



Microsoft 365 Fundamentals

Exam Ref MS-900

Craig Zacker

FREE SAMPLE CHAPTER
SHARE WITH OTHERS



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.

Copyright © 2020 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions/. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

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

	<i>Introduction</i>	<i>ix</i>
	<i>Important: How to use this book to study for the exam</i>	<i>xiii</i>
CHAPTER 1	Understand cloud concepts	1
CHAPTER 2	Understand core Microsoft 365 services and concepts	21
CHAPTER 3	Understand security, compliance, privacy, and trust in Microsoft 365	101
CHAPTER 4	Understand Microsoft 365 pricing and support	167
	<i>Index</i>	<i>215</i>

This page intentionally left blank

Contents

Introduction	ix
<i>Organization of this book</i>	<i>ix</i>
<i>Microsoft certifications</i>	<i>x</i>
<i>Errata, updates, & book support</i>	<i>xi</i>
<i>Stay in touch</i>	<i>xi</i>
Important: How to use this book to study for the exam	xiii
Chapter 1 Understand cloud concepts	1
Skill 1.1: Detail and understand the benefits and considerations of using cloud services	1
Understanding cloud services	2
Advantages of cloud computing	3
Skill 1.2: Understand the different types of cloud services available	8
Cloud architectures	8
Cloud service models	13
Summary	19
Thought experiment	19
Thought experiment answer	19
Chapter 2 Understand core Microsoft 365 services and concepts	21
Skill 2.1: Describe the core Microsoft 365 components	21
Windows 10 Enterprise	22
Exchange Online	25
SharePoint Online	27
Microsoft Teams	29
Enterprise Mobility + Security	31

Skill 2.2: Compare core services in Microsoft 365 with corresponding on-premises services.	35
Deployment	35
Updates	35
Cost	35
Administration	36
Security	38
Service comparisons	38
Skill 2.3: Understand the concept of modern management	42
Transitioning to modern management	43
Windows as a Service	44
Using the Microsoft 365 portals	46
Understanding the Microsoft deployment and release model	49
Skill 2.4: Understand Office 365 ProPlus.	59
Comparing Office 365 ProPlus with on-premises Office	61
Deploying Office	63
Skill 2.5: Understand collaboration and mobility with Microsoft 365	66
Microsoft 365 collaboration tools	67
Collaborating in Microsoft 365	78
Enterprise mobility	84
Skill 2.6: Describe analytics capabilities in Microsoft 365	87
Microsoft Advanced Threat Analytics	88
Microsoft 365 Usage Analytics	92
MyAnalytics	94
Workplace Analytics	96
Summary	99
Thought experiment.	99
Thought experiment answer	100

Chapter 3 Understand security, compliance, privacy, and trust in Microsoft 365 101

Skill 3.1: Understand security and compliance concepts with Microsoft 365.	101
Risk management	103
Key security pillars	112

Skill 3.2: Understand identity protection and management	123
Identities	124
Authentication	132
Protecting documents	139
Skill 3.3: Understand the need for unified endpoint management, security usage scenarios and services	140
Microsoft 365 and Directory Services	143
SCCM and Intune co-management	148
Security usage scenarios	152
Addressing common threats	153
Skill 3.4: Understand the Service Trust Portal and Compliance Manager	156
Service Trust Portal	156
Compliance Manager	157
Cloud adoption showstoppers	158
Summary	164
Thought experiment	165
Thought experiment answer	166

Chapter 4 Understand Microsoft 365 pricing and support 167

Skill 4.1: Understand licensing options available in Microsoft 365	167
Microsoft 365 subscriptions	168
Selling Microsoft 365	177
Licensing Microsoft 365	185
Implementing best practices	187
Skill 4.2: Plan, predict, and compare pricing	188
Cost-benefit analysis for cloud vs. on-premises networks	188
Volume licensing	190
Billing and bill management	194
Skill 4.3: Describe support offerings for Microsoft 365 services	195
Service level agreements	195
Creating support requests	200
Determining service health	204

Skill 4.4: Understand the service lifecycle in Microsoft 365	208
Summary	212
Thought experiment.....	212
Thought experiment answer	213
<i>Index</i>	215

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

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.

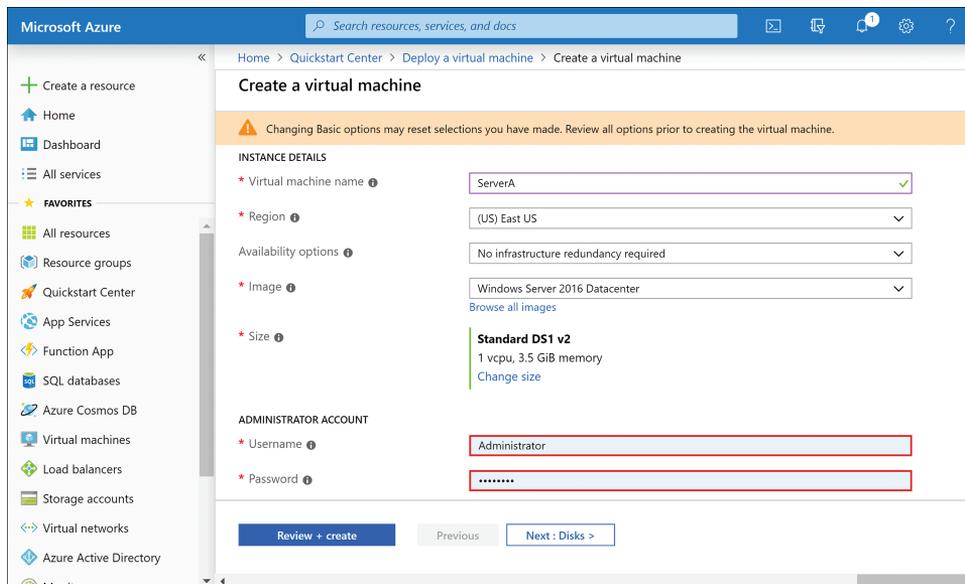


FIGURE 1-1 The Create a Virtual Machine interface in the Windows Azure Portal

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.

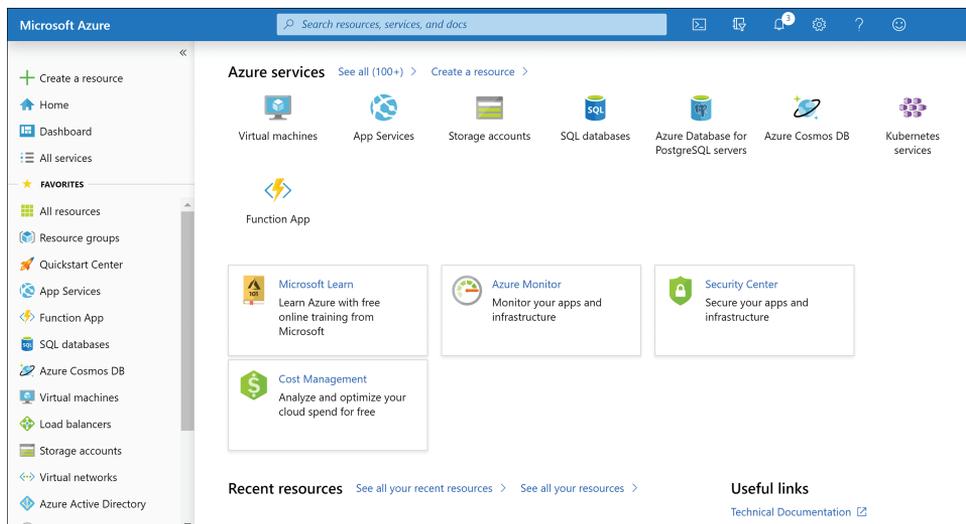


FIGURE 1-2 The management interface in the Windows Azure Portal

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.

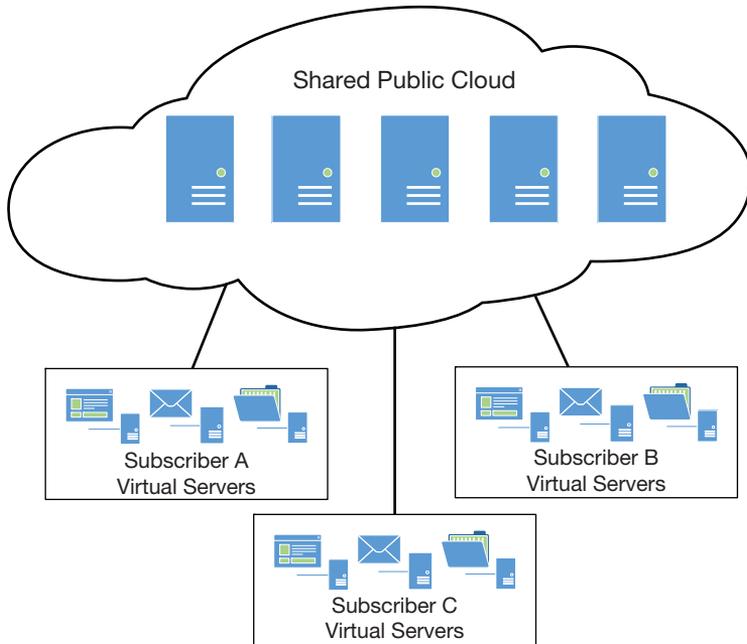


FIGURE 1-3 Virtual servers running in a shared public cloud

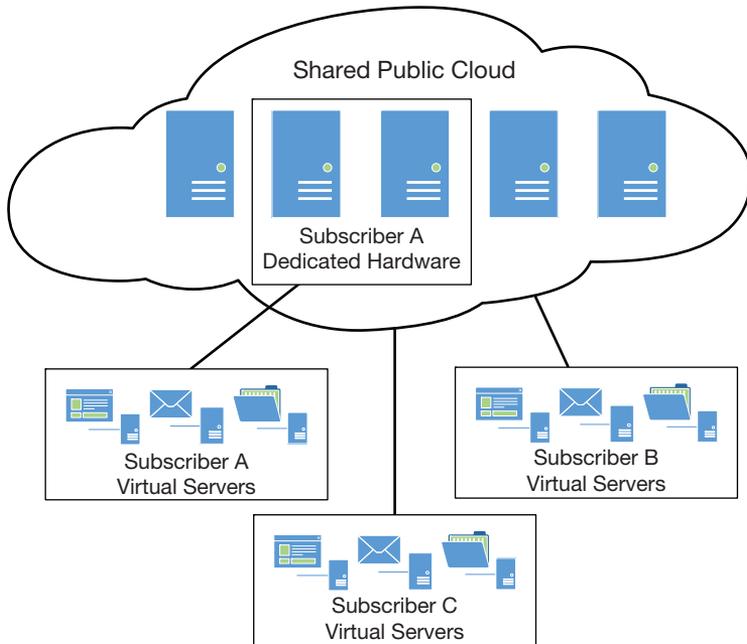


FIGURE 1-4 Virtual servers running in a dedicated public cloud

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

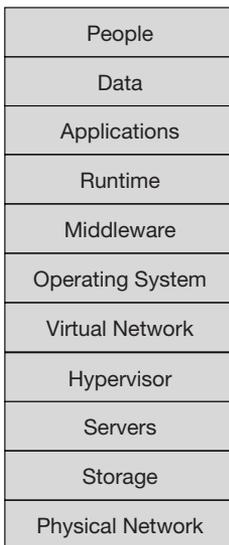


FIGURE 1-5 The layers of the cloud infrastructure

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.

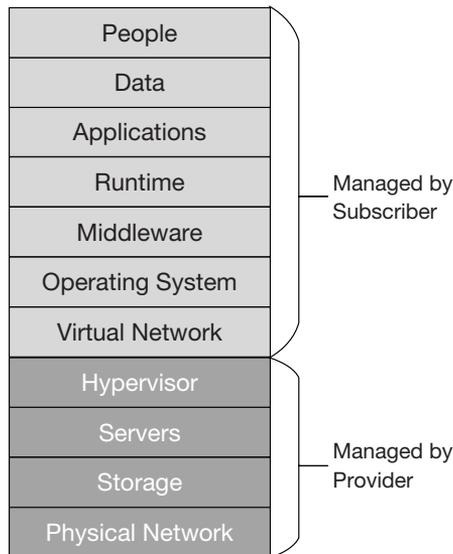


FIGURE 1-6 The shared responsibility model for IaaS

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.

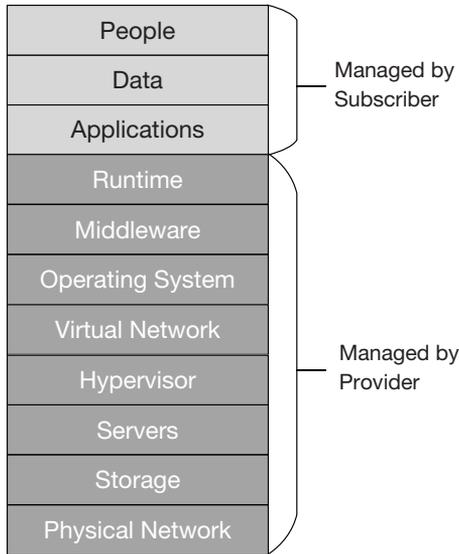


FIGURE 1-7 The shared responsibility model for PaaS

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.

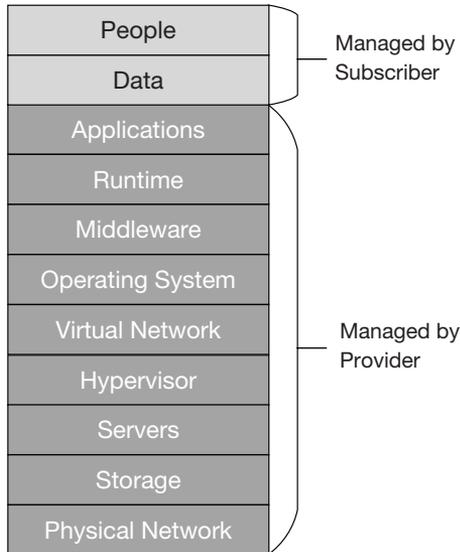


FIGURE 1-8 The shared responsibility model for SaaS

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

A

- A1/A3/A5 subscriptions. *See* Microsoft 365 Education
- Abnormal Behavior Machine Learning, 89
- access control lists (ACLs), 116–117
- Access from anywhere chart (Usage Analytics), 94
- ACLs (access control lists), 116–117
- activating applications, 178
- Active Directory. *See* AD DS (Active Directory Domain Services); AD FS (Active Directory Federation Services); Azure AD (Active Directory)
- AD DS (Active Directory Domain Services)
 - Active Directory Users and Computers, 125
 - compared to on-premises services, 40–41
 - features and capabilities of, 114–116, 146–148
 - password policies, 133–134
 - on-premises identities, 124–125
 - structure and hierarchy of, 146–148
 - user accounts, creating, 114–116
- AD FS (Active Directory Federation Services), 52, 131
- Add-on USL (user subscription license), 186
- Admin Center
 - Billing menu, 185, 194–195
 - Exchange Online settings, 26–27
 - features and capabilities of, 46–47
 - Health menu, 204–208
 - Licenses page, 185
 - New Group interface, 71
 - Purchase Services page, 185–186
 - Service Health page, 204–208
 - Support menu, 200–205
 - Try The New Admin Center option, 209
- Admin Centers menu (Admin Center), 47
- administration, 36
- Adoption chart (Usage Analytics), 94
- Advanced Threat Analytics (ATA), 33–34, 85, 88–91, 143
- Advanced Threat Protection (ATP), 22, 35, 143, 182
- advisories, 205
- AIP (Azure Information Protection), 33, 85, 105–106, 117–118, 139–143, 182
- alerts, 154
- analytics
 - Microsoft 365 Usage Analytics, 92–94
 - Microsoft ATA (Advanced Threat Analytics), 33–34, 85, 88–91, 143
 - MyAnalytics, 94–96
 - Workplace Analytics, 96–99
- anomalous logins, 89
- anticipation of threats, 111
- Application Proxy, 129
- Application Proxy Connector, 129
- application scans, 112
- Application Virtualization (App-V), 24, 64
- applications, defined, 13. *See also individual applications and services*
- App-V (Application Virtualization), 24, 64
 - architecture, cloud, 8
 - architecture, cloud services, 9–11
 - hybrid cloud, 12–13
 - private cloud, 11–12
- Assess phase (compliance), 184
- asset inventory, 104–106
- ATA (Advanced Threat Analytics), 33–34, 85, 88–91, 143
- ATP (Advanced Threat Protection), 22, 35, 143, 182
- audit reports, 156
- authentication
 - with Azure AD (Active Directory), 130–132
 - federated authentication, 131
 - pass-through authentication, 130
 - password authentication, 128
 - definition of, 113–114
 - multifactor
 - biometric scans, 134
 - cell phone-based, 134
 - definition of, 134
 - overview of, 132
 - password
 - Azure AD (Active Directory), 128
 - password changes, 153
 - password hash synchronization, 129
 - password policies, 133–134
 - SSPR (Self Service Password Reset), 52–53, 153
- authorization, 113–114
- automatic feature updates, 61
- Automatically Register New Windows 10 Domain Joined Devices
 - With Azure Active Directory Client setting, 150
- Autopilot, 24
- availability
 - definition of, 105
 - high, 108
- Azure. *See also* Azure AD (Active Directory); cloud services
 - AIP (Azure Information Protection), 33, 85, 105–106, 117–118, 139–143, 182
 - ATP (Advanced Threat Protection), 22, 35, 143, 182
 - management interface, 6
 - regions, 162

Azure, continued

Azure. *See also* Azure AD (Active Directory); cloud services, *continued*

- reliability mechanisms, 6
- Rights Management (RMS), 33
- RMS (Rights Management), 33
- Update Management, 16

Azure AD (Active Directory)

- Azure AD Connect, 142
- Azure Information Protection, 145
- cloud identities, 126–127
- features and capabilities of, 13, 32, 85, 143–145
- features and services of, 144–145
- hybrid identities
 - Application Proxy, 129
 - authentication, 130–132
 - definition of, 127
 - first synchronization, 128
 - SSO (single sign-on), 129
 - synchronization, 128–129
- Identity Protection, 136–139, 182
- licenses, 143
- MFA (multifactor authentication) in, 135–136
- on-premises services versus, 40–41
- Premium plans, 142, 144–145
- user accounts, creating, 114–116

B

barriers to cloud adoption, overcoming

- cost factors, 160–161
- data security concerns, 161
- data storage locations, 162
- overview of, 158–159
- performance latency, 159
- personnel requirements, 163
- sample scenario for, 165–166
- service provider selection, 159–160
- transition process, 163
- vendor lock-in, 160
- vendor robustness, 160

big switch transitions, 43

Billing Accounts option (Billing menu), 194

billing and bill management, 194–196

Billing menu (Admin Center), 47, 185, 194–195

Billing Notifications option (Billing menu), 194

Bills & Payments option (Billing menu), 194

biometric scans, 134

BranchCache, 45

Bring Your Own Device. *See* BYOD (Bring Your Own Device)

brute force attacks, 89

business subscriptions. *See* Microsoft 365 Business

BYOD (Bring Your Own Device), 57, 102, 120, 141

C

calendars, Exchange Online, 25, 68, 69

CapEx (capital expenditures), 188–190

CASB (cloud access security broker), 34

CBA (cost-benefit analysis), 188–190, 212–213

cell phone-based authentication, 134

CJIS (Criminal Justice Information Services) Policy, 173

classification of users, 109–111

Classification tools, 155

Click-to-Run, 64–66

client health monitoring, 150

Client Management Tools (CMTs), 140

cloud access security broker (CASB), 34

Cloud App Security, 34, 121–122, 143, 182

cloud identities, 126–127

cloud services. *See also* Azure

adoption barriers, overcoming

Contoso Corp. case study, 165–166

cost factors, 160–161

data security concerns, 161

data storage locations, 162

overview of, 158–159

performance latency, 159

personnel requirements, 163

service provider selection, 159–160

transition process, 163

vendor lock-in, 160

vendor robustness, 160

advantages of, 3

administration, 36

consolidation, 4–5

costs and monetary savings, 3–4, 35–36

deployment, 35

infrastructure, 7–8

manageability, 6

reliability, 5–6

sample scenario for, 19

scalability, 5

security, 7, 38

updates, 35

architecture of, 8

hybrid cloud, 12–13

private cloud, 11–12

public cloud, 9–11

concept of, 1–2

disadvantages of, 8

online resources, 15

service models

FaaS (Function as a Service), 17

IaaS (Infrastructure as a Service), 14–16

infrastructure layers, 13–14

PaaS (Platform as a Service), 16–17

SaaS (Software as a Service), 18

transitioning to, 163

Wingtip Toys case study, 19

Cloud Solution Provider (CSP) program, 190–193, 204

cmdlets

Enable-App, 24

New-ADUser, 125

Set-MsolPasswordPolicy, 133

Set-MsolUser, 133

CMTs (Client Management Tools), 140

Collaboration chart (Usage Analytics), 94

Collaboration pane (MyAnalytics), 95

- collaboration tools. *See also* EMS (Enterprise Mobility + Security)
 - analytics for
 - MyAnalytics, 95
 - Usage Analytics, 94
 - Workplace Analytics, 97
 - Exchange Online
 - Admin Center settings, 26–27
 - collaboration tools, 67–68
 - compared to Exchange Server, 39–40
 - features and capabilities of, 67–68
 - services, 25–26
 - subscription plans, 26
 - Microsoft Graph, 81–82
 - Microsoft Planner, 72, 76
 - Microsoft Stream, 75
 - Microsoft Teams, 29–31, 77, 180
 - Microsoft Yammer, 72
 - Office 365 groups, 69–73
 - Office 365 ProPlus, 62
 - OneDrive for Business, 62, 75, 180
 - overview of, 66–67, 179–181
 - Planner, 180
 - selection of, 78–80
 - SharePoint Online
 - features and capabilities of, 27–29, 73–74, 180
 - SharePoint Server compared to, 40
 - Skype for Business Online, 31, 77
 - Stream, 75, 180
 - Yammer, 74–75, 175, 180
 - Co-management Configuration Wizard, 150–151
 - co-management model, 44, 148–152
 - Communication chart (Usage Analytics), 94
 - compliance
 - Compliance Manager, 157–158
 - device compliance and configuration, 86–87
 - services for, 182–184
 - Compliance Manager, 157–158
 - conditional access, 149
 - confidentiality, 105
 - consolidation, cloud-based services and, 4–5
 - Contact Support pane, 202
 - Cotoso Corp. case study, 165–166
 - core services. *See also* EMS (Enterprise Mobility + Security)
 - advantages of
 - administration, 36
 - costs, 35–36
 - deployment, 35
 - security, 38
 - updates, 35
 - Exchange Online
 - Admin Center settings, 26–27
 - collaboration tools, 67–68
 - compared to Exchange Server, 39–40
 - EOP (Exchange Online Protection), 25
 - features and capabilities of, 180
 - services, 25–26
 - subscription plans, 26
 - Microsoft Teams, 29–31, 180
 - Office 365 ProPlus
 - deployment of, 54–56, 63–66
 - features of, 59–61, 178–179
 - Microsoft Office suite compared to, 38–39, 61–63
 - on-premises services versus
 - Active Directory, 40–41
 - Exchange, 39–40
 - hybrid service deployments, 40
 - Office, 38–39
 - SharePoint, 40
 - SharePoint Online
 - Admin Center, 72
 - collaboration with, 180
 - compared to SharePoint Server, 40
 - features and capabilities of, 27–29, 73–74, 180
 - SharePoint Server compared to, 40
 - Windows 10 Business, 25
 - Windows 10 Enterprise
 - deployment of, 53–54
 - features and capabilities of, 22
 - management, 24
 - security, 22
 - updates, 22–24
 - Core Services and Engineering Operations (CSEO) group, 103
 - cost models, 3–4, 35–36, 160–161
 - cost-benefit analysis (CBA), 188–190, 212–213
 - Create a Virtual Machine interface, 2
 - Criminal Justice Information Services (CJIS) Policy, 173
 - Critical (Sev A) severity level, 203
 - CSEO (Core Services and Engineering Operations) group, 103
 - CSP (Cloud Solution Provider) program, 190, 191–193, 204
 - Cybersecurity Reference Architecture, 155
- ## D
- Data Loss Prevention (DLP), 26, 59, 139–140, 182
 - data privacy standards, compliance with, 182–184
 - data storage locations, 162
 - database scans, 112
 - dedicated public cloud, 9
 - Defense Federal Acquisition Regulation Supplement (DFARS), 174
 - Delivery Optimization, 45
 - DEM (device enrollment manager), 58
 - deployment, 35
 - hybrid service, 40
 - Microsoft 365, 49–59
 - deployment strategies, 49–50
 - documentation for, 50
 - identity, 51–53
 - information protection, 58–59
 - MAM (Mobile Application Management), 57
 - MDM (Mobile Device Management), 56–58
 - networking, 51
 - Office 365 ProPlus, 54–56
 - Windows 10 Enterprise, 53–54
 - modern management processes, 43
 - Office 365 ProPlus, 63–66
 - applications to install, selecting, 63–64
 - Click-to-Run, 64–66

deployment, continued

deployment, *continued*

- customization options, 64–65
- Office 2016 and 2019 deployments, 66
- sample scenario for, 99–100
- self-deployment, 50
- Desktop Analytics, 23
- device enrollment manager (DEM), 58
- Device Health (Desktop Analytics), 23
- device protection, 178
 - BYOD (Bring Your Own Device), 57, 102, 120, 141
 - with Cloud App Security, 121–122
 - with MAM (Mobile Application Management), 121
 - with MDM (Mobile Device Management), 121
 - with Microsoft Intune, 119–120
 - overview of, 118–119
 - security usage scenarios, 152–153
- Devices menu (Admin Center), 46
- DFARS (Defense Federal Acquisition Regulation Supplement), 174
- digital estate, 102
- directory services. *See* AD DS (Active Directory Domain Services); Azure AD (Active Directory)
- disaster recovery, 108
- distribution lists, 67
- DLP (Data Loss Prevention), 26, 59, 117–118, 139–140
- document protection
 - ACLs (access control lists)
 - AIP (Azure Information Protection), 117–118
 - definition of, 116–117
 - DLP (Data Loss Prevention), 117–118
 - AIP (Azure Information Protection), 33, 105–106, 117–118, 139–140, 143
 - DLP (Data Loss Prevention), 26, 59, 117–118, 139–140
 - overview of, 116–118
- Documents & Resources (Service Trust Portal), 157
- Domain Services. *See* AD DS (Active Directory Domain Services)
- downtime, 198–199
- Driving Value phase of onboarding, 163
- dynamic distribution lists, 67

E

- E3/E5 subscriptions. *See* Microsoft 365 Enterprise
- EA (Enterprise Agreement), 190
- education subscriptions. *See* Microsoft 365 Education
- email hosting, 62
- EMM (enterprise mobility management), 141
- EMS (Enterprise Mobility + Security). *See also* Azure AD (Active Directory)
 - AIP (Azure Information Protection), 33, 85, 105–106, 117–118, 139–143, 182
 - ATA (Advanced Threat Analytics), 33–34, 143
 - ATP (Advanced Threat Protection), 22, 35, 143, 182
 - Cloud App Security, 34, 121–122, 143, 182
 - features and capabilities of, 31, 84–85, 142–143
 - Microsoft Intune
 - co-management feature, 148–152
 - device compliance and configuration, 86–87

- features and capabilities of, 32–33, 85, 107, 141–142, 182
- service architecture, 119–120
- obstacles to mobility and, 85
- Enable-App cmdlet, 24
- endpoints, UEM (unified endpoint management)
 - development of, 140–143
 - EMS (Enterprise Mobility + Security), 142–143
- Enterprise Agreement (EA), 190
- Enterprise Mobility + Security. *See* EMS (Enterprise Mobility + Security)
- enterprise mobility management (EMM), 141
- Enterprise Source Licensing Program, 191
- enterprise subscriptions. *See* Microsoft 365 Enterprise
- Envisioning phase of onboarding, 163
- EOP (Exchange Online Protection), 25
- Exchange Online
 - Admin Center settings, 26–27
 - collaboration tools, 67–68
 - EOP (Exchange Online Protection), 25
 - Exchange Server compared to, 39–40
 - features and capabilities of, 180
 - services, 25–26
 - subscription plans, 26
- Exchange Server, Exchange Online compared to, 39–40
- ExcludeApp, 64
- expenditures, capital versus operational, 188–190
- Express Updates, Windows 10, 45
- Extended Recovery indicator (Service Health), 206
- Extended Support, 209
- External collaboration metrics (Workplace Analytics), 97

F

- F1 subscriptions. *See* Microsoft 365 F1
- FaaS (Function as a Service), 17
- facial recognition, 134
- Fail-Over Rights, 191
- Family Educational Rights and Privacy Act (FERPA), 183
- FastTrack program, 49, 163, 203
- FBI, Criminal Justice Information Services (CJIS) Policy, 173
- Federal Information Security Modernization Act (FISMA), 182
- Federal Risk and Authorization Management Program (FedRAMP), 156, 174
- federated authentication, 131
- FERPA (Family Educational Rights and Privacy Act), 183
- fingerprint readers, 134
- first line workers, 170
- FISMA (Federal Information Security Modernization Act), 182
- Fixed Lifecycle Policy, 209
- Focus pane (MyAnalytics), 94
- folders, public, 68
- Forged PAC attacks, 88
- From SA USL (user subscription license), 186
- Full USL (user subscription license), 186
- Function as a Service (FaaS), 17

G

GA (General Availability) releases, 210
 Gateway (ATA), 90
 GDPR (General Data Protection Regulation), 156, 183
 Geography button (Microsoft Graph), 81
 Golden Ticket attacks, 88
 government subscriptions. *See* Microsoft 365 Government
 Gramm-Leach-Bliley Act (GLBA), 183
 Graph (Microsoft), 81–82
 groups
 Group Policy, 133–134
 group-by-group transition, 43
 Group-to-group queries (Workplace Analytics), 98
 modification of, 89
 Office 365, 69–73
 Groups menu (Admin Center), 46

H

hardware inventory, 106–108
 hardware requirements, 3
 hashes, 128–129
 Health Insurance Portability and Accountability Act (HIPAA), 11–12, 183
 Health menu (Admin Center), 47, 204–208
 High (Sev B) severity level, 203
 high availability, 108
 HIPAA (Health Insurance Portability and Accountability Act), 11–12, 183
 horizontal scaling, 5
 host scans, 112
 Hunting tools, 155
 Hybrid Azure AD, 149
 hybrid cloud, 12–13
 hybrid identities, 127–132
 in Azure AD (Active Directory)
 Application Proxy, 129
 authentication, 130–132
 passwords, 128
 SSO (single sign-on), 129
 definition of, 127
 first synchronization, 128–129
 hybrid service deployments, 40
 hypervisors, 14

I

IaaS (Infrastructure as a Service), 14–16
 Identity phase (deployment), 51–53
 identity protection
 in AD DS (Active Directory Domain Services)
 hybrid identities, 127–132
 on-premises identities, 124–125
 user accounts, creating, 114–116

authentication
 definition of, 113–114
 multifactor, 134–136
 overview of, 132
 password, 128–129, 133–134
 authorization, 113–114
 in Azure AD (Active Directory), 13, 114–116
 Application Proxy, 129
 authentication, 130–132
 cloud identities, 126–127
 hybrid identities, 127–132
 Identity Protection, 136–139, 182
 passwords, 128
 SSO (single sign-on), 129
 user accounts, creating, 114–116
 cloud identities, 126–127
 hybrid identities, 127–132
 modern management processes, 43
 overview of, 113–116, 123, 170
 password authentication
 in Azure AD (Active Directory), 128
 password changes, 153
 password hash synchronization, 129
 password policies, 133–134
 SSPR (Self Service Password Reset), 52–53, 153
 on-premise identities, 124–125
 risk levels, 136–139
 Windows Hello for Business, 116
 In Development release status, 210
 incidents, 205
 indirect providers, 193
 indirect resellers, 193
 Individual service usage chart (Usage Analytics), 94
 Industries & Regions (Service Trust Portal), 157
 infected devices, 153
 information protection, 58–59, 170
 infrastructure, cloud services, 7–8
 Infrastructure as a Service (IaaS), 14–16
 Insert Data button (Microsoft Graph), 82
 Insert From File pane (Microsoft Graph), 81
 installation. *See* deployment
 integrity, data, 105
 Internal networks metrics (Workplace Analytics), 97
 International Organization for Standardization (ISO), 156
 International Traffic in Arms Regulations (ITAR), 173–174
 international users, 173
 Internet of Things (IoT), 141–142
 Intune. *See* Microsoft Intune
 inventory
 assets, 104–106
 hardware, 106–108
 Investigating indicator (Service Health), 206
 Investigation Suspended indicator (Service Health), 206
 IoT (Internet of Things), 141–142
 ISO (International Organization for Standardization), 156
 ITAR (International Traffic in Arms Regulations), 173–174

J-K-L

Kerberos, 41, 125

KMS (Key Management Service), 66, 178

labels

retention, 58

sensitivity, 58–59

lateral movement, 89

Launched release status, 210

Licenses option (Billing menu), 194

Licenses page, 185

licensing options

Azure AD (Active Directory), 143

basic components, 167–168

best practices, 187

CBA (cost-benefit analysis) of, 188–190, 212–213

feature comparison, 171–173

Microsoft 365 Business, 168–169, 171–173

Microsoft 365 Education, 174–177

Microsoft 365 Enterprise, 169–173

Microsoft 365 F1, 170–173

Microsoft 365 Government, 173–174

Office 365 ProPlus, 61

USL (user subscription license), 185–186

volume licensing

CSP (Cloud Solution Provider) program, 191–193

licensing agreement types, 190

Software Assurance, 190–191

support, 203

lifecycle policies, 208–211

lists, distribution, 67

loss of devices, 152

LTSB (Long Term Servicing Branch), 24

LTSC (Long Term Servicing Channel), 24

M

mailboxes, Exchange Online, 25, 68–69

mail-enabled security groups, 68

Mainstream Support, 209

MAKs (Multiple Activation Keys), 66, 178

malicious replications, 88

MAM (Mobile Application Management), 57, 121, 152

manageability, cloud-based services, 6

management

modern. *See also* Admin Center

concept of, 42–43

configuration, 43

deployment, 43

identity, 43

Microsoft deployment and release model, 49–59

Office 365 portal, 47–49

traditional management compared to, 42

transitioning to, 43–44

updates, 43

WaaS (Windows as a Service), 44–45

workloads and scenarios, 59

traditional approach to, 42

Windows 10 Enterprise, 24

Management and coaching metrics (Workplace Analytics), 97

MDM (Mobile Device Management), 56–58, 121, 140, 152

MDOP (Microsoft Desktop Optimization Pack), 191

Meeting queries (Workplace Analytics), 98

Meetings overview metrics (Workplace Analytics), 97

@mentions, 81

Message Center page, 207–208

messaging

Exchange Online

Admin Center settings, 26–27

services, 25–26

subscription plans, 26

Microsoft Teams, 29–31, 180

MFA (multifactor authentication)

Azure AD (Active Directory) and, 135–136

biometric scans, 134

cell phone-based, 134

definition of, 134

overview of, 52

Microsoft 365 Business, 168–169, 171–173

Microsoft 365 DoD, 174

Microsoft 365 Education, 174–177

Microsoft 365 Enterprise, 169–173

Microsoft 365 F1, 170–173

Microsoft 365 Government, 173–174

Microsoft 365 Roadmap, 210–211

Microsoft 365 U.S. Government Community (GCC), 174

Microsoft 365 U.S. Government Community (GCC) High, 174

Microsoft 365 Usage Analytics, 92–94

Microsoft Application Virtualization (App-V), 24, 64

Microsoft ATA (Advanced Threat Analytics). *See* ATA (Advanced Threat Analytics)

Microsoft Azure. *See* Azure

Microsoft CSEO (Core Services and Engineering Operations) group, 103

Microsoft Cybersecurity Reference Architecture, 155

Microsoft Defender Advanced Threat Protection (ATP), 22

Microsoft Desktop Optimization Pack (MDOP), 191

Microsoft FastTrack. *See* FastTrack program

Microsoft Global Network, 108

Microsoft Graph, 81–82

Microsoft Intelligent Security Graph, 155

Microsoft Intune

co-management feature, 148–152

device compliance and configuration, 86–87

features and capabilities of, 32–33, 85, 107, 141–142, 182

Intune for Education, 176

service architecture, 119–120

Microsoft Office 365. *See* Office 365 ProPlus

Microsoft Office suite, 38–39, 61–63

Microsoft Planner, 72, 76, 180

Microsoft Products and Services Agreement (MPSA), 190

Microsoft Professional Support, 204

Microsoft Services Hub, 204–205

Microsoft Stream, 75, 180

Microsoft Teams, 29–31, 77, 180

Microsoft Threat Protection, 153–155

Microsoft Unified Support, 204

Microsoft User Experience Virtualization (UE-V), 24

Microsoft Volume Licensing Service Level Agreement for Microsoft Online Services, 198–200

Microsoft Yammer. *See* Yammer
 middleware, 13
 Minecraft Education Edition with Code Builder, 175
 Mobile Application Management (MAM), 57, 121, 152
 mobile apps, 178
 Mobile Device Management (MDM), 56–58, 121, 140, 152
 mobile devices. *See* device protection
 mobility. *See* EMS (Enterprise Mobility + Security)
 Modern Lifecycle Policy, 209
 modern management. *See also* Admin Center
 concept of, 42–43
 configuration, 43
 deployment, 43
 identity, 43
 Microsoft deployment and release model, 49–59
 deployment strategies, 49–50
 documentation for, 50
 identity, 51–53
 information protection, 58–59
 MAM (Mobile Application Management), 57, 121, 152
 MDM (Mobile Device Management), 56–58, 121, 140, 152
 networking, 51
 Office 365 ProPlus, 54–56
 Windows 10 Enterprise, 53–54
 Office 365 portal, 47–49
 traditional management compared to, 42
 transitioning to, 43–44
 updates, 43
 WaaS (Windows as a Service), 44–45
 workloads and scenarios, 59
 monitoring
 client health, 150
 service health, 204–208
 Monthly Channel, 56
 Monthly Channel (Targeted), 56
 MPSA (Microsoft Products and Services Agreement), 190
 multifactor authentication. *See* MFA (multifactor authentication)
 Multiple Activation Keys (MAKs), 66, 178
 multiple master replication, 124–125
 My Library (Service Trust Portal), 157
 MyAnalytics, 94–96

N

National Institute of Standards and Technology (NIST), 156
 Need Help? pane, 201–202
 Network pane (MyAnalytics), 95
 Networking phase (deployment), 51
 networks
 requirements for, 3–4
 scans of, 112
 security model, 118–119
 VPNs (virtual private networks), authentication over, 115
 New Object - User dialog box, 125
 New Version Rights, 191
 New-ADUser cmdlet, 125
 NIST (National Institute of Standards and Technology), 156

Non-critical (Sev C) severity level, 203
 notebooks, OneNote, 70, 175
 NT LAN Manager (NTLM), 41

O

OAuth (Open Authorization), 41, 127
 ODT (Office Deployment Tool), 55, 63–65
 Office 365 groups, 69–73
 Office 365 portal, 47–49
 Office 365 ProPlus
 deployment of, 54–56, 63–66
 applications to install, selecting, 63–64
 Click-to-Run, 64–66
 customization options, 64–65
 Office 2016 and 2019 deployments, 66
 features of, 59–61, 178–179
 Microsoft Office suite compared to, 38–39, 61–63
 Office activation chart (Usage Analytics), 94
 Office Deployment Tool (ODT), 55, 63–65
 Office Lens, 176
 Onboarding phase of onboarding, 163
 OneDrive for Business, 62, 75, 180
 OneNote notebooks, 70, 175
 one-time passwords (OTPs), 135–136
 Open Authorization (OAuth), 41, 127
 Operating System Upgrade Package option, 53
 operating systems
 defined, 14
 support for, 61–62
 OpEx (operational expenditures), 188–190
 OTPs (one-time passwords), 135–136
 Overpass-the-Hash attacks, 88

P

PaaS (Platform as a Service), 16–17
 PAC (Privileged Attribute Certificate), 88
 Pass-the-Hash (PtH) attacks, 88
 Pass-the-Ticket (PtT) attacks, 88
 pass-through authentication, 130
 password authentication
 Azure AD (Active Directory), 128
 OTPs (one-time passwords), 135–136
 password changes, 153
 password hash synchronization, 129
 password policies, 133–134
 password sharing, 89
 SSPR (Self Service Password Reset), 52–53, 153
 Payment Methods option (Billing menu), 194
 PBX (private branch exchange), 30
 performance latency, 159
 persistence (attacks), 89
 Person queries (Workplace Analytics), 98

Personal Information Protection and Electronic Documents Act (PIPEDA)

Personal Information Protection and Electronic Documents Act (PIPEDA), 183

personnel requirements, 4, 163

Person-to-group queries (Workplace Analytics), 98

physical networks, 14

physical security, 108

PIPEDA (Personal Information Protection and Electronic Documents Act), 183

Planner, 72, 76, 180

Planning Services, 190

Platform as a Service (PaaS), 16–17

policies

- Microsoft 365 security center, 155
- password, 133–134
- threat management, 59

Post-Incident Report Published indicator (Service Health), 206

Power BI. *See* Usage Analytics

PowerShell cmdlets. *See* cmdlets

pricing and support. *See also* subscriptions

- basic components, 167–168
- billing and bill management, 194–196
- key selling points, 177–178
 - collaboration, 179–181
 - compliance, 182–184
 - productivity, 178–179
 - security, 181–182

Office 365 ProPlus, 62

- service health, monitoring, 204–208
- service lifecycle policies, 208–211

SLAs (service level agreements), 195–200

- limitations of, 197
 - Microsoft Volume Licensing Service Level Agreement for Microsoft Online Services*, 198–200
- negotiating, 195–196

support requests, creating, 200–205

- administrator and support team responsibilities, 200–201
- alternative support methods, 203–205
 - Contact Support pane, 202
 - Need Help? pane, 201–202
 - support severity levels, 203
 - support tickets, viewing, 203
 - supported issues, 202–203

USL (user subscription license), 185–186

volume licensing

- CSP (Cloud Solution Provider) program, 191–193
- licensing agreement types, 190
- Software Assurance, 190–191
- support, 203

private branch exchange (PBX), 30

private cloud, 11–12

Private preview, 209

Privileged Attribute Certificate (PAC), 88

Product usage chart (Usage Analytics), 94

productivity services, 178–179

Products & Services option (Billing menu), 194

Protect phase (compliance), 184

PSTN (Public Switched Telephone Network), 30

PtH (Pass-the-Hash) attacks, 88

PtT (Pass-the-Ticket) attacks, 88

public cloud, 9–11

public folders, 68

Public preview, 209

Public Switched Telephone Network (PSTN), 30

Purchase Services option (Billing menu), 194

Purchase Services page, 185–186

Q-R

quarterly uptime percentages, 199–200

Quick Analysis button (Microsoft Graph), 82

reconnaissance, 89

reduced functionality mode (Office 365 ProPlus), 62

redundancy, 4

regions, Microsoft Azure, 162

release cycles, 209–211

reliability of cloud-based services, 5–6

remote actions, 149

remote execution, 89

reports

- audit, 156
 - Microsoft 365 security center, 155
- Reports menu (Admin Center), 47

Resources

- Admin Center, 47
- Service Trust Portal, 157

Respond phase (compliance), 184

Restoring Service indicator (Service Health), 206

retention labels, 58

Rights Management (RMS), 33

risk management

- anticipation of threats, 111
- asset inventory, 104–106
- definition of, 103
- hardware inventory, 106–108
- identity protection risk levels, 136–139
- ongoing nature of, 112
- overview of, 103
- user classification, 109–111
- vulnerability assessments, 112

RMS (Rights Management), 33

Roadmap, 210–211

Rolling Out release status, 210

runtime, 13

S

SaaS (Software as a Service), 18

SAML (Security Assertion Markup Language), 41

scalability of cloud-based services, 5

scans

- application, 112
- biometric, 134
- database, 112
- host, 112
- network, 112

- SCCM (System Center Configuration Manager)
 - co-management feature, 148–152
 - features and capabilities of, 23, 140, 142
 - features of, 148–149
 - in-place upgrade to Windows 10 Enterprise, 53–54
 - Office 365 ProPlus deployment, 63
 - Office 365 ProPlus installation, 54
- SDS (School Data Sync), 175
- seamless single sign-on, 129
- secure score, 155
- security, 22. *See also* identity protection
 - ATA (Advanced Threat Analytics), 33–34, 85, 88–91, 143
 - ATP (Advanced Threat Protection), 22, 35, 143, 182
 - attack types, 88–89
 - challenges of, 101–103
 - Compliance Manager, 157–158
 - device protection, 178
 - BYOD (Bring Your Own Device), 57, 102, 120, 141
 - with Cloud App Security, 121–122
 - with MAM (Mobile Application Management), 121
 - with MDM (Mobile Device Management), 121
 - with Microsoft Intune, 119–120
 - overview of, 118–122
 - security usage scenarios, 152–153
 - document protection
 - ACEs (access control entries), 116–117
 - ACLs (access control lists), 116–117
 - AIP (Azure Information Protection), 33, 105–106, 117–118, 139–140, 143
 - DLP (Data Loss Prevention), 117–118, 139–140
 - overview of, 116–118
 - Microsoft 365 Business, 168–169
 - network security model, 118–119
 - overview of, 7, 38
 - physical, 108
 - risk management
 - anticipation of threats, 111
 - asset inventory, 104–106
 - definition of, 103
 - hardware inventory, 106–108
 - ongoing nature of, 112
 - overview of, 103
 - user classification, 109–111
 - vulnerability assessments, 112
 - SCCM (System Center Configuration Manager), 140, 142, 148–152
 - security center, 154–155
 - security principals, 113
 - security services, 181–182
 - STP (Service Trust Portal), 156–157
 - UEM (unified endpoint management), 140–143
 - usage scenarios, 152–153
- Security Assertion Markup Language (SAML), 41
- Self Service Password Reset (SSPR), 52–53, 153
- self-deployment, 50
- Semi-annual Channel
 - Office 365 ProPlus, 56
 - Windows 10, 44
- Semi-annual Channel (Targeted), 56
- Send button (Microsoft Graph), 81
- sensitivity labels, 58–59
- Server Disaster Recovery Rights, 191
- serverless computing, 17
- service credits, 199
- Service Degradation indicator (Service Health), 206
- Service Health page, 204–208
- Service Interruption indicator (Service Health), 206
- service level agreements. *See* SLAs (service level agreements)
- service lifecycle policies, 208–211
- service models (cloud services)
 - FaaS (Function as a Service), 17
 - IaaS (Infrastructure as a Service), 14–16
 - infrastructure layers, 13–14
 - PaaS (Platform as a Service), 16–17
 - SaaS (Software as a Service), 18
- Service Organization Controls (SOC), 156
- service providers
 - robustness of, 160
 - selection of, 159–160
 - vendor lock-in, 160
- Service Restored indicator (Service Health), 206
- Service Trust Portal (STP), 156–157
- Set Up School PCs app, 175
- Set-MsolPasswordPolicy cmdlet, 133
- Set-MsolUser cmdlet, 133
- Settings menu (Admin Center), 47
- Setup menu (Admin Center), 47
- severity levels support, 203
- Shadow IT, 34
- shared mailboxes, 68–69
- shared public cloud, 9
- SharePoint Online
 - Admin Center, 72
 - features and capabilities of, 27–29, 73–74, 180
 - SharePoint Server compared to, 40
- sign-in risk, 137
- single master replication, 126–127
- single sign-on (SSO), 129
- six nines contract, 4
- Sizing Tool (ATA), 90
- Skype for Business Online, 31, 77
- SLAs (service level agreements), 159, 195–200
 - limitations of, 197
 - Microsoft Volume Licensing Service Level Agreement for Microsoft Online Services*, 198–200
 - negotiating, 195–196
- SOC (Service Organization Controls), 156
- Software as a Service (SaaS), 18
- Software Assurance, 190–191
- software licenses, 3
- spread payments, 191
- SSPR (Self Service Password Reset), 52–53, 153
- Status indicators (Service Health), 206
- Step-up USL (user subscription license), 186
- storage, 14, 178
- Storage use chart (Usage Analytics), 94
- STP (Service Trust Portal), 156–157
- Stream, 75, 180
- subscriptions, 168
 - Azure AD (Active Directory), 145
 - best practices for, 187
 - CBA (cost-benefit analysis) of, 188–190, 212–213

subscriptions, continued

subscriptions, *continued*

- Exchange Online, 26
- feature comparison, 171–173
- Microsoft 365 Business, 168–169, 171–173
- Microsoft 365 Education, 174–177
- Microsoft 365 Enterprise, 169–173
- Microsoft 365 F1, 170–173
- Microsoft 365 Government, 173–174
- volume licensing
 - CSP (Cloud Solution Provider) program, 191–193
 - licensing agreement types, 190
 - Software Assurance, 190–191
 - support, 203
- support. *See* pricing and support
- Support menu (Admin Center), 47, 200–205
- synchronization
 - Azure AD (Active Directory), 128–129
 - device data, 153
- System Center Configuration Manager. *See* SCCM (System Center Configuration Manager)
- Systems Management Server, 148

T

- Take a Test app, 175
- TAMs (technical account managers), 204
- TCO (total cost of ownership)
 - calculating, 188–190
 - cost models, comparison of, 160–161
 - sample software licensing scenario, 212–213
- Teams (Microsoft), 29–31, 77, 180
- Teams collaboration metrics (Workplace Analytics), 97
- technical account managers (TAMs), 204
- threats. *See* security
- three nines contract, 4
- tiered cloud service model, 16–17
- total cost of ownership. *See* TCO (total cost of ownership)
- training vouchers, 191
- transitioning to cloud, 163
- Trust Center (Service Trust Portal), 157
- Try The New Admin Center option, 209
- two nines contract, 4

U

- UEM (unified endpoint management), 140–143
- UE-V (Microsoft User Experience Virtualization), 24
- UM (Unified Messaging), 25
- Unified Messaging (UM), 25
- Update Management (Azure), 16
- updates/upgrades, 3, 22–24, 35, 43, 178
- Upgrade Readiness (Desktop Analytics), 23
- U.S. Government regions, 162
- Usage Analytics, 92–94
- usage scenarios, security, 152–153
- user classification, 109–111
- user risk, 137

- user subscription license (USL), 185–186
- Users menu (Admin Center), 46
- USL (user subscription license), 185–186

V

- VDA (Windows Virtual Desktop Access Rights), 191
- vendors
 - robustness of, 160
 - selection of, 159–160
 - vendor lock-in, 160
- vertical scaling, 5
- View Service Requests option (Support menu), 203
- VMs (virtual machines), 4–5
- VoIP (Voice over IP), 30
- volume licensing
 - CSP (Cloud Solution Provider) program, 191–193
 - licensing agreement types, 190
 - Software Assurance, 190–191
 - support, 203
- VPNs (virtual private networks), authentication over, 115
- vulnerability assessments, 112

W-X-Y-Z

- WaaS (Windows as a Service), 44–45
- WDAC (Windows Defender Application Control), 22
- Week in the life metrics (Workplace Analytics), 96
- Wellbeing pane (MyAnalytics), 95
- Windows 10 Business, 25
- Windows 10 Enterprise
 - deployment of, 53–54
 - features and capabilities of, 22
 - management, 24
 - security, 22
 - updates, 22–24
- Windows as a Service (WaaS), 44–45
- Windows Autopilot, 24, 150, 168
- Windows Defender
 - Application Guard, 22
 - ATP (Advanced Threat Protection), 22
 - WDAC (Windows Defender Application Control), 22
- Windows Hello for Business, 116, 134
- Windows Information Protection (WIP), 59
- Windows Insider Channel, 44
- Windows Server Update Service (WSUS), 23
- Windows Thin PC, 191
- Windows to Go Use Rights, 191
- Windows Update for Business, 23
- Windows Virtual Desktop Access Rights (VDA), 191
- WIP (Windows Information Protection), 59
- wireless network scans, 112
- wizards, Co-management Configuration, 150–151
- Workplace Analytics, 96–99
- WSUS (Windows Server Update Service), 23

- Yammer, 72, 74–75, 175, 180