

Describe cloud computing

1. Introduction to Microsoft Azure Fundamentals

<https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/1-introduction-microsoft-azure-fundamentals>

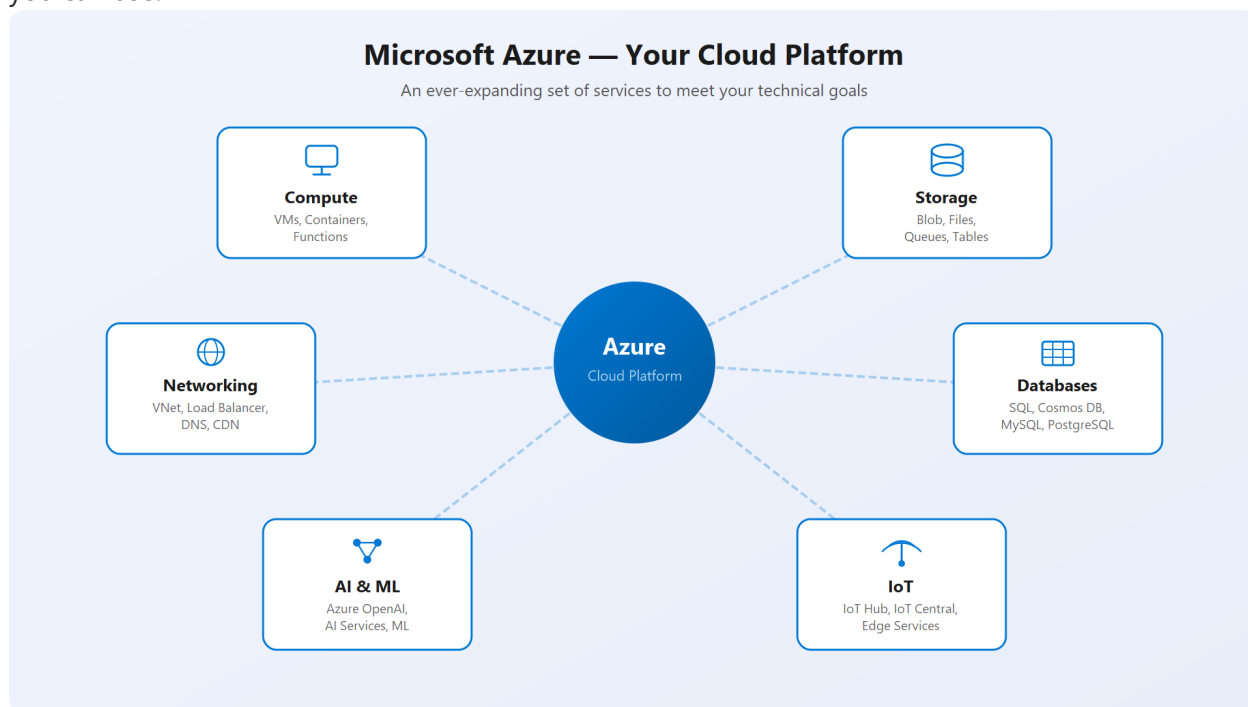
Introduction to Microsoft Azure Fundamentals

Completed

Microsoft Azure is a cloud computing platform with an ever-expanding set of services to help you build solutions that meet your technical goals. Azure services support everything from simple to complex. You can host simple web services for internet-facing apps, run fully virtualized computers for custom software solutions, or use cloud-based services like remote storage, database hosting, and centralized account management. Azure also offers capabilities in artificial intelligence (AI) and Internet of Things (IoT).

In this series, you cover cloud computing basics, get introduced to some of the core services provided by Microsoft Azure, and learn more about the governance and compliance services that

you can use.



What is Azure Fundamentals?

Azure Fundamentals is a series of three learning paths that familiarize you with Azure and its many services and features and one learning path that gives you a chance to explore Azure and build solutions to realistic IT challenges.

Whether you're interested in compute, networking, or storage services; learning about cloud security best practices; or exploring governance and management options, think of Azure Fundamentals as your curated guide to Azure.

Azure Fundamentals includes guided content and knowledge checks that reinforce key concepts.

Technical IT experience isn't required; however, having general IT knowledge will help you get the most from your learning experience.

Why should I take Azure Fundamentals?

If you're just beginning to work with the cloud, or if you already have cloud experience, Azure Fundamentals provides you with everything you need to get started.

No matter your goals, Azure Fundamentals has something for you. You should take this course if you:

- Have general interest in Azure or in cloud computing
- Want to earn official certification from Microsoft (AZ-900)

The Azure Fundamentals learning path series can help you prepare for Exam AZ-900: Microsoft Azure Fundamentals. This exam includes three knowledge domain areas:

AZ-900 Domain Area	Weight
Describe cloud concepts	25-30%
Describe Azure architecture and services	35-40%
Describe Azure management and governance	30-35%

Each domain area maps to a learning path in Azure Fundamentals. The percentages shown indicate the relative weight of each area on the exam. The higher the percentage, the more questions that part of the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.

This training helps you develop a broad understanding of Azure.

2. Introduction to cloud computing

<https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/2-introduction-cloud-compute>

Introduction to cloud computing

Completed

In this module, you're introduced to general cloud concepts. You start with an introduction to the cloud in general. Then you dive into concepts like shared responsibility, different cloud models, and explore the unique pricing method for the cloud.

If you're already familiar with cloud computing, this module may be largely review for you.

Learning objectives

After completing this module, you'll be able to:

- Define cloud computing.
- Describe the shared responsibility model.
- Define cloud models, including public, private, and hybrid.
- Identify appropriate use cases for each cloud model.
- Describe the consumption-based model.
- Compare cloud pricing models.

3. What is cloud computing

What is cloud computing

Completed

Cloud computing is the delivery of computing services over the internet. Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking. Cloud services also expand the traditional IT offerings to include things like Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI).

Because cloud computing uses the internet to deliver these services, it doesn't have to be constrained by physical infrastructure the same way that a traditional datacenter is. That means if you need to increase your IT infrastructure rapidly, you don't have to wait to build a new datacenter—you can use the cloud to rapidly expand your IT footprint.

Practical example

Suppose a retail team expects high traffic during a seasonal launch. Instead of buying and configuring extra physical servers months in advance, they can deploy additional compute capacity in the cloud for the launch period and scale down afterward. This approach improves agility and helps align spending to actual demand.

At a fundamentals level, cloud computing changes infrastructure planning from long procurement cycles to on-demand provisioning. Teams can test faster, recover faster, and adapt capacity as requirements change.

Cloud platforms also offer global reach, so teams can place services closer to users and design for regional resilience without building multiple physical datacenters.

This short video provides a quick introduction to cloud computing.

4. Describe the shared responsibility model

Describe the shared responsibility model

Completed

You may have heard of the shared responsibility model, but you may not understand what it means or how it impacts cloud computing.

How responsibilities shift in cloud

Start with a traditional on-premises datacenter. Your team is responsible for maintaining the physical space, ensuring security, and maintaining or replacing the servers if anything happens. The IT department is responsible for maintaining all the infrastructure and software needed to keep the datacenter up and running. They're also likely to be responsible for keeping all systems patched and on the correct version.

With the shared responsibility model, these responsibilities get shared between the cloud provider and the consumer. Physical security, power, cooling, and network connectivity are the responsibility of the cloud provider. The consumer isn't collocated with the datacenter, so it wouldn't make sense for the consumer to have any of those responsibilities.

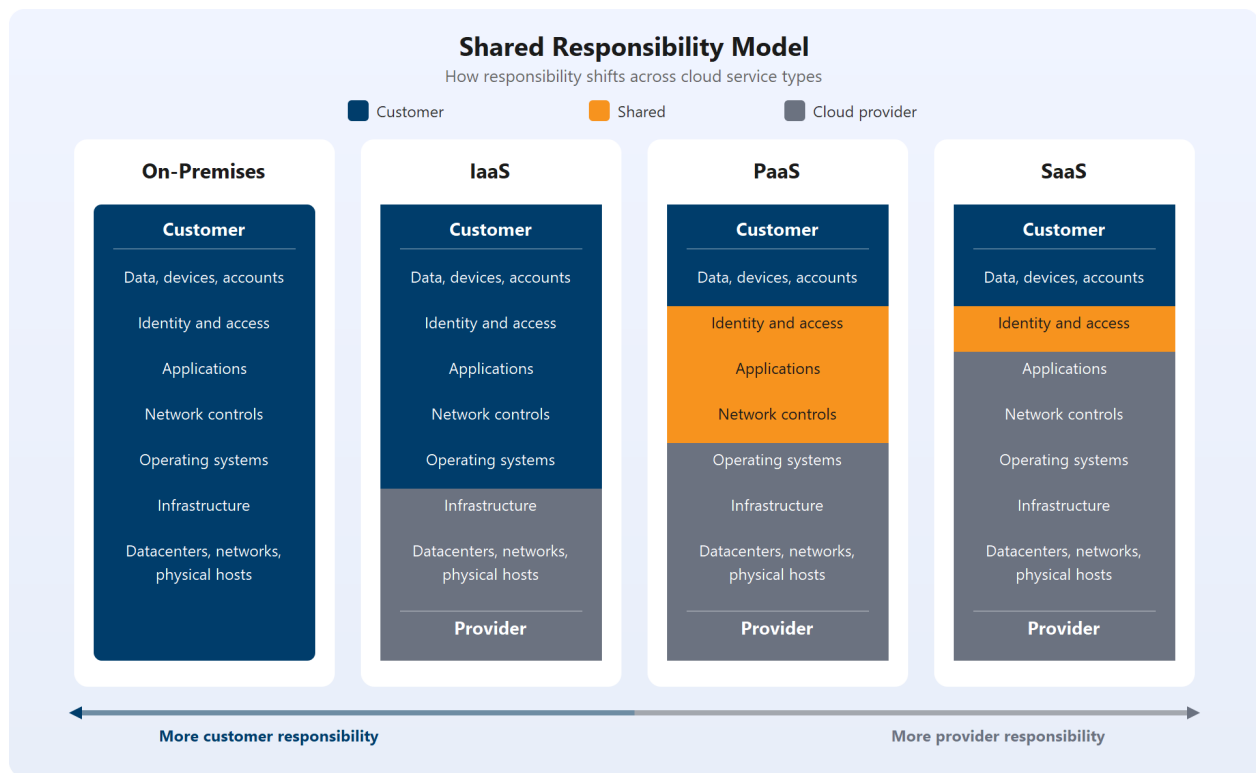
At the same time, the consumer is responsible for the data and information stored in the cloud. (You wouldn't want the cloud provider to be able to read your information.) The consumer is also responsible for access security, meaning you only give access to those who need it.

Then, for some things, the responsibility depends on the situation. If you're using a cloud SQL database, the cloud provider would be responsible for maintaining the actual database. However, you're still responsible for the data that gets ingested into the database. If you deployed a virtual machine and installed an SQL database on it, you'd be responsible for database patches and updates, as well as maintaining the data and information stored in the database.

With an on-premises datacenter, you're responsible for everything. With cloud computing, those responsibilities shift. The shared responsibility model is heavily tied into the cloud service types (covered later in this learning path): infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS places the most responsibility on the consumer, with the cloud provider being responsible for the basics of physical security, power, and connectivity. On the other end of the spectrum, SaaS places most of the responsibility with the cloud provider. PaaS, being a middle ground between IaaS and SaaS, rests somewhere in the middle and evenly distributes responsibility between the cloud provider and the consumer.

Responsibility by service model

The following diagram highlights how the Shared Responsibility Model informs who is responsible for what, depending on the cloud service type.



When using a cloud provider, you'll always be responsible for:

What always stays with you

- The information and data stored in the cloud
- Devices that are allowed to connect to your cloud (cell phones, computers, and so on)
- The accounts and identities of the people, services, and devices within your environment

The cloud provider is always responsible for:

What the provider always owns

- The physical datacenter
- The physical network
- The physical hosts

Your service model will determine responsibility for things like:

What depends on the service type

- Operating systems
- Network controls

- Applications
- Identity and access
- Infrastructure

For example, identity and access is shared in PaaS and SaaS—you manage your own users, roles, and policies, while the provider runs the authentication platform (such as Microsoft Entra ID).

Infrastructure, on the other hand, shifts entirely to the provider as soon as you move off-premises to IaaS.

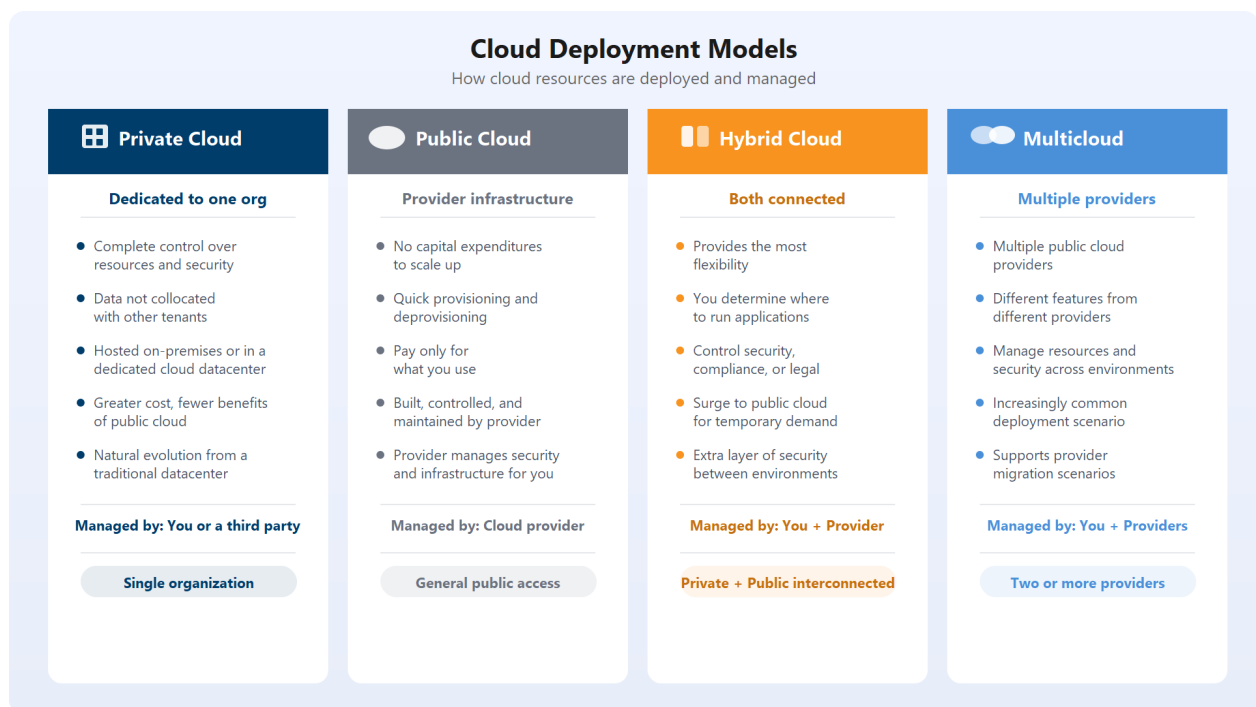
5. Define cloud models

<https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/5-define-cloud-models>

Define cloud models

Completed

What are cloud models? The cloud models define the deployment type of cloud resources. The three main cloud models are: private, public, and hybrid.



Private cloud

A private cloud is a cloud environment used by a single entity. It evolved naturally from the traditional datacenter model, delivering IT services over the internet while keeping resources dedicated to one organization. Private cloud provides much greater control for your IT team. However, it also comes with greater cost and fewer of the benefits of a public cloud deployment. A private cloud may be hosted from your on-site datacenter, or in a dedicated datacenter offsite, potentially even by a third party.

Public cloud

A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources. The general public availability is a key difference between public and private clouds.

Hybrid cloud

A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources. Hybrid cloud can be used to provide an extra layer of security. For example, users can flexibly choose which services to keep in public cloud and which to deploy to their private cloud infrastructure.

The following table highlights a few key comparative aspects between the cloud models.

Public cloud	Private cloud	Hybrid cloud
No capital expenditures to scale up	You have complete control over resources and security	Provides the most flexibility
Applications can be quickly provisioned and deprovisioned	Data isn't collocated with other tenants' data	You determine where to run your applications
You pay only for what you use	Hardware must be purchased for startup and maintenance	You control security, compliance, or legal requirements
You don't have complete control over resources and security	You are responsible for hardware maintenance and updates	

Multicloud

A fourth, and increasingly likely scenario is a multicloud scenario. In a multicloud scenario, you use multiple public cloud providers. Maybe you use different features from different cloud providers. Or maybe you started your cloud journey with one provider and are in the process of migrating to a different provider. Regardless, in a multicloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments.

Azure Arc

Azure Arc is a set of technologies that helps manage your cloud environment. Azure Arc can help manage your cloud environment whether it's a public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration, or even a multicloud environment running on multiple cloud providers at once.

Azure VMware Solution

What if you're already established with VMware in a private cloud environment but want to migrate to a public or hybrid cloud? Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability.

6. Describe the consumption-based model

<https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/6-describe-consumption-based-model>

Describe the consumption-based model

Completed

Cloud computing operates on a consumption-based model. You pay for the IT resources you use, and nothing more. Instead of buying and maintaining your own datacenter infrastructure, you rent compute power and storage and release those resources when you're done.

In traditional IT budgeting, you may hear the terms capital expenditure (CapEx) and operational expenditure (OpEx). CapEx refers to up-front spending on physical infrastructure like servers, network hardware, and datacenter space. OpEx refers to ongoing spending on services over time. Because you pay for cloud services as you consume them, cloud computing is classified as an operational expense.

The consumption-based model offers several key benefits:

- No upfront costs for hardware or datacenter infrastructure.
- No need to purchase and manage capacity that may go underutilized.
- The ability to add resources when demand increases.
- The ability to release resources when demand decreases.

Capacity planning: traditional vs. cloud

Capacity Planning



With a traditional datacenter, you estimate future resource needs in advance. Overestimate, and you overspend on infrastructure that sits idle. Underestimate, and your applications suffer degraded performance. Fixing the problem means ordering, installing, and provisioning additional hardware, power, and cooling.

In a cloud-based model, you adjust resources to match actual demand. Add virtual machines when you need more capacity; remove them when demand drops. You pay only for what you use, not for idle capacity. In practice, you can scale out during peak demand and scale back in when traffic subsides.

Cloud pricing

Cloud providers use a pay-as-you-go pricing model. You typically pay only for the services you consume, which helps you:

- Plan and manage operating costs.
- Run infrastructure more efficiently.
- Scale as workload needs change.

The cloud provider maintains the underlying infrastructure, including power, cooling, hardware, and networking, so you can focus on solving business problems and delivering new capabilities to your users.

7. Module assessment

Module assessment

Completed

8. Summary

<https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/8-summary>

Summary

Completed

In this module, you learned about general cloud concepts. You started with an understanding of what cloud computing is. You also learned about the shared responsibility model and how you and your cloud provider share the responsibility of keeping your information in the cloud secure. You covered the differences between the cloud models (public, private, hybrid, and multicloud). Then, you wrapped up with a unit on how the cloud shifts IT spend from a capital expense to an operational expense.

Learning objectives

You should now be able to:

- Define cloud computing.
- Describe the shared responsibility model.
- Define cloud models, including public, private, and hybrid.
- Identify appropriate use cases for each cloud model.
- Describe the consumption-based model.
- Compare cloud pricing models.

Additional resources

The following resources provide more information on topics in this module or related to this module.

- [Shared responsibility model](#) - The sharing of responsibilities for the cloud between you and your cloud provider.

- [Introduction to Azure VMware Solution](#) - A Microsoft Learn course that dives deeper into Azure VMware Solution.
- [Introduction to Azure hybrid cloud services](#) - A Microsoft Learn course that explains hybrid cloud in greater detail.

Explore with Copilot

Tip

Try one of these prompts in Copilot Chat:

- "Explain shared responsibility across on-premises, IaaS, PaaS, and SaaS using one concrete business application example."
- "Compare public, private, hybrid, and multicloud models, then recommend the best fit for three different organizational scenarios."
- "Create a financial comparison of CapEx versus OpEx for moving a workload to a consumption-based cloud model."