Microsoft

Microsoft 365 Fundamentals

Exam Ref MS-900

Craig Zacker

Microsoft

Exam Ref MS-900 Microsoft 365 Fundamentals

Craig Zacker

Exam Ref MS-900 Microsoft 365 Fundamentals

Published with the authorization of Microsoft Corporation by
Pearson Education, Inc.

ISBN-13: 978-0-13-648487-5
ISBN-10: 0-13-648487-5

Library of Congress Control Number: 2019956209

ScoutAutomatedPrintCode

TRADEMARKS

Microsoft and the trademarks listed at *http://www.microsoft.com* on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at
corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

ASSISTANT SPONSORING
EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Erika Millen

PROOFREADER
Charlotte Kughen

TECHNICAL EDITOR
J. Boyd Nolan

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITION
codeMantra

Contents at a glance

This page intentionally left blank

Contents

Introduction

The Microsoft 365 Certified Fundamentals certification is the initial entry point into a hierarchy of Microsoft 365 certifications. The MS-900 Microsoft 365 Fundamentals exam tests the candidate's knowledge of the components and capabilities of the Microsoft 365 products without delving into specific administrative procedures. With the Fundamentals certification in place, IT pros can then move up to Associate level certifications that concentrate on specific areas of Microsoft 365 administration, such as messaging, security, desktop, and teamwork. The ultimate pinnacle in the hierarchy is the Enterprise Administrator Expert certification, achievable by passing the MS-100 and MS-101 exams.

This book covers all the skills measured by the MS-900 exam, with each of the four main areas covered in a separate chapter. Each chapter is broken down into individual skill sections, which cover all the suggested topics for each skill. It is recommended that you access a trial version of Microsoft 365 as you work your way through this book. Nothing can replace actual hands-on experience, and Microsoft provides a fully functional evaluation platform of Microsoft 365 Enterprise—all the components of which are accessible in the cloud and require no hardware other than a computer with Internet access. Microsoft also provides a wealth of documentation for all the Microsoft 365 components at *docs.microsoft.com*. With these tools, as well as some time and dedication, you can prepare yourself for the MS-900 exam and the first step toward your Microsoft 365 career.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

Errata, updates, & book support

We’ve made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

This page intentionally left blank

Important: How to use this book to study for the exam

Certification exams validate your on-the-job experience and product knowledge. To gauge your readiness to take an exam, use this Exam Ref to help you check your understanding of the skills tested by the exam. Determine the topics you know well and the areas in which you need more experience. To help you refresh your skills in specific areas, we have also provided "Need more review?" pointers, which direct you to more in-depth information outside the book.

The Exam Ref is not a substitute for hands-on experience. This book is not designed to teach you new skills.

This page intentionally left blank

About the Author

Craig Zacker is the author or coauthor of dozens of books, manuals, articles, and websites on computer and networking topics. He has also been an English professor, a technical and copy editor, a network administrator, a webmaster, a corporate trainer, a technical support engineer, a minicomputer operator, a literature and philosophy student, a library clerk, a photographic darkroom technician, a shipping clerk, and a newspaper boy. He lives in a little house with his beautiful wife and a neurotic cat.

This page intentionally left blank

CHAPTER 1

Understand cloud concepts

The cloud is one of the biggest buzzwords ever to emerge from the IT industry, but it is a term that is difficult to define in any but the most general terms. For a simple definition, you can say that the *cloud* is an Internet-based resource that provides subscribers with various types of IT services on demand. For users, the cloud enables them to run applications, stream video, download music, read email, and perform any number of other tasks, all without having to worry about where the servers are located, what resources they utilize, how much data is involved, and—in most cases—whether the service is operational. Like the electricity or the water in your house, you turn it on, and it is there—most of the time. For IT professionals, however, defining the cloud can be more difficult.

Skills in this chapter:

- Detail and understand the benefits and considerations of using cloud services
- Understand the different types of cloud services available

Skill 1.1: Detail and understand the benefits and considerations of using cloud services

System administrators, software developers, database administrators, and user-support personnel all see the cloud in a different light and use it for different purposes. Cloud providers, such as Microsoft, Google, and Amazon, typically offer a wide variety of resources and services. They can provide virtualized hardware, such as servers, storage, and networks; software in the form of back-end server and user applications; as well as tools for messaging, content management, collaboration, identity management, analytics, and others. Services are provided on an *à la carte* basis, with the subscribers only paying for what they use.

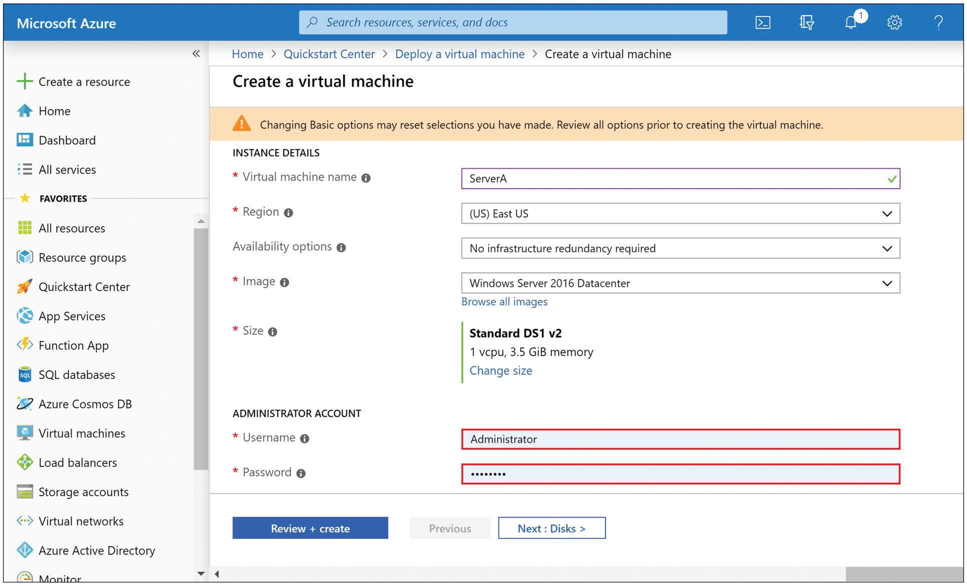
This section covers how to:

- Understand cloud services
- Understand the advantages of cloud computing

Understanding cloud services

Different types of IT professionals understand the cloud in different ways. For a system administrator, the cloud can provide virtual machines that function as servers, in place of or alongside physical servers in the organization's data center. For software developers, the cloud can provide a variety of preconfigured platforms and development environments for application deployment and testing. For a database administrator, the cloud can provide complex storage architectures and preconfigured database management solutions. Cloud services can then organize the data and use artificial intelligence to develop new uses for it. For user support technicians, the cloud can provide productivity applications and other software, such as Office 365, that are more easily deployed than standalone applications, automatically updated on a regular basis, and accessible on any device platform.

In each of these specializations, cloud services can eliminate the tedious set-up processes that administrators often have to perform before they can get down to work. For example, the process of adding a new physical server to a data center can require many separate tasks, including assessing the hardware needs, selecting a vendor, waiting for delivery, assembling the hardware, and installing and configuring the operating system and applications. These tasks can result in days or weeks wasted before the server is even ready for use. With a cloud provider, the process of adding a new virtual server takes only a matter of minutes. A remote management interface, such as the Windows Azure portal shown in Figure 1-1, enables the subscriber to select the desired virtual hardware resources for the server, and within a few minutes, the new server is running and ready for use.



Create a virtual machine

Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

INSTANCE DETAILS

* Virtual machine name: ServerA

* Region: (US) East US

Availability options: No infrastructure redundancy required

* Image: Windows Server 2016 Datacenter
Browse all images

* Size: Standard DS1 v2
1 vcpu, 3.5 GiB memory
Change size

ADMINISTRATOR ACCOUNT

* Username: Administrator

* Password: ••••••••

FIGURE 1-1 The Create a Virtual Machine interface in the Windows Azure Portal

Advantages of cloud computing

When an organization is building a new IT infrastructure or expanding an existing one, the question of whether to use on-premises resources or subscriber-based cloud services is a critical decision to make these days. Cloud-based services might not be preferable for every computing scenario, but they can provide many advantages over on-premises data centers. When designing an IT strategy, a business should consider both the practical needs of the organization, including data security and other business factors, as well as the relative costs of the required services.

Some of the advantages that cloud computing can provide are discussed in the following sections.

Economy

Cloud services incur regular charges, but the charges are usually based solely on the subscribers' needs and what they use at a particular time. The monetary savings that result from using cloud services can be significant. Some of the expenses that can be reduced or eliminated by using cloud services include the following:

- **Hardware** The high-end server hardware used by a large enterprise, aside from the standard computer components, can include elaborate storage arrays and other hardware that is an expensive initial outlay before any actual work starts. The fees for equivalent virtualized hardware in the cloud are amortized over the life of project for which it is used.
- **Upgrades** In a large enterprise, servers and other hardware components have a documented life expectancy, after which they must be replaced. Cloud hardware is virtual, so the subscriber is isolated from the maintenance costs of the provider's physical hardware. Those costs are, of course, factored into the price of the service, but they eliminate another substantial hardware outlay for the subscriber.
- **Software** Software licenses are a significant expense, especially for server-based products. In addition to operating systems and applications, utility software for firewalls, antivirus protection, and backups adds to the expenditure. As with hardware, software furnished on a subscription basis by a cloud provider requires little or no initial outlay. Typically, cloud-based software also includes updates applied by the provider on a regular basis.
- **Environment** Outfitting a large data center often involves much more expenditure than the cost of the computer hardware alone. In addition to the cost of the square footage, a data center typically needs air conditioning and other environmental controls, electricity and power regulation equipment, racks and other mounting hardware, network connectivity equipment, and a physical security infrastructure. Depending on the needs of the organization, these costs can range from significant to astronomical. None of these expenses are required for cloud-based services, although their costs are certainly factored into the fees paid by the subscriber.
- **Network** A data center requires an Internet connection and may also require cross-connections between locations within the data center. The size and functionality of the data center determine how much throughput is required and what technology

can best supply it. More speed costs more money, of course. Cloud-based resources eliminate this expense because connectivity is part of the service. Internet access is still required to administer the cloud resources, but the amount of data transferred is relatively small.

- **Redundancy** Depending on the needs of the organization, fault tolerance can take the form of backup power supplies, redundant servers, or even redundant data centers in different cities, which can cause the operational costs to grow exponentially. Typically, cloud providers can provide these various types of fault tolerance at a substantial savings. A contract with a cloud provider can include a service level agreement (SLA) with an uptime availability percentage that insulates the subscriber from the actual fault tolerance mechanisms employed and simply guarantees that the contracted services will suffer no more than a specified amount of downtime. For example, a contract specifying 99 percent uptime (colloquially called a *two nines contract*) allows for 3.65 days of downtime per year. A 99.9 percent (or *three nines*) contract allows for 8.76 hours of downtime per year. Contract stipulations go up from there, with the cost rising as the allowed downtime goes down. A 99.9999 percent (or *six nines*) contract allows only 31.5 seconds of downtime per year. Typically, if the provider fails to meet the uptime percentage specified in the SLA, the contract calls for a credit toward part of the monthly fee.
- **Personnel** A data center requires trained people to install, configure, and maintain all the equipment. While cloud-based service equivalents do require configuration and maintenance performed through a remote interface, the elimination of the need for hardware maintenance greatly reduces the manpower requirements.

The costs of cloud-based services are not insignificant, but the nature of the financial investment is such that many organizations find them to be more practical than building and maintaining a physical data center. The initial outlay of cloud services is minimal, and the ongoing costs are easily predictable.

Consolidation

Originally, IT departments provided services to users by building and maintaining data centers that contained servers and other equipment. One of the problems with this model was that the servers often were underutilized. To accommodate the increased workload of the “busy season,” servers were often built with resources that far exceeded their everyday needs. Those expensive resources therefore remained idle most of the time. Virtual machines (VMs), such as those administrators can create using products like Microsoft Hyper-V and VMware ESX, are a solution to this problem. Virtual machines make it possible to consolidate multiple servers into one physical computer. Administrators can scale virtual machines by adding or subtracting virtualized resources, such as memory and storage, or they can move the virtual machines from one physical computer to another, as needed.

Cloud providers use this same consolidation technique to provide subscribers with virtual machines. For example, when a subscriber to Microsoft Azure creates a new server, what actually happens is that the Azure interface creates a new virtual machine on one of Microsoft’s physical servers. The subscriber has no access to the underlying physical computer hosting the VM, nor does the subscriber even know where the computer is physically located. The virtual machines on the physical server are completely isolated from each other, so if even the fiercest competitors were to have VMs running on the same host computer, they would never know it. The provider can—and probably does—move VMs from one host computer to another when necessary, but this process is completely invisible to the subscribers.

The end result of this consolidation model is that each VM receives exactly the virtual hardware resources it needs at any particular time. Subscribers pay only for the virtualized resources they are using. Nothing goes to waste.

Scalability

Business requirements change. They might increase or decrease over a course of years, and they might also experience regular cycles of activity that are seasonal, monthly, weekly, or even daily. A physical data center must be designed to support the peak activity level for the regular business cycles and also anticipate an expected degree of growth over several years. As mentioned earlier, this can mean purchasing more equipment than the business needs for most of its operational time, leaving that excess capacity often underused.

Cloud-based services avoid these periods of underutilization by being easily scalable. Because the hardware in a virtual machine is itself virtualized, an administrator can modify its resources through a simple configuration change. An on-premises (that is, noncloud) virtual machine is obviously limited by the physical hardware in the computer hosting it and the resources used by other VMs on the same host. In a cloud-based VM, however, these limitations do not apply. The physical hardware resources are invisible to the cloud subscriber, so if the resources the subscriber desires for a VM are not available on its current host computer, the provider can invisibly move the VM to another host that does have sufficient resources.

A cloud-based service is scalable in two ways:

- **Vertical scaling** Also known as *scaling up*, vertical scaling is the addition or subtraction of virtual hardware resources in a VM, such as memory, storage, or CPUs. The scaling process is a simple matter of adjusting the VM's parameters in a remote interface; it can even be automated to accommodate regular business cycles. Therefore, the subscriber pays only for the resources that the VMs are actually using at any given time.
- **Horizontal scaling** Also known as *scaling out*, horizontal scaling is the addition or subtraction of virtual machines to a cluster of servers running a particular application. For example, in the case of a cloud-based web server farm, incoming user requests can be shared among multiple VMs. If the web traffic should increase or decrease, the administrators can add or subtract VMs from the cluster, as needed.

Reliability

In an on-premises data center, data backup, disaster recovery, and fault tolerance are all expensive services that require additional hardware, deployment time, and administration. A small business might require only a backup storage medium and software. However, for businesses with highly critical IT requirements, these services can call for anything up to duplicate data centers in different cities with high-speed data connections linking them.

In the case of a large-scale cloud provider, however, this is exactly what their infrastructure entails. Therefore, cloud providers are in an excellent position to provide these elaborate services without the need for infrastructure upgrades, and they often can do it for fees that are much less than would be required for businesses to provide them themselves.

For example, Microsoft Azure provides the following reliability mechanisms for its cloud-based services:

- Azure maintains three redundant copies of all data, with one of those copies located in a separate data center.
- Azure provides automatic failover to a backup server to minimize downtime in the event of an outage.
- Azure hosts all applications on two separate server instances to minimize downtime caused by hardware failure.

Manageability

Because subscribers do not have physical access to the servers hosting their cloud services, they must access them remotely. This is common for organizations with on-premises servers as well, particularly those with large data centers. It is often far more convenient for administrators to access servers from their desks than travel to a data center that might be on another floor, in another building, or even in another city. Today's remote management typically provides comprehensive and reliable access to all server functions.

There are various remote management tools available for both cloud and on-premises resources, but the large third-party cloud providers typically provide a secured web-based portal that enables administrators to access all their subscription services using one interface, such as the one for Microsoft Azure shown in Figure 1-2.

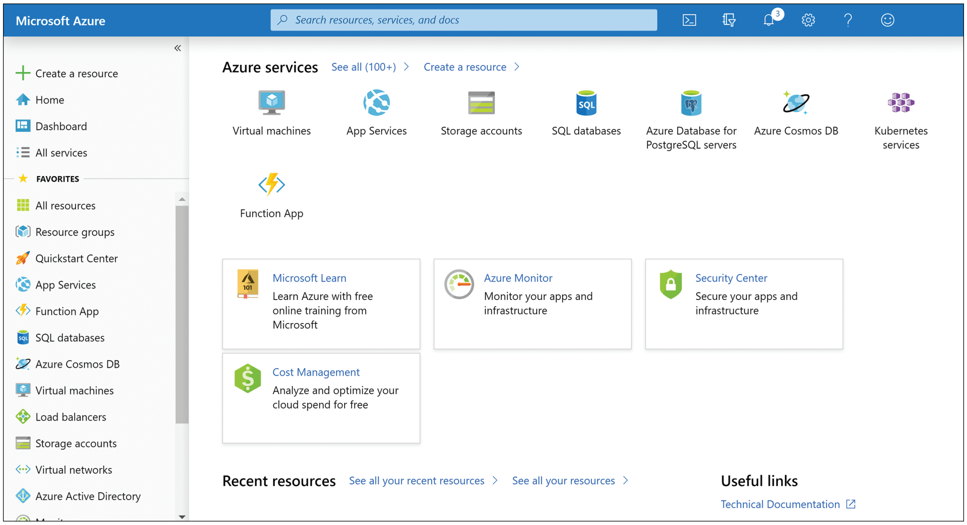


FIGURE 1-2 The management interface in the Windows Azure Portal

A web-based portal enables administrators to access their services from any location, including from home or while traveling.

Security

Security is a major issue for any data center, which administrators typically address by concerning themselves with issues such as data loss and unauthorized access. These are important concerns whether the data center is local or virtual. However, in the case of an on-premises data center, there is another potential attack vector: the physical. Servers and other equipment can be stolen outright, damaged by fire or other disasters or physically accessed by intruders. Therefore, there are additional security measures that might be required, such as door locks, surveillance equipment, access credentials, or even manned security checkpoints.

Cloud-based services eliminate the need for physical security, which is furnished by the provider. There is still the issue of software-based security, however, and cloud providers nearly always provide an array of controls and services that enable you to harden the security of your servers and applications to accommodate your business needs.

NOTE **YOU ARE ALWAYS RESPONSIBLE FOR YOUR DATA**

Organizations using cloud resources to implement their servers must be conscious of the fact that they are still responsible for the security and privacy of their data. For example, if an organization stores patient medical records on a cloud-based file server, the organization remains responsible for any data breaches that occur. Therefore, contracts with cloud providers should stipulate the security policies they must maintain.

Infrastructure

In an on-premises data center, the administrators are responsible for all aspects of the servers and other equipment, including hardware installation and maintenance, operating system configuration and updates, and application deployment and management. Cloud-based services enable subscribers to specify which elements of the infrastructure they are responsible for maintaining.

For example, a subscriber can contract with a provider for a virtual machine running a server operating system, so that the subscriber is responsible for the entire operation and maintenance of the server. The subscriber does not have direct access to the physical hardware of the host system, of course, but he or she does have control over the virtual hardware on which the server runs, as well as all the software running on the server, including the operating system. In some situations, this is desirable, or even essential.

In other situations, cloud-based services can take the form of preinstalled server platforms or applications. In this case, the subscriber might have limited access to the server or no access at all. In the case of a subscriber contracting for Microsoft Exchange Online, the provider grants the subscriber with administrative access to the Exchange Server application, but it does not grant subscriber access to the underlying operating system on which the server application is running. For an Office 365 subscriber, the provider grants access only to the Office applications themselves. The subscriber knows nothing about the servers on which the applications are running or their operating systems.

These options enable cloud service subscribers to exercise administrative responsibility over specific components only in situations in which their business requirements demand it. For the elements administered by the service provider, contracts typically stipulate hardware maintenance requirements and software update policies. The end result can be substantial savings in time and training for the subscriber's in-house IT personnel.

Alleged Disadvantages of Cloud Computing

There are some IT professionals who persist in stating that cloud-based services are inferior to on-premises services. They might say that an on-premises data center is more secure, more reliable, provides greater access to equipment, or suffers less downtime. While one cannot say that the cloud is always a preferable solution, these arguments mostly date from a time when the cloud was a new and immature technology. They have now largely been debunked by years of proven performance.

There are still reasons why businesses can and should maintain on-premises data centers. For example, they might have special security requirements, or they might have already made a large investment in facilities and equipment. However, each year sees a greater percentage of servers deployed in the cloud and clients accessing cloud-based services. Microsoft 365 is the next step in bringing the cloud to the desktop productivity environment.

Skill 1.2: Understand the different types of cloud services available

Flexibility is an important aspect of cloud computing, and Microsoft 365 can accommodate a wide variety of IT environments. While some organizations might be building a Microsoft 365 deployment from scratch, others might have existing infrastructure that they want to incorporate into a Microsoft 365 solution. Before it is possible to explore how this can be done, it is important to understand the various types of cloud architectures and service models.

This section covers how to:

- Position Microsoft 365 in a SaaS, IaaS, PaaS, Public, Private, and Hybrid scenario

Cloud architectures

Organizations today use cloud resources in different ways and for various reasons. A new business or division of a business might decide to build an entirely new IT infrastructure using only cloud-based resources. Meanwhile, a business that has already invested in a traditional IT infrastructure might use the cloud for expansions or for the addition of selected services. Organizations planning their infrastructures can use any of the three cloud architecture permutations described in the following sections.

Public cloud

A *public cloud* is a network of servers owned by a third-party service provider at a remote location, which provides subscribers with access to virtual machines or services through the Internet, often for a fee. Prices are based on the resources or services you use. Microsoft Azure, Amazon Web Services, and Google Cloud are all examples of public cloud service providers that organizations use to host their virtual machines and access other services.

NOTE **PUBLIC DOES NOT MEAN UNPROTECTED**

The term *public cloud* is something of a misnomer; it does not mean that the virtual machines an organization creates in a provider's cloud are public—that is, open to access by anyone. It means only that the provider furnishes services to the public by subscription, which are accessible from any location at any time via the Internet.

These major players in the public cloud industry maintain thousands of servers in data centers located around the world. They can accommodate large enterprise clients by providing services on a global scale. There are other, smaller cloud providers offering the same services, which might not be able to function on such a massive scale, but these can have their advantages as well. Because the cloud service providers are responsible for managing and maintaining the physical servers, the subscribers save a great deal of time, expense, and human resources.

There are two basic types of public cloud deployment that organizations can use, as follows:

- **Shared public cloud** Subscribers access services that a third-party provider implements on hardware that might be used by other subscribers at the same time. For example, a physical host server at a provider site can run virtual machines belonging to different subscribers simultaneously, as shown in Figure 1-3. The VMs are secured individually and functionally isolated from each other. This is what is typically meant by a public cloud.
- **Dedicated public cloud** Subscribers contract with a third-party provider for a hardware infrastructure that is dedicated to their exclusive use. (See Figure 1-4.) The services provided are the same as those in a shared public cloud; the only difference is the hardware the provider uses to furnish the services. Obviously, this arrangement is more expensive than a shared public cloud, but some organizations need the additional security and fault tolerance provided by having hardware dedicated to their own use.

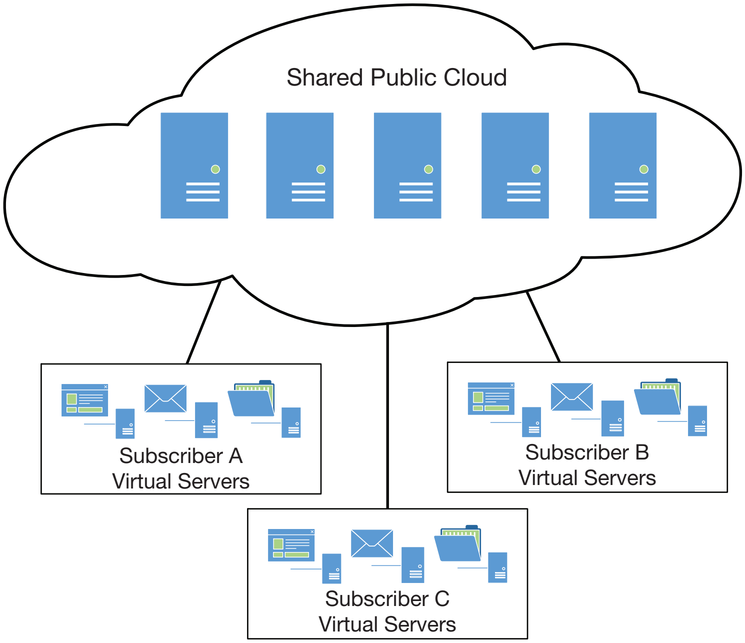


FIGURE 1-3 Virtual servers running in a shared public cloud

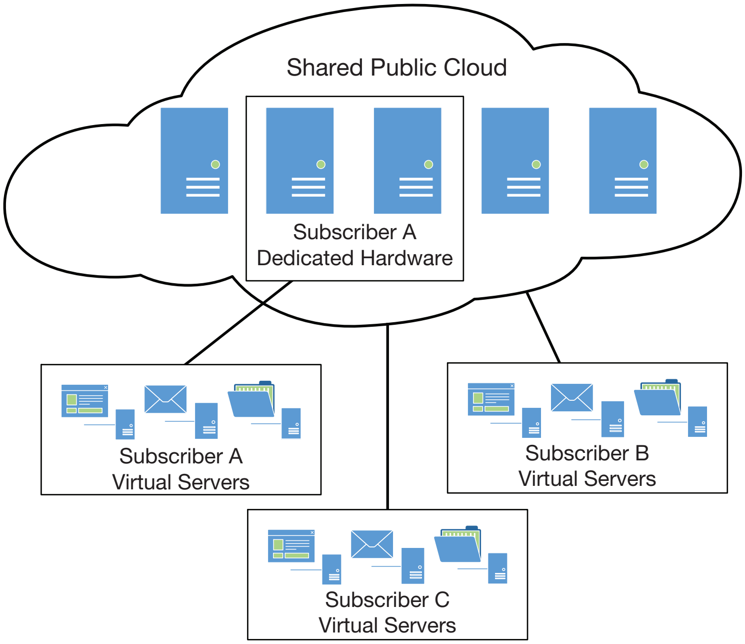


FIGURE 1-4 Virtual servers running in a dedicated public cloud

Therefore, the term *public cloud* can refer to a provider that enables businesses to build their IT networks virtually instead of physically. Microsoft 365 subscribers can make use of these services to implement all or part of their productivity infrastructure. However, this is not the only function of the public cloud. When people stream movies to their televisions, use web-based banking services, access their email online, or use the Office 365 productivity applications, they are using public cloud providers. The difference in these cases is that the provider is furnishing specific services instead of an IT infrastructure.

Private cloud

A *private cloud* is a network of servers owned and operated by a business solely for its own use. While the services can be the same and appear identical to their end users, the primary difference is that the organization has control over the physical hardware as well.

In a public cloud deployment of an IT infrastructure, either the subscriber creates virtual machines on the provider's servers and uses them to install and run specific applications or contracts with the provider for access to services running on the provider's own virtual machines. A private cloud deployment usually works in much the same way. The organization still creates and utilizes virtual machines to run its applications in most cases, but it creates those virtual machines on physical host servers that it owns.

Another variation on the private cloud is the *hosted private cloud*, in which hardware that is owned or leased by an organization is housed and managed by a third-party provider. The organization has exclusive use of the hardware and avoids the expenses of building and managing a data center. They do have to pay ongoing fees to the provider, and this arrangement might not satisfy all data storage stipulations, but the overall cost is likely to be less than an on-premises private cloud.

NOTE **PRIVATE CLOUDS AND INTERNET TRAFFIC**

The term *private cloud* can be something of an oxymoron. Typically, the definition of the cloud includes access to services over the Internet. In a public cloud, both administrative and user access to the cloud resources are through the Internet. While a private cloud can provide users and administrators with access to services via the Internet, it typically does not use the Internet when the administrators and users are located at the same site as the data center housing the cloud.

When a large enterprise maintains facilities at multiple locations, users at all those facilities can access a private cloud using the Internet. However, a small- or medium-sized organization running Microsoft 365 Business at a single location can conceivably run what is technically called a private cloud without the need for user and administrator traffic to ever leave the facility.

The private cloud architecture can provide a level of security and privacy that a public cloud provider might not be able to meet. An organization might have government contract stipulations or legal requirements that compel them to maintain their own hardware and store sensitive data on site rather than use third-party hardware that is not subject to the same stipulations or requirements. For example, the Health Insurance Portability and Accountability Act (HIPAA) dictates how medical data must be secured and protected in the United States. Whether a third-party cloud provider is involved, a company is legally responsible for all the data stored on its servers. An organization might also need to run a legacy application that requires a specific hardware or software configuration that a third-party provider cannot supply.

A private cloud also provides a greater degree of customization than public cloud resources. Public cloud providers are successful because of the scale of their businesses; their services are configurable using the options that are most desired by most of their clients. They are not likely to provide access to obscure software options that only a few of their clients will need. In the case of a private cloud, an organization has access to any and all the customization options provided by the software they choose to install.

EXAM TIP

The difference between a private cloud and a dedicated public cloud is who owns and operates the hardware. Exam candidates should be aware that some documentation uses the term *private cloud*, instead of *dedicated public cloud*, to describe hardware owned and operated by a third-party provider for the exclusive use of one subscriber.

The advantages of a private cloud are its disadvantages as well. The owner of the hardware is responsible for purchasing, housing, deploying, and maintaining that hardware, which can add greatly to the overall expense, as described earlier in this chapter. There are no ongoing subscriber fees for a private cloud, as there are with a public cloud provider, but there are ongoing fees for operating a data center, including floor space, power, insurance, and personnel.

The organization is also responsible for purchasing and maintaining licenses for all the software products needed to provide the necessary services. This can include operating system licenses, application server licenses, and user licenses, as well as the cost of additional software utilities. Typically, the overall costs of a private cloud infrastructure are higher than that of a public cloud and can be enormously higher. It is up to the organization to determine whether the advantages of the private cloud are worth the additional expense.

Hybrid cloud

A *hybrid cloud* combines the functionality of a public and a private cloud, enabling an organization to enjoy the best of both architectures. There are a variety of scenarios in which an organization might prefer to implement a hybrid cloud architecture.

If an organization has existing services implemented on its own physical hardware, it might want to maintain those services while adding others from a public cloud provider. For example, the organization might have reached the physical capacity of its own data center and does not want to invest in a major facility expansion.

An organization might also use public cloud resources to extend the capacity of its private cloud or its in-house network during temporary periods of greater need, such as seasonal business increases. This technique, called *cloudbursting*, eliminates the need for the organization to pay for hardware and other resources that are only required for brief periods of time. Because it is possible to connect the public and private services, the resources can interact in any way that is necessary. For example, a business with an e-commerce website implemented in a private cloud can add public cloud-based servers to its web server farm to accommodate the increase in traffic during its Christmas busy season.

Another possibility is that an organization might be subject to the type of data storage or other security requirements described in the previous section, but they do not want to build out their entire infrastructure in a private cloud. In this scenario, the organization could conceivably deploy a database containing the sensitive data in a private cloud and use a public cloud provider for a website implementation that is linked to the database. This way, the network can comply with the storage requirements without having to go to the expense of deploying web servers and other services in the private cloud. The same is true for a variety of other services; organizations can keep their sensitive data and services in the private cloud and use the public cloud for the nonsensitive services. Organizations can also use private cloud resources to run legacy equipment or applications, while all the other services run on a less expensive public cloud.

Some cloud providers supply tools that enable administrators to manage their public and private cloud resources through a single interface. Microsoft Azure provides Azure Active directory, for example, which enables a subscriber to use the same directory service for public and private cloud resources, so that administrators can access both with a single sign-on. Azure also provides management and security interfaces, both of which have built-in support for hybrid cloud architectures.

Cloud service models

The offerings of cloud service providers are typically broken down into service models, which specify what elements of the cloud infrastructure are included with each product. There are three primary cloud service models, called Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

A cloud infrastructure can be broken down into layers forming a stack, as shown in Figure 1-5. The functions of the layers are as follows:

- **People** The users working with the application
- **Data** The information that the application creates or utilizes
- **Application** The top-level software program running on virtual machine
- **Runtime** An intermediate software layer, such as .NET or Java, that provides the environment in which applications run
- **Middleware** A software component that provides intermediate services between an operating system and applications

- **Operating system** The software that provides the basic functions of a virtual machine
- **Virtual network** The logical connections between virtual machines running on servers
- **Hypervisor** The software component on the physical servers that enables virtual machines to share the server's physical resources
- **Servers** The physical computers that host the virtual machines that provide cloud services
- **Storage** The hard drives and other physical components that make up the subsystem providing data storage for the physical servers
- **Physical network** The cables, routers, and other equipment that physically connect the servers to each other and to the Internet

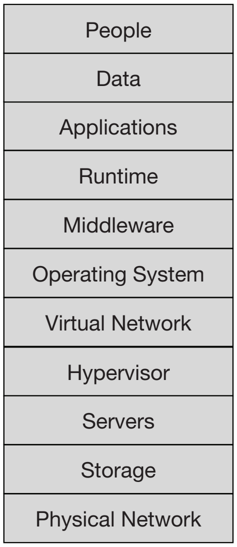


FIGURE 1-5 The layers of the cloud infrastructure

In an organization that uses its own on-premises servers for everything, there is no cloud involved, and the organization is obviously responsible for managing all the layers of the stack. However, when an organization uses cloud-based services, the cloud service provider manages some layers of the stack, and the organization manages the rest. This is called a *shared responsibility model*. Which layers are managed by the organization and which are managed by the provider depends on the service model used to furnish the cloud product. The three basic cloud service models are described in the following sections.

IaaS

Infrastructure as a Service (IaaS) is a cloud computing model in which a cloud service provider furnishes the client with the physical computing elements: the network, the storage subsystem, the physical servers, and the hypervisor running on the servers. This provides subscribers with everything they need to create their own virtual machines and manage them by themselves.

Therefore, all the cloud infrastructure layers above the hypervisor are the responsibility of the subscriber, as shown in Figure 1-6.

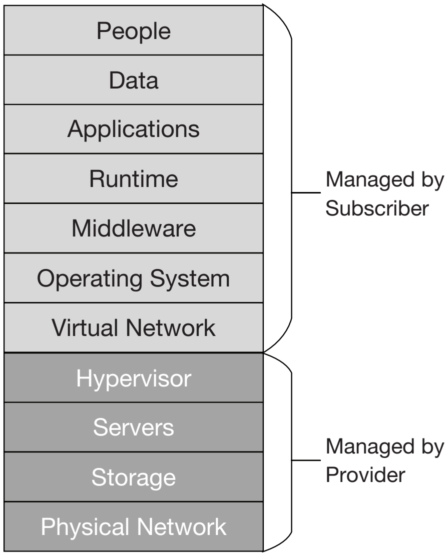


FIGURE 1-6 The shared responsibility model for IaaS

For example, when a subscriber uses Microsoft Azure to create a virtual machine, the provider is furnishing access to a physical server with hypervisor software—presumably Microsoft Hyper-V—running on it. The server has a physical storage subsystem and is connected to a physical network that provides it with access to the provider's other servers and to the Internet. Using the management tools that Azure provides, the subscriber can create a virtual machine containing a specific amount of memory and storage, and a number of CPUs, all of which are realized virtually.

NEED MORE REVIEW? **CLOUD COMPUTING WITH MICROSOFT AZURE**

For more information on cloud computing as realized in Microsoft Azure, see https://azure.microsoft.com/en-ca/overview/what-is-cloud-computing.

The end result is a virtual machine that the subscriber can install, configure, and use to run applications just like a VM running on an on-premises server. The difference is that the subscriber does not have to outfit a data center, build a network, procure a physical computer, and install the hypervisor. Instead, the subscriber pays a regular fee for the actual resources that the VM uses. The subscriber can add memory, storage, and CPUs to the VM or remove them, as needed, and the subscriber can configure many other settings through a remote management interface. Additional resources incur additional fees, but the process of building a new server takes a matter of minutes instead of days or weeks.

With the IaaS model, the provider is responsible for the physical servers and the physical network, but the subscriber is responsible for managing and maintaining its virtual machines and the virtual network on which they run, as shown earlier in Figure 1-6. Therefore, the provider installs operating system updates on the physical servers, but the subscriber must install any operating system and application updates needed on the virtual machines. Any other VM software, maintenance, and management issues that arise also are the subscriber's responsibility.

NOTE **VM UPDATE MANAGEMENT**

For an additional fee, Microsoft Azure can provide an Update Management solution that automates the installation of updates and patches on a subscriber's virtual machines.

Of all the cloud service models, IaaS places the greatest amount of responsibility on the subscriber, and in many instances, this is how administrators want it. By creating and configuring their own virtual machines, administrators can duplicate the environment of their on-premises servers, creating a hybrid cloudbursting infrastructure that can handle overflow traffic during a busy season.

Organizations with high traffic websites often use a dedicated web hosting service provider to run their sites. However, building the site using virtual machines furnished by a cloud service provider using the IaaS model often can be a far less expensive proposition.

Subscribers can also use IaaS to create a testing and development environment for applications. Rapid deployment and modification of VMs makes it possible for administrators to create multiple temporary evaluation and testing platforms and take them down just as easily.

IaaS can also provide subscribers with VMs containing massive amounts of virtual hardware resources that would be impractical to implement in on-premises servers. Large data sets and high-performance computing can require huge amounts of memory and processing power to perform the tasks required for applications, such as weather patterning, data mining, and financial modeling. The resources of a high-end cloud service provider make it far less expensive to equip VMs with the necessary virtual hardware than to build equivalent physical servers.

PaaS

In what is sometimes referred to as a *tiered cloud* service model infrastructure, *Platform as a Service (PaaS)* is the second tier, in that it builds on the provider's responsibilities from the first (IaaS) tier. PaaS is designed to provide subscribers with a ready-made developmental platform that enables them to avoid spending time repeatedly building out the hardware and software infrastructure for a test system before they can run a new application.

Because the platform is accessible through the Internet like all cloud services, an organization with multiple developers working on the same project can provide them all with access to the test environment, even if they are located at different sites.

The PaaS model expands the responsibility of the cloud service provider over the IaaS model by adding the virtual network, operating system, middleware, and runtime layers, as shown in Figure 1-7. The greater the responsibility of the provider, the less that of the subscriber.

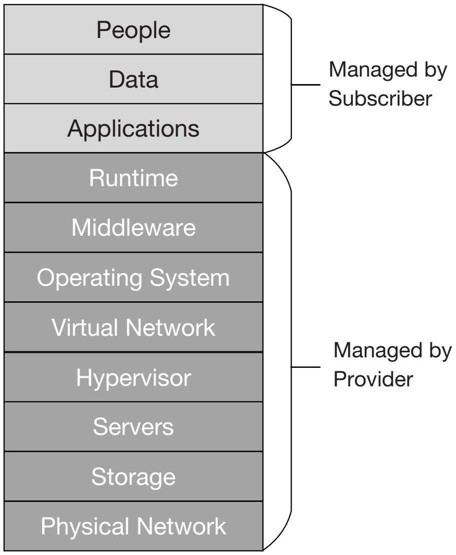


FIGURE 1-7 The shared responsibility model for PaaS

Unlike virtual machines on the IaaS model, the cloud provider is entirely responsible for the VM operating system, applying updates and patches and performing maintenance as needed. The platform can also include (for an extra fee) additional components specified by the subscriber, such as development tools, middleware, and database management systems. The object of the PaaS model is to eliminate the need for software developers to do anything but actually develop, build, customize, test, and deploy their applications.

Serverless

The fees for PaaS and IaaS virtual machines are typically based on the resources they are configured to use and the time they are running. However, there is another cloud service model for application development, related to PaaS, called *serverless computing*. In serverless computing (sometimes known as *Function as a Service*, or FaaS), the cloud provider takes on even more of the server management responsibility by dynamically allocating virtual machine resources in response to application requests or events.

Pricing is based on the VM resources as they are actually used. Therefore, this model can be less expensive than a PaaS VM that is incurring charges all the time it is running. The term *serverless*, in this instance, does not mean that there is no server involved; the name derives from the fact that the cloud subscriber does not have to provision a virtual machine on which the developer's code will run.

SaaS

Software as a Service (SaaS) is the third tier of the cloud service model infrastructure, and in this model, the cloud provider is responsible for nearly all the layers. Only the people and data layers are left to the subscriber, as shown in Figure 1-8. This means that the provider is responsible for the applications, as well as all the layers beneath.

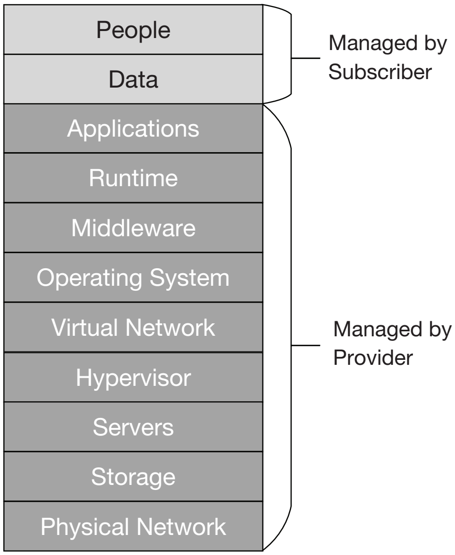


FIGURE 1-8 The shared responsibility model for SaaS

The SaaS model enables endusers to access cloud-based applications using a web or other thin-client interface, without the need to install the applications first. Office 365 is an example of an SaaS product, as are Microsoft Teams and other Microsoft 365 components. While Office 365 makes it possible to install its productivity applications on a client computer, it is not necessary for the user to do so. The applications are accessible directly through a web browser, with everything but the user's own data files provided through the cloud.

EXAM TIP

The MS-900 exam requires you to understand the role of the public, private, and hybrid architectures, as well as the IaaS, PaaS, and SaaS service models, in cloud computing. However, be sure also to understand how these elements fit in with the Microsoft 365 product.

Summary

- Cloud computing can provide organizations with many benefits, including economy scalability, reliability, manageability, and security.
- There are three basic cloud architectures:
  - **Public** Cloud resources are furnished by a third-party provider on the Internet.
  - **Private** An organization provides its own cloud resources.
  - **Hybrid** The public and private architectures are combined.
- There are three cloud service models—IaaS, PaaS, and SaaS, which specify how much of the resource management is the responsibility of the cloud provider and how much is the responsibility of the subscriber.

Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answer to this thought experiment in the next section.

Wingtip Toys has a website on which they sell their products to customers worldwide; it is the company's primary source of sales. The website is hosted on a server farm in the company's data center, which is a small room in the building's basement. The incoming traffic is distributed among the servers by a load-balancing switch. Richard, the administrator of the site, regularly monitors the website traffic and, as the holiday season approaches, he sees the traffic level rise almost to the point at which the servers are overwhelmed.

There is no budget for the purchase of additional web server computers, and there is also no room for more servers in the data center. Reading about cloud options, Richard thinks that there might be a solution there. How can Richard expand the web server farm to handle the increased traffic for the least expense by using the cloud?

Thought experiment answer

For a minimal expenditure, Richard can create additional web servers using cloud-based virtual machines and add them to his web server farm, forming a hybrid cloud architecture. The cloud-based servers can help to handle the busy season web traffic, and when the traffic levels go down, Richard can remove the VMs from the server farm until they are needed again.

Index