# **Module 1**

# **Introduction to Cloud Computing**

|  |
| --- |
| At a Glance |

## Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

## Overview

Only a few years ago, the term “cloud computing” seemed more like a marketing gimmick than a legitimate evolution in technology. Today, it’s become clear that cloud computing is here to stay and, within a few years, will likely be as much a standard mode of operation for most data centers as virtualization is today. This means that, as an IT professional, you have a responsibility to understand how to use the cloud and how to integrate those tasks within your job role in whatever specialty area you pursue. Furthermore, cloud technicians must understand a great deal about the context of services provided through the cloud, including business goals and processes, software development processes, infrastructure concepts, and necessary adaptations to security strategies specific to cloud-hosted resources. This course prepares you to take the CompTIA Cloud+ CV0-002 exam, which is a vendor-neutral exam covering a broad array of foundational and intermediate cloud computing concepts within the context of an organization’s entire IT system.

## Module Objectives

After reading this module and completing the exercises, the student will be able to:

* Evaluate reasons for pursuing a Cloud+ certification.
* Explore defining characteristics of cloud computing.
* Determine new skill sets required for working in the cloud.
* Identify various cloud deployment models, including public cloud, private cloud, hybrid cloud, multi-cloud, and community cloud.
* Analyze security concerns specific to each cloud deployment model.
* Identify various cloud service models, including SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).
* Analyze security concerns specific to each cloud service model.
* Recognize popular cloud service providers.
* Evaluate common cloud service types, including compute, storage, network, and security services.
* Analyze security concerns specific to each cloud service model.
* Anticipate common cloud issues.
* Explain the troubleshooting steps.
* Identify helpful preventive measures.

## Teaching Tips

**Module 1 Scenario**

1. Summarize the introductory case study scenario presented in this module.
2. Review the ways the school in the scenario can save money by migrating to the cloud.
3. Review the action list questions identified by the team to commence their cloud conversion project. Use them to introduce the purpose of the course.

**Section 1-1 Characteristics of Cloud Computing**

1. Review the section learning objectives students should understand after completing this section:

* Evaluate reasons for pursuing a Cloud+ certification.
* Explore defining characteristics of cloud computing.
* Determine new skill sets required for working in the cloud.

**Reading 1-1-1 Cloud Computing Certifications**

1. Explain the history of the CompTIA Cloud+ certification. Be sure to emphasize that the newest version of the Cloud+ certification, CV0-002, became available to the public in early 2018.
2. Use Figure 1-1 to illustrate how the Cloud+ certification builds upon the knowledge gained from the CompTIA A+, Network+, and Security+ exams. Emphasize that Cloud+ takes the foundational concepts covered in these earlier exams and applies that information to a cloud environment.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Mention that while the CompTIA A+, Network+, and Security+ certifications are not required for the Cloud+ exam, the knowledge covered by their objectives is directly relevant to the skills required of a Cloud+ certified technician. |

***CompTIA Cloud+ Certification***

1. Explain what “vendor neutral” means and how this characteristic sets the Cloud+ exam apart from other certifications.
2. Review four reasons for pursuing the Cloud+ certification.

* Prepare for a new job or a promotion that likely will include assuming responsibility for interacting with an organization’s existing cloud services.
* Build a foundational understanding of cloud computing in preparation for vendor-specific cloud certifications.
* Complement certifications in other specialty areas (such as infrastructure, security, database management, or programming).
* Develop a big-picture perspective of cloud computing technologies, major players, and industry expectations in preparation for choosing vendors and migrating on-premises (“on-prem” for short) services to the cloud.

***Other Cloud Certifications***

1. Describe other vendor-neutral certifications.

* CCSP (Certified Cloud Security Professional) certification from CSA (Cloud Security Alliance)
* (ISC)2, which is the International Information System Security Certification Consortium

1. Describe vendor-specific cloud certifications.

* Amazon Web Services (AWS) - A subsidiary of Amazon that is headquartered in Seattle, WA, and provides extensive cloud computing services to businesses and individuals.
* Azure - Microsoft’s cloud computing platform, designed for optimal compatibility with existing Microsoft products.
* Google Cloud Platform (GCP) - Google’s collection of public cloud computing services, designed to take advantage of Google’s own extensive physical infrastructure around the globe.
* Cisco’s CCNA Cloud
* VMware Certified Professional 7 – Cloud Management and Automation (VCP7-CMA) cert

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | 5 Best Cloud Certifications 2019: <https://www.businessnewsdaily.com/10748-top-5-cloud-certifications.html> |

**Reading 1-1-2 What Is Cloud Computing?**

1. Introduce the NIST (National Institute of Standards and Technology) agency’s five essential characteristics of cloud computing. Refer to Figure 1-2 during the discussion.
2. Introduce the cloud computing characteristic of on-demand self-service, explaining that it refers to the ability of the service subscriber or other users to add, adjust, or remove cloud services at any time.
3. Introduce the cloud computing characteristic of broad network access, explaining that it refers to the ability to connect to cloud-hosted resources from anywhere on the Internet using a variety of device types. Compare broad network access to VPN access used by traditional network resources.
4. Introduce the cloud computing characteristic of resource pooling, explaining that it refers to the availability of physical and virtual cloud resources to multiple subscribers according to consumer demand without regard to geographic location.
5. Introduce the cloud computing characteristic of rapid elasticity, explaining that it refers to the ability to scale cloud resources up or down according to demand.
6. Introduce the cloud computing characteristic of being a measured service, explaining that it refers to the ability to charge for cloud resource usage according to an incremented schedule based on the type of service being used.
7. Identify and describe additional cloud computing characteristics and benefits for cloud providers:

* Self-patching/self-healing infrastructure
* Adaptive, intelligent security
* Cross-platform

1. Discuss the many reasons an organization might cite for transitioning to a cloud environment.
2. Explain that with mergers, acquisitions, and divestitures, cloud services that support the business will in turn need to be adapted, migrated, or replaced.

**Reading 1-1-3 What Do I Need to Know?**

1. Emphasize that IT professionals must continuously acquire new skills to stay relevant as cloud computing technologies emerge and mature.
2. Explain how security skills must be updated as cloud technologies emerge and mature.
3. Review other specialty areas that must be updated as cloud technologies emerge and mature.

* Business goals and the business processes and workflows that affect every department within an organization
* Software development processes
* Infrastructure concepts, skills, and tools
* Security vulnerabilities, technologies, and best practices that are specific to cloud-hosted resources

1. Emphasize how process automation is often a big cloud migration advantage. Describe how orchestration refers to the design, development, and optimization of automation processes.
2. Explain how lifelong learning ultimately requires the ability to teach oneself.

Section 1-2 Cloud Deployment Models

1. Review the section learning objectives students should understand after completing this section:

* Identify various cloud deployment models, including public cloud, private cloud, hybrid cloud, multi-cloud, and community cloud.
* Analyze security concerns specific to each cloud deployment model.

**Reading 1-2-1 Cloud Deployment Models**

1. Compare the advantages and disadvantages of using someone else’s hardware to host applications, data, and network infrastructures.
2. Emphasize how cloud computing simultaneously increases convenience while reducing an organization’s control of the hardware supporting their IT resources. Point out that security concerns arise in this situation.

**Reading 1-2-2 Public Cloud**

1. Use Figure 1-4 to illustrate a public cloud deployment model in which shared and flexible data storage, applications, or services are managed centrally by service providers. Emphasize that hardware resources managed by the cloud service provider (CSP) are not accessible by the customer.
2. Explain the security implications from both the CSP and customer points of view, focusing on the responsibility for data security.
3. Review the CSP’s industry certifications and available audit compliance reports to assist in ensuring the security of a public cloud:

* ISO/IEC 27001
* SSAE 18
* PCI DSS
* HIPPA
* GDPR

1. Introduce the SLA (service level agreement) as a contract defining service standards a telecommunications company promises to meet for its customer and options for recourse should those service levels not be met. Explain the importance of reviewing the CSP’s SLA for security standards.
2. Describe how a consumer should go about investigating the CSP’s security measures by asking questions regarding the handling of data leakage between tenants, use of third-party vendors, and measures in place to ensure those organizations’ compliance with standards and compliance measures.
3. Explain the importance of understanding CSP recommendations and requirements for each organization’s security measures.

**Reading 1-2-3 Private Cloud**

1. Explain how a private cloud represents a deployment model in which flexible data storage, applications, or services are managed centrally by an organization or service provider on hardware dedicated to that one organization.
2. Review the security implications within a private cloud.
3. Compare a private cloud hosted on-prem to the traditional data center that most organizations already have.
4. Explain how a cloud API (application programming interface) layer of communication managed by comprehensive virtualization software allows a cloud to be abstracted from the physical hardware in the data center.
5. Use Figure 1-5 to illustrate the use of an on-prem data center that is running a private cloud.
6. Discuss reasons why private cloud security requires more of a traditional approach to securing a network perimeter.
7. Remind students to implement security measures that do not rely solely on having a secure boundary around network resources. Provide examples, which might include thorough and secure data encryption, host firewalls, internal network monitoring, and both internal and external access controls.
8. Remind students to secure the virtual environment, hypervisor, VMs, and physical hosts.

**Reading 1-2-4 Hybrid Cloud**

1. Explain how a hybrid cloud represents a deployment model in which both private and public clouds or both cloud-based and on-prem services are used simultaneously.
2. Use Figure 1-6 to illustrate the hybrid cloud’s mix of both public and private cloud components where those components and services interact with each other in a direct and seamless manner.
3. Describe the different ways an organization might move applications and services to the hybrid cloud.
4. Explain why a hybrid cloud model is the most common cloud deployment.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | For more information on public, private, and hybrid clouds, see: <https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/> |

**Reading 1-2-5 Multi-Cloud**

1. Use Figure 1-7 to illustrate how a multi-cloud model involves using cloud services from multiple vendors at one time.
2. Provide examples of how a multi-cloud model involves multiple CSPs to custom build a cloud best suited to the organization’s needs.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Emphasize that the rise in popularity of hybrid and multi-clouds necessitates an expansion of skills for IT professionals. No longer is it sufficient to develop expertise in only one cloud platform. Student skill sets should cross several cloud platforms at many levels of available services. |

**Reading 1-2-6 Community Cloud**

1. Introduce and describe a community cloud deployment model as one in which flexible data storage, applications, or services are managed centrally by an organization or service provider on hardware dedicated to a specific group of organizations. It is accessible to multiple organizations with similar concerns, but not to the general public.

## Quick Quiz 1

1. What term refers to the ability to connect to cloud-hosted resources from anywhere on the Internet using a variety of device types?
2. Resource pooling
3. Broad network access
4. On-demand self-service
5. Rapid elasticity

Answer: B

1. What term refers to the ability to scale cloud resources up or down according to demand?
2. Resource pooling
3. Broad network access
4. On-demand self-service
5. Rapid elasticity

Answer: D

1. True or False: A cloud is more abstracted from the physical hardware in the data center, relying on a virtualization layer of communication that is managed by comprehensive virtualization software.

Answer: False

1. Which term refers to a legal agreement designed to restrict sharing of proprietary information by employees, partners, vendors, or customers?
   1. HIPPA
   2. On-demand self-service
   3. SLA
   4. NDA

Answer: D

1. Which certification document refers to a European Union law establishing broad-reaching data protection standards for any information that could be tied to a single individual?
   1. The Health Insurance Portability and Accountability Act (HIPAA)
   2. General Data Protection Regulation (GDPR)
   3. NDA (nondisclosure agreement)
   4. ISO/IEC 27001

Answer: B

#### Section 1-3 Cloud Service Models

1. Review the section learning objectives students should understand after completing this section:

* Identify various cloud service models, including SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service).
* Analyze security concerns specific to each cloud service model.

**Reading 1-3-1 Cloud Service Models**

1. Remind students that cloud computing takes functions and resources that would normally happen/reside on a local network, abstracts those functions to a software-defined level, and then provides those services back to the local network from across the Internet or another network.
2. Introduce the concept of FWaaS (firewall as a service) and explain the advantages it provides.
3. Use Figure 1-8 to introduce cloud computing modules.
4. Introduce and explain the features of SaaS (Software as a Service). Note that most cloud consumers are familiar with SaaS. Define SaaS as the provision of application services through the cloud where those applications can be accessed from many different types of devices without having to manage any of the underlying infrastructure.
5. Introduce and explain the features of PaaS (Platform as a Service). Define PaaS as an intermediate level of cloud capability that allows consumers to deploy applications on various platforms without having to manage lower-layer infrastructure.
6. Introduce and explain the features of IaaS (Infrastructure as a Service). Note that IaaS is more technically challenging. Define IaaS as a cloud service that allows consumers to deploy a cloud-based network with services such as operating systems, applications, storage, and virtual devices.
7. Refer to Figure 1-9 and explain that these service models are often characterized according to how much a customer must know about configuring and managing cloud networks in order to use the service, and how much control that customer has over the exact configurations, features, and security measures.
8. Refer to Figure 1-10 to illustrate how each type of cloud service is accessible to users.

**Reading 1-3-2 Service Model Security Concerns**

1. Point out that as organizations transition to the cloud, security strategies must also evolve to protect new vulnerabilities and defend against new types of attacks.
2. Explain why each service model has different security concerns.
3. Describe the two primary areas of security concerns that organizations using SaaS must address: data security and application access.
4. Describe the two primary areas of security concerns that organizations using PaaS must address: data security and application access. Explain that PaaS users must also be concerned with application configurations and administrative or root access.
5. Explain that IaaS customers must consider similar security concerns as when running their own, on-prem infrastructure. Point out that the issues include compliance regulations, audit requirements, and identity management in addition to all the other concerns previously listed. Also note that that because IaaS customers have no control over the hardware underlying their cloud infrastructure, they must ensure that the CSP complies with standards common to the customer’s industry.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | SaaS, PaaS, and IaaS: three cloud models; three very different risks: <https://www.zdnet.com/article/saas-paas-and-iaas-three-cloud-models-three-very-different-risks/> |

**Section 1-4 Cloud Service Providers**

1. Review the section learning objectives students should understand after completing this section:

* Recognize popular cloud service providers.
* Evaluate common cloud service types, including compute, storage, network, and security services.
* Analyze security concerns specific to each cloud service model.

**Reading 1-4-1 Cloud Providers and Platforms**

1. Remind students that cloud service providers (CSPs) offer a variety of cloud services, noting that some services are specific to a particular market niche whereas others are more generalized to meet a wider base of consumer needs.
2. Mention that salesforce.com focuses on its SaaS CRM products.
3. Mention that AWS (Amazon Web Services), Microsoft Azure, and GCP (Google Cloud Platform) are three of the top contenders for market share in the PaaS and IaaS consumer area.
4. Introduce AWS (aws.amazon.com) CSP and describe its consumer offerings in the cloud arena.
5. Introduce Microsoft Azure (azure.microsoft.com) and describe its consumer offerings in the cloud arena.
6. Introduce GCP (cloud.google.com) and describe its consumer offerings in the cloud arena.
7. Introduce IBM Cloud (ibm.com/cloud) and describe its consumer offerings in the cloud arena.
8. Introduce Oracle Cloud (cloud.oracle.com) and describe its consumer offerings in the cloud arena.
9. Introduce Alibaba Cloud (alibabacloud.com) and describe its consumer offerings in the cloud arena.
10. Mention that there are companies that can assist you in hosting your own private cloud—essentially DIY cloud computing—using cloud management software of some kind.
11. Introduce OpenStack (openstack.org) and describe its consumer offerings in the private DIY cloud arena.
12. Introduce VMware (vmwarecom) and describe its consumer offerings in the private DIY cloud arena.
13. Introduce Eucalyptus (eucalyptus.cloud) and describe its consumer offerings in the private DIY cloud arena.

**Reading 1-4-2 Common Cloud Services**

1. Remind students that each CSP offers different cloud services and configures their user interfaces and product offerings in different ways.
2. Introduce the concept of a product type and explain that the major CSPs offer the same basic product types.
3. Introduce the compute product type, explaining how it refers to cloud functions that process data in some way.
4. Introduce the storage function, explaining that it refers to cloud services that store or preserve data.
5. Introduce options for configuring network functions such as connection configurations, subnets, IP addressing, VPNs, trunk lines, DHCP services, and load balancing. Note that other tools include migration resources and content delivery products, which might be grouped into their own categories.
6. Mention the traditional security functions that also apply to the cloud: security functions in the cloud include perimeter security (firewalls, IPS/IDS, and proxies for the virtual network), identity management, certificate or key management, authentication services, access controls, and token or federation services.
7. Explain why cloud services, by definition, present a larger attack surface than do traditional networks, where access can be more tightly monitored and controlled. Point out that because of this, the security tools selected—especially when configuring a public cloud—will take the needs of this abstracted, remote environment into account.
8. Describe some of the CSP application components tools that can be used for building and hosting cloud-based applications. Cloud services optimized for app development, such as testing or hosting environments, micro services, templates, security auditing, e-commerce, machine learning, and mobile services, might also be available.
9. Describe some of the CSP management and monitoring tools, which include dashboards, monitoring services, and data analytics services.

**Section 1-5 Troubleshooting Methodology**

1. Review the section learning objectives students should understand after completing this section:

* Anticipate common cloud issues.
* Explain the troubleshooting steps.
* Identify helpful preventive measures.

**Reading 1-5-1 Common Cloud Computing Problems**

1. Discuss how the troubleshooting method defined by CompTIA can help a student organize their thoughts and their approach to solving problems.
2. Provide an overview of common cloud issues that can be addressed by a methodical troubleshooting process.

* Connectivity issues
* Latency
* Capacity
* Security

**Reading 1-5-2 Troubleshooting Steps**

1. Refer to Figure 1-11 to identify and describe each of the six steps in the CompTIA troubleshooting methodology:

* Step 1: Identify the problem.
* Step 2: Establish a theory of probable cause.
* Step 3: Test the theory to determine cause.
* Step 4: Establish a plan of action to resolve the problem and implement the solution.
* Step 5: Verify full system functionality, and, if applicable, implement preventive measures.
* Step 6: Document findings, actions, and outcomes.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Emphasize that the Cloud+ exam might give a student a troubleshooting scenario that requires them to identify the next step according to the troubleshooting method described in this section. Explain how to do this by using the information given to identify which steps of the troubleshooting process have been completed so far in the scenario, and then identifying which step should come next and which of the task options would accomplish that step. |

**Reading 1-5-3 Preventive Measures**

1. Introduce and explain the measures that can be taken to help minimize the likelihood of problems cropping up in a cloud environment:

* Maintain good monitoring and analysis techniques.
* Thoughtfully configure your dashboards to show the most helpful information.
* Follow good change management processes.
* Understand your cloud services and how to identify where problems are likely to occur, how to locate those problems, and how best to address them.

## Quick Quiz 2

1. Under which cloud computing service does Google’s office productivity suite fall?
   1. PaaS
   2. IaaS
   3. SaaS
   4. DBaaS

Answer: C

1. True or False: IaaS customers must understand more about configuring their cloud infrastructure than do SaaS customers.

Answer: True

1. Which cloud computing platform is open-source software designed by Rackspace and NASA to create do-it-yourself compute, storage, and networking cloud services?
   1. GCP
   2. Eucalyptus
   3. Alibaba Cloud
   4. OpenStack

Answer: D

1. What are the two primary areas of security concern for organizations using SaaS?
2. Data security and network security
3. Root access to servers and application access
4. Network security and server monitoring
5. Data security and application access

Answer: D

1. “\_\_\_\_\_\_\_\_\_\_” is the first step in the troubleshooting process.

Answer: Identify the problem

## Class Discussion Topics

1. As a class, discuss the differences between IT security implementations for a traditional local data center and a cloud environment.
2. As a class, discuss the difference between a private cloud service and public cloud services. Why are both necessary?

## Additional Projects

1. The students have learned that there are several cloud services providers. AWS (Amazon Web Services), Microsoft Azure, and GCP (Google Cloud Platform) are the three top contenders for cloud platform market share. Have each student research these CSPs, comparing them in relation to the cloud services features they support and their prices. The students should then prepare a report summarizing their research.

## Additional Resources

1. What is cloud computing? Everything you need to know about the cloud, explained:

<https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/>

1. What is Firewall as a Service (FWaaS) and Why You Need It: <https://www.techwalls.com/firewall-as-service-fwaas-why-you-need-it/>
2. Seven Key Challenges to Cloud Computing: <https://e2logy.com/blog/seven-key-challenges-to-cloud-computing/>
3. How to diagnose cloud performance issues: <https://www.infoworld.com/article/3237824/how-to-diagnose-cloud-performance-issues.html>

**Key Terms**

For definitions of key terms, see the Glossary near the end of the book.

* **acquisition**
* **Alibaba Cloud**
* **API (application programming interface)**
* **automation**
* **AWS (Amazon Web Services)**
* **Azure**
* **broad network access**
* **cloud bursting**
* **community cloud**
* **compute**
* **CRM (customer relationship management) system**
* **CSP (cloud service provider)**
* **DevOps (development and operations)**
* **divestiture**
* **DR (disaster recovery)**
* **Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems)**
* **G Suite**
* **GCP (Google Cloud Platform)**
* **GDPR (General Data Protection Regulation)**
* **HA (high availability)**
* **HIPAA (Health Insurance Portability and Accountability Act)**
* **hybrid cloud**
* **IaaS (Infrastructure as a Service)**
* **IBM Cloud**
* **ISO/IEC 27001**
* **knowledge base**
* **latency**
* **measured service**
* **merger**
* **NDA (nondisclosure agreement)**
* **NIST (National Institute of Standards and Technology)**
* **on-demand self-service**
* **OpenStack**
* **Oracle Cloud**
* **orchestration**
* **PaaS (Platform as a Service)**
* **PCI DSS (Payment Card Industry Data Security Standard)**
* **private cloud**
* **public cloud**
* **rapid elasticity**
* **resource pooling**
* **SaaS (Software as a Service)**
* **SLA (service level agreement)**
* **SOC (Service Organization Control) report**
* **SSAE (Statement on Standards for Attestation Engagements No. 18)**
* **storage**
* **tenant**
* **virtualization**
* **VMware**
* **VPN (virtual private network)**