# CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-7-cloud_and_virtualization_concepts
Title: Cloud and Virtualization Concepts
Subtitle: CompTIA Security+ (SY0-501)

## 3.7 Cloud and Virtualization Concepts

- 3.7 Summarize cloud and virtualization concepts.
  - Hypervisor
    - Type I (Baremetal)
    - Type II (Hosted)
    - Application cells/containers
      - Application cells
        - Mobile Virtualization allowing for multiplexed access to the kernel
        - Allows for multiple virtual smartphone instances to run on a single device
        - Containers or Containerization
        - Considerations
          - Drop priviledges
          - Run services in non-priviledge modes
          - Containers can maximize the amount of applications running on a server(without the need for additional VMs for each container)
  - Cloud storage
    - Is a service provided by a provider that allows businesses to store and access data accross the Internet
    - Personal
      - OneDrive
      - Dropbox
      - Carbonite
    - Enterprise
      - OneDrive for Business
      - Microsoft Azure
      - Dropbox for Business
      - Amazon S3 or AWS S3
  - Cloud deployment models
    - SaaS
    - PaaS
    - IaaS
    - SECaaS or Security as a Service
      - Outsourcing security to a third-party
      - Third party offers management of:
        - Monitoring, Policies, reporting, security analysis, antivirus, IDS/IPS, content filtering, application control, VPN connections, firewall services
    - Private
    - Public
    - Hybrid
    - Community
  - On-premise vs. hosted vs. cloud
  - VDI/VDE
    - VDI
      - Virtualization components that serve desktops to end users via an image or images stored on a centralized server
      - Delivered over the network
      - Requires good bandwidth, traditional PCs, mobile devices or thin clients
      - Persistant vs Non-persistant VDE
        - Persistant Virutal Desktop Environment
          - A stateful VDE solution
          - Every time the user logs into the VDI the VDE retains configuration settings
          - User profile information is retained
          - Desktop configuration state is retain
          - Application state data is retained
          - Requires a larger amount of storage for every user
          - Larger backups
          - Management is really not much different that a phyiscal desktop infratstruct
          - Image maintenance is more complex
        - Non-persistant Virutal Desktop Environment
          - A stateless VDE solution
          - Every time the user logs into the VDE they are served a fresh instance if the desktop
          - User profile and user data is removed
          - Application state information and data is erased after every logoff
          - Requires Folder direction to a central file share
          - Requires a user state environment magagement solution to maintain a familiar environment for the end user

        - Stoarage capacities requirements are smaller
- Cloud access security broker
    - Also known by it's name CASB
    - Acts as the gateway or gatekeeper between the on-premise and cloud-based solutions
    - Can secure access across multipe technologies such as mobile devices
- VM sprawl avoidance
    - Virtual Machines can be easily created.
    - Virtual machine have license requirements just like physical machines.
    - Too many virtuals machines creates/deployed on a single. (resource exhaustion)
    - An abundance of VMs can make the administration very challenging.
    - Some VMs maybe created then fail to be properly utilized. (Wasted resources)
    - Increased amounts of VM fragementation
    - Large amounts of storage accrual
    - Are machines part of the test environment? or production environment?
    - Which machines can be decommissioned and which machines are essential to the vitality of the company?
- VM escape protection
    - Virutalization allows for an isolated computing environment between the guest operating system (the VM) and the host operating system
    - VM escaping is when the VMs communications break the boundaries of the isolation allowing communication with the host, other VMs on the host and the host's network.
    - VEMON (Virutalized Envrionment Neglected Operations Manipulation)