by limiting the impact of credential exposure. To fully authenticate, an attacker who has a user's password would also need to have possession of their phone or their fingerprint, for example. Authentication with only a single factor is insufficient and, without MFA, an attacker would be unable to use those credentials to authenticate. MFA should be enabled wherever possible as MFA adds enormous benefits to security.

¹¹ <https://azure.microsoft.com/en-us/services/active-directory/>

MFA comes as part of the following Azure service offerings:

- *Azure Active Directory Premium licenses.* These licenses provide full-featured use of Azure Multi-Factor Authentication Service (cloud) or Azure Multi-Factor Authentication Server (on-premises).
- *Multi-Factor Authentication for Office 365.* A subset of Azure Multi-Factor Authentication capabilities are available as a part of your Office 365 subscription.
- *Azure Active Directory global administrators.* Because global administrator accounts are highly sensitive, a subset of Azure Multi-Factor Authentication capabilities are available as a means to protect these accounts.

Note: You can read more about MFA at [How it works: Azure Multi-Factor Authentication](#) ¹².

¹² <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

Security Tools and Features

Video: Video Azure Security Center



<https://www.youtube.com/watch?v=W9JsNvm4slU>

Azure Security Center

Azure Security Center is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises. Security Center can:

- Provide security recommendations based on your configurations, resources, and networks.
- Monitor security settings across on-premises and cloud workloads, and automatically apply required security to new services as they come online.
- Continuously monitor all your services, and perform automatic security assessments to identify potential vulnerabilities before they can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines and services. You can also define a list of allowed applications to ensure that only the apps you validate are allowed to execute.
- Analyze and identify potential inbound attacks, and help to investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffic that you require.



Azure Security Center is part of the **Center for Internet Security**¹³ (CIS) recommendations.

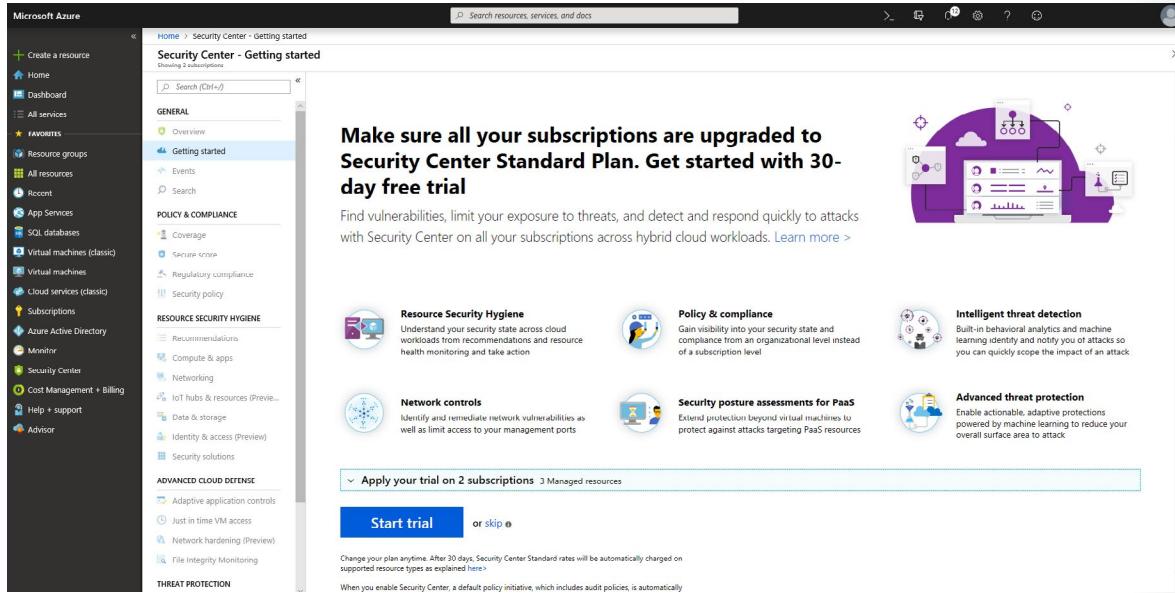
Azure Security Center Versions

Azure Security Center is available in two tiers:

- *Free*. Available as part of your Azure subscription, this tier is limited to assessments and recommendations of Azure resources only.
- *Standard*. This tier provides a full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports, and more.

¹³ <https://www.cisecurity.org/cis-benchmarks/>

To access the full suite of Azure Security Center services you will need to upgrade to a Standard tier subscription. You can access the 30-day free trial from within the Azure Security Center dashboard in the Azure Portal.



- To upgrade a subscription to the Standard tier, you must be assigned the role of *Subscription Owner*, *Subscription Contributor*, or *Security Admin*.
- After the 30-day trial period is over, Azure Security Center is priced as per details on the **Security Center pricing¹⁴** page.

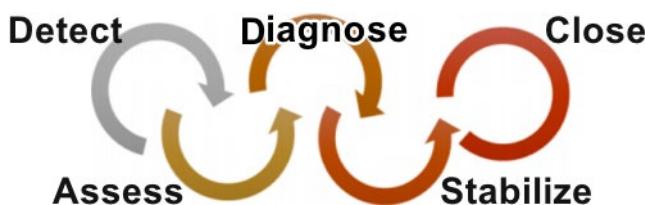
Note: You can read more about Azure Security Center at [Azure Security Center¹⁵](#).

Azure Security Center usage scenarios

You can integrate Security Center into your workflows and use it in many ways. Here are two examples.

1. Use Security Center for an incident response.

Many organizations learn how to respond to security incidents only after suffering an attack. To reduce costs and damage, it's important to have an incident response plan in place before an attack occurs. You can use Azure Security Center in different stages of an incident response.



¹⁴ <https://azure.microsoft.com/en-us/pricing/details/security-center/>

¹⁵ <https://azure.microsoft.com/en-us/services/security-center/>

You can use Security Center during the detect, assess, and diagnose stages. Here are examples of how Security Center can be useful during the three initial incident response stages:

- *Detect.* Review the first indication of an event investigation.
Example: Use the Security Center dashboard to review the initial verification that a high-priority security alert was raised.
- *Assess.* Perform the initial assessment to obtain more information about the suspicious activity.
Example: Obtain more information about the security alert.
- *Diagnose.* Conduct a technical investigation and identify containment, mitigation, and workaround strategies.
Example: Follow the remediation steps described by Security Center in that particular security alert.

2. Use Security Center recommendations to enhance security.

You can reduce the chances of a significant security event by configuring a security policy, and then implementing the recommendations provided by Azure Security Center.

A *security policy* defines the set of controls that are recommended for resources within that specified subscription or resource group. In Security Center, you define policies according to your company's security requirements.

Security Center analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations based on the controls set in the security policy. The recommendations guide you through the process of configuring the needed security controls. For example, if you have workloads that do not require the *Azure SQL Database Transparent Data Encryption* (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.

Note: You can read more about Azure Security Center at [Azure Security Center¹⁶](#). More implementation and scenario detail is also available in the [Azure Security Center planning and operations guide¹⁷](#).

Walkthrough-Implement Azure Security Center

In this walkthrough task we will create Azure resources to monitor, enable Security Center for your subscription and then from within Security Center, install Agents on a virtual machine to allow more detailed monitoring. We will then evaluate and apply a security recommendation to increase the Secure score value in Security Center.

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 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 today¹⁸](#) webpage.

¹⁶ <https://azure.microsoft.com/en-us/services/security-center/>

¹⁷ <https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide>

¹⁸ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

Steps

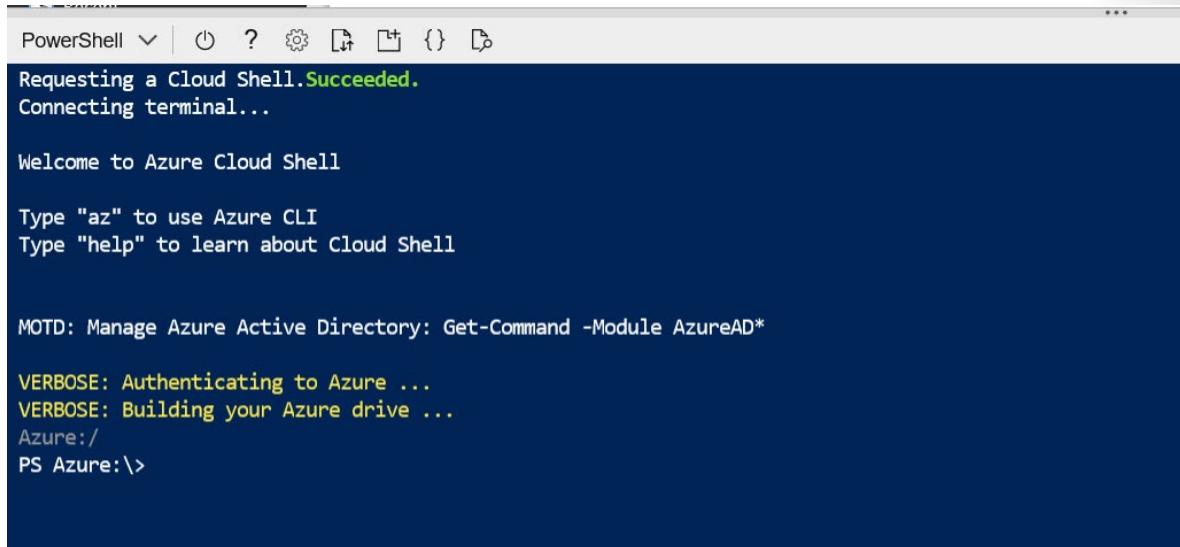
Create Azure resources to monitor

Firstly we will deploy some resources to Azure to provide us with some resources to monitor.

1. Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.



3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** or **bash** console.

```
az group create \
    --name seccentrg \
    --location westeurope
```

```
PS Azure:> az group create ` 
>>   --name seccentrgrg ` 
>>   --location westeurope 
{ 
  "id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/seccentrgrg", 
  "location": "westeurope", 
  "managedBy": null, 
  "name": "seccentrgrg", 
  "properties": { 
    "provisioningState": "Succeeded" 
  }, 
  "tags": null, 
  "type": null 
} 
Azure:/ 
PS Azure:> 
```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
az vm create ` 
  --name vmseccent1 ` 
  --resource-group seccentrgrg ` 
  --image Win2019Datacenter ` 
  --location westeurope ` 
  --admin-username azureuser ` 
  --admin-password Password0134! 
```

```
PS Azure:> az vm create ` 
>>   --name vmseccent1 ` 
>>   --resource-group seccentrgrg ` 
>>   --image Win2019Datacenter ` 
>>   --location westeurope ` 
>>   --admin-username azureuser ` 
>>   --admin-password Password0134! 
{ 
  "fqdns": "", 
  "id": "/subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourceGroups/seccentrgrg/providers/Microsoft.Compute/virtualMachines/vmseccent1", 
  "location": "westeurope", 
  "macAddress": "00-0D-3A-27-4D-9C", 
  "powerState": "VM running", 
  "privateIpAddress": "10.0.0.4", 
  "publicIpAddress": "51.136.54.9", 
  "resourceGroup": "seccentrgrg", 
  "zones": "" 
} 
Azure:/ 
PS Azure:> 
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. Do not continue to the next step until the virtual machine deployment is complete. You can close the Azure Cloud Shell once it is complete.

Enable Security Center for your subscription

We will now enable Security Center for our subscription

1. Select **All services** in the upper, left corner of the Azure portal, then select **Security**, and then select **Security Center**.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like Home, Dashboard, and All services, which is highlighted with a red box. The main content area is titled 'All services' and contains a search bar. A sidebar on the right lists various service categories under 'SECURITY (8)'. The 'Security Center' option is highlighted with a red box. Below it, other security-related services listed include Azure Information Protection, Application security groups, Storage, Web, Mobile, Containers, Databases, Analytics, AI + machine learning, Internet of things, Integration, Identity, DevOps, Migrate, Management + governance, Intune, and Other.

2. In the **Security Center** pane click on the **GENERAL > Getting Started** pane, expand the section **Apply your trial on X subscriptions**, and ensure you have the subscription that you wish to enable security center for checked, i.e. your free trial subscription, and any other subscription you do not wish to enable security center for, unchecked.

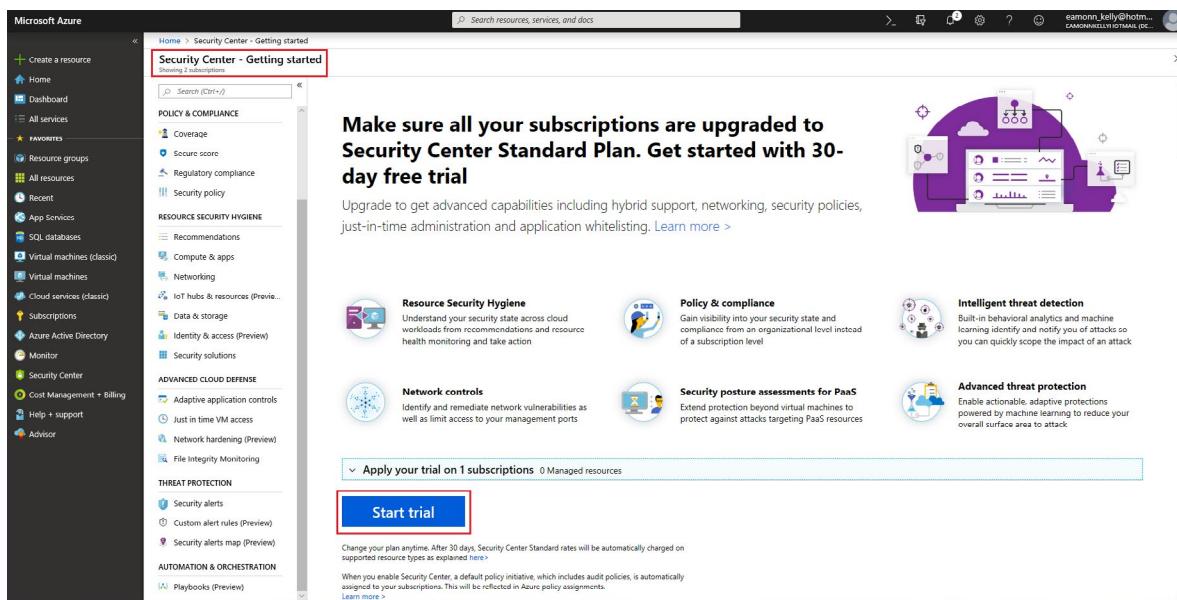
The screenshot shows the 'General > Getting Started' pane of the Security Center. It features several sections: 'Resource Security Hygiene', 'Policy & compliance', 'Intelligent threat detection', 'Network controls', 'Security posture assessments for PaaS', and 'Advanced threat protection'. At the bottom, there is a section titled 'Apply your trial on 1 subscriptions' which shows '3 Managed resources'. A table below lists the subscriptions:

NAME	COVERAGE	UNPROTECTED RESOURCES	UNPROTECTED RESOURCE TYPES	
<input type="checkbox"/> Pay-As-You-Go	Free (30 days left in trial)	0	All	Edit plan >
<input checked="" type="checkbox"/> Visual Studio Ultimate with MSDN	Free (30 days left in trial)	3	All	Edit plan >

Note: the screenshot above selects a *Visual Studio Ultimate with MSDN* subscription, but the subscription you wish to enable Security Center for may be different i.e. *Azure-Free-Trial*, *Pay-As-You-Go*, or another type subscription

MCT USE ONLY. STUDENT USE PROHIBITED

3. Still in the **Security Center - Getting Started** pane, click the **Start trial** button.



4. Security Center is now enabled on your subscription. Note the button text change to install agents onto your virtual machine. We have not yet installed any agents on our virtual machine and do not do so yet, we will install agents shortly.

5. Go to **General > Overview** and note the various sections and dashboard detail that is available for areas such as the below.

- **Policy & compliance**

- **secure score:** A numerical guide to indicate how secure your resources are. Note the current score value as we will perform an action to increase the score. The screenshot lists a value of **220 out of 280**. Your value may be different depending on your environment.
- **Regulatory compliance:** ISO, Azure CIS, PCI DDS etc
- **Policy Management and governance:** Ability to integrate policies

- **Resource security Hygiene**

- **Recommendations:** security recommendations to consider implementing
- **Resource health monitoring:** resource monitoring date
- **Top recommendations by secure score impact:**

- **Threat Detection**

- **Security alerts by severity:** security alert data prioritized.
- **security alerts over time:** cumulative security alert data to provide trend view.

Take a few moments to click into some of the areas that interest you, some areas will not display detailed data as you drill through them, as they are only available on *Standard* tier, and we have only enabled the trial version. Many areas however, do have data available in the free tier, and without having any agents installed.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Azure Security Center - Overview page. On the left, there's a navigation menu with sections like General, Policy & Compliance, Resource Security Hygiene, Advanced Cloud Defense, and Threat Protection. The main area is divided into three main sections: Policy & compliance, Resource security hygiene, and Threat protection.

- Policy & compliance:** Shows a secure score of 220 out of 280, regulatory compliance status for SOC TSP, PCI DSS 3.2, and ISO 27001, and subscription coverage (2 total, 1 fully covered, 1 partially covered, 0 not covered).
- Resource security hygiene:** Shows recommendations (3 total, 2 high severity, 0 medium, 1 low), resource health monitoring for compute & apps (0 unhealthy resources), data & storage (1 healthy resource), networking (1 healthy resource), and identity & access (1 healthy resource).
- Threat protection:** Shows security alerts by severity (High, Medium, Low) and over time (No security alerts).

On the right, there are manage and govern your security posture options and a section about top recommendations by secure score impact.

Install Agent on virtual machine

- In Security Center go to **RESOURCE SECURITY HYGIENE > Compute & apps**, note the recommendations listed, and the tabs available i.e. **Overview, VMs and Computers, VM Scale Sets, Cloud Services, App Services, Containers and Compute resources**. Some will be greyed out as we have no resources relevant to that section and some data will take several hours to populate when initially enabled. Select the **Overview** tab and click on **Install monitoring agent on your virtual machines**

The screenshot shows the Azure Security Center - Compute & apps page. The left sidebar has sections like General, Policy & Compliance, Resource Security Hygiene, and Advanced Cloud Defense. The main area shows a list of recommendations:

RECOMMENDATION	SECURE SCORE IMP...	FAILED RESOURCES	SEVERITY
Install a vulnerability assessment solution on your virtual machines	+30	1 of 1 virtual machines	High
Install monitoring agent on your virtual machines	+25	1 of 2 virtual machines	Medium
Install endpoint protection solution on virtual machines	+15	2 of 2 virtual machines	Low
Resolve monitoring agent health issues on your machines	+15	1 of 2 virtual machines	Low
Apply disk encryption on your virtual machines	+10	2 of 2 virtual machines	Low

The "Compute & apps" tab is highlighted in the top navigation bar.

Note: If you have already clicked **Install agents** for your subscription, this recommendation will not be present in your list of recommendations, even if you have a new virtual machine as it is enabled at subscription level. If the install agent is already enabled, you can proceed to the next task.

2. On the subsequent **Getting started** pane, select the subscription that you have selected for the Security Center trial period, and then click **Install agents**

Getting started

Security Center detected virtual machines without the data collection agent installed!

Protect your virtual machines now by installing the Security Center data collection agent on each VM. To receive security alerts and recommendations, the agent must be installed.

[Learn more >](#)



Install agents automatically

The Microsoft Monitoring Agent will be automatically installed on all the virtual machines in selected subscription.

^ Select subscriptions on which agents will be installed 1 Managed resources

NAME	UNPROTECT...
Pay-As-You-Go	0
Visual Studio Ultimate with MSDN	1

Install agents [Remind me later](#)



Install agents manually

If you already have another workspace you may want to connect virtual machines to it and install agents on your own from the Security Policy blade



Continue without installing agents

Many important security features won't work if you don't install agents.

[Continue without installing agents](#)

3. The agent may take 2 to 3 minutes to install, but continue to refresh the **Compute & apps** pane until the **Install monitoring agent on your virtual machines** option is no longer present.

Security Center - Compute & apps

Showing 2 subscriptions

Overview **VMs and Computers** **VM scale sets** **Cloud services** **App services** **Containers (Preview)** **Compute resources**

Search recommendations

RECOMMENDATION	SECURE SCORE IMPROVEMENT	FAILED RESOURCES	SEVERITY
Resolve monitoring agent health issues on your machines	+30	1 of 1 virtual machines	High
Install endpoint protection solution on virtual machines	+15	1 of 1 virtual machines	Medium
Apply disk encryption on your virtual machines	+10	1 of 1 virtual machines	Medium

Evaluate and Apply a Security recommendation to increase the Secure score value

- In the **RESOURCE SECURITY HYGIENE > Compute & apps** blade, **Overview** tab, note the recommendations listed,
 - Resolve monitoring agent health issues on your machines**
 - Install endpoint protection solution on virtual machines**
 - Apply disk encryption on your virtual machines**

RECOMMENDATION	SECURE SCORE IMP...	FAILED RESOURCES	SEVERITY
Resolve monitoring agent health issues on your machines	+30	1 of 1 virtual machines	High
Install endpoint protection solution on virtual machines	+15	1 of 1 virtual machines	Critical
Apply disk encryption on your virtual machines	+10	1 of 1 virtual machines	Critical

2. Still in the **Compute & apps > Overview** section, select the **Apply disk encryption on your virtual machines** recommendation

3. In the subsequent **Apply disk encryption on your virtual machines** pane, note the detail that is presented, i.e. **Description** of the issue, **General information**, **Threats**, **Remediation steps**. In the **Remediation steps** section click on the link **Encryption instructions**¹⁹. You are brought to an Azure docs page providing an overview of what disk encryption involves and detailing how to encrypt your disks. If you wish to enable disk encryption, you can follow the guidelines and steps outlined here.

¹⁹ <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>

Apply disk encryption on your virtual machines

Azure Disk Encryption (ADE) leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide OS and data disk encryption to help protect and safeguard your data and help meet your organizational security and compliance commitments in customer Azure key vault. When your compliance and security requirement requires you to encrypt the data end to end using your encryption keys, including encryption of the ephemeral (locally attached temporary) disk, use Azure disk encryption. Alternatively, by default, Managed Disks are encrypted at rest by default using Azure Storage Service Encryption where the encryption keys are Microsoft managed keys in Azure. If this meets your compliance and security requirements, you can leverage the default Managed disk encryption to meet your requirements.

General Information

Recommendation score	i	0/10
Recommendation impact	+10	
User impact	Low	
Implementation cost	Low	

Threats

- Data exfiltration
- Data spillage
- Account breach

Remediation steps

To enable disk encryption on your virtual machines, follow [Encryption instructions](#).

Unhealthy resources	Healthy resources
1	0

[Unhealthy resources \(1\)](#) [Healthy resources \(0\)](#) [Unscanned resources \(0\)](#)

Search virtual machines

NAME

 [vmseccent1](#)

4. Return to the **Compute & apps > Overview** section, select the **Resolve monitoring agent health issues on your machines** recommendation. Under the **Unhealthy resources** section at the bottom of the pane, under **Monitoring State**, note the message i.e. **Agent not responsive or missing ID**, then click on the link **following instructions**.

Note: You may not have this message present depending on your subscription and environment, and as such you will not have the same link as outlined here present. You may have a message such as **Pending automatic agent installation**, or some other message. Regardless of the message present, you can proceed to the next step.

Resolve monitoring agent health issues on your machines

Description
Security Center uses the Microsoft Monitoring Agent (MMA) to collect security events from your Azure virtual machines. To make sure your virtual machines are successfully monitored, you need to enable data collection in Security Center and make sure the MMA agent is both installed on the virtual machines and properly collects security events to the configured workspace. In some cases, the MMA agent may fail to properly report security events, due to multiple reasons. In these cases, coverage may be partial - security events won't be properly processed, and in turn threat detection for the affected VMs may fail to function.

General Information
Recommendation score: 0/30
Recommendation impact: +30
User impact: High
Implementation cost: Moderate

Threats

- Missing coverage

Remediation steps
To resolve monitoring agent health issues and see the different resolution for each issue, please see the [following instructions](#).

Unhealthy resources: 1 Healthy resources: 0

Unhealthy resources (1) [Healthy resources \(0\)](#) [Unscanned resources \(0\)](#)

Search virtual machines

NAME	MONITORING STATE
vmseccent1	Agent not responsive or missing ID

- On the subsequent **Azure Security Center Troubleshooting Guide**²⁰ page, under the **Monitoring agent health issues** section locate the error message and note the remediation steps listed.

Note: Again, you can just view the list of potential messages and possible solution detail if you do not have the same message as included in the earlier screenshot. The detail here is provided just for informational purposes, and you can proceed to the next step.

Agent not responsive or missing ID	Security Center is unable to retrieve security data scanned from the VM, even though the agent is installed.	The agent is not reporting any data, including heartbeat. The agent might be damaged or something is blocking traffic. Or, the agent is reporting data but is missing an Azure resource ID so it's impossible to match the data to the Azure VM. To troubleshoot Linux, see Troubleshooting Guide for Log Analytics Agent for Linux . To troubleshoot Windows, see Troubleshooting Windows Virtual Machines .
------------------------------------	--	---

- Return to the **Compute & apps > Overview** section, select the **Install endpoint protection solution on virtual machines** recommendation.
- On the subsequent **Endpoint Protection not installed on Azure VMs** pane, ensure the virtual machine you created earlier is checked i.e. **vmseccent1**, and click on the **Install on 1 VMs** option.

²⁰ <https://docs.microsoft.com/en-us/azure/security-center/security-center-troubleshooting-guide#monitoring-agent-health-issues->

The screenshot shows a blade titled 'Endpoint Protection not installed on Azure VMs'. At the top, there is a red box around the 'Install on 1 VMs' button. Below it, a table lists three virtual machines:

VIRTUAL MACHINE	STATE	SEVERITY	...
vmseccent1	Open	High	
VMWeb1	Resolved	High	
vmmgmt1	Resolved	High	

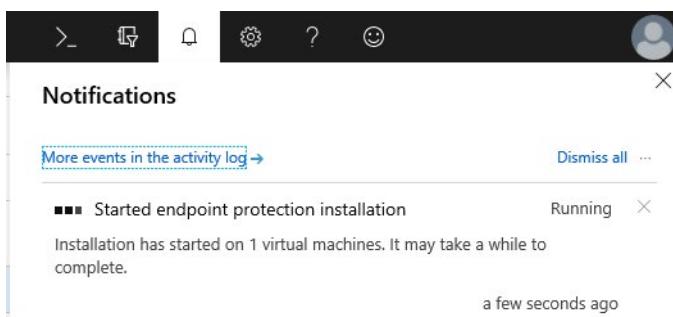
8. In the subsequent **Select Endpoint Protection** pane, select **Microsoft Antimalware**

The screenshot shows a 'Select Endpoint Protection' pane. A red box highlights the 'Microsoft Antimalware' option by Microsoft Corp.

9. In the **Microsoft Antimalware** blade click **Create** and in the subsequent **Install Microsoft Antimalware** blade leave all the default values as they are, and click **OK**.

The screenshot shows two windows side-by-side. On the left is the 'Microsoft Antimalware' configuration blade, which contains instructions for enabling antimalware with default or custom configurations, and details about antimalware event collection. It also includes sections for Legal Terms and useful links to documentation and PowerShell cmdlets. At the bottom left is a 'Create' button. On the right is the 'Install Microsoft Antimal...' dialog box, which contains fields for excluded files, processes, and protection settings, along with options for scheduled scans, scan type, day, and time. At the bottom right is an 'OK' button.

10. Microsoft Antimalware will start installation.



Note: It could take between 10 to 20 minutes to complete the installation, depending on the environment. If it is taking a prolonged period of time, you can continue with the next topic in the lesson and return to your Azure environment when it has completed.

11. After the installation is complete return to the Return to the **Compute & apps > Overview** section and note the recommendation to **Install endpoint protection solution on virtual machines** is no longer present. You may need to refresh the console display if it is still present.

The screenshot shows the Azure Security Center interface for Compute & apps. On the left, there's a navigation menu with sections like Overview, Getting started, Events, Search, Policy & Compliance, Resource security hygiene, Recommendations, Compute & apps (which is selected and highlighted with a red box), and Networking. The main area has tabs for Overview, VMs and Computers, VM scale sets, Cloud services, App services, Containers (Preview), and Compute resources. A red box highlights the 'Overview' tab under the Recommendations section. Below it, there's a table with two rows of recommendations:

RECOMMENDATION	SECURE SCORE IMP...	FAILED RESOURCES	SEVERITY
Resolve monitoring agent health issues on your machines	+30	1 of 1 virtual machines	██████████
Apply disk encryption on your virtual machines	+10	1 of 1 virtual machines	██████████

12. Go to the **GENERAL > Overview** blade and note the **Secure score** value. Since the completion of the security recommendation, the **Secure score** value has increased. In the screenshot it has gone up to a value of **285 out of 385**, again your value may be different depending on your environment.

The screenshot shows the Azure Security Center - Overview blade. The left sidebar includes sections for General (selected and highlighted with a red box), Overview, Getting started, Events, Search, Policy & compliance, Resource security hygiene, Threat protection, Advanced cloud defense, and Threat protection. The main content area is divided into several sections: Policy & compliance, Resource security hygiene, Threat protection, and Top recommendations by secure score impact. The Policy & compliance section features a prominent 'Secure score' card with a blue shield icon, showing '285 OF 385' in large numbers, with a note below stating 'Secure score impact changed. Learn more'. The Resource security hygiene section includes a pie chart showing 5 total resources (3 healthy, 1 medium severity, 1 low severity) and lists for Compute & apps, Data & storage, Networking, and Identity & access. The Threat protection section shows security alerts by severity (High, Medium, Low) and over time. The Top recommendations by secure score impact section lists three items: 'Enable MFA for accounts with owner permission...', 'Resolve monitoring agent health issues on your...', and 'Apply disk encryption on your virtual machines...'. The overall layout is clean with a light grey background and blue header elements.

Congratulations! You have created Azure resources to monitor, enabled Security Center for your subscription and from within Security Center, installed an agent on a virtual machine to allow more detailed monitoring. You then evaluated and applied security recommendations to increase the Secure score value in Security center.

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.

Video: Security Tools and Services



<https://www.youtube.com/watch?v=VS6FteQnzak>

Key Vault

Azure Key Vault is a centralized cloud service for storing your applications' secrets. Key Vault helps you control your applications' secrets by keeping them in a single, central location and by providing secure access, permissions control, and access logging capabilities.



Usage Scenarios

- *Secrets management.* You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, *Application Programming Interface* (API) keys, and other secrets.
- *Key management.* You also can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
- *Certificate management.* Key Vault lets you provision, manage, and deploy your public and private *Secure Sockets Layer/ Transport Layer Security* (SSL/ TLS) certificates for your Azure, and internally connected, resources more easily.
- *Store secrets backed by hardware security modules* (HSMs). The secrets and keys can be protected either by software, or by FIPS 140-2 Level 2 validated HSMs.

Key Vault benefits

The benefits of using Key Vault include:

- *Centralized application secrets.* Centralizing storage for application secrets allows you to control their distribution, and reduces the chances that secrets may be accidentally leaked.
- *Securely stored secrets and keys.* Azure uses industry-standard algorithms, key lengths, and HSMs, and access requires proper authentication and authorization.
- *Monitor access and use.* Using Key Vault, you can monitor and control access to company secrets.
- *Simplified administration of application secrets.* Key Vault makes it easier to enroll and renew certificates from public Certificate Authorities (CAs). You can also scale up and replicate content within regions, and use standard certificate management tools.

- *Integrate with other Azure services.* You can integrate Key Vault with storage accounts, container registries, event hubs and many more Azure services.

Note: You can read more about Key Vault on the [Key Vault](#)²¹ webpage.

Walkthrough-Create Password secret with Azure Key Vault

In this walkthrough task we will create an Azure Key vault and then create a password secret within that key vault, providing a securely stored, centrally managed password for use with applications.

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

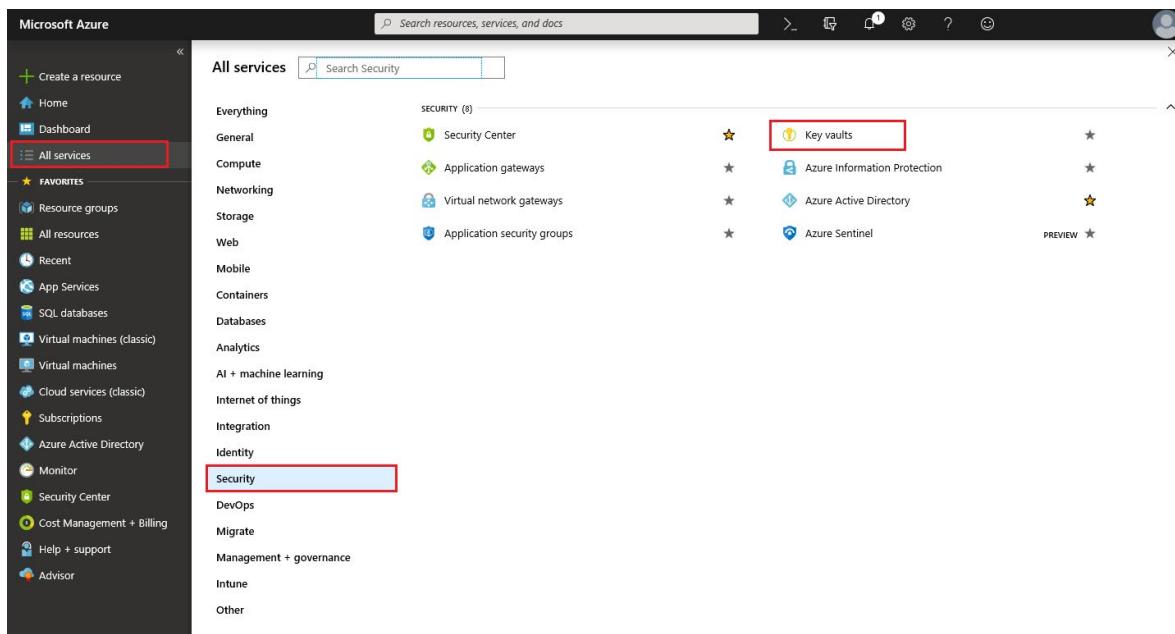
- You require an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today](#)²² webpage.

Steps

Create a vault in Azure Key Vault

Firstly we will create a vault

1. Sign into the Azure Portal and go to **All services > Security** and then select **Key vaults**.



2. In the **Key vaults** pane click on **Create key vault**.

²¹ <https://azure.microsoft.com/en-us/services/key-vault/>

²² https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

The screenshot shows the 'Key vaults' blade in the Azure portal. At the top, there's a breadcrumb navigation: Home > Key vaults. Below it, a red box highlights the 'Key vaults' tab. On the left, there are buttons for 'Add', 'Edit columns', 'Refresh', and 'Assign tags'. A message says 'Subscriptions: All 2 selected - Don't see a subscription? Open Directory + Subscription settings'. Below that are filter options: 'Filter by name...', 'All subscriptions', 'All resource gro...', 'All locations', 'All tags', and 'No grouping'. It shows '0 items' and a table header with columns: NAME, TYPE, RESOURCE GROUP, LOCATION, and SUBSCRIPTION. A large key icon is centered with the text 'No key vaults to display' and 'Try changing your filters if you don't see what you're looking for.' A blue button labeled 'Create key vault' is highlighted with a red box.

3. In the **Create key vault** blade, enter the details as below and click **Create**

- **Name:** a name for your vault i.e. **akvtest1**
- **Subscription:** < your subscription >
- **Resource Group:** select **Create new** and enter a new resource group name i.e. **akvrg**
- **Location:** < a data center location near you i.e. **Central US** >
- **Pricing Tier:** Standard
- **Access policies:** < accept default value i.e. **1 principal selected** >
- **Virtual Network Access:** < accept default value i.e. **all networks can access** >

Create key vault

* Name ✓

* Subscription

* Resource Group [Create new](#)

* Location

Pricing tier >

Access policies >

Virtual Network Access >

Create [Automation options](#)

4. Go to the newly created Key vault and verify it is present. You can take a moment to browse through some of the options available within it, primarily under **Settings** and then options concerning **Keys**, **Secrets**, **Certificates**, **Access Policies**, **Firewalls** and **virtual networks**.

akvtest1 Key vault

Search (Ctrl+)

Overview

Resource group (change) : akvrg
 Location : Central US
 Subscription (change) : Visual Studio Ultimate with MSDN
 Subscription ID : 6e9a285a-37ea-40e6-b2fc-28539051852e
 DNS Name : https://akvtest1.vault.azure.net/
 Sku (Pricing tier) : Standard
 Directory ID : 0c0ded62-0a9c-498d-b068-10e155c23935
 Directory Name : emannkelly@hotmail (Default Directory)

Monitoring

Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 days Click for additional metrics.

Total requests

Average latency

12 PM 6 PM May 22 6 AM

vault akvtest1 6

Support + troubleshooting

Resource health New support request

5. Take note of two values in the key vault

- **Vault Name:** In the example it is **akvtest1**
- **DNS name** (also sometimes referred to as the **Vault URI**): In this example it is <https://akvtest1.vault.azure.net/>. Applications that use your vault through its REST API must use this URI.

Note: Your Azure account is the only one authorized to perform operations on this new vault. You can modify this if you wish in the **Settings > Access policies** section

Add a secret to the Key Vault

We will now add a password that could be used by an application.

1. On the Key Vault properties pages select **Secrets**, then select **Generate/Import**.

NAME	TYPE	STATUS	EXPIRATION DATE
There are no secrets available.			

2. On the **Create a secret** blade enter the below values, leave the other values at their defaults and then click **Create**.

- **Upload options:** Manual
- **Name:** ExamplePassword
- **Value:** hVFkk965BuUv96!

MCT USE ONLY. STUDENT USE PROHIBITED

Create a secret

Upload options
Manual

* Name ⓘ ExamplePassword ✓

* Value
*****| ✓

Content type (optional)

Set activation date? ⓘ

Set expiration date? ⓘ

Enabled? Yes No

Create

- Once the secret has been successfully created, on the **Secrets** pane, click on the **ExamplePassword**, and note it has a status of **Enabled**

ExamplePassword		Versions	
		<input type="button"/> New Version <input type="button"/> Refresh <input type="button"/> Delete <input type="button"/> Download Backup	
VERSION	STATUS	ACTIVATION DATE	EXPIRATION DATE
CURRENT VERSION			
abbd62f1b76a49bb9d5670ada93bbc96	✓ Enabled		

- Double click on the password and in the password pane, note the presence of the **Secret Identifier**. This is the url value that you can now use with applications. It provides a centrally managed and securely stored password for use with applications.

Properties

Created 5/22/2019 10:37:46 AM
Updated 5/22/2019 10:37:46 AM

Secret Identifier

https://akvtest1.vault.azure.net/secrets/ExamplePassw...

Settings

Set activation date?

Set expiration date?

Enabled?

Tags >
0 tags

Secret

Content type (optional)

Show Secret Value

5. In the same pane click the button **Show Secret Value**, to display the password you specified earlier.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Azure Key Vault 'Secrets' blade. At the top, there's a lock icon and the secret identifier 'abbd62f1b76a49bb9d5670ada93bbc96'. Below that are 'Save' and 'Discard' buttons. The main area has sections for 'Properties' (Created: 5/22/2019 10:37:46 AM, Updated: 5/22/2019 10:37:46 AM), 'Secret Identifier' (a URL), 'Settings' (activation and expiration date checkboxes, 'Enabled?' set to 'Yes'), 'Tags' (0 tags), and 'Secret' (Content type optional field, a large text input field containing 'hVFkk965BuUv96!', and a 'Hide Secret Value' button). A red box highlights the 'Secret' section.

Note: It is also possible to set time limitations on when a password is available for use, using the activation and expiration date settings.

Congratulations! You have created an Azure Key vault and then created a password secret in that key vault, providing a securely stored, centrally managed password for use with applications.

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.

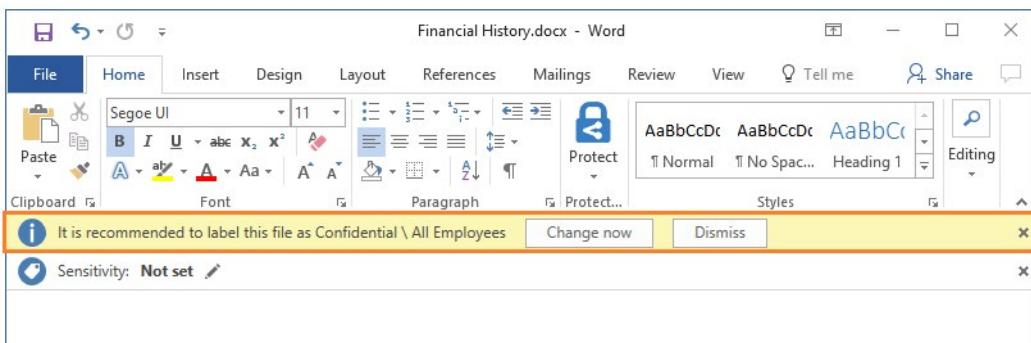
Azure Information Protection (AIP)

Microsoft Azure Information Protection (MSIP) is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels. Labels can be applied automatically (by administrators who define rules and conditions), manually (by users), or with a combination of both (where users are guided by recommendations).



Usage scenario

The following screen capture is an example of MSIP in action on a user's computer. In this example, the administrator has configured a label with rules that detect sensitive data. When a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labeling the file as *Confidential/ All Employees*, which is a label that the administrator has configured. This label classifies the document and protects it.



After your content is classified (and optionally protected), you can then track and control how the content is used. For example, you can analyze data flows to gain insight into your business; detect risky behaviors and take corrective measures; track access to documents; and prevent data leakage or misuse.

Note: You can purchase MSIP either as a standalone solution, or through one of the following Microsoft licensing suites:

Enterprise Mobility + Security, or Microsoft 365 Enterprise. Purchasing details are available on the [Azure Information Protection pricing²³](#) webpage.

Note: You can read more about MSIP on the [What is Azure Information Protection?²⁴](#) webpage.

Azure Advanced Threat Protection (ATP)

Azure Advanced Threat Protection (Azure ATP) is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

Azure ATP components

Azure ATP consists of the following components:

- *Azure ATP portal.* Azure ATP has its own portal, through which you can monitor and respond to suspicious activity. The Azure ATP portal allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors. You can also use the portal to monitor, manage, and investigate threats in your network environment. You can sign in to the Azure ATP portal at <https://portal.atp.azure.com²⁵>. You must sign in with a user account that is assigned to an Azure AD security group which has access to the Azure ATP portal.

²³ <https://azure.microsoft.com/en-us/pricing/details/information-protection/>

²⁴ <https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection/>

²⁵ <https://portal.atp.azure.com>

- *Azure ATP sensor.* Azure ATP sensors are installed directly on your domain controllers. The sensor monitors domain controller traffic without requiring a dedicated server, or configuring port mirroring.
- *Azure ATP cloud service.* Azure ATP cloud service runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia. Azure ATP cloud service is connected to Microsoft's intelligent security graph.

The screenshot shows the Azure Advanced Threat Protection Timeline interface. It displays a list of threat events with their times and descriptions:

- 4:04 PM Today: Honeypot activity (Bob Minion) - Logged in to 2 computers via Contoso-DC, Authenticated from 2 computers using Kerberos when accessing 3 resources against Contoso-DC, Authenticated from ITARGOET-T4705 using NTLM against corporate resources via Contoso-DC.
- 3:23 PM Jan 22, 2018: Remote execution attempt detected (ALICE-DESKTOP) - Attempted remote execution of one or more WMI methods by AdminUser.
- 3:06 PM Jan 22, 2018: Suspicious service creation (AdminUser) - AdminUser created 10 services in order to execute potentially malicious commands on Contoso-DC.
- 3:03 PM Jan 22, 2018: Brute force attack using LDAP simple bind - 200 password guess attempts were made on 2 accounts from ALICE-DESKTOP, 2 account passwords were successfully guessed.
- 2:59 PM Jan 22, 2018: Reconnaissance using account enumeration - Suspicious account enumeration activity using Kerberos protocol, originating from ALICE-DESKTOP, was detected. The attacker performed a total of 101 guess attempts for account names, 2 guess attempts matched existing account names in Active Directory.
- 12:38 PM Jan 21, 2018: Malicious replication of directory services (Alice Liddell) - Malicious replication requests were attempted by Alice Liddel, from ALICE-DESKTOP against Contoso-DC.
- 11:59 AM Jan 21, 2018: Reconnaissance using DNS - Suspicious DNS activity was observed, originating from ALICE-DESKTOP (which is not a DNS server) against Contoso-DC.

Purchasing

Azure ATP is available as part of the Enterprise Mobility + Security 5 suite (EMS E5), and as a standalone license. You can acquire a license directly from the **Enterprise Mobility + Security Pricing Options page²⁶**, or through the Cloud Solution Provider (CSP) licensing model. It is not available to purchase via the Azure portal.

Note: You can read more about Azure Advanced Threat Protection on the [Azure Advanced Threat Protection²⁷](#) webpage.

²⁶ <https://www.microsoft.com/en-ie/cloud-platform/enterprise-mobility-security-pricing>

²⁷ <https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/>

Azure Governance methodologies

Video: Governance methodologies



<https://www.youtube.com/watch?v=auNrKaQ6WWI>

Azure Policy

Azure Policy is a service in Azure that you use to create, assign, and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements (SLAs).



Azure Policy does this by using policies and initiatives. It runs evaluations of your resources and scans for those not compliant with the policies you have created. For example, you can have a policy to allow only a certain stock keeping unit (SKU) size of virtual machines (VMs) in your environment. Once you implement this policy, it will evaluate resources when you create new ones or update existing ones. It will also evaluate your existing resources.

Azure Policy comes with a number of built-in policy and initiative definitions that you can use, under categories such as Storage, Networking , Compute, Security Center, and Monitoring.

Azure Policy can also integrate with Azure DevOps, by applying any continuous integration and delivery pipeline policies that apply to the pre-deployment and post-deployment of your applications.

Azure Policy also has the ability to automatically remediate resources and configurations that are deemed non-compliant, thus ensuring the integrity of the state of the resources.

Note: You can read more about Azure Policy on the [Azure Policy²⁸](https://azure.microsoft.com/en-us/services/azure-policy/) webpage.

Policies

The journey of creating and implementing a policy in Azure Policy begins with creating a policy definition. Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met.

The process of applying a policy to your resources consist of the following steps:

1. Create a policy definition.

²⁸ <https://azure.microsoft.com/en-us/services/azure-policy/>

2. Assign a definition to a scope of resources.
3. View policy evaluation results.

Policy definition

A *policy definition* expresses what to evaluate and what action to take. For example, you could prevent VMs from being deployed if they are exposed to a public IP address. You also could prevent a particular hard disk from being used when deploying VMs to control costs.

The following list contains example policy definitions:

- *Allowed Storage Account SKUs*. This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
- *Allowed Resource Type*. This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
- *Allowed Locations*. This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
- *Allowed Virtual Machine SKUs*. This policy enables you to specify a set of VM SKUs that your organization can deploy.

A List of sample policies is available on the [Azure Policy Samples²⁹](#) page.

Policy assignment

To implement these policy definitions, whether custom or built-in, you will need to assign them. A *policy assignment* is a policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to a resource group. Policy assignments are inherited by all child resources. This means that if a policy is applied to a resource group, it is applied to all the resources within that resource group. However, you can exclude a subscope from the policy assignment.

Note: You can read more about Azure Policy on the [Azure Policy³⁰](#) webpage.

Initiatives

Initiatives work alongside policies in Azure Policy. An *initiative definition* is a set of policy definitions to help track your compliance state for a larger goal.

Even if you have a single policy, we recommend using initiatives if you anticipate increasing the number of policies over time.

Like a policy assignment, an *initiative assignment* is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.

Initiatives can be assigned just as policies can.

²⁹ <https://docs.microsoft.com/en-us/azure/governance/policy/samples/>

³⁰ <https://azure.microsoft.com/en-us/services/azure-policy/>

Initiative definitions

Initiative definitions simplify the process of managing and assigning policy definitions by grouping a set of policies as one single item. For example, you could create an initiative named *Enable Monitoring in Azure Security Center*, with a goal to monitor all the available security recommendations in your Azure Security Center.

Under this initiative, you would have the following policy definitions:

- *Monitor unencrypted SQL Database in Security Center* – For monitoring unencrypted SQL databases and servers.
- *Monitor OS vulnerabilities in Security Center* – For monitoring servers that do not satisfy the configured baseline.
- *Monitor missing Endpoint Protection in Security Center* – For monitoring servers without an installed endpoint protection agent.

Initiative assignments

Like a policy assignment, an *initiative assignment* is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope. This scope could also range from a management group to a resource group.

Walkthrough-Create a policy assignment with Azure Policy

In this walkthrough task we will locate an Azure Policy to restrict deployment of Azure resources to a particular datacenter, and then assign that allowed location policy to a subscription. We will then verify that creating an Azure resource, such as a virtual machine, outside of the allowed location is blocked. We will finally remove the allowed location policy assignment, to allow us deploy resources again to any datacenter location using that same subscription.

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 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 today³¹](#) webpage.

Steps

Create a Policy assignment

1. Launch the Azure Policy service in the Azure portal by clicking **All services** then, **Everything**, then type **Policy** in the search box and select **Policy**

³¹ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

All services X

Policy

Service endpoint policies
Keywords: Service endpoint policy PREVIEW ★

Application security groups
Keywords: Policy ★

General

Compute

Networking

Storage

Web

Mobile

Containers

Databases

Analytics

AI + machine learning

Internet of things

Integration

Note: Azure Policy is also accessible under the **All services > Management + governance** section in the portal

2. Go to **Authoring > Definitions** and take a moment to have a quick browse through the list of built-in policy definitions that are available for you to use.

NAME	DEFINITION LOCATION	POLICIES	TYPE	DEFINITIO...	CATEGORY
Audit Windows VMs in which the Ad...		2	Built-in	Initiative	Guest Configura...
Audit Windows VMs in which the Ad...		2	Built-in	Initiative	Guest Configura...
[Preview]: Enable Monitoring in Azure...		76	Built-in	Initiative	Security Center
Audit Windows VMs that do not have...		2	Built-in	Initiative	Guest Configura...
[Preview]: Audit VMs with insecure pa...		18	Built-in	Initiative	Guest Configura...
Audit Windows VMs that are not set t...		2	Built-in	Initiative	Guest Configura...
[Preview]: Enable Azure Monitor for V...		6	Built-in	Initiative	Monitoring
Audit Windows VMs that are not joine...		2	Built-in	Initiative	Guest Configura...
[Preview]: Enable Azure Monitor for V...		6	Built-in	Initiative	Monitoring
[Preview]: Audit ISO 27001:2013 cont...		61	Built-in	Initiative	Regulatory Com...
Audit Windows web servers that are n...		2	Built-in	Initiative	Guest Configura...
[Preview]: Enable Data Protection Suite		1	Built-in	Initiative	Security Center
Audit Windows Server VMs on which...		2	Built-in	Initiative	Guest Configura...

3. Select **Assignments** on the left side of the **Policy** page. An assignment is a policy that has been assigned to take place within a specific scope.

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Azure Policy - Assignments page. On the left, there's a sidebar with links like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring (with 'Assignments' highlighted), Definitions, Blueprints, and Resources. The main area displays statistics: Total Assignments (3), Initiative Assignments (3), and Policy Assignments (0). Below these are three rows of assignment details:

NAME	SCOPE	TYPE	POLICIES
ASC DataProtection (subscription: 6e9a285a...)	Visual Studio Ultimate with M...	Initiative	1
ASC Default (subscription: 6e9a285a-37ea-4...)	Visual Studio Ultimate with M...	Initiative	76
ASC Default (subscription: 974e6e39-73eb-4...)	Pay-As-You-Go	Initiative	76

4. Select **Assign Policy** from the top of the **Policy - Assignments** page and on the subsequent **Assign Policy** page, select the Scope selector by clicking the ellipsis and setting the following values, then click **Select** at the bottom of the **Scope** page
 - **Subscription:** < choose your own subscription >
 - **Resource Group:** < accept the default value i.e. leave blank >

The screenshot shows the 'Scope' dialog box. It contains two dropdown menus: 'Subscription' (set to 'Visual Studio Ultimate with MSDN') and 'Resource Group' (set to 'Optional choose a Resource Group'). At the bottom are three buttons: 'Select' (highlighted with a red box), 'Cancel', and 'Clear All Selections'.

Note: A scope determines what resources or grouping of resources the policy assignment gets enforced on. In our case we could assign this policy to a specific resource group, however we will assign the policy at subscription level. Also, be aware that resources can be excluded based on the Scope. Exclusions are optional.

5. Select the **Policy definition** ellipsis button to open the list of available definitions. Azure Policy comes with built-in policy definitions you can use, this is the same list that we saw earlier in the **Definitions**

pane. Many are available, such as the below, but again you can take a quick moment to scroll through and search for ones that may interest you:

- Require tag and its value
- Append tag and its value
- Require SQL Server version 12.0

In the **Available Definitions** pane in the **Search** box type **location** and click on the **Allowed locations** definition, then click **Select**.

Available Definitions

Type Search

Policy Definitions (3)

Audit resource location matches resource group location
Built-in
Audit that the resource location matches its resource group location

Allowed locations
Built-in
This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.

Allowed locations for resource groups
Built-in
This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.

Select **Cancel**

Note: This **Allowed Locations** policy definition will specify a location into which all resources must be deployed. If a different location is chosen deployment will not be allowed. For a partial list of available built-in policies, you can also see them at the [Azure Policy Samples³²](#) page.

6. In the **Assign policy** pane, in the **PARAMETERS** section, click on the arrow at the end of the **Allowed locations** box and from the subsequent list choose **Japan West**. Leave all other values as they are and Click **Assign**.

³² <https://docs.microsoft.com/en-us/azure/governance/policy/samples/index>

MCT USE ONLY. STUDENT USE PROHIBITED

Assign policy

Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition
Allowed locations

* Assignment name
Allowed locations

Description

Assigned by
Eamonn Kelly

PARAMETERS

* Allowed locations
Japan West

MANAGED IDENTITY

Policies with effect type deployIfNotExist need the ability to deploy resources. To do this, a managed identity will be created to deploy the resources for you.
Learn more about Managed identity.

Create a Managed identity

* Managed Identity location
East US

Assign **Cancel**

Note: The **Assignment name** is automatically populated with the policy name you selected, but you can change it if you wish. You can also add an optional **Description** and **Assigned by** will automatically fill based on whoever is logged in. This field is optional, so custom values can be entered. Leave the **Create a Managed Identity** option unchecked. However, this box **must** be checked when the policy or initiative includes a policy with the **deployIfNotExists** effect.

7. The **Allowed locations** policy assignment is now listed on the **Policy - Assignments** pane and it is now in place and available to enforce at the scope level we specified i.e. at subscription level.

Policy - Assignments

Search (Ctrl+F)

Assign initiative Assign policy Refresh

Scope: 2 selected Definition type: All definition types Search: Filter by name or id...

NAME	SCOPE	TYPE	POLICIES
Allowed locations	Visual Studio Ultimate with MSDN	Policy	1
ASC DataProtection (subscription: 6e9a285a-37ea-40e6-b2fc-28...)	Visual Studio Ultimate with MSDN	Initiative	1
ASC Default (subscription: 6e9a285a-37ea-40e6-b2fc-28539051...)	Visual Studio Ultimate with MSDN	Initiative	76
ASC Default (subscription: 974e6e39-73eb-48b0-9226-dae3142...)	Pay-As-You-Go	Initiative	76

Test Allowed location policy

1. In the Azure Portal, in the **FAVORITES** list on the left hand side, then click **Create virtual machine**

2. In the **Create a virtual machine** pane on the **Basics** tab fill in the fields with the following values, leaving all other values as default, and Click **Review + create**.
- Subscription:** < select your own subscription. Ensure it is the same subscription you assigned the allowed locations policy to earlier >
 - Resource group:** < click **Create new** and enter a value i.e. **vmpolcheckrg**
 - Virtual machine name:** vmpolcheck1
 - Region:** < select any Datacenter location other than the one that you used as a parameter value earlier in the policy assignment i.e. we assigned **Japan West** earlier as the allowed datacenter location, so use **(Europe) North Europe** now >
 - Authentication type:** Password
 - Username:** azureuser
 - Password:** Password0134!

Home > Virtual machines > Create a virtual machine

Create a virtual machine

Create new

INSTANCE DETAILS

- * Virtual machine name
- * Region
- Availability options
- * Image
- Browse all images
- * Size
[Change size](#)

ADMINISTRATOR ACCOUNT

- Authentication type Password SSH public key
- * Username
- * Password
- * Confirm password

INBOUND PORT RULES

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

- * Public inbound ports None Allow selected ports
- Select inbound ports
- All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Review + create Previous Next : Disks >

3. You will receive a Validation failed message, and click on the **Click here to view details** message

Create a virtual machine

Validation failed. Click here to view details.

Pricing not available for this offering

Debian Linux by Debian

Standard D2s v3 by Microsoft

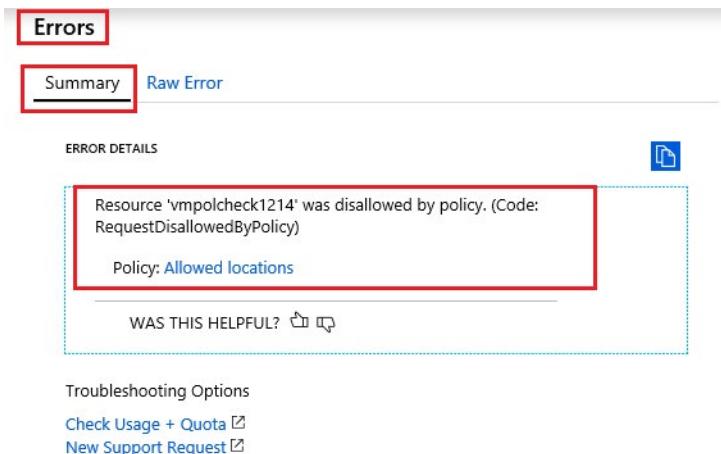
TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

BASICS

Subscription	Visual Studio Ultimate with MSDN
Resource group	(new) vmpolcheckrg
Virtual machine name	vmpolcheck1
Region	(Europe) North Europe
Availability options	No infrastructure redundancy required
Authentication type	Password
Username	azureuser
Public inbound ports	None

4. In the resultant **Errors** blade, on the **Summary** tab note the error message, **Resource xyz was disallowed by Policy** and the policy name listed as **Allowed locations**



Troubleshooting Options

[Check Usage + Quota](#)

[New Support Request](#)

Note: You can dig in further for specifics, by clicking on the **Raw Error** tab and viewing the output and also by clicking on the Allowed locations policy, to view the policy that blocked the deployment.

Delete the policy assignment

We will delete the policy assignment to ensure we are not blocked on any future work we wish to do.

1. In the Azure Portal click **All Services > Management + governance** then **Policy** and on the **Policy** pane select **Compliance** in the left side of the page. Within this pane you can view the compliance state of the various policies you have assigned.

NAME	SCOPE	COMPLIANCE STATE	NON-COMPLIANT RESOURCES	NON-COMPLIANT POLICIES
Allowed locations	Visual Studio Ultimate wit...	Non-compliant	6	1
ASC DataProtection (subscription...)	Visual Studio Ultimate wit...	Compliant	0	0
ASC Default (subscription: 6e9a2...)	Visual Studio Ultimate wit...	Non-compliant	2	3
ASC Default (subscription: 974e6...)	Pay-As-You-Go	Non-compliant	1	10

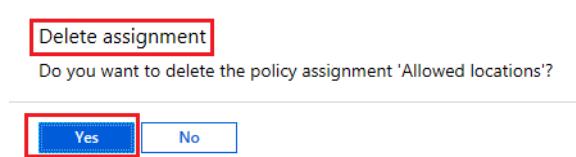
Note: The Allowed location policy is listed as non-compliant in the screenshot, as there are pre-existing resources deployed outside of **Japan West**, which were created prior to the policy assignment, when using Azure Cloud Shell and other Azure resources.

2. Go to **Assignments** and click on the ellipsis at the end of the **Allowed locations** policy assignment. Then select **Delete Assignment** from the resultant menu.

MCT USE ONLY. STUDENT USE PROHIBITED

Name	Scope	Type	Policies	
Allowed locations	Visual Studio Ultimate with MSDN	Policy	1	View compliance ...
ASC DataProtection (subscription: 6e9a285a-37ea-40e...	Visual Studio Ultimate with MSDN	Initiative	1	View definition ...
ASC Default (subscription: 6e9a285a-37ea-40e6-b2fc-2...	Visual Studio Ultimate with MSDN	Initiative	76	Delete assignment ...
ASC Default (subscription: 974e6e39-73eb-48b0-9226-...	Pay-As-You-Go	Initiative	76	Duplicate assignment ...

3. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**



You are now able to create resources in your subscription in any location you wish again.

Note: Some scenarios where the **Allowed locations** policy can be useful include:

- *Cost Tracking:* You could have different subscriptions for different regional locations and ensuring that all resources are deployed in that region to help cost tracking.
- *Data Residency and Security compliance:* You could also have data residency requirements, and create subscriptions per customer or specific workloads, and define that all resources must be deployed in a particular datacenter to ensure data and security compliance requirements.

Congratulations! You have located an Azure Policy to restrict deployment of Azure resources to a particular datacenter, and then assigned that allowed location policy to a subscription. You then verified that creating an Azure resource, such as a virtual machine, outside of the allowed location was blocked. You finally removed the allowed location policy assignment, to allow you deploy resources again to any datacenter location using that same subscription.

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.

Role-Based Access Control (RBAC)

Role-based access control (RBAC) provides fine-grained access management for Azure resources, enabling you to grant users only the rights they need to perform their jobs. RBAC is provided at no additional cost to all Azure subscribers.

Usage Scenarios

Examples of when you might use RBAC include when you want to:

- Allow one user to manage VMs in a subscription, and another user to manage virtual networks.
- Allow a database administrator (DBA) group to manage SQL databases in a subscription.

- Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.
- Allow an application to access all resources in a resource group.

To view access permissions, access the **Access Control (IAM)** blade in the Azure portal. On this blade, you can see who has access to an area and their role. Using this same blade, you can also grant or remove access.

The following shows an example of the **Access Control (IAM)** blade for a resource group. In this example, *Alain Charon* has been assigned the Backup Operator role for this resource group.

The screenshot shows the 'Access Control - Role assignment' blade in the Azure portal. The left sidebar includes links for Overview, Activity log, and the highlighted 'Access control (IAM)' option. The main pane displays a table of role assignments with columns for NAME, TYPE, ROLE, and SCOPE. A single row is selected, showing 'Alain Charon' as a User assigned the 'Backup Operator' role at the 'This resource' scope. The 'ROLE' dropdown in the top right shows '5 selected'. The 'SCOPE' dropdown shows 'All scopes'.

RBAC uses an *allow model*. This means that when you are assigned a role, RBAC *allows* you to perform certain actions, such as read, write, or delete. Therefore, if one role assignment grants you read permissions to a resource group, and a different role assignment grants you write permissions to the same resource group, you will have write permissions on that resource group.

Best Practices

The following list details RBAC best practices:

- Using RBAC, segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only certain actions at a particular scope.
- When planning your access control strategy, grant users the lowest privilege level that they need to do their work.

Note: You can read more about RBAC at [What is role-based access control \(RBAC\)?³³](#)

Walkthrough-Manage access to Azure resources using RBAC

In this walkthrough task we will create some Azure resources that we can manage using Role-Based-Access-Control (RBAC), then we will view access control at subscription level, then view roles and permissions at resource group level for azure resources, and view individual user and all role assignments. You will then add a new role assignment for the virtual machine contributor role and then remove a role assignment for the resources you deployed.

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

³³ <https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

Prerequisites

- You require 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 today³⁴](#) webpage.

Steps

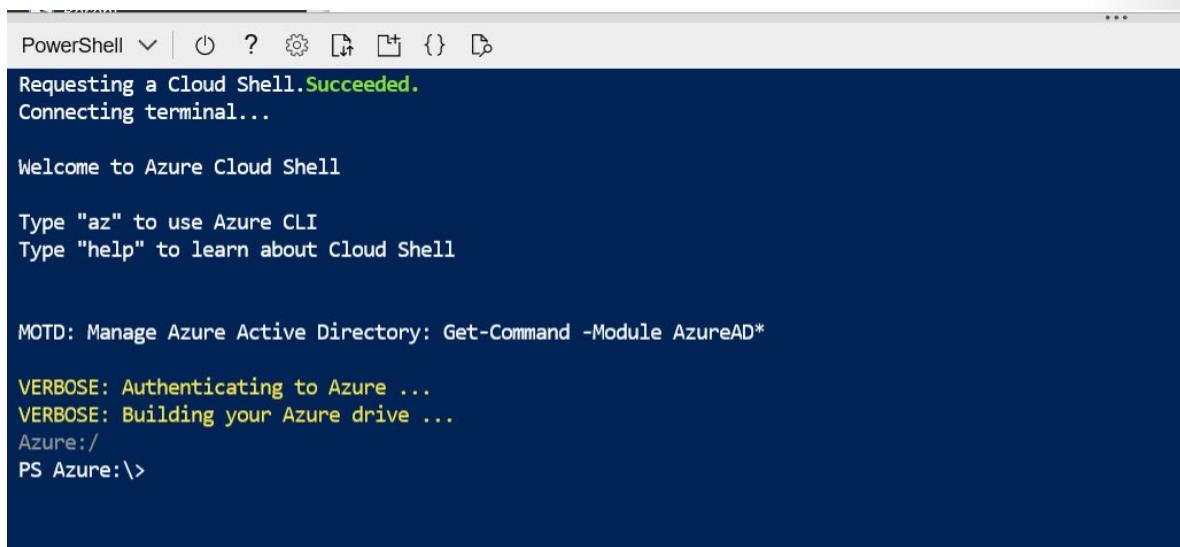
Create Azure resources to manage

Firstly, we will deploy some resources to Azure to provide us with some resources to manage.

1. Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.



3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** or **bash** console.

```
az group create `  
  --name rbacrg `  
  --location westeurope
```

³⁴ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

```
Azure:/  
PS Azure:> az group create `  
>>   --name rbacrg `  
>>   --location westeurope  
{  
  "id": "/subscriptions/                               ./resourceGroups/rbacrg",  
  "location": "westerurope",  
  "managedBy": null,  
  "name": "rbacrg",  
  "properties": {  
    "provisioningState": "Succeeded"  
  },  
  "tags": null,  
  "type": null  
}  
Azure:/  
PS Azure:> █
```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
az vm create `  
  --name vmrbac1 `  
  --resource-group rbacrg `  
  --image Win2019Datacenter `  
  --location westeurope `  
  --admin-username azureuser `  
  --admin-password Password0134!
```

```
PS Azure:> az vm create `  
>>   --name vmrbac1 `  
>>   --resource-group rbacrg `  
>>   --image Win2019Datacenter `  
>>   --location westeurope `  
>>   --admin-username azureuser `  
>>   --admin-password Password0134!  
{  
  "fqdns": "",  
  "id": "/subscriptions/                               ./resourceGroups/rbacrg/providers/Microsoft.Compute/virtualMachines/vmrbac1",  
  "location": "westerurope",  
  "macAddress": "00-0D-3A-49-7E-5E",  
  "powerState": "VM running",  
  "privateIpAddress": "10.0.0.4",  
  "publicIpAddress": "40.114.211.116",  
  "resourceGroup": "rbacrg",  
  "zones": ""  
}  
Azure:/  
PS Azure:> █
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.

View access control at subscription level

The next thing we need to do, in the context of access control, is to decide where to open the **Access control (IAM)** blade, through which we configure Role-Based-Access-Control (RBAC), and that depends on what resources you want to manage access for. i.e. do you want to manage access for everything in a management group, everything in a subscription, everything in a resource group, or a single resource?

MCT USE ONLY. STUDENT USE PROHIBITED

The **Access control (IAM)** blade is available at all of these levels and provides the same functionality in each. We will firstly have a look at the **Access control (IAM)** options for a subscription.

1. In the Azure portal, click **All services** and the **Subscriptions**, double click on a subscription from the subscriptions listed and then click on Access control (IAM) the scope.

- **Note:** The screenshot above shows an example of the **Access control (IAM)** blade for a subscription. If you make any access control changes here, they would apply to the entire subscription. Likewise, any changes made at management group, resource group or individual resource level apply just at those levels.

View roles and permissions

A role definition is a collection of permissions that you use for role assignments. Azure has over 70 built-in roles for Azure resources. Follow these steps to view the available roles and permissions for the resources we deployed earlier.

1. Go to **Resource groups** and choose **rbacrg** i.e. the resource group you created earlier.
2. Within the **rbacrg** resource group, click on **Access control (IAM)** and then select the **Roles** tab to see a list of all the built-in and custom roles.

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Name	Type	Users	Groups
Owner	BuiltInRole	2	0
Contributor	BuiltInRole	24	0
Reader	BuiltInRole	0	0
AcrDelete	BuiltInRole	0	0
AcrImageSigner	BuiltInRole	0	0
AcrPull	BuiltInRole	0	0
AcrPush	BuiltInRole	0	0
AcrQuarantineReader	BuiltInRole	0	0
AcrQuarantineWriter	BuiltInRole	0	0
API Management Service Contributor	BuiltInRole	0	0
API Management Service Operator Role	BuiltInRole	0	0
API Management Service Reader Role	BuiltInRole	0	0
Application Insights Component Contributor	BuiltInRole	0	0

Note: You can see the number of users and groups that are assigned to each role at the current scope.

- Click on the **Owner** role to see who has been assigned this role and also view the permissions for the role.

NAME	ACCESS
Eamonn Kelly	Subscription (Inherited)
VSTSPU	Subscription (Inherited)

Note: As per the screenshot, there are two users listed who are assigned the Owner role. Your list of users will be different.

View individual user and all role assignments for a resource

When managing access, you want to know who has access, what are their permissions, and at what scope. To list access for a user, group, service principal, or managed identity, you view their role assignments.

- In the resource group you created earlier i.e. **rbacrg** go to **Access control (IAM)** and select the **Check Access** tab

rbacrg - Access control (IAM)

Check access

Add a role assignment

View role assignments

View deny assignments

- In the **Find** boxes enter the below values, to search the directory for display names, email addresses, or object identifiers. The matching results are displayed below the **Find** boxes
 - Azure AD user, group, or service principal
 - < your own user name i.e. in this case we used eamonn kelly >

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the 'Check access' section of the Azure portal. On the left, there's a search interface for finding users, groups, or service principals, with 'Azure AD user, group, or service principal' selected and 'eamonn kelly' entered. Below it is a list of users, with 'Eamonn Kelly' highlighted. To the right, three cards provide options for managing role assignments:

- Add a role assignment**: Grants access by assigning a role to a user, group, service principal, or managed identity. Includes a 'Add' button and a 'Learn more' link.
- View role assignments**: Shows users, groups, service principals, and managed identities with role assignments. Includes a 'View' button and a 'Learn more' link.
- View deny assignments**: Shows users, groups, service principals, and managed identities denied access. Includes a 'View' button and a 'Learn more' link.

Note: Your results will be different and related to your own user account.

- Click the matching result to open the < name > assignments - scope pane. On this pane, you can see the roles assigned to the selected user and the scope. If there are any deny assignments at this scope or inherited to this scope, they will be listed. We can see the user has the role of **Owner** assigned and can manage everything.

The screenshot shows the 'Eamonn Kelly assignments - rbacr' pane. It displays the following information:

- Role assignments (1)**: A table showing one assignment for the 'Owner' role, which lets you manage everything. The scope is 'Subscription (Inherited)' and the group assignment is '--'. The table has columns: ROLE, DESCRIPTION, SCOPE, and GROUP ASSIGNMENT.
- Deny assignments (0)**: Shows 0 deny assignments.
- Classic administrators (1)**: A table showing one assignment for the 'Service Administrator' role, which has full access to all resources in the subscription. The table has columns: ROLE and DESCRIPTION.

4. Still on the resource group **Access control (IAM)** pane, click the **Role assignments** tab to view all the role assignments at this scope. On the **Role assignments** tab, you can see who has access at this scope.

The screenshot shows the 'Role assignments' tab selected in the top navigation bar. Below the tabs, there is a message: 'Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. [Learn more](#)'.

Filtering options include:

- Name: Search by name or email
- Type: All (selected)
- Role: 2 selected
- Scope: All scopes
- Group by: Role

The table below lists 26 items (1 Users, 25 Service Principals). The columns are:

<input type="checkbox"/>	NAME	TYPE	ROLE	SCOPE
<input type="checkbox"/>	ansibleApp	App	Contributor	Subscription (Inherited)
<input checked="" type="checkbox"/>	DevOpsLab02_yqJnxnCvz	App	Contributor	Subscription (Inherited)
<input type="checkbox"/>	DevOpsLab2_SanEav5LW	App	Contributor	Subscription (Inherited)
<input type="checkbox"/>	DevOpsLabs1_moOKZAx	App	Contributor	Subscription (Inherited)
<input type="checkbox"/>	DevOpsLabs1_n9f31tB1m	App	Contributor	Subscription (Inherited)
<input type="checkbox"/>	eamDevopsCI1-12mar20	App	Contributor	Subscription (Inherited)

Note: Some of roles present, are listed as **(Inherited)**. This means they are assigned from another scope. Access, in general, is either assigned specifically to this resource, or inherited from an assignment to the parent scope. Your values will be different to those displayed here.

Add a role assignment

In RBAC, to grant access, you assign a **Role** to a user, group, service principal, or managed identity. We will assign the a role to a user in the following steps.

1. Open the resource group **Access control (IAM)** and click the **Role assignments** tab, then click **Add** and choose **Add role assignment** to open the **Add role assignment** pane.

MCT USE ONLY. STUDENT USE PROHIBITED

Note: If you don't have permissions to assign roles, the **Add role assignment** option will be disabled.

2. In the **Add role assignment** pane fill in the following values, then click **Save** to assign the role.
 - **Role:** select a Role from the drop down list i.e. *Virtual Machine Contributor*
 - **Assign access to:** Azure AD user, group, or service principal
 - **Select:** < type your own user name, and your user name should appear in the list, then click on a user name to select it >

Selected members:

	Eamonn Kelly eamonn_kelly@hotmail.com	Remove
--	--	------------------------

Save	Discard
----------------------	-------------------------

3. The user is now assigned the specified role at the selected scope.

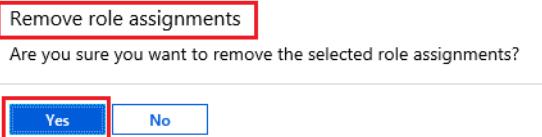
Remove role assignments

In RBAC, to remove access, you remove a role assignment.

1. Open the resource group **Access control (IAM)** and click the **Role assignments** tab,
2. Scroll down through the list of users until you find the user you just added as a **Virtual Machine Contributor**, click on the user, then select **Remove**

OWNER			
Eamonn Kelly	User	Owner	Subscription (Inherited)
VSTSPU	App	Owner	Subscription (Inherited)
VIRTUAL MACHINE CONTRIBUTOR			
<input checked="" type="checkbox"/> Eamonn Kelly	User	Virtual Machine Contributor	This resource

3. In the remove role assignment message that appears, click **Yes**.



Note: Inherited role assignments cannot be removed. If you need to remove an inherited role assignment, you must do it at the scope where the role assignment was created. In the **Scope** column, the column where **(Inherited)** appears, there is a link that takes you to the scope where this role was assigned in this case the subscription, then you can go to the **Access control (IAM)** blade and remove the role assignment there.

Congratulations! You have created some Azure resources that you can manage using Role-Based-Access-Control (RBAC), you have viewed access control at subscription level, and then viewed roles and permissions at resource group level for azure resources, and viewed individual user and all role assignments. You then added a new role assignment for the virtual machine contributor role and finally removed a role assignment for the resources you deployed.

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.

Locks

Locks help you prevent accidental deletion or modification of your Azure resources. You can manage these locks from within the Azure portal. To view, add, or delete locks, go to the **SETTINGS** section of any resource's settings blade.

You may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to **CanNotDelete** or **ReadOnly**:

- **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

In the Azure portal, the locks are called *Delete* and *Read-only* respectively.

Note: You can read more about Locks at [Lock resources to prevent unexpected changes³⁵](#).

Walkthrough-Manage Azure resources using Locks

In this walkthrough task we will create Azure resources to allow us to create a lock against them, then you will add a **Delete** Lock to prevent deletion of a resource group. You will then verify that deletion of the resource group is indeed blocked, and also that any resources within the resource group are also blocked from being deleted by the parent Lock. You will then remove the lock and verify it has been removed by deleting the resource group.

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 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 today³⁶](#) webpage.

Steps

Create Azure resources to allow us to create a lock against them

Firstly, we will deploy some resources to Azure to provide us with some resources to manage. If you have resources available from a previous deployment, you can use those instead of deploying new ones.

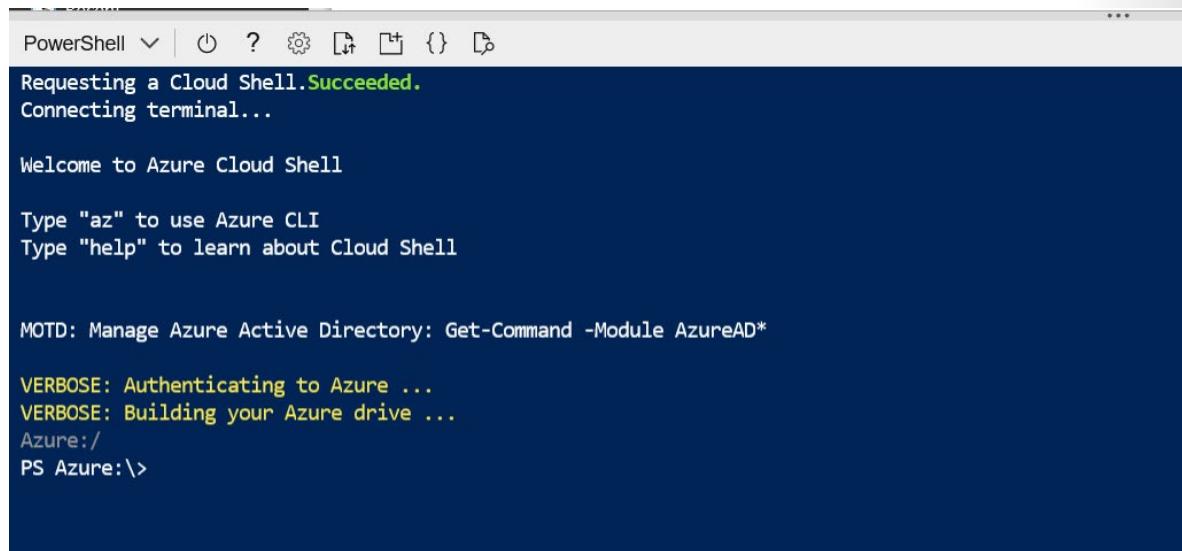
1. Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.

³⁵ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

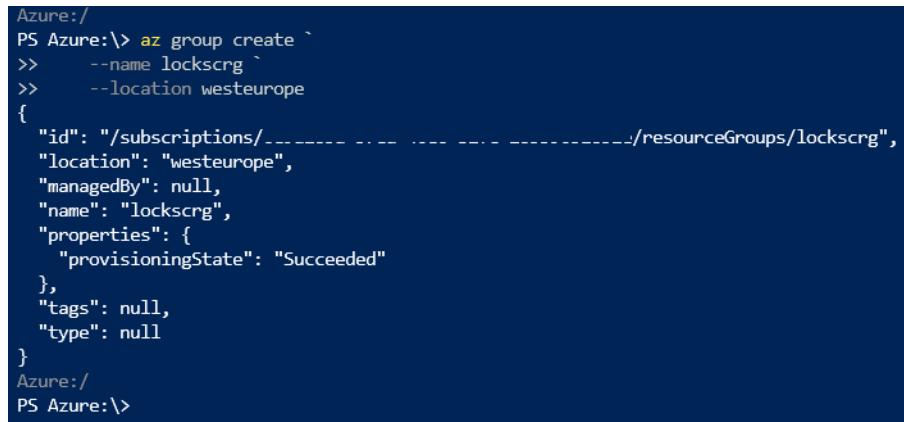
³⁶ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio



The screenshot shows the Azure Cloud Shell interface. It displays a success message: "Requesting a Cloud Shell.Succeeded." followed by "Connecting terminal...". Below this, it says "Welcome to Azure Cloud Shell" and provides instructions: "Type "az" to use Azure CLI" and "Type "help" to learn about Cloud Shell". A MOTD message follows: "MOTD: Manage Azure Active Directory: Get-Command -Module AzureAD*". The session then shows verbose output: "VERBOSE: Authenticating to Azure ..." and "VERBOSE: Building your Azure drive ...". The prompt is "Azure:/ PS Azure:\>".

3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** or **bash** console.

```
az group create ` 
  --name lockscrg ` 
  --location westeurope
```



The screenshot shows the Azure Cloud Shell interface with the command "az group create" entered. The output is a JSON object representing the newly created resource group "lockscrg". The JSON includes fields like "id", "location", "managedBy", "name", "properties", "tags", and "type", all set to their respective values. The command "az group create" is shown again at the bottom.

```
Azure:/ 
PS Azure:\> az group create ` 
>>   --name lockscrg ` 
>>   --location westeurope 
{ 
  "id": "/subscriptions/____-/resourceGroups/lockscrg", 
  "location": "westeurope", 
  "managedBy": null, 
  "name": "lockscrg", 
  "properties": { 
    "provisioningState": "Succeeded" 
  }, 
  "tags": null, 
  "type": null 
} 
Azure:/ 
PS Azure:\>
```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
az vm create ` 
  --name vmlocks1 ` 
  --resource-group lockscrg ` 
  --image Win2019Datacenter ` 
  --location westeurope ` 
  --admin-username azureuser ` 
  --admin-password Password0134!
```

```
Azure:/  
PS Azure:\> az vm create -  
>>   --name vmlocks1  
>>   --resource-group lockscrg  
>>   --image Win2019Datacenter  
>>   --location westeurope  
>>   --admin-username azureuser  
>>   --admin-password Password0134!  
{  
    "fqdns": "",  
    "id": "/subscriptions/-----/resourceGroups/lockscrg/providers/Microsoft.Compute/virtualMachines/vmlocks1",  
    "location": "westeurope",  
    "macAddress": "00-0D-3A-2A-FB-87",  
    "powerState": "VM running",  
    "privateIpAddress": "10.0.0.4",  
    "publicIpAddress": "13.94.150.254",  
    "resourceGroup": "lockscrg",  
    "zones": ""  
}  
Azure:/  
PS Azure:\>
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.

Add a Lock to prevent deletion of a resource

You can apply a **Lock** to a subscription, resource group, or individual resource to prevent other users in your organization from accidentally deleting or modifying critical resources. We will apply a lock to a resource, however it is the same process regardless of the scope in which it is used.

1. In the Azure Portal go to the resource group you just created i.e. **lockscrg**, then go to **Settings > Locks**

The screenshot shows the Azure Portal interface for the 'lockscrg' resource group. On the left, there's a navigation sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Deployments, Policies, Properties, Locks (which is highlighted with a red box), Export template, Cost Management, Cost analysis, Cost alerts, Budgets, Advisor recommendations, Monitoring, and Insights (preview). The main content area is titled 'lockscrg - Locks' and shows a table with one row: 'This resource has no locks.' The table has columns for LOCK NAME, LOCK TYPE, SCOPE, and NOTES.

2. To add a lock, select **Add** and then enter the following values, clicking **OK** when finished.

- **Lock name:** resource group lock
- **Lock Type:** Delete (the other lock type available to us here is *Read-only*)

MCT USE ONLY. STUDENT USE PROHIBITED

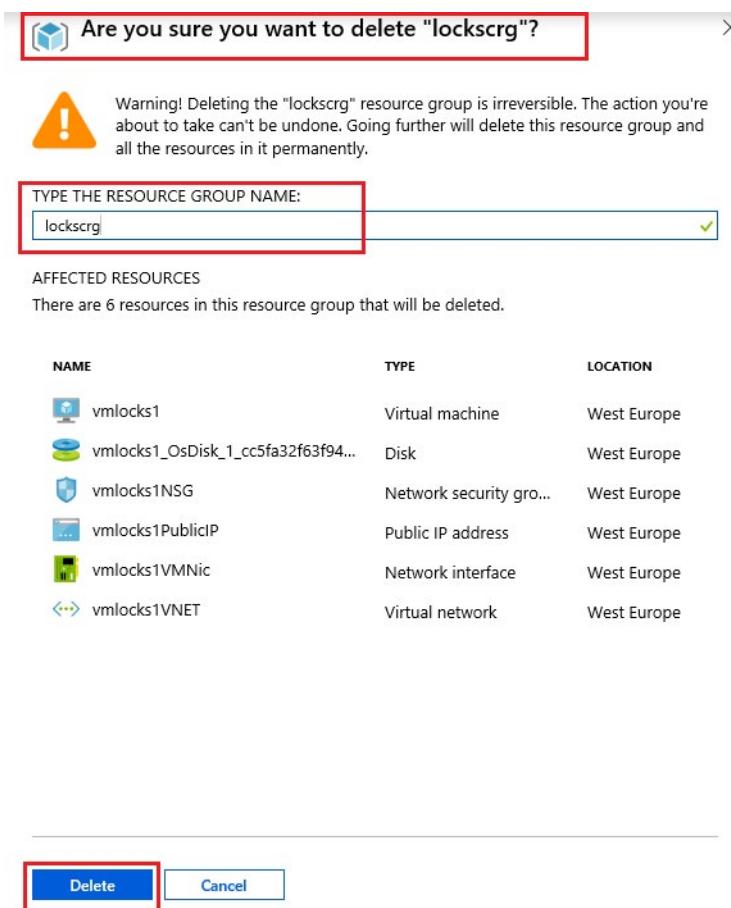
The screenshot shows the 'locksrg - Locks' blade in the Azure portal. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Deployments, Policies, and Properties. The 'Overview' option is selected. In the main area, there's a 'Search (Ctrl+ /)' input field, a 'Subscription' dropdown, and a 'Refresh' button. A modal window titled 'Add lock' is open, containing fields for 'Lock name' (set to 'resource group lock') and 'Lock type' (set to 'Delete'). Below these fields is a 'Notes' input field, which is currently empty. At the bottom of the modal are 'OK' and 'Cancel' buttons, with 'OK' also highlighted with a red box.

- Now let us try delete the resource group we just created the **Delete** lock for, by going to the resource group i.e. **locksrg**, then the clicking on **Overview** and selecting **Delete resource group**

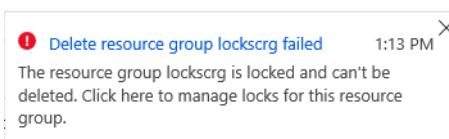
The screenshot shows the 'locksrg - Resource group' blade in the Azure portal. The left sidebar includes 'Overview' (highlighted with a red box), Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Deployments, Policies, Properties, Locks (highlighted with a red box), Export template, Cost Management, Cost analysis, and Cost alerts. The main area displays basic information about the resource group: Subscription (Visual Studio Ultimate with MSDN), Subscription ID (6e9a285a-37ea-40e6-b2fc-28539051852e), and Tags (Click here to add tags). It also shows deployment details: 1 Succeeded. Below this is a table listing resources: NAME, TYPE, LOCATION, and three dots for each item. The first item listed is 'vmlock1' (Virtual machine, West Europe).

NAME	TYPE	LOCATION
vmlock1	Virtual machine	West Europe
vmlock1_OsDisk_1_cc5fa32f63f94c51acf...	Disk	West Europe
vmlock1NSG	Network security group	West Europe
vmlock1PublicIP	Public IP address	West Europe
vmlock1VMNic	Network interface	West Europe
vmlock1VNET	Virtual network	West Europe

- In the **Are you sure you want to delete "locksrg"**? blade, type the name of the resource group i.e. **locksrg** and click the **Delete** button



5. You receive an error message stating the resource group is locked and can't be deleted



6. Within the same resource group open the virtual machine i.e.**vmlocks1**, go to the **Overview** pane and select **Delete**

The screenshot shows the Azure portal interface for a virtual machine named 'vmlocks1'. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Disks, Size, Security, Extensions, Continuous delivery (Preview), Availability set, Configuration, Identity, Properties, Locks, and Export template. The 'Overview' tab is selected and highlighted in red. At the top right, there are buttons for Connect, Start, Restart, Stop, Capture, Delete (which is also highlighted in red), and Refresh. Below the top bar, detailed information about the VM is listed, including its resource group ('lockscr'), status ('Running'), location ('West Europe'), subscription ('Visual Studio Ultimate with MSDN'), and various network and security details. To the right of this information are three performance charts: CPU (average), Network (total), and Disk bytes (total), each showing data over a 30-day period.

7. In the resultant **Delete virtual machine** pane, select **Yes** to confirm your wish to delete the virtual machine.

This screenshot shows a confirmation dialog box titled 'Delete virtual machine'. It contains the message: 'This action will permanently delete the virtual machine 'vmlocks1'. Associated resources (disks, virtual networks, etc) will not be deleted and can be removed manually. Do you want to continue?'. At the bottom, there are two buttons: 'Yes' (highlighted in red) and 'No'.

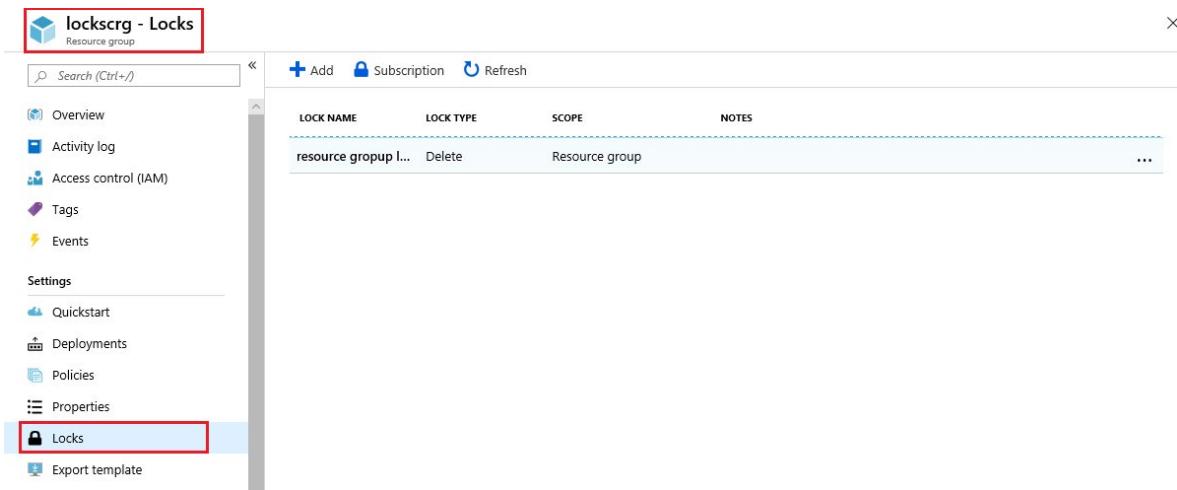
8. You receive an error message stating

This screenshot shows a notification message from the Azure portal. It has an exclamation icon and the text 'Failed to delete the virtual machine'. Below it, a timestamp '1:20 PM' is shown. The message continues: 'Failed to delete the virtual machine 'vmlocks1''. Error: The scope 'vmlocks1' cannot perform delete operation because following scope(s) are locked: 'lockscr'. Please remove the lock and try again.'

Note: Although we did not create a lock specifically for the virtual machine, we did create a lock at the resource group level, which contains the virtual machine resource. As such this *parent* level lock prevents us from deleting the virtual machine, the virtual machine resource inherits the lock from the parent.

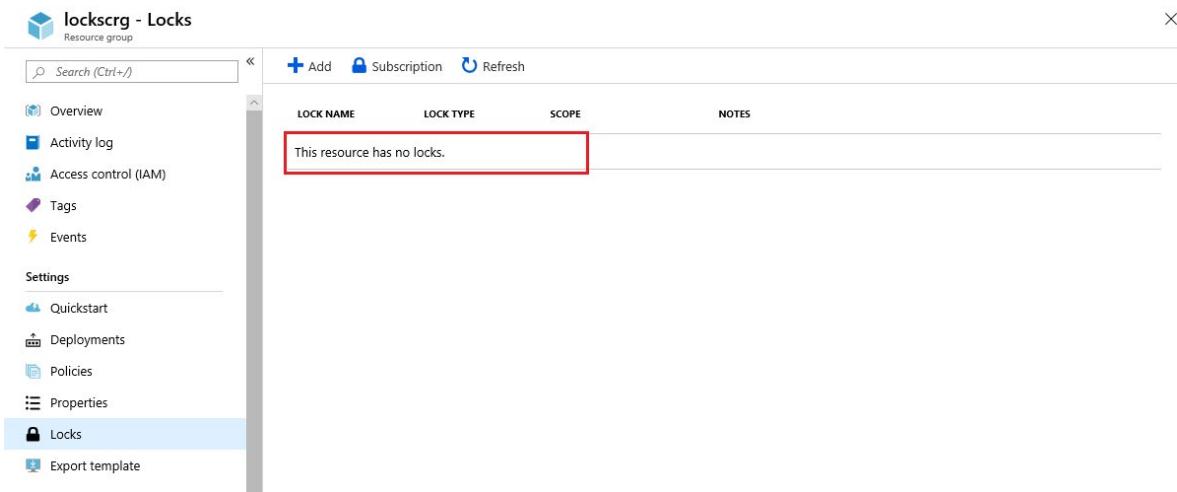
Remove a lock

1. Return to the resource group and go to **Settings > Locks**



The screenshot shows the Azure portal interface for a resource group named 'lockscrg'. On the left, there's a navigation sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Events, Settings (Quickstart, Deployments, Policies, Properties), and Locks. The 'Locks' option is currently selected and highlighted with a red box. The main content area displays a table with columns: LOCK NAME, LOCK TYPE, SCOPE, and NOTES. A single row is present in the table, showing 'resource group lock' as the lock name, 'Delete' as the lock type, 'Resource group' as the scope, and an empty notes field. At the top of the main area, there are buttons for Add, Subscription, Refresh, and an ellipsis menu.

2. Click the ellipsis at the end of the Delete lock that you created earlier and select **Delete** on the resultant menu



This screenshot shows the same Azure portal interface as the previous one, but now the 'Locks' blade is displayed. The message 'This resource has no locks.' is centered in a box, which is highlighted with a red box. The rest of the interface, including the sidebar and the table structure, remains the same.

3. In the resource group **Overview** pane, click on **Delete resource group** and in the resultant **Are you sure you want to delete "lockscrg"?** pane, type in the name of the resource group and click **Delete** to delete the resource group.

The resource group and all resources within it are successfully deleted now, because the delete lock has been removed.

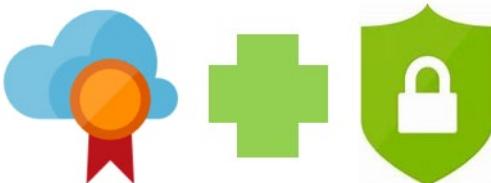
Congratulations! You have created Azure resources to allow us to create a lock against them, then you added a **Delete** Lock to prevent deletion of a resource group. You then verified that deletion of the resource group was indeed blocked as a result of the created Lock, and also that any resources within the resource group were also blocked from being deleted by the parent Lock. You then removed the lock and verified it has been removed by successfully deleting the resource group.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Azure Advisor security assistance

As discussed earlier in the course, *Azure Advisor* is a free service built into Azure that provides recommendations on high availability, security, performance, and cost. Advisor analyzes your deployed services and looks for ways to improve your environment across those four areas.

Azure Advisor and Azure Security Center



Azure Advisor provides security recommendations by integrating with Azure Security Center. You can view the security recommendations on the **Security tab** of the Advisor dashboard. You can then click deeper into the Security Center recommendations.

Advisor recommendations

[Download as CSV](#) [Download as PDF](#) [Configure](#)

Subscriptions: All 2 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

All subscriptions [All types](#) [Active](#) [No grouping](#)

Overview [High Availability \(3\)](#) [Security \(11\)](#) [Performance \(0\)](#) [Cost \(1\)](#) [All \(15\)](#)

Your security experience may be limited. Click here to learn more →

Total recommendations	Recommendations by impact	Impacted resources	Security alerts	Learn more
11	11 High impact 0 Medium impact 0 Low impact	13	Standard plan feature	What is Security Center Explore Security Center Recommendations
IMPACT	DESCRIPTION	POTENTIAL BENEFITS	RECOMMENDATIONS	UPDATED AT
High	Follow Security Center recommendations	Prevent potential security breaches	11 Recommendations	12/5/2018 2:51:11 PM

Azure Blueprints

Azure Blueprints enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements. Azure Blueprint enables development teams to rapidly build and deploy new environments with the knowledge that they're building within organizational compliance with a set of built-in components that speed up development and delivery.



Azure Blueprint is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

The process of implementing Azure Blueprint consists of the following high-level steps:

1. Create an Azure Blueprint.
2. Assign the blueprint.
3. Track the blueprint assignments.

With Azure Blueprint, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved deployment tracking and auditing.

Azure Blueprints are different from Azure Resource Manager Templates. When Azure Resource Manager Templates deploy resources, they have no active relationship with the deployed resources (they exist in a local environment or in source control). By contrast, with Azure Blueprint, each deployment is tied to an Azure Blueprint package. This means that the relationship with resources will be maintained, even after deployment. Maintaining relationships, in this way, improves auditing and tracking capabilities.

Usage Scenario

Adhering to security or compliance requirements, whether government or industry requirements, can be difficult and time-consuming. To help you with auditing, traceability, and compliance with your deployments, use Azure Blueprint artifacts and tools. Time-consuming paperwork is no longer needed, and your path to certification is expedited.

Azure Blueprint are also useful in Azure DevOps scenarios, where blueprints are associated with specific build artifacts and release pipelines, and can be tracked more rigorously.

NOTE: At the time of writing, Azure Blueprint is in preview and has not been released generally.

Note: You can read more about Azure Blueprints at [Azure Blueprints³⁷](https://azure.microsoft.com/en-us/services/blueprints/).

Subscription Governance

Subscription governance

We will discuss and define subscriptions in more detail later in the course, however we wish to briefly mention them here in the context of governance.

There are mainly three aspects to consider in relation to creating and managing subscriptions: *Billing*, *Access Control* and *Subscription limits*.

- *Billing*: Reports can be generated by subscriptions, if you have multiple internal departments and need to do “chargeback”, a possible scenario is to create subscriptions by department or project.
- *Access Control*: A subscription is a deployment boundary for Azure resources and every subscription is associated with an Azure AD tenant that provides administrators the ability to set up role-based access control (RBAC). When designing a subscription model, one should consider the deployment boundary factor, some customers have separate subscriptions for Development and Production, each one is completely isolated from each other from a resource perspective and managed using RBAC.
- *Subscription Limits*: Subscriptions are also bound to some hard limitations. For example, the maximum number of Express Route circuits per subscription is 10. Those limits should be considered during the design phase, if there is a need to go over those limits in particular scenarios, then additional subscriptions may be needed. If you hit a hard limit, there is no flexibility.

Also available to assist with managing subscriptions are management groups, which manage access, policies, and compliance across multiple Azure subscription. We will discuss these in more detail later.

Note: For more information about subscription limits, refer to [Azure subscription and service limits, quotas, and constraints³⁸](#).

³⁷ <https://azure.microsoft.com/en-us/services/blueprints/>

³⁸ <https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits>

Monitoring and Reporting in Azure

Tags

You apply tags to your Azure resources giving metadata to logically organize them into a taxonomy.



Each tag consists of a name and a value pair. For example, you can apply the name **Environment** and the value **Production** to all the resources in production, or tag by company departments i.e. apply the name of **Department** and a value of **IT** etc

Name	Value
Environment	Production
Department	IT

After you apply tags, you can retrieve all the resources in your subscription with that tag name and value. Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Tag Limitations

There are some limitations with using **Tags**, such as:

- Not all resource types support tags. To determine if you can apply a tag to a resource type, see Tag support for Azure resources. [Tag support for Azure resources³⁹](#)
- Each resource or resource group can have a maximum of 15 tag name/value pairs. This limitation applies only to tags directly applied to the resource group or resource. A resource group can contain many resources that each have 15 tag name/value pairs. If you have more than 15 values that you need to associate with a resource, use a JSON string for the tag value. The JSON string can contain many values that are applied to a single tag name.
- The tag name is limited to 512 characters, and the tag value is limited to 256 characters. For storage accounts, the tag name is limited to 128 characters, and the tag value is limited to 256 characters.
- Virtual Machines and Virtual Machine Scale Sets are limited to a total of 2048 characters for all tag names and values.
- Tags applied to the resource group are not inherited by the resources in that resource group.
- Tags can't be applied to classic resources such as Cloud Services.

Note: You can use **Azure Policy** to enforce tagging values and rules on resources.

Walkthrough-Use Tags with Azure resources

In this walkthrough task we will create Azure resources to allow us to apply Tags to them. We will then view the tags for a resource and a resource group, and then add Tags to resource groups and resources. We will then bulk assign tags to resources and view all resources with a specific tag. We will finally delete assigned tags.

³⁹ <https://docs.microsoft.com/en-us/azure/azure-resource-manager/tag-support>

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

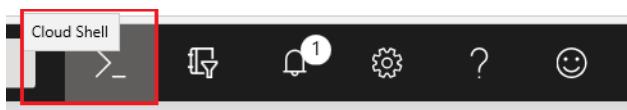
- You require an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today⁴⁰](#) webpage.

Steps

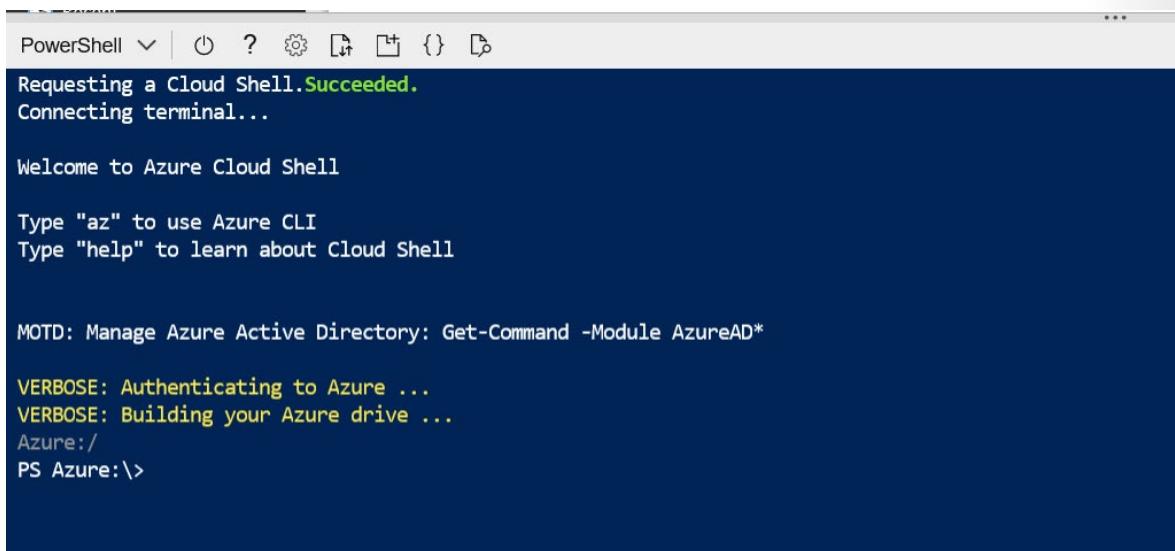
Create Azure resources to allow us to apply Tags to them

Firstly, we will deploy some resources to Azure to provide us with some resources to use Tags with. If you have resources available from a previous deployment, you can use those instead of deploying new ones.

1. Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner



2. The **Cloud Shell** is launched in the bottom of the browser window.



3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** or **bash** console.

```
az group create \
    --name tagrg \
    --location westeurope
```

⁴⁰ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

```
Azure:/  
PS Azure:\> az group create `  
>>   --name tagrg `  
>>   --location westeurope  
{  
  "id": "/subscriptions/...`  
  "location": "westerurope",  
  "managedBy": null,  
  "name": "tagrg",  
  "properties": {  
    "provisioningState": "Succeeded"  
  },  
  "tags": null,  
  "type": null  
}  
Azure:/  
PS Azure:\> [ ]
```

- Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

```
az vm create `  
  --name vmtag1 `  
  --resource-group tagrg `  
  --image Win2019Datacenter `  
  --location westeurope `  
  --admin-username azureuser `  
  --admin-password Password0134!
```

```
Azure:/  
PS Azure:\> az vm create `  
>>   --name vmtag1 `  
>>   --resource-group tagrg `  
>>   --image Win2019Datacenter `  
>>   --location westeurope `  
>>   --admin-username azureuser `  
>>   --admin-password Password0134!  
{  
  "fqdns": "",  
  "id": "/subscriptions/...`  
  "location": "westerurope",  
  "macAddress": "00-0D-3A-47-12-B2",  
  "powerState": "VM running",  
  "privateIpAddress": "10.0.0.4",  
  "publicIpAddress": "104.214.224.40",  
  "resourceGroup": "tagrg",  
  "zones": ""  
}  
Azure:/  
PS Azure:\> [ ]
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.

View the tags for a resource or a resource group

- In the Azure Portal, open the resource group we just created i.e. **tagrg**, on the **Overview** pane alongside **Tags**, note there are no values listed and a message reads **Click here to add tags**. This indicates no tags have been applied to the resource group or resources.

MCT USE ONLY. STUDENT USE PROHIBITED

NAME	TYPE	LOCATION
vmtag1	Virtual machine	West Europe
vmtag1_OsDisk_1_b04fc039779a4261b9ad2...	Disk	West Europe
vmtag1NSG	Network security group	West Europe
vmtag1PublicIP	Public IP address	West Europe
vmtag1VMNic	Network interface	West Europe
vmtag1VNET	Virtual network	West Europe

Add tags

- Still in the **Tagrg** resource group click on the **Click here to add tags** link and in the subsequent **Tags** pane enter the values below, click **Save** and then **Close**
 - Name:** Environment
 - Value:** Production

NAME	VALUE
Environment	Production

- In the **Tagrg** resource group **Overview** section, the **Tags** section now has the tag Name:Value pair of **Environment: Production** present

Subscription (change) : Visual Studio Ultimate with MSDN
Subscription ID :
Tags (change) : Environment : Production

NAME	TYPE	LOCATION
vmtag1	Virtual machine	West Europe
vmtag1_OsDisk_1_b04fc039779a4261b9a...	Disk	West Europe

3. Open up the virtual machine resource and in the **Overview** pane note that the tags assigned to the resource group are **not** present in the resource beneath it.

Resource group (change) : tagrg
Status : Running
Location : West Europe
Subscription (change) : Visual Studio Ultimate with MSDN
Subscription ID :
Tags (change) : Click here to add tags

Computer name	Operating system	Size
vmtag1	Windows (Windows Server 2019 Datacenter)	Standard DS1 v2 (1 vcpus, 3.5 GiB memory)
		Public IP address : 104.214.224.40
		Private IP address : 10.0.0.4
		Virtual network/subnet : vmtag1VNET/vmtag1Subnet
		DNS name : Configure

Bulk assign tags to resources

1. Return to the resource group **tagrg** check the checkboxes beside all resources listed under the resource group by clicking on the **NAME** checkbox then click the **Assign Tags** button

Subscription (change) : Visual Studio Ultimate with MSDN
Subscription ID : 6e9a285a-37ea-40e6-b2fc-28539051852e
Tags (change) : Environment : Production

NAME	TYPE	LOCATION
vmtag1	Virtual machine	West Europe
vmtag1_OsDisk_1_b04fc039779a4261b9a...	Disk	West Europe
vmtag1NSG	Network security group	West Europe
vmtag1PublicIP	Public IP address	West Europe
vmtag1VMNic	Network interface	West Europe
vmtag1VNET	Virtual network	West Europe

2. In the **Tags** pane enter the values below, click **Save** and then **Close**

- **Name:** Department

- **Value:** IT

and

- **Name:** Environment

- **Value:** Production

The screenshot shows the 'Tags' pane in the Azure portal. At the top, there's a header with 'Assign tags to 6 resources', a 'Save' button (which is highlighted with a red box), and a 'Delete all' link. Below the header, a descriptive text says 'Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.' followed by a 'Learn more' link. The main area displays a table with columns 'NAME' and 'VALUE'. Two rows have been added: 'Department' with 'IT' and 'Environment' with 'Production'. Both rows have a red box around them. Below the table, there's a list of resources ready to be tagged, each with a '1 to be added' link and a delete icon. The resources listed are: vmtag1 (Virtual machine), vmtag1_OsDisk_1_b04fc039779a4261b9a... (Disk), vmtag1NSG (Network security group), and vmtag1PublicIP (Public IP address). At the bottom left is a 'Close' button, which is also highlighted with a red box.

3. Open up the virtual machine resource and note the presence of the two tags **Department:IT** and **Environment:Production**

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Azure Portal interface for a virtual machine named 'vmtag1'. The left sidebar includes options like 'Create a resource', 'Home', 'Dashboard', and 'All services'. The main area has tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. Under 'Settings', there are sections for Networking, Disks, Size, Security, Extensions, Continuous delivery (Preview), Availability set, Configuration, Identity, Properties, and Locks. The 'Tags' section is highlighted with a red box. It shows a list of tags: 'Resource group (change) : tagrg', 'Status : Running', 'Location : West Europe', 'Subscription (change) : Visual Studio Ultimate with MSDN', 'Subscription ID : ', 'Computer name : vmtag1', 'Operating system : Windows (Windows Server 2019 Datacenter)', 'Size : Standard DS1 v2 (1 vcpu, 3.5 GB memory)', 'Public IP address : 104.214.224.40', 'Private IP address : 10.0.0.4', 'Virtual network/subnet : vmtag1VNET/vmtag1Subnet', and 'DNS name : Configure'. Below this, a 'Tags (change)' section shows filters for 'Department : IT' and 'Environment : Production'. A time range selector shows 'Show data for last: 1 hour, 6 hours, 12 hours, 1 day, 7 days, 30 days'. Two performance charts are displayed: 'CPU (average)' and 'Network (total)'. The CPU chart shows usage spikes between 10:20 PM and 11:15 PM. The Network chart shows traffic spikes between 10:20 PM and 11:15 PM, with values ranging from 0B to 143.05MB.

View all resources with a specific tag

1. In the azure Portal go to **All Services** type the text tags in the search box. The **Tags** service appears and you can open it.

The screenshot shows the 'All services' search results in the Azure Portal. The left sidebar includes 'Create a resource', 'Home', 'Dashboard', and 'All services'. The main area shows a search bar with 'tags' and a list of services categorized under 'Everything'. The 'Tags' service is highlighted with a red box. Other categories listed include General, Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, and AI + machine learning. To the right, there's a note about 'Azure Cosmos DB Keywords datastore'.

2. In the **Tags** pane a number of tags are listed. To view all resources with a specific tag, click the **Name:Value** pair that you want to view resources for i.e. click **Department:IT**

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more](#)

Subscriptions: 2 of 5 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

Filter items... 2 subscriptions

TAGS

Department : IT
Environment : Production
ms-resource-usage : azure-cloud-shell

- After clicking on the Name Value pair **Department:IT**, in the resultant **Department:IT** pane, all resources with this *Name:Value* pair are listed

Department : IT

Tag

Refresh

Subscriptions: 2 of 5 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

Filter items... 2 subscriptions

NAME	SUBSCRIPTION
vmtag1_OsDisk_1_b04fc039779a4261b9ad2d7	Visual Studio Ultimate with MSDN
vmtag1	Visual Studio Ultimate with MSDN
vmtag1VMNic	Visual Studio Ultimate with MSDN
vmtag1NSG	Visual Studio Ultimate with MSDN
vmtag1PublicIP	Visual Studio Ultimate with MSDN
vmtag1VNET	Visual Studio Ultimate with MSDN

Note: For quick access, you could pin the **Tags** service view to the dashboard.

Delete tags

- In the resource group you created earlier i.e. **tagrg**, open the virtual machine and click on the **Tags** section. In the resultant **Tags** pane we have an option to **Delete All** tags, or click the *dustbin icon* beside individual *Name:Value* pairs, to delete individual tags. Click **Delete All** then **click Save** and **Close**

vmtag1 - Tags

Tags

NAME	VALUE
Department	: IT
Environment	: Production

2. In the virtual machine **Overview** pane note that the values for **Tags** has returned of the link stating **Click here to add tags.**, indicating there are no tags now present.

vmtag1 - Virtual machine

Overview

Tags (change) : Click here to add tags

Resource group (change) : tagrg	Computer name : vmtag1
Status : Running	Operating system : Windows (Windows Server 2019 Datacenter)
Location : West Europe	Size : Standard DS1 v2 (1 vcpus, 3.5 GiB memory)
Subscription (change) : Visual Studio Ultimate with MSDN	Public IP address : 104.214.224.40
Subscription ID : 6e9a285a-37ea-40e6-b2fc-28539051852e	Private IP address : 10.0.0.4
	Virtual network/subnet : vmtag1VNET/vmtag1Subnet
	DNS name : Configure

Congratulations! You have created Azure resources to allow us to apply Tags to them, you then viewed the tags for a resource and a resource group, and then added Tags. You then bulk assigned tags to resource groups and resources and viewed all resources with a specific tag. You finally deleted assigned tags.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Video: Azure Monitor



<https://www.youtube.com/watch?v=D8hf43a4tJE>

Azure Monitor

Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.



What data does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- *Application monitoring data*: Data about the performance and functionality of the code you have written, regardless of its platform.
- *Guest OS monitoring data*: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.
- *Azure resource monitoring data*: Data about the operation of an Azure resource.
- *Azure subscription monitoring data*: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- *Azure tenant monitoring data*: Data about the operation of tenant-level Azure services, such as Azure Active Directory.

Diagnostic settings

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data.

- *Activity Logs* record when resources are created or modified.

- Metrics tell you how the resource is performing and the resources that it's consuming.

You can extend the data you're collecting into the actual operation of the resources by enabling **diagnostics** and adding an agent to compute resources. Under the resource settings you can enable Diagnostics

- Enable guest-level monitoring*
- Performance counters*: collect performance data
- Event Logs*: enable various event logs
- Crash Dumps*: enable or disable
- Sinks*: send your diagnostic data to other services for more analysis
- Agent*: configure agent settings

Note: You can read more about Azure Monitor the page [Azure Monitor⁴¹](#)

Walkthrough-Monitor VMs using Azure Monitor

In this walkthrough task we will create Azure resources to provide some resources to us to monitor, then we will view the default available monitoring data from within the virtual machine resource data and then from within Azure Monitor. We will then view some of the monitoring options available in Azure Monitor.

We will then create a Log Analytics workspace, and enable Insights in our virtual machine, we will review the retrieved data in Azure Monitor. Then we will enable diagnostic settings in the virtual machine and query and analyze virtual machine logs in Log Analytics workspace and Azure Monitor Logs.

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 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 today⁴²](#) webpage.

Steps

Create Azure resources to allow us to monitor them

Firstly, we will deploy some resources to Azure to provide us with some resources to manage. If you have resources available from a previous deployment, you can use those instead of deploying new ones.

- Sign into the Azure Portal and click on the **Cloud Shell** icon in the top right hand corner



- The **Cloud Shell** is launched in the bottom of the browser window.

⁴¹ <https://azure.microsoft.com/en-us/services/monitor/>

⁴² https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

The screenshot shows the Azure Cloud Shell interface. It displays the following text:

```

PowerShell | ⚡ ? 🚂 🛡 { } ⚙
Requesting a Cloud Shell. Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: Manage Azure Active Directory: Get-Command -Module AzureAD*

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:\

```

3. Create a resource group into which we will place our resources by running the following Azure CLI command. You can copy and paste the command from the below directly into the Cloud Shell console, then press **Enter** to run the command. This command will run fine in either **powershell** or **bash** console.

```
az group create \
    --name monitorrg \
    --location westeurope
```

```

Azure:/
PS Azure:\az group create \
>>   --name monitorrg \
>>   --location westeurope
{
  "id": "/subscriptions//resourceGroups/monitorrg",
  "location": "westeurope",
  "managedBy": null,
  "name": "monitorrg",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": null
}
Azure:/
PS Azure:\

```

4. Run the below Azure CLI command to create a virtual machine. Again, you can copy and paste the command from below directly into the Cloud Shell console and press **Enter** to run it.

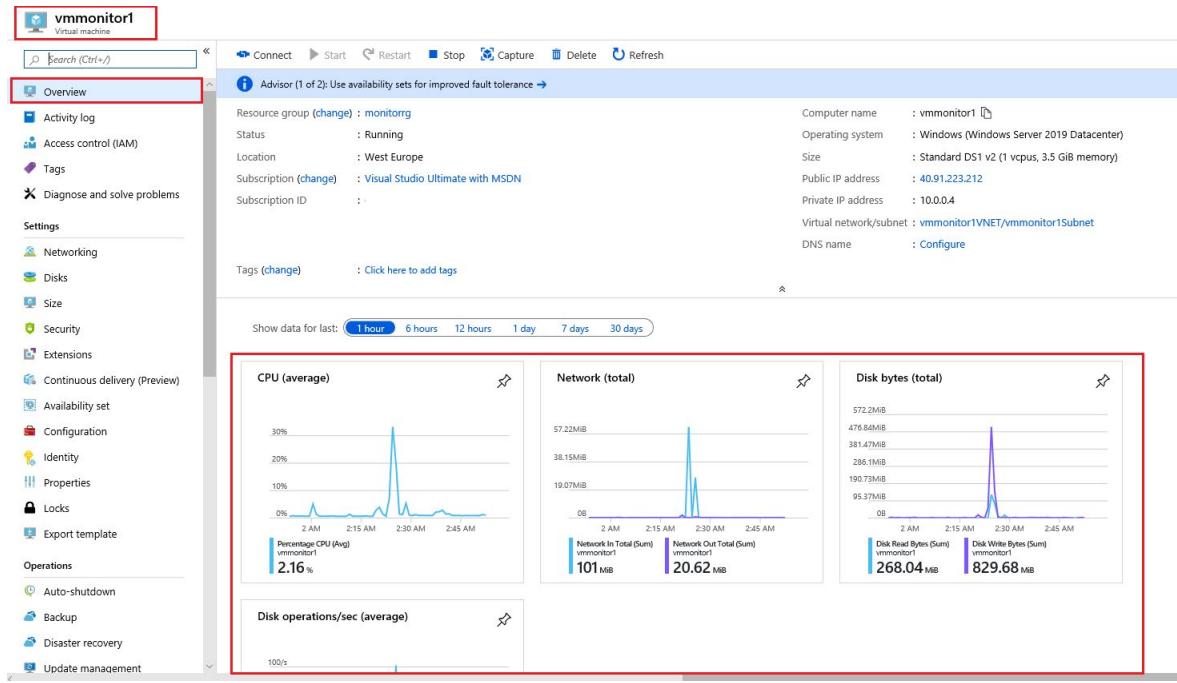
```
az vm create \
    --name vmmonitor1 \
    --resource-group monitorrg \
    --image Win2019Datacenter \
    --location westeurope \
    --admin-username azureuser \
    --admin-password Password0134!
```

```
Azure:/
PS Azure:> az vm create \
>>   --name vmmonitor1 \
>>   --resource-group monitorrg \
>>   --image Win2019Datacenter \
>>   --location westeurope \
>>   --admin-username azureuser \
>>   --admin-password Password0134!
{
  "fqdns": "",
  "id": "/subscriptions/-----/resourceGroups/monitorrg/providers/Microsoft.Compute/virtualMachines/vmmonitor1",
  "location": "westeurope",
  "macAddress": "00-0D-3A-21-D4-23",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "40.91.223.212",
  "resourceGroup": "monitorrg",
  "zones": ""
}
Azure:/
PS Azure:> []
```

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. You can close the Azure Cloud Shell once it is complete.

View default available monitoring data within the virtual machine resource

1. Go to the resource group you just created i.e. **monitorrg**, then open the virtual machine and go to the **Overview** pane



Note the presence of default metric data for **CPU**, **Network**, **Disk bytes** and **Disk operations/sec** present by default in the virtual machine resource.

2. Now click on the **Activity log** and note the presence of operations listed i.e. **Activity logs** record when resources are created or modified. These are subscription level events in Azure, written to an **Activity log**.

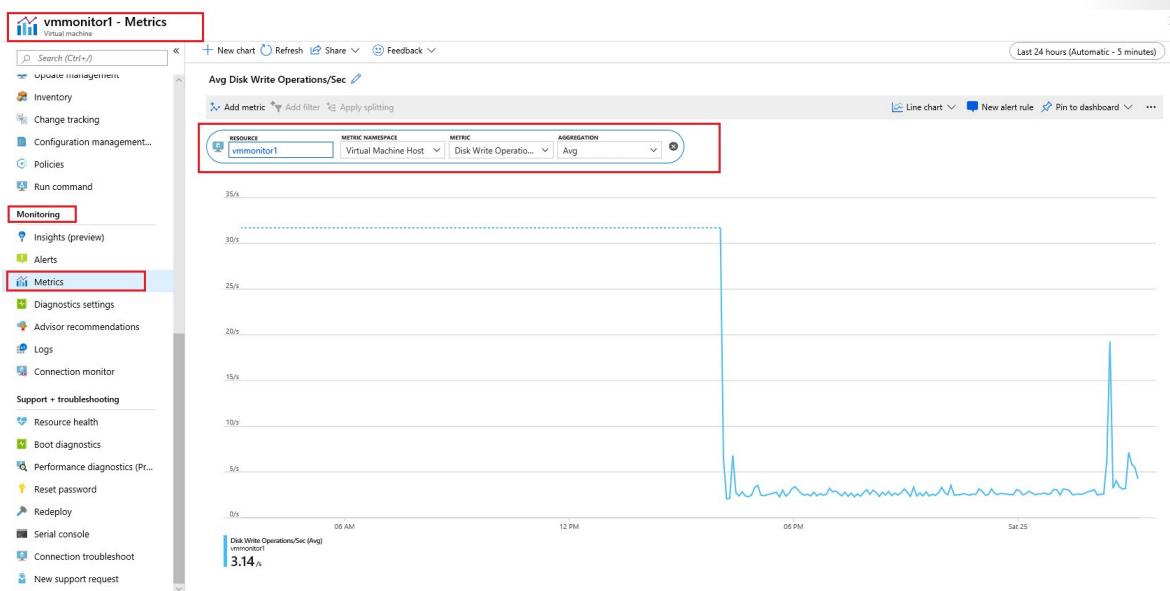
MCT USE ONLY. STUDENT USE PROHIBITED

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Create or Update Virtual Machine Extension	Accepted	7 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_jelly@hotmail.c...
Create or Update Virtual Machine Extension	Succeeded	23 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	Windows Azure Security R...
Write Tasks	Succeeded	38 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	
AuditIfNotExists	Succeeded	3 h ago	Fri May 24 2...	Visual Studio Ultimate with MSDN	Microsoft Azure Policy Ins...

Subscription level events in Azure are written to an **Activity log** that you can view from the Azure Monitor menu

- Now click on the **Monitoring > Metrics** and select the following

- Resource:** < your virtual machine i.e. vmmonitor1 >
- Metric Namespace:** virtual machine host
- Metric:** Disk Write Operations/Sec (or any other metric you wish to view)
- Aggregation:** Avg



Note: **Metric** data tells you how the resource is performing and the resources that it's consuming. Both the **Activity log** and some **Metric** data is available by default and visible from within the resource being monitored i.e. the virtual machine in this case. There not be a lot of data to display for the virtual machine at this point as it has just been installed and no actions have been performed by or to the virtual machine.

View default available monitoring data for resources using Azure Monitor

The default metric data is also available for view and analysis via Azure Monitor.

- In the Azure Portal on the left hand side select **Monitor**

Monitor - Overview

Monitor & Visualize Metrics
Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

Query & Analyze Logs
Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

Setup Alert & Actions
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Quick Starts

Learn how to collect data from...	Learn how to monitor...	Learn how to onboard...
Azure VMs	Azure Web Apps	ASP.NET Apps from Visual Studio
Linux Computers	Azure Cloud Services	Node.js Apps
Windows Computers	Docker Apps	Java Apps from Eclipse
Azure Kubernetes	Azure Functions	Mobile Apps from VS App Center
Docker & Windows Containers	Service Fabric Apps	

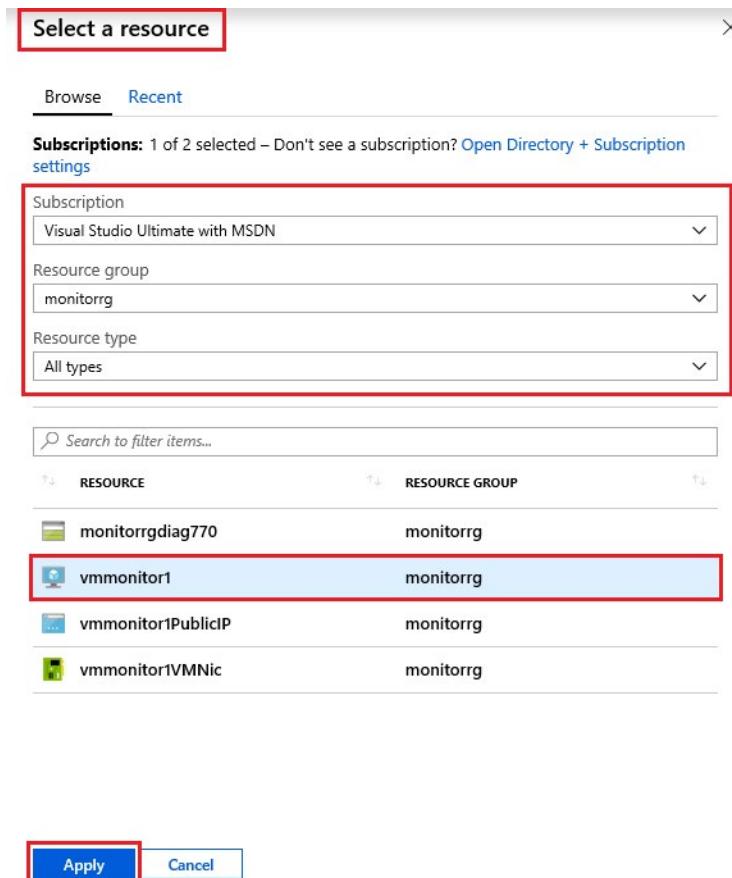
2. Now click on the **Activity log** and note the presence of operations listed. There are more **Activity log** operations present here, as they are being pulled at subscription level, not just the single resource level, the virtual machine, that we saw earlier.

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
► Audit	Succeeded	18 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	Microsoft Azure Policy Ins...
► List Storage Account Keys	Succeeded	24 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights
► List Storage Account Keys	Succeeded	24 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights
► Create new OMS solution	Succeeded	25 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Update insights component	Succeeded	32 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Create Deployment	Succeeded	35 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Validate Deployment	Succeeded	36 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Create Deployment	Succeeded	42 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Validate Deployment	Succeeded	42 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► Update resource group	Succeeded	42 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	eamonn_kelly@hotmail.c...
► List Storage Account Keys	Succeeded	46 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights
► List Storage Account Keys	Succeeded	46 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights
► List Storage Account Keys	Succeeded	49 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights
► Create or Update Virtual Machine Exte...	Succeeded	49 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	Windows Azure Security R...
► List Storage Account Keys	Succeeded	51 min ago	Sat May 25...	Visual Studio Ultimate with MSDN	AzureApplicationInsights

3. Now click on the **Metrics**, click **select a resource** and in the resultant **select a resource** pane and fill in the data as below and click **Apply**

- **subscription:** < select your subscription >

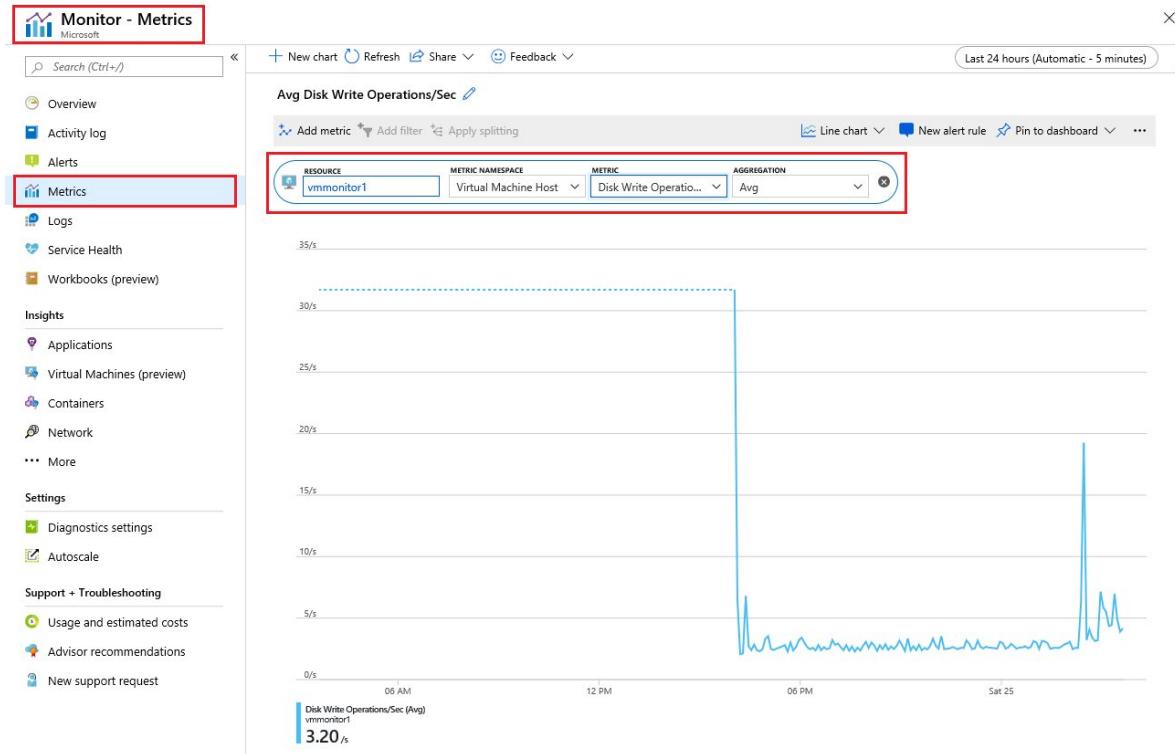
- **resource group:** < select the resource group you created earlier i.e. monitorrg >
- **resource type:** All types
- **Resource:** < select the virtual machine i.e. vmmonitor1 >



Note: Metric data tells you how the resource is performing and the resources that it's consuming

4. Fill in the remainder of the fields as below

- **Resource:** < your virtual machine i.e. **vmmonitor1** should now be selected >
- **Metric Namespace:** Virtual Machine Host
- **Metric:** Disk Write Operations/Sec
- **Aggregation:** Avg



Note: Both **Activity Log** and **Metric** data is available for resources within the Azure Monitor pane as well as via the individual resource pane. Most resources will write operational information to a diagnostic log that you can forward to different locations. Azure Monitor Logs is a log data platform that collects activity logs and diagnostic logs along with other monitoring data to provide deep analysis across your entire set of resources.

View Monitoring options within Azure Monitor

In Azure Monitor we are able to monitor all resource types, and we also have available some default scenarios configured for us to use. Take a moment to have a quick look through them. The data available within these requires collection and analysis of logs beyond the default metrics and additional configuration is required.

1. In Azure Monitor go to **Insights > Applications**

Monitor - Applications

Subscriptions: 1 of 2 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
No results.				

Insights

Applications

No Application Insights app to display
Try changing your filters if you don't see what you're looking for.
[Create Application Insights apps](#)

2. In Azure Monitor go to **Insights > Virtual machine (Preview)**

Monitor - Virtual Machines (preview)

Get Started **Health** **Performance** **Map**

Get more visibility into the health and performance of your virtual machines

Azure Monitor for VMs monitors your Azure virtual machines (VM) at scale by analyzing the performance and health of your Windows and Linux VMs, including their different processes and interconnected dependencies on other resources and external processes. [Learn more](#)

Onboard insights for a single VM
Visit the Azure VM resource blade and go to Insights (preview) in the Monitoring menu.
You will need contributor access on the VM, and Log Analytics contributor access on the Resource Group of your chosen Log Analytics workspace.

Onboard at scale with Azure Policy
Use Azure Policy to ensure all VMs and VM Scale Sets in your subscriptions and resource groups are configured for monitoring.
You will need role access as Owner or User Access Administrator for the selected subscriptions, and you will need to configure your Log Analytics workspace.

Onboard non-Azure computers
Use the Log Analytics (OMS) Agent to extend Azure Monitor capabilities to computers running outside of Azure, including resources running on-premises and in other clouds.

[Learn more](#)

3. In Azure Monitor go to **Insights > Container**

4. In Azure Monitor go to **Insights > Network**. This uses the **Network Watcher** service, which is a regional service that enables you to monitor and diagnose conditions at a network level.

NAME	REGION	STATUS
Visual Studio Ultimate with MSDN	28 regions	Partially enabled
	West US	Enabled
	East US	Disabled
	North Europe	Disabled
	West Europe	Enabled
	East Asia	Disabled
	Southeast Asia	Disabled
	North Central US	Disabled
	South Central US	Disabled
	Central US	Disabled
	East US 2	Disabled
	Japan East	Disabled

Note: Network Watcher provides for investigating and analyzing areas such as network **Topology**, **Packet capture**, **IP flow**, **Virtual Network Gateway** and **Connection** troubleshooting as well as other areas.

Create an Azure Monitor log workspace (also known as Log Analytics workspace)

Log data collected by Azure Monitor is stored in a Log Analytics workspace. It collects telemetry from a variety of sources and uses the **Kusto⁴³** query language used by **Data Explorer⁴⁴** to retrieve and analyze data.

⁴³ <https://docs.microsoft.com/en-us/azure/kusto/query/>

⁴⁴ <https://docs.microsoft.com/en-us/azure/data-explorer/data-explorer-overview>

Once the obtained data is stored and organized, we can then monitor, analyze, visualize and create alerts for that data.

We create a *workspace* to allow us to store and process the data collected. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular workspace. You require a Log Analytics workspace if you intend on collecting data from, Azure resources in your subscription, On-premises computers or Diagnostics or log data from Azure storage.

Note: You will see references to **Azure Monitor logs** in documentation as well as **Log Analytics**

1. In the Azure portal, click **All services**, then in the search box type **Log Analytics**. As you begin typing, the list filters based on your input, and select **Log Analytics workspaces**.

The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the text "log analyt". Below the search bar, the results are displayed under the heading "All services". The "Log Analytics workspaces" item is highlighted with a red box. Other items listed include "Everything", "General", "Compute", "Networking", "Storage", "Web", "Mobile", "Containers", "Databases", and "Analytics". To the right of the search results, there are sections for "HDInsight clusters", "Machine Learning service workspaces", and "Cognitive Services".

2. Click **Create log analytics workspace**. If there is a default workspace present already, click the **+ Add** button instead.

The screenshot shows the "Log Analytics workspaces" blade in the Azure portal. The title bar says "Log Analytics workspaces" and "eamonnkelly@hotmail (Default Directory)". Below the title, there are buttons for "+ Add", "Edit columns", "Refresh", and "Assign tags". A message "Subscriptions: All 2 selected - Don't see a subscription? Open Directory + Subscription settings" is displayed. There are several filter buttons: "Filter by name...", "All subscriptions", "All resource gro...", "All locations", "All tags", and "No grouping". Below these, it says "0 items" and lists columns: "NAME", "RESOURCE GROUP", "LOCATION", and "SUBSCRIPTION". A message "No results." is shown. At the bottom, a large "Create log analytics workspace" button is highlighted with a red box.

3. In the **Log Analytics workspace** pane enter the following values and click **OK**

- **Create new:** < select the radio button to indicate Yes >
- **Log Analytics workspace:** azmon1-lawrkspc

- **Subscription:** < select your own subscription >
- **Resource group:** select **Use Existing** and specify the resource group you created earlier that contains your virtual machine i.e. **monitorrg**.
- **Location:** < a data center near you that supports **Log Analytics** - Not all regions support **Log Analytics**, to see supported regions, go to the page **Products available by region**⁴⁵ and search for Azure Monitor from the Search for a product field.
- **Pricing tier:** Per GB (Standalone) or Per GB (2018), depending on which is available to you - see the page **Azure Monitor pricing**⁴⁶ for more details on pricing.

Note: We have now created somewhere for the log data to be collected and organized. It will take 1 to 2 minutes to create the Log Analytics workspace and it should display in the Log Analytics workspace pane once created. You may need to refresh the workspace pane to see it, if it is not present after completion.

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
azmon1-lawrkspc	monitorrg	West Europe	Visual Studio Ultimate with MSDN
DefaultWorkspace-6e9a285a-37ea...	DefaultResourceGroup-WEU	West Europe	Visual Studio Ultimate with MSDN

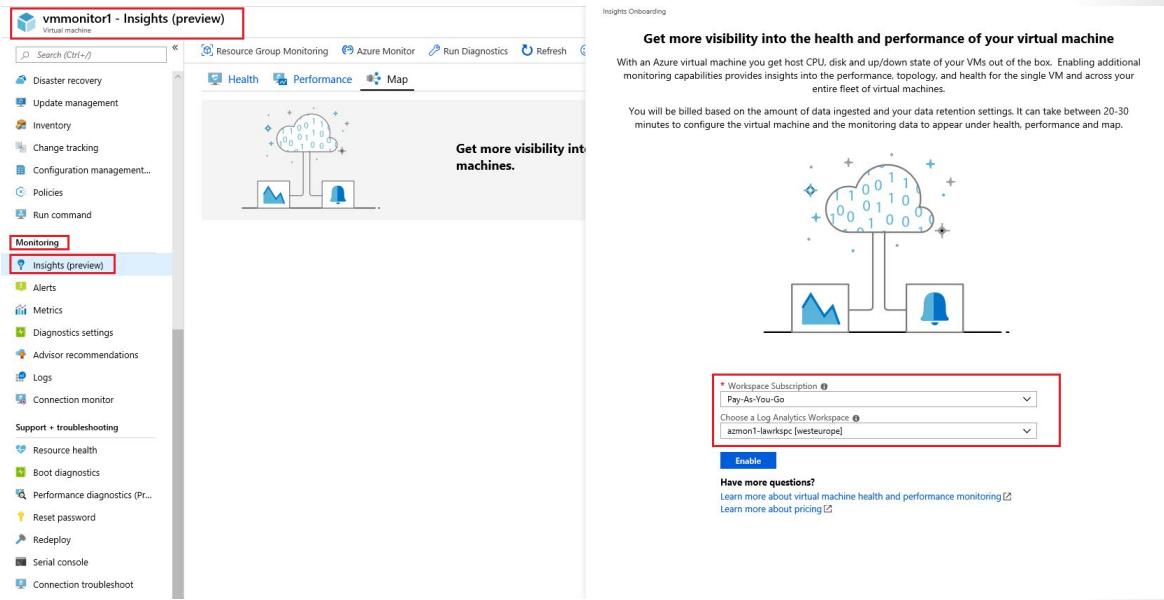
Enable Insights in the virtual machine resource

To allow us to view monitoring data in Azure Monitor for our virtual machine, outside of the core metrics that are available for CPU, Network and Disk metrics, we need to enable the **Insights** settings within our virtual machine. Enabling these additional monitoring capabilities provides insights into the performance, topology, and health for one or many virtual machines. There are several options available to us to do that for example, using ARM templates, PowerShell or Azure Policy, but we will enable it directly in the resource itself, in the Azure portal.

1. Go to the resource group you created earlier i.e. **monitorrg**, then open the virtual machine i.e. **vmonitor1**, and go to **Monitoring > Insights (Preview)**. The **Azure Monitor - Insights Onboarding** pane automatically launches read the messages that appear, fill in the fields as below, then click **Enable** and click the **Try Now** button.
 - **Workspace subscription:** < your subscription >
 - **Choose a Log Analytics Workspace:** azmon1-lawrkspc (the Log Analytics workspace you created earlier)

⁴⁵ <https://azure.microsoft.com/en-us/global-infrastructure/services/>

⁴⁶ <https://azure.microsoft.com/en-us/pricing/details/monitor/>



Note: If the **Azure Monitor - Insights Onboarding** pane does not launch automatically, you can click the **Try now** button on the **Insights (preview)** pane to launch it.

It will take 2 to 3 minutes to complete the deployment.

2. You will receive a message saying deployment was successful and then a message will display on the **Azure Monitor - Insights Onboarding** stating that **Monitoring data is being collected and routed to Insights and that it can take up to 20 minutes to arrive.....**, additional messages may also display then as the process progresses, stating the **..virtual machine is already collecting data... and to return shortly**, and possibly others. With a simple single VM configuration as ours, it may take approx. 10 minutes.

Azure Monitor
Insights Onboarding

Monitoring data is being collected and routed to Insights. It can take up to 20 minutes to arrive. Please try again in a few minutes. [Workspace ID: /subscriptions/6e9a285a-37ea-40e6-b2fc-28539051852e/resourcegroups/defaultresourcegroup-weu/providers/microsoft.operationalinsights/workspaces/defaultworkspace-6e9a285a-37ea-40e6-b2fc-28539051852e-weu]

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance, topology, and health for the single VM and across your entire fleet of virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 20-30 minutes to configure the virtual machine and the monitoring data to appear under health, performance and map.



Have more questions?
[Learn more about virtual machine health and performance monitoring](#)

Note: As stated, It can take up to 20 minutes for log data to appear, while it is collected and organized. If there is no data present at the moment you can proceed through the next series of tasks below and return to this section later, when it is completed and ready to view the retrieved data.

3. Data will eventually display and be available from within this **Insights (preview)** pane as per the below screenshot.

MCT USE ONLY. STUDENT USE PROHIBITED

DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPS READ	P95 IOPS WRITE	P95 IOPS TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL	P95 LATENCY READ (ms)	P95 LATENCY WRITE (ms)
C:	126.51	8%	9.28	6.63	16.13	0.24	0.13	0.41	5.89	0.98
D:	7	13%	3.68	3.7	4.91	0.02	0.71	0.71	0.37	12.05
HarddiskVolume1	0.49	7%	0	0	0	0	0	0	0	0
Total	133.99	8%	10.98	10.2	16.98	0.26	0.73	0.73	5.89	6.12

View Insights data in Azure Monitor

1. Return to **Azure Monitor** and select **Virtual Machines (preview)** and go to the **Health** tab and ensure your subscription and resource group are selected, then view the health data for the virtual machine.

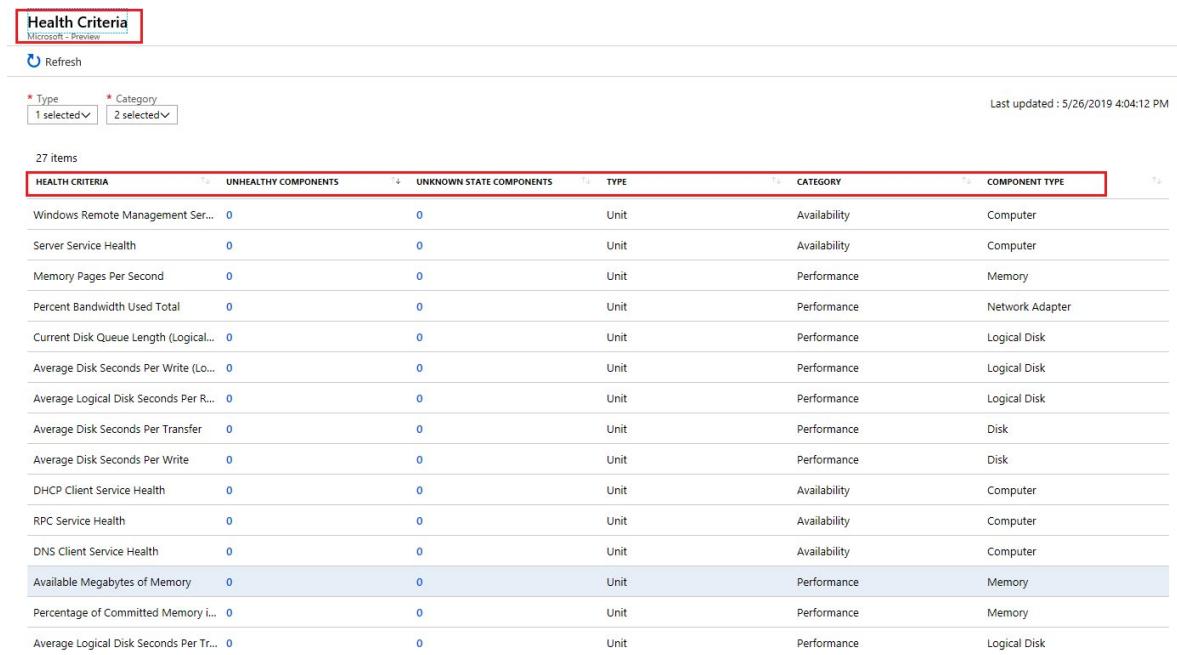
OPERATING SYSTEM	OS TYPE	VM COUNT	Critical	Warning	Healthy	Unknown
Microsoft Windows Server...	Windows	1	0	0	1	0

COMPONENTS	Critical	Warning	Healthy	Unknown
CPU	0	0	1	0
Disk	0	0	1	0
Memory	0	0	1	0
Network	0	0	1	0

Note: It can take up to 20 minutes for log data to appear, if there is no data present at the moment you can proceed to the next task below and return to this section later, when complete to view the

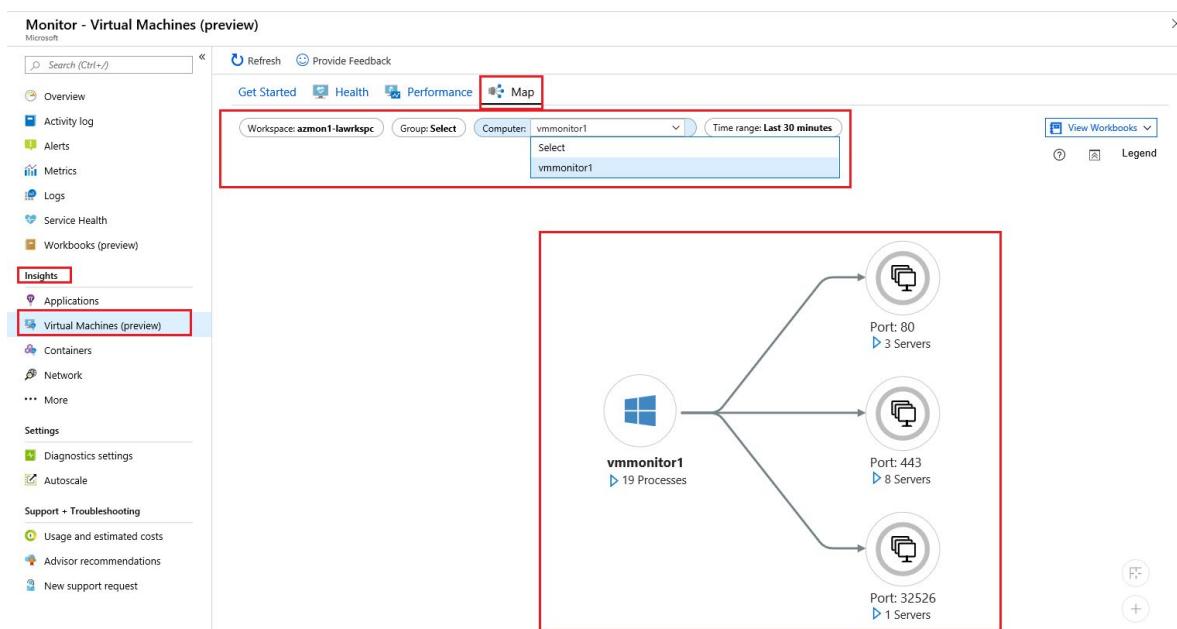
retrieved data. With a simple single VM configuration as ours however, it should take approx. 10 minutes.

- Click on the link **View all health criteria** and view the listed health criteria and the state of the various listed components.



The screenshot shows a table titled 'Health Criteria' with the following columns: HEALTH CRITERIA, UNHEALTHY COMPONENTS, UNKNOWN STATE COMPONENTS, TYPE, CATEGORY, and COMPONENT TYPE. The table lists various system metrics such as Windows Remote Management Service, Server Service Health, Memory Pages Per Second, and Percent Bandwidth Used Total. Most metrics show 0 unhealthy or unknown components. The 'Available Megabytes of Memory' row is highlighted in blue. The table has a red border around its top edge.

- Select the **Performance** and **Map** tabs also, and view the data that's present there. You will need to specify a specific resource group and resource to view data for in those tabs. If you have time you should also click deeper into the various components listed under these tabs to view the data and detail.

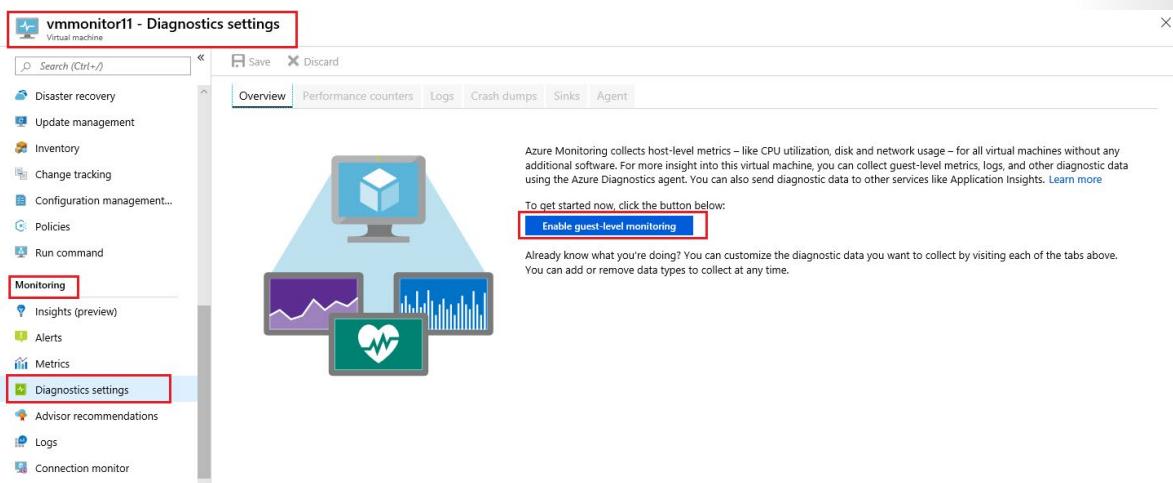


Enable Diagnostic settings in virtual machine

As mentioned earlier, Azure Monitoring collects host-level metrics like CPU utilization, disk and network usage, for all virtual machines without any additional software. For more insight into this virtual machine, you can also collect guest-level metrics, logs, and other diagnostic data using the **Azure Diagnostics agent**. You can also then send diagnostic data to other services like **Application Insights**. We will now enable collection of **Diagnostic data**.

Extend the data you're collecting into the actual operation of the resources by enabling diagnostics and adding an agent to compute resources. This will collect telemetry for the internal operation of the resource and allow you to configure different data sources to collect logs and metrics from Windows and Linux guest operating system.

1. Return to the resource group you created earlier i.e. **monitorrg**, then open the virtual machine i.e. **vmmonitor1**, and go to **Monitoring > Diagnostic settings** and click the **Enable guest-level monitoring** button. It can take approx. 2 to 3 minutes to complete.



2. Once enabled, on the **Overview** tab, details about **Performance counters** and **Event Logs, Crash Dumps, Sinks, Agents** etc. are listed and you are able to configure them within the VM, to decide what type of data you wish to collect.

The screenshot shows the 'Diagnostics settings' page for a virtual machine named 'vmmonitor11'. The left sidebar under 'Monitoring' has several tabs: Insights (preview), Alerts, Metrics, and **Diagnostics settings**. The 'Diagnostics settings' tab is highlighted with a red box. The main content area has a tab bar with 'Overview' (highlighted with a red box), Performance counters, Logs, Crash dumps, Sinks, and Agent. The 'Overview' tab displays sections for 'Performance counters' (collecting data for CPU, Memory, Disk, Network) and 'Event logs' (collecting data for Application, Security, System logs). It also includes sections for 'Directories', 'Crash dumps', and 'Sinks'.

Take a moment to click on the various tabs available i.e. **Performance counters**, **Logs**, **Crash Dumps**, **Sinks** and **Agent** and view their content and the items we can configure and collect.

Query and Analyze virtual machine logs in Log Analytics workspace and Azure Monitor Logs

Now we will access the Log Analytics workspace and query and analyze some of the log data that we configured earlier to be collected.

1. In the Azure portal, click **All services**, then in the search box type **Log Analytics**. As you begin typing, the list filters based on your input, and select **Log Analytics workspaces**.

The screenshot shows the Microsoft Azure portal search results for 'log analyt'. The search bar contains 'log analyt'. Below it, the 'Log Analytics workspaces' item is highlighted with a red box. Other items listed include 'Cognitive Services', 'Monitor', 'HDInsight clusters', and 'Machine Learning service workspaces'. The left sidebar shows navigation options like 'Create a resource', 'Home', 'Dashboard', and 'All services'.

2. From the list of workspaces displayed open the Log Analytics workspace we created earlier i.e. **azmon-lawrkspc**

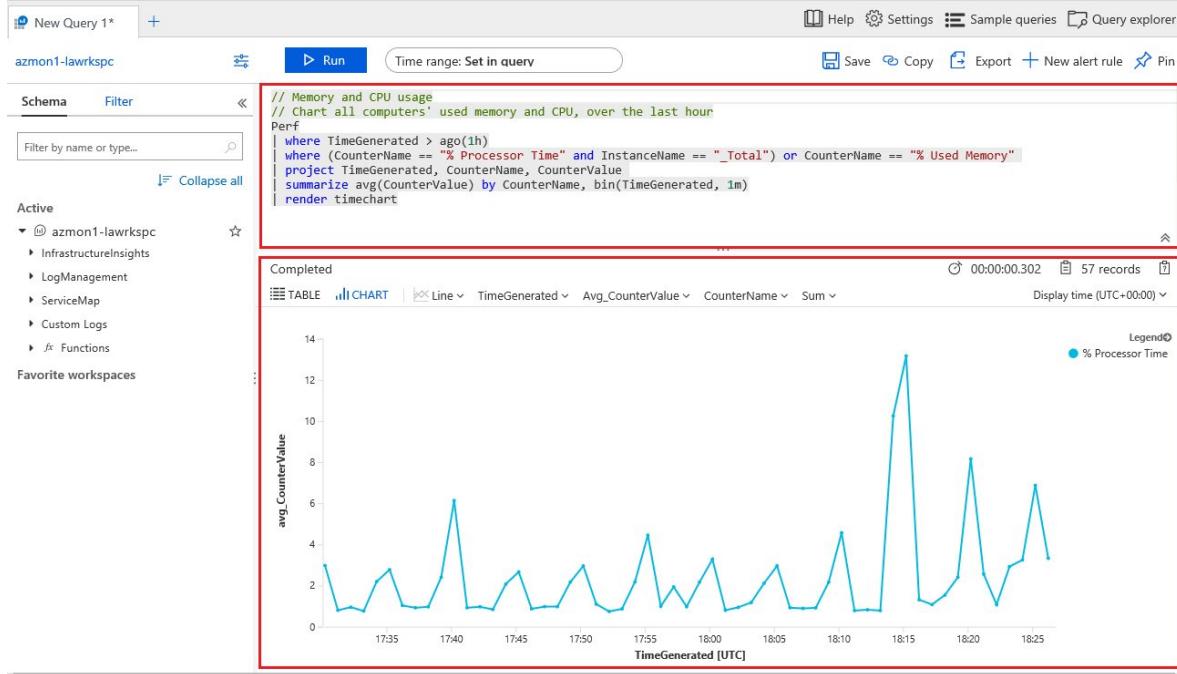
MCT USE ONLY STUDENT USE PROHIBITED

The screenshot shows the 'Log Analytics workspaces' page in the Azure portal. At the top, it displays the workspace name 'earmonnkelly@hotmail (Default Directory)'. Below this, there are buttons for 'Add', 'Edit columns', 'Refresh', and 'Assign tags'. A message at the top says 'Subscriptions: 1 of 2 selected – Don't see a subscription? Open Directory + Subscription settings'. There are filters for 'Filter by name...', 'Pay-As-You-Go', 'All resource groups', 'All locations', 'All tags', and 'No grouping'. A table below shows one item: 'azmon1-lawrkspc' under 'monitorrg', located in 'West Europe' with 'Pay-As-You-Go' as the subscription.

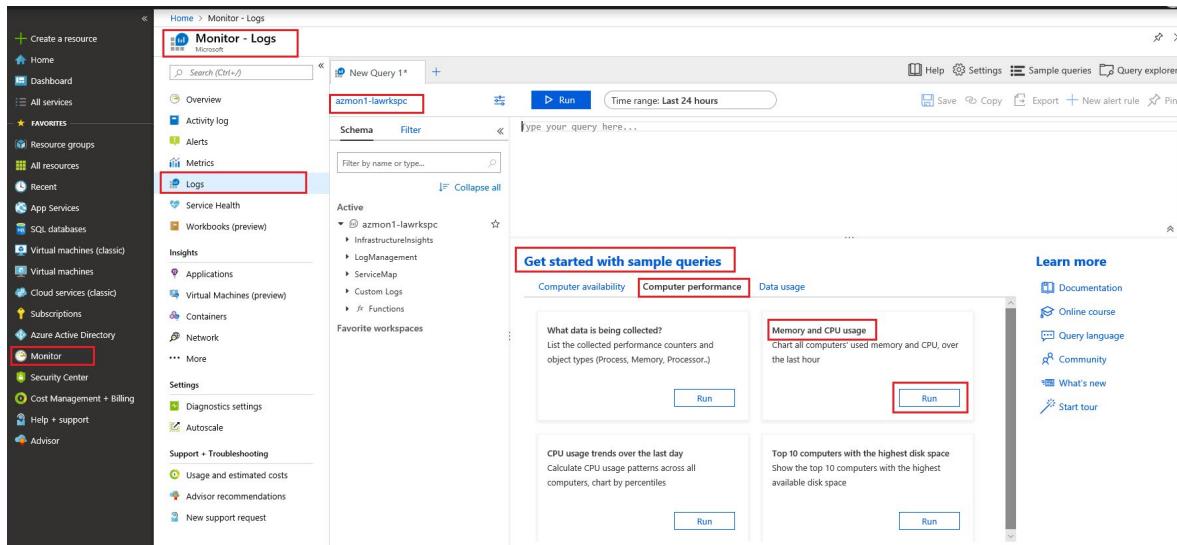
3. Go to **General > Performance** and select **Logs** and under **Getting started with sample queries** click on **Computer Performance** and under **Memory and CPU usage** click **Run**

The screenshot shows the 'azmon1-lawrkspc - Logs' workspace. On the left, the navigation menu is open, with 'Logs' highlighted. The main area shows a 'Get started with sample queries' section. Under 'Computer performance', there is a box titled 'Memory and CPU usage' which includes the text: 'Chart all computers' used memory and CPU, over the last hour'. Below this box is a 'Run' button. To the right, there are other sample query cards: 'What data is being collected?' (Run button), 'CPU usage trends over the last day' (Run button), and 'Top 10 computers with the highest disk space' (Run button). On the far right, there is a 'Learn more' sidebar with links to Documentation, Online course, Query language, Community, What's new, and Start tour.

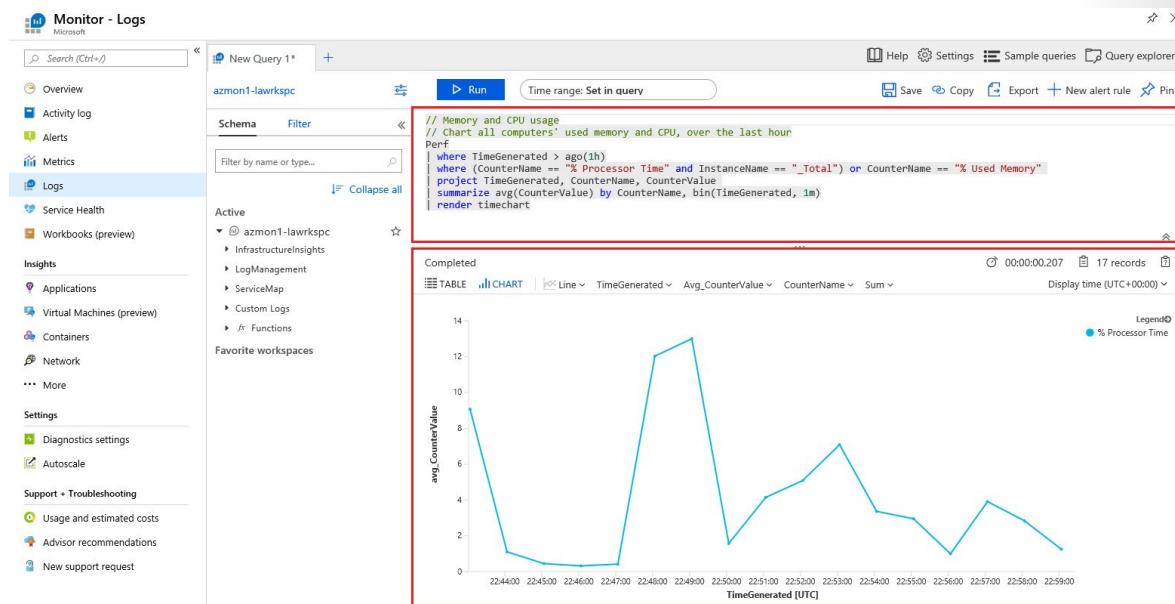
4. The sample query is run, the query is displayed along with the log data output.



- This workspace query and analysis can also be performed directly within **Azure Monitor** and the same results achieved. To do this, in the Azure Portal go to **Monitor**, and in Azure Monitor select **Logs**, and as before under **Getting started with sample queries** click on **Computer Performance** and under **Memory and CPU usage** click **Run**.



- The resultant query displays along with the charted output of the query for you to analyze



If you have time you can browse and run some of the other sample queries available and view the output.

Congratulations! You have created Azure resources to provide some resources to us to monitor, then you viewed the default available monitoring data from within the virtual machine resource data, and the viewed the default available monitoring data from with Azure Monitor. You then viewed some of the monitoring options from within Azure Monitor. You then created a Log Analytics workspace, enabled Insights in your virtual machine and then reviewed the retrieved data in Azure Monitor. You then enabled diagnostic settings in the virtual machine and queried and analyzed virtual machine logs in Log Analytics workspace and Azure Monitor Logs.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Video: Azure Service Health



<https://www.youtube.com/watch?v=xB2wemil7eQ>

Azure Service Health

Azure Service Health is a suite of experiences that provide personalized guidance and support when issues with Azure services affect you. It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved. Azure Service Health can also help you prepare for planned maintenance and changes that could affect the availability of your resources.



Azure Service Health is composed of the following:

- *Azure Status* provides a global view of the health state of Azure services. With Azure Status, you can get up-to-the-minute information on service availability. Everyone has access to Azure Status and can view all services that report their health state.
- *Service Health* provides you with a customizable dashboard that tracks the state of your Azure services in the regions where you use them. In this dashboard, you can track active events such as ongoing service issues, upcoming planned maintenance, or relevant *Health advisories*. When events become inactive, they are placed in your *Health history* for up to 90 days. Finally, you can use the **Service Health** dashboard to create and manage service *Health alerts*, which notify you whenever there are service issues that affect you.
- *Resource Health* helps you diagnose and obtain support when an Azure service issue affects your resources. It provides you details with about the current and past state of your resources. It also provides technical support to help you mitigate problems.

In contrast to Azure Status, which informs you about service problems that affect a broad set of Azure customers, *Resource Health* gives you a personalized dashboard of your resources' health. *Resource Health* shows you times, in the past, when your resources were unavailable because of Azure service problems. It's then easier for you to understand if an SLA was violated.

Together, the Azure Service Health components provide you with a comprehensive view of the health status of Azure, at the level of granularity that is most relevant to you.

Note: You can read more about Azure Service Health on the [Azure Service Health⁴⁷](#) webpage.

Monitoring Applications and Services

Data monitoring is only useful if it improves your visibility of the operations in your computing environment. *Azure Monitor* includes several features and tools that provide valuable insights into your applications, and the other resources they may depend on. Monitoring solutions and features, such as *Application Insights* and *Container Insights*, provide you with a deeper look into different aspects of your application and Azure services.

Azure Monitor features can be organized into four categories, these categories are: *Analyze*, *Respond*, *Visualize* and *Integrate*.

Analyze

- *Application Insights* is a service that monitors the availability, performance, and usage of your web applications, whether they're hosted in the cloud or on-premises. It leverages the powerful data analysis platform in Log Analytics to provide you with deeper insights into your application's operations. Application Insights can diagnose errors, without waiting for a user to report them. Application Insights includes connection points to a variety of development tools, and integrates with Microsoft Visual Studio to support your DevOps processes.

⁴⁷ <https://azure.microsoft.com/en-us/features/service-health/>

- *Azure Monitor for containers* is a service that is designed to monitor the performance of container workloads, which are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). It gives you performance visibility by collecting memory and processor metrics from controllers, nodes, and containers, which are available in Kubernetes through the metrics API. Container logs are also collected.
- *Azure Monitor for VMs* is a service that monitors your Azure VMs at scale, by analyzing the performance and health of your Windows and Linux VMs (including their different processes and interconnected dependencies on other resources, and external processes). Azure Monitor for VMs includes support for monitoring performance and application dependencies for VMs hosted on-premises, and for VMs hosted with other cloud providers.

Integrating any, or all, of these monitoring services with Azure Service Health has additional benefits. Staying informed of the health status of Azure services will help you understand if, and when, an issue affecting an Azure service is impacting your environment. What may seem like a localized problem could be the result of a more widespread issue, and Azure Service Health provides this kind of insight. Azure Service Health identifies any issues with Azure services that might affect your application. Azure Service Health also helps you to plan for scheduled maintenance.

Respond

In addition to allowing you to analyze your monitoring data interactively, an effective monitoring solution must respond proactively to any critical conditions that are identified within the data it collects. This might involve, for example, sending a text or email to an administrator who is responsible for investigating an issue, or launching an automated process that attempts to correct an error condition.

- *Alerts*. Azure Monitor proactively notifies you of critical conditions using Alerts, and can potentially attempt to take corrective actions. Alert rules based on metrics can provide alerts in almost real-time, based on numeric values. Alert rules based on logs allow for complex logic across data, from multiple sources.
- *Autoscale*. Azure Monitor uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively. Autoscale enables you to create rules that use metrics, collected by Azure Monitor, to determine when to automatically add resources to handle increases in load. Autoscale can also help reduce your Azure costs by removing resources that are not being used. You can specify a minimum and maximum number of instances, and provide the logic that determines when Autoscale should increase or decrease resources.

Visualize

Visualizations, such as charts and tables, are effective tools for summarizing monitoring data and for presenting data to different audiences. Azure Monitor has its own features for visualizing monitoring data, and it leverages other Azure services for publishing data for different audiences. Other tools you may use for visualizing data, for particular audiences and scenarios, include:

- Dashboards
- Views
- Power BI

Integrate

You'll often need to integrate Azure Monitor with other systems, and build customized solutions that use your monitoring data. Other Azure services can work with Azure Monitor to provide this integration.

Privacy, Compliance and Data Protection standards in Azure

Video: Compliance Terms and requirements



<https://www.youtube.com/watch?v=UeUliq9O-pE>

Compliance Terms and requirements

When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards. Some questions to ask about a potential provider include:

- How compliant is the cloud provider when it comes to handling sensitive data?
- How compliant are the services offered by the cloud provider?
- How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future.

Note: Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider.

While the following image is not a full list of compliance offerings, it will provide you with an idea of the level of compliance offerings that are available with Azure.

Global	<input checked="" type="checkbox"/> ISO 27001:2013 <input checked="" type="checkbox"/> ISO 27017:2015 <input checked="" type="checkbox"/> ISO 27018:2014	<input checked="" type="checkbox"/> ISO 22301:2012 <input checked="" type="checkbox"/> ISO 9001:2015 <input checked="" type="checkbox"/> ISO 20000-1:2011	<input checked="" type="checkbox"/> SOC 1 Type 2 <input checked="" type="checkbox"/> SOC 2 Type 2 <input checked="" type="checkbox"/> SOC 3	<input checked="" type="checkbox"/> CSA STAR Certification <input checked="" type="checkbox"/> CSA STAR Attestation <input checked="" type="checkbox"/> CSA STAR Self-Assessment <input checked="" type="checkbox"/> WCAG 2.0 (ISO 40500:2012)	
US Gov	<input checked="" type="checkbox"/> FedRAMP High <input checked="" type="checkbox"/> FedRAMP Moderate <input checked="" type="checkbox"/> EAR	<input checked="" type="checkbox"/> DFARS <input checked="" type="checkbox"/> DoD DISA SRG Level 5 <input checked="" type="checkbox"/> DoD DISA SRG Level 4 <input checked="" type="checkbox"/> DoD DISA SRG Level 2	<input checked="" type="checkbox"/> DoE 10 CFR Part 810 <input checked="" type="checkbox"/> NIST SP 800-171 <input checked="" type="checkbox"/> NIST CSF <input checked="" type="checkbox"/> Section 508 VPATs	<input checked="" type="checkbox"/> FIPS 140-2 <input checked="" type="checkbox"/> ITAR <input checked="" type="checkbox"/> CJIS <input checked="" type="checkbox"/> IRS 1075	
Industry	<input checked="" type="checkbox"/> PCI DSS Level 1 <input checked="" type="checkbox"/> GLBA <input checked="" type="checkbox"/> FFIEC <input checked="" type="checkbox"/> Shared Assessments <input checked="" type="checkbox"/> FISC (Japan) <input checked="" type="checkbox"/> APRA (Australia)	<input checked="" type="checkbox"/> FCA (UK) <input checked="" type="checkbox"/> MAS + ABS (Singapore) <input checked="" type="checkbox"/> 23 NYCCR 500 <input checked="" type="checkbox"/> HIPAA BAA <input checked="" type="checkbox"/> HITRUST	<input checked="" type="checkbox"/> 21 CFR Part 11 (GxP) <input checked="" type="checkbox"/> MARS-E <input checked="" type="checkbox"/> NHS IG Toolkit (UK) <input checked="" type="checkbox"/> NEN 7510:2011 (Netherlands) <input checked="" type="checkbox"/> FERPA	<input checked="" type="checkbox"/> CDSA <input checked="" type="checkbox"/> MPAA <input checked="" type="checkbox"/> DPP (UK) <input checked="" type="checkbox"/> FACT (UK) <input checked="" type="checkbox"/> SOX	
Regional	<input checked="" type="checkbox"/> Argentina PDPA <input checked="" type="checkbox"/> Australia IRAP Unclassified <input checked="" type="checkbox"/> Australia IRAP PROTECTED <input checked="" type="checkbox"/> Canada Privacy Laws <input checked="" type="checkbox"/> China GB 18030:2005 <input checked="" type="checkbox"/> China DJCP (MLPS) Level 3	<input checked="" type="checkbox"/> EN 301 549 <input checked="" type="checkbox"/> EU ENISA IAF <input checked="" type="checkbox"/> EU Model Clauses <input checked="" type="checkbox"/> EU – US Privacy Shield <input checked="" type="checkbox"/> Germany C5	<input checked="" type="checkbox"/> China TRUCS / CCCPPF <input checked="" type="checkbox"/> EU – US Privacy Shield <input checked="" type="checkbox"/> Japan CS Mark Gold <input checked="" type="checkbox"/> Japan My Number Act <input checked="" type="checkbox"/> Netherlands BIR 2012 <input checked="" type="checkbox"/> New Zealand Gov CC	<input checked="" type="checkbox"/> Germany IT-Grundschutz <input checked="" type="checkbox"/> India MeitY <input checked="" type="checkbox"/> Japan My Number Act <input checked="" type="checkbox"/> New Zealand Gov CC	<input checked="" type="checkbox"/> Singapore MTCS Level 3 <input checked="" type="checkbox"/> Spain ENS <input checked="" type="checkbox"/> Spain DPA <input checked="" type="checkbox"/> UK Cyber Essentials Plus <input checked="" type="checkbox"/> UK G-Cloud <input checked="" type="checkbox"/> UK PASF

Compliance Offerings:

The following list provides details about *some* (but most definitely not all) of the compliance offerings available on Azure:

- **CJIS.** Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhering to the same requirements that law enforcement and public safety entities must meet.
- **CSA STAR Certification.** Azure, Intune, and Microsoft Power BI have obtained STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture. This STAR certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It demonstrates that a cloud service provider conforms to the applicable requirements of ISO/IEC 27001, has addressed issues critical to cloud security as outlined in the CCM, and has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.
- **General Data Protection Regulation (GDPR).** As of May 25, 2018, a European privacy law—GDPR—is in effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.
- **EU Model Clauses.** Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud from Europe to the rest of the world.
- **HIPAA.** The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

MCT USE ONLY. STUDENT USE PROHIBITED

- *ISO/IEC 27018*. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
- *Multi-Tier Cloud Security (MTCS) Singapore*. After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 Certification across all three service classifications—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and SaaS. Microsoft was the first global cloud solution provider (CSP) to receive this certification across all three classifications.
- *Service Organization Controls (SOC) 1, 2, and 3*. Microsoft-covered cloud services are audited at least annually against the SOC report framework by independent third-party auditors. The Microsoft cloud services audit covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.
- *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)*. NSIT CSF is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft cloud services have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits, and are certified according to the FedRAMP standards. Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.
- *UK Government G-Cloud*. The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received official accreditation from the UK Government Pan Government Accreditor.

Note: You can view all the Microsoft compliance offerings on the [Compliance Offerings⁴⁸](#) webpage.

Video: Microsoft Privacy Statement



<https://www.youtube.com/watch?v=uHTrFEJS0Dc>

Microsoft Privacy Statement

The Microsoft privacy statement explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

The statement applies to the interactions Microsoft has with you and Microsoft products such as Microsoft services, websites, apps, software, servers, and devices.

It is intended to provide openness and honesty about how Microsoft deals with personal data in its products and services.

Note: You can read the entire Microsoft Privacy Statement on the [Microsoft Privacy Statement⁴⁹](#) webpage.

⁴⁸ <https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>

⁴⁹ <https://privacy.microsoft.com/en-us/privacystatement>

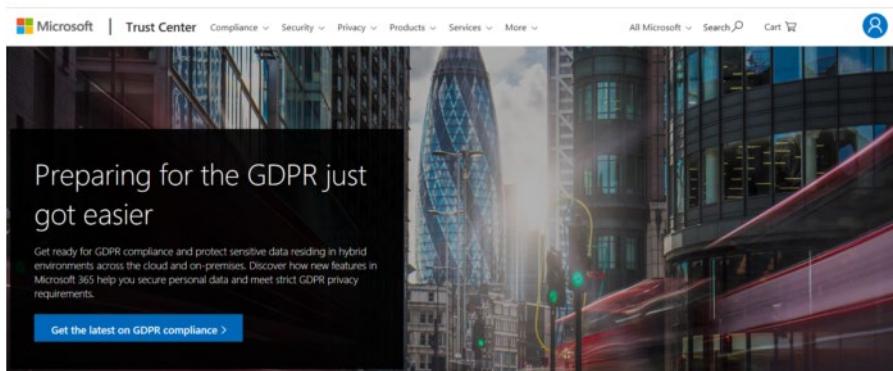
Video: Trust Center and Service Trust Portal



<https://www.youtube.com/watch?v=w-CQ5pr4zKU>

Trust Center

Trust Center is a website resource containing information and details about how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud Initiative, and provides support and resources for the legal and compliance community.



The Trust Center site provides:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources in the form of a curated list of the most applicable and widely-used resources for each topic.
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Cross-company document search, which is coming soon and will enable existing cloud service customers to search the Service Trust Portal.
- Direct guidance and support for when you can't find what you're looking for.

Note: For more information, visit the [Microsoft Trust Center](#)⁵⁰ webpage.

Service Trust Portal

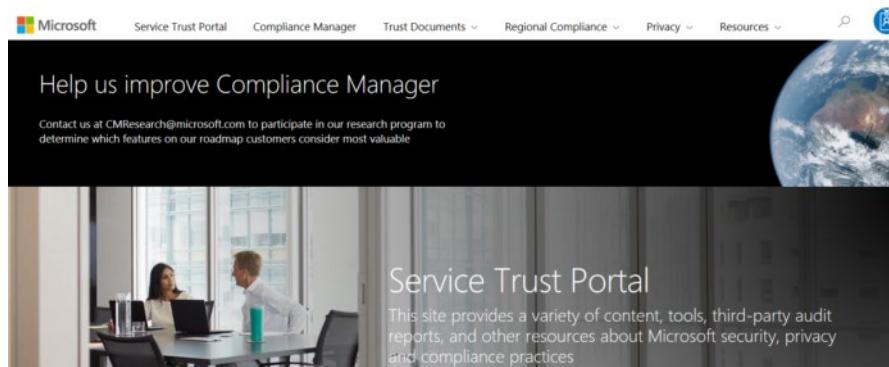
The *Service Trust Portal* (STP) hosts the Compliance Manager service, and is the Microsoft public site for publishing audit reports and other compliance-related information relevant to Microsoft's cloud services.

⁵⁰ <https://www.microsoft.com/en-us/trustcenter>

STP users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports that provide details on how Microsoft builds and operates its cloud services.

STP also includes information about how Microsoft online services can help your organization maintain and track compliance with standards, laws, and regulations, such as:

- ISO
- SOC
- NIST
- FedRAMP
- GDPR



STP is a companion feature to the Trust Center, and allows you to:

- Access audit reports across Microsoft cloud services on a single page.
- Access compliance guides to help you understand how you can use Microsoft cloud service features to manage compliance with various regulations.
- Access trust documents to help you understand how Microsoft cloud services help protect your data.

Accessing the STP

To access some STP materials, you must sign in as an authenticated user with your Microsoft cloud services account (either an Azure AD organization account or a Microsoft account), and then review and accept the Microsoft Non-Disclosure Agreement for Compliance Materials.

Existing customers can access the STP at the **Service Trust Portal⁵¹** webpage, with one of the following online subscriptions (trial or paid):

- Office 365
- Dynamics 365
- Azure

⁵¹ <https://aka.ms/STP>

Video: Compliance Manager



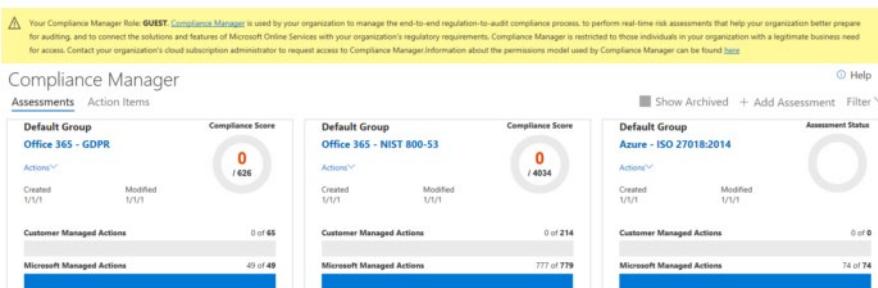
https://www.youtube.com/watch?v=_kJJPLArecM

Compliance Manager

Compliance Manager is a workflow-based risk assessment dashboard within the Trust Portal that enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services such as Office 365, Dynamics 365, and Azure.

Compliance Manager provides the following features:

- Combines the following three items:
 1. Detailed information provided by Microsoft to auditors and regulators, as part of various third-party audits of Microsoft's cloud services against various standards (for example, ISO 27001, ISO 27018, and NIST).
 2. Information that Microsoft compiles internally for its compliance with regulations (such as HIPAA and the EU GDPR).
 3. An organization's self-assessment of their own compliance with these standards and regulations.
- Enables you to assign, track, and record compliance and assessment-related activities, which can help your organization cross team barriers to achieve your organization's compliance goals.
- Provides a Compliance Score to help you track your progress and prioritize auditing controls that will help reduce your organization's exposure to risk.
- Provides a secure repository in which to upload and manage evidence and other artifacts related to compliance activities.
- Produces richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and your organization, which can be provided to auditors, regulators, and other compliance stakeholders.



Compliance Manager provides ongoing risk assessments with a risk-based scores reference displayed in a dashboard view for regulations and standards. Alternatively, you can create assessments for the regulations or standards that matter more to your organization.

As part of the risk assessment, Compliance Manager also provides recommended actions you can take to improve your regulatory compliance. You can view all action items, or select the action items that correspond with a specific certification.

NOTE: Compliance Manager is a dashboard that provides a summary of your data protection and compliance stature, and recommendations to improve data protection and compliance. The Customer Actions provided in Compliance Manager are recommendations only; it is up to each organization to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementation. Recommendations found in Compliance Manager should not be interpreted as a guarantee of compliance.

Walkthrough-Accessing Trust Center STP and Compliance Manager

In this walkthrough task we will access the Trust Center and browse through some of its content. Then we will access the Service Trust Portal (STP) and some of its resources and content, and finally we will access Compliance Manager and some of its available resources.

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 a Microsoft Cloud service account, such as 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 today⁵²](#) webpage.

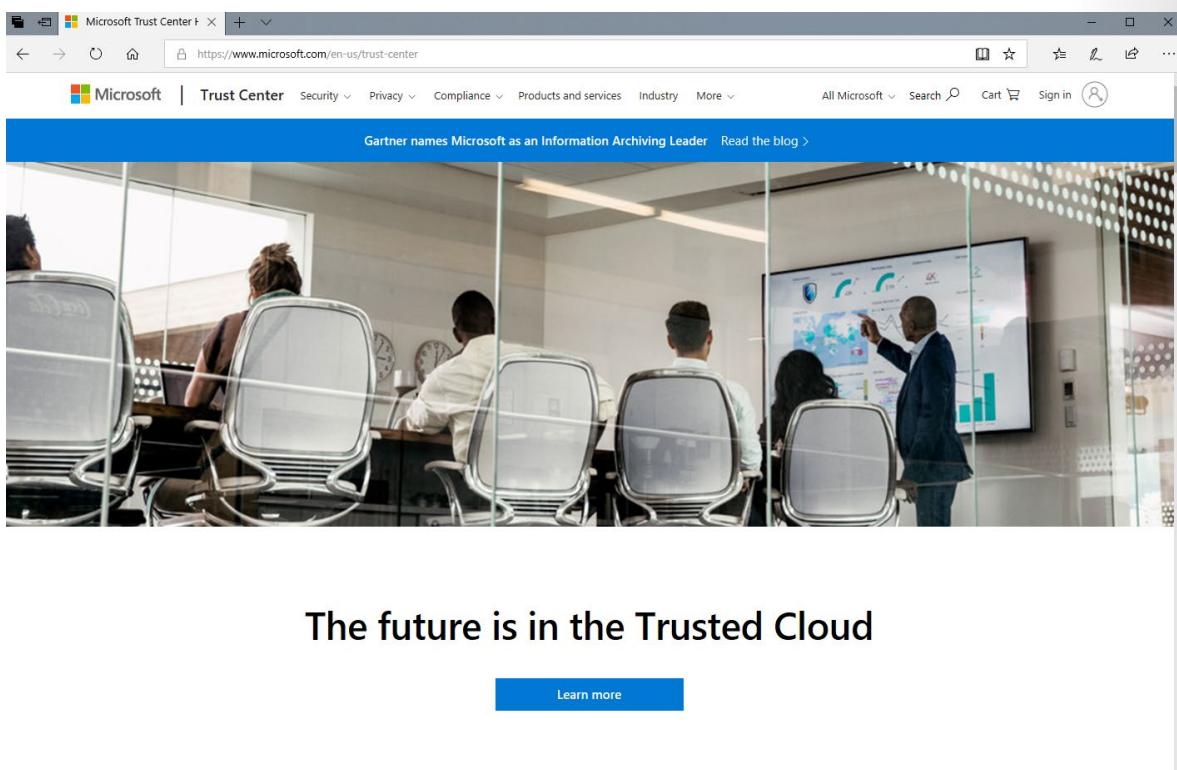
Steps

Access the Trust Center

1. Go to the **Microsoft Trust Center** at the URL <https://www.microsoft.com/en-us/trust-center⁵³>

⁵² https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

⁵³ <https://www.microsoft.com/en-us/trust-center>



The future is in the Trusted Cloud

[Learn more](#)

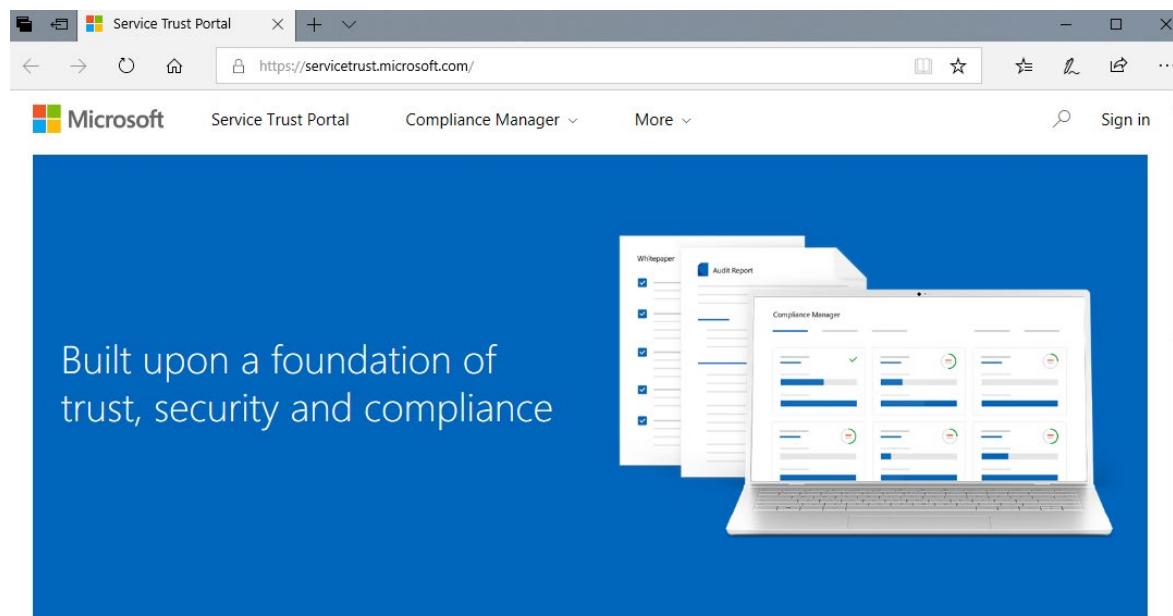
2. Scroll down through the **Trust Center**, and select some of the items such as **Security**, or **Privacy** and follow the links to download and browse some of the available reports.

Access Service Trust Portal (STP)

1. Go to the **Service Trust Portal (STP)** at the URL <https://servicetrust.microsoft.com>⁵⁴

⁵⁴ <https://servicetrust.microsoft.com/>

MCT USE ONLY. STUDENT USE PROHIBITED



Audit Reports

Review the available independent audit reports for Microsoft's Cloud services, which provide information about compliance with data protection standards and regulatory requirements, such as International Organization for Standardization (ISO), Service Organization Controls (SOC), National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FedRAMP), and the General Data Protection Regulation (GDPR).



SOC



FedRAMP



ISO 27001



PCI/DSS

2. Scroll down through the **Trust Center**, and click on **View all audit reports**, and the select some of the industries to filter some of the audit reports.

MCT USE ONLY. STUDENT USE PROHIBITED

Audit Reports

Resources to help information security and compliance professionals understand cloud features, and to verify technical compliance and control requirements

New and Archived Audit Reports

Use these reports to stay current on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Select start date to Select end date

Banking

[Sign in](#) with your Microsoft Account to access locked files and save to your library.

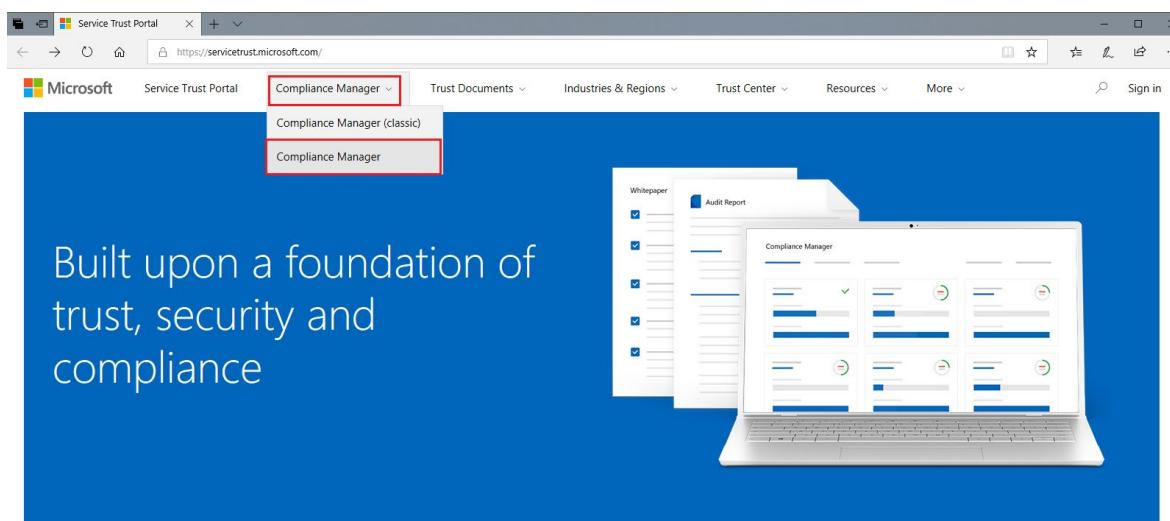
[ENS Audit Reports and Certificates](#) [FedRAMP Reports](#) [GRC Assessment Reports](#) [ISO Reports](#) [PCI DSS](#) [SOC Reports](#)

3. Browse through some of the audit reports, and when finished return to the **Trust Center** home page and browse through some of the other items available on the page, such as **Documents and Resources, Industry Compliance, Services Risk Assessment** etc.

Access Compliance Manager

1. On the **Microsoft Service Trust Portal** at the URL [55](https://servicetrust.microsoft.com/) select **Compliance Manager** from the list of options at the top.

[55](#) <https://servicetrust.microsoft.com/>



2. When prompted to sign in enter your credentials for your Microsoft account i.e. as stated in the message when signing in to Compliance Manager, **To access this resource, you must be signed in to your cloud service (Office 365, Dynamics 365, Azure, or other)**, click **Sign In**.

You have selected a free, but protected, resource

Already a Microsoft cloud services customer? Sign in to your account.

To access this resource, you must be signed in to your cloud service (Office 365, Dynamics 365, Azure, or other). Click "Sign in" to open your cloud service's sign in page. You will only need to sign in once per session.

[SIGN IN >](#)

Not a customer? Sign up for a free trial.

To gain access to this resource (and other protected resources on the Trust Center site), please sign up for a free trial. You do not need to use a credit card to sign up.

After you register for the trial, please sign in with your new credentials and return to the Trust Center site to access this resource.

[FREE TRIAL >](#)

[Cancel](#)

3. Once logged in, take some time to browse through the various elements available within **Compliance Manager**

MCT USE ONLY. STUDENT USE PROHIBITED

Assessment	Certification	Product	Created	Modified	Assessment Score
Office 365 ISO/IEC 27001:2013	ISO 27001	Office 365	4/27/2019	5/23/2019	1% (Green)
Office 365 HIPAA/HITECH	HIPAA/HITECH	Office 365	4/27/2019	5/6/2019	2% (Green)
Office 365 ISO/IEC 27018:2019	ISO 27018	Office 365	4/27/2019	5/13/2019	1% (Green)

Congratulations! In this walkthrough task you accessed the Trust Center and browsed through some of its content. You then accessed the Service Trust Portal (STP) and some of its resources and content, and finally you accessed Compliance Manager and some of its available resources.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Azure Government services

Microsoft Azure Government is a separate instance of the Microsoft Azure service. It addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers. Azure Government offers physical isolation from non-US government deployments, and provides screened US personnel.

Azure Government services handle data that is subject to certain government regulations and requirements, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS. To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks (located only in the US). Azure Government customers (US federal, state, and local government or their partners) are subject to validation of eligibility.

Azure Government provides the broadest compliance and Level 5 Department of Defense (DoD) approval. You can choose from six government-only datacenter regions, including two regions granted an Impact Level 5 Provisional Authorization. Azure Government also offers the most compliance certifications of any cloud provider.

Most services are the same on both Azure Government and Public Azure. However, there are some differences that you should be aware of. Details are available at **Compare Azure Government and global Azure.**⁵⁶

⁵⁶ <https://docs.microsoft.com/en-us/azure/azure-government/compare-azure-government-global-azure>

Note: You can read more about Azure Government on the [Azure Government⁵⁷](#) webpage.

Azure Germany services

Microsoft Azure Germany is built on the Microsoft trusted cloud principles of security, privacy, compliance, and transparency. It brings data residency in transit and at rest in Germany, and data replication across German datacenters for business continuity.

Customer data in the two datacenters is managed under the control of a data trustee, T-Systems International. This trustee is an independent German company and a subsidiary of Deutsche Telekom. It provides additional controls for customers' data, because access is provided only with the permission of customers or the data trustee. Microsoft commercial cloud services in these new datacenters adhere to German data-handling regulations, and give customers additional choices for how and where data is processed.

Anyone who requires data to reside in Germany can use this service.

Azure Germany includes the core components of IaaS, PaaS, and SaaS. These components include infrastructure, network, storage, data management, identity management, and many other services.

Azure Germany supports most of the same great features that global Azure customers use, such as geosynchronous data replication and autoscaling.

Most technical content that's currently available assumes that applications are being developed for global Azure, rather than for Azure Germany. It's important to ensure that developers are aware of key differences for applications being developed for hosting in Azure Germany:

- Certain services and features that are in specific regions of global Azure might not be available in Azure Germany.
- Features that are offered in Azure Germany have configuration differences from global Azure. You should review your sample code, configurations, and steps to ensure that you are building and executing within the Azure Germany environment.

Note: You can read more about Microsoft Azure Germany on the [Microsoft Azure Germany⁵⁸](#) webpage.

Azure China 21Vianet

Microsoft Azure operated by 21Vianet (Azure China 21Vianet) is a physically separated instance of cloud services located in China, independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

The Azure services are based on the same Azure, Office 365, and Power BI technologies that make up the Microsoft global cloud service, with comparable service levels. Agreements and contracts for Azure in China, where applicable, are signed between customers and 21Vianet.

As the first foreign public cloud service provider offered in China in compliance with government regulations, Azure China 21Vianet provides world-class security as discussed on the Trust Center, as required by Chinese regulations for all systems and applications built on its architecture.

Azure includes the core components of IaaS, PaaS, and SaaS. These components include network, storage, data management, identity management, and many other services.

Azure China 21Vianet supports most of the same services that global Azure has, such as geosynchronous data replication and autoscaling. Even if you already use global Azure services, to operate in China you may need to rehost or refactor some or all of your applications or services.

⁵⁷ <https://azure.microsoft.com/en-us/global-infrastructure/government/>

⁵⁸ <https://azure.microsoft.com/en-us/global-infrastructure/germany/>

According to the China Telecommunication Regulation (in Chinese), providers of cloud services (IaaS and PaaS) must have value-added telecom permits. Only locally-registered companies with less than 50-percent foreign investment qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.

Note: You can read more about Azure China on the [Azure China 21Vianet⁵⁹](#) webpage.

⁵⁹ <https://docs.microsoft.com/en-us/azure/china/>

Module 3 Review Questions

Security, Privacy, Compliance and Trust Review Questions

About review questions

End of module review questions are for practice only and are not included in your grade for the course. The final assessment at the end of the course is graded.

Review Question 1

Which descriptions from the following list describes a feature or characteristic of Azure Firewall?

(choose three)

- Azure Firewall is a stateful firewall service, with built-in high availability and unrestricted cloud scalability.
- You can create and manage access control lists for databases using Azure Firewall.
- You can prevent DDoS attacks on your network using Azure Firewall.
- You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- Azure Firewall is fully integrated with Azure Monitor for logging and analytics.

Review Question 2

There has been an attack on your public-facing website, and the application's resources have been overwhelmed and exhausted, and are now unavailable to users. What service should you use to prevent this type of attack?

- DDoS protection
- Azure Firewall
- Network security group
- Application Gateway

Review Question 3

You want to filter inbound and outbound network traffic to and from Azure resources in your Azure virtual network. Which Azure service should you use?

- Azure Firewall
- VPN Gateway
- Network security group
- Azure AD

Review Question 4

Azure AD is capable of providing which of the following functions?

(choose all that apply)

- Authentication
- SSO
- Application management
- B2B identity services
- B2C identity services
- Device management

Review Question 5

You want to store certificates in Azure to centrally manage them for your services. Which Azure service should you use?

- MSIP
- Azure AD
- Azure ATP
- Azure Key Vault

Review Question 6

True or false: You can download published audit reports and other compliance-related information related to Microsoft's cloud service from the Service Trust Portal.

- True
- False

Review Question 7

Which of the following services provides up-to-date status information about the health of Azure services?

- Compliance Manager
- Service Trust Portal
- Azure Monitor
- Azure Service Health

Review Question 8

Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

- Microsoft Privacy Statement
- Compliance Manager
- Azure Service Health
- Azure Government

Module 3 Summary

Module 3 Summary

In this module you've learned about securing network connectivity in Azure, core identity services, security tools and features, Azure governance methodologies, monitoring and reporting in Azure, and privacy, compliance, and data protection standards in Azure.

Securing network connectivity in Azure

In this lesson you learned about Azure Firewalls, Azure DDoS protection, NSGs, and choosing Azure network security solutions.

Core Azure identity services

In this lesson you learned about authentication and authorization, Azure AD, and MFA.

Security tools and features

In this lesson you learned about Azure Security Center and some usage scenarios for it, Key Vault, MSIP, and Azure ATP.

Azure governance methodologies

In this lesson you learned about Azure Policy, policies, initiatives, RBAC, locks, Azure Advisor, security assistance, and Azure Blueprint.

Monitoring and reporting in Azure

In this lesson you learned about Azure Monitor and Azure Service Health.

Privacy, compliance and data protection standards in Azure

In this lesson you learned about compliance terms and requirements, the Microsoft Privacy statement, Trust Center, the Service Trust Portal, Compliance Manager, Azure Government, Azure Germany, and Azure China.

Answers

Review Question 1

Which descriptions from the following list describes a feature or characteristic of Azure Firewall?

(choose three)

- Azure Firewall is a stateful firewall service, with built-in high availability and unrestricted cloud scalability.
- You can create and manage access control lists for databases using Azure Firewall.
- You can prevent DDoS attacks on your network using Azure Firewall.
- You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- Azure Firewall is fully integrated with Azure Monitor for logging and analytics.

Explanation

The following three features and characteristics are correct:

Azure Firewall is a stateful firewall service, with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall is fully integrated with Azure Monitor for logging and analytics.

You can create and manage access control lists for databases using Azure Firewall is incorrect.

You can prevent DDoS attacks on your network using Azure Firewall is also incorrect, because you need to use DDoS protection to prevent DDoS attacks on your public-facing resources.

S attacks on your network using Azure Firewall is incorrect, you need to use DDoS Protection to prevent DDoS attacks on your public facing resources.

Review Question 2

There has been an attack on your public-facing website, and the application's resources have been overwhelmed and exhausted, and are now unavailable to users. What service should you use to prevent this type of attack?

- DDoS protection
- Azure Firewall
- Network security group
- Application Gateway

Explanation

DDoS protection is the correct answer, because it will help prevent DDoS attacks.

Azure Firewall is incorrect. It will help control access to your network, but may not prevent DDoS attacks.

Network security group is incorrect, because while it will help protect access to your virtual network, it may not prevent a DDoS attack.

Application Gateway is incorrect. While it will help make an application available and help protect it, and it also has a built in web application firewall, it may not prevent DDoS-style attacks.

Review Question 3

You want to filter inbound and outbound network traffic to and from Azure resources in your Azure virtual network. Which Azure service should you use?

- Azure Firewall
- VPN Gateway
- Network security group
- Azure AD

Explanation

NSG is the correct answer, because it allows you to filter network traffic to and from Azure resources in an Azure virtual network. It can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

Azure Firewall will control access in and out of your network but will not control inbound and outbound network traffic within a virtual network.

VPN Gateway is a particular gateway type that allows secure connections from on-premises to Azure over the internet.

Azure AD is Azure's cloud-based identity and access management service that will provide authentication capabilities for identities, but will not control network traffic on a virtual network.

Review Question 4

Azure AD is capable of providing which of the following functions?

(choose all that apply)

- Authentication
- SSO
- Application management
- B2B identity services
- B2C identity services
- Device management

Explanation

Azure AD is capable of delivering all of the services listed, and many more.

Review Question 5

You want to store certificates in Azure to centrally manage them for your services. Which Azure service should you use?

- MSIP
- Azure AD
- Azure ATP
- Azure Key Vault

Explanation

Azure Key Vault is the correct answer, because it is a centralized cloud service for storing application secrets, referred to as a secret store.

All other answers are incorrect.

MSIP is a cloud-based solution that helps an organization classify, and optionally, protect its documents and emails by applying labels.

Azure AD is Microsoft's cloud-based identity and access management service that helps employees of an organization sign in and access resources.

Azure ATP is a cloud-based security solution that identifies, detects, and helps organizations investigate advanced threats, compromised identities, and malicious insider actions directed at that organization.

Review Question 6

True or false: You can download published audit reports and other compliance-related information related to Microsoft's cloud service from the Service Trust Portal.

- True
- False

Explanation

True is the correct answer. You can download published audit reports and other compliance-related information related to Microsoft's cloud service from the Service Trust Portal.

Review Question 7

Which of the following services provides up-to-date status information about the health of Azure services?

- Compliance Manager
- Service Trust Portal
- Azure Monitor
- Azure Service Health

Explanation

Azure Service Health is the correct answer, because it provides you with a global view of the health of Azure services. With Azure Status, a component of Azure Service Health, you can get up-to-the-minute information on service availability.

Compliance Manager enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services.

Service Trust Portal provides information about compliance with standards, laws, and regulations, in addition to hosting the Compliance Manager application.

Azure Monitor collects, analyzes, and provides actions on telemetry from your cloud and on-premises environments.

Review Question 8

Where can you obtain details about the personal data Microsoft processes, how Microsoft processes it, and for what purposes?

- Microsoft Privacy Statement
- Compliance Manager
- Azure Service Health
- Azure Government

Explanation

Microsoft Privacy Statement is the correct answer.

Compliance Manager enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft professional services and Microsoft cloud services.

Azure Service Health will provide you with a global view of the health of your Azure services.

Azure Government is a separate instance of the Microsoft Azure service that addresses the security and compliance needs of United States federal agencies, state and local governments, and their solution providers.

Module 4 Azure Pricing and Support

Learning Objectives

Learning Objectives

After completing this module, you will be able to:

- Understand and describe Microsoft Azure subscriptions and management groups.
- Recognize ways to plan and manage Azure costs.
- Identify Azure support options.
- Understand and describe features of Azure service-level agreements (SLAs).
- Understand and describe the service lifecycle in Azure.

Azure Subscriptions

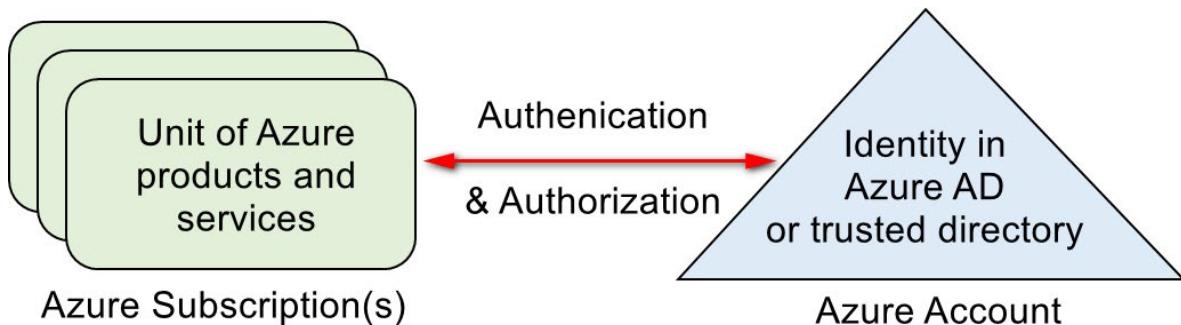
Video: Azure Subscriptions



<https://www.youtube.com/watch?v=CXIJUfTMBLM>

Azure Subscriptions

Using Azure requires an Azure subscription, which provides you with authenticated and authorized access to Azure products and services, and allows you to provision resources. An Azure subscription is a logical unit of Azure services that links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that an Azure AD trusts.



Azure offers free and paid subscription options to suit different needs and requirements. An account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies.

Note: For more information about Azure subscriptions, refer to [Azure IaaS V2 \(ARM\) Design Series¹](#).

Subscription Uses and Options

You can use Azure subscriptions to define boundaries around Azure products, services, and resources. There are two types of subscription boundaries that you can use, including:

- *Billing boundary.* This subscription type determines how an Azure account is billed for using Azure. You can create multiple subscriptions for different types of billing requirements, and Azure will generate separate billing reports and invoices for each subscription so that you can organize and manage costs.
- *Access control boundary.* Azure will apply access-management policies at the subscription level, and you can create separate subscriptions to reflect different organizational structures. An example is that within a business, you have different departments to which you apply distinct Azure subscription

¹ <https://social.technet.microsoft.com/wiki/contents/articles/33800.azure-iaas-v2-arm-design-series-azure-subscriptions.aspx>

policies. This allows you to manage and control access to the resources that users provision with specific subscriptions.

Note: For more information about grouping resources by subscription, refer to the [Create resource groups and resources at the subscription level²](#) page.

Subscription options

The screenshot shows a list of Azure subscription offers. Each offer includes a small icon, the offer name, a brief description, and a 'Learn more' link.

- Pay-As-You-Go Dev/Test**
This offer is for teams of active Visual Studio subscribers to run dev/test workloads on Microsoft Azure, providing discounted rates on Windows virtual machines and access to exclusive images in the Azure Gallery.
[Learn more](#)
- Visual Studio Enterprise: BizSpark**
Enjoy monthly credits and lower rates.
Use MSDN software at no additional charge.
[Learn more](#)
- Visual Studio Professional**
Enjoy monthly credits and lower rates.
Use MSDN software for development and test at no additional charge.
[Learn more](#)

You can select from a range of Azure subscription options, including:

- *A free account.* This subscription is for 30 days and includes a \$200 credit. This allows you unlimited access to the free Azure products and then a limit of \$200 to spend on the paid products. Your Azure services are disabled when the trial ends or when your credit expires for paid products, unless you upgrade to a paid subscription.
- *Pay-As-You-Go.* This subscription allows you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply to Microsoft for invoicing privileges.
- *Member offers.* Your existing membership to certain Microsoft products and services affords you credits for your Azure account and reduced rates on Azure services. For example, member offers are available to Microsoft Visual Studio subscribers, Microsoft Partner Network members, Microsoft BizSpark members, and Microsoft Imagine members.

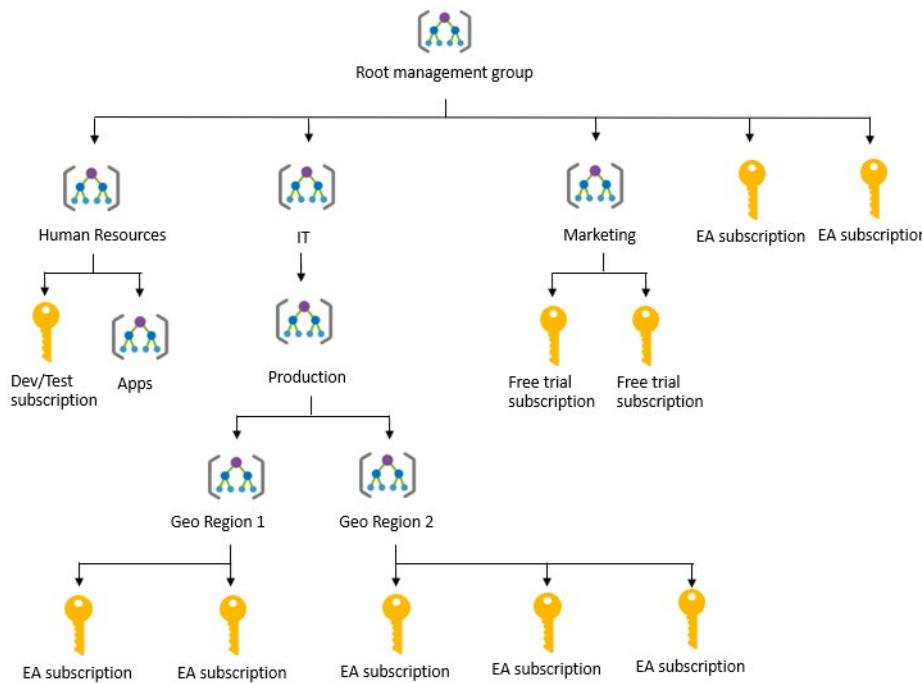
Note: For more information on Azure subscription offers, refer to [Current Offers³](#).

Management Groups

Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions. Management groups allow you to order your Azure resources hierarchically into collections, which provides a further level of classification that is above the level of subscriptions.

² <https://docs.microsoft.com/en-us/azure/azure-resource-manager/deploy-to-subscription>

³ <https://azure.microsoft.com/en-us/support/legal/offer-details/>



You can manage your Azure subscriptions more effectively by using Azure Policy and Azure role-based access controls (RBACs). These provide distinct governance conditions that you can apply to each management group. The resources and subscriptions you assign to a management group automatically inherit the conditions that you apply to that management group.

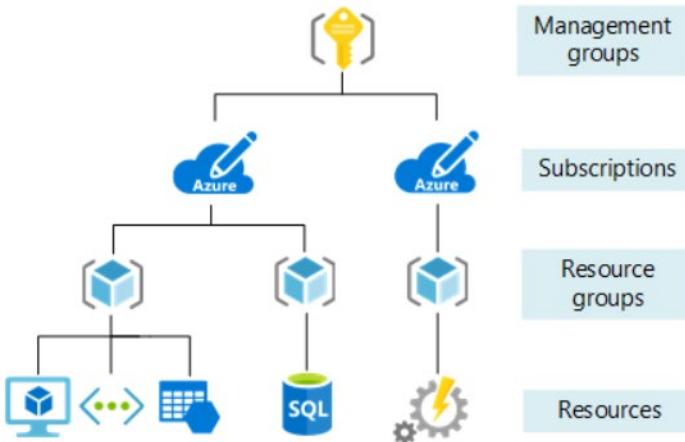
Note: For more information about management groups, refer to [Create management groups for resource organization and management⁴](#) and [Organize your resources with Azure management groups⁵](#).

Object Hierarchy

The organizing structure for resources in Azure has four levels: **Management groups, subscriptions, resource groups, and resources**. The following image shows the relationship of these levels i.e. the hierarchy of organization for the various objects

⁴ <https://docs.microsoft.com/en-us/azure/governance/management-groups/create?toc=%2Fazure%2Fbilling%2FTOC.json>

⁵ <https://docs.microsoft.com/en-us/azure/governance/management-groups/>



- **Management groups:** These are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
- **Subscriptions:** A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Resource groups:** A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Resources:** Resources are instances of services that you create, like virtual machines, storage, or SQL databases

Walkthrough-Manage Subscriptions and Management groups

In this walkthrough task we will create Azure Subscriptions based on organization structure and specific project use, we will then create Management groups to manage those newly created subscriptions. We will then elevate the logged in user account access, to allow it to manage all Azure subscriptions and management groups and add our subscriptions to our Management groups. We will then assign an Azure Policy for allowed locations to a Management group and subscription. We will then delete an Azure Subscription and delete the Management groups.

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 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 today⁶](https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio) webpage.

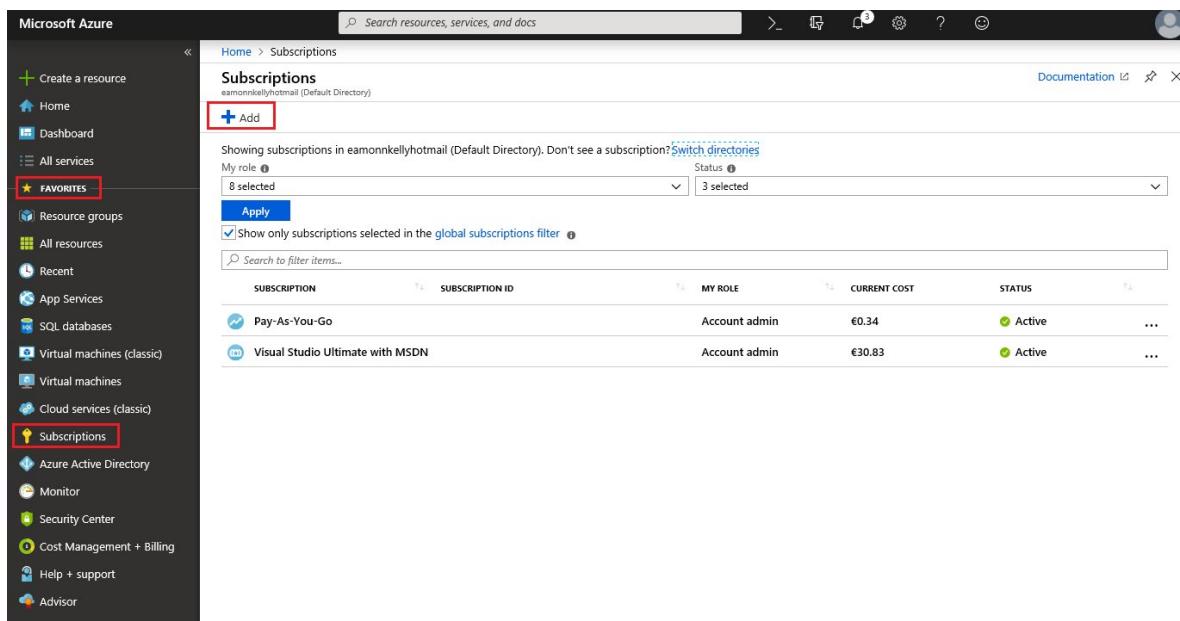
⁶ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

- You will also need access to credit card details, or a valid payment method, which is required for setting up new Azure subscriptions. The credit card will **not** be charged anything as we will not be deploying any resources to the subscriptions we created with it.

Steps

Create Subscriptions based on organization structure and specific project use

1. In the Azure Portal select **Subscriptions** from the left hand side **FAVORITES** menu and on the subscriptions pane click **+ Add**



Subscription	Subscription ID	My Role	Current Cost	Status
Pay-As-You-Go		Account admin	€0.34	Active
Visual Studio Ultimate with MSDN		Account admin	€30.83	Active

Note: The subscriptions listed in your Subscription pane will be different to what is displayed in the screenshot.

2. Sign into your Azure account when prompted, and in the subsequent **Add subscription** under the **Select an Offer** section, select **Pay-As-You-Go**

The screenshot shows the Microsoft Azure 'Add subscription' interface. On the left, there's a sidebar with the 'Add subscription' button highlighted by a red box. The main content area has a blue header bar with 'SELECT AN OFFER'. Below it, five offer cards are listed, each with a blue icon and a question mark icon. The first card is 'Pay-As-You-Go', which is also highlighted with a red box. The other four cards are 'Pay-As-You-Go Dev/Test', 'Developer support', 'Professional Direct support', and 'Standard support'. At the bottom of the page, there are links for English, © 2019 Microsoft, Privacy & Cookies, Trademarks, Legal, Support, Give Us Feedback, and the Microsoft logo.

3. In the subsequent **Azure Pay-As-You-Go signup** page, under the **Identity verification by phone** section, ensure the **Country code** and **Phone number** details are correct then select either **Text me** or **Call me** and follow the prompts to complete the identity validation process.

MCT USE ONLY. STUDENT USE PROHIBITED



Azure Pay-As-You-Go signup

With an Azure pay-as-you-go subscription, you only pay for the resources you use. No upfront costs, and no commitment.

1 Identity verification by phone

A text or phone call helps us make sure this is you.

Country code

Ireland (+353)

Phone number

85 7145284

[Text me](#)

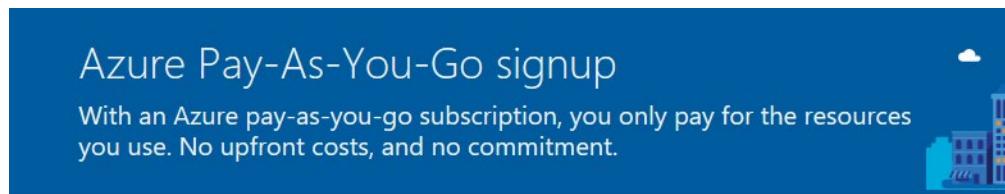
[Call me](#)

2 Payment Information

3 Add technical support

4 Agreement

4. In the **Payment information** either accept the existing payment method or add a new one and follow the prompts by clicking the **Add a new payment method** link and when complete click **Next**



1 Identity verification by phone

2 Payment Information

We found this payment method associated with your account:



Eamonn Kelly **0599 9/2021

Add a new payment method

Next

3 Add technical support

4 Agreement

5. In the **Add technical support** section select the radio button for **No technical support...** and click **Next**

1 Identity verification by phone ▼

2 Payment Information ▼

3 Add technical support ^

For one-on-one technical support, you'll need a [support plan](#). Whether you're new to Azure or already building business-critical applications, our support plans provide expert guidance from Azure engineers who will work with you to prevent and solve problems. By upgrading to a plan you agree to the [offer details](#).

- Getting started on Azure - Developer plan** 24.46 €/month
For developers or teams looking to quickly and effectively get started on Azure, technical support is available weekdays from 9:00 AM to 5:00 PM with initial response times under 8 business hours.
- Production use of Azure - Standard plan** 84.33 €/month
For teams running production applications, get 24x7 technical support and fast initial response times under 2 hours.
- Business-critical use of Azure - Professional Direct plan** 843.30 €/month
For business-critical applications, a cloud advisor provides guidance and advocacy to help improve reliability and optimize costs. You also get 24x7 technical support with the fastest initial response times under 1 hour.

No technical support, or I am already covered through Microsoft Premier support.

Next

4 Agreement ▼

6. In the **Agreement** section check the checkbox for **I agree to the subscription agreement....** and click the **Sign Up** button

Azure Pay-As-You-Go signup
With an Azure pay-as-you-go subscription, you only pay for the resources you use. No upfront costs, and no commitment.

1 Identity verification by phone

2 Payment Information

3 Add technical support

4 Agreement

I agree to the [subscription agreement](#), [offer details](#), and [privacy statement](#)

I would like information, tips, and offers from Microsoft or selected partners about Azure, including Azure Newsletter, Pricing updates, and other Microsoft products and services.

Sign up

7. You will be taken then to the **Quickstart Center** page in the Azure Portal. If you have time you can take a moment click on the **Open >** link in the **Introduction to Azure Setup** and read through some of the Steps and details available within it, such as **Organize resources** and then the **Azure management groups and hierarchy** tab. You will also receive a mail informing you that your Azure subscription is ready.

Quickstart Center
Microsoft Azure

Get started Take an online course

Setup guide
Our guide walks you through deployment scenarios to help you set up, manage, and secure your Azure environment.

Introduction to Azure Setup
Step-by-step guidance to help admins plan, set up, and secure Azure for your organization.
[Open >](#)

Start a project
Choose from the popular services below to create your first resource and launch your project. [Otherwise, see All services.](#)

Create a web app Build and deploy web apps that can scale Start >	Deploy a virtual machine Run your workloads in the cloud and reduce the redundancy and maintenance of physical hardware Start >	Set up a database Explore options for managing relational or nonrelational databases in the cloud Start >
Start a data analytics project Put machine learning and artificial intelligence to work on your apps Start >	Store, backup, or archive data Extend data storage to the cloud and leverage it for disaster recovery Start >	

8. Return Subscriptions pane and verify your new subscription is listed under subscriptions. If it is not displaying you may have to uncheck the box **Show only subscriptions selected in the global subscriptions filter**

Subscriptions
eamonnkelly@hotmail (Default Directory)

Documentation [Switch directories](#)

+ Add

Showing subscriptions in eamonnkelly@hotmail (Default Directory). Don't see a subscription? [Switch directories](#)

My role [?](#) Status [?](#)

8 selected 3 selected

Apply

Show only subscriptions selected in the [global subscriptions filter](#)

Search to filter items...

SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
Pay-As-You-Go		Account admin	€0.34	Active
Pay-As-You-Go	02693c6d-e4b8-47cf-b605-4dff43732d43	Account admin	Not available	Active
Visual Studio Ultimate with...		Account admin	€31.15	Active

9. Double click on the subscription to open it, and in the **Pay-As-You-Go** pane, note the various fields and data available, then go to the **Overview** section and click **Rename**

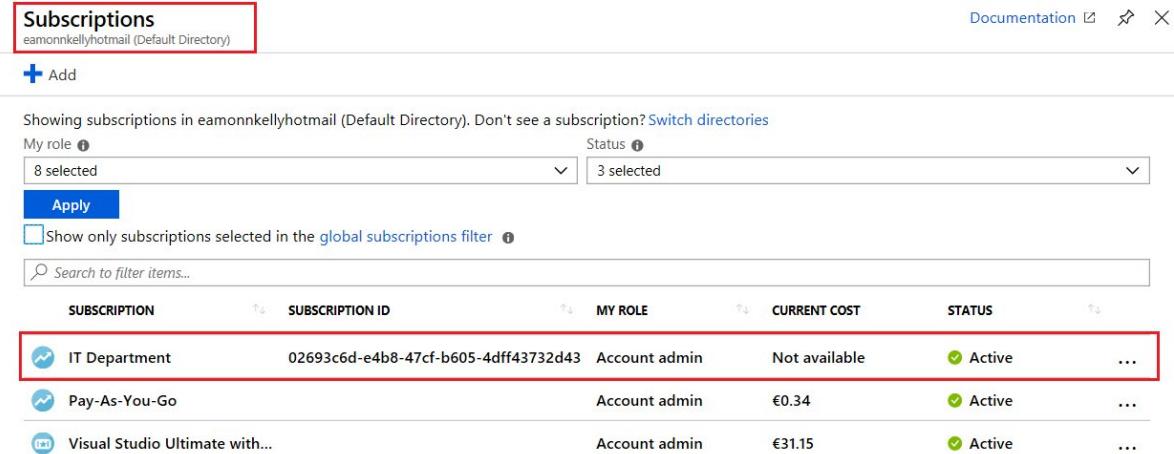
The screenshot shows the Azure Subscription blade for a subscription named "Pay-As-You-Go". The left sidebar lists various management options like Overview, Activity log, Access control (IAM), etc. The main area displays subscription details such as ID, Directory, Role, Offer, and Status. A prominent red box highlights the "Rename" button in the top right corner. Below it, a purple banner suggests trying Azure Cost Management.

10. In the **Subscription name** blade enter a user friendly name based on an organization structure i.e. **IT Department**, and click **Save**, and close the pane.

This screenshot shows the "Subscription name" blade. It has a "Save" button highlighted with a red box, indicating it should be clicked to update the subscription name. A note below says: "After you update the name, it may take some time for the portal to reflect the change. Please try refreshing the page after 10 minutes." The subscription name field contains "IT Department".

Note: After you update the name, it may take some time for the portal to reflect the change. Please try refreshing the page after approx. 5 minutes.

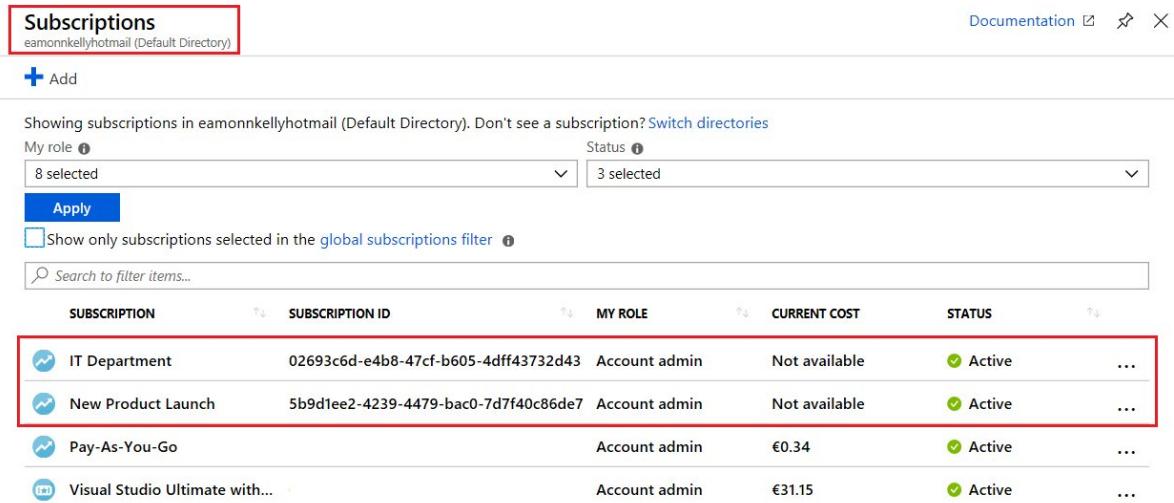
11. Return to the **Subscriptions** pane and verify the newly renamed subscription is present.



The screenshot shows the Azure Subscriptions page. At the top, there's a header with 'Subscriptions' and a note about showing subscriptions in the default directory. Below this are filters for 'My role' (8 selected) and 'Status' (3 selected), with an 'Apply' button. There's also a checkbox for 'Show only subscriptions selected in the global subscriptions filter'. A search bar is present. The main table lists three subscriptions:

Subscription	Subscription ID	My Role	Current Cost	Status
IT Department	02693c6d-e4b8-47cf-b605-4dff43732d43	Account admin	Not available	Active
Pay-As-You-Go		Account admin	€0.34	Active
Visual Studio Ultimate with...		Account admin	€31.15	Active

12. Repeat Steps **1** to **12** to create another Pay-As-You-Go subscription, entering the same data entered previously when required except this time, use the subscription name **New Product Launch**. When finished both newly created subscriptions should be present in the Subscriptions pane.



The screenshot shows the Azure Subscriptions page after creating a new subscription. The table now includes a fourth row:

Subscription	Subscription ID	My Role	Current Cost	Status
IT Department	02693c6d-e4b8-47cf-b605-4dff43732d43	Account admin	Not available	Active
New Product Launch	5b9d1ee2-4239-4479-bac0-7d7f40c86de7	Account admin	Not available	Active
Pay-As-You-Go		Account admin	€0.34	Active
Visual Studio Ultimate with...		Account admin	€31.15	Active

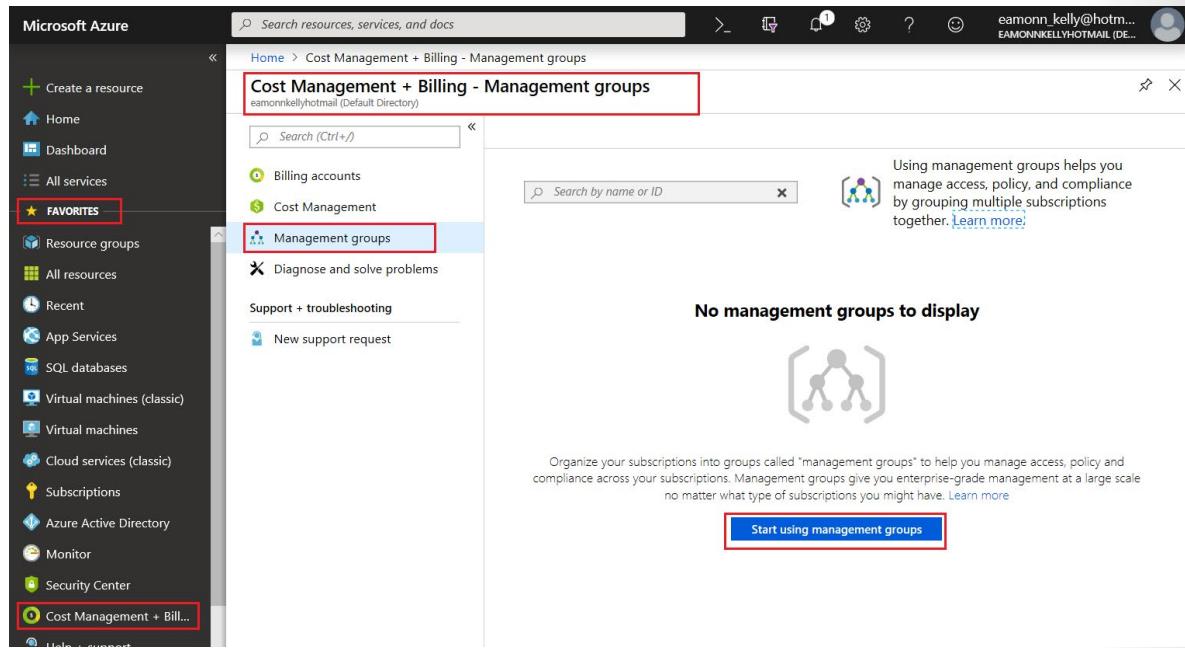
Note: Creating multiple subscriptions and naming them for specific purposes allows us manage them more easily, particularly from a security and billing/cost management perspective. We could also create subscriptions specific to other criteria such as geography, workload or any other requirement you have to differentiate resources.

Create Management groups to manage newly created subscriptions

If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure **Management groups** provide a level of scope above subscriptions. You organize subscriptions into containers called **Management groups** and then apply your governance conditions to the **Management groups**. If you have multiple subscriptions in a **Management group** this helps to greatly simplify the management of those subscriptions. The key aspect is

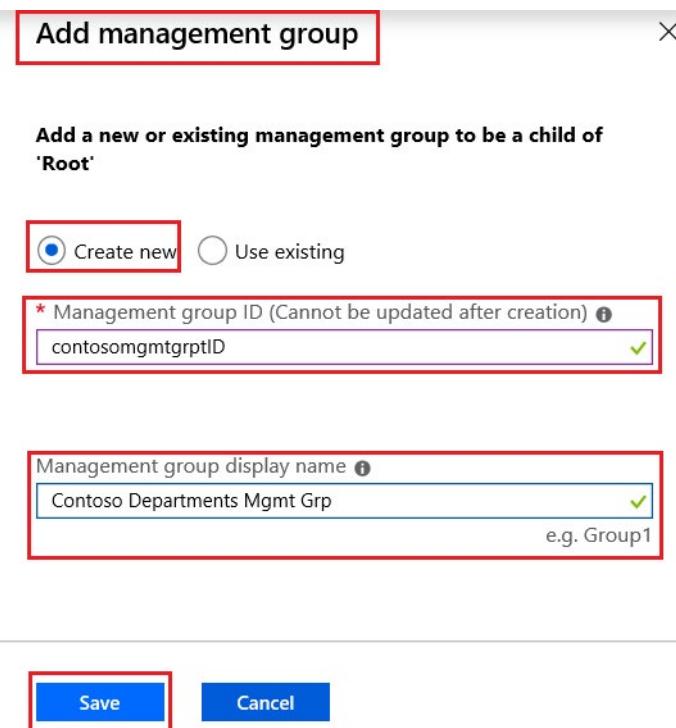
to create **Management groups** representing various parts of your business or your needs, and placing subscriptions in those **Management groups**, which will have similar management requirements.

1. In the Azure Portal select **Cost Management + Billing** from the left hand side **FAVORITES** menu and then go to **Management groups** and click on the **Start using management groups** button



2. In the **Add management group** pane fill in the following details and click **Save** when finished.

- **Create New:** Check radio button
- **Management group ID:** contosomgmtgrptIDDepts (unique identifier that is used to submit commands on this management group)
- **Management group display name:** Contoso Departments Mgmt Grp (name that is displayed within the Azure portal)



Note: We will create a management group to help organize our departmental subscriptions.

3. Repeat steps **1** and **2** and create another management group, using the below values, clicking Save when finished. This time we create a management group to hold projects that a company may be undertaking, such as Marketing initiatives, product launches etc.
 - **Create New:** Check radio button
 - **Management group ID:** contosomgmtgrptIDProjects (unique identifier that is used to submit commands on this management group)
 - **Management group display name:** Contoso Projects Mgmt Grp (name that is displayed within the Azure portal)
4. Both Management groups should display when completed.

The screenshot shows the 'Cost Management + Billing - Management groups' blade. On the left, there's a sidebar with 'Billing accounts', 'Cost Management', 'Management groups' (selected), 'Diagnose and solve problems', 'Support + troubleshooting', and 'New support request'. The main area shows a 'Tenant Root Group' with a note: 'You are registered as a directory admin but do not have the necessary permissions to access the root management group. Click to learn more.' Below is a table of management groups:

NAME	ID	TYPE	MY ROLE
Contoso Departments Mgmt Grp	contosomgmtgrptID	Management group	Owner
Contoso Projects Mgmt Grp	contosomgmtgrptIDProjects	Management group	Owner
IT Department	02693c6d-e4b8-47cf-b605-4dff4373...	Subscription	Owner
New Product Launch	5b9d1ee2-4239-4479-bac0-7d7f40c...	Subscription	Owner
Pay-As-You-Go		Subscription	Owner
Visual Studio Ultimate with MSDN		Subscription	Owner

Elevate logged in user access, to allow the account to manage all Azure subscriptions and Management groups

1. Still in the **Cost Management + Billing** pane under the **Management groups** section there is a message present stating **You are registered as a directory admin but do not have the necessary permissions to access the root management group.**

Tenant Root Group

Search by name or ID

Using management groups helps you manage access, policy, and compliance by grouping multiple subscriptions together. [Learn more.](#)

NAME	ID	TYPE	MY ROLE	...
Contoso Departments Mgmt Grp	contosomgmtgrptID	Management group	Owner	...
Contoso Projects Mgmt Grp	contosomgmtgrptIDProjects	Management group	Owner	...
IT Department	02693c6d-e4b8-47cf-b605-4dff4373...	Subscription	Owner	...
New Product Launch	5b9d1ee2-4239-4479-bac0-7d7f40c...	Subscription	Owner	...

Note: Each directory is given a single top-level management group called the **Root management group**. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and RBAC assignments to be applied at the directory level. The **Azure AD Global Administrator** needs to elevate themselves to the **User Access Administrator** role of this root group initially. After elevating access, the administrator can assign any **RBAC** role to other directory users or groups to manage the hierarchy.

2. In the Azure portal or the **Azure Active Directory** and then go to **Manage > Properties** and under **Access management for Azure resources**, set the toggle to **Yes**, then click **Save**

The screenshot shows the Azure portal interface. On the left, the navigation menu is visible with various services like Home, Dashboard, All services, FAVORITES, Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, Azure Active Directory, Monitor, Security Center, Cost Management + Billing, Help + support, and Advisor. The 'Azure Active Directory' item is highlighted with a red box. In the main content area, the 'Properties' tab is selected under the 'Manage' section. The 'Access management for Azure resources' section contains a note that Eamonn Kelly can manage access to all Azure subscriptions and management groups in this directory, with a 'Learn more' link. Below this is a toggle switch with 'Yes' and 'No' options, where 'Yes' is highlighted with a red box.

When you set the toggle to **Yes**, you are *assigned* the **User Access Administrator** role in Azure RBAC at the root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This toggle is only available to users who are assigned the **Global Administrator** role in Azure AD.

When you set the toggle to **No**, the **User Access Administrator** role in Azure RBAC is *removed* from your user account. You can no longer assign roles in all Azure subscriptions and management groups that are associated with this Azure AD directory. You can view and manage only the Azure subscriptions and management groups to which you have been granted access.

Add subscriptions to your Management groups

1. Go to **Cost Management + Billing** from the left hand side **FAVORITES** menu, then go to **Management groups**, double click on the **Contoso Departments Mgmt Grp** and then click on the **details** link

The screenshot shows the 'Cost Management + Billing - Management groups' page. The left sidebar includes 'Billing accounts', 'Cost Management', 'Management groups' (highlighted with a red box), 'Diagnose and solve problems', 'Support + troubleshooting', and 'New support request'. The main content area shows a table with one row for 'Contoso Departments Mgmt Grp'. The 'NAME' column shows 'Contoso Departments Mgmt Grp', the 'ID' column shows '(details)', and the 'TYPE' and 'MY ROLE' columns are empty. A tooltip on the right explains that management groups help manage access, policy, and compliance by grouping multiple subscriptions together.

2. In the **Contoso Departments Mgmt grp** pane, in the **Overview** section click on the **+ Add subscription** button and in the **Add subscription** blade, in the **Subscription** drop down list select **IT Department**, then click **Save**

The screenshot shows the 'Add subscription' dialog for the 'Contoso Departments Mgmt Grp'. The 'Subscription' dropdown is set to 'IT Department (02693c6d-e4b8-47cf-b605-4dff43732d43)'. The 'Save' button is highlighted with a red box.

3. Go to **Cost Management + Billing** then **Management groups**, double click on the **Contoso Departments Mgmt grp** and verify the **IT Department** subscription is now listed.

The screenshot shows the 'Management groups' list for the Tenant Root Group. The 'Contoso Departments Mgmt Grp' is selected, and its details show the 'IT Department' subscription listed under 'NAME' and 'ID'. The 'Save' button is highlighted with a red box.

4. Repeat steps **1** and **3** this time for the below management group and subscription.

- Management group** = Contoso Projects Mgmt Grp
- Subscription** = New Product Launch

5. Go to **Cost Management + Billing** then **Management groups**, double click on the **Contoso Projects Mgmt Grp** and verify the **New Product Launch** subscription is now listed.

The screenshot shows the 'Management groups' list for the Tenant Root Group. The 'Contoso Projects Mgmt Grp' is selected, and its details show the 'New Product Launch' subscription listed under 'NAME' and 'ID'. The 'Save' button is highlighted with a red box.

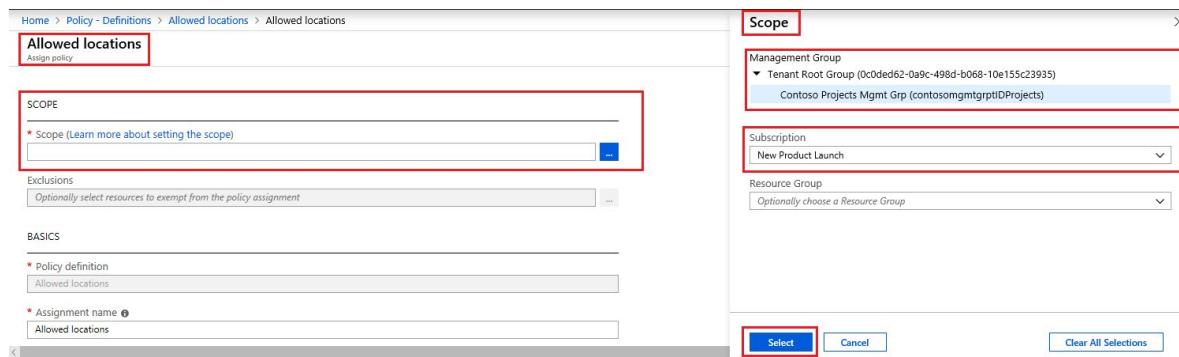
We could create more subscriptions, for company departments such as HR, Marketing, Dev etc. and Projects, then add those subscriptions to the management groups and then apply policies and access control settings across them as we wish.

MCT USE ONLY. STUDENT USE PROHIBITED

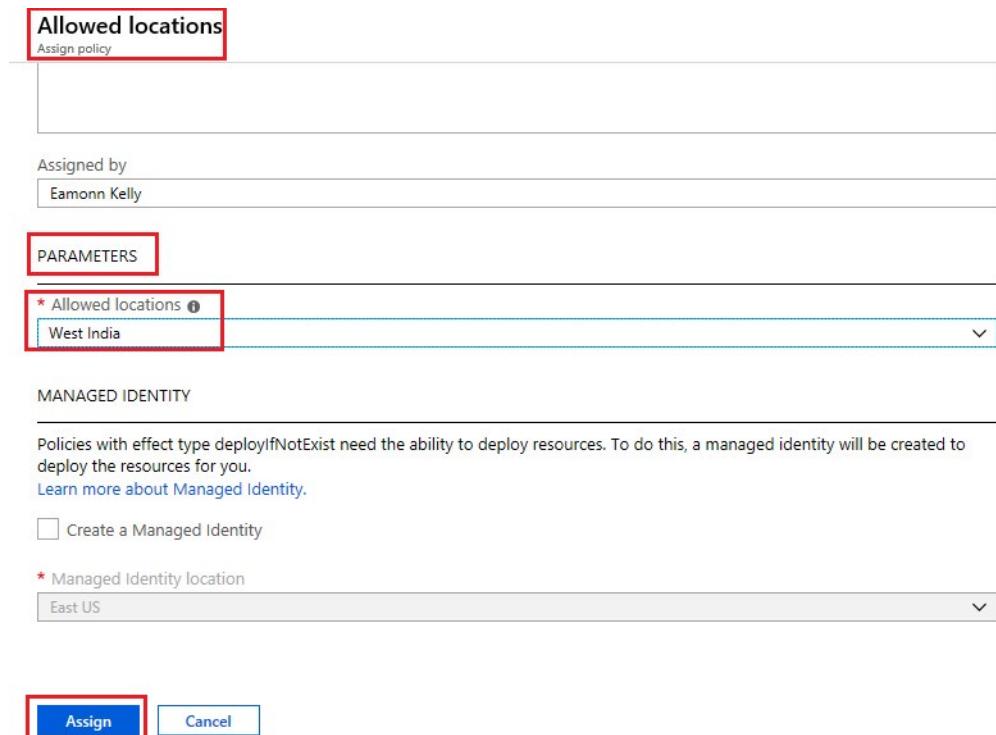
Assign Azure Policy for allowed locations to a Management group and subscription

We will now assign a policy to a Management group and subscription

1. Open **Azure Policy** then under the **Authoring** section, go to **Definitions**, search for the definition **Allowed Locations**, double click on it when located, and in the **Allowed Locations - policy definition** pane click the **Assign** button. Then in the **Scope** pane click the *ellipsis* three dots alongside **Scope** and select the **Contoso Project Mgmt Grp** management group, and then the subscription **New Product Launch**, then click the **Select** button.



2. Under the **Parameters** section, from the drop down list select a region i.e. **West india** then click **Assign**.

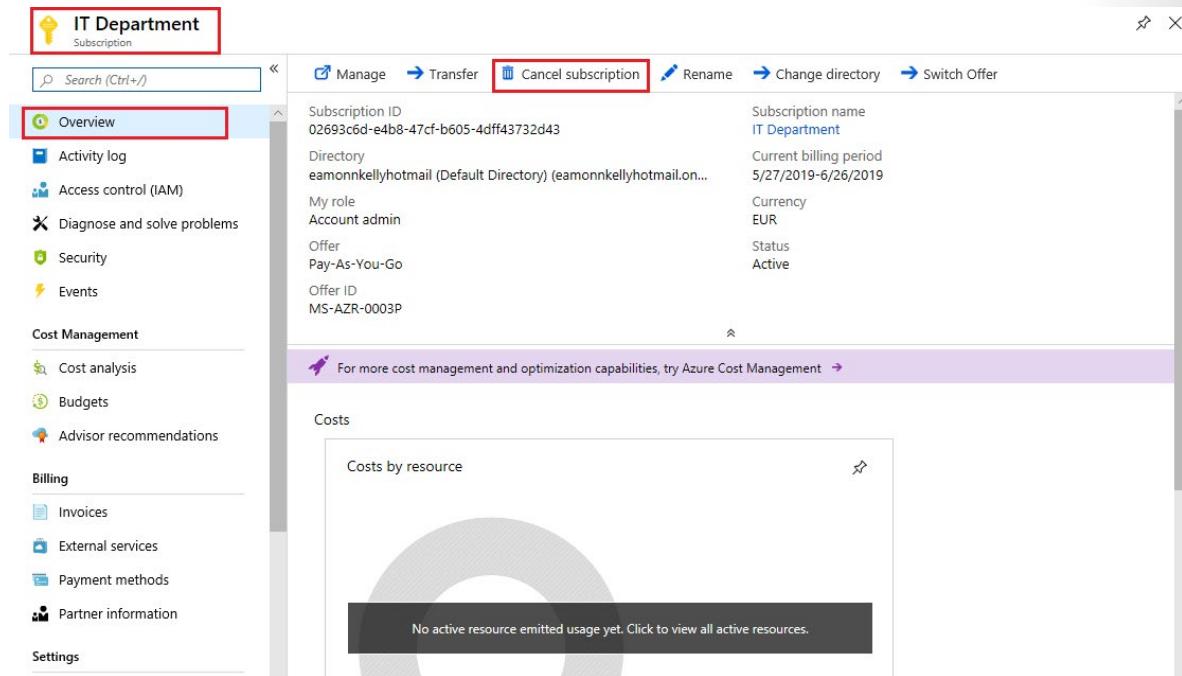


The subscription **New Product Launch** now requires all of its resources to be deployed to **West india** only. A case where this might be useful is related to a product launch, Marketing initiative taking place in West India. This policy has been applied at Management group level and is applicable to the subscription selected. You could also assign many of the other out of box policies at this management

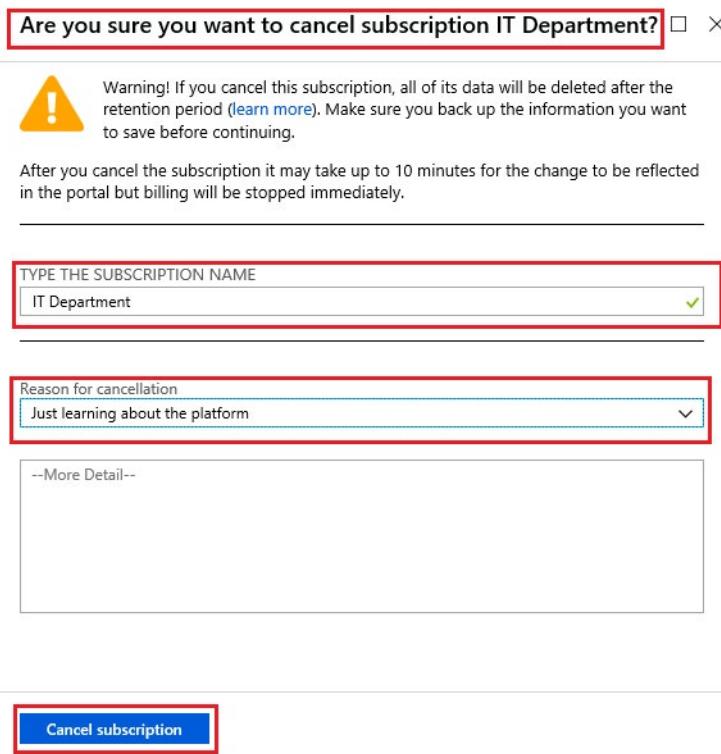
group level to apply to multiple subscriptions, or divide them up as most suitable to your organization and apply various policies needed.

Delete Azure Subscriptions

1. Go to **Subscriptions** and double click on the **IT Department** subscription, go to **Overview** section and then select **Cancel subscription**



2. In the **Are you sure you want to cancel subscription IT Department?** pane type the subscription name, i.e. **IT Department** and select reason for cancellation and then click **Cancel Subscription**.



You will receive an email stating **Since you cancelled your subscription, we've disabled your services. We'll keep your account and any associated data for 90 more days before deleting them on < some date >. Please log in and save any important data you may have stored in this subscription before then.** The subscription will remain listed in the Subscription pane for period of time before it is no longer present.

3. Repeat steps **1** and **2** for the **New Product Launch** subscription.
4. In the subscription **Overview** pane, approx. 10-15 minutes after deletion, despite the subscription still being listed, the status is listed as **Disabled** and a **Re-activate** button is now present, both indicating the subscription is no longer active, while it is waiting to be completely removed.

Subscription ID : 5b9d1ee2-4239-4479-bac0-7d7f40c86de7	Subscription name : New Product Launch
Directory : Default Directory (eamonnkelly@hotmail.onmicrosoft.com)	Current billing period : 5/27/2019-6/26/2019
My role : Account admin	Currency : EUR
Offer : Pay-As-You-Go	Status : Disabled
Offer ID : MS-AZR-0003P	

Delete Management groups

To delete a management group, the following conditions must be met:

- There are no child management groups or subscriptions under the management group.

- You have write permissions on the management group ("Owner", "Contributor", or "Management Group Contributor"). You can see what permissions you have in the Management group Access control (IAM) pane.

As a result of these conditions, we will not be able to delete the management group until the subscription has been deleted, or we move the subscription out of the management group. We will move the subscription.

- Open to the **Contoso Departments Mgmt Grp** and under the **Overview** section click the *ellipsis* alongside the **IT Departments** subscription and select Move from the subsequent context menu

The screenshot shows the 'Contoso Departments Mgmt Grp' management group overview page. On the left, there's a sidebar with links like Overview, Access control (IAM), Policies, Activity Log, Cost Management, Cost analysis, and Budgets. The main area shows the management group details: Name: Contoso Departments Mgmt Grp, ID: contosomgmtgrptID, Access Level: Owner. Below this is a list of subscriptions, with 'IT Department' selected. A context menu is open over the 'Move' button, with the 'Move' option highlighted by a red box.

Note: The Delete button on the Management group page is currently greyed out.

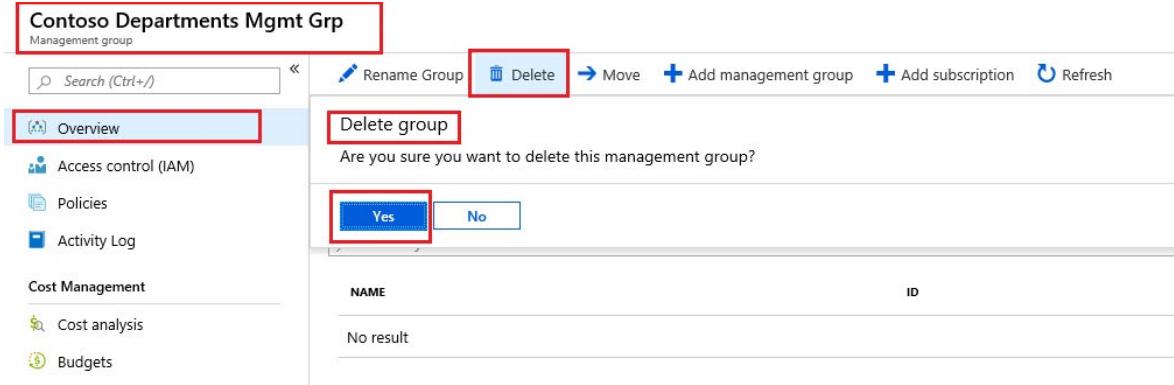
- In the **Move** pane, from the **New parent management group** drop down list choose the **Tenant Root Group (GUID)** then click **Save**

The screenshot shows the 'Move' dialog box. It has fields for 'Resource ID' (02693c6d-e4b8-47cf-b605-4dff43732d43) and 'Resource type' (Subscription). Below these is a dropdown labeled 'New parent management group' which contains 'Tenant Root Group (l...)' and is highlighted by a red box. At the bottom, there are 'Save' and 'Cancel' buttons.

Note the message saying moving a subscription may affect policies and access.

- Back in the **Contoso Departments Mgmt Grp** pane and under the **Overview** section, note that the subscription is no longer present and the **Delete** button is now no longer greyed out. Click **Delete** and in the **Delete group** prompt click **Yes**

MCT USE ONLY. STUDENT USE PROHIBITED



The management group is deleted and no longer present.

4. Repeat steps 1 to 3 for the **Contoso Projects Mgmt Grp** and management group and the **New Product Launch** subscription.

Congratulations! You have created Azure Subscriptions based on organization structure and specific project use, you then created Management groups to manage those newly created subscriptions. You then elevated the logged in user account access, to be able to manage all Azure subscriptions and management groups and then added our subscriptions to our Management groups. You then assigned an Azure Policy for allowed locations to a Management group and subscription. You then deleted your Azure Subscriptions and Management groups.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Planning and Managing costs

Video: Purchasing Options



<https://www.youtube.com/watch?v=Ll6gdDCmU2w>

Purchasing Azure Products and Services

There are three main customer types on which the available purchasing options for Azure products and services is contingent, including:

- *Enterprise*. Enterprise customers sign an Enterprise Agreement with Azure that commits them to spending a negotiated amount on Azure services, which they typically pay annually. Enterprise customers also have access to customized Azure pricing.
- *Web direct*. Web Direct customers sign up for Azure through [the Azure website](#)⁷. Web direct customers pay general public prices for Azure resources, and their monthly billing and payments occur through the Azure website.
- *Cloud Solution Provider*. Cloud Solution Provider (CSP) typically are Microsoft partner companies that a customer hires to build solutions on top of Azure. Payment and billing for Azure usage occurs through the customer's CSP.



Enterprise



Resellers



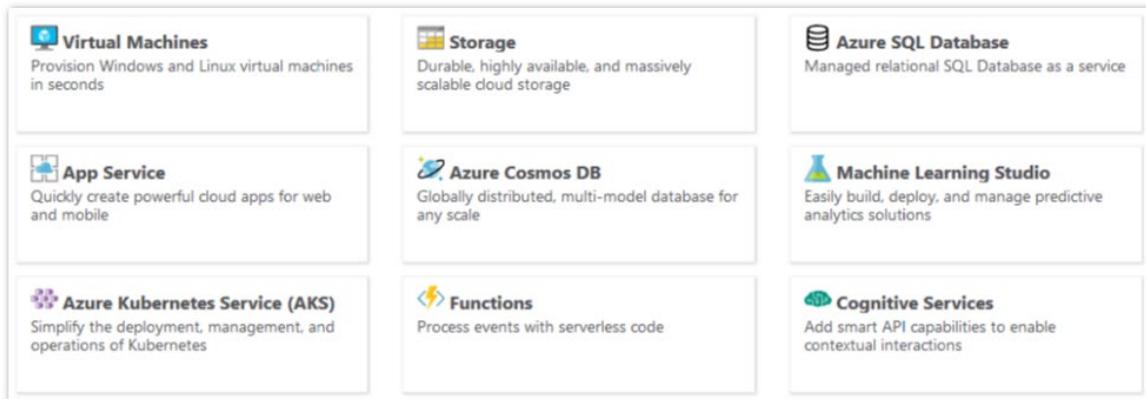
Partners



Personal

Products and services in Azure are arranged by category, which have various resources that you can provision. You select the Azure products and services that fit your requirements, and your account is billed according to Azure's pay-for-what-you-use model.

⁷ <https://azure.microsoft.com>



Usage meters

When you provision an Azure resource, Azure creates one or more meter instances for that resource. The meters track the resources' usage, and each meter generates a usage record that is used to calculate your bill.

For example, a single virtual machine that you provision in Azure might have the following meters tracking its usage:

- Compute Hours
- IP Address Hours
- Data Transfer In
- Data Transfer Out
- Standard Managed Disk
- Standard Managed Disk Operations
- Standard IO-Disk
- Standard IO-Block Blob Read
- Standard IO-Block Blob Write
- Standard IO-Block Blob Delete

Note: For more information about purchasing Azure products and services, refer to [Explore flexible purchasing options for Azure⁸](#).

Azure Free Account

An Azure free account provides subscribers with a \$200 Azure credit that they can use for paid Azure products during a 30-day trial period. Once you use that \$200 credit or reach your trial's end, Azure suspends your account unless you sign up for a paid account.

⁸ <https://azure.microsoft.com/en-us/pricing/purchase-options/>

Azure Free Account

\$200 Azure credit
+
12 months of free services

No commitment – free account does not automatically upgrade to a paid subscription

Frequently asked questions ▾

Free Account sign up

1 About you

* Country/Region ⓘ
United States

* First Name

* Last Name

* Email address for important notifications ⓘ
someone@example.com

* Work Phone
Example: (425) 555-0100

Organization
- Optional -

If you upgrade to a Pay-As-You-Go subscription within the 30-day trial period, by providing your credit or debit card details, you can use a limited selection of free services for 12 months. After 12 months, you will be billed for the services and products in use on your account at the pay-as-you-go rate.

Note: For more information about Azure free accounts, refer to [Create your Azure free account today⁹](#).

Video: Factors Affecting Costs



<https://www.youtube.com/watch?v=9sMaAVG8wnk>

Factors Affecting Costs

The following sections describe the main factors that affect Azure costs, including resource type, services, and the user's location.

Resource type

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

⁹ <https://azure.microsoft.com/en-us/free/>

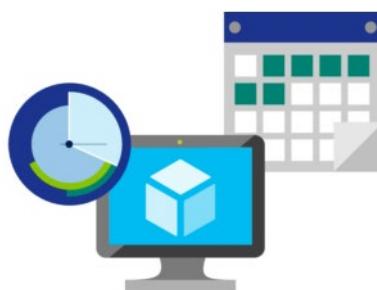
Note: Each meter tracks a *particular kind of usage*. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits-per-second), number of operations, size (storage capacity in bytes), or similar items.

The usage that a meter tracks correlates to a quantity of billable units. Those are charged to your account for each billing period, and the rate per billable unit depends on the resource type you are using.

Services

Azure usage rates and billing periods can differ between Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers. Some subscription types also include usage allowances, which affect costs.

The Azure team develops and offers first-party products and services, while products and services from third-party vendors are available in the [Azure marketplace¹⁰](#). Different billing structures apply to each of these categories.



Location

The Azure infrastructure is globally distributed, and usage costs might vary between locations that offer particular Azure products, services, and resources.

For example, you might want to build your Azure solution by provisioning resources in locations that offer the lowest prices, but this would require transferring data between locations, if dependent resources and their users are located in different parts of the world. If there are meters tracking the volume of data that transfers between the resources you provision, any potential savings you make from choosing the cheapest location could be offset by the additional cost of transferring data between those resources.

Note: For more information about Azure usage charges, refer to [Understand terms on your Microsoft Azure invoice¹¹](#).

Zones for Billing Purposes

Bandwidth refers to data moving in and out of Azure datacenters. Some inbound data transfers, such as data going into Azure datacenters, are free. For outbound data transfers, such as data going out of Azure datacenters, data transfer pricing is based on **Zones**.

¹⁰ <https://azuremarketplace.microsoft.com>

¹¹ <https://docs.microsoft.com/en-us/azure/billing/billing-understand-your-invoice>



A **Zone** is a geographical grouping of Azure Regions for billing purposes. the following **Zones** exist and include the sample regions as listed below:

- Zone 1 – West US, East US, Canada West, West Europe, France Central and others...
- Zone 2 – Australia Central, Japan West, Central India, Korea South and others...
- Zone 3 - Brazil South
- DE Zone 1 - Germany Central, Germany Northeast

Note: To avoid confusion, be aware that a *Zone for billing purposes* is not the same as an *Availability Zone*. In Azure, the term *Zone* is for billing purposes only, and the full term *Availability Zone* refers to the failure protection that Azure provides for datacenters.

Note: For more information about data transfer pricing and Zones, refer to the FAQ section on the page [Bandwidth Pricing Details¹²](#).

Video: Planning Costs



https://www.youtube.com/watch?v=_snVprbVm20

Pricing Calculator

The *Pricing Calculator* is a tool that helps you estimate the cost of Azure products. It displays Azure products in categories, and you choose the Azure products you need and configure them according to your specific requirements. Azure then provides a detailed estimate of the costs associated with your selections and configurations.

Note: The pricing calculator provides estimates, *not* actual price quotes. Actual prices may vary depending upon the date of purchase, the payment currency you are using, and the type of Azure customer you are.

Get a new estimate from the pricing calculator by adding, removing, or reconfiguring your selected products. You also can access pricing details, product details, and documentation for each product from the pricing calculator.

¹² <https://azure.microsoft.com/en-us/pricing/details/bandwidth/>

Your Estimate

The screenshot shows the Azure Pricing Calculator interface. At the top, it displays "Virtual Machines" and "1 D2 v3 (2 vCPU(s), 8 GB RAM) x 730 Hours;" with a total price of "\$188.57". Below this, there's a summary section for "Virtual Machines" with dropdown menus for "REGION: West US", "OPERATING SYSTEM: Windows", "TYPE: (OS Only)", and "TIER: Standard". A "Clone" and "Delete" button are also present. To the right, there are links for "More info", "Pricing details", "Product details", and "Documentation". At the bottom, a summary box shows "D2 v3: 2 vCPU(s), 8 GB RAM, 50 GB Temporary storage, \$0.209/hour".

The options that you can configure in the pricing calculator vary between products, but basic configuration options include:

- *Region*. Lists the regions from which you can provision a product. Southeast Asia, central Canada, the western United States, and Northern Europe are among the possible regions available for some resources.
- *Tier*. Sets the type of tier you wish to allocate to a selected resource, such as Free Tier, Basic Tier, etc.
- *Billing Options*. Highlights the billing options available to different types of customer and subscriptions for a chosen product.
- *Support Options*: Allows you to pick from included or paid support pricing options for a selected product.
- *Programs and Offers*. Allows you to choose from available price offerings according to your customer or subscription type.
- *Azure Dev/Test Pricing*. Lists the available development and test prices for a product. Dev/Test pricing applies only when you run resources within an Azure subscription that is based on a Dev/Test offer.

Note: For more information about the pricing calculator, refer to [Pricing Calculator¹³](#).

Demo: Generate an Azure Pricing Calculator estimate



https://www.youtube.com/watch?v=rm3d_6Si0QU

¹³ <https://azure.microsoft.com/en-us/pricing/calculator/>

Walkthrough-Generate an Azure Pricing Calculator estimate

In this walkthrough, you will generate and then download a cost estimate for a specific resource configuration in Azure, using the Azure Pricing Calculator. The estimate will outline the costs of running a Virtual Machine (VM) and related network resources in Azure.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Note: To create an Azure Pricing Calculator estimate, this walkthrough provides example configurations for the VM and related resources. Use the example configurations or provide the Azure Pricing Calculator with details of your *actual* resource requirements instead.

Steps

1. In a browser, navigate to the [Azure Pricing Calculator](#)¹⁴ webpage.
2. To add details of your VM configuration, select **Virtual Machines** from the **Products** tab. Inside the **Virtual Machines added** message dialog, choose **View**.

The screenshot shows the Azure Pricing Calculator web interface. At the top, there's a navigation bar with 'Products' (selected), 'Estimates', and 'FAQ'. Below the header, a blue banner says 'Select a product to include it in your estimate.' On the left, a sidebar lists various service categories: Featured, Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, and AI + Machine Learning. The 'Featured' category is highlighted with a blue background. In the main content area, there are several product cards: 'Virtual Machines' (highlighted with a red box), 'Storage', 'Azure SQL Database', 'App Service', 'Azure Cosmos DB', 'Azure Kubernetes Service (AKS)', 'Azure Functions', 'Cognitive Services', and a 'Virtual Machines added' message dialog (also highlighted with a red box). The message dialog contains text about optimizing costs and a 'View' link.

3. Enter a name for your Azure Pricing Calculator estimate, and a name for your VM configuration. This walkthrough example uses **My Pricing Calculator Estimate** for the estimate, and **Windows VM** for the VM configuration.

¹⁴ <https://azure.microsoft.com/en-us/pricing/calculator/>

The screenshot shows a summary of a pricing calculator estimate. At the top, it says "My Pricing Calculator Estimate". Below that, it details a "Virtual Machines: Windows VM" configuration: "1 D2 v3 (2 vCPU(s), 8 GB RAM) x 730 Hours;..." with a total cost of "\$152.62". On the left, there's a small icon of a computer monitor with a blue cube on it, followed by the text "Windows VM". To the right of the monitor icon are three buttons: "Clone" (with a plus sign and a copy icon) and "Delete" (with a trash can icon). Above the monitor icon, there are three circular icons with arrows: a blue one with a clockwise arrow, a green one with a counter-clockwise arrow, and a red one with a delete icon.

4. Modify the default VM configuration to match the following VM details.

Region	Operating system	Type
North Europe	Windows	(OS only)

Tier	Instance
Standard	A2: 2 Core(s), 3.5 GB RAM, 135 GB Temporary storage

The screenshot shows the "Windows VM" configuration screen. It has four main sections: "REGION:" with a dropdown set to "North Europe", "OPERATING SYSTEM:" with a dropdown set to "Windows", "TYPE:" with a dropdown set to "(OS Only)", and "TIER:" with a dropdown set to "Standard". Below these, there's a "INSTANCE:" section with a dropdown containing the text "A2: 2 Cores(s), 3.5 GB RAM, 135 GB Temporary storage, \$0.18/hour". The entire "INSTANCE:" section is highlighted with a red rectangle. The background of the page is light gray.

Note: The VM instance specifications and pricing may differ from those in this example. Follow this walkthrough by choosing an instance that matches the example as closely as possible. To view details about the different VM product options, choose **Product details** from the **More info** menu on the right.

5. Set the **Billing Option** to **Pay as you go**.

Billing Option

1 year reserved option is not available for your instance selection.

3 year reserved option is not available for your instance selection.

Pay as you go

1 year reserved

3 year reserved

Save up to 40% with Windows Server Licenses you already own. [Learn more about Azure Hybrid Benefit to save compute costs.](#)



6. In Azure, a month is defined as 730 hours. If your VM needs to be available 100 per cent of the time each month, you set the hours-per-month value to 730. This walkthrough example requires one VM to be available 50 per cent of the time each month.

Leave the number of VMs set at 1, and change the hours-per-month value to 365.

Billing Option

1 year reserved option is not available for your instance selection.

3 year reserved option is not available for your instance selection.

Pay as you go

1 year reserved

3 year reserved

Save up to 40% with Windows Server Licenses you already own. [Learn more about Azure Hybrid Benefit to save compute costs.](#)



Virtual machines

Hours

= \$65.70
Per month

7. In the **Managed OS Disks** pane, modify the default VM storage configuration by adding the following details.

Tier	Disk size	Number of disks	Snapshot	Storage transactions
Standard HDD	S30: 1024 GiB	1	Off	10,000

The screenshot shows the Azure Pricing Calculator interface. A red box highlights the configuration for 'Managed OS Disks'. It specifies a 'TIER: Standard HDD' and a 'DISK SIZE: S30: 1024 GiB, \$40.960/month'. Below this, it shows '1 Disks' at '\$40.96 Per month' with a total of '\$40.96'. Another red box highlights the 'Storage transactions' section, which shows '10000 Transaction units (10,000 transactions)' at '\$0.0005 Per unit' with a total of '\$5.00'.

- To add networking bandwidth to your estimate, go to the top of the Azure Pricing Calculator webpage. Select **Networking** from the product menu on the left, then choose the **Bandwidth** tile. Inside the **Bandwidth added** message dialog, select **View**.

The screenshot shows the 'Networking' section of the Azure portal. A red arrow points to the 'Networking' link in the sidebar. The main area displays several networking services: Virtual Network, Load Balancer, Application Gateway, VPN Gateway, Azure DNS, Content Delivery Network, Azure DDoS Protection, Traffic Manager, ExpressRoute, Network Watcher, Bandwidth, and IP Addresses. The 'Bandwidth' tile is highlighted with a red box and a message 'Bandwidth added. [View](#)'. A red box also surrounds the 'Bandwidth' tile.

- Add a name for your VM bandwidth configuration. This walkthrough example uses the name **Bandwidth: Windows VM**. Modify the default bandwidth configuration by adding the following details.

Region	Zone 1 Outbound Data Transfer Amount
North Europe	50 GB

MCT USE ONLY. STUDENT USE PROHIBITED

Outbound Data Transfer

The first 5 GB/Month of data transfer is free in each zone.

Zone 1: North America, Europe

50	= \$3.91
GB	

10. To add an Application Gateway, return to the top of the Azure Pricing Calculator webpage. From within the **Networking** product menu, choose the **Application Gateway** tile. Inside the **Application Gateway** message dialog, select **View**.

- Featured
- Compute
- Networking**
- Storage
- Web
- Mobile
- Containers
- Databases
- Analytics
- AI + Machine Learning
- Internet of Things
- Integration
- Identity

Virtual Network
Provision private networks, optionally connect to on-premises datacenters

Load Balancer
Deliver high availability and network performance to your applications

Application Gateway
Build secure, scalable, and highly available web front ends in Azure

VPN Gateway
Establish secure, cross-premises connectivity

Azure DNS
Host your DNS domain in Azure

Content Delivery Network
Ensure secure, reliable content delivery with broad global reach

Azure DDoS Protection
Protect your applications from Distributed Denial of Service (DDoS) attacks

Traffic Manager
Route incoming traffic for high performance and availability

ExpressRoute
Dedicated private network fiber connections to Azure

Network Watcher
Network performance monitoring and diagnostics solution

Bandwidth
Data transferred out of Azure data centers

IP Addresses
A dynamic or reserved address used to identify a given Virtual Machine or Cloud Service

11. Add a name for your Application Gateway configuration. This walkthrough uses the name **App Gateway: Windows VM**. Modify the default Application Gateway configuration by adding the following details.

Region	Tier	Size
North Europe	Basic	Small
Instances	Hours	
1	365	

Data processed
50 GB

Zone 1: North America, Europe
50 GB

 App Gateway: Windows VM

REGION: North Europe TIER: Basic
SIZE: Small

Gateway hours
1 Instances × 365 Hours = \$10.22

Data processed
50 GB = \$0.40

Zone 1: North America, Europe
50 GB = \$3.91

Sub-total \$14.54

12. Go to the bottom of the Azure Pricing Calculator webpage to view your total **Estimated monthly cost**.

Note: Explore the various options available within the Azure Pricing Calculator. For example, this walkthrough requires you to update the currency to Euro.

Change the currency to Euro, then select **Export** to download a copy of the estimate for offline viewing in Microsoft Excel (.xlsx) format.

The screenshot shows the Microsoft Azure Pricing Calculator interface. At the top right, the estimated monthly cost is displayed as €109.72. Below it, there are three buttons: 'Export' (highlighted with a red box), 'Save' (highlighted with a blue box), and 'Share'. To the right of the cost, a dropdown menu shows 'Euro (€)' with a red box around it. A large red arrow points down from the 'Save' button to a file download dialog box. The dialog box has 'Save' highlighted with a blue box and contains the text: 'What do you want to do with ExportedEstimate.xlsx (56.2 KB)? From: azure.microsoft.com'. Other buttons in the dialog are 'Open', 'Cancel', and 'X'.

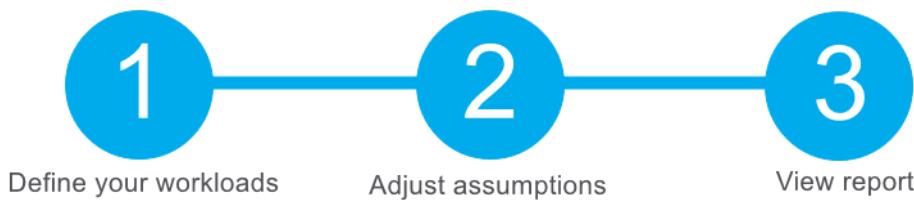
Microsoft Azure Estimate				
My Pricing Calculator Estimate				
Service type	Custom name	Region	Description	Estimated Cost
Virtual Machines	Windows VM	North Europe	1 A2 (2 vCPU(s), 3.5 GB RAM) x 365 Hours; Windows – (OS Only): P	€94.16
Bandwidth	Bandwidth: Windows VM	North Europe	Zone 1: North America, Europe, 50 GB	€3.30
Application Gateway	App Gateway: Windows VM	North Europe	Basic tier, Small Instance size: 1 Gateway hours instance(s) x 365 H	€12.26
Support			Support	€0.00
			Licensing Program	Microsoft Online S
			Monthly Total	€109.72
			Annual Total	€1,316.66

Disclaimer
All prices shown are in Euro (€). This is a summary estimate, not a quote. For up to date pricing information please visit [this link](#).
This estimate was created at 3/30/2019 10:01:38 PM UTC.

Congratulations! You downloaded an estimate from the Azure Pricing Calculator.

Total Cost of Ownership (TCO) Calculator

The *Total Cost of Ownership* (TCO) Calculator is a tool that you use to estimate cost savings you can realize by migrating to Azure. To use the TCO calculator, complete the three steps that the following sections explain.



Step 1: Define your workloads

Enter details about your on-premises infrastructure into the TCO calculator according to four groups:

- *Servers*. Enter details of your current on-premises server infrastructure.
- *Databases*. Enter details of your on-premises database infrastructure in the **Source** section. In the **Destination** section, select the corresponding Azure service you would like to use.
- *Storage*. Enter the details of your on-premises storage infrastructure.

MCT USE ONLY. STUDENT USE PROHIBITED

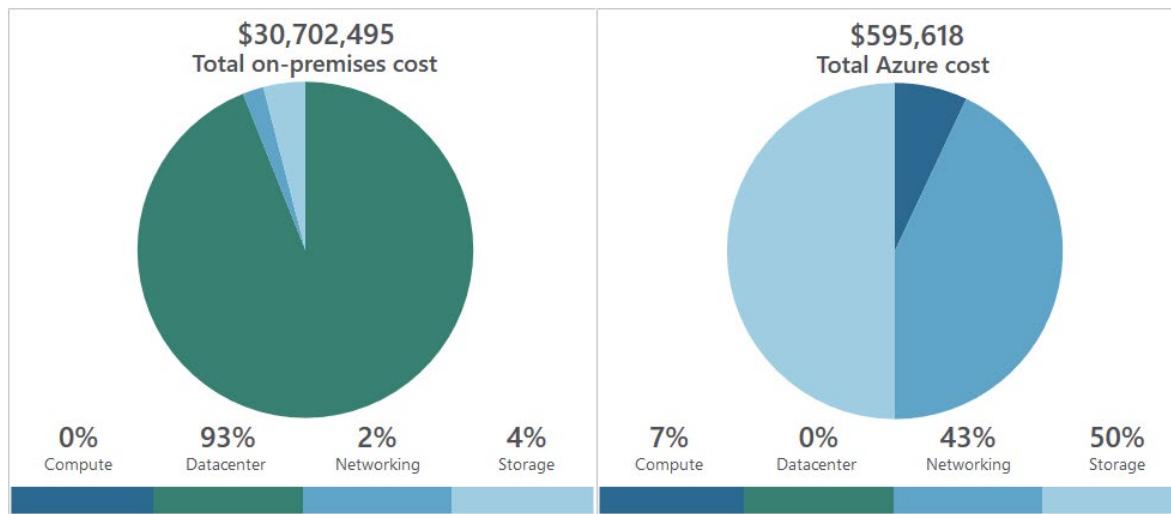
- *Networking.* Enter the amount of network bandwidth you currently consume in your on-premises environment.

Step 2: Adjust assumptions

Adjust the values of key assumptions that the TCO calculator makes, which might vary between customers. To improve the accuracy of the TCO calculator, you should adjust the values so they match the costs of your current on-premises infrastructure. The assumption values you can adjust include:

- Storage costs
- IT labor costs
- Hardware costs
- Software costs
- Electricity costs
- Virtualization costs
- Datacenter costs
- Networking costs
- Database costs

Step 3: View the report



The TCO calculator generates a detailed report based on the details you enter and the adjustments you make. The report allows you to compare the costs of your on-premises infrastructure with the costs using Azure products and services to host your infrastructure in the cloud.

Note: For more information about the TCO Calculator, refer to **Total Cost of Ownership (TCO) Calculator¹⁵**.

¹⁵ <https://azure.microsoft.com/en-us/pricing/tco/>

Demo: Generate an Azure TCO Calculator cost comparison report



<https://www.youtube.com/watch?v=Y1H3aQqERuM>

Walkthrough-Generate an Azure TCO Calculator cost comparison report

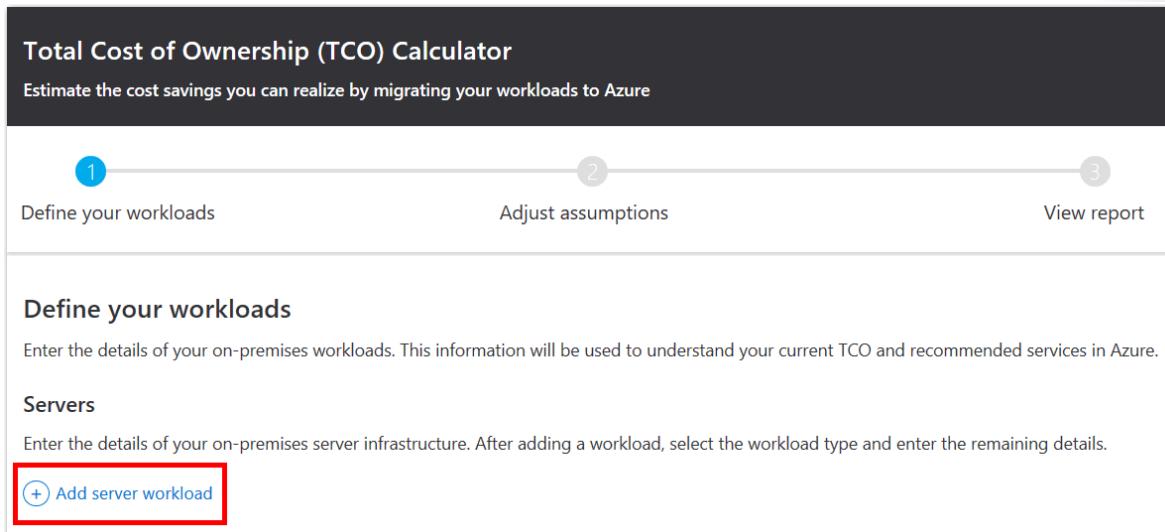
In this walkthrough, you will generate and then download a cost comparison report for infrastructure and resources running in an on-premises environment versus running in Azure, using the *Total Cost of Ownership (TCO) Calculator* in Azure. To create the report, the TCO Calculator uses information that you provide about your on-premises infrastructure and workloads to recommend cost savings that you can make with Azure.

Note: This walkthrough provides example definitions of on-premises infrastructure and workloads for a typical datacenter. To create a TCO Calculator report, use the example definitions or provide details of your *actual* on-premises infrastructure and workloads.

Finish this walkthrough by completing the steps that follow, or by reading through them.

Steps

1. In a browser, navigate to the **Total Cost of Ownership (TCO) Calculator¹⁶** webpage.
2. To add details of your on-premises server infrastructure, select **+ Add server workload** in the **Servers** pane.



The screenshot shows the 'Total Cost of Ownership (TCO) Calculator' interface. At the top, it says 'Total Cost of Ownership (TCO) Calculator' and 'Estimate the cost savings you can realize by migrating your workloads to Azure'. Below this is a progress bar with three steps: 1. Define your workloads (highlighted with a red box), 2. Adjust assumptions, and 3. View report. The main area is titled 'Define your workloads' and contains a 'Servers' section. It says 'Enter the details of your on-premises server infrastructure. After adding a workload, select the workload type and enter the remaining details.' A blue button labeled '+ Add server workload' is visible, with a red box drawn around it to indicate it is the next step to take.

¹⁶ <https://azure.microsoft.com/en-us/pricing/tco/calculator/>

3. Provide a name for your server workloads definition. This example uses the name **Servers: Windows VMs**. Enter the following details into the TCO Calculator.

Workload	Environment	Operating system	VMS	Virtualization	Core(s)	RAM	Optimize by
Windows/ Linux server	Virtual machines	Windows	500	VMware	8	16	CPU

Servers: Windows VMs

Workload	Environment	Operating system	VMs	Virtualization	Core(s)	
Windows/Linux Server	Virtual Machines	Windows	500	VMware	8	
RAM (GB)			(1 - 9999)	(1 - 32)		
Optimize by			Windows Server 2008/2008 R2			
16	CPU					
(1 - 448)						

4. Select **+ Add server workload** to make a row for a new server workloads definition. Provide a name for the server workloads definition. This example uses the name **Servers: Linux VMs**. Enter the following details into the TCO Calculator.

Workload	Environment	Operating system	VMS	Virtualization	Core(s)	RAM	Optimize by
Windows/ Linux server	Virtual machines	Linux	500	VMware	8	16	CPU

Servers: Linux VMs

Workload	Environment	Operating system	VMs	Virtualization	Core(s)	
Windows/Linux Server	Virtual Machines	Linux	500	VMware	8	
RAM (GB)			(1 - 9999)	(1 - 32)		
Optimize by			Windows Server 2008/2008 R2			
16	CPU					
(1 - 448)						

5. This example definition does not require a database. Leave the **Databases** pane empty. In the **Storage** pane of the TCO Calculator, provide a name for your storage infrastructure definition. Enter the following details into the TCO Calculator.

Storage type	Disk type	Capacity	Backup	Archive
Local Disk/ SAN	HDD	60 TB	0 TB	0 TB

MCT USE ONLY. STUDENT USE PROHIBITED

Storage					
Storage type	Disk type	Capacity	Backup	Archive	
Local Disk/SAN	HDD	60	0	0	
		TB	TB	TB	
(1 - 5000)			(1 - 5000)		(1 - 5000)

6. In the **Networking** pane of the TCO Calculator, enter the following details, then select **Next**.

Outbound bandwidth
15 TB

Networking

Enter the amount of network bandwidth you currently consume in your on-premises environment.

Outbound bandwidth: 15 TB (1 - 2000)

Next

7. Explore the options and make any adjustments that you require. The currency used in this example is Euros. No other adjustments are required by this example. Select **Next**, at the end of the page.

1
2
3

Define your workloads
Adjust assumptions
View report

Adjust assumptions

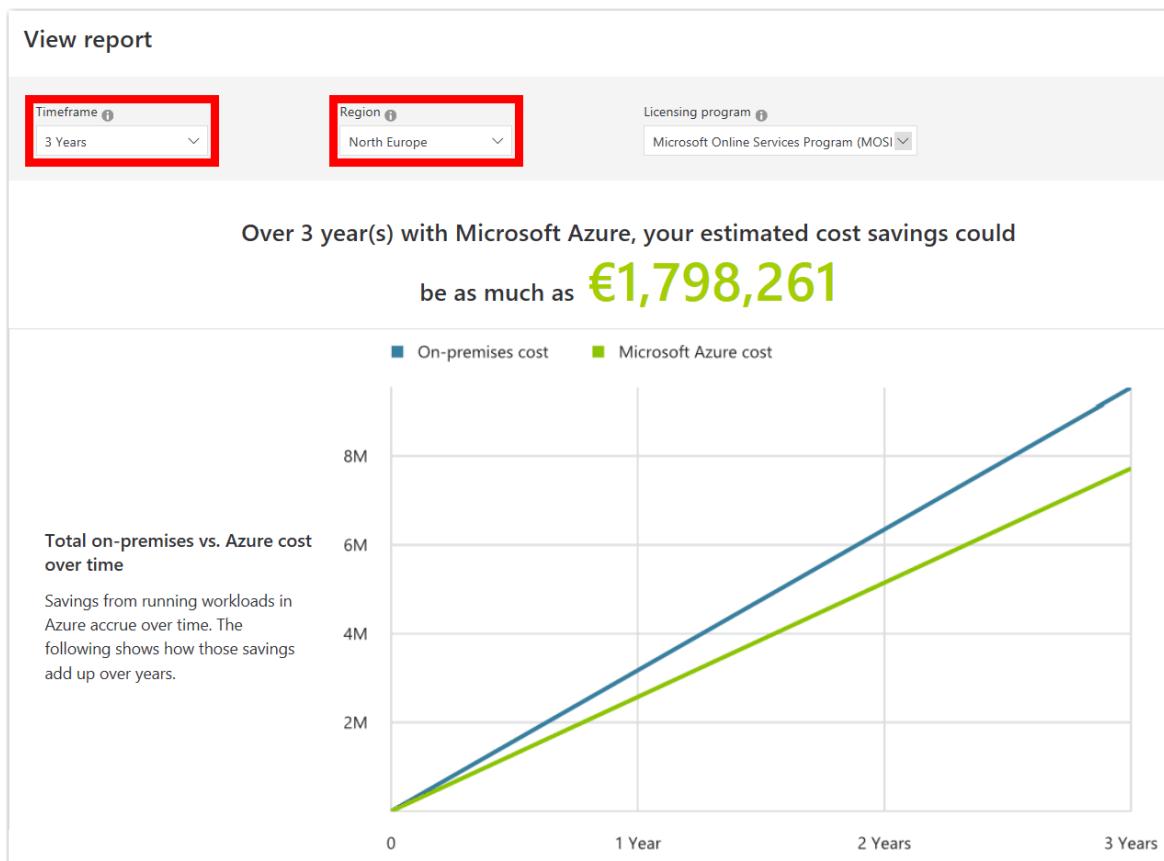
The following assumptions are being made as part of the TCO model. These key assumptions usually vary among customers. We recommend reviewing these values for accuracy.

Currency: Euro (€)

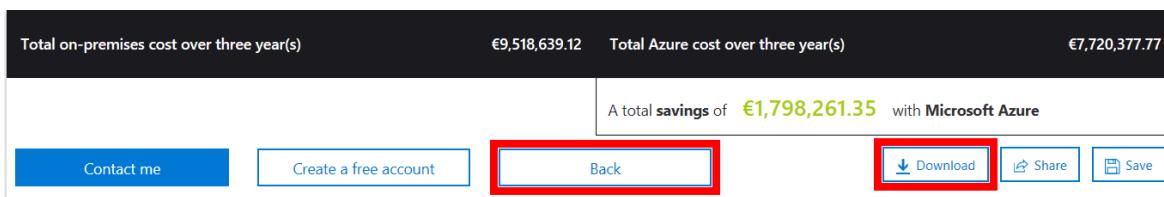
Virtualization costs
Data center costs
Networking costs
Database costs

Next

8. Review the Azure cost saving recommendations and visualizations in the TCO calculator report. This example requires you to adjust the **Timeframe** to **3 years**, and the region to **North Europe**.



9. To modify the information you provided to the TCO calculator, go to the bottom of the page, and select **Back**. To save or print a PDF copy of the report select **Download**.



Congratulations! You downloaded a cost comparison report from the TCO Calculator in Azure.

Video: Minimizing Costs



<https://www.youtube.com/watch?v=FEEHuM0Xjuw>

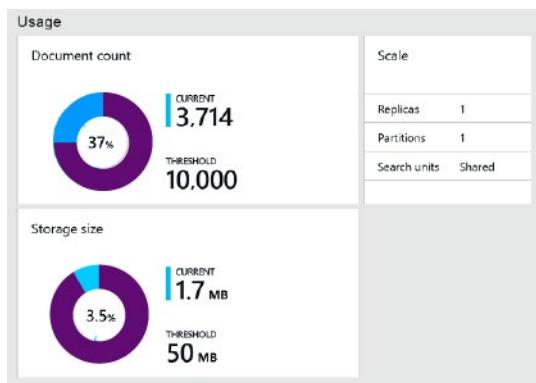
Minimizing Costs

The following best practice guidelines can help minimize your Azure costs.

Perform cost analyses

Plan your Azure solution wisely. Carefully consider the products, services, and resources you need, and read the relevant documentation to understand how each of your choices are metered and billed. Additionally, you should calculate your projected costs by using the Azure Pricing and Total Cost of Ownership (TCO) calculators, only adding the products, services, and resources you need.

Monitor usage with Azure Advisor



In an efficient architecture, provisioned resources match the demand for those resources. The *Azure Advisor* feature identifies unused or under-utilized resources, and you can implement its recommendations by removing unused resources and configuring your resources to match your actual demand.

Note: For more information about Azure Advisor, refer to [Azure Advisor¹⁷](#).

Use spending limits

Free trial customers and some credit-based Azure subscriptions can use the *Spending Limits* feature. Azure provides the Spending Limits feature to help prevent you from exhausting the credit on your account within each billing period. If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.

The spending limit feature is not available for customers who aren't using credit-based subscriptions, such as Pay-As-You-Go subscribers.

Note: For more information on Azure spending limits, refer to [Understand Azure spending limit and how to remove it¹⁸](#).

Note: Azure spending limits are not the same as Subscription, Service, or Resource Group limits and quotas. For more information, refer to [Azure subscription and service limits, quotas, and constraints¹⁹](#).

¹⁷ <https://azure.microsoft.com/en-us/services/advisor/>

¹⁸ <https://docs.microsoft.com/en-us/azure/billing/billing-spending-limit/>

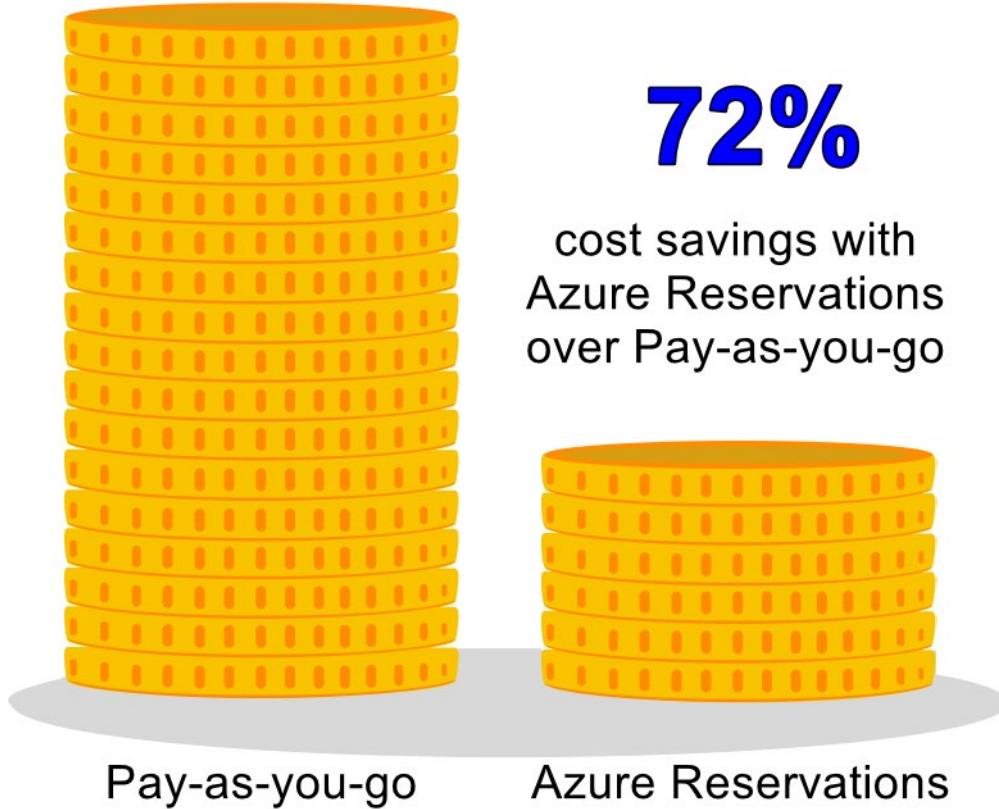
¹⁹ <https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits/>

Use Azure Reservations

Azure Reservations offer discounted prices on certain Azure products and resources. To get a discount, you reserve products and resources by paying in advance. You can pre-pay for one year or three years of use of Virtual Machines, SQL Database Compute Capacity, Azure Cosmos Database Throughput, and other Azure resources.

Azure Reservations are only available to Enterprise or CSP customers and for Pay-As-You-Go subscriptions.

Note: For more information on Azure Reservations, refer to [What are Azure Reservations?](#)²⁰



Choose low-cost locations and regions

The cost of Azure products, services, and resources can vary across locations and regions, and if possible, you should use them in those locations and regions where they cost less.

Note: Some resources are metered and billed according to how much outgoing network bandwidth they consume (egress). *You should provision connected resources that are bandwidth metered in the same region to reduce egress traffic between them.*

Research available cost-saving offers

Keep up-to-date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

²⁰ <https://docs.microsoft.com/en-us/azure/billing/billing-save-compute-costs-reservations>

Go to the [Azure Updates page²¹](#) for information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements.

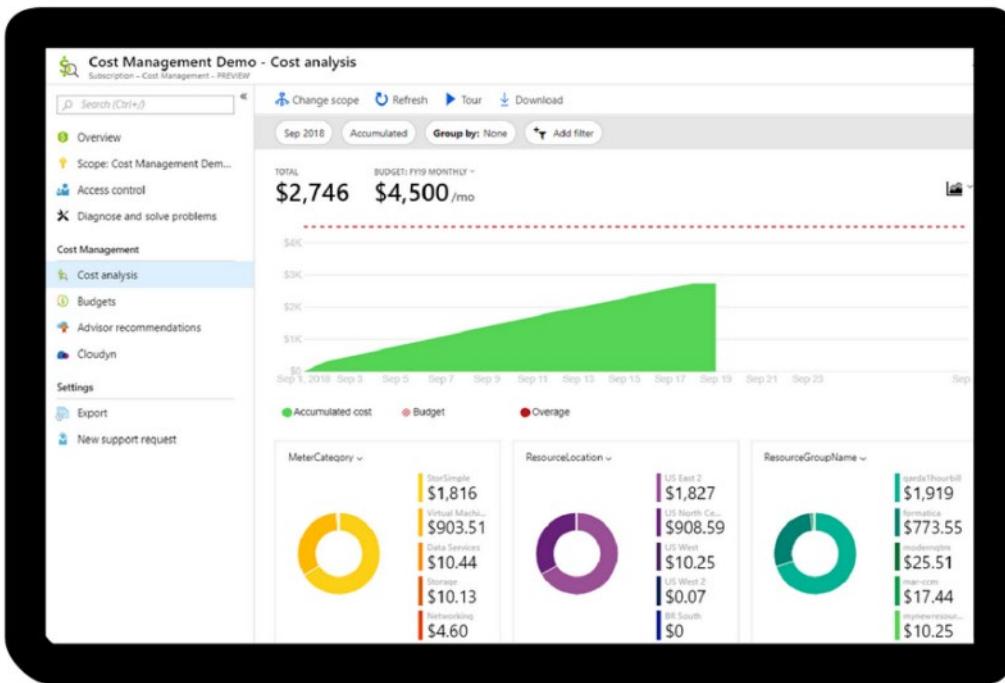
Apply tags to identify cost owners

Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure products and resources to organize billing data. For example, if you run several virtual machines for different teams, you can use tags to categorize costs by department, such as Human Resources, Marketing, or Finance, or by environment, such as Production or Test. Tags make it easy to identify groups that generate the biggest Azure costs, so you can adjust your spending accordingly.

Note: For more information about tags, refer to [Use tags to organize your Azure resources²²](#).

Azure Cost Management

Cost Management is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.



The main features of the Azure Cost Management toolset include:

- *Reporting*. Generate reports using historical data to forecast future usage and expenditure.
- *Data enrichment*. Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.
- *Budgets*. Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.

²¹ <https://azure.microsoft.com/en-us/updates/>

²² <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

- *Alerting*. Get alerts based on your cost and usage budgets.
- *Recommendations*. Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.
- *Price*. Free to Azure customers.

Note: For more information about Cost Management, refer to **Cost Management²³**.

²³ <https://azure.microsoft.com/en-us/services/cost-management/>

Support Options Available with Azure

Video: Support Plan Options



https://www.youtube.com/watch?v=_F3AHwc2JQI

Support Plan Options

Every Azure subscription includes free access to the following basic support services:

- Billing and subscription support.
- Azure products and services documentation.
- Online self-help documentation.
- Whitepapers.
- Community support forums.

Paid Azure support plans

Microsoft offers four paid Azure support plans for customers who require technical and operational support. Providing different Azure support options allows Azure customers to choose a plan that best fits their needs.

			
Documentation	Support FAQ	Issues signing up	Learn about billing
			
Azure Advisor	Azure Service Health	SLAs	Support community

The following descriptions explain how Azure paid support plans extend the free basic support services.

	Developer	Standard	Professional Direct	Premier
Scope	Trial and non-production environments	Production workload environments	Business-critical dependence	Substantial dependence across multiple products
Technical Support	Business hours access to Support Engineers via email	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone

	Developer	Standard	Professional Direct	Premier
Case Severity/ Response Times	Minimal business impact (Sev C): <8 business hours ¹	Critical business impact (Sev A): <1 hour	Critical business impact (Sev A): <1 hour	Critical business impact (Sev A): <1 hour <15 minutes (with Azure Rapid Response or Azure Event Management)
Architecture Support	General guidance	General guidance	Architectural guidance based on best practice delivered by ProDirect Delivery Manager	Customer specific architectural support such as design reviews, performance tuning, configuration and more
Operations Support			Onboarding services, service reviews, Azure Advisor consultations	Technical account manager-led service reviews and reporting
Training			Azure Engineering-led web seminars	Azure Engineering-led web seminars, on-demand training
Proactive Guidance			ProDirect Delivery Manager	Designated Technical Account Manager
Launch Support				Azure Event Management (available for additional fee)

Support-plan availability and billing

The support plans you can select and how you are billed for support depends on the type of Azure customer you are, and on the type of Azure subscription you have.

For example, Developer support is not available to Enterprise customers. Enterprise customers can purchase Standard, Professional Direct, and Premier support plans, and be billed for support as part of an Enterprise Agreement (EA). Alternatively, if you purchase a support plan within a pay-as-you-go subscription, your support plan is charged to your monthly Azure subscription bill.

Note: For more information about Azure support options, refer to [Azure support plans²⁴](#).

²⁴ <https://azure.microsoft.com/en-us/support/plans/>

Video: Accessing Support



https://www.youtube.com/watch?v=8JHlu_9uhD4

Alternative Support Channels

There are several additional support channels that are available outside Azure's official support plans, and the following sections detail them.

Microsoft Developer Network (MSDN) Forums



Get support by reading responses to Azure technical questions from Microsoft's developers and testers on the [MSDN Azure discussion forums²⁵](#).

Stack Overflow



You can review answers to questions from the development community on [StackOverflow²⁶](#).

²⁵ <https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform>

²⁶ <https://stackoverflow.com/questions/tagged/azure>

Server Fault



Review community responses to questions about System and Network Administration in Azure on [ServerFault²⁷](https://serverfault.com/questions/tagged/azure).

Azure Feedback Forums



Read ideas and suggestions for improving Azure made by Azure users and customers on the [Azure Feedback Forums²⁸](https://feedback.azure.com/forums/34192--general-feedback).

Twitter



Tweet @AzureSupport to get answers and support from the [official Microsoft Azure Twitter channel²⁹](#).

Note: For more information about alternative Azure support channels, refer to [Azure Community Support³⁰](#).

Knowledge Center

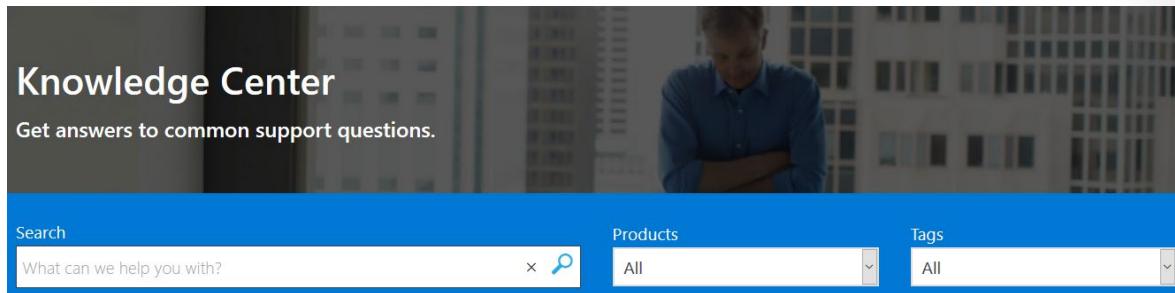
The Azure Knowledge Center is a searchable database that contains answers to common support questions, from a community of Azure experts, developers, customers, and users.

²⁷ <https://serverfault.com/questions/tagged/azure>

²⁸ <https://feedback.azure.com/forums/34192--general-feedback>

²⁹ <https://twitter.com/azuresupport>

³⁰ <https://azure.microsoft.com/en-us/support/community/>



You can browse through all answers within the Azure Knowledge Center. Find specific solutions by entering keyword search terms into the text-entry field and further refine your search results by selecting products or tags from the lists provided by two dropdown lists.

Note: For more information about Azure Knowledge Center, refer to [Knowledge Center³¹](#).

Walkthrough-Open a Support Request

In this walkthrough task we will view available support plan options and then create a new support request. Once created we will then see how to monitor and interact with a support request.

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 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 today³²](#) webpage.

Steps

View available support plan options and create a new support request

1. Log into the Azure portal.
2. Choose **Help + support** from the left navigation menu, to open the **Help + Support** blade:

³¹ <https://azure.microsoft.com/en-us/resources/knowledge-center/>

³² https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

3. On the **Help + Support** blade, select **New support request**, then on the **Basics** tab fill in the fields as below. Once finished click **Next: Solutions >>**. The fields which appear are dependent on the values you placed in the preceding field.

- Issue type:** Technical
- Subscription:** < choose your subscription >
- Service:** < check the radio button **All services** then scroll down through the drop down list of issues, and select **Virtual Machine running Linux** >
- Problem Type:** VM performance
- Problem subtype:** Disk throughput is lower than expected
- Subject:** Slow disk perf

Note: All Azure customers can access billing, quota, and subscription-management support. *The availability of support for other issues depends on the support plan you have.*

4. On the **New support request > Solutions** tab read through the recommended solutions then click **Next: Details >>**

The screenshot shows the 'Help + support - New support request' interface. The left sidebar has a 'Support' section with a 'New support request' button highlighted by a red box. The main area has tabs: 'Basics' (highlighted), 'Solutions' (highlighted with a red box), 'Details', and 'Review + create'. A section titled 'Want a solution right now?' contains a 'Recommended Solution' box. This box includes a heading 'Recommended Solution', a note '4 out of 5 customers resolved their performance issue using the below steps.', a section 'Recommended Documents' with a list of links, and a 'Was this helpful? Yes No' feedback section. Navigation buttons at the bottom include '<< Previous: Basics' and 'Next: Details >>'.

5. On the **New support request > Details** tab read the message stating what support you are entitled to access with your current support plan, click **View Plans** and view the support plan options that we are currently entitled to and those we can upgrade to, along with the details, and costs of them i.e. we can upgrade to **Developer, Standard or Professional Direct**

Support Plans				
	BASIC ✓	DEVELOPER Upgrade	STANDARD Upgrade	PROFESSIONAL DIRECT Upgrade
Scope	Microsoft Azure: Billing and subscription support; online self-help 24x7 access to customer service, documentation, whitepapers, and support forums	Microsoft Azure: Trial and non-production environments 24x7 access to customer service, documentation, whitepapers, and support forums	Microsoft Azure: Production workload environments 24x7 access to customer service, documentation, whitepapers, and support forums	Microsoft Azure: Business-critical dependence 24x7 access to customer service, documentation, whitepapers, and support forums
Customer Service and Communities	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations
Best Practices				
Health Status and Notifications	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API
Technical Support		Business hours access to Support Engineers via email*	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone
Who Can Open Cases		Unlimited contacts / unlimited cases	Unlimited contacts / unlimited cases	Unlimited contacts / unlimited cases
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
Case Severity/Response Times		Minimal business impact (Sev C): <8 business hours*	Moderate business impact (Sev B): <4 hours Critical business impact (Sev A): <1 hour	Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour
Architecture Support		General guidance	General guidance	Architectural guidance based on best practice delivered by ProDirect Delivery Manager
Operations Support				Onboarding services, service reviews, Azure Advisor consultations
Training				Azure Engineering-led web seminars
Proactive Guidance				ProDirect Delivery Manager
Launch Support				
Pricing		\$29/mo	\$100/mo ³	\$1,000/mo

Note: If you have existing support benefits, not appearing for your subscription, you can add them by clicking **Link support benefits** and providing your *Access* and *Contract ID*.

- Still on the **Details** tab, click the **Azure community support** link. You are brought to the **Azure community Support** page where you can access community support and resources such as the **MSDN Forums**, **StackOverflow**, **Serverfault**, **Azure Feedback** and more support options.

The screenshot shows the Azure Community Support page with the following sections:

- Products**: A search bar and a browse dropdown.
- MSDN Forum**: Microsoft response to Azure technical questions. Categories: Most Recent, Popular, Trending. Topics include: Install specific SQL Server version on specific Windows Server version?, Forum: Azure SQL Database, ARM Linux VM Encryption Fails, Forum: Azure Disk Encryption, AD B2C Custom Policy - User creation issue - Block Sign In set to Yes, Forum: Azure Active Directory, Not working:, Forum: Azure Backup.
- StackOverflow**: Community responses to development questions. Categories: Most Recent, Popular, Trending. Topics include: Pushing Fortis in cloud foundry using docker image, Tags: azure google-cloud-platform cloud cloudfoundry private-cloud-foundry, How to configure fetch base url on deployment in docker for react app?, Tags: javascript reactjs azure docker, How to copy the data based on the Last modified time using Azure data factory from F..., Tags: azure azure-data-factory.
- Serverfault**: Community responses to Sys/Net admin questions. Categories: Most Recent, Popular, Trending. Topics include: Add-AzVMDataDisk not attaching disk, Tags: powershell azure, How Azure or AWS will be beneficial in my current architecture?, Tags: amazon-web-services azure.
- Azure Feedback**: Do you have an idea or suggestion based on your experience with Azure? Categories: Most Recent, Popular, Trending. Topics include: CMS Web Development Company Dubai, Are you searching for a reputed IT company complete your entire need? Then go with Ovocon Inc which is the one.., How to solve active directory 'Needs attention'?, Impossible to solve issue on active directory. Needs your attention., say backup must be done but backup cannot be..., Azure AD risk events - change sign in from infected device to sign in from bad IP address.

7. Return to the **New support request** section and the **Basics** tab fill in the fields as below. We will modify our selections to allow us create a support ticket under our **Pay-As-You-Go** subscription i.e. we will create a support request in the concerning billing for which we are entitled to access Microsoft support. Once finished click **Next: Solutions >>**.

- **Issue type:** Billing
- **Subscription:** < choose your subscription >
- **Problem Type:** Assistance with Bill or Usage
- **Problem subtype:** My issue is not listed here
- **Subject:** Test Issue - Charge Query

The screenshot shows the 'Help + support - New support request' page. On the left, there's a sidebar with links like Overview, Support Plans, Service Health, Advisor, and Get started with Azure. The main area has tabs: Basics (which is selected and highlighted in red), Solutions, Details, and Review + create. Below the tabs, there's a descriptive text about creating a support request for assistance with billing, subscription, technical, or quota management issues. It encourages users to provide detailed information to help solve their issues faster. A 'here' link is provided for the old experience.

* Issue type	Billing
* Subscription	Pay-As-You-Go (J ▾ Can't find your subscription? Show more ⓘ)
* Problem type	Assistance with Bill or Usage
* Problem subtype	My issue is not listed here
* Subject	Charge Query

At the bottom of the form, there's a button labeled 'Next: Solutions >>'.

8. On the **Solutions** tab, have a quick look at the recommendations and then click **Next: Details >>**

MCT USE ONLY. STUDENT USE PROHIBITED

Basics **Solutions** **Details** **Review + create**

Want a solution right now?
Try following the recommended steps below. These solutions are written by Azure engineers, and will solve most common issues.

Recommended Solution

Recommended Steps

Change/update your profile information

1. Sign in to the [Azure Account Center](#)
2. Select the **Edit details** button, and then update the **Profile** information

Learn more: [Manage account](#)

Frequently asked questions

- **Can notifications be sent to a different email address other than the Account Administrator email address associated with my account?**
Yes. The email address on the account gets important notifications about all the subscriptions under the account. We recommend that you specify a contact email address that the Account Administrator checks regularly.
- **Can I change the Account Administrator email address in my profile?**
Yes. The Account Administrator is the person who set up the Azure account and who receives important email notifications about all the subscriptions under the account. We recommend that you specify a contact email address that the Account Administrator checks regularly.
- **Does updating my profile email also update my login email address?**
No. Updating the profile email address does not update your login email address. To change your login email address, you have to transfer ownership of the account.
- **Does updating my profile address also update my credit card billing address?**
To learn how to update your billing information, see [Change the credit card used to pay for an Azure subscription](#).
- **Why can't I update the country?**
Because of technical constraints, we cannot change the country on an existing account. However, you can create an account in the desired country and then migrate your services to that account.

Recommended Documents

- [How to manage payment - Update, Change or Remove payment methods](#)

[**<< Previous: Basics**](#) [**Next: Details >>**](#)

9. On the **Details** tab fill in the fields as below, we will not fill in all fields in the interest of time, however when submitting a real support request you should provide as much information as possible to allow for a speedy resolution of the issue. Click **Next: Review + create >>** when finished.
- **Problem start date:** todays date
 - **Please provide details about your issue:** Test Issue
 - **Severity:** B-moderate impact
 - **Preferred contact method:** contact me later > email
 - **Response hours:** Business hours
 - **Support language:** < enter your preferred language >
 - **Contact info:** Enter your own personal contact details >

Help + support - New support request

Search (Ctrl+ /)

Basics Solutions **Details** Review + create

Information provided on this tab will be used to further assess your issue and help the support engineer troubleshoot the problem. Verify the contact information before moving to the Review + Create.

PROBLEM DETAILS

Problem Start Date: 2019-04-28 12:00 AM

Invoice # (if applicable): *Provide your Invoice #*

* Please provide details about your issue:

- Describe your problem, providing as much detail as possible.

File upload: Choose file to upload

SUPPORT METHOD

Support plan:	Basic support
* Severity:	B - Moderate impact
* Preferred contact method:	<input checked="" type="radio"/> Contact me later  Email
	<input type="radio"/> Call me later  Phone
* Response hours:	<input checked="" type="radio"/> Business Hours
* Support language:	English

CONTACT INFO

<< Previous: Solutions **Next: Review + create >>**

10. On the **Review + create** tab review the information and click **Create**

Help + support - New support request

BASICS

Issue type	Billing
Subscription	Pay-As-You-Go (?)
Service	Billing
Problem type	Assistance with Bill or Usage
Problem subtype	My issue is not listed here
Subject	Charge Query

TERMS, CONDITIONS AND PRIVACY POLICY

By clicking "Create" you accept the [terms and conditions](#) [\[?\]](#),
View our [privacy policy](#) [\[?\]](#).

DETAILS

Problem Start Date	4/28/2019 12:00:00 AM
Please provide details about your issue	Test issue

SUPPORT METHOD

Severity	B - Moderate impact
Support plan	Basic support
Response hours	Business Hours
Support language	English
Contact method	Email

CONTACT INFO

Contact name	
Email	
Country/region	

[<< Previous: Details](#) **Create**

11. After it is created, in the **Notifications** area, there is a notification of the **New Support request** having been created and a support request number is displayed.

Notifications

[More events in the activity log →](#) Dismiss all ...

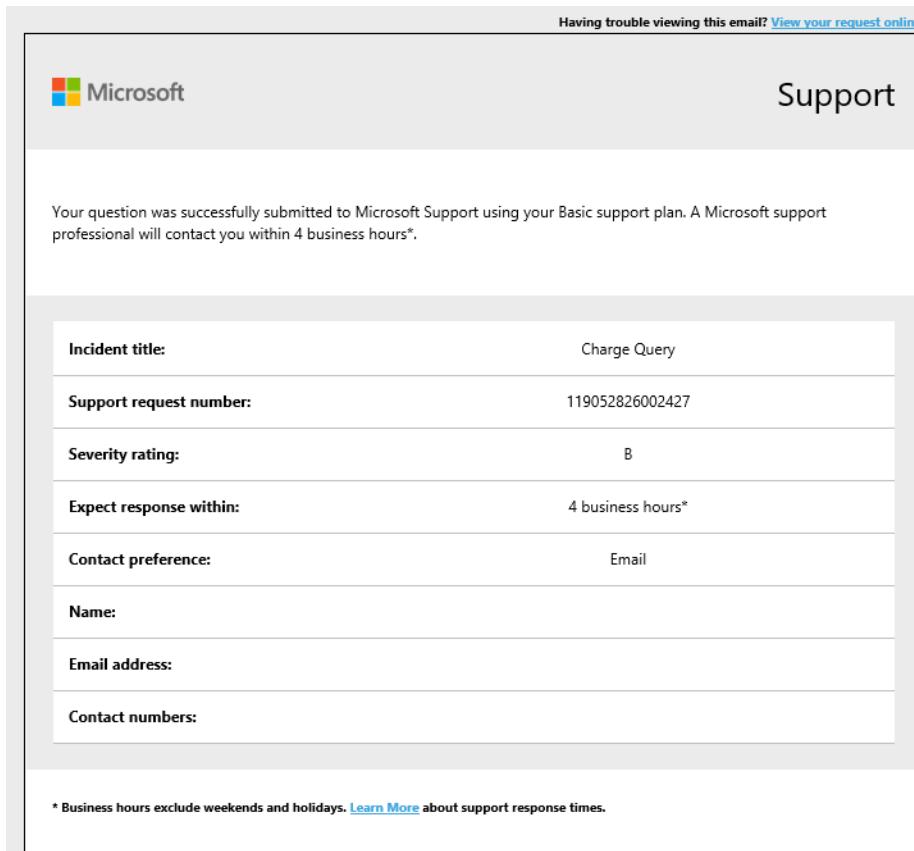
3 ×

New Support Request ×

We created support request 119052826002427 for you: 'Charge Query'

3 minutes ago

12. An email is also sent to your email address containing details of the support request.

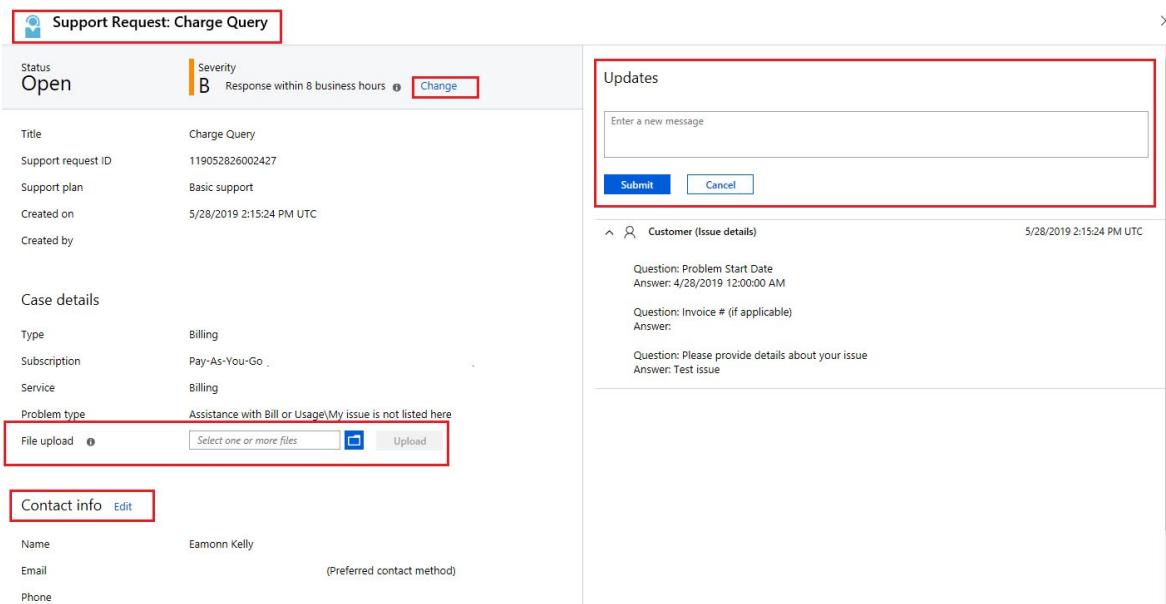


Monitor and interact with a support request

- To check the status and details of your support request, go to **Help + support** and then in the **Help + support** pane choose **All support requests**. Your support request should now be listed.

TITLE	ID	CREATED (UTC)	SUBSCRIPTION	RESOURCE TYPE	UPDATED	STATUS
Charge Query	1190528260...	Tue, May 28, 2019 2:...	Pay-As-You-Go	Billing	6 min ago	Open

- Double click the new support request and within the support request pane, you can view status, change severity, modify contact details, upload files and send messages related to the request.



Note: It is not currently possible for a user who opened a support request, to close it themselves. The Microsoft support team will review the item, and contact the user who opened the support request to verify they can close the support request. You can leave this support request as is for now, and later, when contacted by support, verify it is fine to close the support request.

If you would like to provide feedback to Microsoft regarding adding this as a feature, go to the **(General Feedback)**³³ page, and search to see if the issue is open already and vote for it, or add it as a new issue.

Congratulations! You have viewed available support plan options, and then created a new support request. You then saw how to monitor and interact with a support request.

Note: For more information about creating an Azure support ticket, refer to **Create a support ticket**³⁴

³³ <https://feedback.azure.com/forums/34192--general-feedback>

³⁴ <https://azure.microsoft.com/en-us/support/create-ticket/>

Azure Service Level Agreements (SLAs)

Service Level Agreements (SLAs)

Microsoft maintains its commitment to providing customers with high-quality products and services by adhering to comprehensive operational policies, standards, and practices. Formal documents known as *Service-Level Agreements* (SLAs) capture the specific terms that define the performance standards that apply to Azure.



- SLAs describe Microsoft's commitment to providing Azure customers with certain performance standards.
- There are SLAs for individual Azure products and services.
- SLAs also specify what happens if a service or product fails to perform to a governing SLA's specification.

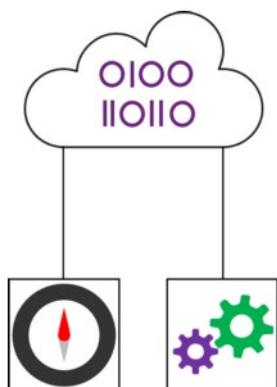
SLAs for Azure Products or Services

There are three key characteristics of SLAs for Azure products and services, which the following sections detail.

1. Performance Targets, Uptime and Connectivity Guarantees

A SLA defines performance targets for an Azure product or service. The performance targets that a SLA defines are specific to each Azure product and service.

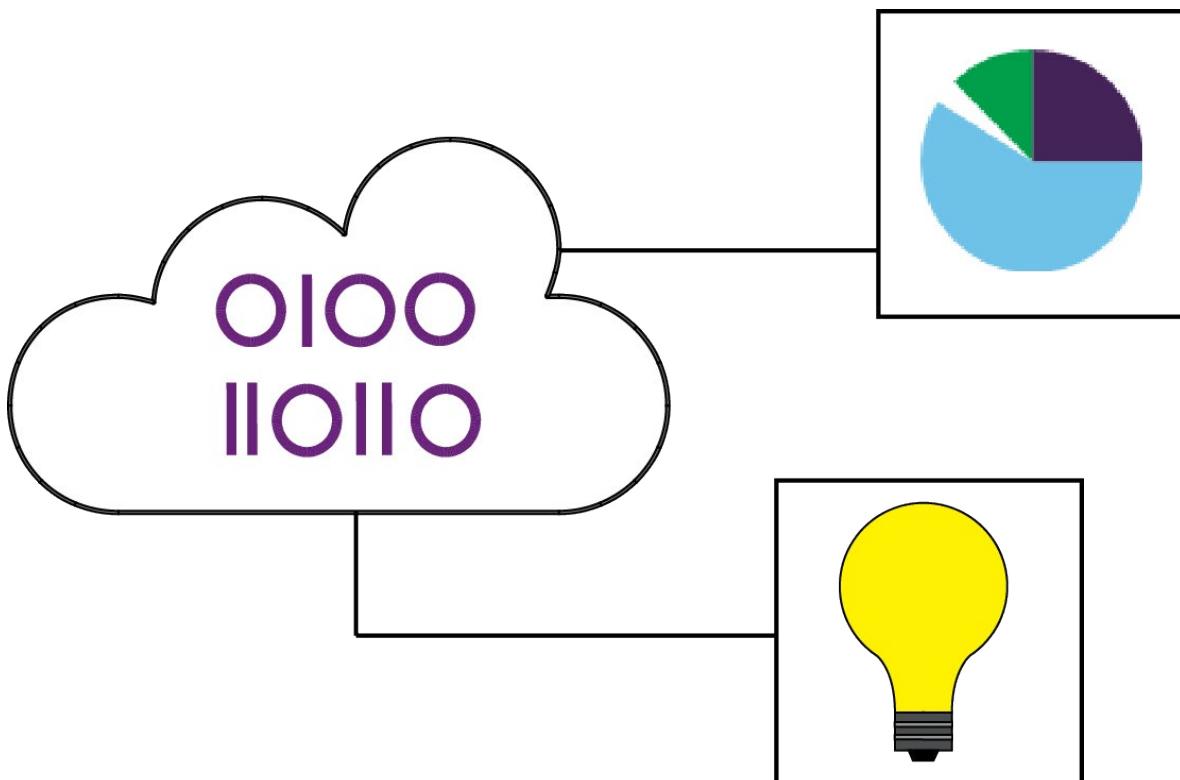
For example, performance targets for some Azure services are expressed in terms of uptime or connectivity rates.



2. Performance targets range from 99.9 percent to 99.99 percent

A typical SLA specifies performance-target commitments that range from 99.9 percent ("three nines") to 99.99 percent ("four nines"), for each corresponding Azure product or service. These targets can apply to such performance criteria as uptime, or response times for services.

For example, the SLA for the Azure Database for MySQL service guarantees 99.99 percent uptime. The Azure Cosmos DB (Database) service SLA offers 99.99 percent uptime, which includes low-latency commitments of less than 10 milliseconds on DB read operations and less than 15 milliseconds on DB write operations.



3. Service Credits

SLAs also describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLA's specification.

For example, customers may have a discount applied to their Azure bill, as compensation for an under-performing Azure product or service. The table below explains this example in more detail.

The first column in the table below shows monthly uptime percentage SLA targets for a single instance Azure Virtual Machine. The second column shows the corresponding service credit amount you receive, if the *actual* uptime is less than the specified SLA target for that month.

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT PERCENTAGE
< 99.9	10
< 99	25
< 95	100

Note: Azure does not provide SLAs for many services under the *Free* or *Shared* tiers. Also, free products such as Azure Advisor do not typically have a SLA.

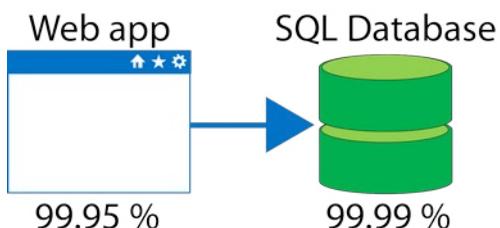
Note: For more information about specific Azure SLAs for individual products and services, refer to [Service Level Agreements³⁵](#).

Composite SLAs

When combining SLAs across different service offerings, the resultant SLA is called a *Composite SLA*. The resulting composite SLA can provide higher or lower uptime values, depending on your application architecture.

Consider an App Service web app that writes to Azure SQL Database. At the time of this writing, these Azure services have the following SLAs:

- App Service Web Apps is 99.95 percent.
- SQL Database is 99.99 percent.



Maximum downtime you would expect for this example application

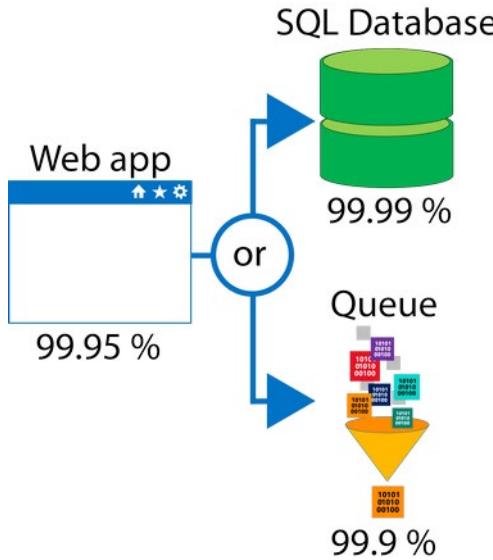
In the example above, if either service fails the whole application will fail. In general, the individual probability values for each service are independent. However, the composite SLA value for this application is:

$$99.95 \text{ percent} \times 99.99 \text{ percent} = \text{approx } 99.94 \text{ percent}$$

This means the combined probability of failure value is lower than the individual SLA values. This isn't surprising, because an application that relies on multiple services has more potential failure points.

Conversely, you can improve the composite SLA by creating independent fallback paths. For example, if **SQL Database** is unavailable, you can put transactions into a **Queue** for processing at a later time.

³⁵ <https://azure.microsoft.com/en-us/support/legal/sla/summary/>



With the design shown in the image above, the application is still available even if it can't connect to the database. However, it fails if both the SQL Database **and** the Queue fail simultaneously. If the expected percentage of time for a simultaneous failure is 0.0001×0.001 , i.e. $(1.0 - 0.9999) \times (1.0 - 0.999)$, the composite SLA for this combined path would be:

$$\text{Database *OR* Queue} = 1.0 - (0.0001 \times 0.001) = 99.99999 \text{ percent}$$

Therefore, the total composite SLA is:

$$\text{Web app *AND* (Database *OR* Queue)} = 99.95 \text{ percent} \times 99.99999 \text{ percent} = \sim 99.95 \text{ percent}$$

However, there are tradeoffs to using this approach such as, the application logic is more complex, you are paying for the queue, and there may be data-consistency issues which you need to consider.

Improving Application SLAs

Azure customers can use SLAs to evaluate how their Azure solutions meet their business requirements and the needs of their clients and users. By creating your own SLAs, you can set performance targets to suit your specific Azure application. This is an *Application SLA*.

Understand your requirements

Building an efficient and reliable Azure solution requires knowing your workload requirements. You then can select Azure products and services, and provision resources according to those requirements. To apply your solution successfully, it is important to understand the Azure SLAs that define performance targets for the Azure products and services within your solution. This understanding will help you create achievable Application SLAs.

In a distributed system, failures will happen. Hardware can fail. The network can have transient failures. It is rare for an entire service or region to experience a disruption, but even this must be planned for.

Resiliency

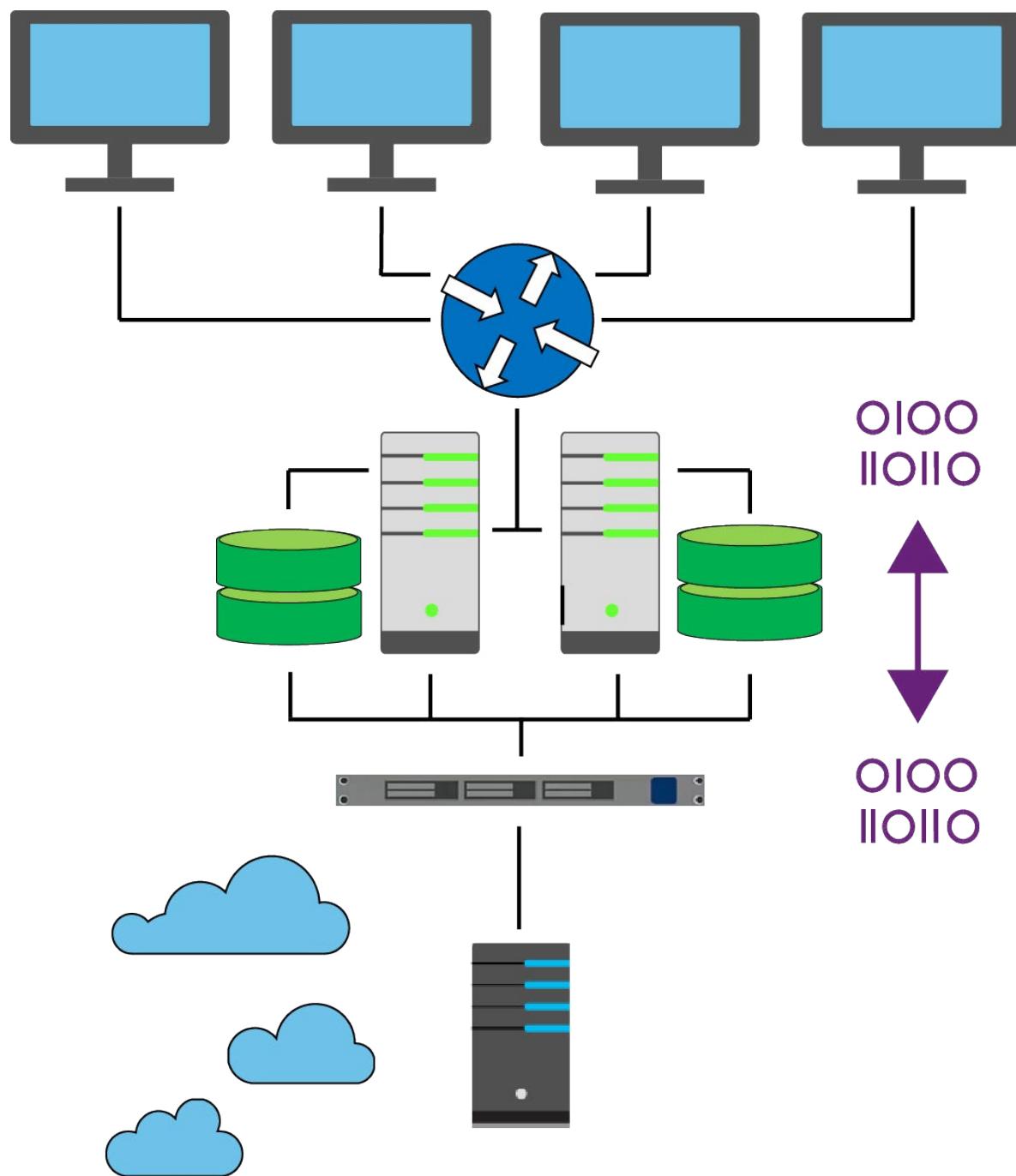
Resiliency is the ability of a system to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss. The goal of resiliency is to return the application to a fully functioning state following a failure. High availability and disaster recovery are two important components of resiliency.

When designing your architecture you need to design for resiliency, and you should perform a *Failure Mode Analysis* (FMA). The goal of a FMA is to identify possible points of failure, and to define how the application will respond to those failures.

Cost and complexity vs. high availability

Availability refers to time that a system is functional and working. Maximizing availability requires implementing measures to prevent possible service failures. However, devising preventative measures can be difficult and expensive, and often results in very complex solutions.

As your solution grows in complexity, you will have more services depending on each other. Therefore, you might overlook possible failure points in your solution if you have several interdependent services.



For example: A workload that requires 99.99 percent uptime shouldn't depend upon a service with a 99.9 percent SLA.

Most providers prefer to maximize the availability of their Azure solutions by minimizing downtime. However, as you increase availability, you also increase the cost and complexity of your solution.

For example: An SLA that defines an uptime of 99.99% only allows for about 5 minutes of total downtime per month.

The risk of potential downtime is cumulative across various SLA levels, which means that complex solutions can face greater availability challenges. Therefore, how critical high availability is to your

requirements will determine how you handle the addition of complexity and cost to your application SLAs.

The following table lists the potential cumulative downtime for various SLA levels over different durations:

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

Considerations for defining application SLAs

- If your application SLA defines four 9's (99.99 percent) performance targets, recovering from failures by manual intervention may not be enough to fulfill your SLA. Your Azure solution must be self-diagnosing and self-healing instead.
- It is difficult to respond to failures quickly enough to meet SLA performance targets above four 9's.
- Carefully consider the time window against which your application SLA performance targets are measured. The smaller the time window, the tighter the tolerances. If you define your application SLA in terms of hourly or daily uptime, you need to be aware that these tighter tolerances might not allow for achievable performance targets.

Note: For more information about improving application SLAs, refer to [Designing resilient applications for Azure](#)³⁶.

Walkthrough-Calculate Composite SLA for an Application

In this walkthrough task we will determine the SLA uptime percentages for each of the services in a sample application and then calculate the composite SLA uptime percentage for our application.

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

In our sample scenario our application consists of the below Azure services.

- **Web App service:** To host the application
- **Azure AD B2C:** To authenticate user login, manage profiles
- **Application Gateway:** To manage application access, scaling, Firewall
- **SQL Database:** To store application data. It will be a general purpose database, running as standard tier, not configured for Zone Redundant Deployments. It will have two replicas.

Note: We will not go in to deep architectural configuration and considerations, the intention here is to give an high level example.

³⁶ <https://docs.microsoft.com/en-us/azure/architecture/resiliency/>

Prerequisites

- There are no prerequisites. You do not need an Azure subscription.

Steps

Determine the SLA uptime percentage values for our application

- Go to the **SLA summary for Azure services**³⁷ page
- On the SLA webpage locate the **Azure Active Directory B2C** service and determine SLA uptime value, and note it down i.e. **99.9%**. You can also scroll down to the SLA detail section to determine more SLA detail such as **Service Credit**

The screenshot shows a Microsoft Azure webpage titled "SLA for Azure Active Directory B2C". The URL in the address bar is https://azure.microsoft.com/en-us/support/legal/sla/active-directory-b2c/v1_0/. The page content includes a red box highlighting the statement: "We guarantee at least 99.9% availability of the Azure Active Directory B2C service. The service is considered available for a directory in the following scenarios:". Below this, a bulleted list specifies the service's functionality. A note states: "No SLA is provided for the Free tier of Azure Active Directory B2C."

- On the SLA webpage locate the **Azure App Service** SLA uptime value and note it down, i.e. **99.95%**. You can also scroll down to the SLA detail section to determine more SLA detail such as **Service Credit**

The screenshot shows a Microsoft Azure webpage titled "SLA for App Service". The URL in the address bar is https://azure.microsoft.com/en-us/support/legal/sla/app-service/v1_0/. The page content includes a red box highlighting the statement: "We guarantee that Apps running in a customer subscription will be available 99.95% of the time. No SLA is provided for Apps under either the Free or Shared tiers."

³⁷ <https://azure.microsoft.com/en-us/support/legal/sla/summary/>

4. On the SLA webpage locate the **Azure Application Gateway** SLA uptime value and note it down, i.e. **99.95%**. You can also scroll down to the SLA detail section to determine more SLA detail such as **Service Credit**

LEGAL: SERVICE LEVEL AGREEMENTS / Application Gateway

SLA for Application Gateway

Last updated: May 2019

We guarantee that each Application Gateway Cloud Service having two or more medium or larger instances, or deployments capable of supporting autoscale or zone redundancy, will be available at least 99.95% of the time.

5. On the SLA webpage locate the **Azure SQL Database** SLA uptime value for the configuration we have specified earlier, and note it down, i.e. **99.99%**. You can also scroll down to the SLA detail section to determine more SLA detail such as **Service Credit**

LEGAL: SERVICE LEVEL AGREEMENTS / Azure SQL Database

SLA for Azure SQL Database

Last updated: May 2019

Azure SQL Database is a fully managed relational database with built-in regional high availability and turnkey geo-replication to any Azure region. It includes intelligence to support self-driving features such as performance tuning, threat monitoring, and vulnerability assessments and provides fully automated patching and updating of the code base.

- Azure SQL Database Business Critical or Premium tiers configured as Zone Redundant Deployments have an availability guarantee of at least 99.995%.
- Azure SQL Database Business Critical or Premium tiers not configured for Zone Redundant Deployments, General Purpose, Standard, or Basic tiers, or Hyperscale tier with two or more replicas have an availability guarantee of at least 99.99%.
- Azure SQL Database Hyperscale tier with one replica has an availability guarantee of at least 99.95% and 99.9% for zero replicas.

Note: There are different uptime values for different configurations and deployments of Azure SQL Database. It is important you are clear on your required uptime values, when planning and costing your deployment and configuration. Small changes in uptime can have impact on service costs as well as potentially increase complexity in configuration. Some other services that may be of interest to look at for examples on the Azure SLA summary web page would include **Virtual Machines, Storage Accounts** and **Cosmos DB**.

Calculate the Application Composite SLA percentage uptime

1. If any of the services that comprises our application are not available our application will not be available for users to sign in to and use. As such the total uptime for our application consists of the following:
 - **Azure AD B2C % uptime X App Service % uptime X Azure Application Gateway % uptime X Azure SQL Database % uptime = Total % Uptime**

MCT USE ONLY. STUDENT USE PROHIBITED

which in percentage term is as follows:

- **99.9% X 99.95% X 99.95% X 99.99% = 99.79%**

This is the percentage uptime that our application will be able to achieve with the current services and architecture.

Congratulations! You have determined the SLA uptime percentages for each of the services in our sample application and then calculated the composite SLA uptime percentage for the application.

Note: Remember to delete the resources you have just deployed, if they are still present and 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.

Service Lifecycle in Azure

Video: Feature Release and Access



<https://www.youtube.com/watch?v=7xgZNq5kCNA>

Public and Private Preview Features

Microsoft offer previews of Azure services, features and functionality for evaluation purposes. With *Azure Previews*, you can test beta and other pre-release features, products, services, software, and even regions. This allows users early access to functionality and users providing feedback on the features they preview also helps Microsoft improve the Azure service.

Categories

There are two categories of preview which are available:

- **Private Preview.** This means that an Azure feature is available to *certain* Azure customers for evaluation purposes.
- **Public Preview.** This means that an Azure feature is available to *all* Azure customers for evaluation purposes.

Azure Preview Terms and and Conditions

Azure feature previews are available under certain terms and conditions that are specific to each particular Azure preview. All preview specific terms and conditions supplement your existing service agreement, which governs your use of Azure.

Note: Some previews are *not covered by customer support* for example. You can see the full terms of Azure Preview feature on the **Supplemental Terms of Use for Microsoft Azure Previews³⁸** page.

Accessing Preview Features

You can access publicly available Preview features directly via the Azure Portal both.

Preview - New Services:

You can view preview services by doing the following

- Sign into the **Azure Portal**
- Click **Create a resource**
- Type **preview** in the search box and press **Enter**

³⁸ <https://azure.microsoft.com/en-us/support/legal/preview-supplemental-terms/>

- A list of services is returned and displayed for you to browse through. You can select one to learn more about it, and also create an instance of the service and try it out.

The screenshot shows the Azure Marketplace interface. On the left is a navigation sidebar with various service categories like Home, Dashboard, All services, Favorites, Resource groups, etc. The main area is titled 'Get Started' and shows a search bar with 'preview' typed in. Below the search bar are filters for Pricing (All), Operating System (All), and Publisher (All). A table titled 'Results' lists several Azure services marked as preview, each with a small icon, name, publisher, and category. One service, 'Personalizer (Preview)', has a blue heart icon next to it, indicating it's a favorite. The table has columns for NAME, PUBLISHER, and CATEGORY.

NAME	PUBLISHER	CATEGORY
Azure SQL Analytics (Preview)	Microsoft	Management Tools
Logic Apps Management (Preview)	Microsoft	Management Tools
Azure Data Factory Analytics (Preview)	Microsoft	Management Tools
Office 365 Analytics (Preview)	Microsoft	Management Tools
System Center Operations Manager Health Check (Preview)	Microsoft	Management Tools
DNS Analytics (Preview)	Microsoft	Management Tools
Personalizer (Preview)	Microsoft	AI + Machine Learnin...
HDIInsight HBase Monitoring	Microsoft	Management Tools
Windows Server OS Monitoring [Preview]	Lumagate AS	Analytics
Windows Server Gen2 Preview	Microsoft	Compute

Preview - New Functionality/Features within an existing service:

Some preview features relate to a specific area of an existing Azure Service. These preview features are accessible as you deploy, configure and manage the particular service. One such example is **Azure Kubernetes Service (AKS)**, where you can view preview functionality available within AKS by doing the following.

- Sign in to **Azure portal**
- Open the **Azure Kubernetes Services (AKS)** then click **Create Kubernetes service** button
- Under the **Cluster Details > Kubernetes version** section expand the drop down list to display versions.
- The latest version **1.14.0** is listed as currently in preview i.e. **1.14.0 (preview)**. It is being made available to provide new functionality in AKS and allow testing.

Create Kubernetes cluster

Basics Scale Authentication Networking Monitoring Tags Review + create

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment, making it quick and easy to deploy and manage containerized applications without container orchestration expertise. It also eliminates the burden of ongoing operations and maintenance by provisioning, upgrading, and scaling resources on demand, without taking your applications offline. [Learn more about Azure Kubernetes Service](#)

PROJECT DETAILS

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription [?](#) Visual Studio Ultimate with MSDN

* Resource group [?](#) Select existing... Create new

CLUSTER DETAILS

* Kubernetes cluster name [?](#)

* Region [?](#) (Asia Pacific) Japan East

* Kubernetes version [?](#) 1.14.0 (preview)

* DNS name prefix [?](#)

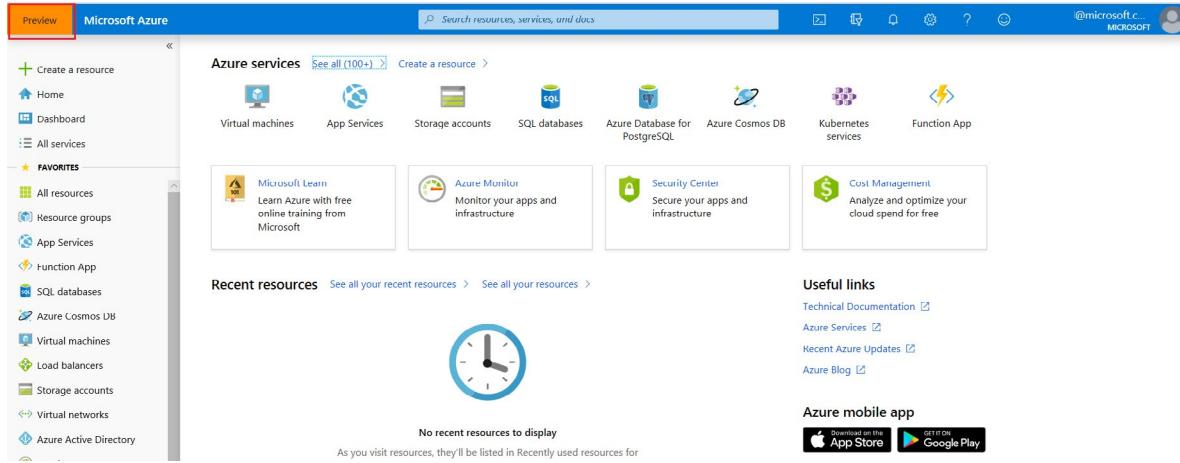
Review + create Previous Next : Scale >

Note: In these scenarios, although you may be using the Azure service in production, the preview feature or functionality may not yet be ready for production deployments. And you should make sure you are aware of any limitations around its use before deploying to production.

Accessing Azure Portal Preview

You can access preview features that are specific to the Azure Portal from the [https://preview.portal.azure.com³⁹](https://preview.portal.azure.com) page. Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

³⁹ <https://preview.portal.azure.com>



Providing Feedback

Azure customers can provide feedback on the portal preview features they've tested by *sending a smile* in the portal or by posting ideas and suggestions on the *Azure Portal Feedback Forum*. You can revert to the default Azure portal by going to the <https://portal.azure.com>⁴⁰ page.



Note: For more information about Azure portal preview features, refer to **Get early access to the newest Azure portal features⁴¹**.

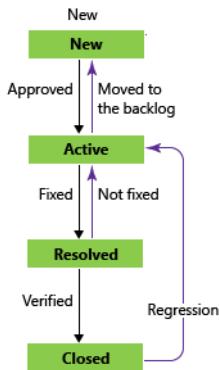
General Availability (GA)

Once a feature is evaluated and tested successfully, it may be released to customers as part of Azure's default product, service or feature set.

In other words, the feature may be made available for all Azure customers, and a feature released to all Azure customers typically goes to *General Availability* or GA.

⁴⁰ <https://portal.azure.com>

⁴¹ <https://azure.microsoft.com/en-us/updates/get-early-access-to-new-portal-features-2/>



The above image outlines the general progress and process for features and bugs during product and feature development lifecycle.

Note: It's common for features to move from Azure preview features to GA, based on customer evaluation and feedback.

Monitoring Service and Feature Updates

Go to the <https://azure.microsoft.com/en-us/updates/>⁴² page for information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements.

From the **Azure updates** page, you can:

- View details about all Azure updates.
- See which updates are in general availability, Preview, or Development.
- Browse updates by product category or update type, by using the provided dropdown lists.
- Search for updates by keyword by entering search terms into a text-entry field.
- Subscribe to get Azure update notifications by RSS.
- Access the Microsoft Connect page to read Azure product news and announcements.

⁴² <https://azure.microsoft.com/en-us/updates/>

Note: For more information about Azure updates, refer to [Azure Updates⁴³](#).

Walkthrough-Access Azure Preview features

In this walkthrough task we will access preview services and features in Azure and then identify preview service and feature information, and latest information on the Azure Updates.

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 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 today⁴⁴](#) webpage.

Steps

Access preview services and features

1. Go to **Azure Portal**, click on **Create a resource**, and in the **Search the Marketplace** box type **preview** and press **Enter**

⁴³ <https://azure.microsoft.com/en-us/updates/>

⁴⁴ https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

MCT USE ONLY. STUDENT USE PROHIBITED

The screenshot shows the Microsoft Azure portal interface. On the left, there's a dark sidebar with various navigation links like Home, Dashboard, All services, and Favorites. A red box highlights the 'Create a resource' button. The main area is titled 'New' and shows the 'Azure Marketplace' section. A search bar at the top of this section has the word 'preview' typed into it, with a red box around the search term. Below the search bar, there are two tabs: 'See all' and 'Popular'. A list of services is displayed, each with an icon and a link to a 'Quickstart tutorial'. The services listed are: Windows Server 2016 Datacenter, Ubuntu Server 18.04 LTS, Web App, SQL Database, Function App, Azure Cosmos DB, Kubernetes Service, and DevOps Project.

Service	Icon	Description
Windows Server 2016 Datacenter	Windows logo	Quickstart tutorial
Ubuntu Server 18.04 LTS	Ubuntu logo	Learn more
Web App	Web app icon	Quickstart tutorial
SQL Database	SQL logo	Quickstart tutorial
Function App	Lightning bolt icon	Quickstart tutorial
Azure Cosmos DB	Asterisk and planet icon	Quickstart tutorial
Kubernetes Service	Kubernetes logo	Quickstart tutorial
DevOps Project	Cloud and gear icon	Quickstart tutorial

2. In the **Marketplace > Get Started** pane a list of services in **Preview** is returned.

NAME	PUBLISHER	CATEGORY
Azure SQL Analytics (Preview)	Microsoft	Management Tools
Logic Apps Management (Preview)	Microsoft	Management Tools
Azure Data Factory Analytics (Preview)	Microsoft	Management Tools
Office 365 Analytics (Preview)	Microsoft	Management Tools
System Center Operations Manager Health Check (Preview)	Microsoft	Management Tools
DNS Analytics (Preview)	Microsoft	Management Tools
Personalizer (Preview)	Microsoft	AI + Machine Learn... Heart
HDInsight HBase Monitoring	Microsoft	Management Tools
Windows Server OS Monitoring [Preview]	Lumagate AS	Analytics
Windows Server Gen2 Preview	Microsoft	Compute
Ink Recognizer (Preview)	Microsoft	AI + Machine Learn...
Windows Server SAC Datacenter Preview	Microsoft	Networking
Azure API for FHIR (preview)	Microsoft	Databases

3. Locate the **DNS Analytics (Preview)** service in the list of services, open it and click **Create**

DNS Analytics (Preview)
Microsoft

Create Save for later

The DNS Analytics solution provides security, performance and operations related insights into the DNS infrastructure of your organization by collecting, analyzing and correlating analytic and audit logs and other related data from the DNS servers. Available insights include:

- Ability to identify clients which are trying to resolve malicious domain names
- Ability to identify unused resource records
- Identify most popular DNS clients and domain names
- View into requests load on DNS servers

Requirements: For DNS related insights, the DNS server should be Windows Server 2012 R2 or above.

Useful Links
[Watch Video](#) [Learn More](#) [Documentation](#)

4. You can proceed and create a **Log Analytics workspace** as prompted, and start to use and work with **DNS Analytics** if you wish, however there is no need to do so and we will not do so here as the intention is just to demonstrate its availability and demonstrate a preview services usage.
5. Close the **DNS Analyzer** panes, and in the Azure Portal go to **All services > Compute**. Note the presence of services listed as **Preview**

Click on several other groupings, such as **Network**, **Storage**, **Internet of Things** and note the presence of preview services listed and available.

6. View preview functionality in an existing service by locating and opening the **Azure Kubernetes Service (AKS)** and in the **Kubernetes services** pane select **Create Kubernetes service**

7. In the **Create Kubernetes cluster** pane go to the **Cluster details** section and expand the drop down list and select **1.14.0 (preview)**. This is a preview version of Kubernetes. This preview version is to allow users gain access to new functionality as soon as possible.

Create Kubernetes cluster

Basics Scale Authentication Networking Monitoring Tags Review + create

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment, making it quick and easy to deploy and manage containerized applications without container orchestration expertise. It also eliminates the burden of ongoing operations and maintenance by provisioning, upgrading, and scaling resources on demand, without taking your applications offline. [Learn more about Azure Kubernetes Service](#)

PROJECT DETAILS

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription	Visual Studio Ultimate with MSDN
* Resource group	Select existing... Create new

CLUSTER DETAILS

* Kubernetes cluster name	
* Region	(Asia Pacific) Japan East
* Kubernetes version	1.14.0 (preview)
* DNS name prefix	

PRIMARY NODE POOL

The number and size of nodes in the primary node pool in your cluster. For production workloads, at least 3 nodes are recommended for resiliency. For development or test workloads, only one node is required. You will not be able to change the number of nodes after you create the cluster.

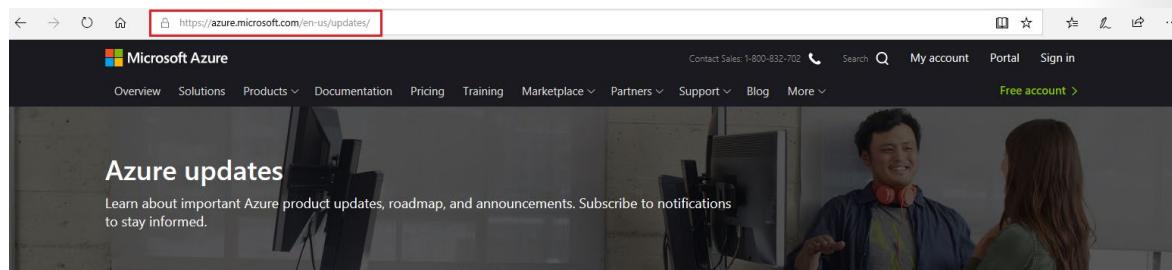
Review + create Previous Next : Scale >

Note: In these scenarios, where new functionality or features are made available within an existing generally available Azure service or product, although you may be using the Azure service in production, the preview feature or functionality may not yet be ready for production deployments. And you should make sure you are aware of any limitations around its use before deploying to production.

Identify preview information and latest information on the Azure Updates page

1. Go to the **Azure Updates** page <https://azure.microsoft.com/en-us/updates/>⁴⁵. Note the presence of four tab options i.e. **All**, **Now Available**, **In preview** and **In development**

⁴⁵ <https://azure.microsoft.com/en-us/updates/>



All Now available In preview In development

Products

Browse ▾

Search for a product

Update type

All ▾

RSS feed

May 2019

May 28 General availability: Azure Kubernetes Service in South Africa North

TARGET AVAILABILITY: Q2 2019

Azure Kubernetes Service (AKS) is now generally available in South Africa North.

[Azure Kubernetes Service \(AKS\)](#) [Regions & Datacenters](#) [Services](#)

May 28 Application Change Analysis for Azure Monitor is now in public preview

Change Analysis public preview with integration into App Services Diagnose and solve problems tool.

Explore

Read the Azure blog for the latest news.

[Blog >](#)

Tell us what you think of Azure and what you want to see in the future.

[Provide feedback >](#)

Azure is available in more regions than any other cloud provider.

[Check product availability in your region >](#)

- Click on the **In preview** tab and type **Kubernetes** in the search for a search box, then select Azure Kubernetes Service (AKS) when prompted. The page returns a list of items in preview related to Kubernetes

All Now available In preview In development

Products

Browse ▾

Search for a product

Update type

All ▾

RSS feed

[Azure Kubernetes Service \(AKS\)](#) X

May 2019

May 17 Azure Kubernetes Service (AKS) now supports Windows Server containers

Use managed Kubernetes for all of your workloads whether they're in Windows, Linux or both.

[Azure Kubernetes Service \(AKS\)](#) [Features](#)

May 6 Azure Container Registry virtual network and firewall rules support is now in preview

Virtual network and firewall rules support is now available in Azure Container Registry in preview.

[Azure Kubernetes Service \(AKS\)](#) [Container Registry](#) [Features](#) [Microsoft Build](#)

May 6 Authenticated IP for Azure Kubernetes Service (AKS) is now in preview

Your organization can now restrict access to its Kubernetes control plane to specific IP addresses or IP ranges.

[Azure Kubernetes Service \(AKS\)](#) [Features](#) [Microsoft Build](#)

Explore

Read the Azure blog for the latest news.

[Blog >](#)

Tell us what you think of Azure and what you want to see in the future.

[Provide feedback >](#)

Azure is available in more regions than any other cloud provider.

[Check product availability in your region >](#)

- Click on the first item in the list to get more details

Updates / Azure Kubernetes Service (AKS) now supports Windows Server containers

Azure Kubernetes Service (AKS) now supports Windows Server containers

Posted on Friday, May 17, 2019

Windows Server container support in the Azure Kubernetes Service is now available in public preview. With this preview, you can:

- Lift and shift Windows applications to run on AKS
- Seamlessly manage Windows and Linux applications through a single unified API
- Mix Windows and Linux applications in the same Kubernetes cluster – with consistent monitoring experience and deployment pipelines

Now you can get the best of managed Kubernetes for all of your workloads whether they're in Windows, Linux or both.

[Learn more](#)

Azure Kubernetes Service (AKS) Features

Related feedback

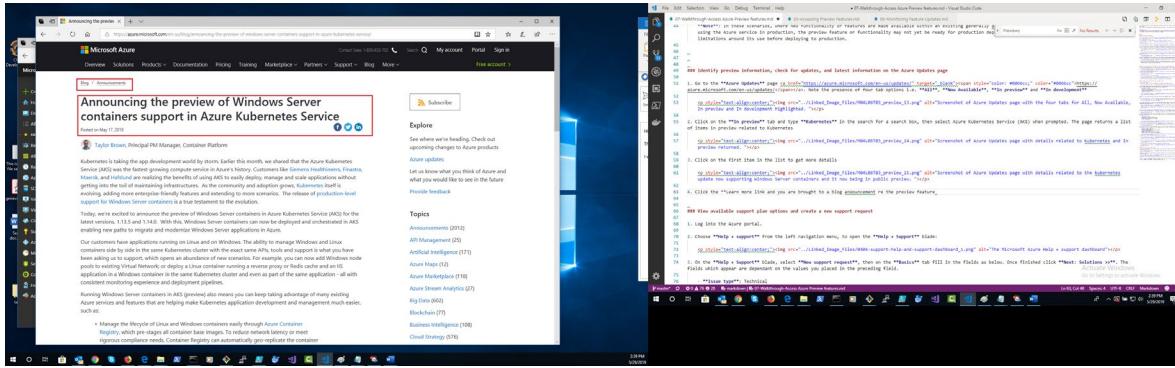
Be the first to submit Azure feedback for this Update entry

[View more Azure updates >](#)

Related products

Azure Kubernetes Service (AKS)

- Click the **Learn more** link and you are brought to a blog announcement re the preview feature. There is more detail available on this page and links to further documentations and details.



- You can repeat steps 1 to 4 for other products and services and see what other services have preview features available.
- Returning to the **Azure Updates** page, view items that are now have a status of **General Availability** by clicking **Now available** and noting the items now displaying

The screenshot shows the Azure updates page. At the top, there's a banner with the text "Azure updates" and a subtext: "Learn about important Azure product updates, roadmap, and announcements. Subscribe to notifications to stay informed." Below the banner, there are navigation tabs: "All" (selected), "Now available" (highlighted with a red box), "In preview", and "In development".

The main content area has two sections: "Products" and "Update type". The "Products" section includes a "Browse" dropdown, a search bar with placeholder "Search for a product", and a magnifying glass icon. The "Update type" section includes a dropdown menu set to "All" and an "RSS feed" link.

A large red box highlights the "Now available" tab and the three news items listed below it:

- May 28 General availability: Azure Kubernetes Service in South Africa North**
TARGET AVAILABILITY: Q2 2019
Azure Kubernetes Service (AKS) is now generally available in South Africa North.
[Azure Kubernetes Service \(AKS\)](#) [Regions & Datacenters](#) [Services](#)
- May 24 Application Insights Availability in US West Region**
Application Insights is now available in US West region.
[Azure Monitor](#) [Application Insights](#) [Regions & Datacenters](#) [Services](#)
- May 24 General availability: Zone-redundant SQL databases and elastic pools are now generally available in three additional regions**
TARGET AVAILABILITY: Q2 2019
Zone-redundant SQL databases and elastic pools are now generally available in these additional regions: UK South, East US and East US 2.

Explore
Read the Azure blog for the latest news.
[Blog >](#)
Tell us what you think of Azure and what you want to see in the future.
[Provide feedback >](#)
Azure is available in more regions than any other cloud provider.
[Check product availability in your region >](#)

7. Now click on the In development tab and note the items returned that are currently in development.

The screenshot shows the Azure Updates page. At the top, there's a banner with the text "Azure updates" and a subtext: "Learn about important Azure product updates, roadmap, and announcements. Subscribe to notifications to stay informed." Below the banner, there's a video thumbnail of a man wearing headphones. A navigation bar at the top has tabs: "All", "Now available" (which is highlighted with a red box), "In preview", and "In development".

The main content area has two sections: "Products" and "Update type". The "Products" section includes a "Browse" dropdown, a search bar, and a "Search for a product" input field. The "Update type" section includes a dropdown set to "All" and an "RSS feed" button.

A section titled "May 2019" lists three items:

- May 28 General availability: Azure Kubernetes Service in South Africa North
TARGET AVAILABILITY: Q2 2019
Azure Kubernetes Service (AKS) is now generally available in South Africa North.
Azure Kubernetes Service (AKS) Regions & Datacenters Services
- May 24 Application Insights Availability in US West Region
Application Insights is now available in US West region.
Azure Monitor Application Insights Regions & Datacenters Services
- May 24 General availability: Zone-redundant SQL databases and elastic pools are now generally available in three additional regions
TARGET AVAILABILITY: Q2 2019
Zone-redundant SQL databases and elastic pools are now generally available in these additional regions: UK South, East US and East US 2.

On the right side, there's an "Explore" section with links: "Read the Azure blog for the latest news.", "Blog >", "Tell us what you think of Azure and what you want to see in the future.", "Provide feedback >", "Azure is available in more regions than any other cloud provider.", and "Check product availability in your region >".

Congratulations! You have accessed preview services and features in Azure and identified preview service and feature information, and latest information on the Azure Updates.

Note: For more information about creating an Azure support ticket, refer to [Create a support ticket⁴⁶](#)

⁴⁶ <https://azure.microsoft.com/en-us/support/create-ticket/>

Module 4 Review Questions

Azure Pricing and Support Review Questions

About review questions

End-of-module review questions are for practice only and don't count against your course grade. However, the final assessment at the end of the course is graded.

Review Question 1

Which of the following defines an Azure subscription correctly?

- Using Azure does not require a subscription
- All Azure subscriptions are always free
- An Azure subscription is a logical unit of Azure services that is linked to an Azure account
- An account cannot have more than one subscription

Review Question 2

True or false: Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions?

- True
- False

Review Question 3

Available purchasing and billing options for Azure products and services depend on what?

- Usage meters
- Customer type
- Cloud Solution Providers
- Uptime

Review Question 4

Which of the following are used to determine Azure costs for each billing period?

- The Azure website
- Virtual machines
- Microsoft partner companies
- Usage meters

Review Question 5

Which of the following are factors affecting costs?

(choose two)

- Global infrastructure
- Resource type
- Location
- Availability zone

Review Question 6

Complete the following sentence. As an Azure customer, Azure Reservations offer discounted prices if you...

- provision many resources.
- pay in advance
- have a free account.
- use Spending Limits.

Review Question 7

Which of the following statements is correct?

- Paid support plans extend Azure free basic support.
- There is no free basic support.
- All Azure support is free.

Review Question 8

Complete the following sentence. Performance targets defined within a SLA...?

(choose one)

- automatically shutdown resources by default.
- are specific to each Azure product and service.
- typically range from 9.9% to 9.99%.

Review Question 9

True or false: As you increase availability, you also increase the cost and complexity of your solution?

- True
- False

Review Question 10

A feature released to all Azure customers is said to have which of the following?

- Free Availability
- High Availability
- General Availability
- Preview Availability

Module 4 Summary

Module 4 Summary

In this module, you learned about Azure Pricing and Support. We defined Azure subscriptions and detailed the various Azure subscription options and uses; explored purchasing Azure Products and Services; and examined factors that affect Azure costs and how you can minimize them. Additionally, we detailed Azure support plans and channels, and outlined Azure SLAs and how you can improve their application. Finally, we followed the service life cycle in Azure from the preview phase through general availability to update.

Azure subscriptions

In this lesson, we defined an Azure subscription as a logical unit of services, and we detailed the free and paid subscriptions that suit different customer requirements. Additionally, you learned that using Azure requires a subscription and that billing and management policies apply on a per-subscription basis for accounts with multiple subscriptions. We defined management groups as containers for collections of Azure resources, arranged hierarchically. Lastly, we discussed how you can apply governance and access policies to each management group.

Planning and managing costs

In this lesson, we discussed the four Azure customer types, which include Free Account, Enterprise, Web Direct, and Cloud Solution Providers (CSP), and how those customer types determine purchasing and billing options for products and services. We introduced Azure's pay-for-what-you-use model and discussed how usage meters determine costs. We also examined the factors that affect costs including resource type, first-party and third-party service categories, and location. Lastly, we discussed how you can minimize your Azure costs by using tools such as Azure's Pricing and Cost of Ownership (TCO) calculators, and products such as Azure Advisor recommendations and Azure Reservations.

Support options available with Azure

In this lesson, you learned that all customers receive free billing and subscription support, and free access to documentation and self-help. We discussed how you can extend Azure free support with a paid support plan, like Developer, Standard, Professional Direct, and Premier Support. You discovered that available support-plan options can vary between Azure customer and subscription type. Lastly, you learned how you can get additional help by opening a support ticket, by visiting alternative support channels (such as MSDN Forums and Stack Overflow), or from the Azure Knowledge Center.

Azure SLAs

In this lesson, you learned how SLAs set performance targets specific to each Azure product and service. You saw how SLA performance targets typically range from 99.9 percent (three nines) to 99.99 percent (four nines), and you learned that SLAs define how Microsoft responds if an Azure product or service under-performs. You also learned how to create your own Application SLAs and how increasing availability can also raise the cost and complexity of your Azure solution.

Service life cycle in Azure

In this lesson, you learned about the components of the Azure service life cycle, and how Microsoft offers public and private previews of Azure features for evaluation purposes. You also learned how you can access the Azure Preview Features page and that successfully tested features are made available to Azure customers through GA releases. Finally, you learned how to get details of the latest updates to Azure products, services, and features from the Azure Updates web page.

Answers

Review Question 1

Which of the following defines an Azure subscription correctly?

- Using Azure does not require a subscription
- All Azure subscriptions are always free
- An Azure subscription is a logical unit of Azure services that is linked to an Azure account
- An account cannot have more than one subscription

Explanation

It's true that an Azure subscription is a logical unit of Azure services that is linked to an Azure account. All other answers are incorrect.

Using Azure requires an Azure subscription. Azure offer free and paid subscription options to suit different customer needs and requirements, and an account can have one or more subscriptions, with different billing models and access-management policies applied to each. A subscription provides authenticated and authorized access to Azure products and services, and allows you to provision resources.

Review Question 2

True or false: Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions?

- True
- False

Explanation

True, Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions.

Management groups facilitate the hierarchical ordering of Azure resources into collections, at a level of scope above subscriptions. Distinct governance conditions can be applied to each management group, with Azure Policy and Azure RBACs, to manage Azure subscriptions effectively. The resources and subscriptions assigned to a management group automatically inherit the conditions applied to the management group.

Review Question 3

Available purchasing and billing options for Azure products and services depend on what?

- Usage meters
- Customer type
- Cloud Solution Providers
- Uptime

Explanation

It's true that available purchasing options for Azure products and services depend on the type of customer you are. All other answers are incorrect.

Products and services in Azure are arranged by category, with various resources available for provisioning in each category. You select the Azure products and services that fit your requirements and your account is billed according to Azure's pay-for-what-you-use model. How you are billed, and which products and services you can choose depends on your customer type. The three main Azure customer types are Enterprise, Web Direct, and Cloud Solution Providers (CSP).

Review Question 4

Which of the following are used to determine Azure costs for each billing period?

- The Azure website
- Virtual machines
- Microsoft partner companies
- Usage meters

Explanation

Usage meters are used to determine Azure costs for each billing period. The Azure website provides information about, and access to, Azure, while virtual machines are a type of Azure resource.

CSPs typically are Microsoft partner companies who have agreed upon a business arrangement with Microsoft.

When you provision an Azure resource, Azure creates one or more meter instances for that resource. The meters track the resource's usage. Each meter generates a usage record that Azure uses to calculate your bill. The usage that a meter tracks correlates to a quantity of billable units, which are charged to your account for each billing period.

Review Question 5

Which of the following are factors affecting costs?

(choose two)

- Global infrastructure
- Resource type
- Location
- Availability zone

Explanation

Resource type and location are factors that affect costs. Global infrastructure refers to a system with architecture that is distributed across many countries, while an availability zone provides failure protection for datacenters.

Azure costs are resource specific. The kind of usage that a meter tracks, and the number of meters associated with a resource, depends on the resource type. The rate of charge per billable unit depends on the resource type. Azure infrastructure is globally distributed. Usage costs between locations offering certain Azure products, services, and resources may vary.

Review Question 6

Complete the following sentence. As an Azure customer, Azure Reservations offer discounted prices if you...

- provision many resources.
- pay in advance
- have a free account.
- use Spending Limits.

Explanation

As an Azure customer, Azure Reservations offer discounted prices if you pay in advance.

There is no requirement to provision many resources to use Azure Reservations, and free accounts can't use Azure Reservations. The Azure Reservations feature is available only for Enterprise or CSP customers, and for those with pay-as-you-go subscriptions.

Spending limits prevent you from exhausting the credit on your account within each billing period. Free-trial customers and some credit-based Azure subscriptions can use the spending limits feature.

Azure Reservations offer discounted prices on certain Azure products and resources. To get a discount, you reserve products and resources by paying in advance. You can prepay for one or three year's use of certain Azure resources.

Review Question 7

Which of the following statements is correct?

- Paid support plans extend Azure free basic support.
- There is no free basic support.
- All Azure support is free.

Explanation

It's true that paid support plans extend Azure free basic support.

There is free basic support for every Azure subscription, which includes access to billing and subscription support, documentation, online self-help, and community-support forums.

Microsoft also offer four paid support plans, including Developer, Standard, Professional Direct, and Premier. Paid support plans extend Azure free basic support, for Azure customers who require technical and operational support. Providing different Azure support options allows Azure customers to choose a plan that best fits their needs. The support plans you can use, and how you are billed for using support, depends on the type of Azure customer you are and on the Azure subscription you have.

Review Question 8

Complete the following sentence. Performance targets defined within a SLA...?

(choose one)

- automatically shutdown resources by default.
- are specific to each Azure product and service.
- typically range from 9.9% to 9.99%.

Explanation

Performance targets defined within a SLA are specific to each Azure product and service, and they won't automatically shutdown resources by default.

A SLA defines performance targets for an Azure product or service. A typical SLA sets out performance target commitments that range from 99.9 percent (three nines) to 99.99 percent(four nines) for each corresponding Azure product or service. Azure SLAs also describe how Microsoft responds when a product or service fails to perform to its governing SLA's specification.

Review Question 9

True or false: As you increase availability, you also increase the cost and complexity of your solution?

- True
- False

Explanation

As you increase availability, you also increase the cost and complexity of your solution.

Availability refers to the proportion of time that a system is functional and working. Maximizing availability requires implementing measures to prevent possible service failures. Devising preventative measures can be difficult and expensive, and often results in complex solutions. Most providers prefer to maximize the availability of their Azure solutions, by minimizing downtime.

But, it is important to carefully consider the time window against which you measure your application SLA performance targets. The smaller the time window, the tighter the tolerance. If you define your application SLA in terms of hourly or daily uptime, or availability, you might not always set achievable SLA performance targets.

Review Question 10

A feature released to all Azure customers is said to have which of the following?

- Free Availability
- High Availability
- General Availability
- Preview Availability

Explanation

A feature released to all Azure customers is said to have General Availability (GA).

All other answers are incorrect.

Once a feature has been evaluated and tested successfully, it may be released to customers as part of Azure's default product, service, or feature set. A feature released to all Azure customers in this way has GA. In the life cycle of a typical Azure feature, it's common for a feature to move from Azure preview to general availability based on customer evaluation and feedback.