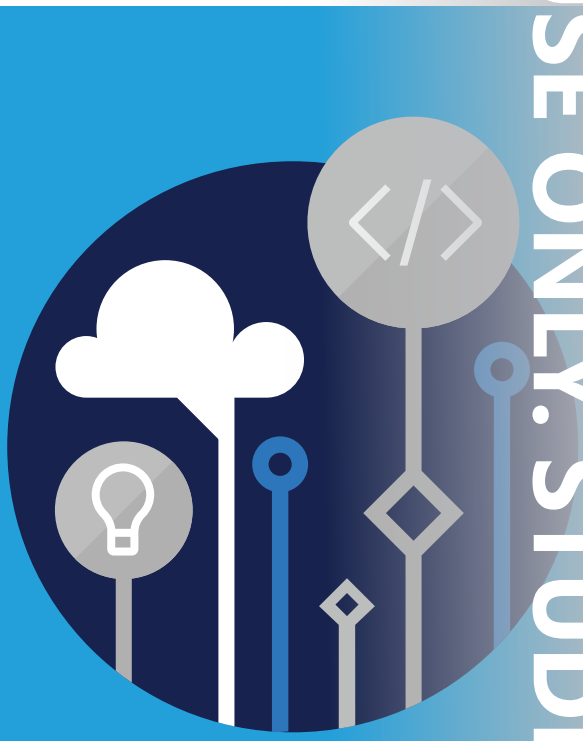
Microsoft

Microsoft Official Course



AZ-900T01

Microsoft Azure Fundamentals

AZ-900T01
Microsoft Azure Fundamentals

Contents

Module 0 Course Introduction

Course overview

Video: About this Course

About this course

About This Course

AZ900T01: Azure Fundamentals

This course will provide foundational level knowledge of cloud services and how those services are provided with Microsoft Azure. The course can be taken as an optional first step in learning about cloud services and Microsoft Azure, before taking further Microsoft Azure or Microsoft cloud services courses.

In this course you will learn how to:

- Understand general cloud computing concepts
- Understand core services available with Microsoft Azure
- Understand security, privacy, compliance and trust with Microsoft Azure
- Understand pricing and support models available with Microsoft

Course prerequisites

There are no pre-requisites for taking this course. Technical IT experience is not required however some general IT knowledge or experience would be beneficial.

Audience

The course is intended for a broad range of candidate backgrounds. It is suitable for candidates with non-technical backgrounds, such as those involved in selling or purchasing cloud based solutions and services or who have or will have some involvement with cloud based solutions and services.

It would also be suitable for candidates with a technical background who may be looking to take a first look at cloud services and Microsoft Azure.

Hands-on

There are no labs or structured hands on components in this course. However we would encourage and recommend, that you sign up for a free Microsoft Azure account, on the page **Create your free account today**[1], at the start of the course and try to identify and try out some of the areas as you come across them in the course.

You can also follow the demo *Create Free Azure Account* at the end of this lesson to assist in creating an Azure Free Account.

Course Syllabus

The course structure is as follows:

- **Module 0: Course Introduction**
  - Course Overview
  - Pre-Course Survey
- **Module 1 - Cloud Concepts**
  - Lesson 1 - Learning Objectives
  - Lesson 2 - Why Cloud Services?
  - Lesson 3 - Types of Cloud models
  - Lesson 4 - Types of Cloud Services
  - Lesson 5 - Module 1 Review Questions
  - Lesson 6 - Module 1 Summary
- **Module 2 - Core Azure Services**
  - Lesson 1 - Learning Objectives
  - Lesson 2 - Core Azure Architectural components
  - Lesson 3 - Core Azure Services and Products
  - Lesson 4 - Azure Solutions
  - Lesson 5 - Azure management tools

1 https://azure.microsoft.com/free

- Lesson 6 - Module 2 Review Questions
- Lesson 7 - Module 2 Summary

- **Module 3 - Security, Privacy, Compliance and Trust**
  - Lesson 1 - Learning Objectives
  - Lesson 2 - Securing network connectivity in Azure
  - Lesson 3 - Core Azure Identity services
  - Lesson 4 - Security tools and features
  - Lesson 5 - Azure governance methodologies
  - Lesson 6 - Monitoring and Reporting in Azure
  - Lesson 7 - Privacy, Compliance and Data Protection standards in Azure
  - Lesson 8 - Module 3 Review Questions
  - Lesson 9 - Module 3 Summary
- **Module 4 - Azure Pricing and Support**
  - Lesson 1 - Learning Objectives
  - Lesson 2 - Azure subscriptions
  - Lesson 3 - Planning and managing costs
  - Lesson 4 - Support options available with Azure
  - Lesson 5 - Azure Service Level Agreements (SLAs)
  - Lesson 6 - Service lifecycle in Azure
  - Lesson 7 - Module 4 Review Questions
  - Lesson 8 - Module 4 Summary
- **Module 5 – Final Exam**
  - Lesson 1 - Graded Final Exam
- **Module 6 – Course End**
  - Lesson 1 - Course Complete
  - Lesson 2 - Post – Course Survey

Course Components

This course is composed of the following elements:

- **Content Topics**: Contain text-based content, graphics, references and notes.
- **Videos and Demos**: Are located throughout the course to explain concepts and key areas of learning as well as walkthrough's of some core component configuration.
- **Module Review Questions:** Are located at the end of each module and check your general understanding of the key concepts. They are for learning purposes only and are not graded.
- **Final Exam:** Located at the end of the course and evaluates your overall knowledge. This a graded event.

- **Pre- and Post-Course Surveys:** Surveys are included at the start and end of the course. We ask users to complete to allow us improve and maintain the course.
- **Hands-on**: There are no labs or structured hands on components in this course. However we would encourage and recommend, that you sign up for a free Microsoft Azure account, on the page **Create your free account today**[2], at the start of the course and try to identify and try out some of the areas as you come across them in the course.

References

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

- **Microsoft Azure Homepage**[3]
- **Microsoft Azure Documentation site**[4]

Demo: Create Free Azure Account

2 https://azure.microsoft.com/free
3 https://azure.microsoft.com/en-us/
4 https://docs.microsoft.com/en-us/azure/

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

Key Concepts and Terms

Key concepts and terms

What is cloud computing?

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

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

- **High availability**. The ability to keep services up and running for long periods of time, with very little downtime, depending on the service in question.
- **Scalability**. The ability to increase or decrease resources for any given workload. You can add additional resources to service a workload (known as *scaling out*), or add additional capabilities to manage an increase in demand to the existing resource (known as *scaling up*). Scalability doesn't have to be done automatically
- **Elasticity**. The ability to automatically or dynamically increase or decrease resources as needed. Elastic resources match the current needs, and resources are added or removed automatically to meet future needs when it's needed, and from the most advantageous geographic location. A distinction between scalability and elasticity is that elasticity is done automatically
- **Agility**. The ability to react quickly. Cloud services can allocate and deallocate resources quickly. They are provided on-demand via self-service, so vast amounts of computing resources can be provisioned in minutes. There is no manual intervention in provisioning or deprovisioning services.
- **Fault tolerance**. The ability to remain up and running even in the event of a component or service no longer functioning. Typically, redundancy is built into cloud services architecture so if one component fails, a backup component takes its place. The type of service is said to be tolerant of faults.
- **Disaster recovery**. The ability to recover from an event which has taken down a cloud service. Cloud services disaster recovery can happen very quickly with automation and services being readily available to use.
- **Global reach**. The ability reach audiences around the globe. Cloud services can have presence in various regions across the globe which you can access, giving you a presence in those regions even though you may not have any infrastructure in that region.

- **Customer latency capabilities**. If customers are experiencing slowness with a particular cloud service, they are said to be experiencing some latency. Even though modern fiber optics are fast, it can still take time for services to react to customer actions if the service is not local to the customer. Cloud services have the ability deploy resources in datacenters around the globe, thus addressing customer latency issues.
- **Predictive cost considerations**. The ability for users to predict what costs they will incur for a particular cloud service. Costs for individual services are made available, and tools are provided to allow you predict what costs a service will incur. You can also perform analysis based on future growth.
- **Technical skill requirements and considerations**. Cloud services can provide and manage hardware and software for workloads. Therefore, getting a workload up and running with cloud services demands less technical resources than having IT teams build and maintain physical infrastructure for handling the same workload. A user can be expert in the application they want to run without having to need skills to build and maintain the underlying hardware and software infrastructure.
- **Increased productivity**. On-site datacenters typically require a lot of hardware setup (otherwise known as *racking and stacking*), software patching, and other time-consuming IT management chores. Cloud computing eliminates the need for many of these tasks, so IT teams can spend time on achieving more important business goals.
- **Security**. Cloud providers offer a broad set of policies, technologies, controls, and expert technology skills that can provide better security than most organizations can otherwise achieve. The result is strengthened security, which helps to protect data, apps, and infrastructure from potential threats.

Note: You can read more conceptual detail about cloud computing on the page **What is cloud computing?**[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

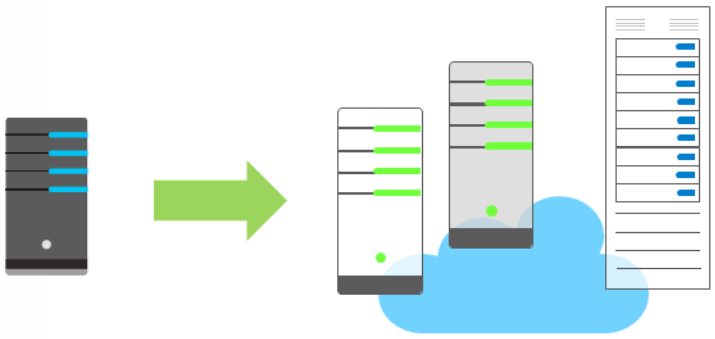
Economies of scale

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

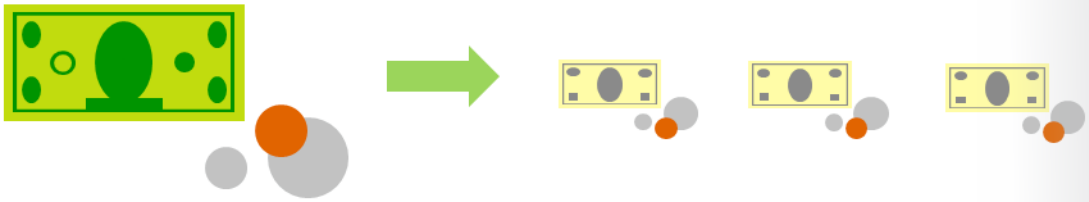
Capital expenditure (CapEx) versus operational expenditure (OpEx)

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

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

These two approaches to investment are referred to as:

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



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

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

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

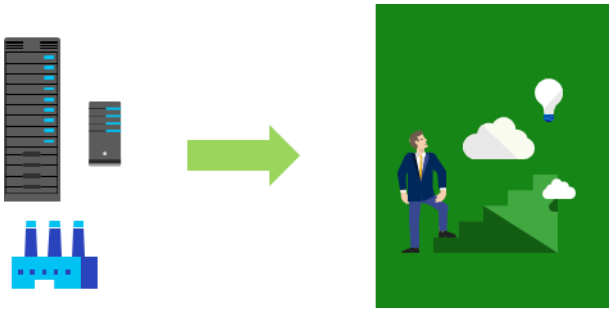
Consumption based model

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

Public Cloud

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.

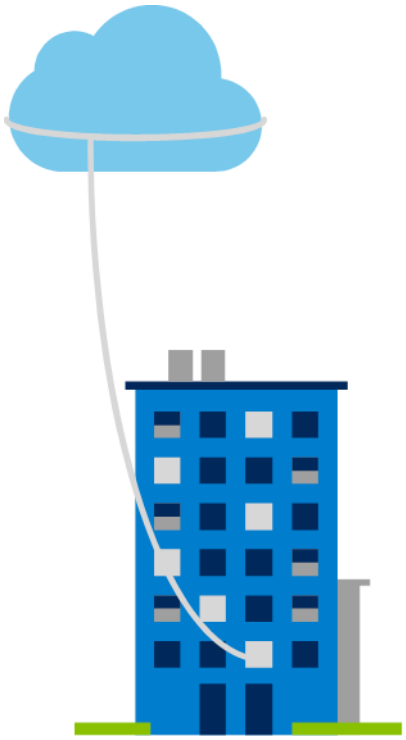
Private Cloud

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

Hybrid cloud

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

Hybrid cloud models have the following characteristics:

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

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

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

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

Note: You can read more about Microsoft Azure Hybrid cloud options from the page **The only consistent and comprehensive hybrid cloud**[3]

Video: Cloud Model Comparison

Cloud Model Comparison

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.

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

- **Security**. Organizations have complete control over security.
- **Compliance**. If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.
- **Specific scenarios**. If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.

- **Disadvantages**:
  - **Upfront CapEx**. Hardware must be purchased for start-up and maintenance.
  - **Agility**. Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.
  - **Maintenance**. Organizations have the responsibility for hardware maintenance and updates.
  - **Skills**. Private clouds requires in-house IT skills and expertise that may be hard to get or be costly.

Hybrid cloud

- **Advantages**:
  - **Flexibility**. The most flexible scenario; with a hybrid cloud setup, an organization can decide to run their applications either in a private cloud or in a public cloud.
  - **Costs**. Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.
  - **Control**. Organizations can still access resources over which they have total control.
  - **Security**. Organizations can still access resources for which they are responsible for security.
  - **Compliance**. Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.
  - **Specific scenarios**. Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications. In this case, they can keep the old system running locally, and connect it to the public cloud for authorization or storage. Additionally, they could host a website in the public cloud, and link it to a highly secure database hosted in their private cloud.

- **Disadvantages**:
  - **Upfront CapEx**. Upfront CapEx is still required before organizations can leverage a private cloud.
  - **Costs**. Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.
  - **Skills**. Deep technical skills are still required to be able to set up a private cloud.
  - **Ease of management**. Organizations need to ensure there are clear guidelines to avoid confusion, complications or misuse.

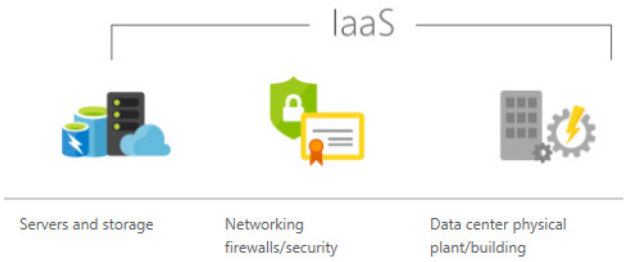
Types of Cloud Services

Video: Cloud Services

IaaS

Infrastructure as a service (IaaS)

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



IaaS has the following characteristics:

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

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

Common usage scenarios:

- **Migrating workloads**. Typically, IaaS facilities are managed in a similar way as on-premises infrastructure, and provide an easy migration path for moving existing applications to the cloud.

- **Test and development**. Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS makes scaling development testing environments up and down fast and economical.
- **Website hosting**. Running websites using IaaS can be less expensive than traditional web hosting.
- **Storage, backup, and recovery**. Organizations avoid the capital outlay and complexity of storage management, which typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for managing unpredictable demand and steadily growing storage needs. It can also simplify the planning and management of backup and recovery systems.

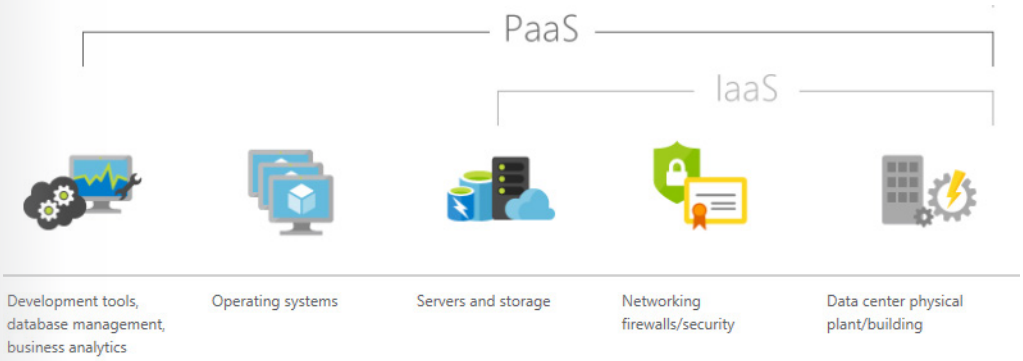
Note: For more information on IaaS see the page **What is IaaS?**[4]

PaaS

Platform as a Service (PaaS)

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

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



PaaS has the following characteristics:

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

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

Common usage scenarios:

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

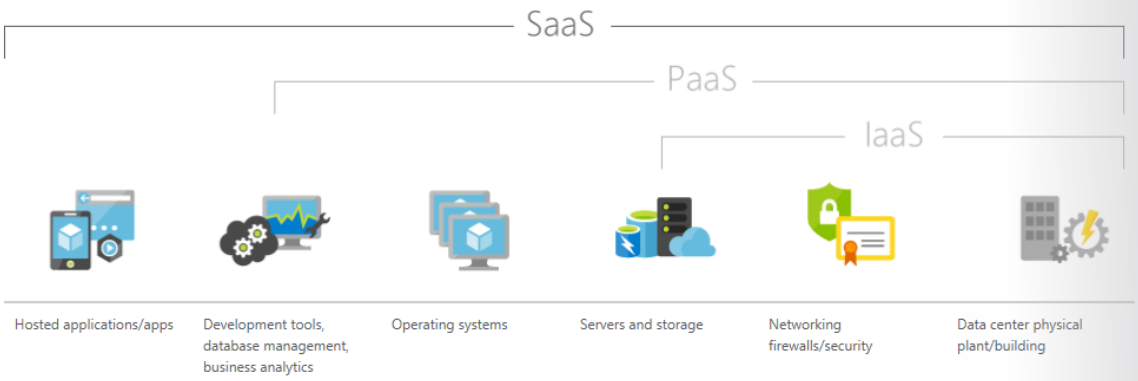
Note: For more information on PaaS see the page **What is PaaS?**[5]

SaaS

Software as a Service (SaaS)

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

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



SaaS has the following characteristics:

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

Common usage scenarios:

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

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

Note: For more information on SaaS see the page **What is SaaS?**[6]

Cloud Service Comparison

Cloud service comparison

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

IaaS

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

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

PaaS

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

- **Advantages**:
  - **No CapEx**. Users have no upfront costs.
  - **Agility**. PaaS is more agile than IaaS, and users do not need to configure servers for running applications.
  - **Consumption-based model**. Users pay only for what they use, and operate on an OpEx model.
  - **Skills**. No deep technical skills are required to deploy, use, and gain the benefits of PaaS.
  - **Cloud benefits**. Users can leverage the skills and expertise of the cloud provider to ensure their workloads are made secure and highly available. In addition, users can gain access to more cutting-edge development tools and toolsets. They then can apply these tools and toolsets across an application's lifecycle.

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

- **Productivity**. Users can focus on application development only, as all platform management is handled by the cloud provider. Working with distributed teams as services is easier, as the platform is accessed over the internet and can be made globally available more easily.

- **Disadvantages**:
  - **Platform limitations**. There may be some limitations to a particular cloud platform that could affect how an application runs. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a particular workload.

SaaS

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

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

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

Summary

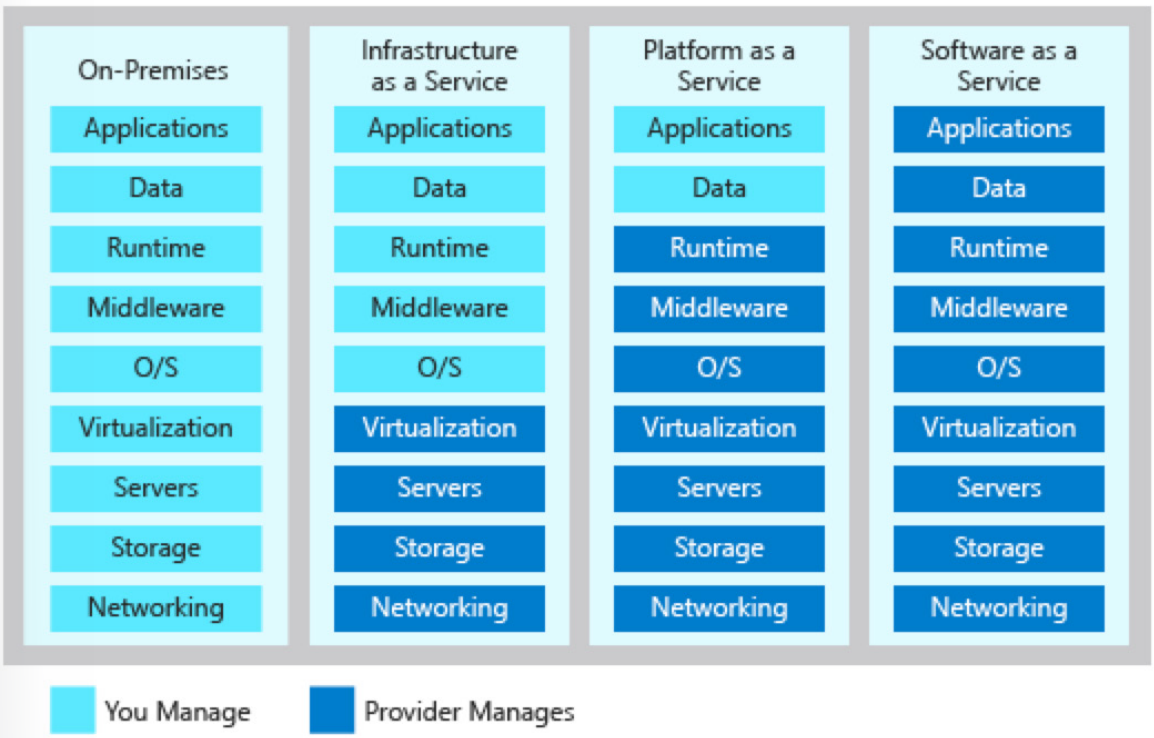
IaaS, PaaS, and SaaS each contain different levels of managed services. You may easily use a combination of these types of infrastructure. You could use Office 365 on your company's computers (SaaS), and in Azure you could host your VMs (IaaS) and use Azure SQL Database (PaaS) to store your data. With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

Management Responsibilities

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

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

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.

Module 2 Core Azure Services

Learning Objectives

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

Regions

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

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

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

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

Note: A list of regions and their locations is available on the page **Azure Regions**[1]

Special Azure regions

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

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

Region pairs

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

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

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

Note: A full list of region pairs is avalable **here**[2].

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

Geographies

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

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

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

Note: See the page **Azure Grographies for more details**[3].

Video: Availability Zones

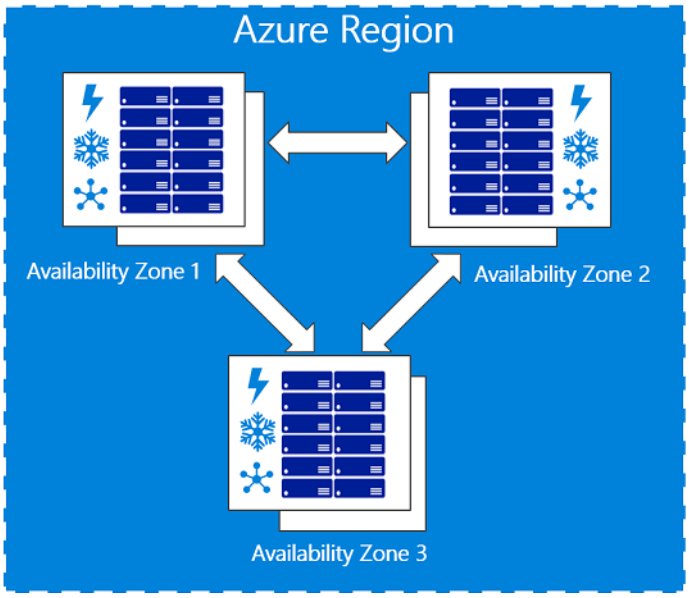
Availability Zones

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: Availaility Sets

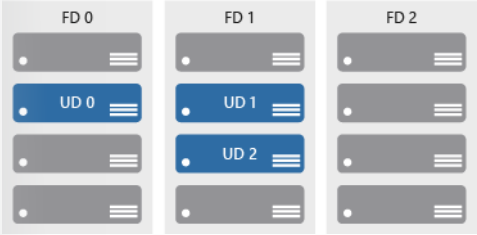
Availability Sets

Availability sets

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

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

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



Video : Resource Groups

Resource Groups

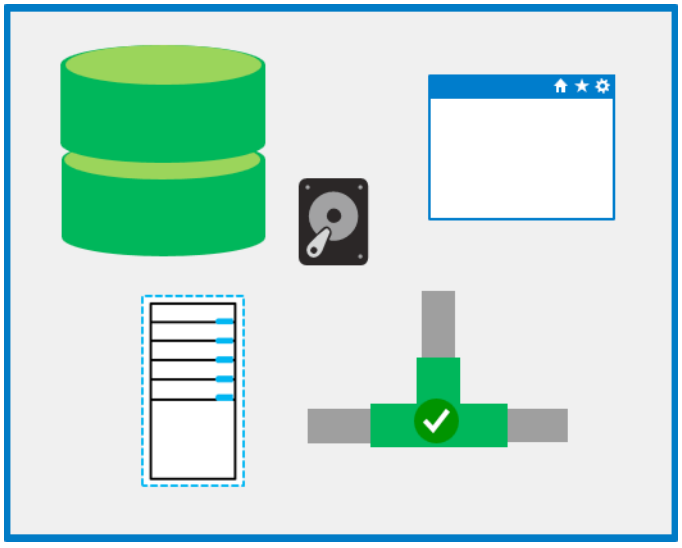
Resource groups

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: Resource Manager

Azure Resource Manager

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

With Azure Resource Manager, you can:

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

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

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

Note: See the page **Azure Resource Manager**[5] for more details.

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

Core Azure Services and Products

Video: Azure Compute Services

Azure Compute Service

Azure Compute Services

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

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

What are virtual machines?

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

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

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

Azure VMs

Azure 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-to-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.

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/

What are containers?

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

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

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

Azure Container Instances

Azure Container Instances offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services. It is a PaaS offering that allows you to upload your containers, which it will run for you. See **Container Instances**[10] 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 **Compute**[12].

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/

Demo: Create Azure Virtual machine

Walkthrough-Create a Virtual machine using Azure Portal

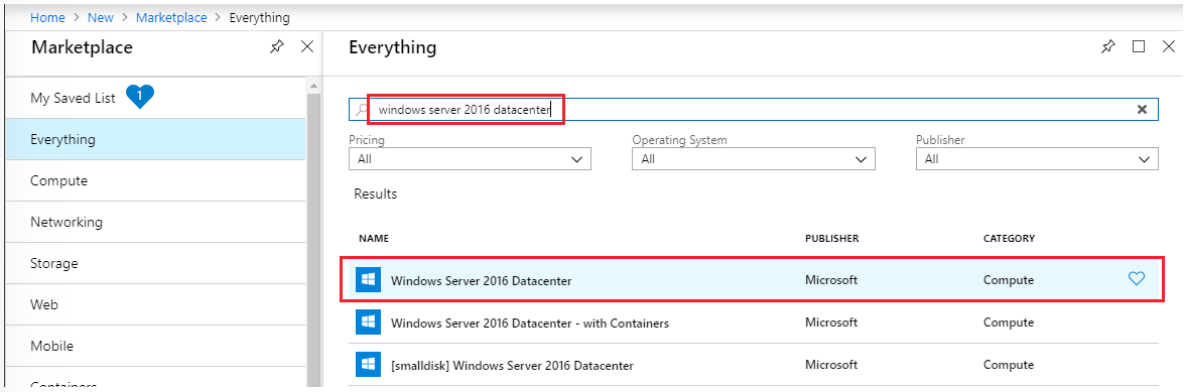
In this walkthrough task we will create a virtual machine in Azure via the Azure Portal, configure it as a web server and connect to the web server over the internet.

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

Prerequisites

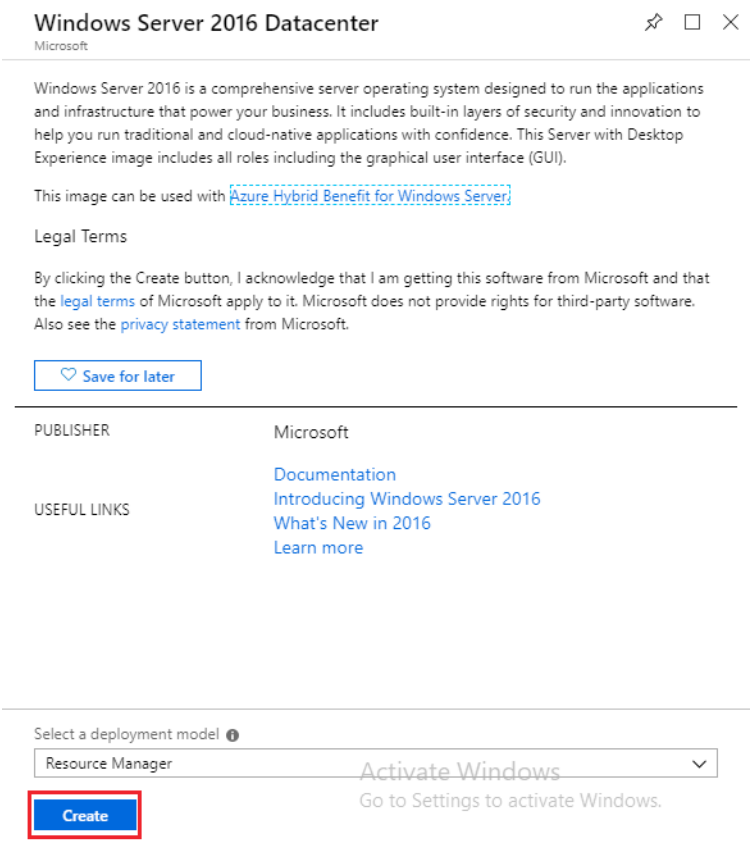
- You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the **Create your Azure free account today**[13] webpage.

Steps

1. Sign in to the Azure portal at **https://portal.azure.com**[14]
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**.
4. 

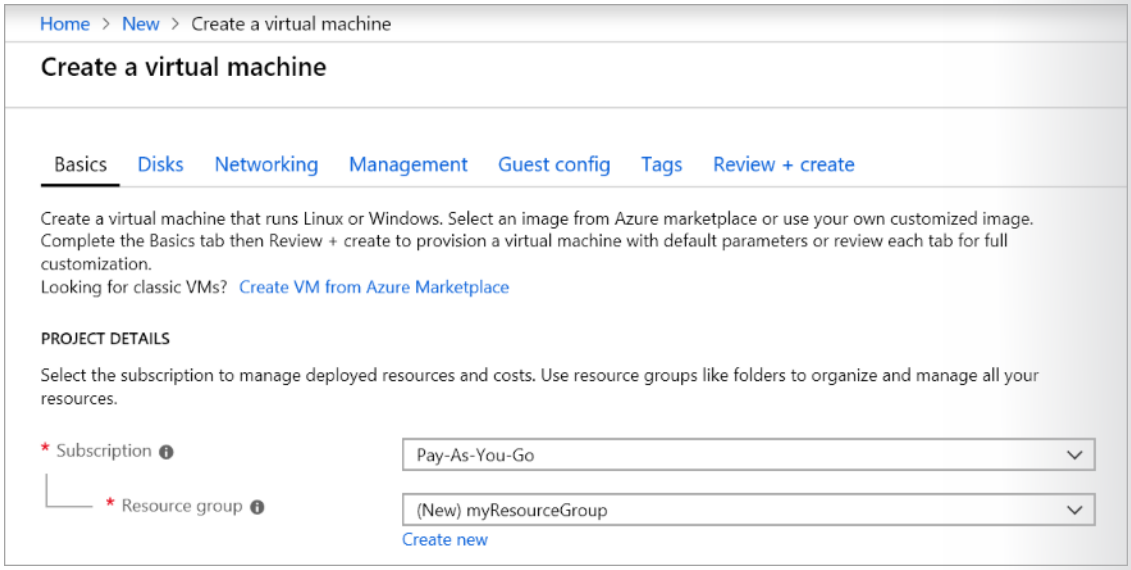
13 https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio

14 https://portal.azure.com



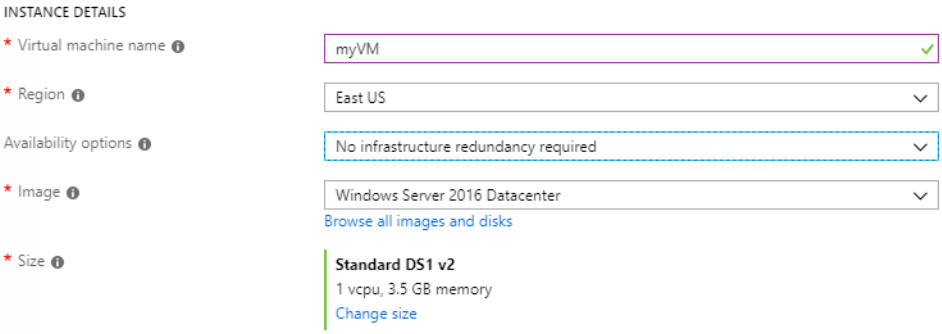
5.

6. 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.



7.

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

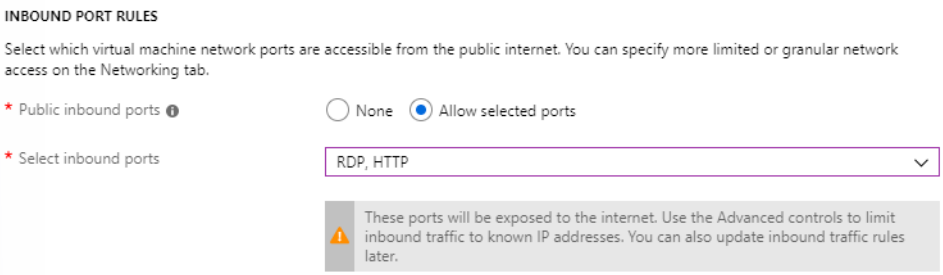


9.

10. 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.

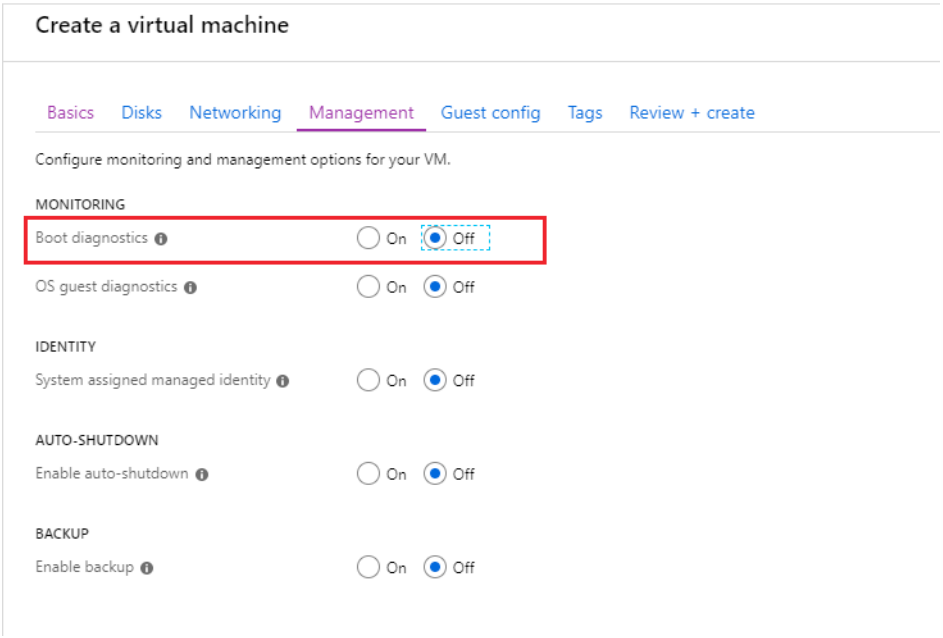
11.

12. 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.



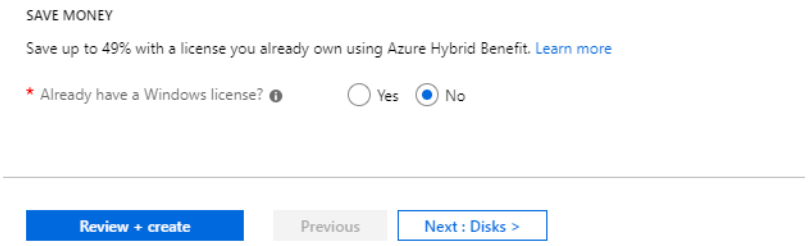
13.

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



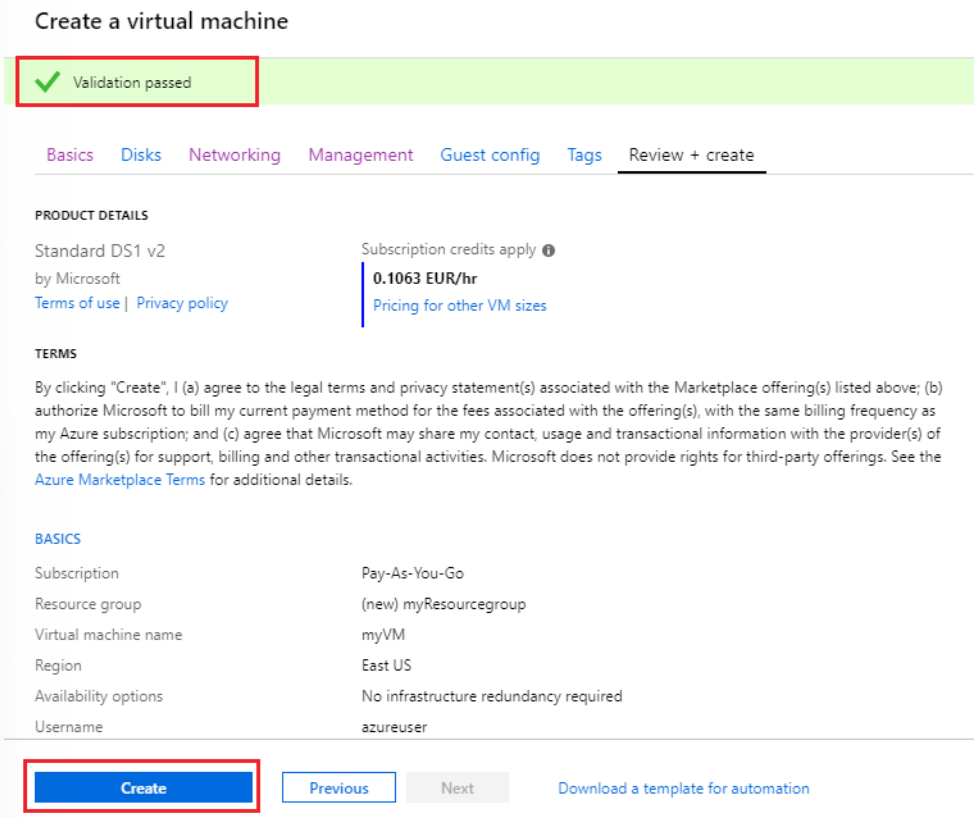
15.

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



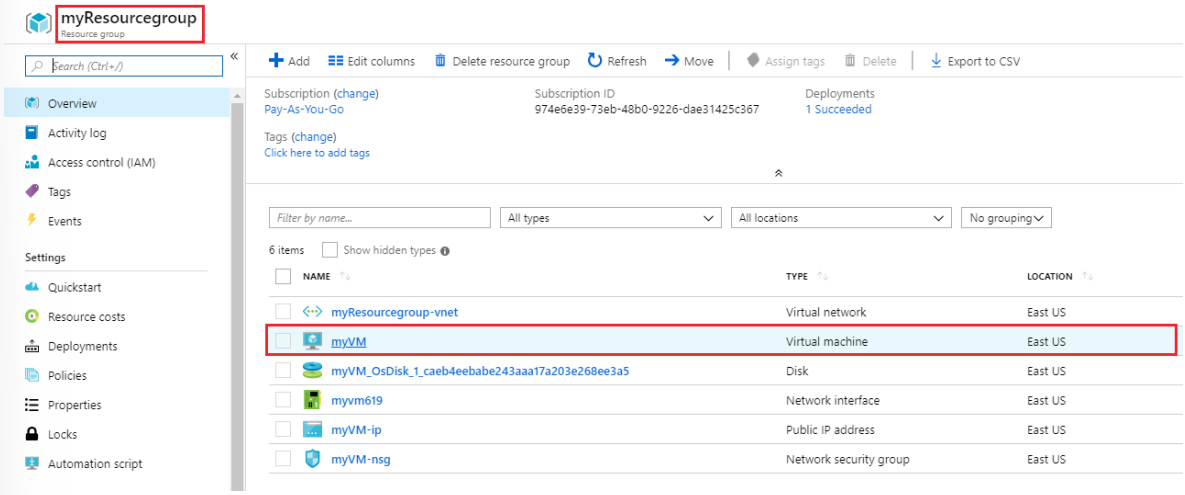
17.

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

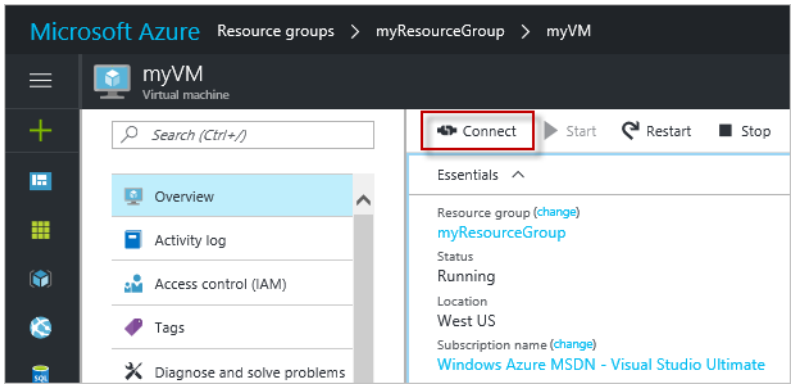


19.

20. 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.



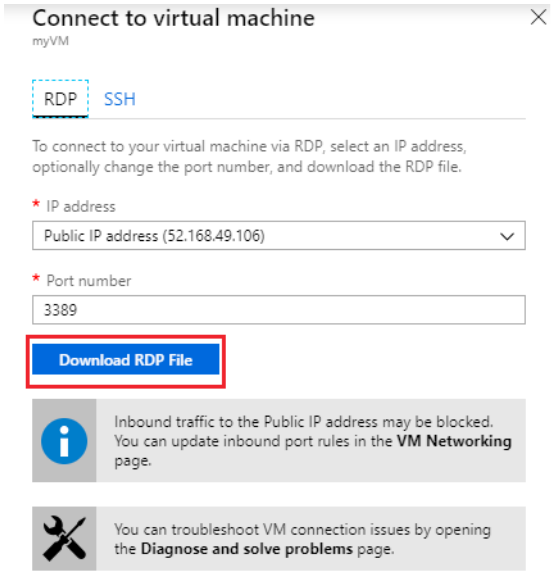
21.



22.

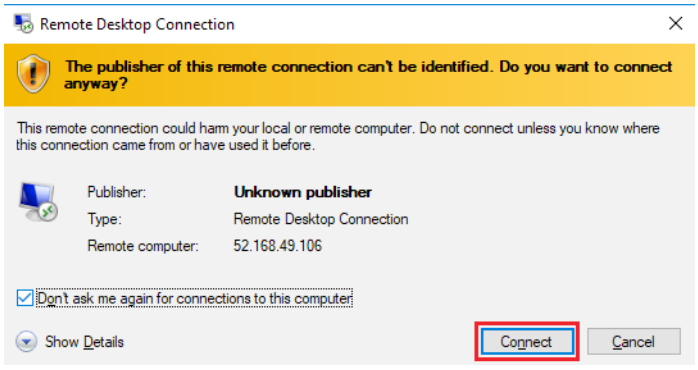
Note: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on Linux virtual machine you could connect directly from a bash shell using `ssh`.

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



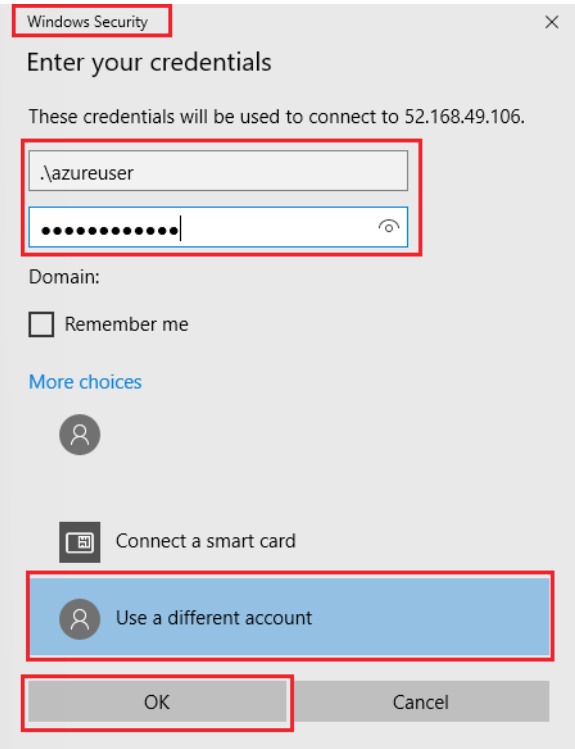
2.

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



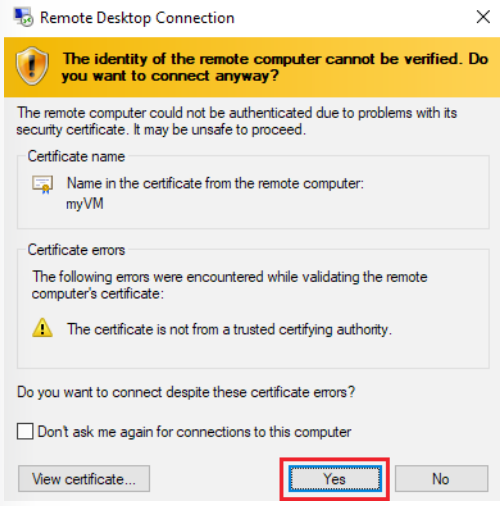
4.

5. 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**.



6.

7. 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.

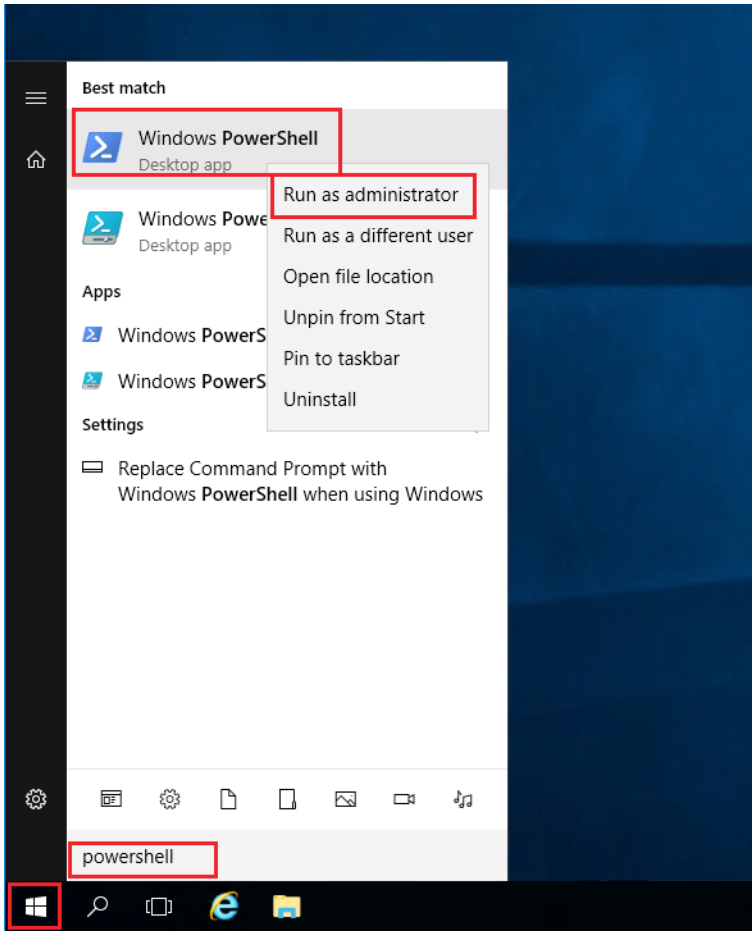


8.

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

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

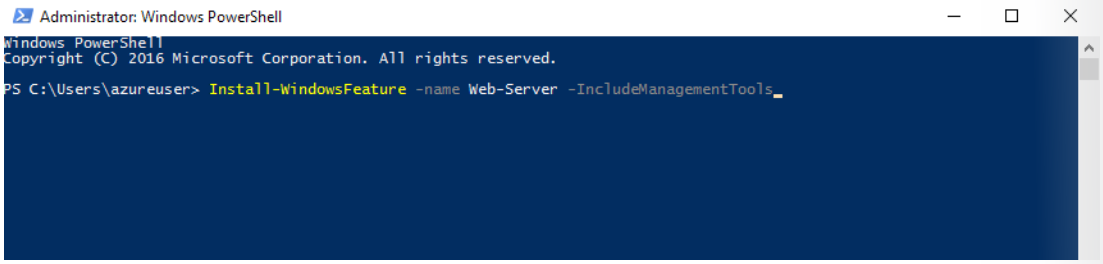
1. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell** right clicking **Windows PowerShell** in the menu and selecting **Run as administrator**



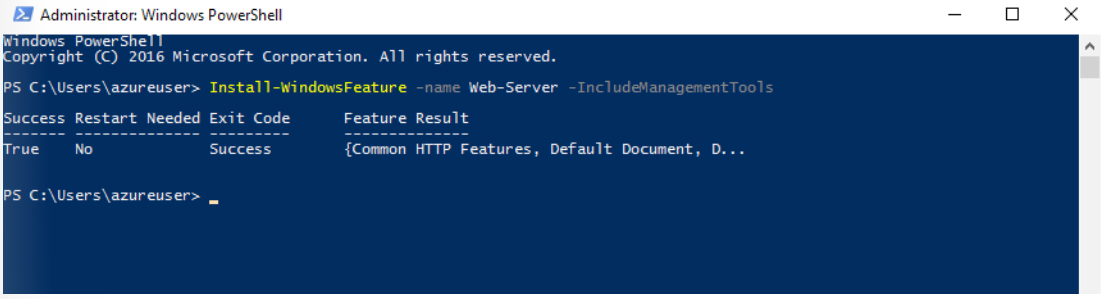
2.

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

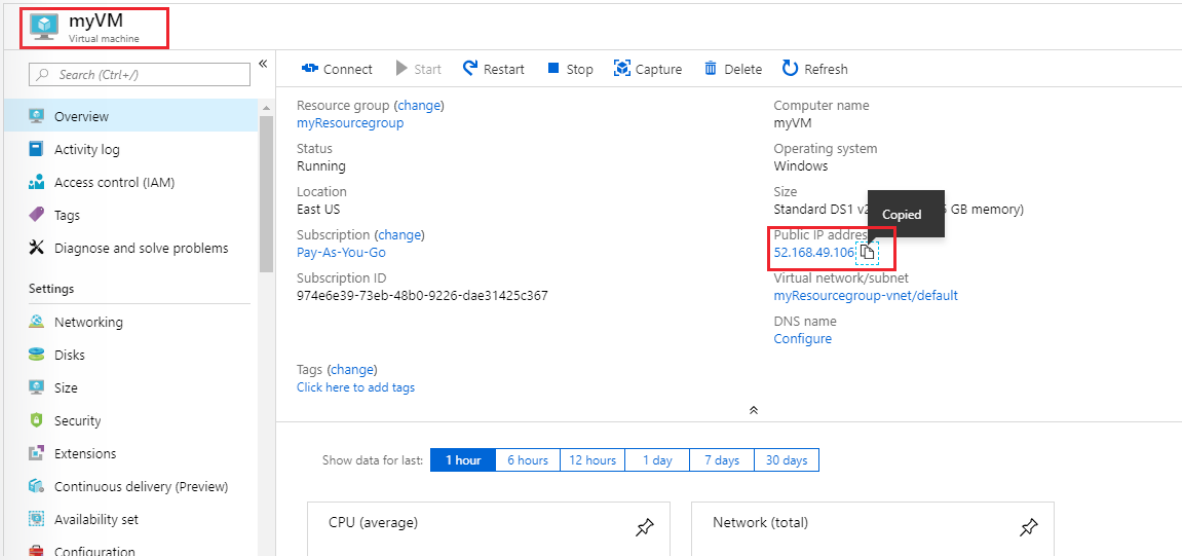
```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```



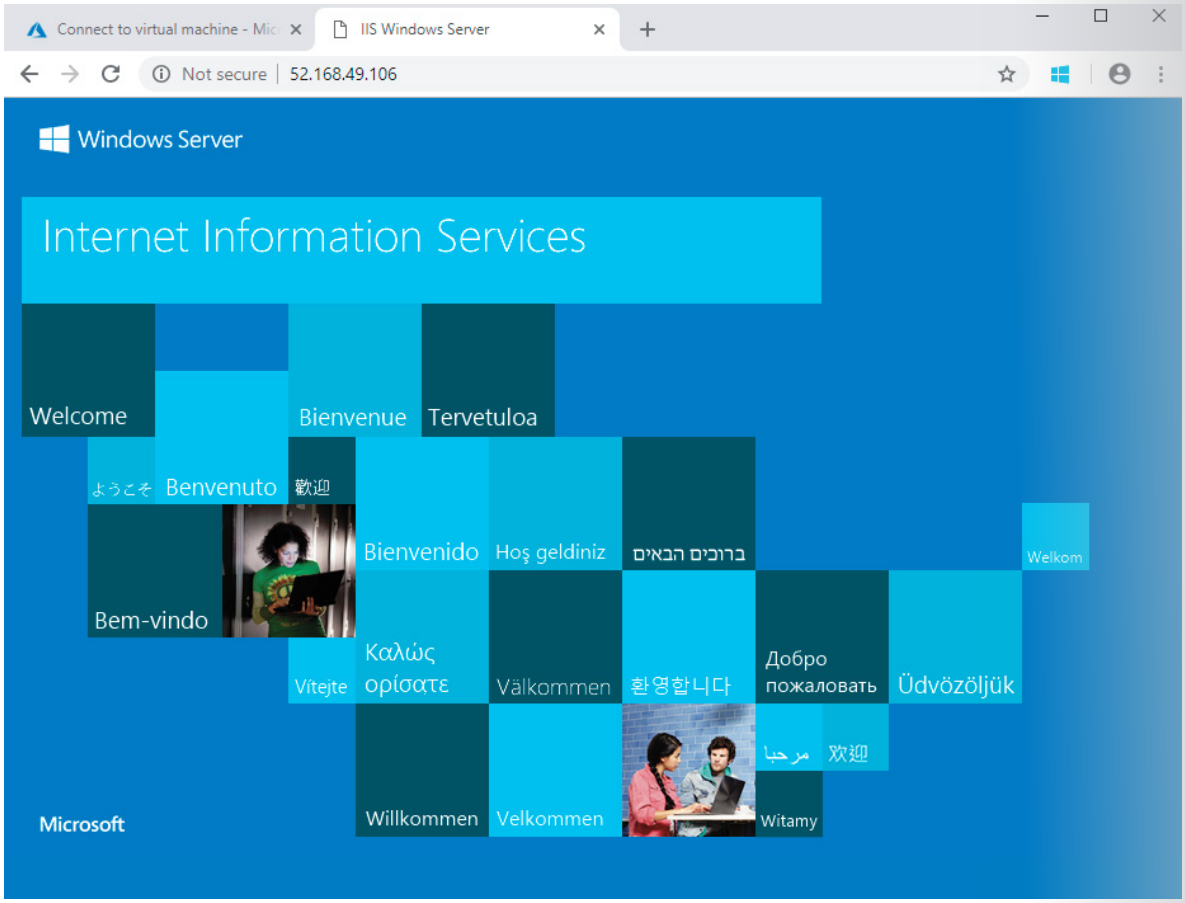
1. When completed you should see a prompt stating **Success** with a value **True**, among other items in the output. You do not need to restart the virtual machine to complete the installation. Close the RDP connection to the VM.



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



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



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

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

Video: Azure Networking Services

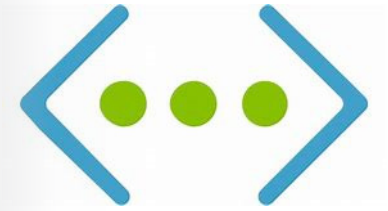
Azure Network Services

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 Network**[15] 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 Balancer**[16] for more details.

15 https://docs.microsoft.com/en-us/azure/virtual-network/
16 https://azure.microsoft.com/en-us/services/load-balancer/

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 Gateway**[17] for more details.

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** [18] 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** [19] for more details.

17 https://azure.microsoft.com/en-us/services/vpn-gateway/
18 https://azure.microsoft.com/en-us/services/application-gateway/
19 https://azure.microsoft.com/en-us/services/cdn/

Note: For a full list of networking services available with Azure, and context on when you use them, see the page **Networking**[20].

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.

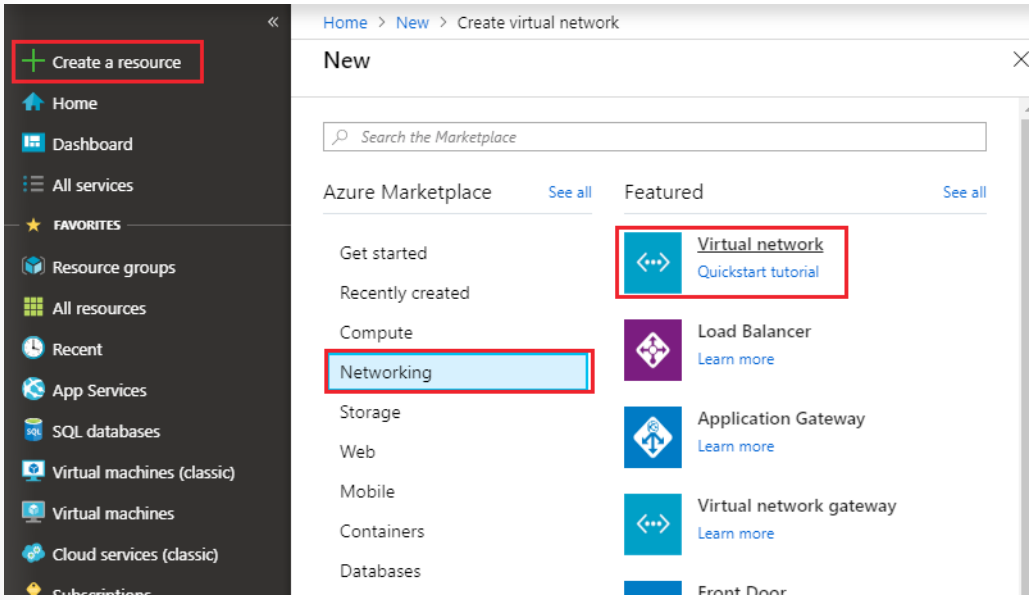
You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time.

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**[21] webpage.

Steps

1. Sign in to the Azure portal at **https://portal.azure.com**[22]
2. Choose **Create a resource** in the upper left-hand corner of the Azure portal, then select **Networking** > **Virtual network**

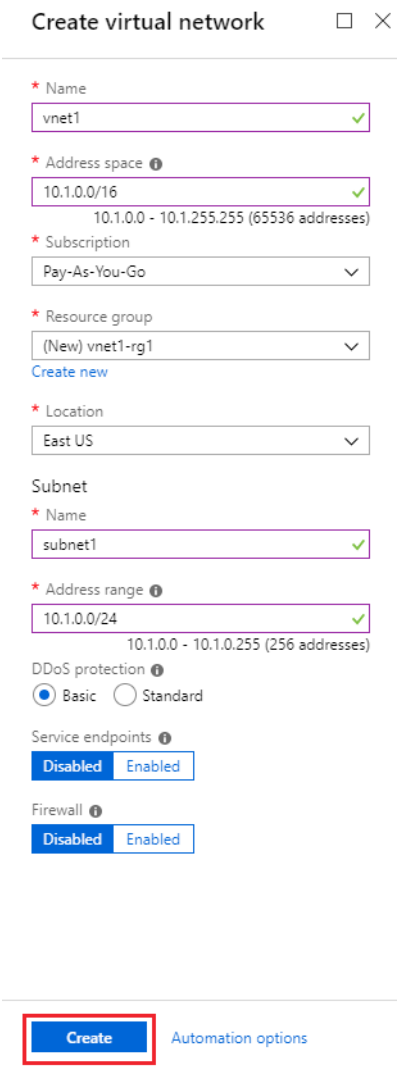


3.
4. In the **Create virtual network** pane above the list of Azure Marketplace resources, search for and select **Windows Server 2016 Datacenter**, then choose **Create**.

20 https://azure.microsoft.com/en-us/product-categories/networking/
21 https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio
22 https://portal.azure.com

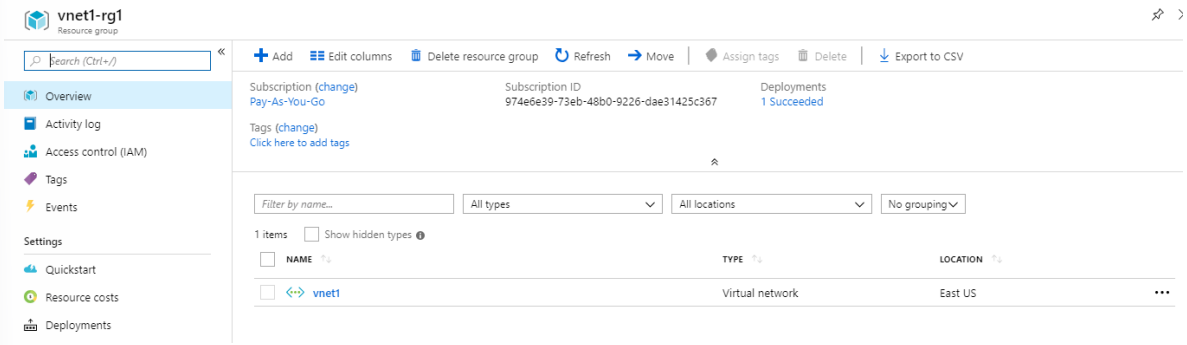
Setting	Value
Name	**vnet1**
Address space	**10.1.0.0/16**
Subscription	< Select your subscription >
Resource group	Select **Create new**, enter **vnet1-rg1**, then select **OK**.
Location	**East US**
Subnet - Name	**subnet1**
Subnet Address range	**10.1.0.0/24**

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



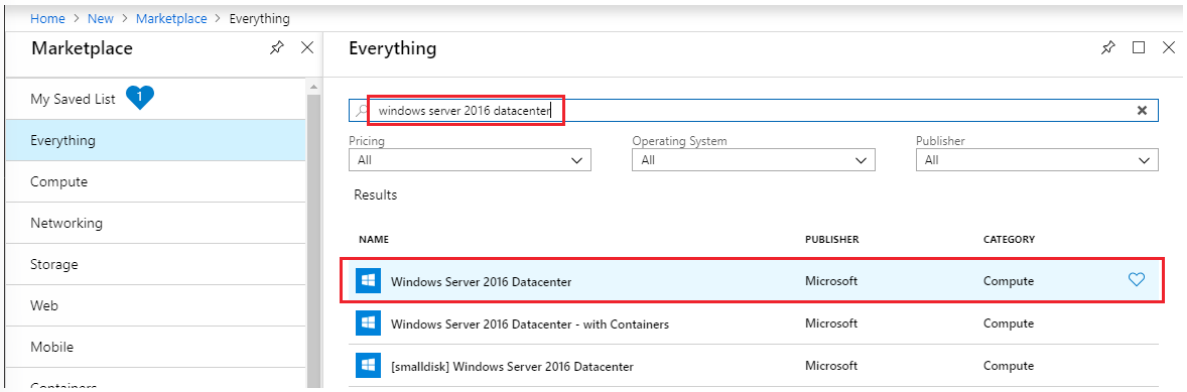
6.

7. 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.

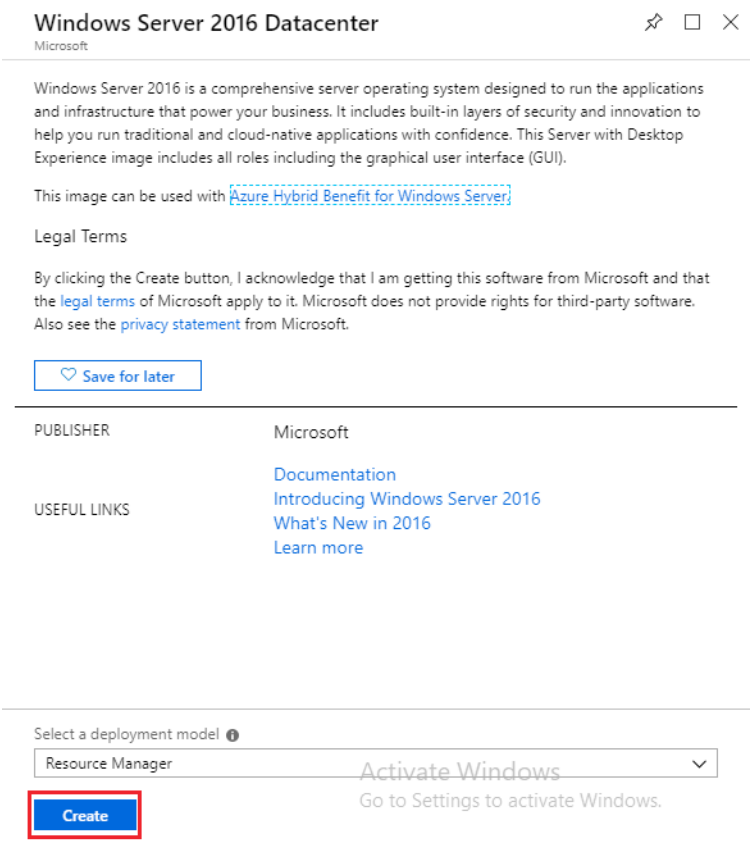


8.

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



10.



11.

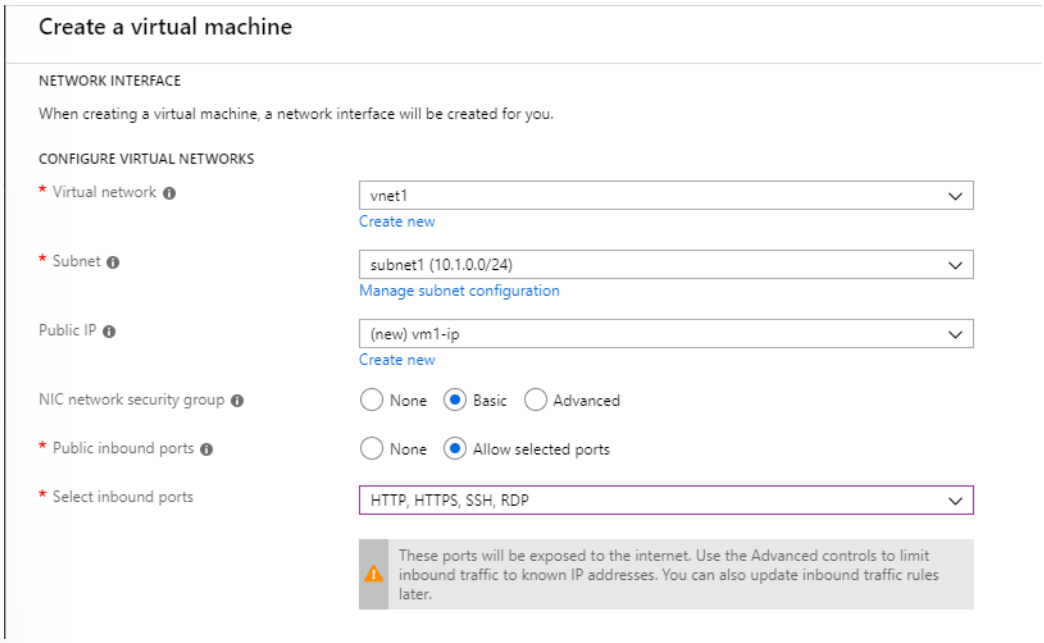
12. In Create a **virtual machine** - **Basics** tab, enter or select this information:

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**
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**

13. Select **Next** : **Disks**, leave the default values.

14. Select **Next** : **Networking**, complete the following details

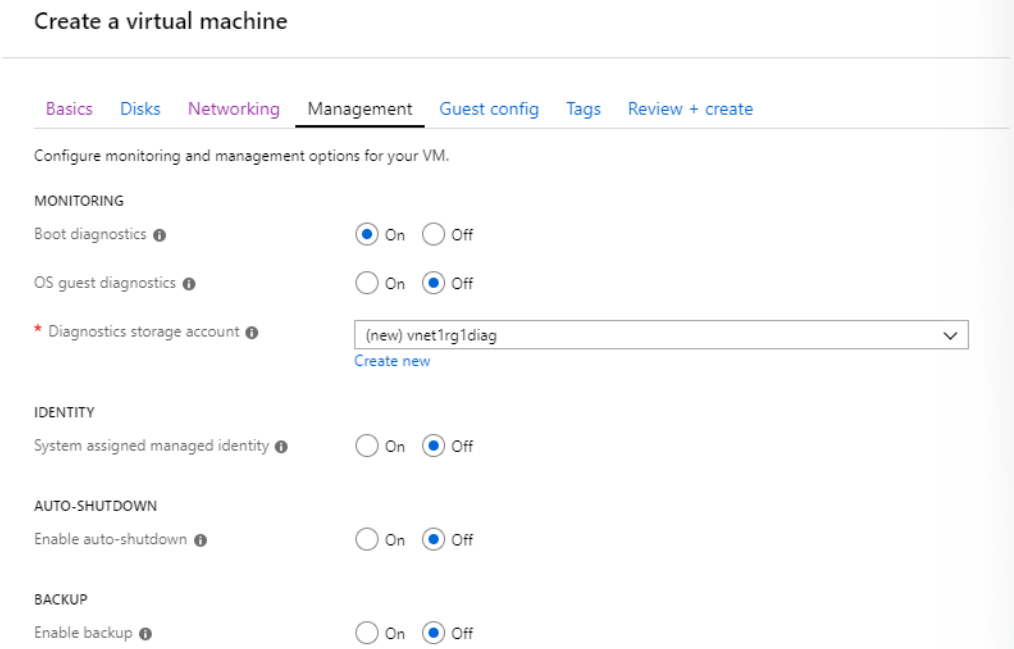
Setting	Value
Virtual network	Leave the default **vnet1**
Subnet	Leave the default **subnet1 (10.1.0.0/24)**
Public IP	Leave the default (new) **vm1-ip**
NIC network security group	accept the default **Basic**
Public inbound ports	Select **Allow selected ports**
Select inbound ports	Select **HTTP**,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



15.

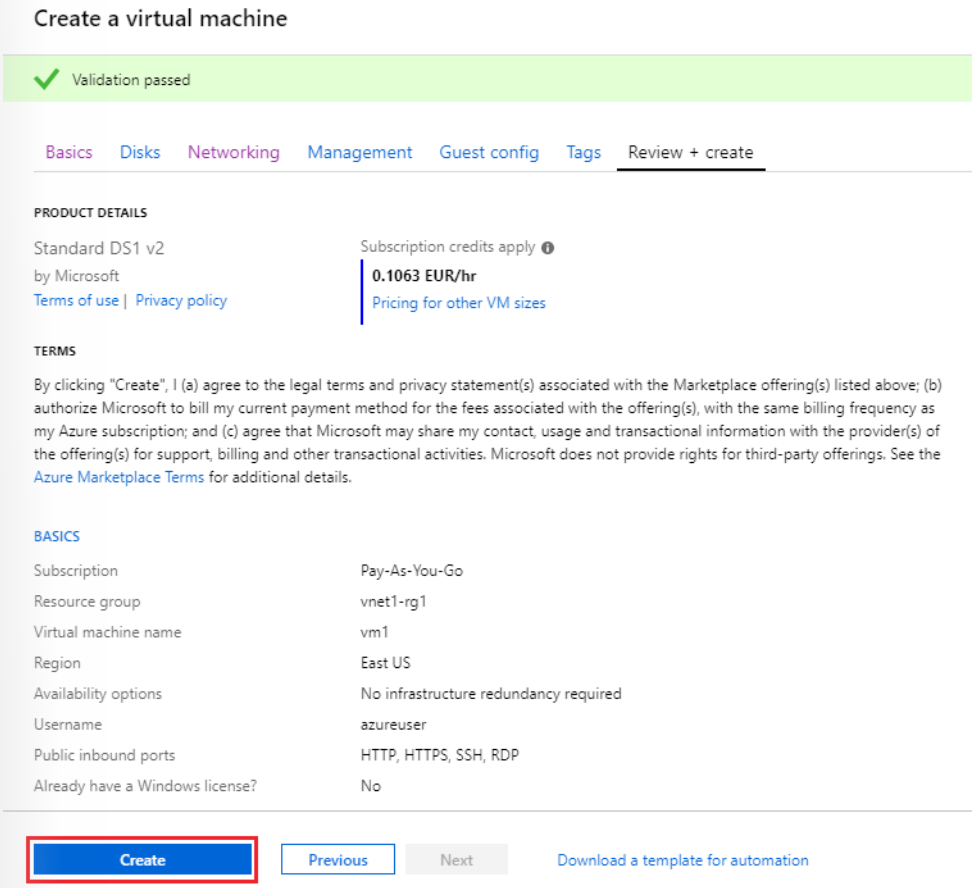
16. Select **Next** : **Management**, accept all the defaut values except for the below settings:

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



17.

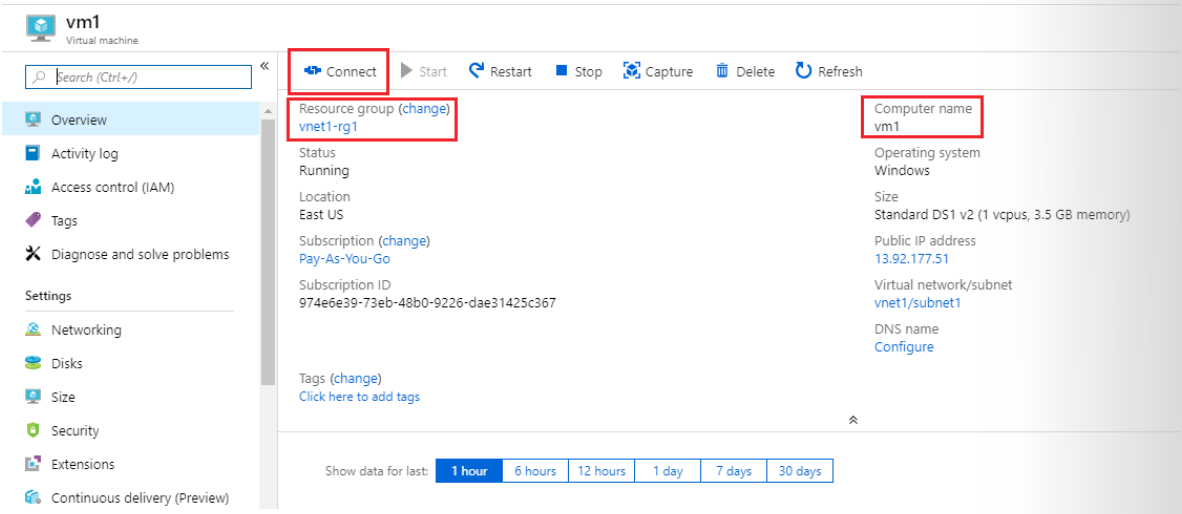
18. Select **Review** + **create**. Azure will validate the configuration. When you see that Validation passed, select **Create**. Deployment times can vary but it can generally take between three to six minutes to deploy.



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

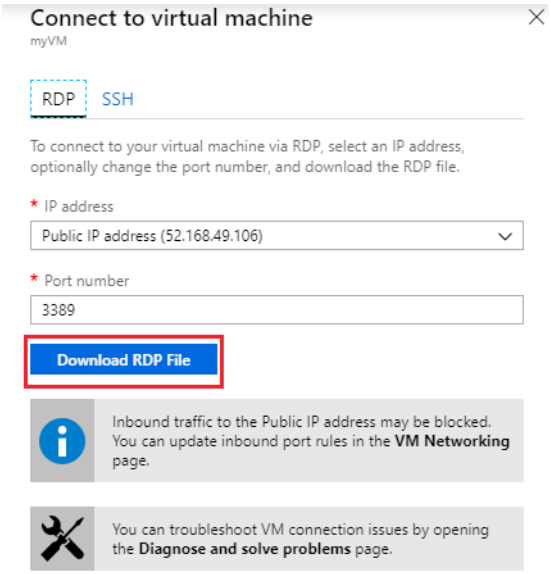
Setting	Value
Virtual machine name	**vm2**
Public IP	Leave the default (new) **vm2-ip**
Diagnostic storage account	Leave the default value i.e. **vnet1rg1diag**

2. When finished filling in the details, validate the configuration by clicking **Review + create** and once successfully validated click **Create**
3. 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.

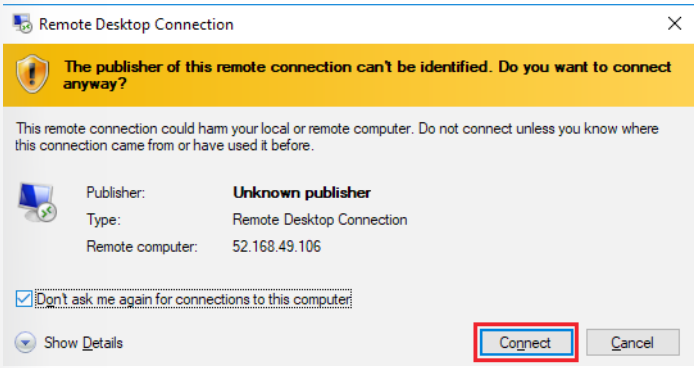


Note: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on Linux virtual machine you could connect directly from a bash shell using `ssh`.

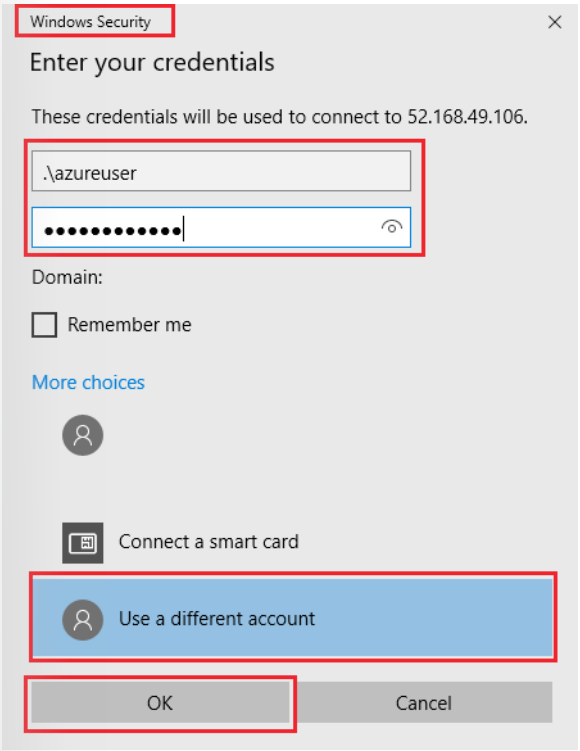
1. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP File**.



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

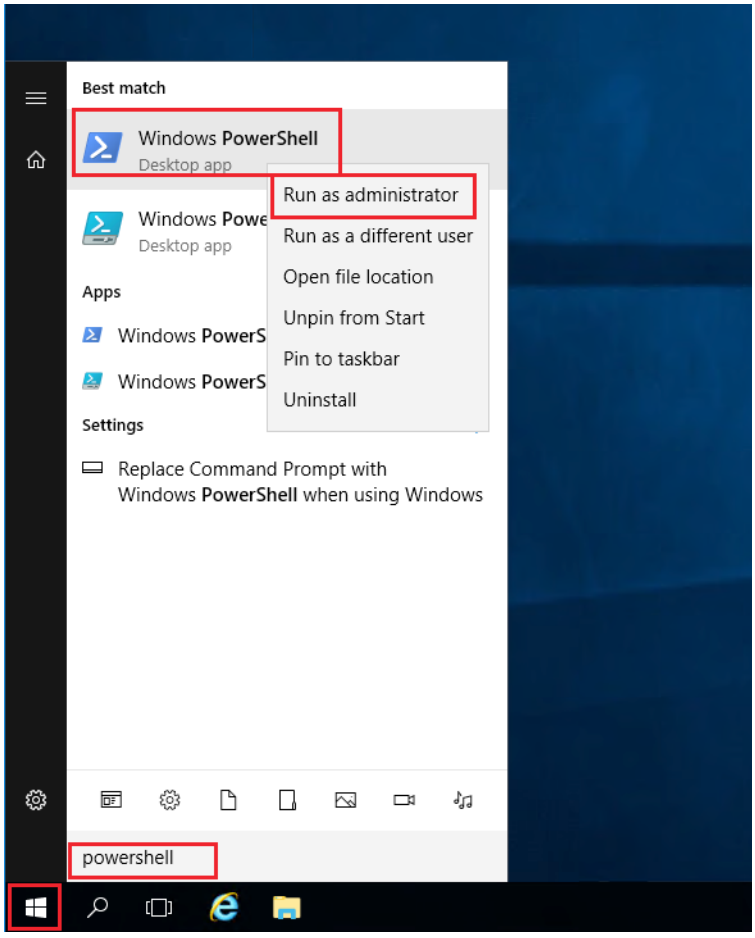


1. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as localhost\username, (you could also type **.\azureuser**) enter password you created for the virtual machine, and then click **OK**.



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

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



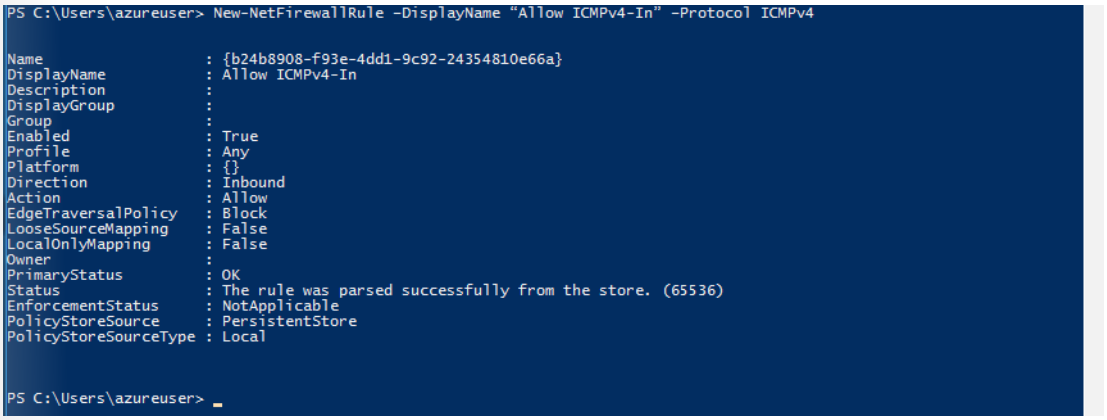
19. Run the command

```
ping vm2
```

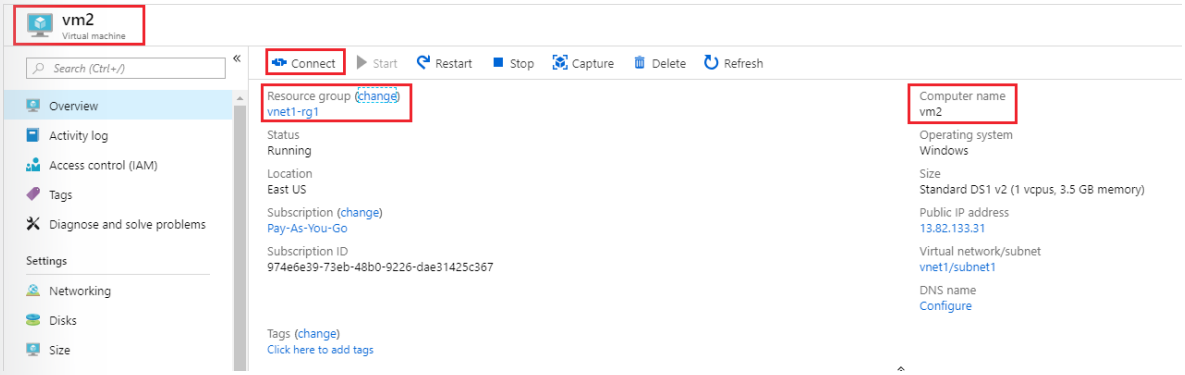
You receive an error, saying request timed out. The `ping` fails, because `ping` uses the **Internet Control Message Protocol (ICMP)**. By default, ICMP isn't allowed through the Windows firewall.

1. 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
```



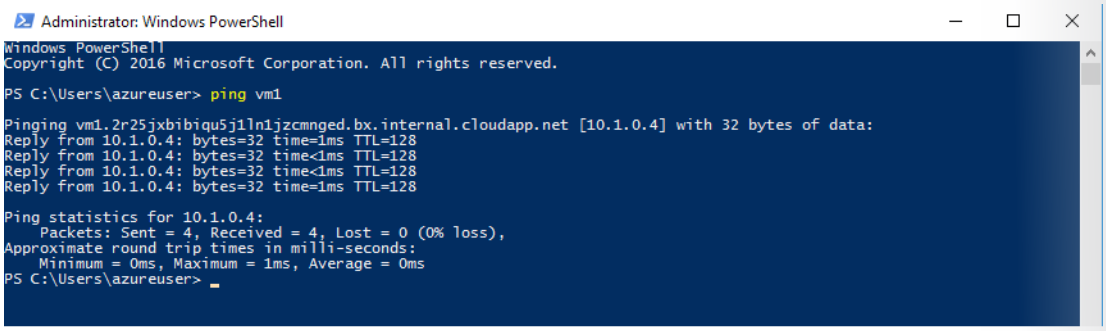
1. Connect to *VM2* as has been done for *VM1*, using rdp. i.e. open **vm2** properties and click the **Connect** button to download and then connect vis RDP



1. 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.



Congratualations! 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 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: Azure Storage Services

Azure Storage Services

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** [23] 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

23 https://azure.microsoft.com/en-us/services/storage/blobs/

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.

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 pricing[24] page. Also, see **Disk Storage**[25] 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 Files**[26] 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 Storage**[27] for more details.

Note: For a full list of storage services available with Azure, and context on when you use them, see the page **Storage**[28].

24 https://azure.microsoft.com/en-us/pricing/details/managed-disks/
25 https://azure.microsoft.com/en-us/services/storage/disks/
26 https://azure.microsoft.com/en-us/services/storage/files/
27 https://azure.microsoft.com/en-us/services/storage/archive/
28 https://azure.microsoft.com/en-us/product-categories/storage/

Demo: Create Blob Storage

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.

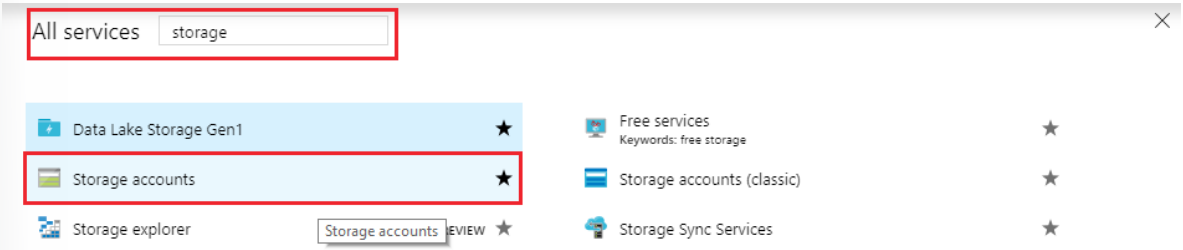
You can complete this walkthrough task by completing the steps outlined below, or you can simply read through them, depending on your available time.

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 today**[29] webpage.

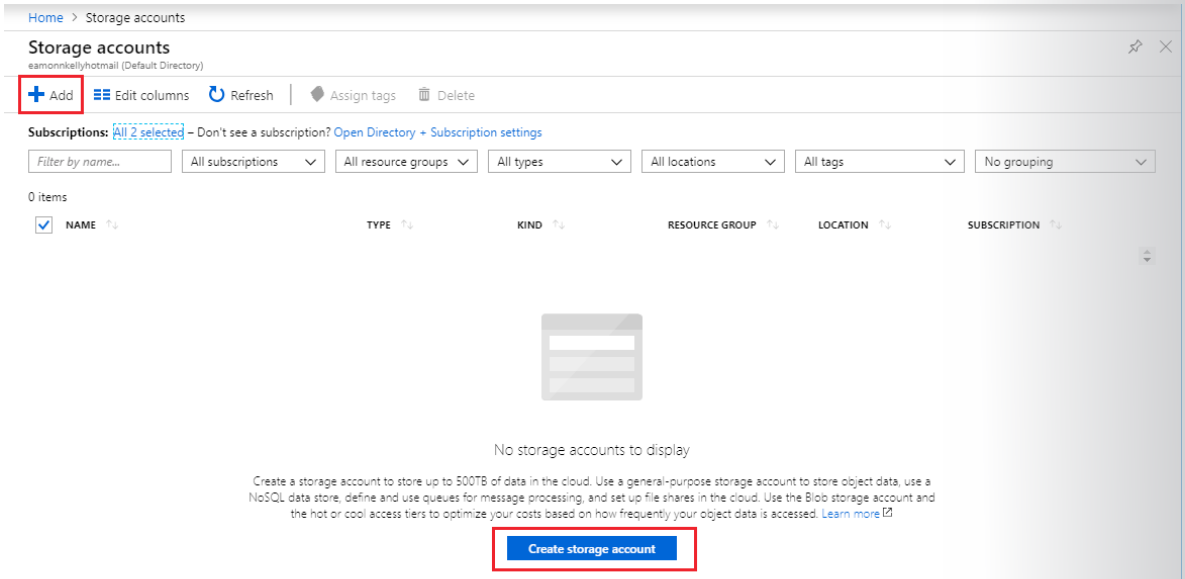
Steps

1. Sign in to the Azure portal at **https://portal.azure.com**[30]
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.
4. 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 nt be present and you can choose the option **+ Add**.

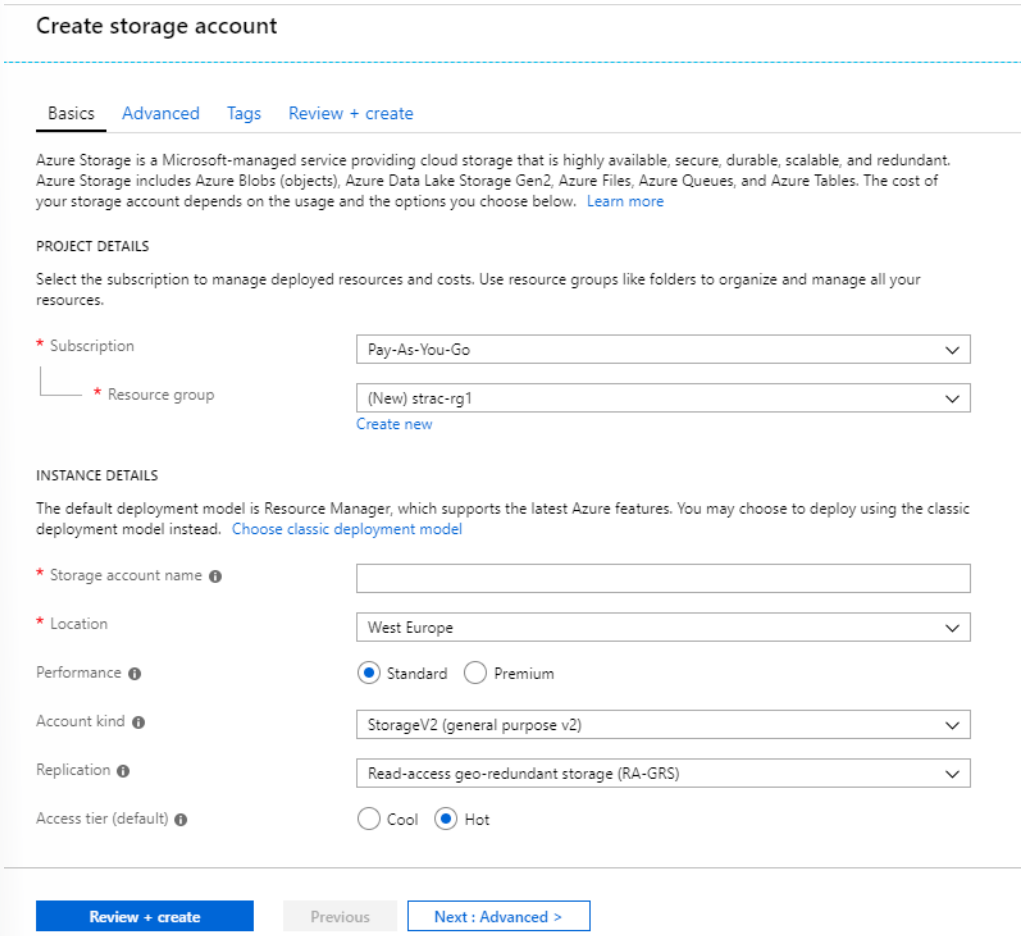
29 https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio
30 https://portal.azure.com



5.

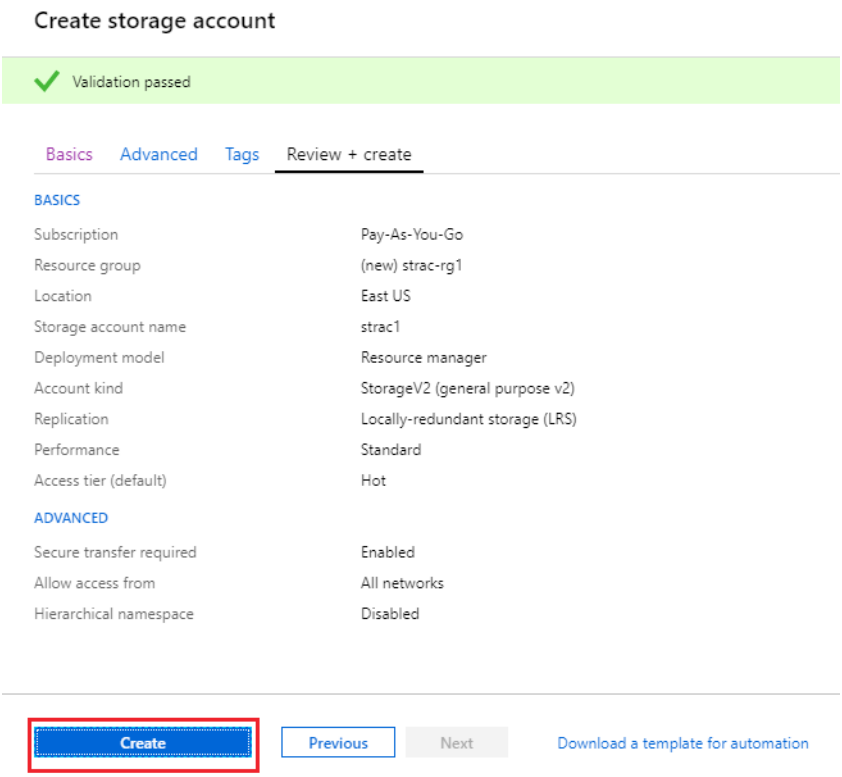
6. Complete the Create storage account blade with the following details

Setting	Value
Subscription	< Select your subscription >
Resource group	Select **Create new**, enter **strac-rg1**, then select **OK**.
Storage account name	< this must be 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**



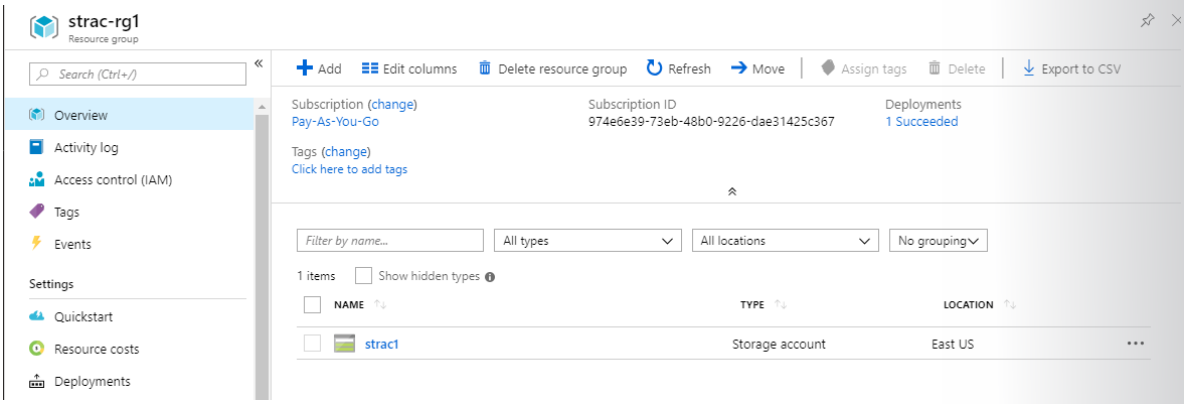
7.

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



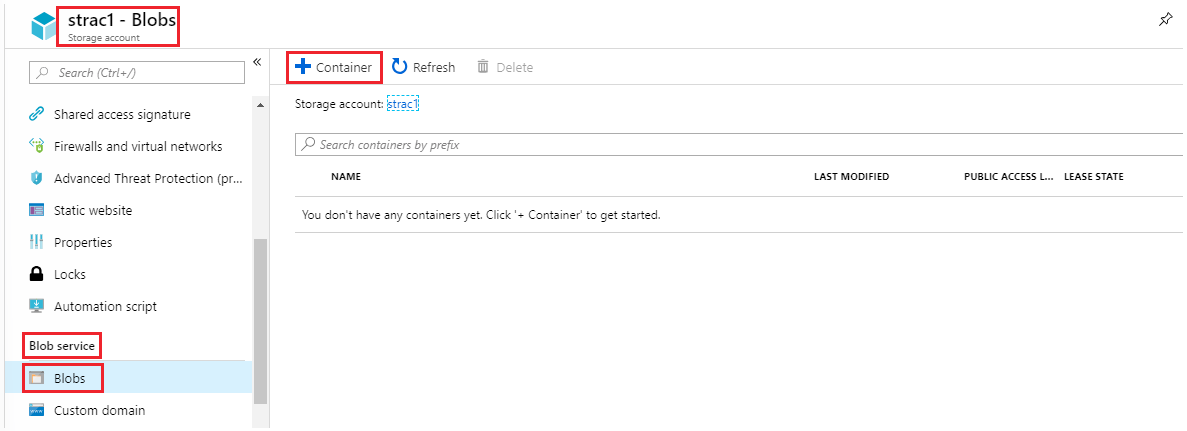
9.

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



11.

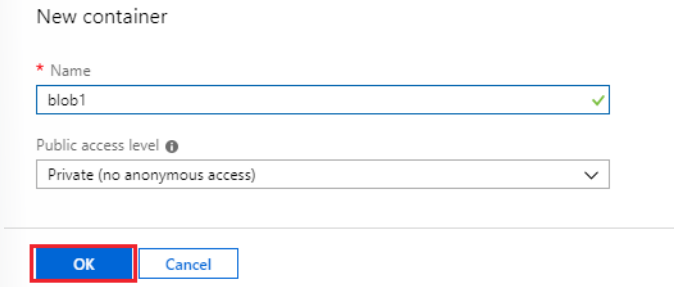
12. Open the storage account and scroll in the left menu for the storage account, scroll to the **Blob** service section, select **Blobs** and then select the **+ Container** button.



13.

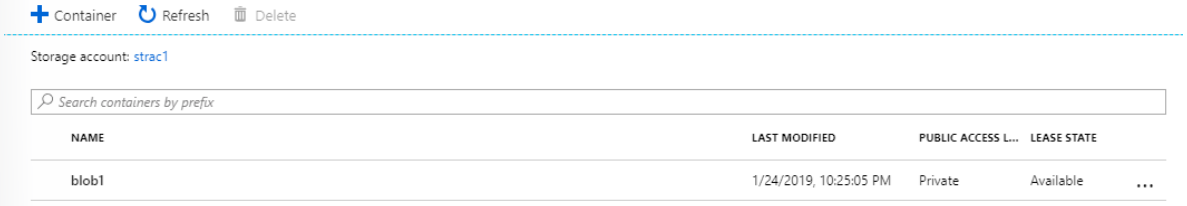
14. Configure the blob container as belwo and select OK when complete to create the blob container.

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)**



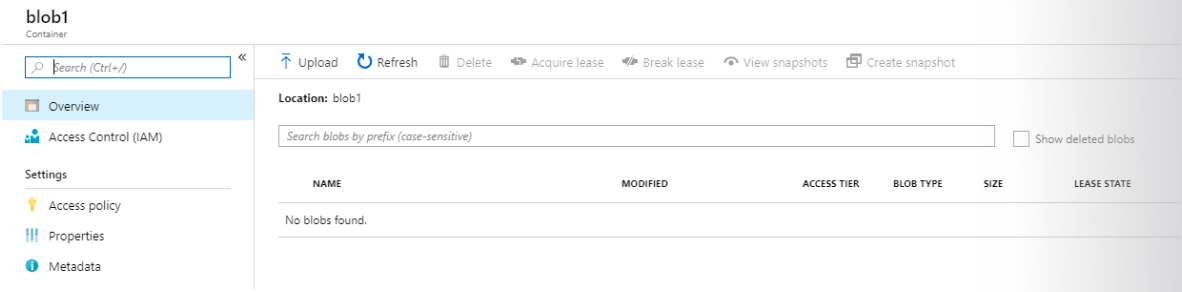
15.

16. The container should be created and available



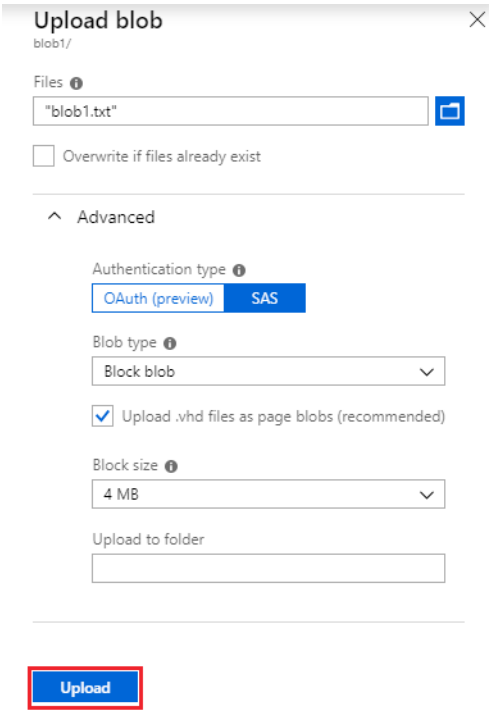
17.

18. 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



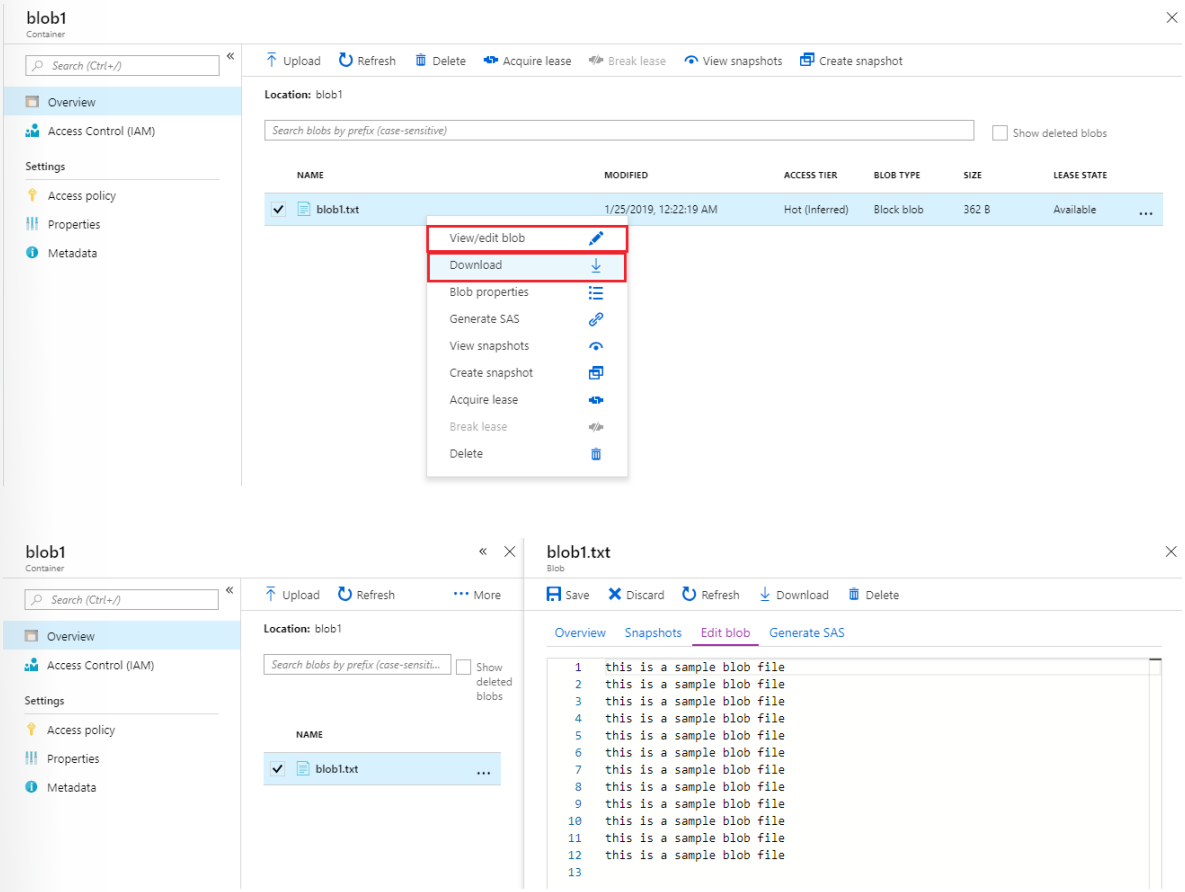
Note: Block blobs consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos.

1. 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.
2. 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**.

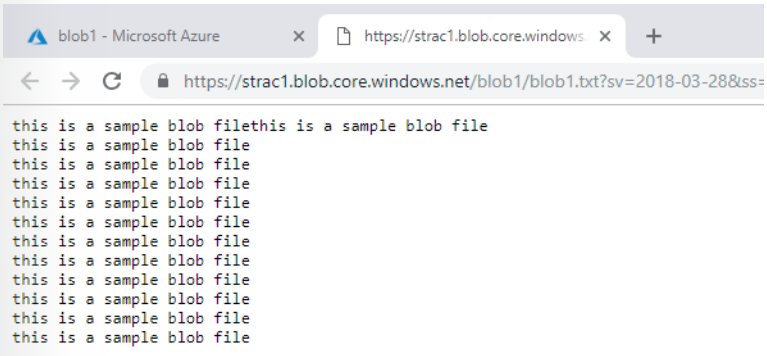


Note: You can upload as many blobs as you like in this way. You'll see that the new blobs are now listed within the container.

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



1. 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



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

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: Azure Data Services

Azure Database Services

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 DB**[31] for more details.

31 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 Database**[32] for more general details.

32 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 Service**[33] for more details.

Note: For a full list of data services available with Azure, and context on when you use them, see the page **Databases**[34].

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

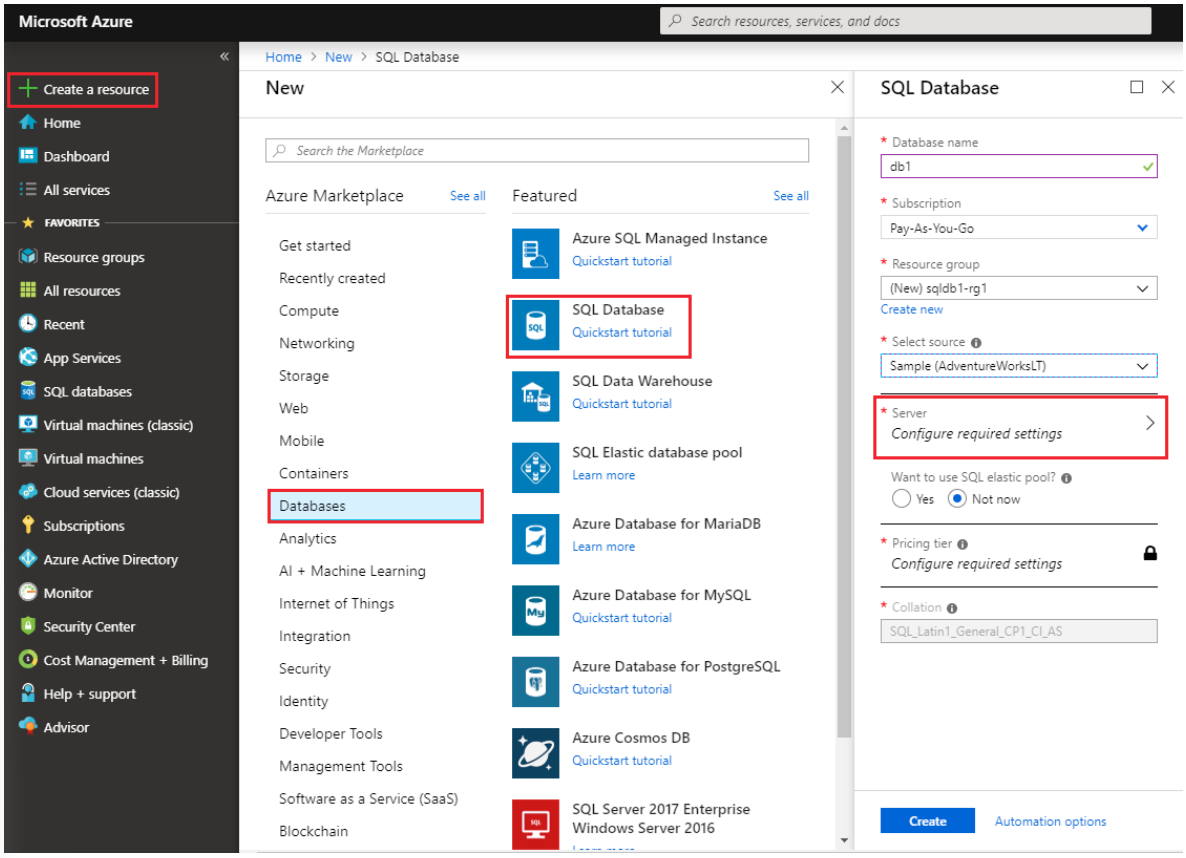
- You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the **Create your Azure free account today**[35] webpage.

Steps

1. Sign in to the Azure portal at **https://portal.azure.com**[36]
2. 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**

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**

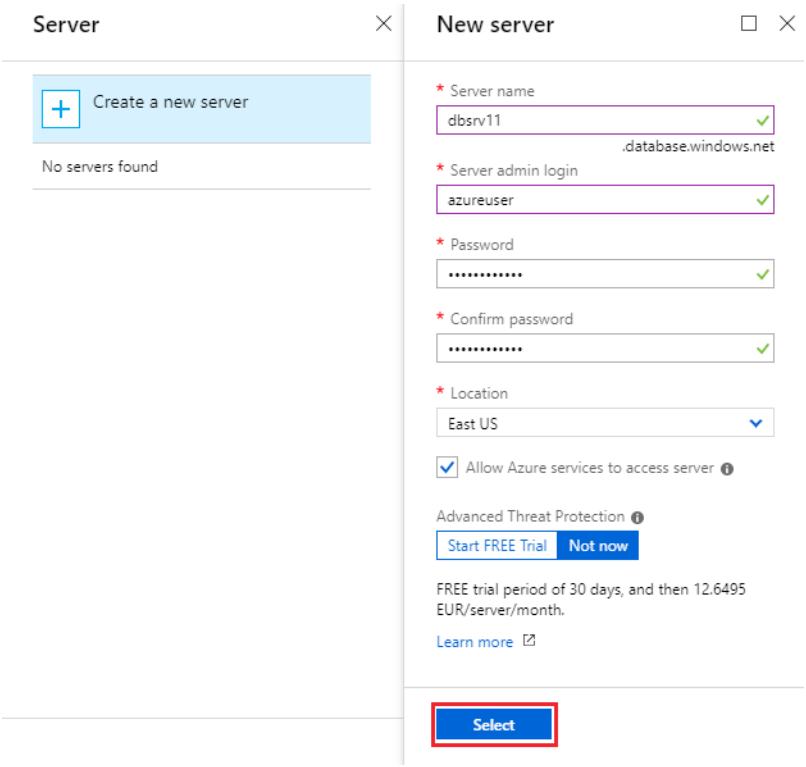
33 https://azure.microsoft.com/en-us/services/database-migration/
34 https://azure.microsoft.com/en-us/product-categories/databases/
35 https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio
36 https://portal.azure.com



3.

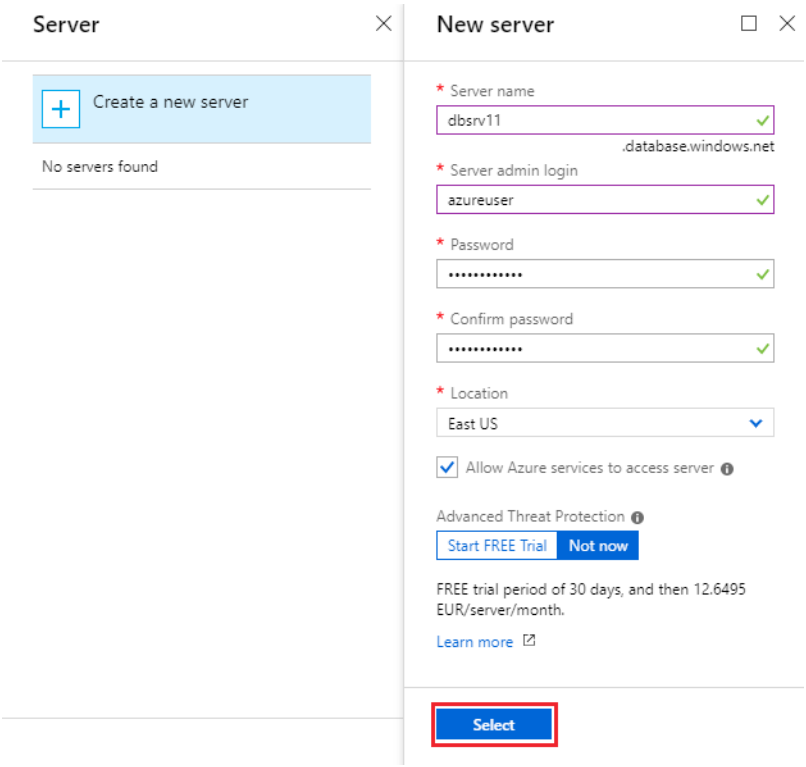
4. In the **Server** pane, choose **Create a new server** and complete the New server pane using below details and click **Select** when finished.

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**



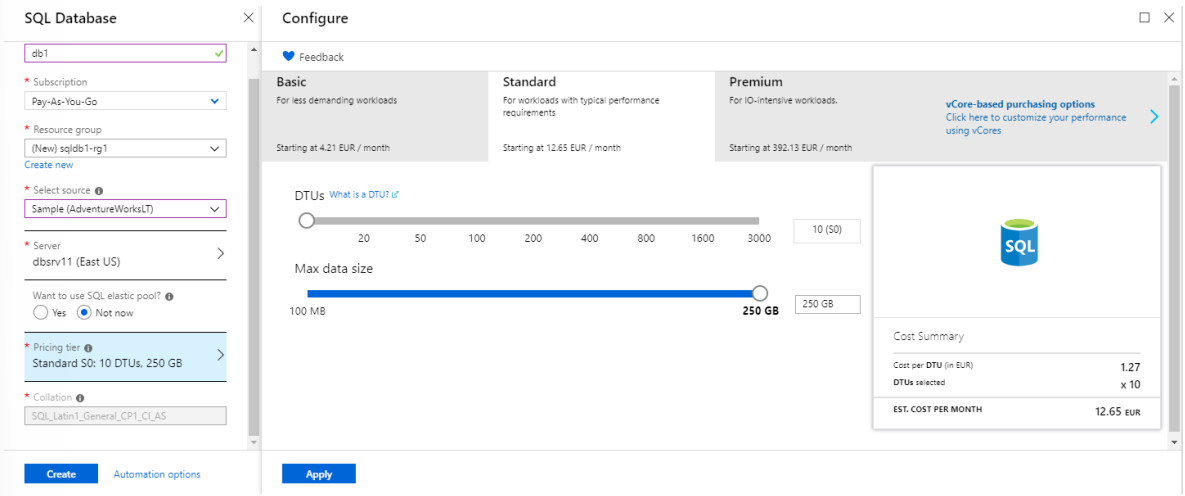
5.

6. 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 nt be present and you can choose the option **+ Add**.



7.

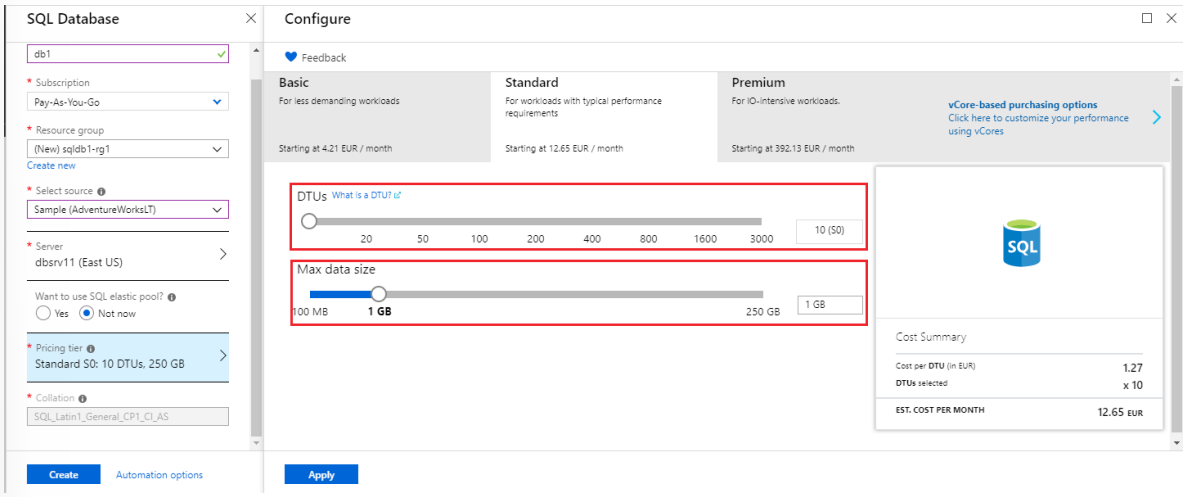
8. On the **SQL Database** pane , select **Pricing tier**. Explore the amount of *DTUs* and *storage* available for each service tier.



9.

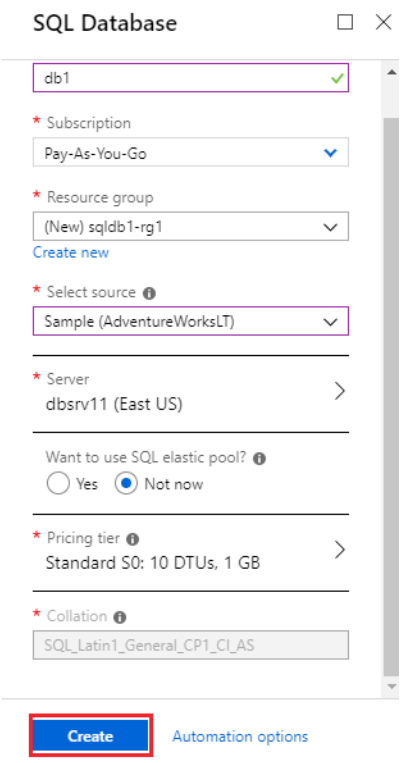
Note: This database uses the DTU-based purchasing model, but there is another, the vCore-based purchasing model, which is also available.

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



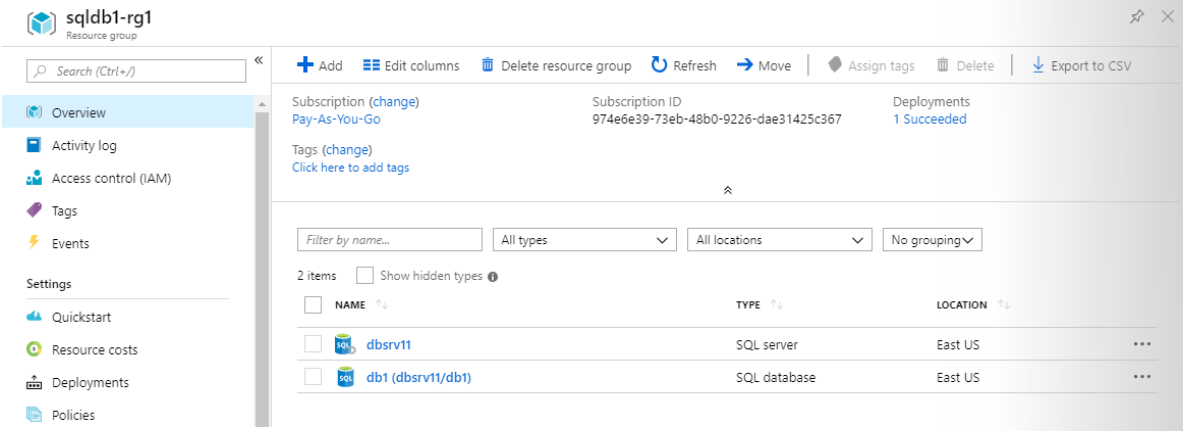
2.

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



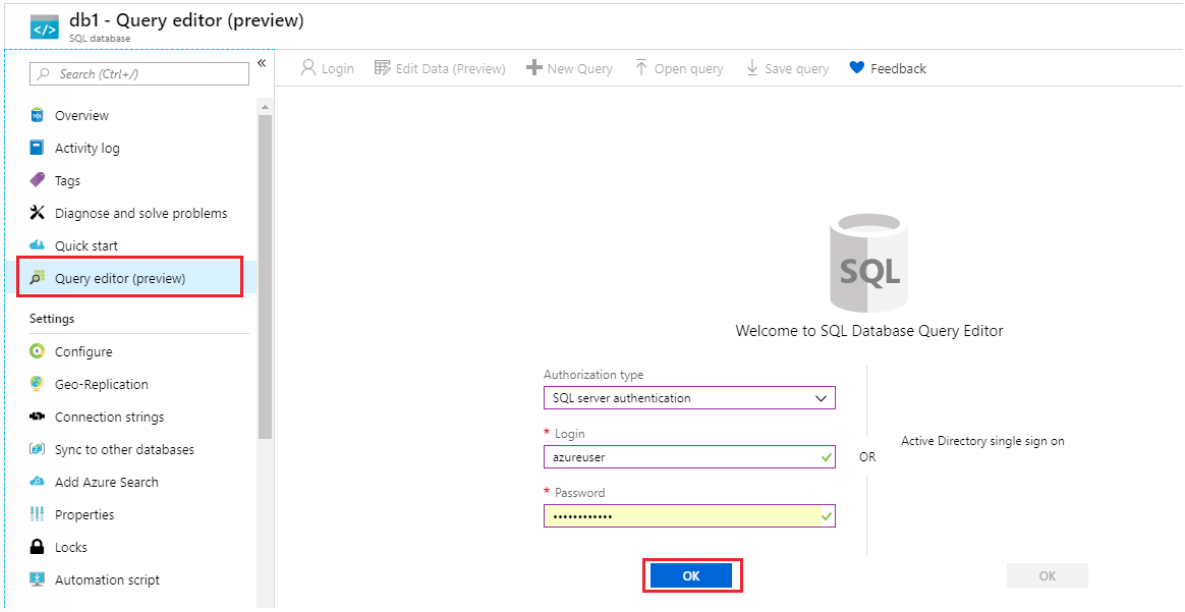
4.

5. 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.



6.

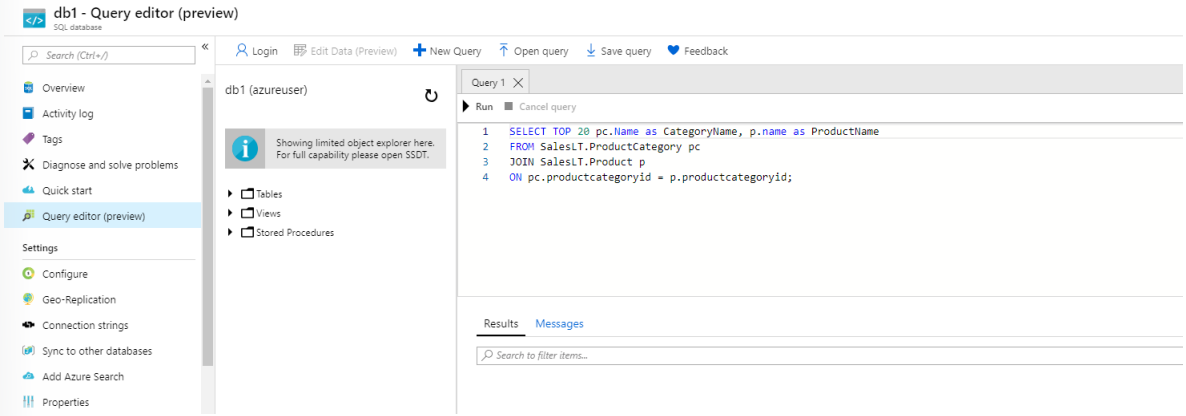
7. Open the SQL database you crated **db1**, go to the **Query Editor (preview)** in the left hand pane, and enter the login details and password. then click **OK**



8.

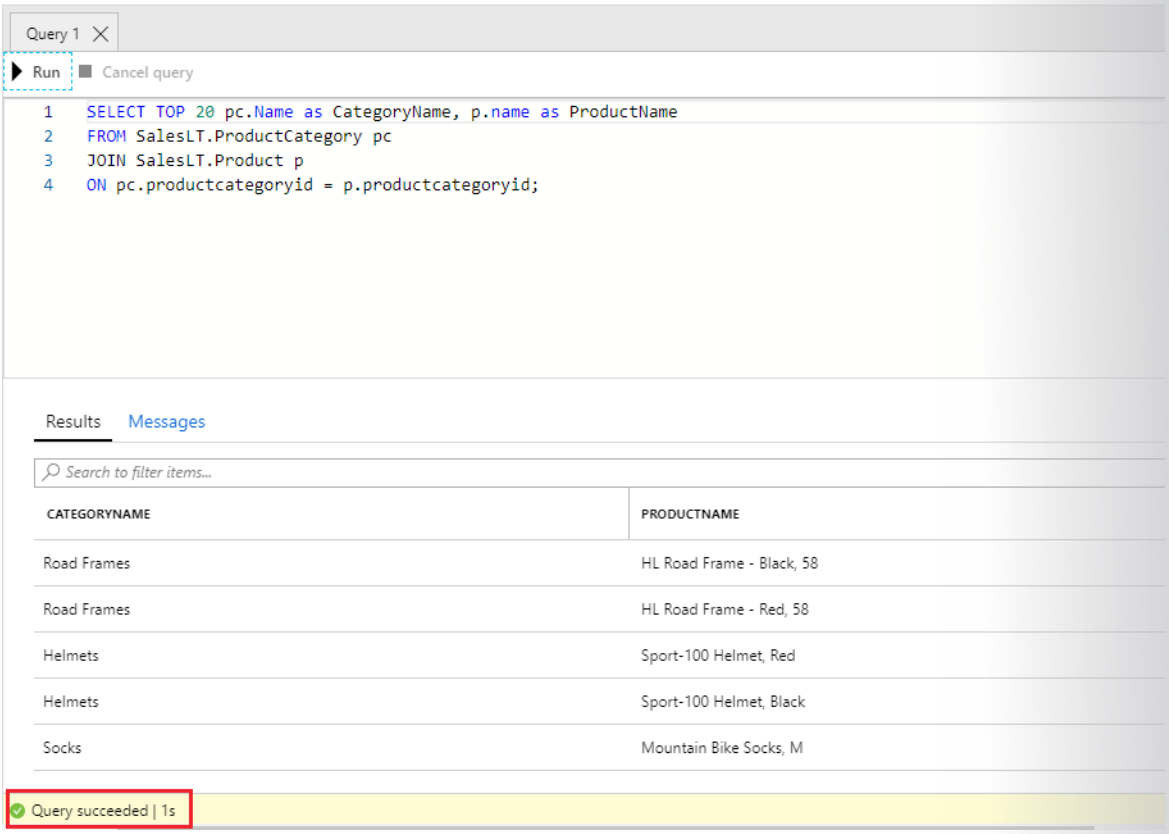
9. Once you log in successfully the query pane appears, enter the following query into the editor pane

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



10.

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



12.

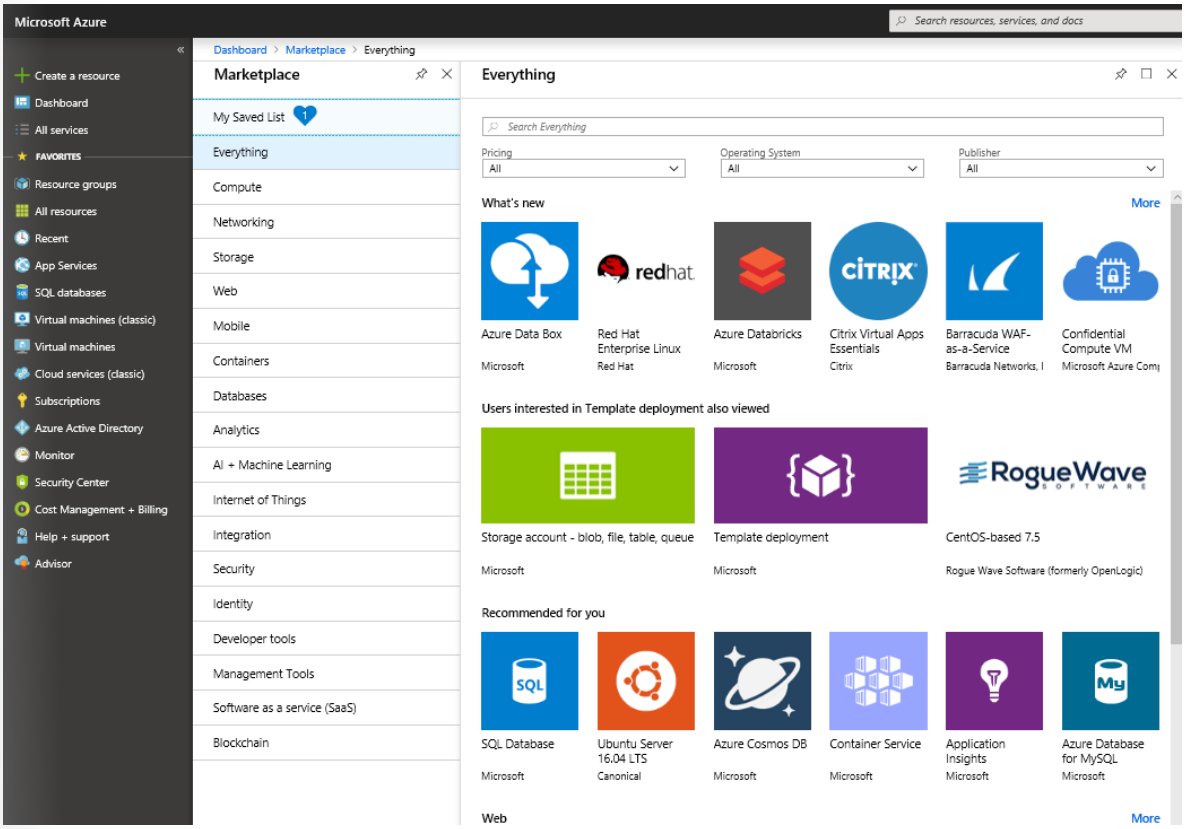
Congratulations! You have created a SQL database in Azure and successfully queried the data in that database.

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: Azure Marketplace

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/**[37] and there is also a **Marketplace FAQ**[38] available.

37 https://azuremarketplace.microsoft.com/en-us/
38 https://azure.microsoft.com/en-us/marketplace/faq/

Azure Solutions

Video: Internet of Things

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 garner 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 Central**[39] for more details.

Azure IoT Hub

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

39 https://azure.microsoft.com/en-us/services/iot-central/

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**[40] 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**[41].

Video: Big Data and Analytics

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

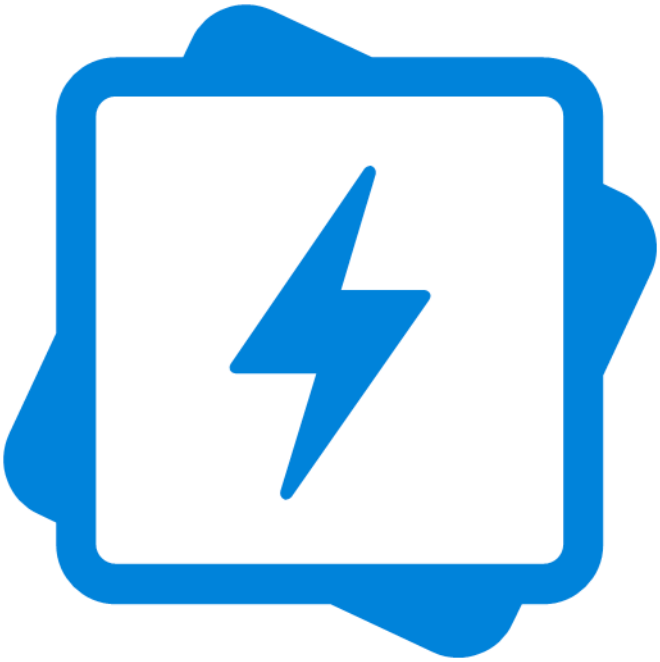
40 https://azure.microsoft.com/en-us/services/iot-hub/
41 https://azure.microsoft.com/en-us/product-categories/iot/

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**[42] 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**[43], **Apache Hadoop**[44], **Apache Kafka**[45], **Apache HBase**[46], **Apache Storm**[47], **Machine Learning Services**[48]. HDInsight also supports a broad range of scenarios such as extraction, transformation, and loading (ETL); data warehousing; machine learning; and IoT. See **HDInsight**[49] for more general details.

Azure Data Lake Analytics



42 https://azure.microsoft.com/en-us/services/sql-data-warehouse/
43 https://docs.microsoft.com/en-us/azure/hdinsight/spark/apache-spark-overview
44 https://docs.microsoft.com/en-us/azure/hdinsight/hadoop/apache-hadoop-introduction
45 https://docs.microsoft.com/en-us/azure/hdinsight/kafka/apache-kafka-introduction
46 https://docs.microsoft.com/en-us/azure/hdinsight/hbase/apache-hbase-overview
47 https://docs.microsoft.com/en-us/azure/hdinsight/storm/apache-storm-overview
48 https://docs.microsoft.com/en-us/azure/hdinsight/r-server/r-server-overview
49 https://azure.microsoft.com/en-us/services/hdinsight/

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**[50] for more details.

Note: For a full list of big data and analytics services available with Azure, see the page **Analytics**[51].

Video: Artificial Intelligence

Artifical Intelligence

Artificial 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 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

50 https://azure.microsoft.com/en-us/services/data-lake-analytics/
51 https://azure.microsoft.com/en-us/product-categories/analytics/

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 service**[52] 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 Studio**[53] for more general details.

Note: For a full list of Artificial Intelligence and Machine Learning services available with Azure, see the page **AI + Machine Learning**[54].

Video: Serverless Computing

Serverless Computing

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.

52 https://azure.microsoft.com/en-us/services/machine-learning-service/
53 https://azure.microsoft.com/en-us/services/machine-learning-studio/
54 https://azure.microsoft.com/en-us/services/

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.

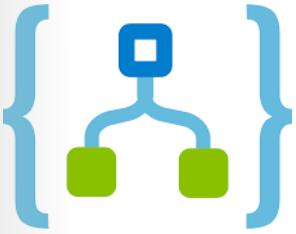
Azure Functions

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.

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 **Functions**[55] 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,

55 https://azure.microsoft.com/en-us/services/functions/

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 Apps**[56] 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 Grid**[57] for more details.

Note: For more details about serverless services available with Azure, see the page **Serverless in Azure**[58].

Video: DevOps

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.

56 https://azure.microsoft.com/en-us/services/logic-apps/
57 https://azure.microsoft.com/en-us/services/event-grid/
58 https://azure.microsoft.com/en-us/solutions/serverless/

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 DevOps**[59] for more details.

Azure DevTest Labs

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**[60] for more general details.

Note: For more general details on DevOps services available with Azure, see the page **DevOps**[61].

59 https://azure.microsoft.com/en-us/services/devops
60 https://azure.microsoft.com/en-us/services/devtest-lab/
61 https://azure.microsoft.com/en-us/solutions/devops

Azure Management Tools

Video: Azure Management Tools

Azure Management Tools

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.

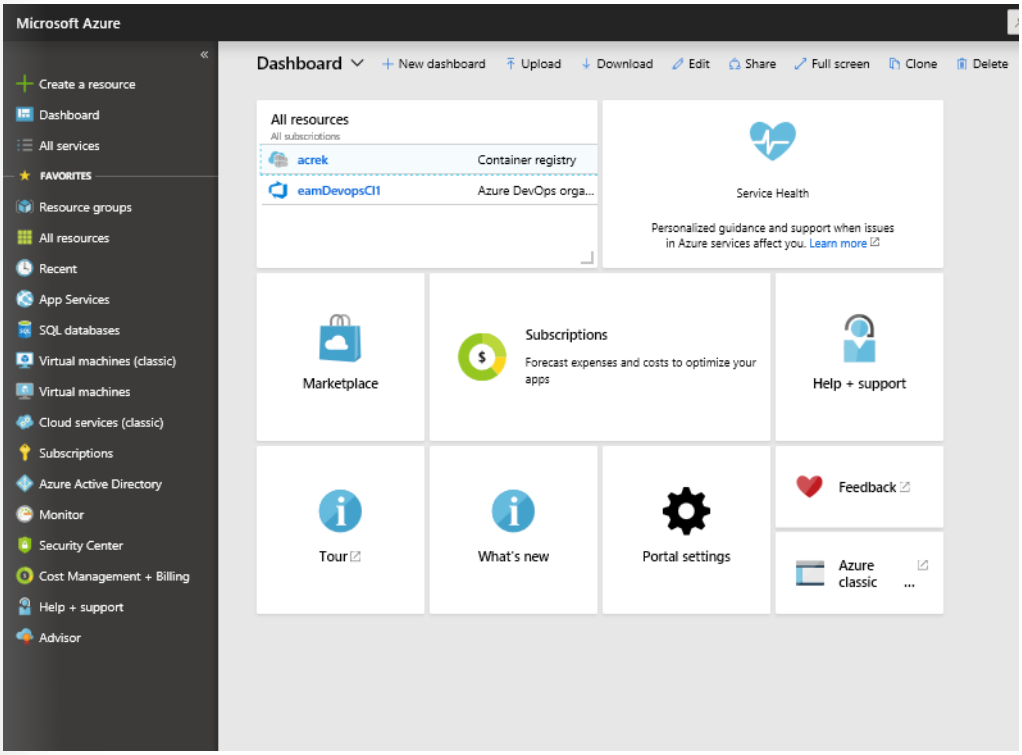
Azure Portal

Azure Portal is a website that you can access with a web browser, by going to the URL **https://portal.azure.com**[62]. 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.

62 https://portal.azure.com

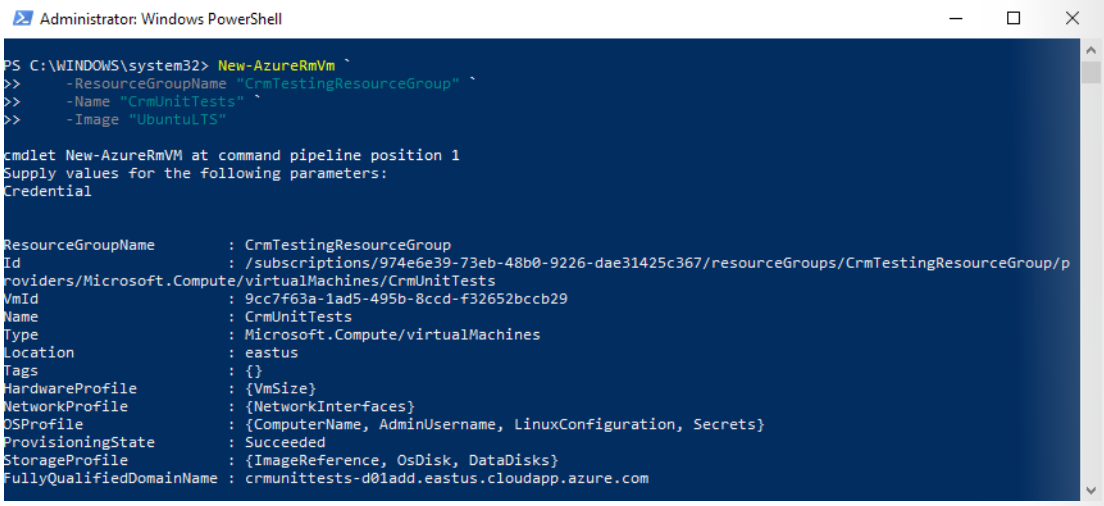


Azure PowerShell

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"
    ...
```

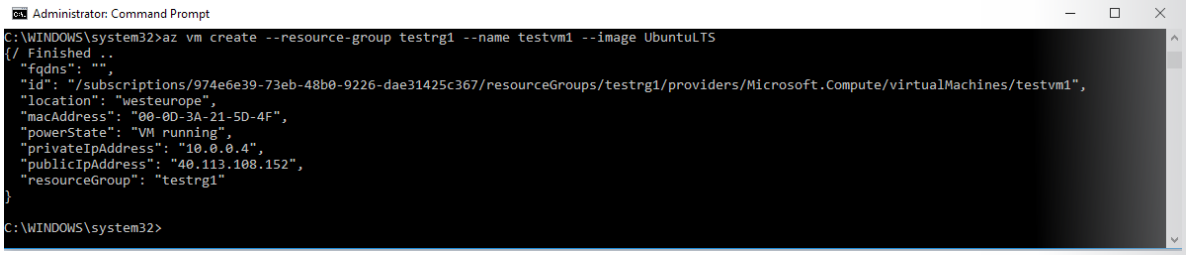


Note: *PowerShell Core* is a cross-platform version of PowerShell that runs on Windows Linux or macOS. Details are available from the page **What's New in PowerShell Core 6.1**[63] which is now also available.

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
  ...
```



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.

63 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/**[64].

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**[65] page.

Demo: Customize the Azure Portal

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**[66] 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**[67] page.

Steps

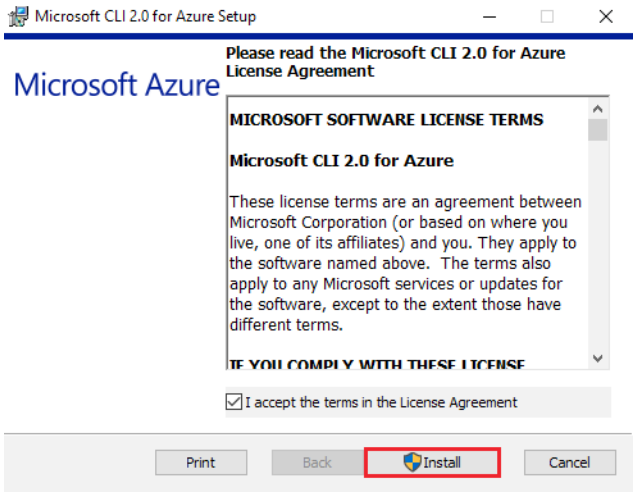
We will install Azure CLI on the Windows operating system using the MSI installer:

1. To download the Azure CLI msi, click on the URL **https://aka.ms/installazurecliwindows**[68], and in the browser, select to **Run**.

2.

64 https://shell.azure.com/
65 https://azure.microsoft.com/en-us/downloads/
66 https://azure.microsoft.com/en-us/free/?ref=microsoft.com&utm_source=microsoft.com&utm_medium=docs&utm_campaign=visualstudio
67 https://docs.microsoft.com/cli/azure/install-azure-cli
68 https://aka.ms/installazurecliwindows

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



4.

5. In the **User Account Control** dialog, select **Yes**.

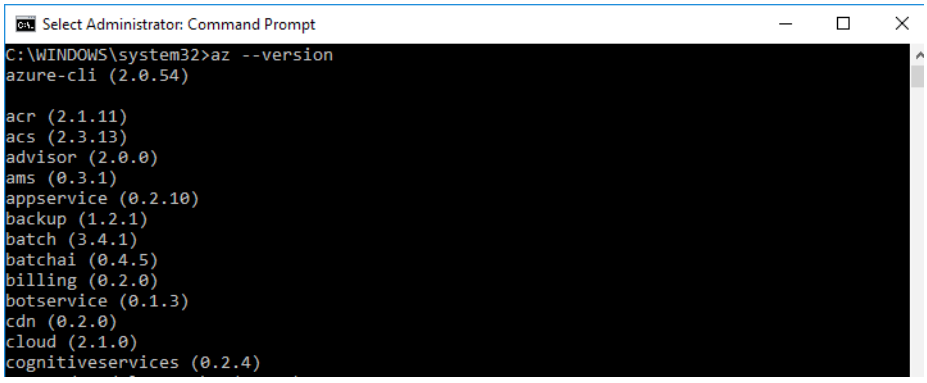
6. Once successfully installed, the Azure CLI is run by opening a Bash shell for Linux or macOS, or from the command prompt or PowerShell for Windows. Open a command prompt as administrator.

7. Login to your Azure subscription by runnning the below command and following the prompts

```
az login
```

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

```
az --version
```



1.

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.

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

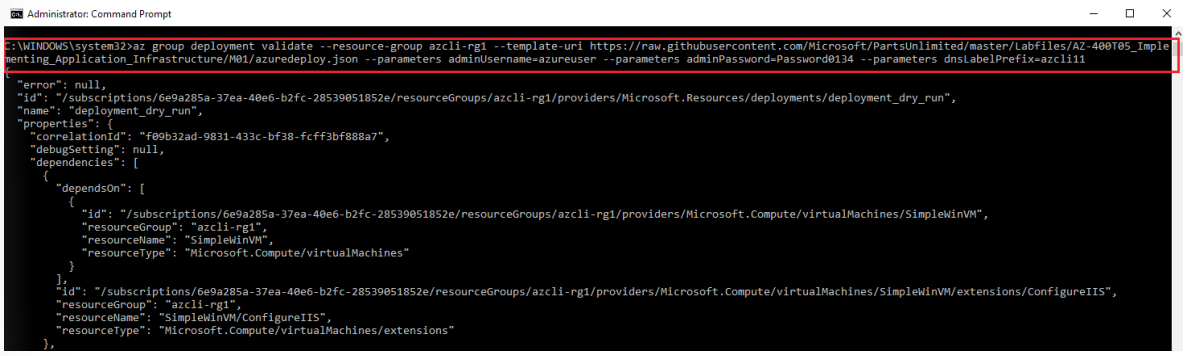
```
az group create --name < resource group name > --location < your nearest datacenter >
```

1.

2. 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**[69], and we will call the script using an Azure CLI command and some other parameters.

3. 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
```



4.

5. 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 \
  --parameters dnsLabelPrefix=$DNS_LABEL_PREFIX
```

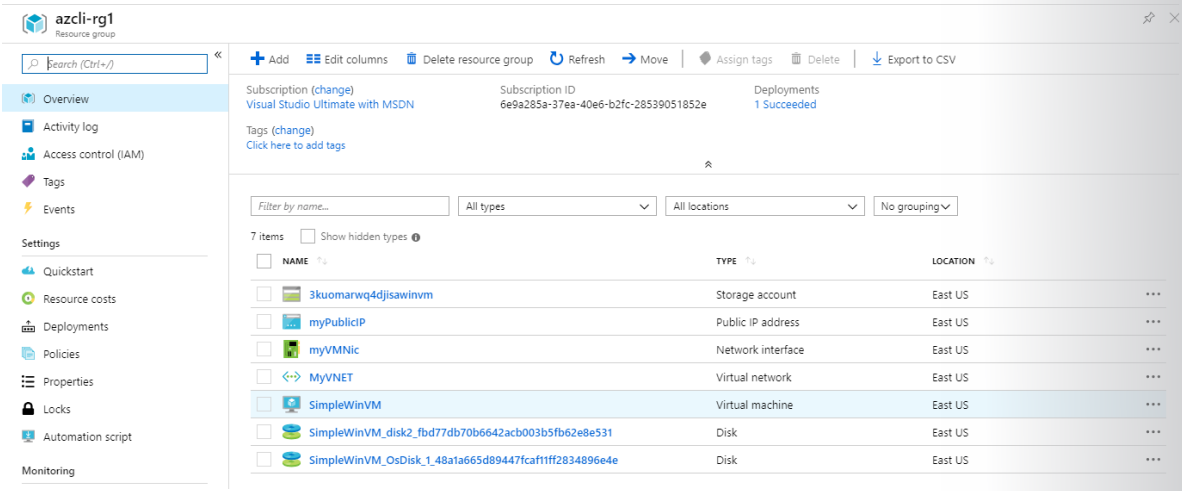
69 https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json

```
C:\WINDOWS\system32>az group deployment create --name MyDeployment --resource-group azcli-rg1 --template-uri https://raw.githubusercontent.com/Microsoft/PartsUnlimited/master/Labfil
es/AZ-400T05_Implementing_Application_Infrastructure/M01/azuredeploy.json --parameters adminUsername=azureuser --parameters adminPassword=Password0134 --parameters dnsLabelPrefix=az
cli11
- Running ..
```

6.

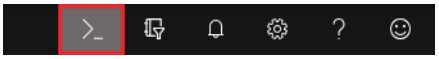
7. Verify the deployment by signing into the Azure portal at **https://portal.azure.com**[70]

8. 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*



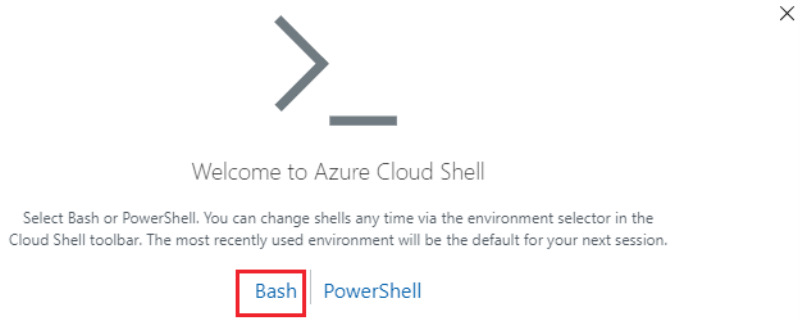
9.

10. 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.



11.

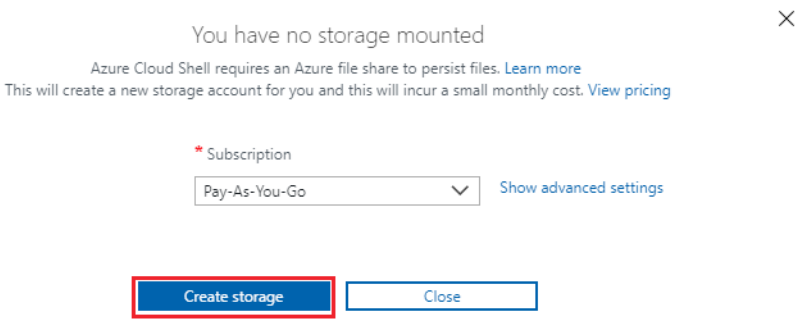
12. The browser becomes split and the Azure cloud Shell opens in the bottom half of your existing browser and you are prompted to select between **Bash** or **PowerShell**, select **Bash**



13.

14. 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 Clod Shell, it does this automatically for you.

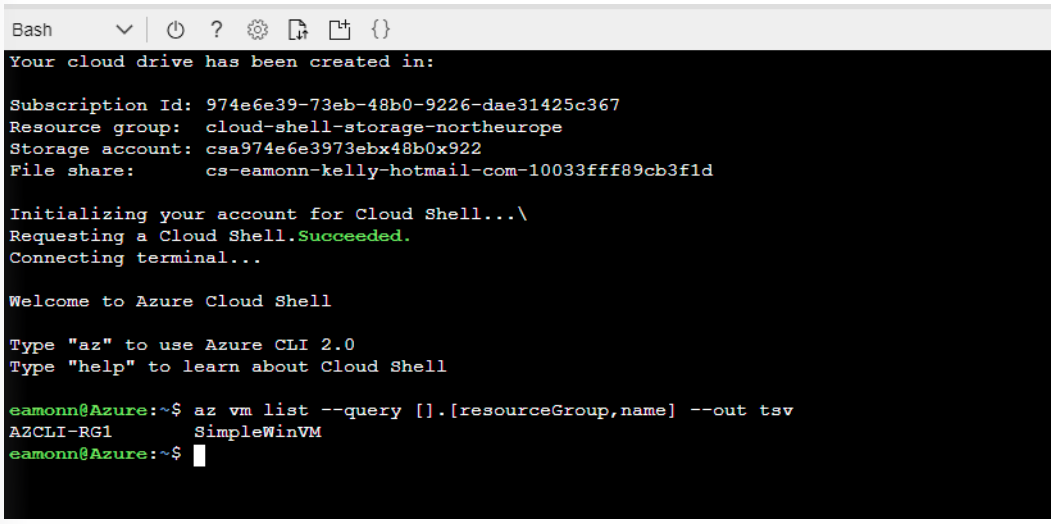
70 https://portal.azure.com



15.

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
```



17.

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.

Video: Azure Advisor

Azure Advisor

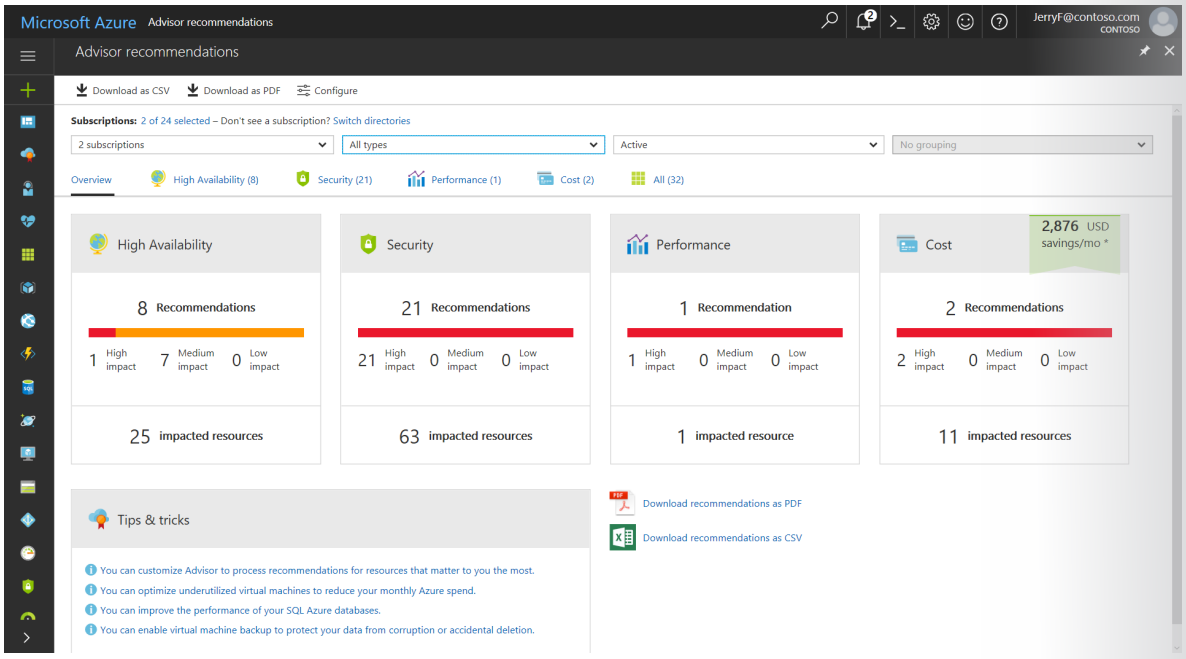
Azure Advisor is a free service built into Azure that provides recommendations on high availability, security, performance, and cost. Advisor analyzes your deployed services and looks for ways to improve your environment across those four areas.

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 Advisor**[71] page.

71 https://azure.microsoft.com/en-us/services/advisor/

Module 2 Review Questions

Core Azure Services Review Questions

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 10

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.

Module 3 Security, Privacy, Compliance and Trust

Learning Objectives

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

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 applica-

tions 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 Firewall**[1] page.

Azure DDoS Protection

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.

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

- *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 Protection**[2].

Network Security Groups (NSG)

Network Security Groups

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.

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.

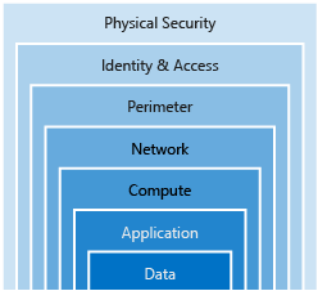
When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

Note: You can read more about NSGs on the **Security groups**[3] page.

2 https://azure.microsoft.com/en-us/services/ddos-protection/
3 https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups

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.

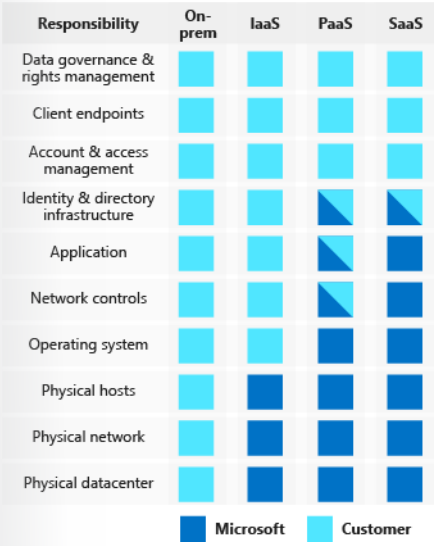
Combining services

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.



Core Azure Identity services

Video: Core Identity Services

Authentication and Authorization

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 Directory**[4] webpage.

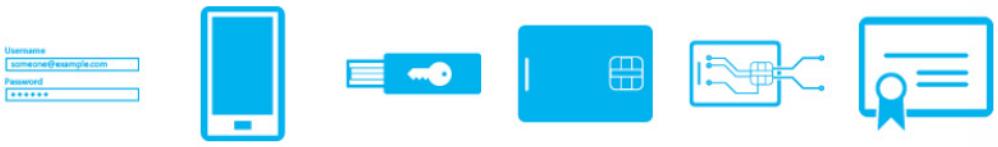
Azure Multi-Factor Authentication

Azure MFA

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.

4 https://azure.microsoft.com/en-us/services/active-directory/



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.

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** [5].

5 https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Security Tools and Features

Video: Video Azure Security Center

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**[6] (CIS) recommendations.

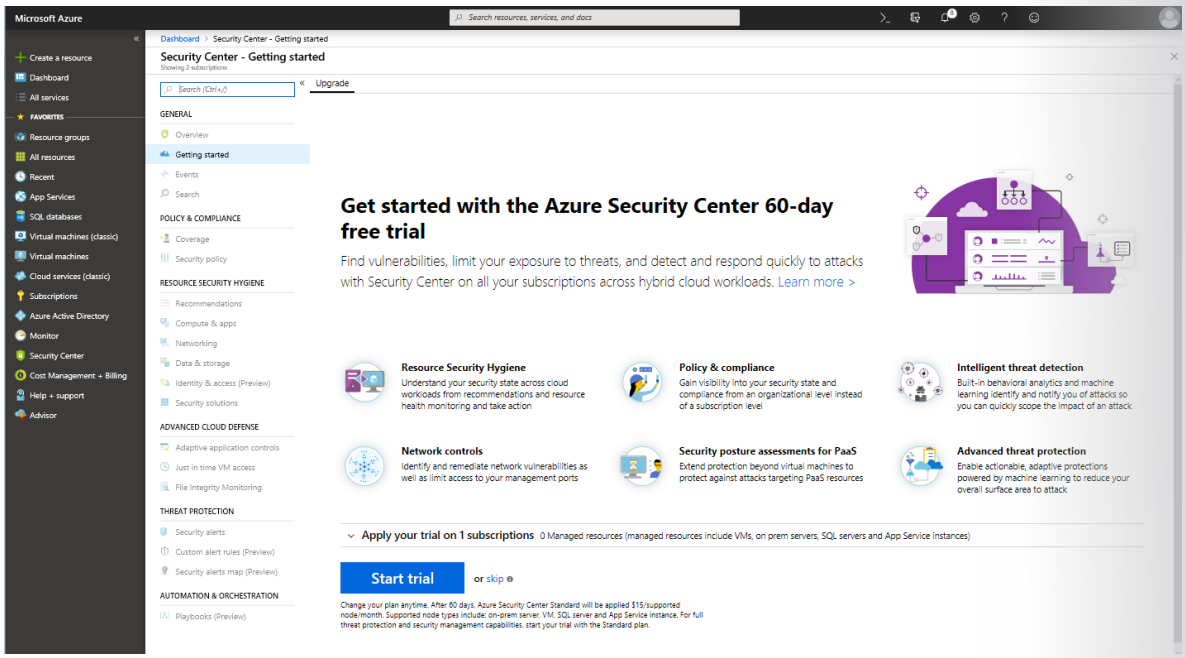
Azure Security Center Versions

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.

6 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 60-day free trial from within the Azure Security Center dashboard in the Azure Portal.



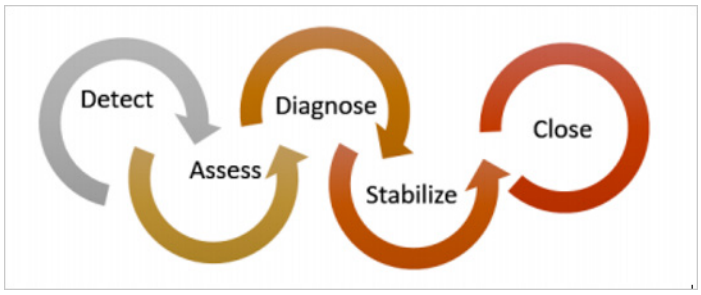
- To upgrade a subscription to the Standard tier, you must be assigned the role of *Subscription Owner*, *Subscription Contributor*, or *Security Admin*.
- After the 60-day trial period is over, Azure Security Center is $15 per node per month.

Note: You can read more about Azure Security Center at **Azure Security Center**[7].

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.
2. 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.



3.

7 https://azure.microsoft.com/en-us/services/security-center/

4. 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.
5. Use Security Center recommendations to enhance security.
6. 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.
7. 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.
8. 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 Center**[8]. More implementation and scenario detail is also available in the **Azure Security Center planning and operations guide**[9].

Video: Security Tools and Services

Key Vault

Azure 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.

8 https://azure.microsoft.com/en-us/services/security-center/
9 https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide

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** [10]webpage.

Azure Information Protection (AIP)

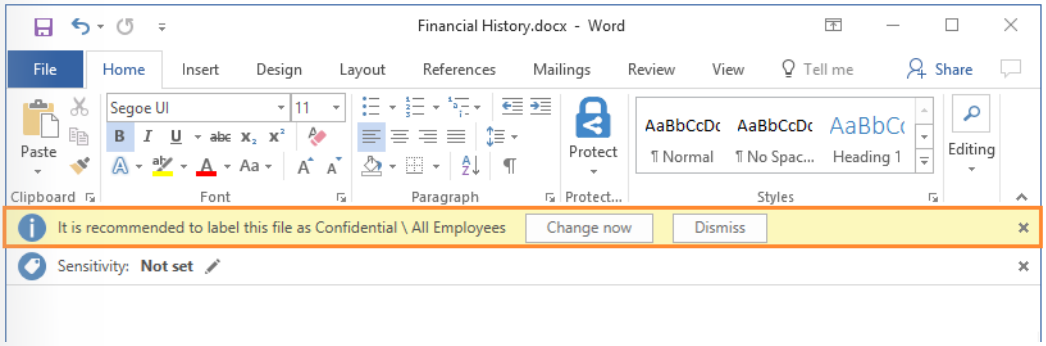
Azure Information Protection

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).

10 https://azure.microsoft.com/en-us/services/key-vault/

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 pricing**[11] webpage.

Note: You can read more about MSIP on the **What is Azure Information Protection?**[12] webpage.

Azure Advanced Threat Protection (ATP)

Azure Advanced Threat Protection

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.

11 https://azure.microsoft.com/en-us/pricing/details/information-protection/
12 https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection/

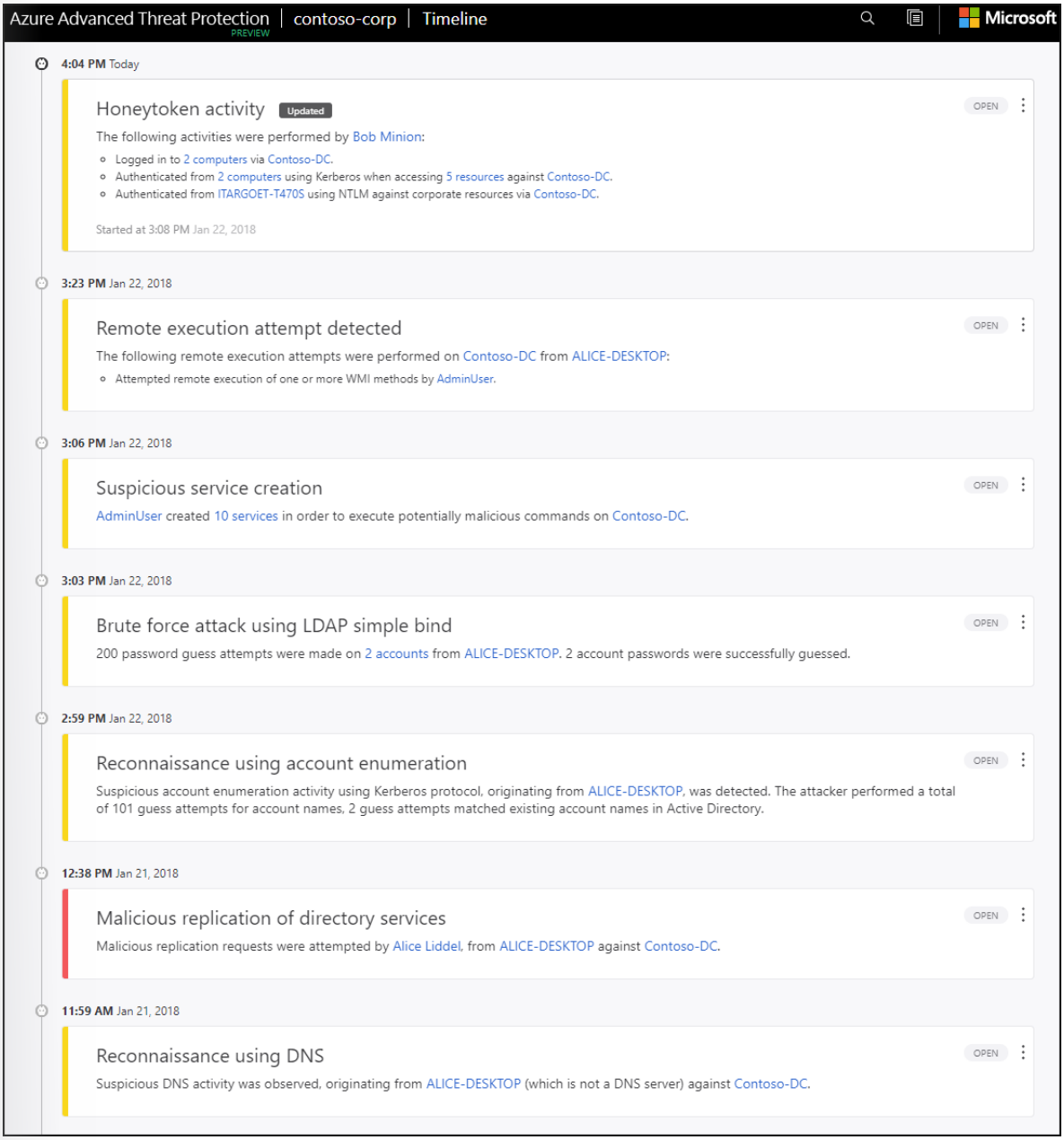
Azure ATP is capable of detecting known malicious attacks and techniques, security issues, and risks against your network.

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.com**[13]. 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.
- *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.

13 https://portal.atp.azure.com



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 page**[14], 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 Protection**[15]webpage.

14 https://www.microsoft.com/en-ie/cloud-platform/enterprise-mobility-security-pricing
15 https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/

Azure Governance methodologies

Video: Governance methodologies

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 Policy**[16] 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.
2. Assign a definition to a scope of resources.

16 https://azure.microsoft.com/en-us/services/azure-policy/

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.

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 Policy**[17] 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.

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.

17 https://azure.microsoft.com/en-us/services/azure-policy/

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.

Role-Based Access Control (RBAC)

Role-based access control

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.

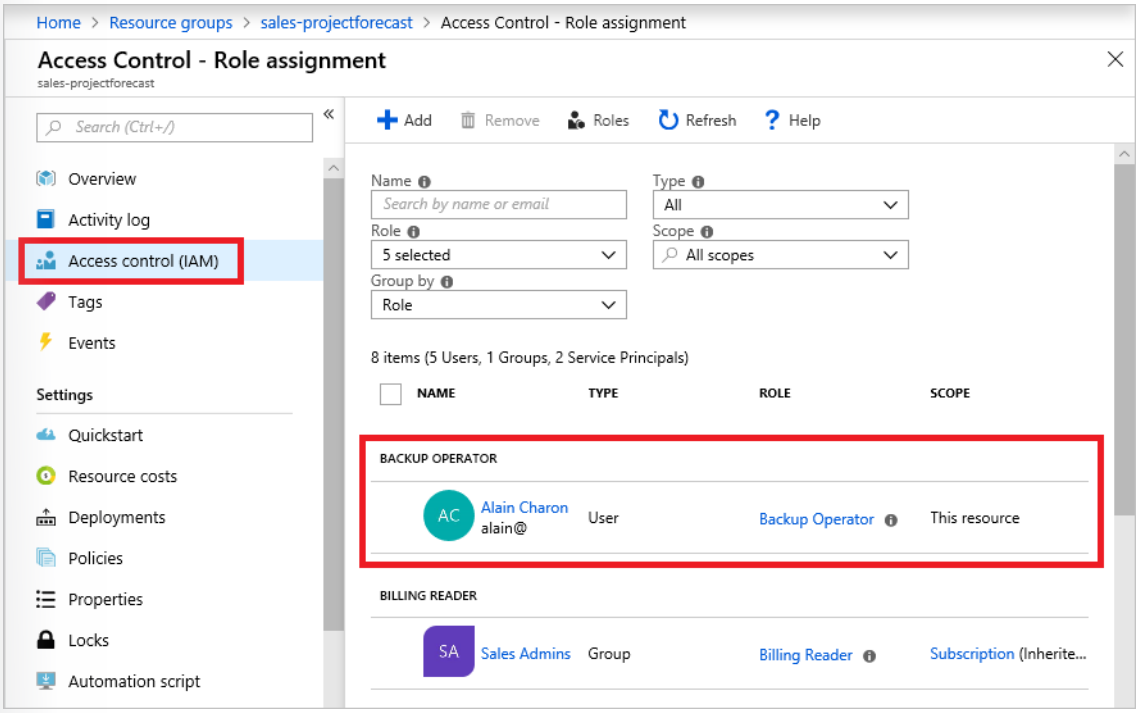
Usage Scenarios

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.



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)?**[18]

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.

18 https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

- **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.

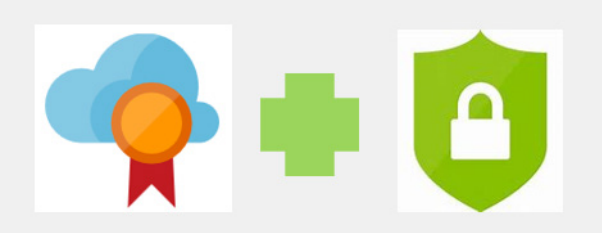
In the Azure portal, the locks are called **Delete* and *Read-only* respectively.

Note: You can read more about Locks at **Lock resources to prevent unexpected changes**[19].

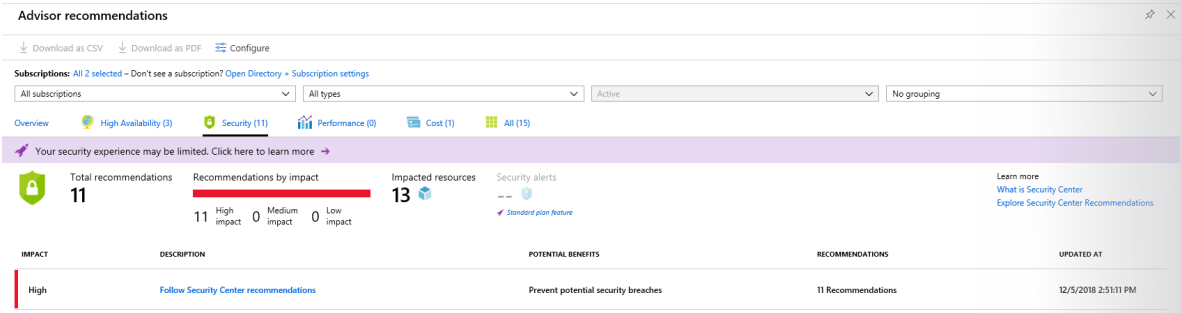
Azure Advisor security assistance

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.



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.

19 https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

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 Blueprints**[20].

20 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 constraints**[21].

21 https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits

Monitoring and Reporting in Azure

Video: Azure Monitor

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 Monitor**[22]

Video: Azure Service Health

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.

22 https://azure.microsoft.com/en-us/services/monitor/

- *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 Health**[23]webpage.

Monitoring Applications and Services

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.
- *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

23 https://azure.microsoft.com/en-us/features/service-health/

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

Compliance Terms and requirements

Compliance terms and requirements

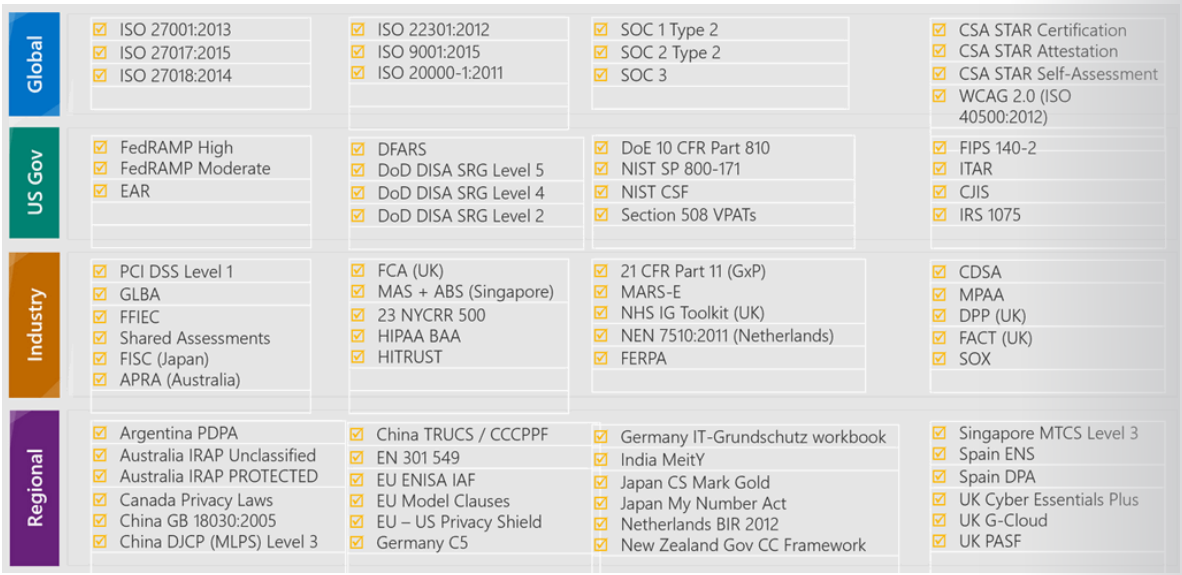
When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards. Some questions to ask about a potential provider include:

- 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.



Compliance Offerings:

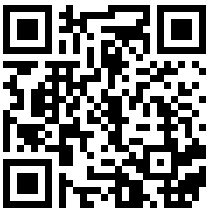
The following list provides details about *some* (but most definitely not all) of the compliance offerings available on Azure:

- *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.

- *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 Offerings**[24] webpage.

Video: Microsoft Privacy Statement



Microsoft Privacy Statement

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.

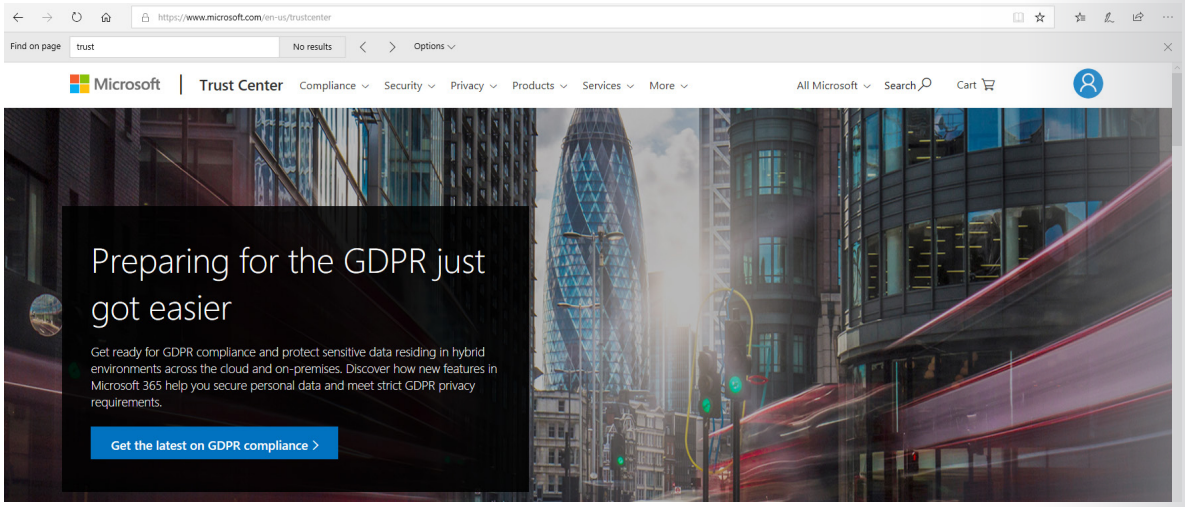
24 https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

Note: You can read the entire Microsoft Privacy Statement on the **Microsoft Privacy Statement**[25] webpage.

Video: Trust Center and Service Trust Portal

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** [26]webpage.

25 https://privacy.microsoft.com/en-us/privacystatement
26 https://www.microsoft.com/en-us/trustcenter

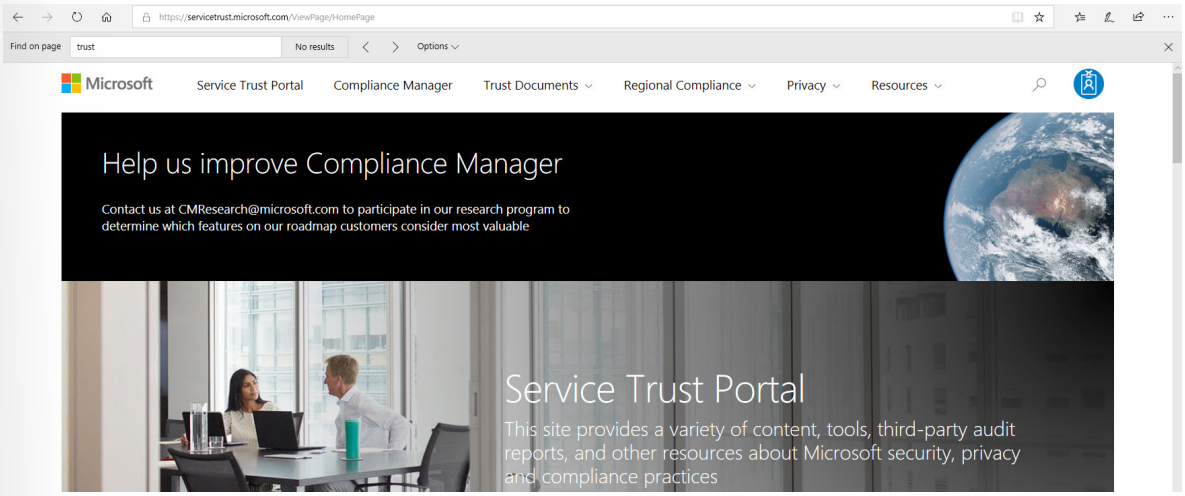
The Service Trust Portal

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. 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 can you 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 Portal**[27] webpage, with one of the following online subscriptions (trial or paid):

- Office 365
- Dynamics 365
- Azure

Video: Compliance Manager

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.

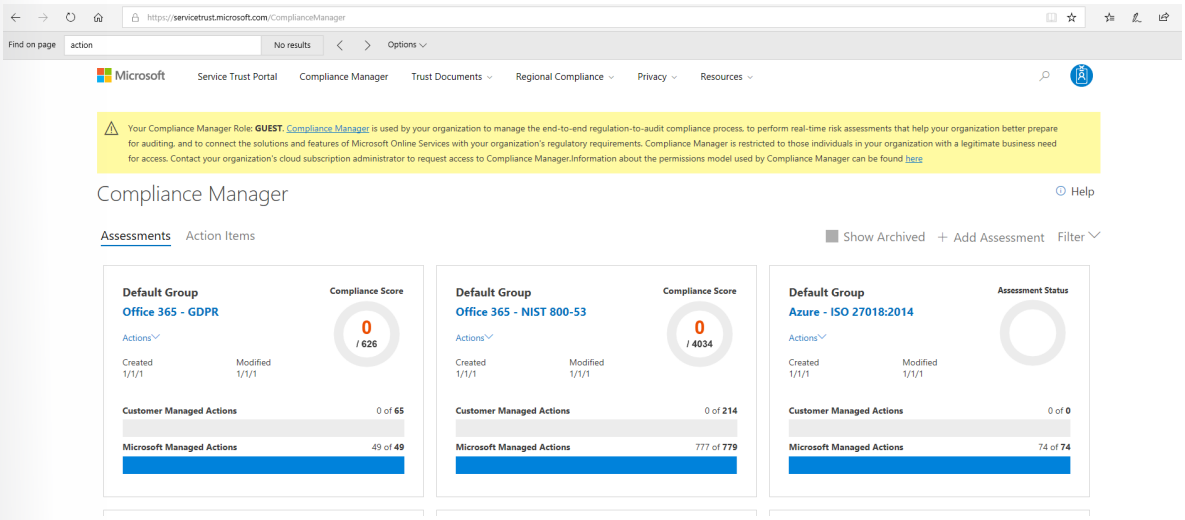
Compliance Manager provides the following features:

- 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.

27 https://aka.ms/STP



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.

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.**[28]

Note: You can read more about Azure Government on the **Azure Government**[29] 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 Germany**[30] 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.

28 https://docs.microsoft.com/en-us/azure/azure-government/compare-azure-government-global-azure
29 https://azure.microsoft.com/en-us/global-infrastructure/government/
30 https://azure.microsoft.com/en-us/global-infrastructure/germany/

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.

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 21Vianet**[31] webpage.

31 https://docs.microsoft.com/en-us/azure/china/

Module 3 Review Questions

Security, Privacy, Compliance and Trust Review Questions

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
- ☐ 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

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.

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.

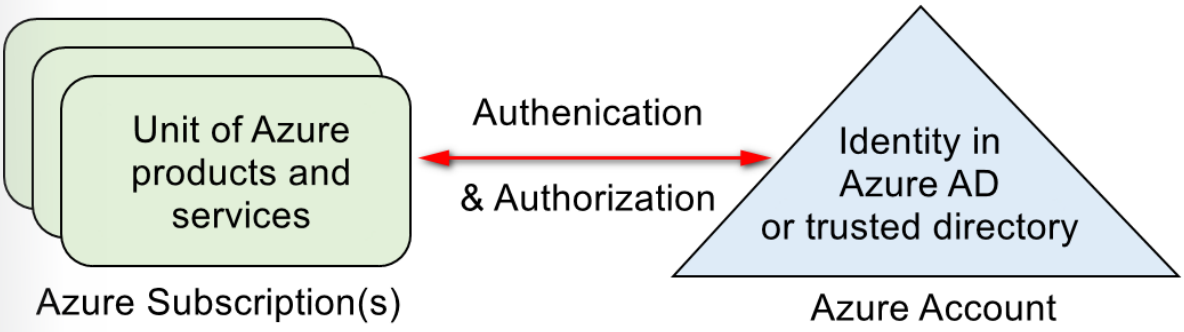
Azure Subscriptions

Video: Azure Subscriptions

Azure Subscriptions

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 Series**[1].

Subscription Uses and Options

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:

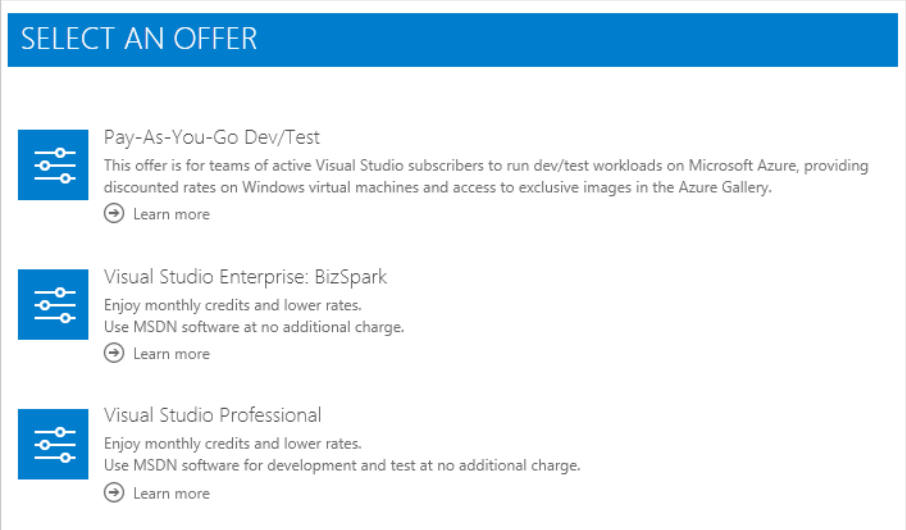
- *Billing boundary*. This subscription type determines how an Azure account is billed for using Azure. You can create multiple subscriptions for different types of billing requirements, and Azure will generate separate billing reports and invoices for each subscription so that you can organize and manage costs.

1 https://social.technet.microsoft.com/wiki/contents/articles/33800.azure-iaas-v2-arm-design-series-azure-subscriptions.aspx

- *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 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 **Azure Subscription Governance**[2].

Subscription options



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 Offers**[3].

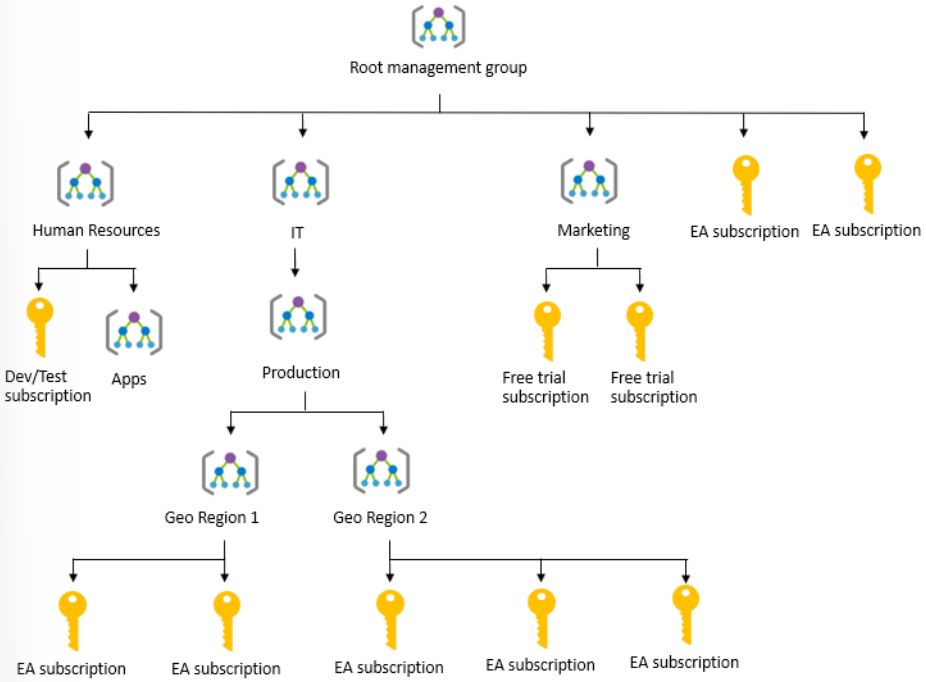
2 https://blogs.technet.microsoft.com/dsilva/2017/11/10/azure-subscription-governance-resource-group-and-naming-convention-strategies/

3 https://azure.microsoft.com/en-us/support/legal/offer-details/

Management Groups

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.



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 management**[4] and **Organize your resources with Azure management groups**[5].

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/

Planning and Managing costs

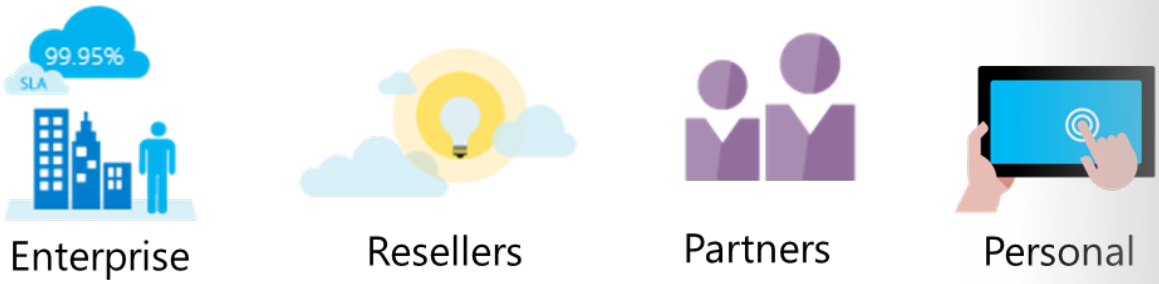
Video: Purchasing Options

Purchasing Azure Products and Services

Purchasing Azure products and services

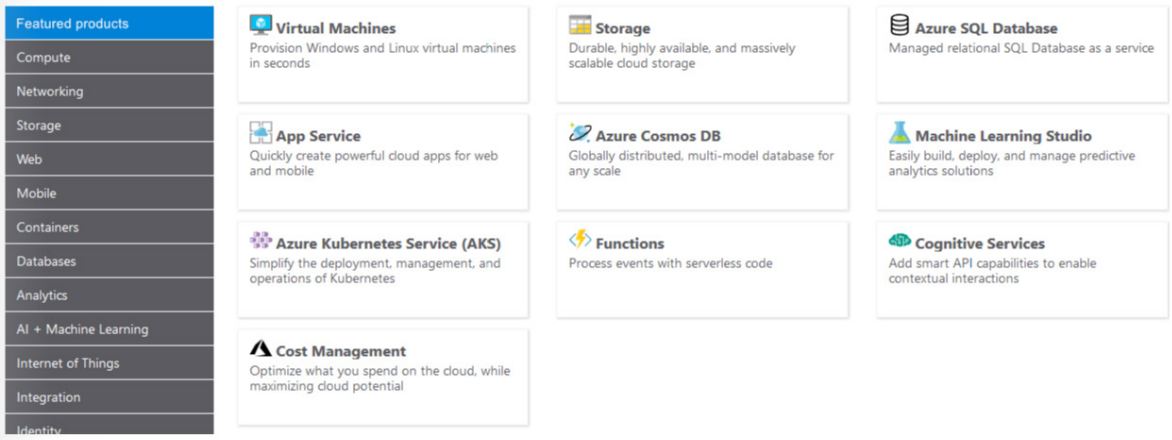
There are three main customer types on which the available purchasing options for Azure products and services is contingent, including:

- *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**[6]. 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.



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.

6 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

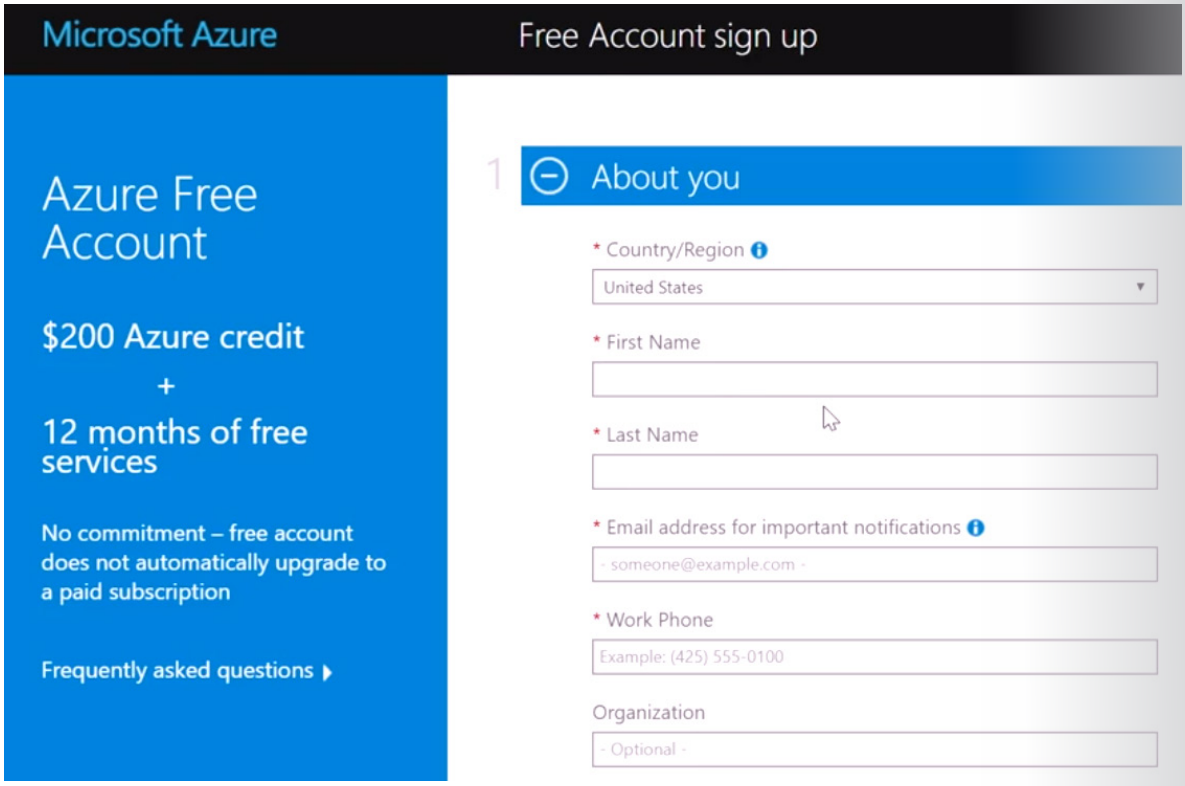
Note: For more information about purchasing Azure products and services, refer to **Explore flexible purchasing options for Azure**[7].

Azure Free Account

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.

7 https://azure.microsoft.com/en-us/pricing/purchase-options/



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 today**[8].

Video-Factors Affecting Costs

Factors Affecting Costs

Factors affecting costs

The following sections describe the main factors that affect Azure costs, including resource type, services, and the user's location.

8 https://azure.microsoft.com/en-us/free/

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.

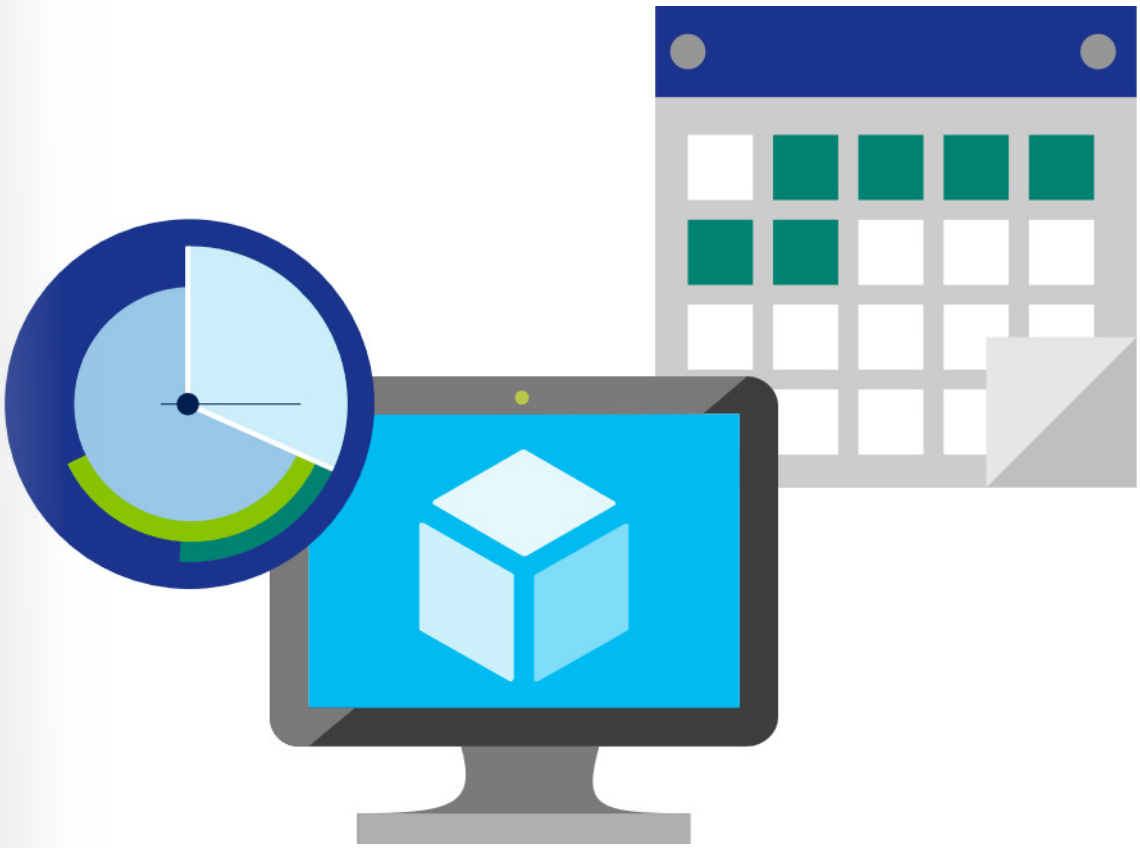
Note: Each meter tracks a *particular kind of usage*. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits-per-second), number of operations, size (storage capacity in bytes), or similar items.

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 marketplace**[9]. 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.

9 https://azuremarketplace.microsoft.com

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 invoice**[10].

Zones for Billing Purposes

Azure billing zones

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**.

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 Details**[11].

Video: Planning Costs

10 https://docs.microsoft.com/en-us/azure/billing/billing-understand-your-invoice
11 https://azure.microsoft.com/en-us/pricing/details/bandwidth/

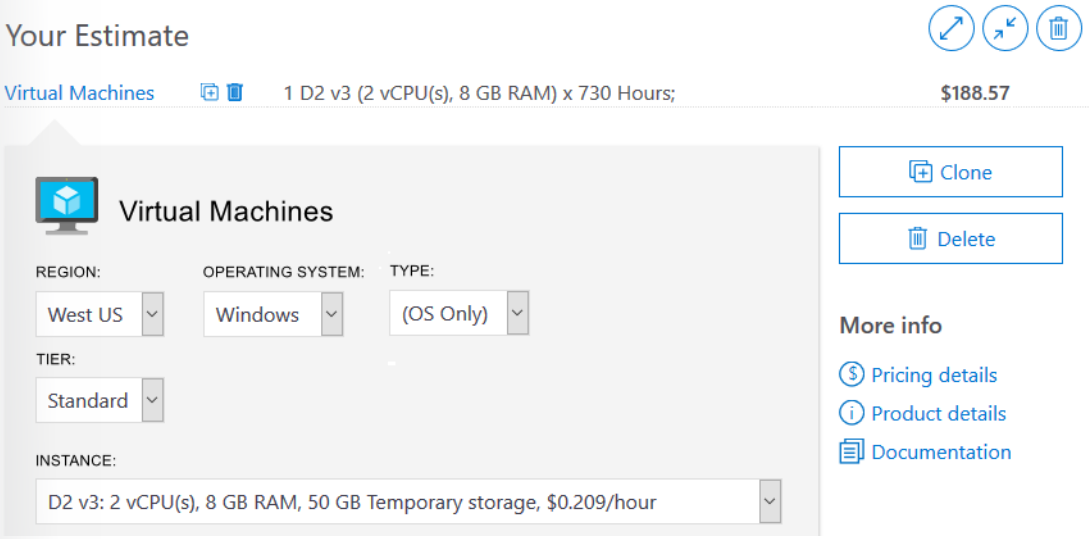
Pricing Calculator

The pricing calculator tool

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.



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 Calculator**[12].

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.
- *Networking*. Enter the amount of network bandwidth you currently consume in your on-premises environment.

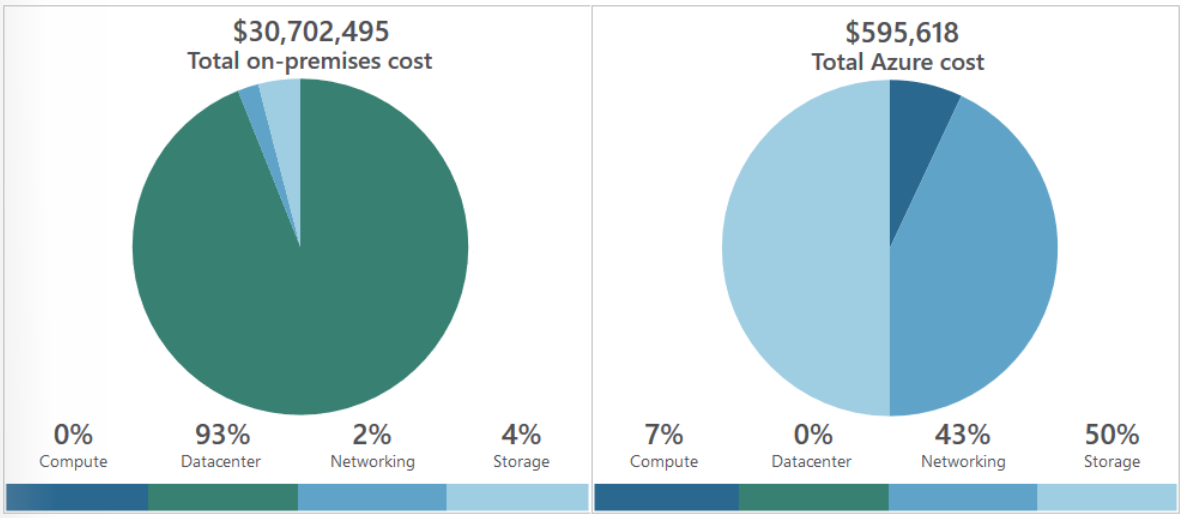
Step 2: Adjust assumptions

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

12 https://azure.microsoft.com/en-us/pricing/calculator/

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) Calculator**[13].

Video: Minimizing Costs

Minimizing Costs

Minimizing costs

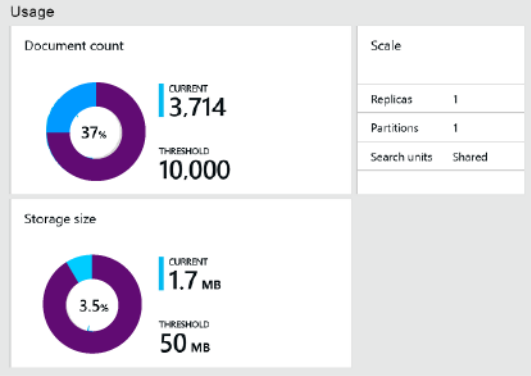
The following best practice guidelines can help minimize your Azure costs.

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.

13 https://azure.microsoft.com/en-us/pricing/tco/

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 Advisor**[14].

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 it**[15].

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 constraints**[16].

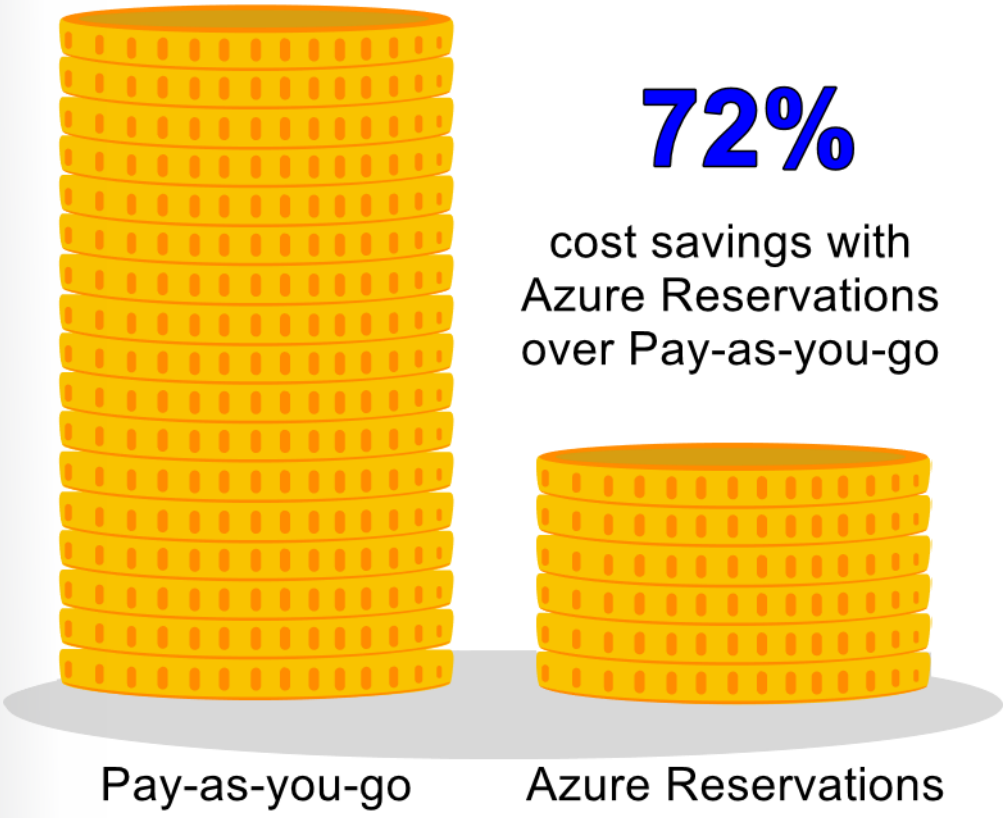
Use Azure Reservations

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?**[17]

14 https://azure.microsoft.com/en-us/services/advisor/
15 https://docs.microsoft.com/en-us/azure/billing/billing-spending-limit/
16 https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits/
17 https://docs.microsoft.com/en-us/azure/billing/billing-save-compute-costs-reservations



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.

Go to the **Azure Updates page**[18] 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

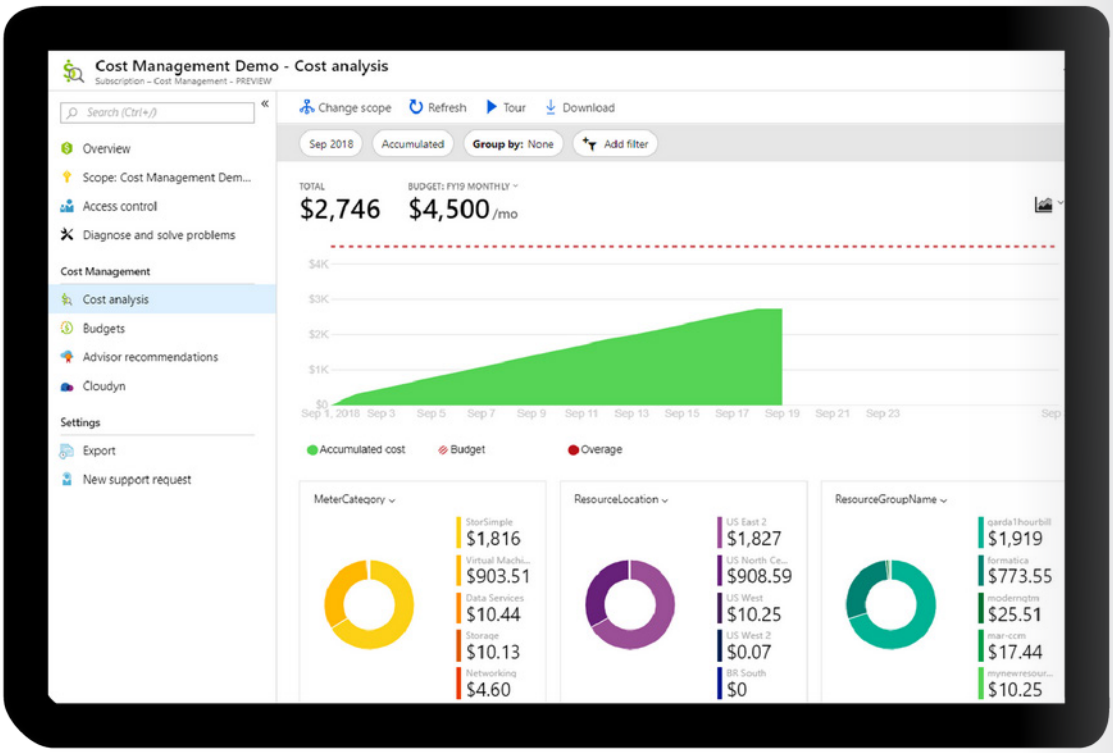
18 https://azure.microsoft.com/en-us/updates/

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 resources**[19].

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.
- *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.

19 https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

Note: For more information about Cost Management, refer to **Cost Management**[20].

20 https://azure.microsoft.com/en-us/services/cost-management/

Support Options Available with Azure

Video: Support Plan Options

Support Plan Options

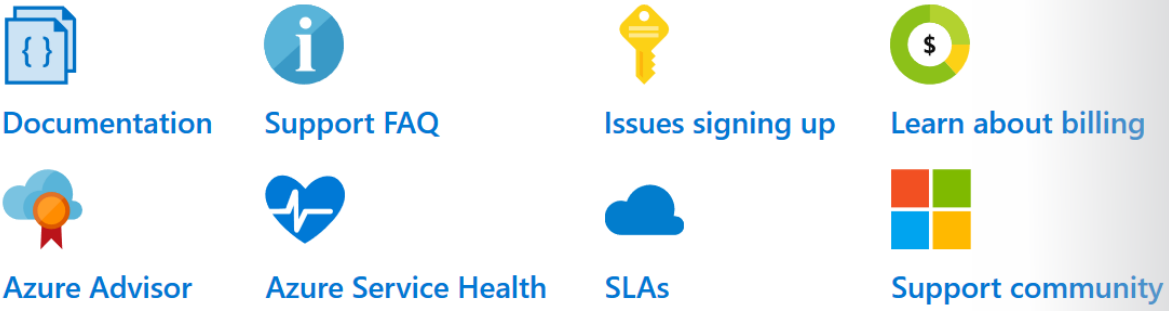
Support plan options

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.



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

	Developer	Standard	Professional Direct	Premier
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
Case Severity/ Response Times	Minimal business impact (Sev C): <8 business hours1	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 plans**[21].

21 https://azure.microsoft.com/en-us/support/plans/

Video: Accessing Support

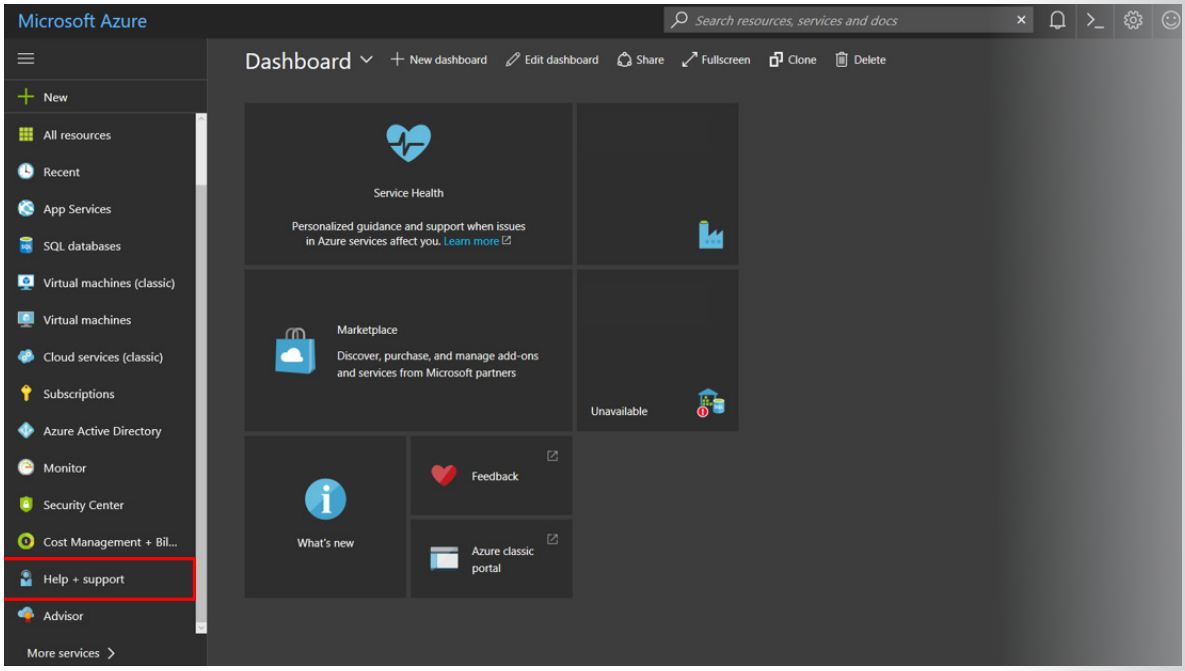
How to Open a Support Ticket

Opening a support ticket

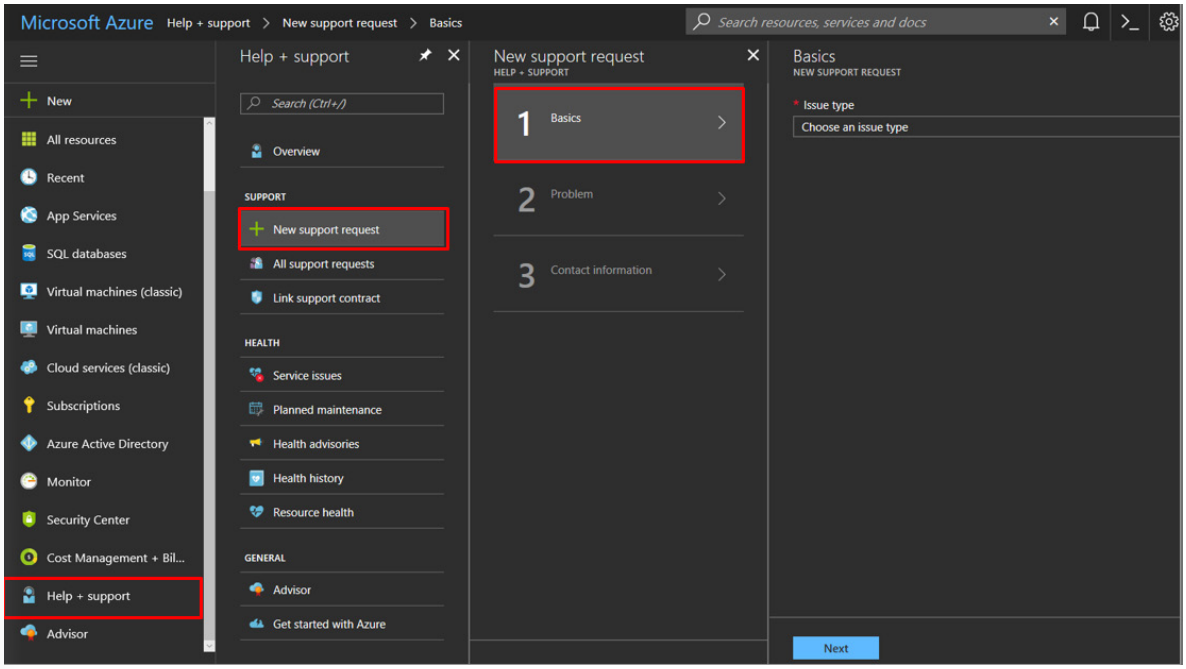
If you have an issue with Azure, you can request assistance from the Azure support team by creating a new *support ticket*.

Create a support ticket

1. Log into the Azure portal.
2. Choose **Help + support** from the left navigation menu, to open the **Help + Support** blade:



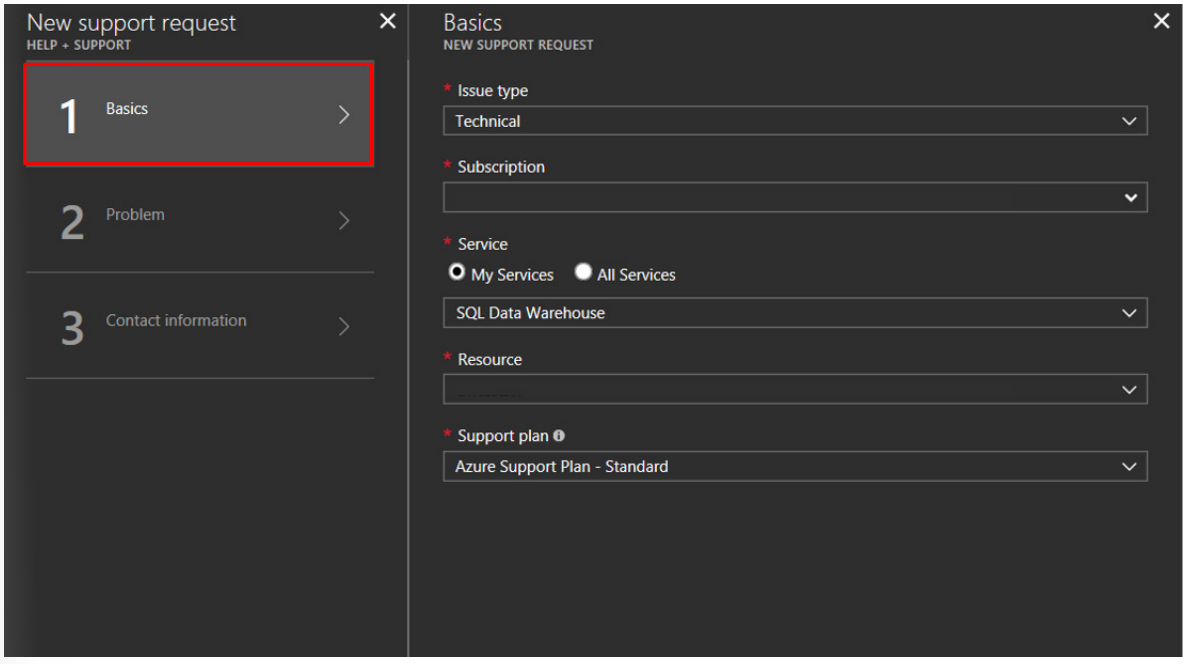
3.
4. On the **Help + Support** blade, select **New support request**:



5.

6. Fill out the **Basics** section of the support request form:

7. Enter the required information by using the provided dropdown lists and check box selectors:

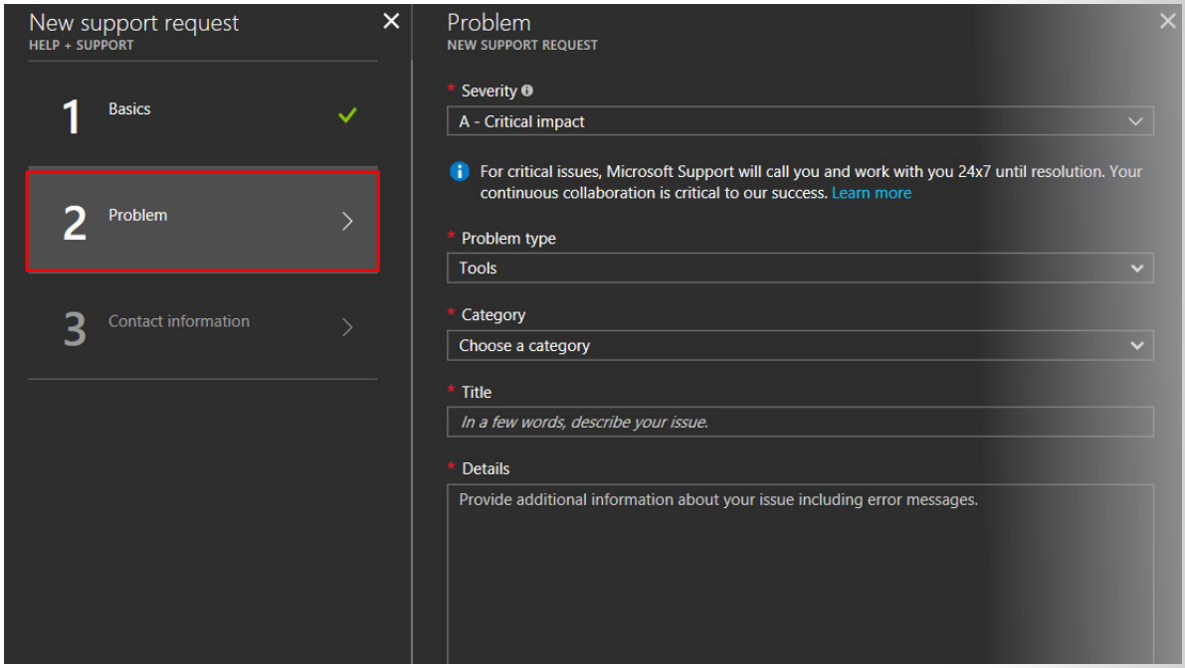


8.

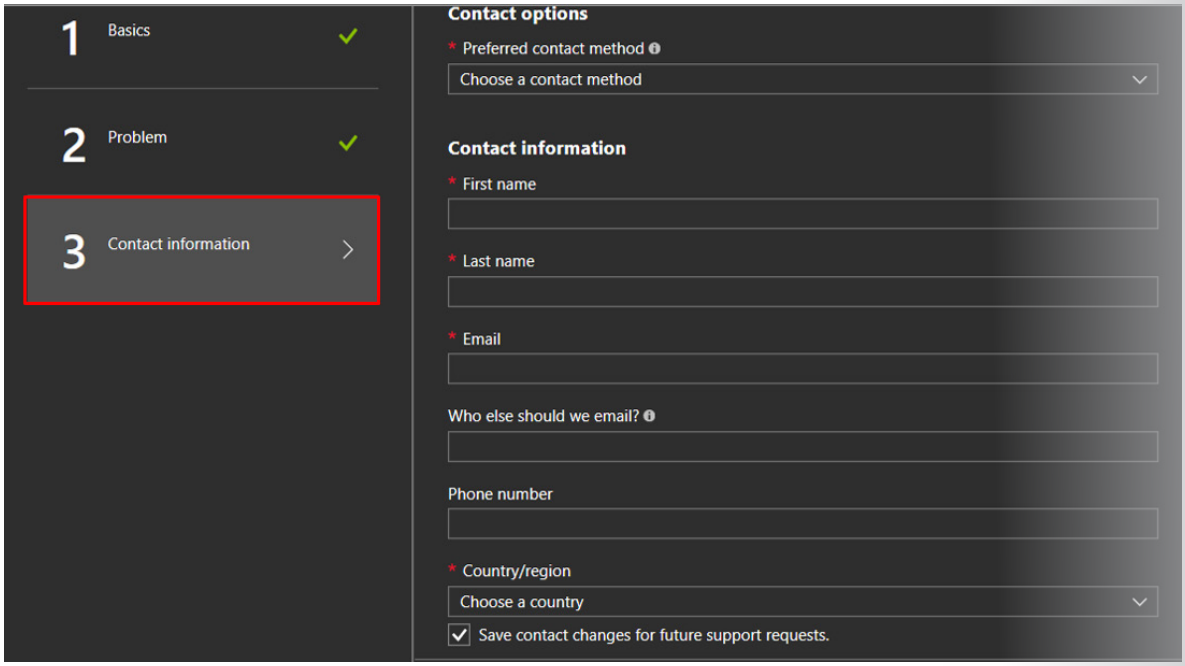
Note: All Azure customers can access billing, quota, and subscription-management support. *The availability of support for other issues depends on the support plan you have*.

1. Complete the **Problem** section of the form by using the provided dropdown lists and text-entry fields:

2. In the **Title** text-entry field, describe your issue briefly. Provide additional information about your issue in the **Details** text-entry field.

3. 

4. Provide your contact information by choosing your **preferred contact method** and entering your contact details, as prompted by the form:

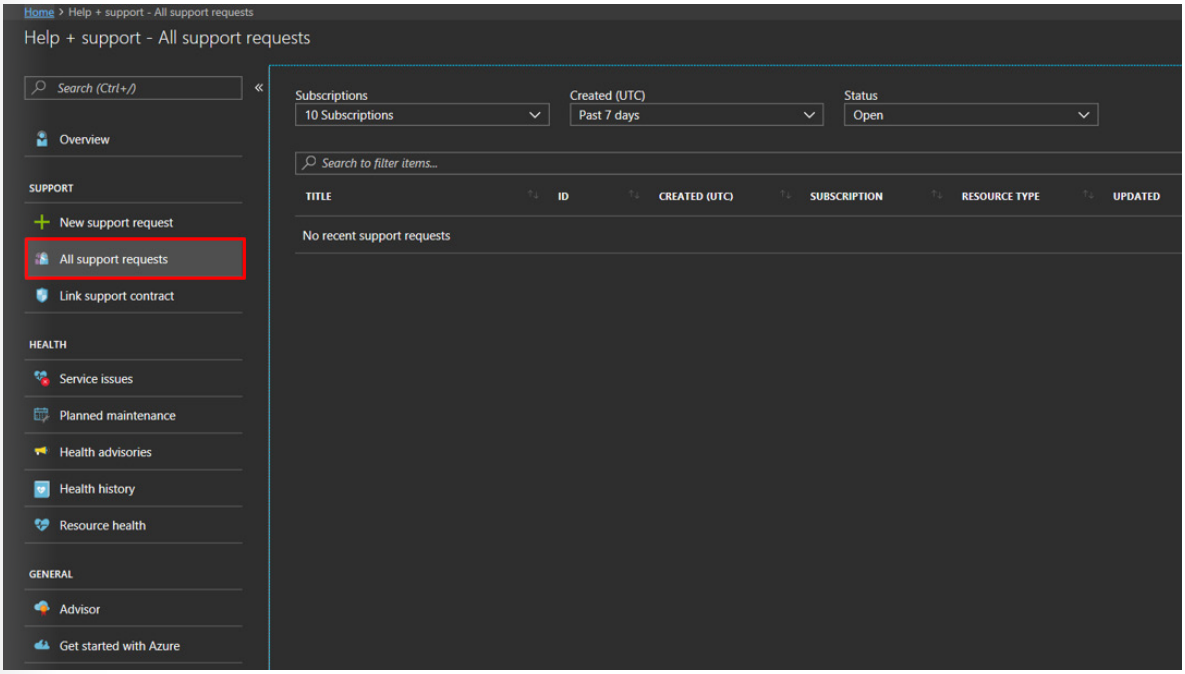
5. 

6. Select **Create** to submit your support request:

7. The Azure support team will contact you after you submit your request.

Monitor a support ticket

To check the status and details of your support request, choose **All support requests** from the **Help + support** blade:



Note: For more information about creating an Azure support ticket, refer to **Create a support ticket**[22] and **How to create a support ticket for SQL Data Warehouse**[23].

Alternative Support Channels

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 forums**[24].

22 https://azure.microsoft.com/en-us/support/create-ticket/
23 https://docs.microsoft.com/en-us/azure/sql-data-warehouse/sql-data-warehouse-get-started-create-support-ticket
24 https://social.msdn.microsoft.com/Forums/en-US/home?category=windowsazureplatform

Stack Overflow

You can review answers to questions from the development community on **StackOverFlow**[25].

Server Fault

Review community responses to questions about System and Network Administration in Azure on **ServerFault**[26].

Azure Feedback Forums

Read ideas and suggestions for improving Azure made by Azure users and customers on the **Azure Feedback Forums**[27].

Twitter

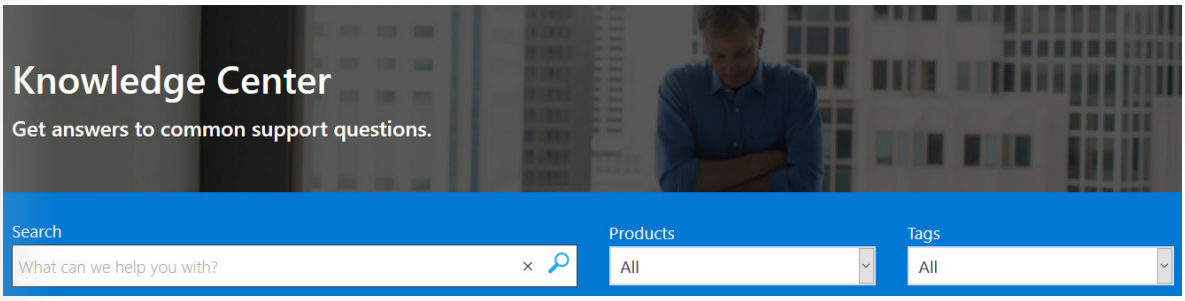
25 https://stackoverflow.com/questions/tagged/azure/
26 https://serverfault.com/questions/tagged/azure
27 https://feedback.azure.com/forums/34192--general-feedback

Tweet `@AzureSupport` to get answers and support from the **official Microsoft Azure Twitter channel**[28].

Note: For more information about alternative Azure support channels, refer to **Azure Community Support**[29].

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.



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 Center**[30].

28 https://twitter.com/azuresupport
29 https://azure.microsoft.com/en-us/support/community/
30 https://azure.microsoft.com/en-us/resources/knowledge-center/

Azure Service Level Agreements (SLAs)

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.

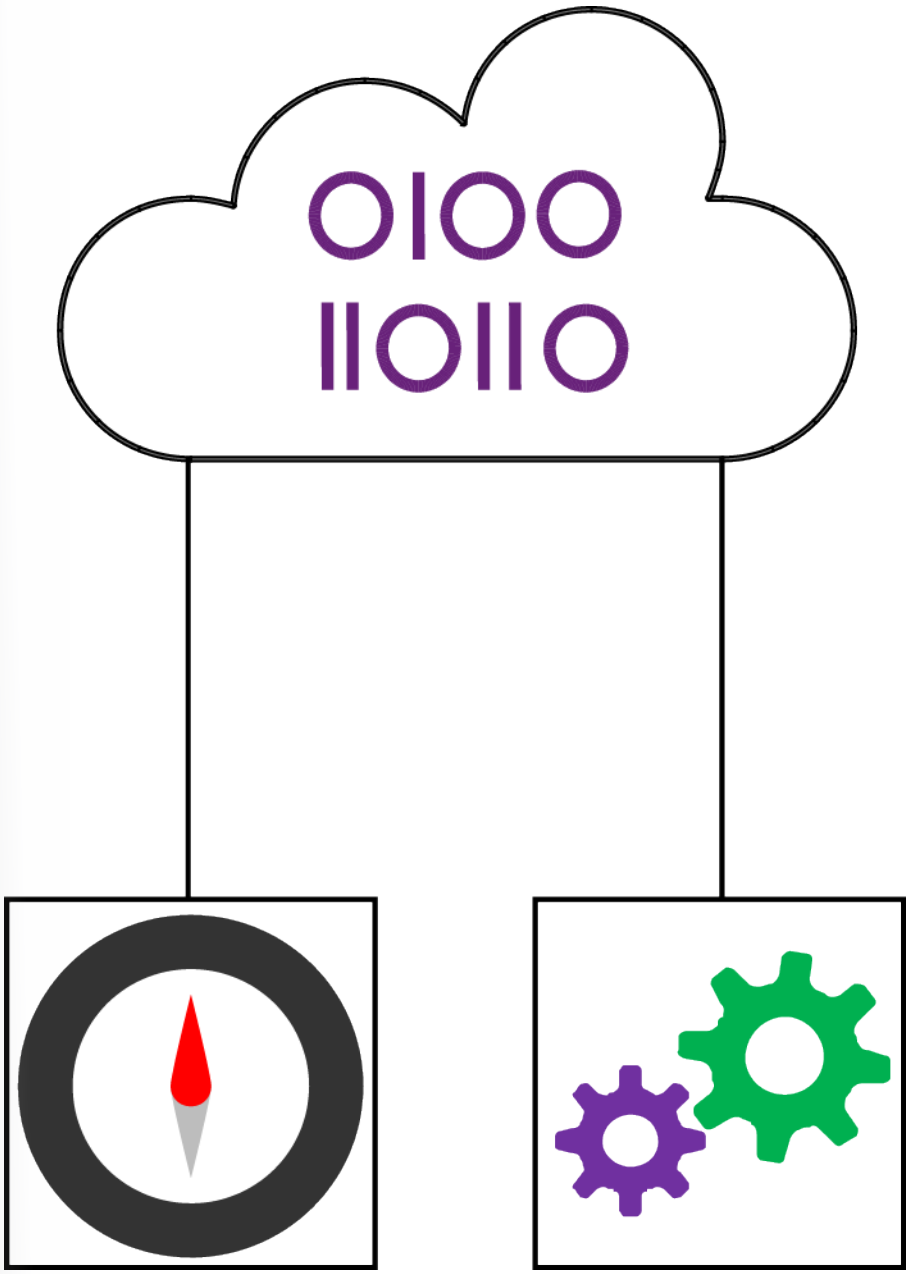
- SLAs describe Microsoft's commitment to providing Azure customers with certain performance standards.
- There are SLAs for individual Azure products and services.
- SLAs also specify what happens if a service or product fails to perform to a governing SLA's specification.

SLAs for Azure Products or Services

SLAs for Azure products and services

There are three key characteristics of SLAs for Azure products and services, which the following sections detail.

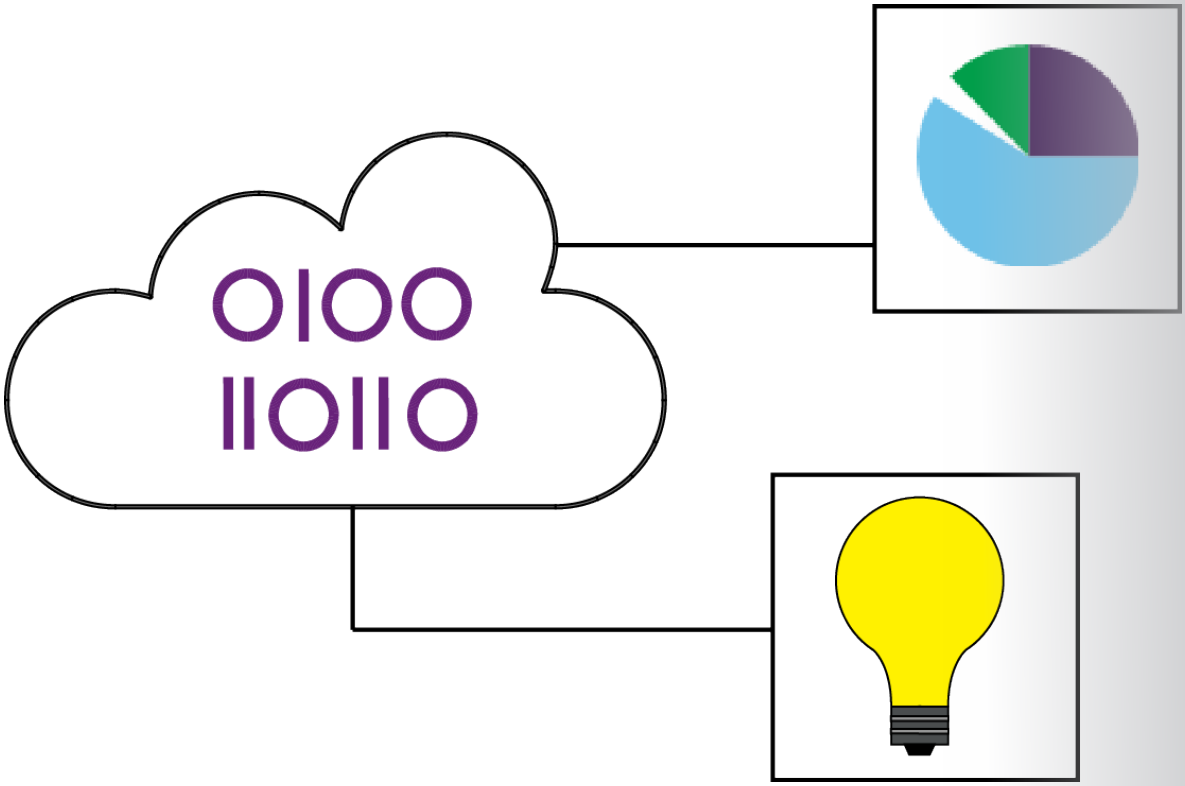
1. **Performance Targets, Uptime and Connectivity Guarantees**
2. A SLA defines performance targets for an Azure product or service. The performance targets that a SLA defines are specific to each Azure product and service.
3. For example, performance targets for some Azure services are expressed in terms of uptime or connectivity rates.

4. 

5. **Performance targets range from 99.9 percent to 99.99 percent**

6. A typical SLA specifics 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.

7. 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.



8.

9. **Service Credits**

10. SLAs also describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLA's specification.

11. 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.

12. 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 Agreements**[31].

31 https://azure.microsoft.com/en-us/support/legal/sla/summary/

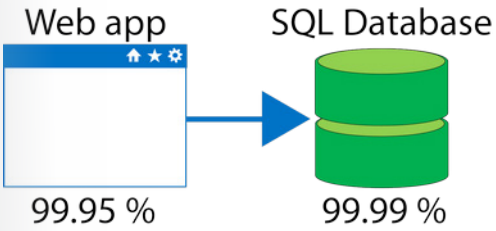
Compsoite SLA's

Composite SLAs

When combining SLAs across different service offerings, the resultant SLA is a 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:

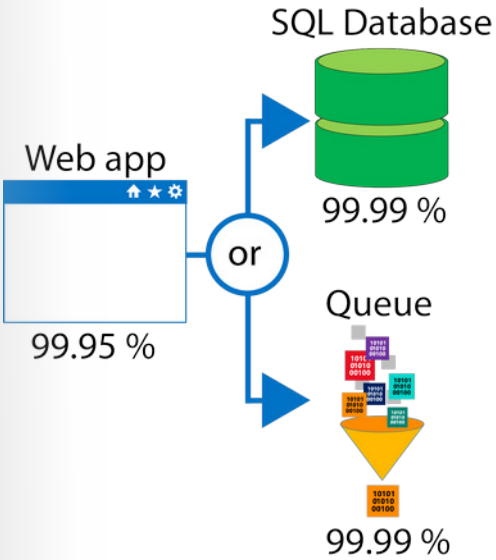
- App Service Web Apps is 99.95 percent.
- SQL Database is 99.99 percent.



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: `99.9 percent × 99.99 percent = 99.94 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.



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 database *and* the queue fail simultaneously. If the expected percentage of time for a simultaneous failure is `0.0001 × 0.001`, the composite SLA for this combined path would be:

Database *OR* queue = `1.0 – (0.0001 × 0.001) = 99.99999 percent`

Therefore, the total composite SLA is:

Web app *AND* database *OR* queue = `99.95 percent × 99.99999 percent = ~99.95 percent`

However, there are tradeoffs to using this approach. The application logic is more complex, you are paying for the queue, and there may be data-consistency issues.

Improving Application SLAs

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

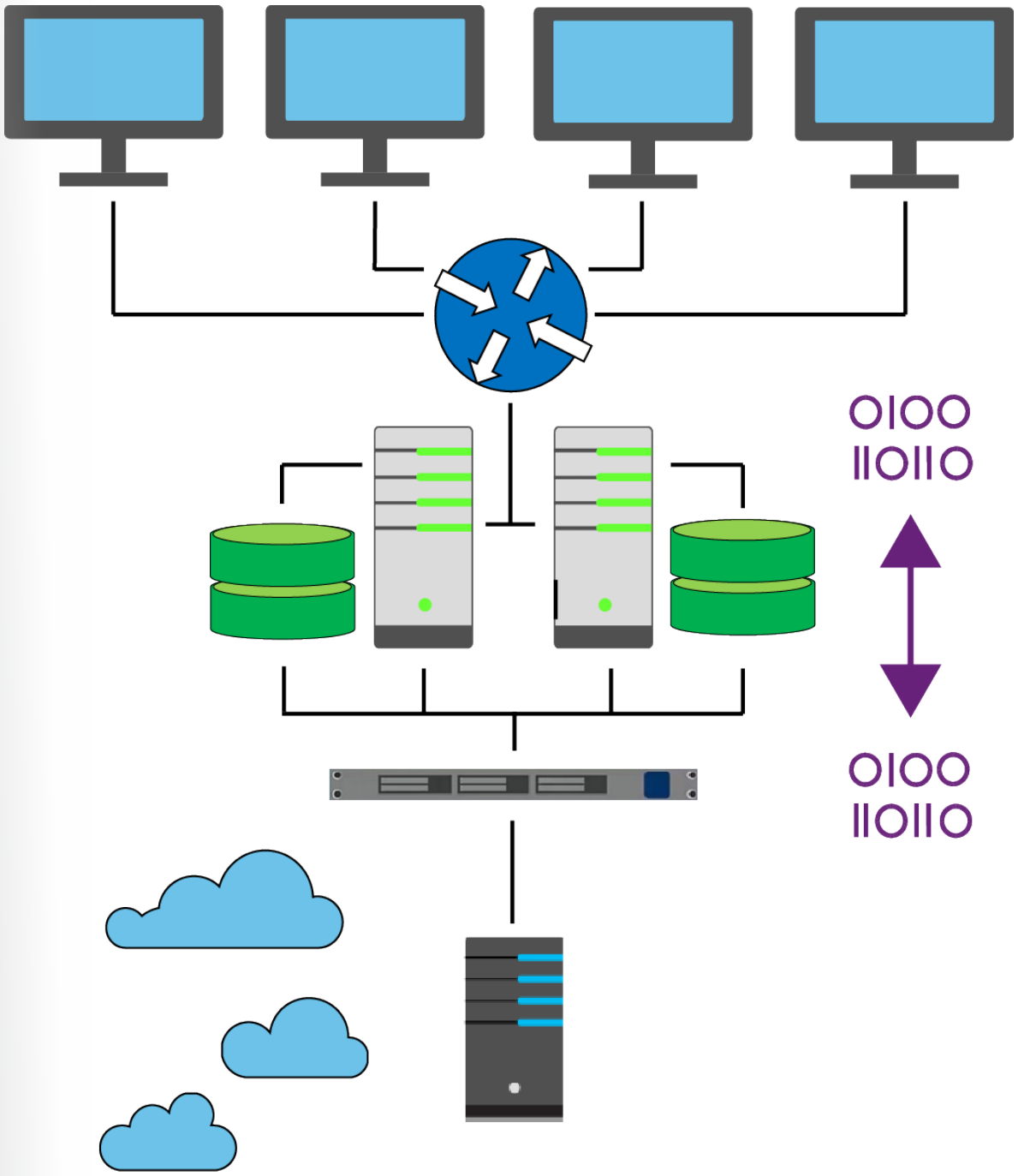
Resiliency is the ability of a system to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss. The goal of resiliency is to return the application to a fully functioning state following a failure. High 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**[32].

32 https://docs.microsoft.com/en-us/azure/architecture/resiliency/

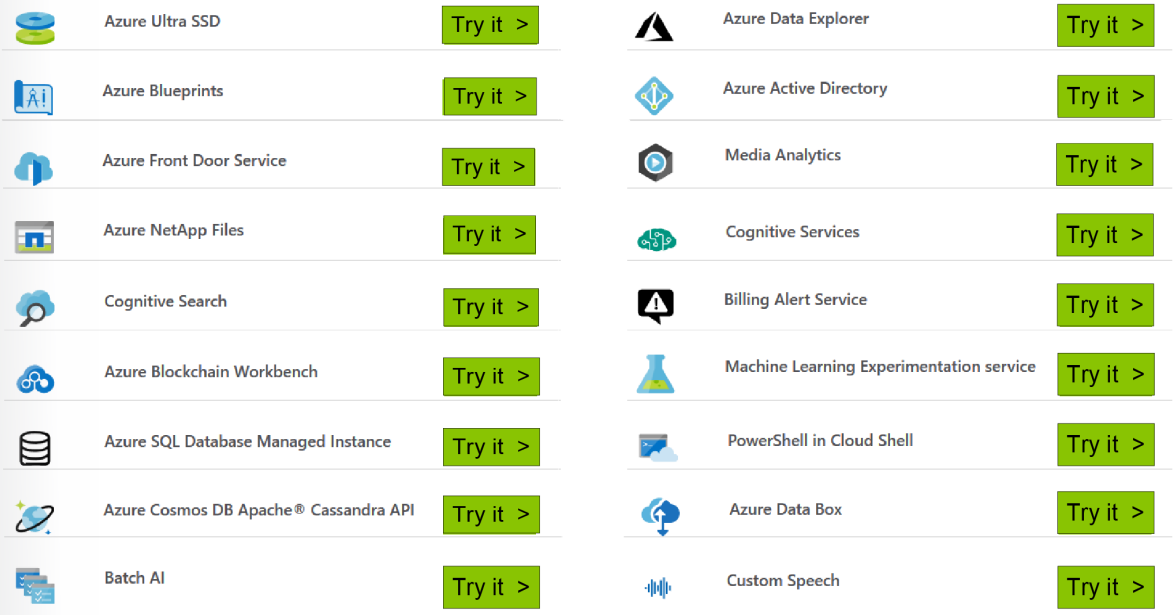
Service Lifecycle in Azure

Video: Feature Release and Access

Public and Private Preview Features

Public and private preview features

Microsoft offer previews of Azure features for evaluation purposes. With *Azure Preview Features*, you can test beta and other prerelease features, products, services, software, and regions. Providing feedback on the features you preview also helps Microsoft improve Azure.



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*.

Feature preview categories

The following describes the two types of Azure preview modes:

- *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.

Note: For more information about Azure Previews, refer to **Preview features**[33].

How to Access Preview Features

How to access preview features

Go to the Azure **Preview Features**[34] page to review a list of preview features that are available for evaluation. To preview a feature, select the **Try it** button for the applicable feature. Additionally, you can find out more information about an Azure preview feature before you try it by choosing **Learn more**.

To see which preview features you are using:

- Sign in to Azure portal
- Open the **New** blade.
- Enter the word *preview*.
- This displays a list of available preview features, with the word **enabled** next to each preview feature that you turn on.
- Choose **disable** to turn off a preview feature.

Portal preview features

You can access preview features that are specific to the Azure Portal from the **Portal Preview Features**[35] page. Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

33 https://azure.microsoft.com/en-us/services/preview/
34 https://azure.microsoft.com/en-us/services/preview/
35 https://preview.portal.azure.com

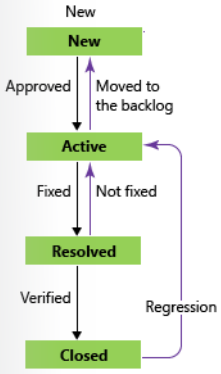
Azure customers can provide feedback on the portal preview features they've tested by *sending a smile* in the portal or by posting ideas and suggestions on the *Azure Portal Feedback Forum*. You can revert to the default Azure portal by going to the **Standard Portal**[36] page.

Note: For more information about Azure portal preview features, refer to **Get early access to the newest Azure portal features**[37].

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*.



The above image outlines the general progress and process for features and bugs during product and feature development lifecycle.

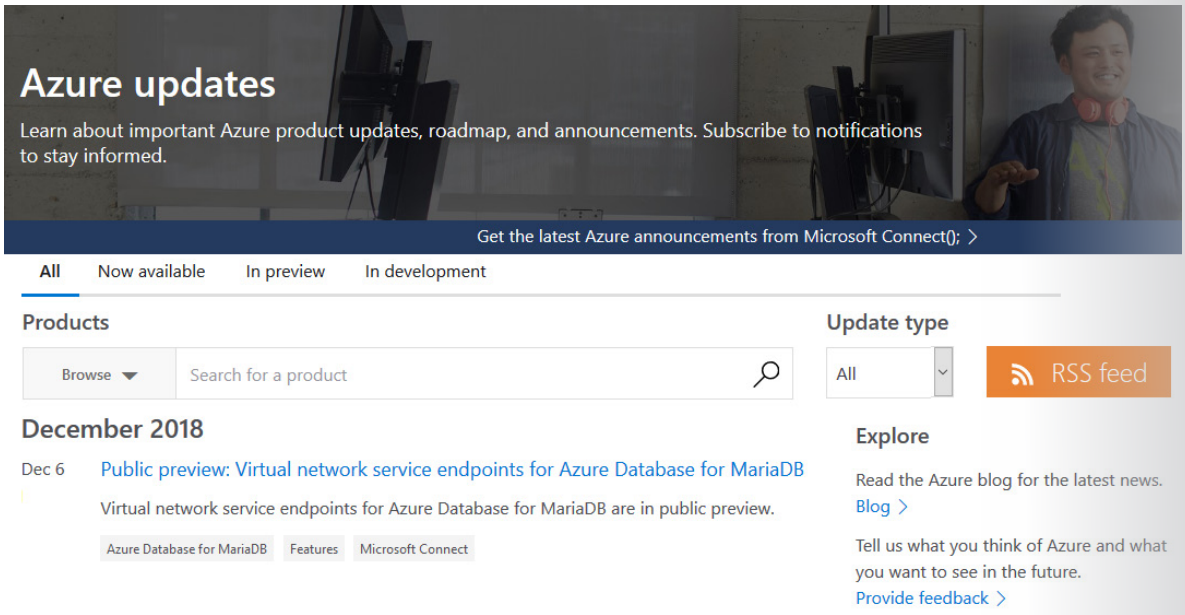
Note: It's common for features to move from Azure preview features to GA, based on customer evaluation and feedback.

36 https://portal.azure.com
37 https://azure.microsoft.com/en-us/updates/get-early-access-to-new-portal-features-2/

Monitoring Feature Updates

Monitoring feature updates

Go to the **Azure Updates**[38] 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.

Note: For more information about Azure updates, refer to **Azure Updates**[39].

38 https://azure.microsoft.com/en-us/updates/
39 https://azure.microsoft.com/en-us/updates/

Module 4 Review Questions

Azure Pricing and Support Review Questions

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

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 polices 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 Azures 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.