Análisis de Malware

Comprensión y Análisis de Código Malicioso

Uso de herramientas, búsqueda en logs, funcionalidad y propósito del malware.

SECCION 1
Conceptos y Definiciones

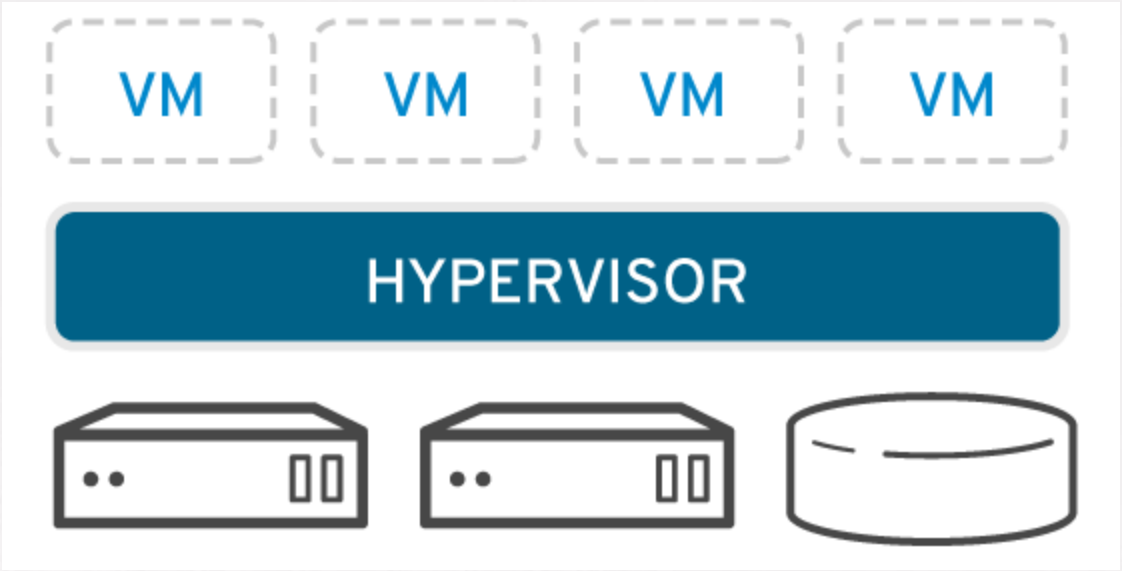
Clase 4

Consideraciones de Hardware.

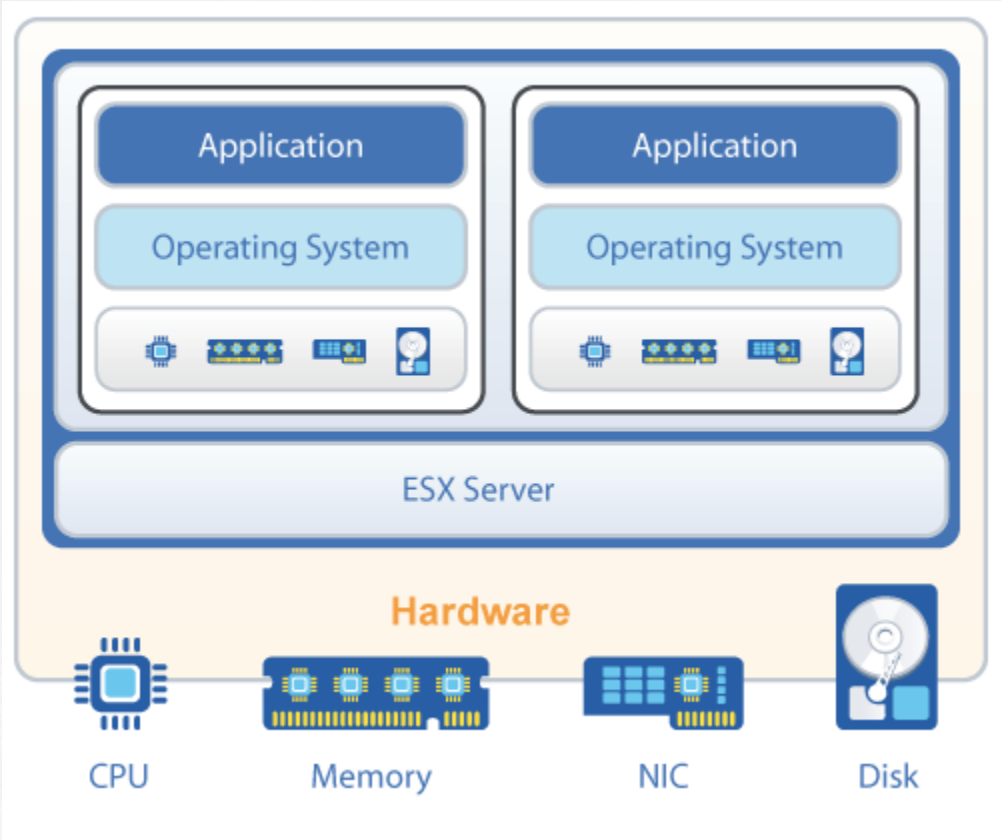
.

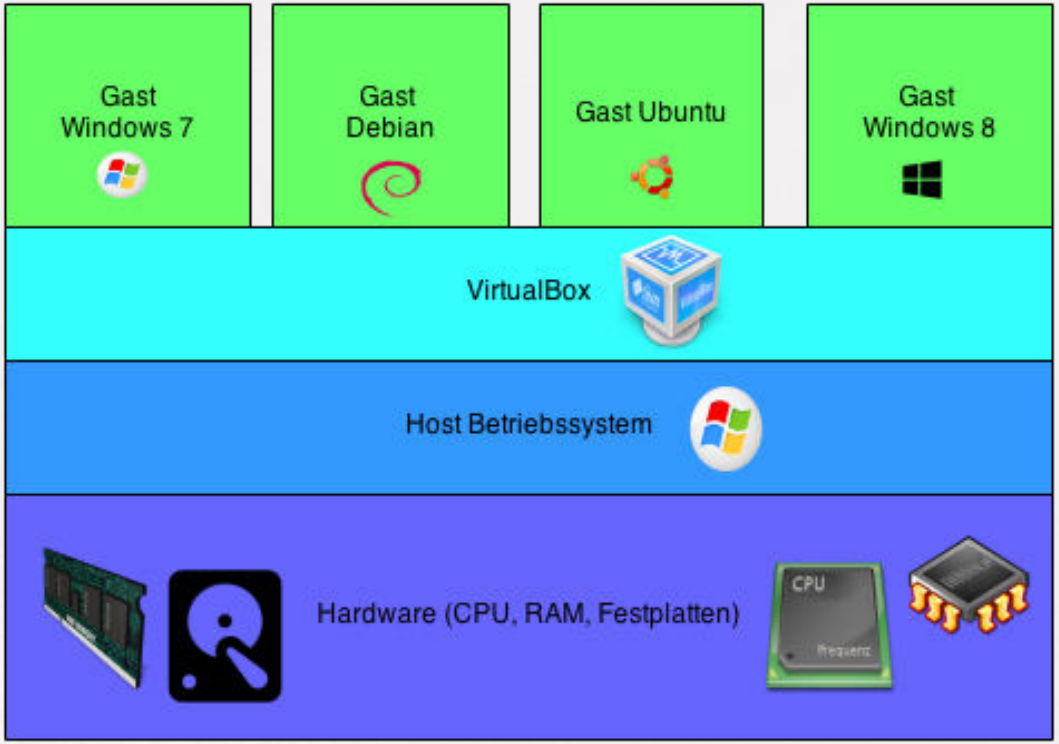
Para la creación de nuestra maquina virtual debemos tener en consideración, la memoria total y la que dedicaremos a la máquina, el procesador y la capacidad limite, así como el espacio de disco libre, para no saturar nuestro equipo. Igualmente, puede instalarse una maquina virtual en un disco externo para no consumir espacio de almacenamiento en nuestro host.

Configuración clásica de un entorno virtual

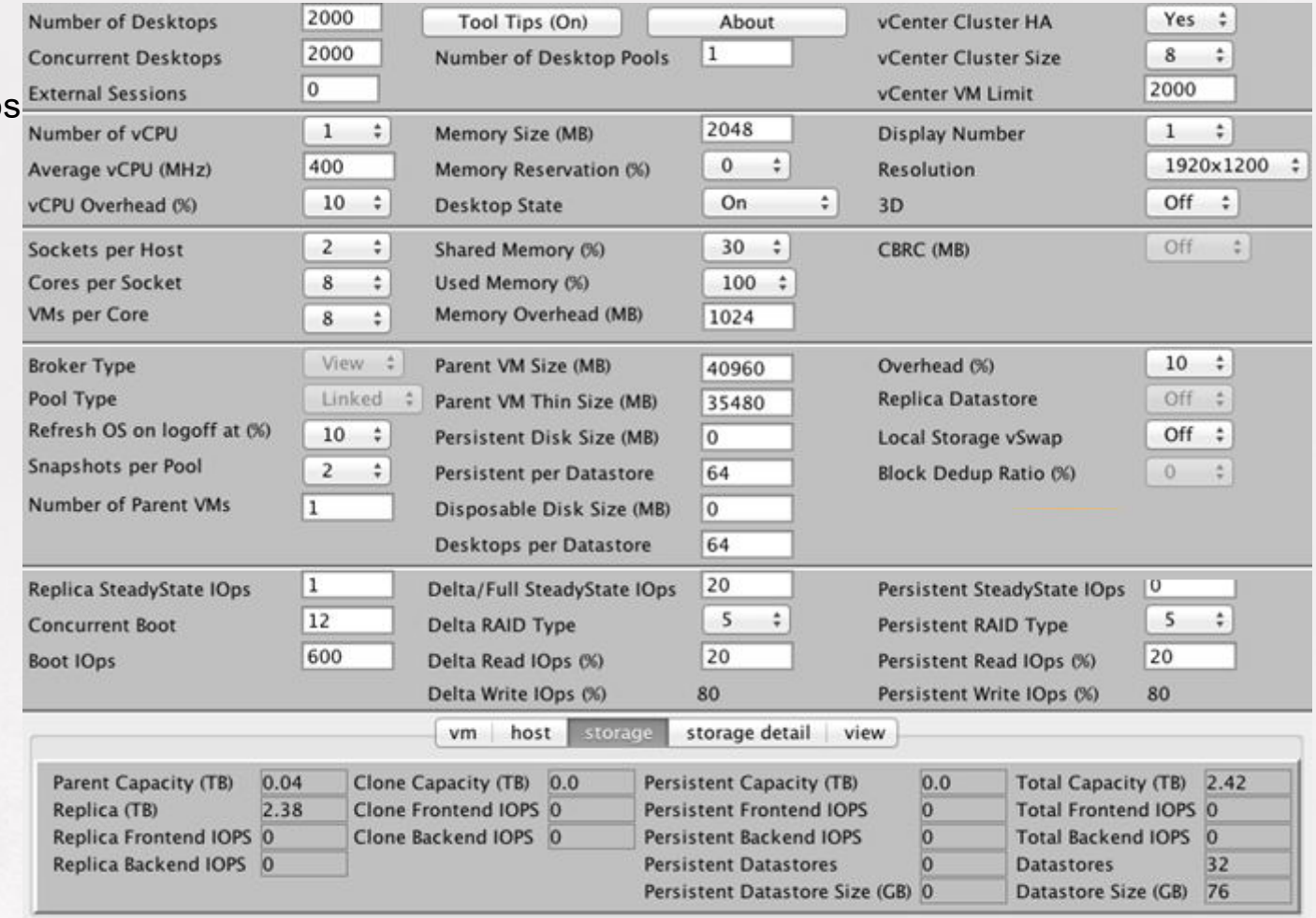


●Uso de Recursos




Gast
Windows 7
Gast
Debian
Gast Ubuntu
Gast
Windows 8
VirtualBox
Host Betriebssystem
Hardware (CPU, RAM, Festplatten)
CPU

- Recursos


Number of Desktops 2000
Concurrent Desktops 2000
External Sessions 0
Tool Tips (On)
About
Number of Desktop Pools 1
vCenter Cluster HA Yes
vCenter Cluster Size 8
vCenter VM Limit 2000
Number of vCPU 1
Average vCPU (MHz) 400
vCPU Overhead (%) 10
Memory Size (MB) 2048
Memory Reservation (%) 0
Desktop State On
Display Number 1
Resolution 1920x1200
3D Off
Sockets per Host 2
Cores per Socket 8
VMs per Core 8
Shared Memory (%) 30
Used Memory (%) 100
Memory Overhead (MB) 1024
CBRC (MB) Off
Broker Type View
Pool Type Linked
Refresh OS on logoff at (%) 10
Snapshots per Pool 2
Number of Parent VMs 1
Parent VM Size (MB) 40960
Parent VM Thin Size (MB) 35480
Persistent Disk Size (MB) 0
Persistent per Datastore 64
Disposable Disk Size (MB) 0
Desktops per Datastore 64
Overhead (%) 10
Replica Datastore Off
Local Storage vSwap Off
Block Dedup Ratio (%) 0
Replica SteadyState IOps 1
Concurrent Boot 12
Boot IOps 600
Delta/Full SteadyState IOps 20
Delta RAID Type 5
Delta Read IOps (%) 20
Delta Write IOps (%) 80
Persistent SteadyState IOps 0
Persistent RAID Type 5
Persistent Read IOps (%) 20
Persistent Write IOps (%) 80
vm
host
storage
storage detail
view
Parent Capacity (TB) 0.04
Replica (TB) 2.38
Replica Frontend IOPS 0
Replica Backend IOPS 0
Clone Capacity (TB) 0.0
Clone Frontend IOPS 0
Clone Backend IOPS 0
Persistent Capacity (TB) 0.0
Persistent Frontend IOPS 0
Persistent Backend IOPS 0
Persistent Datastores 0
Persistent Datastore Size (GB) 0
Total Capacity (TB) 2.42
Total Frontend IOPS 0
Total Backend IOPS 0
Datastores 32
Datastore Size (GB) 76


CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

¡Nos vemos en la siguiente Clase!