General Information - about 11% of the questions pertain to this field. You'll need to be able to compare and contrast ideas in cloud computing and also be able to set up virtualization for the client. It is worth noting that *none* of the questions in this area will begin with a scenario for you to evaluate when answering.

Cloud-Computing Concepts - be able to summarize entire processes. Before cloud computing, **scalability** was difficult, as users were always restricted by their local resources. A common example of cloud computing includes online file storage. **Online file storage** allows users to store documents, photos, and videos **in the cloud** without needing to take up storage on their local hard drive. However, cloud computing covers far more than just file storage. It's now possible to move an entire organization's **infrastructure** (everything from servers to networking equipment) to the cloud.

Common Cloud Models - include the different types of cloud structures that can be used as well as service structures that can be offered within the cloud environment. Cloud services are often sold **as a service**.

Private Cloud - is a cloud model in which the virtualization resources purchased by the user are dedicated solely to the use of the user. This ensures the **greatest level of security** for the user but comes at an **increased price** as well as **less flexibility** for the resources. Think of a cloud as a physical file cabinet. With a private cloud, only the user is able to access or store their information in the file cabinet.

Public Cloud - is a virtualization resource in which the resource is **shared across the open internet**. This means that the same cloud server that contains a user's data also contains the data of anyone else who uses that service. Imagine the physical file cabinet again. With a public cloud, you are able to store your data in a separate file within the file cabinet, but the files of thousands of other people are also stored in the same file cabinet. For this reason, a public cloud is not as secure as a private cloud. An example of a public cloud would be**Dropbox** or **iCloud**.

Hybrid Cloud - is **a mixture** of the public cloud and the private cloud. A portion of the data is stored in a public cloud while other more sensitive data can be stored in a private cloud. A hybrid cloud offers the **security** of a private cloud for more sensitive data as well as the **flexibility** and **scalability** of a public cloud.

Community Cloud - is a cloud that is **shared between a specific set of users**. Imagine the file cabinet again. The file cabinet is shared between users, but only a specific set of users can store their data in the file cabinet, increasing security over a public cloud, which allows for anyone to store data in the file cabinet.

Infrastructure as a Service (IaaS) - can be thought of as a **virtual data center**. As its name suggests, infrastructure as a service (IaaS) providers allow clients to build their entire infrastructure in the cloud. Infrastructure includes items such as servers, firewalls, routers, and switches. In an IaaS environment, clients are entirely responsible for managing, maintaining, and patching operating systems and applications.

Software as a Service (SaaS) - In recent years, there has been a major shift from locally installed software to **web-based software**. Software as a service (SaaS) has become a popular choice for organizations because it allows them to access their programs **anywhere an internet connection is available**. SaaS can be described as any program that is accessed via the web and not locally installed.

Platform as a Service (PaaS) - provides a platform for developers to **build their own applications**. PaaS providers will handle everything on the back end, including servers, operating systems, and development tools. This allows developers to focus on creating, building, and managing their applications.

Cloud Characteristics - are **features available on the cloud**. You must be able to summarize these common features.

Shared Resources - also known as **resource pooling**, is the division of the resources of the provider among the clients of that provider. One physical host machine with a lot of resources (memory, storage capacity) can have its resources shared among multiple virtual machines. This resource sharing can occur both **internally and externally**.

Metered Utilization - refers to the concept of tracking a cloud user's usage and **charging only for the number of services used**. *Note:* The terms "measured service" and "metered service" are commonly used interchangeably when referring to cloud computing. The National Institute of Standards and Technology publication, SP 800-145, "The NIST Definition of Cloud Computing," characterizes a measured service as when "cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."

Rapid Elasticity - It's not always clear how much of a particular resource you are going to need when setting up a new environment. It's entirely possible (and quite common) for your resource needs to grow as the organization grows. An organization that started with five servers might triple its server needs in several years. Virtualization makes it possible to quickly add new servers as you need them without the hassle of purchasing new hardware each time.

High Availability - is the concept of a cloud service being **uninterrupted and responsive** the majority of the time. Service-level availability or **uptime** is measured in **nines**. For example, a provider with three nines of availability has 99.9% uptime while a provider with five nines of availability guarantees 99.999% uptime.
File Synchronization - is the ability to provide the **most recent copy** of data on both the cloud and local devices through the synchronization process.
Desktop Virtualization - multiple virtual desktops running on one physical machine. These machines operate similarly to a physical desktop, but all the **hardware is virtualized**. You must be able to summarize these concepts.
Virtual Desktop Infrastructure (VDI) on Premises - is a means by which to manage virtual desktops. With a VDI on premises, the virtual machine running the virtual desktops is located on the physical premises of the entity using it. A VDI removes the physical hardware of a network, such as switches, cables, and NICs, and replaces them with **virtual hardware contained on a single machine** located at the site.
VDI in the Cloud - removes the virtual **machine** from the physical premises and places it in the cloud environment **run through cloud providers**. This eliminates the responsibility of the user for the physical hardware running the VDI.
Client-Side Virtualization - is the process of running the virtual environment on a device physically located on the premises. The virtualization software is run on the client machine rather than through the cloud. The client device hosts the hypervisor and is responsible for accommodating the necessary requirements to run the virtual machine. Considerations for client-side virtualization include **CPU**, **RAM**, **hard drive space**, and **network capabilities**. To do well on questions about this, you must be able to summarize the following content.
The Purpose of Virtual Machines - is designed to remove the one-to-one hardware and software barrier and **maximize available resources**. Virtual machines can be used to run multiple OSs on a single device or can pool resources from multiple servers into a single powerful system. Virtual machines can also be used to **protect the host system** by separating the virtual machines from one another.
Sandbox - is a **temporary, isolated virtual environment** that can be used for testing or quarantining. A sandbox creates a safe environment separated virtually from the host machine to eliminate the potential contamination of the host machine. Data in the sandbox is only in the sandbox and does not save to the host. When the sandbox is terminated, all data associated with the sandbox is also removed.
Test Development - Virtual machines can be used for test development by creating virtual environments and OSs that can be used for application testing or development.
Application Virtualization - as the name suggests, is the virtualization of applications. Application virtualization is often used with legacy software or legacy OS to offer the functionality of the legacy application. Application virtualization is also used for cross-platform functionality. For example, an application designed for a macOS can be used on a Windows machine by creating a virtual macOS on the Windows machine.
***Legacy Software/OS* -** are **outdated** software and operating systems that are not compatible with modern systems.
***Cross-Platform Virtualization* -** is the process of creating a virtual OS of one platform on a different platform, such as a macOS on a Windows OS.
Resource Requirements - Not all virtual machines are created equal. The individual that is building the virtual machine determines what resources to provide to the virtual machine. This means determining the amount of **hard drive space** and the amount of **memory** that your local machine can afford to give the virtual machine. If your physical machine doesn't have a lot of **RAM**, then you will not be able to provide enough RAM for your virtual machine to run smoothly.
Security Requirements - Just as security is vital in physical computing, it's also important to consider security when working with virtual machines. This means implementing the **same types of security controls** on your virtual desktops as you would on your physical ones, such as strong passwords, account lockout policies, and even multi-factor authentication.