CompTIA Cloud+ Study Guide

# Chapter 1 – Understanding Cloud Concepts

## Topic 1A: Recognize Cloud Concepts

**EXAM OBJECTIVES COVERED**

*1.1 Compare and contrast the different types of cloud models*

The five characteristics defined by the National Institute of Standards and Technology (NIST) are:

* **On-demand self-service:** Consumers can provision resources as needed and automatically.
* **Broad network access:** Services are available across the network from commonly available clients.
* **Resource pooling:** The **cloud service provider (CSP)** pools resources in a multi-tenant model and adjusts resource allocation on an on-demand basis, and the specific distribution of hardware resources is abstracted from the consumer.
* **Rapid elasticity:**Resources are provisioned and released to adjust for changes in demand and consumption. This process may be automatic or manual.
* **Measured service:** Metering of resources is monitored, controlled, and billable.

**Cloud Service Models:**

Cloud service models are initially divided into three types of solutions. These may be differentiated by what responsibilities are being offloaded. Many more cloud service models have since been defined, but these three best exemplify the primary aspects of cloud computing:

* **Software as a Service (SaaS)** : The consumer is being provided with the direct use of the software. Responsibility for the hardware where that software runs, the operating system upon which it runs, and the installation and patching of the software itself are all offloaded to the CSP.
* **Platform as a Service (PaaS)** : The service structure is provided by the CSP. It is up to the consumer to populate that structure, manage it on a day-to-day basis, and assume responsibility for the content. Support for the hardware, as well as the service platform that hosts the content, is offloaded to the CSP.
* **Infrastructure as a Service (IaaS)** : The hardware infrastructure is provided to the consumer. The consumer assumes responsibility for all layers above that hardware. The CSP manages hardware failures, firmware updates, device drivers, and hardware compatibility. The consumer installs and manages the operating system on top of the hardware as well as any services and applications that run above that operating system.
* **Anything as a Service (XaaS)**: “Anything as a service" is a catch-all phrase for technology solutions that are moved to the cloud. There are many IT-oriented examples, including database as a service (DBaaS), desktop as a service (DaaS), and containers as a service (CaaS).

**Software as a Servce (SaaS):**

* OS agnostic
* Licensed for use by Consumer / Subscription Model
* CSP retains responsibility for installing, configuring, maintaining, patching software (and all infrastructure it runs on)
* Examples: Netflix, Office365, G-Suite, DropBox, Webex, Google apps
* Target Audience: End Users

**Platform as a Service (PaaS):**

* Provides hardware, OS, and necessary tools (platform).
* Consumer utilizes tools to manage their data on their own.
* CSP responsible for hardware and operating systems as well as platform maintenance.
* Typically aimed at developers as it provides a development platform (Python, MySQL, etc for example)
* Consumer doesn’t worry about OS updates or hardware.
* PaaS typically support multiple development environments and programming languages.
* Examples: Google App Engine, Heroku, AWS ElasticBeanstalk, Salesforce
* Target Audience: Developers

**Infrastructure as a Service (IaaS):**

* CSP is responsible for hardware (power, network, computers etc)
* Consumer responsible for virtual machines hosted on CSP infrastructure.
* Consumer installs operating systems themselves.
* Very flexible for consumer and scaleable
* Examples: Amazon EC2, Microsoft Azure, Rackspace, Digital Ocean
* Target Audience: IT Administrators

**Anything as a Service (Xaas):**

* Describes practice of shifting anything to an ‘as a serviec’ offering, including email, operating systems, security, etc. Provides reduced Capital Expenditures in exchange for Operational Expenditures.

**Cloud Components and Clients**

1. Client platform – from which cloud services accessed
2. Datacenter – from where cloud services are hosted
3. Network connection In between

**Cloud Deployment Models**

1. **Public cloud** – CSP owns cloud deployment and allocates its resources to external, unaffiliated consumers. Customers share the public cloud’s resources without knowing where their data is in relation to other organizations.
2. **Private Cloud** – Services are only provided to a single organization
3. **Community Cloud** – services are offered to several organizations that may have similar needs but are otherwise autonomous.
4. **Hybrid Cloud** – combo of two or more public,private,community deployments.

**Cloud within a Cloud (VPC)**

A virtual private cloud (VPC) is the concept of a cloud within a cloud, meaning an isolated segment (logical) inside a public cloud that is separated from any resources shared with other companies.

**Multitenancy –** concept behind public clouds that involves multiple consumers, known as tenants share computing resources owned and managed by the CSP. This is the opposite of a VPC deployment. Multitenancy provides cost benefits behind shared resource utilization.

**Multi-Cloud** – cloud services spread among two or more public CSPs (AWS, Azure, GCP) as well as private cloud. Prevents reliance of a single vendor, provides service flexibility, and improved geographic control of data. Helps disaster mitigation.

**Recognize Cloud Services**

* Google Workspace
* Office365
* Digital Ocean
* Rackspace
* Red Hat Cloud Suite – OpenStack (for building opublic/private clouds) Virtualization (for virtual servers) Satellite (for cloud service management, OpenShift (for Kubernetes container management)

**Recognize Advanced Cloud Services**

* **Internet of things (IoT**) – combo of network connectivity and smart devices that facilitate collection and analysis of data. (software, sensors, robotics).
  + Smart Homes, Medical monitoring, agriculture management, energy management, manufacturing/industrial production.
* **Serverless Computing -**aka Function as a Service (AWS Lambda)
* **Machine Learning / Artificial Intelligence** **–** solving complex problems using data.

**Three Largest Cloud Providers**

1. Amazon Web Services
   1. offers around 200 cloud-based services supported by a global infrastructure of datacenters that consists of 77+ availability zones and 24+ regions.
   2. S3, EC2, Lambda, Glacier, SNS, Cloudfront
   3. Built on Linux
2. Microsoft Azure
   1. Microsoft Azure also presents approximately 200 cloud products
   2. Azure Virtual Machines (IaaS), Azure Disk Storage (StaaS), Azure Visual Studio (IDE), Azure Functions (serverless compute), Azure Backup (backup and restore services) Azure SQL(SQL database) Azure Cosmos (NoSQL) Azure Active Directory.
3. Google Cloud Platform
   1. The infrastructure includes 73+ zones and 24+ regions and continues to grow.
   2. Cloud Storage (Staas) Compute Engine (IaaS), App Engine (PaaS) Cloud SQL (SQL), Firestore (NoSQL), Big Query (big data)

**Managed Service Providers (MSP) –** can help with design, migration, deployment, and management. CSP’s offer MSP services too (AWS Managed Services).

**Shared Responsibility Model** – CSP’s and consumers manage different aspects of cloud security.

* CSP responsible for security **OF**  the cloud.
* Consumer responsibility of security **IN** the cloud

A screen shot of a computer

Description automatically generated

## Topic 1B: Recognize Cloud Terms

**EXAM OBJECTIVES COVERED**

*1.1 Compare and contrast the different types of cloud models*

**Subscription Service -**  payment model that uses recurring, periodic billing cycles often based on the length of the subscription (long term is cheaper). Model usually includes **no long term contracts**. Access is provided as soon as the subscription is established. Can terminate at any time.

**Identity Management –** process by which identities are established and access to resources is controlled. Typically, users are identified and assigned a user account. User account is assigned rights/restrictions which are enforced by Access Controll systems such as permissions. Users may be organized into groups. Aka **IAM – Identity and Access Management**

**Provisioning** – one of several steps in cloud service deployment process. Refers to the allocation of cloud resources in the overall enterprise infrastructure. Governed by *Objectives, policies, and procedures.* Can be accomplished by web-based or command line interfaces. Usually self-service. Provisioning happens before server, service, user, or network configuration. Access controls are part of provisioning process.

**Applications** – Installation of applications happens in the cloud rather than local servers. Accessed over network. Advantage of cloud is consistent experience.

**Virtual Machines –** virtualization allocates hardware resources among one or more virtual machines. VM’s have an OS and one or more apps on them. VM Participates on network as a regular node, providing db, auth, storage, etc. VM’s have greater access to hardware resources and can be provided with redundancy for HA. **Key component of IaaS like EC2**

**Containers** – form of virtualization but different than VM. Containers virtualize the OS layer rather than the hardware layer. A container holds a single application and everything needed to run. Excels with microservices due to narrow focus. Containers share a single OS and provide a function.

**Templates** – VM’s may be deployed using VM Templates. Template is like a recipe for a VM.

**Post-Deployment Validation –** ensures deployed apps or services meet required service levels. Regression or functionality testing. Can be automated.

**Auto Scaling** – provides appropriate resources based on demand utilizing templates. Can scale up (better hardware or more resources) or scaled out (more nodes)

**Converged/Hyperconverged** – converged consists of individual compute, storage, or network solutions. Hyperconverged combine compute, storage, and network resources into single component to reduce complexity and increase scaleability.

## Topic 1C: Understand the Troubleshooting Methodology

**EXAM OBJECTIVES COVERED**

*5.1 Given a scenario, use the troubleshooting methodology to resolve cloud issues*

1. Identify the problem.
   1. This problem may be discovered for you by the end-users you support, exposed by log files, identified by monitoring software, or indicated by alerts on dashboard interfaces
2. Determine the scope of the problem.
   1. One of the most important steps is to determine whether the problem exists for only one user, or whether it exists for multiple users. In addition, determining whether cloud service interruptions exist at multiple locations or just a single location will help determine the scope of the problem.
3. Establish a theory of probable cause, or question the obvious.
   1. Identify common elements that might span multiple cloud environments. Keep this step as simple as possible.
4. Test the theory to determine the cause.
   1. Test the theory by verifying that the likely cause is indeed the culprit. This phase may involve research or additional testing. Very simple problems may actually be solved during this step.
5. Establish a plan of action.
   1. Recognize that service interruption and data loss should be avoided. If brought down or data lost, customer must be notified. Should include the steps taken – these steps should be defined ahead of time rather than during implementation of the solution.
6. Implement the solution, or escalate.
   1. Follow the plan without deviating. Escalate to cloud vendor/MSP if need be. Make only one change at a time and test result.
7. Verify full system functionality.
   1. Test for functionality
8. Implement preventive measures.
   1. If possible, preemptively reconfigure services/network devices to avoid a repeat of the problem. If possible, implement other technology or additional practices to prevent problem from happening again.
9. Perform a root cause analysis.
   1. Evaluate why problem has occurred. Identify root cause if possible to avoid problem in future
10. Document findings, actions, and outcomes throughout the process.
    1. Documentation should be maintained throughout the service’s lifecycle, including during the troubleshooting process. Documenting the symptoms of the problem, the results of research into potential solutions, and the results of each step of the plan of action (whether the step was successful or not) will permit you to better understand your environment and therefore help prevent possible future problems. Note that documentation is not a separate step but rather a good practice to be used during each phase of the troubleshooting process.

**Understand Environment including Corporate Policies, procedures, and their impact**

Standard operating procedures govern how a particular task is accomplished – follow procedures during troubleshooting. Cloud policies govern cloud resources and manage case escalation. Have complete view of cloud environment before escalating.

SLA’s might enforce penalties on your org for outage. CSP’s have SLA’s too.

# Chapter 2 – Planning and Designing a Cloud Environment

## Topic 2A: Meet Cloud Business Requirements

**EXAM OBJECTIVES COVERED**

*1.4 Given a scenario, analyze the solution design in support of the business requirements*

### User vs Business Needs

**Hardware**

Users

* Access from any device

Business

* Reliable and fast Internet connectivity
* Constructing and supporting a datacenter for private and hybrid cloud deployments
* Specialized hardware that cloud services cannot provide, such as industrial or manufacturing equipment
* Hardware scalability by the CSP
* Reliability of the CSP's hardware

**Software**

Users

* Familiar user interface for applications
* Consistent software versions
* Requirements that may vary by business roles (accounting, sales, developers, and IT)
* Specialized software that is not cloud native (such as accounting or human resources software)
* Easy cloud billing, reporting, and accounting user interface
* Management of unique data formats
* Easy IT cloud administration tools
* Training for IT cloud administrators

Business

* Specialized line of business or custom in-house developed software
* Software that is cloud only or is not portable to the cloud
* Software scalability
* CSP's offer of SaaS, PaaS, and IaaS solutions

**Integration**

Users

* Integration with existing data sources (SQL and NoSQL databases, big data, and business partners)
* Integration of new cloud-native software with legacy on-premises software
* Integration with business partner systems
* Support by the CSP during integration and cloud migration

Business

* Integration with existing data sources (SQL and NoSQL databases, big data, and business partners)
* Integration of new cloud-native software with legacy on-premises software
* Integration with business partner systems
* Support by the cloud service provider during integration and cloud migration

**Budget**

Users

* Whether the cloud service provider offers managed services for user applications

Business

* Cost of subscriptions
* Cost of scaling resources
* Cost of moving data out of a provider’s cloud
* A shift from capital expenditures to operations expenditures

**Compliance**

Users

* Industry requirements (such as HIPAA,PCI DSS,and PII )
* CSP certificates of compliance
* Research compliance with other businesses in the same industry

Business

* Industry requirements (such as HIPAA, PCI, and PII)
* CSP certificates of compliance
* Research compliance with other businesses in the same industry

**Service-Level Agreements (SLAs)**

Users

* Timely responses to issues by technical support (a concern of both end-users and administrators)

Business

* Consider the business’s own SLAs to partners and customers.
* Consider the CSP's SLAs to the business.
* Research documented uptime, outages, breaches, response times, and reliability.

**Security**

Users

* Straightforward security interfaces for users
* Security easy for cloud administrators to implement

Business

* Virtual private cloud (VPC) options
* Whether data is stored at multiple datacenters for regional security
* Encryption for data at rest and in transit
* How the CSP protects data backups
* How access to data is secured

**Network**

Users

* Performance and availability

Business

* Encrypted connectivity/Virtual private network
* Performance and availability
* Cost of redundancy
* Available virtual network options (such as network size, subnetting/segmentation, and routing)
* Connectivity to the existing on-premises network

Business analysts will develop**business requirements documents (BRDs**) that provide the answers to What? and Why? questions regarding services and applications to ensure the business will benefit from projects such as cloud migrations and web app development.

**Separate Environments**

* Development – where programmers code projects, detect bugs, manage code versions, implement code level security
* Staging – where QA testers validate cloud apps and services including security and testing both automated and manual. May need to scale for performance testing so costs here may not reflect anticipated costs in production
* Production – available to end-users. Security is in place to protect data and availability.

**Disaster Recovery –** businesses also might require a DR environment.

**Blue-Green Release Model** – a variation of the model of dev/stage/production. In this model, there are two identical environments available, one labeled Blue, one Green. At any given time, only one of them is hosting production. The other environment serves as the staging area for next release. **Also serves as a hot-standby for DR**.

**Canary Deployment Model** – similar to blue-green but users are gradually migrated to the newer environment instead of complete and immediate migration. Final QA are performed and users are gradually migrated to the new environment with the canary model.

### Resting Techniques

**Security Testing**

* **Vulnerability Testing** – empirically identifies, quantifies, and ranks vulnerabilities in networks, operating systems, services, and applications. The goal is to identify the vulnerability so that it can be mitigated.
* **Penetration Testing** - is an authorized attempt to identify security misconfigurations, unknown services, unknown devices, and other security aspects that require testing. Such testing begins with an analysis of available resources, looking for older, unpatched, or vulnerable software. The testing also includes an analysis of business practices.
  + Compliance
  + Identify Weaknessess in process/configs
  + Identify Vulnerability in software or OS

**Use Tests**

* **Performance Testing** -  is a quality assurance test to determine a system or application’s functionality under a given workload. For cloud services, this information is useful for determining scalability settings
* **Regression Tests -** are rerun on applications to ensure that any new changes did not break existing functionality. Otherwise, the application has fallen back, or “regressed,” to an earlier stage of functionality.
* **Functional Testing -** is a quality assurance test that evaluates whether a system or application meets its specifications—does it do what it’s supposed to do?
* **Usability Testing -**is accomplished by end-users and provides direct feedback on the interface, features, and practical use. Usability testing helps ensure the application or server meets requirements and will actually be useful upon release.

## Topic 2B: Design Capacity Planning Requirements

**EXAM OBJECTIVES COVERED**

*1.2 Explain the factors that contribute to capacity planning*

Here is a breakdown of the questions involved in capacity planning:

1. What is the current baseline or service level?
2. What is the current capacity?
3. What future needs can we predict, based on upcoming business initiatives?
4. Are there consolidation opportunities for services, applications, or data sources?
5. What recommendations can be made, and what actions can be taken?

**Solution Requirements –** define the criteria for a solution to a given problem that software or services are expected to meet. The requirements define what needs to happen without specifying how the solution will be met (hardware, software, budget, etc)

**Business Needs Analysis –** identifies business needs for which solutions must be found to help the organization achieve its strategic goals. Such goals might include cutting costs, increasing revenue, increasing customer base, etc.

### Templates

Requirements documents typically follow a standard template:

* Project overview
* Project scope
* Success factors
* Stakeholder identification
* Project constraints
* System functionality
* User classes
* User interface requirements

### Licensing

| **Licensing Structure** | **Characteristics** |
| --- | --- |
| Per user | One license for each user that consumes the software or service |
| Socket based | One license for each CPU that attaches to the socket of a motherboard, regardless of the number of cores the CPU might contain |
| Core based | One license for each core in a CPU in a server |
| Volume based | One license that permits a specified number of installations, for example, installation of the software on up to 100 computers |
| Perpetual | One-time fee for a license that may include additional support costs; however, the license is good for the life of the software |
| Subscription | Periodic cost; usually includes at least basic technical support, maintenance, and possibly upgrades |

*Comparison of common licensing structures.*

### User Density

Refers to the number of concurrent connections to cloud services that maintain an acceptable level of performance. In testing, thresholds are established for system responsiveness as compared to user experience. Capacity planning comes into play with cloud-based VMs supporting user applications, web apps, and services such as email and databases.

### System Load

**System Load**is a measure of how busy the system’s central processing unit (CPU) is over a period of time. The load is usually reported over three points in time: one minute, five minutes, and 15 minutes. While there are usually counters for CPU utilization itself, the system load is better measured by using CPU queue length. That value tracks processes currently being run by the CPU as well as those that are awaiting the CPU’s attention (queued up).

*Typically, the queue length value should not exceed the number of logical processors (cores) in the system.*

### Trend Analysis

**Trend Analysis –** attempts to predict future results based on recently observed results. This helps cloud admin anticipate future issues or capacity requirements based on observed utilization of applications or systems.

* **Baselines** – can display two pieces of information: the past situation and the current situation. An initial baseline contains information gathered over a long period of time (if possible) to provide as accurate an understanding as possible of the past. An additional baseline can be used to determine if anything is different from the initial baseline.
* **Patterns** - Performance monitoring and capacity planning patterns might include specific times in the business day when a load is particularly heavy or light, or specific times of the week or year when loads are heavy or light.
* **Anomoly** - An anomaly is a change in performance or other behavior that is not explained by the current workload.

### Performance and Capacity Planning

Ongoing performance monitoring is a critical component of capacity planning. Once a historical baseline is established, deviations from the baseline can inform capacity planning. Information such as solution requirements, user density, and system load—gathered via trend analysis—allows cloud architects and administrators to manage resources more effectively.

# Chapter 3: Administering Cloud Resources

## Topic 3A – Manage Cloud Administration

**EXAM OBJECTIVES COVERED**

*3.1 Given a scenario, integrate components into a cloud solution*

**Subscription services**  refers to a licensing model in which a user or an organization pays a fee on a regular schedule (usually monthly or annually) and gets access to a resource through the term of the subscription. It is a pay-per-identity (user or organization) model that is very common for cloud services. Subscription services match the on-demand self-service cloud characteristic, as consumers can subscribe and unsubscribe from services easily.

*Subscription management may be a shared responsibility between cloud administrators and the financial department. The cloud subscriptions are tied to the organization’s overall spend allowances, hence the shared control.*

**Compare Costs:**

* Third-party studies
* Managed CSPs
* Your own comparison study
* Cloud subscription cost analysis with peer organizations