

# 云计算基础与应用

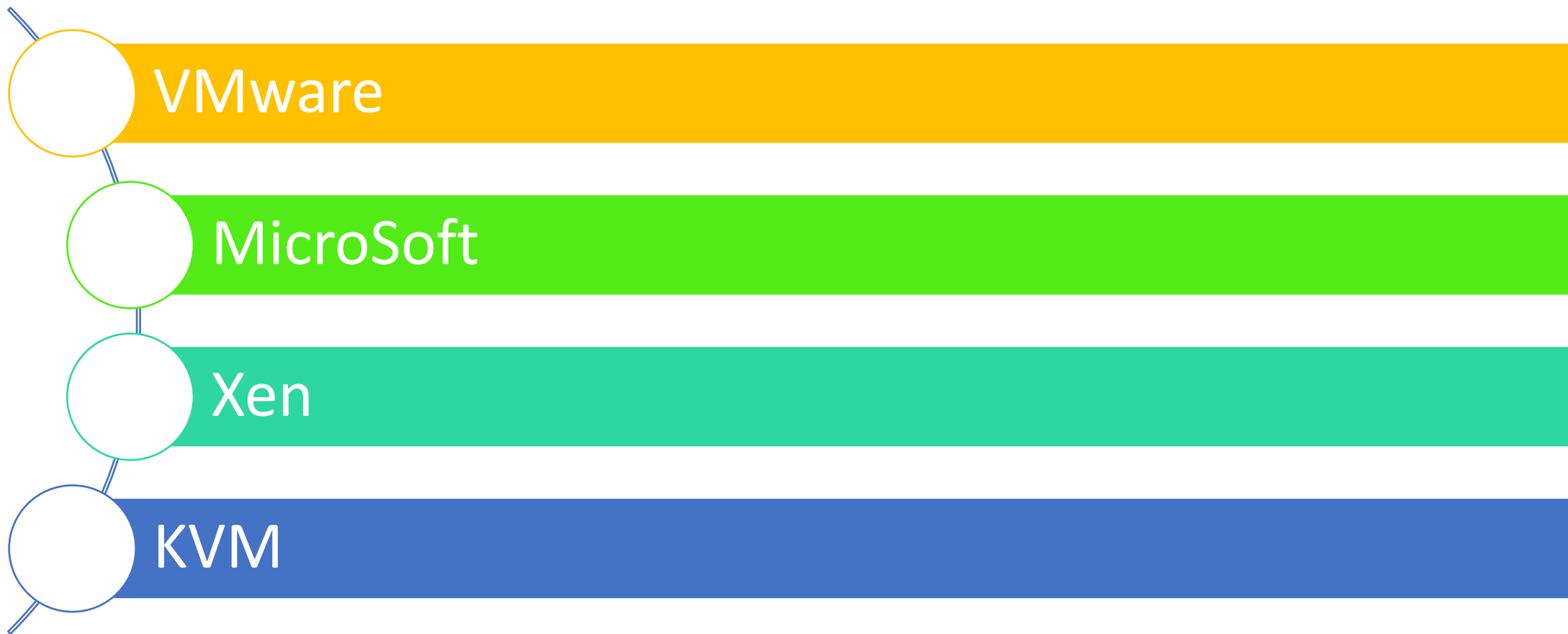


南通师范高等专科学校  
Nantong Normal College

朱亚林

## 4.3.4 主流虚拟化技术

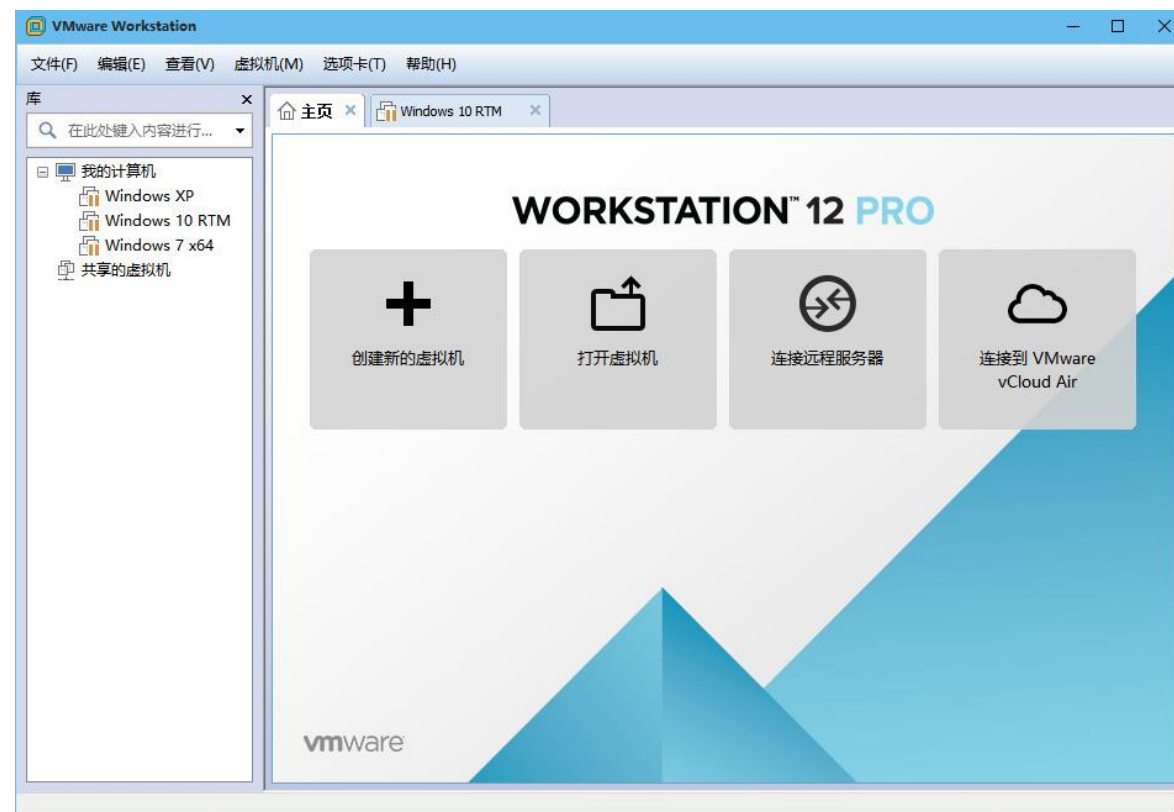
# 常见的虚拟化技术有以下同类





# VMware

VMware这个词组熟悉吗？





VMware将虚拟化技术带到了X86平台，是虚拟化行业的领先者，具有数据中心虚拟化和桌面虚拟化产品。

# VMware的产品及功能

名称	功能
VMware ESXi	VMware ESXi是Hypervisor形式的VMM，直接在安装硬件上构建和运行虚拟机。
VMware vCenter	VMware vCenter用于VMware vSphere环境的管理程序，其作为管理节点来控制和整合属于其域的vSphere主机，既可以安装在物理机的操作系统上，又可以安装在虚拟机的操作系统上。
VMware vCenter Converter	VMware vCenter Converter用于实现对物理服务器到虚拟服务器的转换过程，可以使用冷迁移和热迁移两种方式。
VMware vCenter Site Recovery Manager	VMware vCenter Site Recovery Manager主要用于数据灾难恢复，通过实现恢复流程自动化和降低管理及测试恢复计划的复杂性，加速恢复流程并确保成功执行恢复。
VMware View	VMware View用于简化虚拟桌面管理并提高桌面安全性，将传统的PC替换为可从数据中心进行管理的虚拟桌面

# 名词释义

## 什么是VMware vSphere?

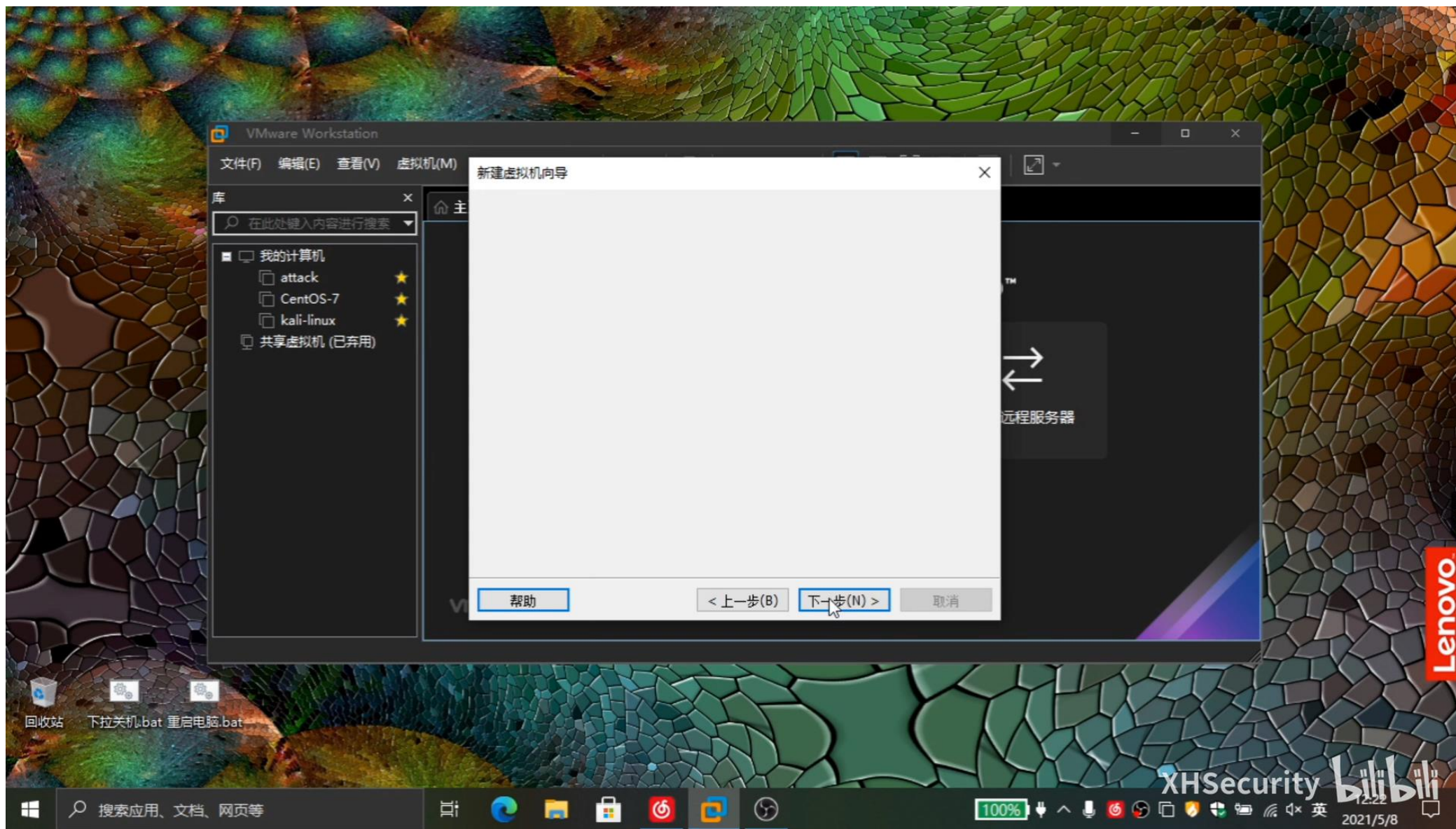
- VMware vSphere不是特定的产品或软件。VMware vSphere是整个VMware套件的商业名称。
- VMware vSphere的两个核心组件是ESXi服务器和vCenter Server。ESXi是hypervisor，用户可以在其中创建和运行虚拟机和虚拟设备。vCenter Server是用于管理网络中连接的多个ESXi主机和池主机资源的服务。

# 名词释义

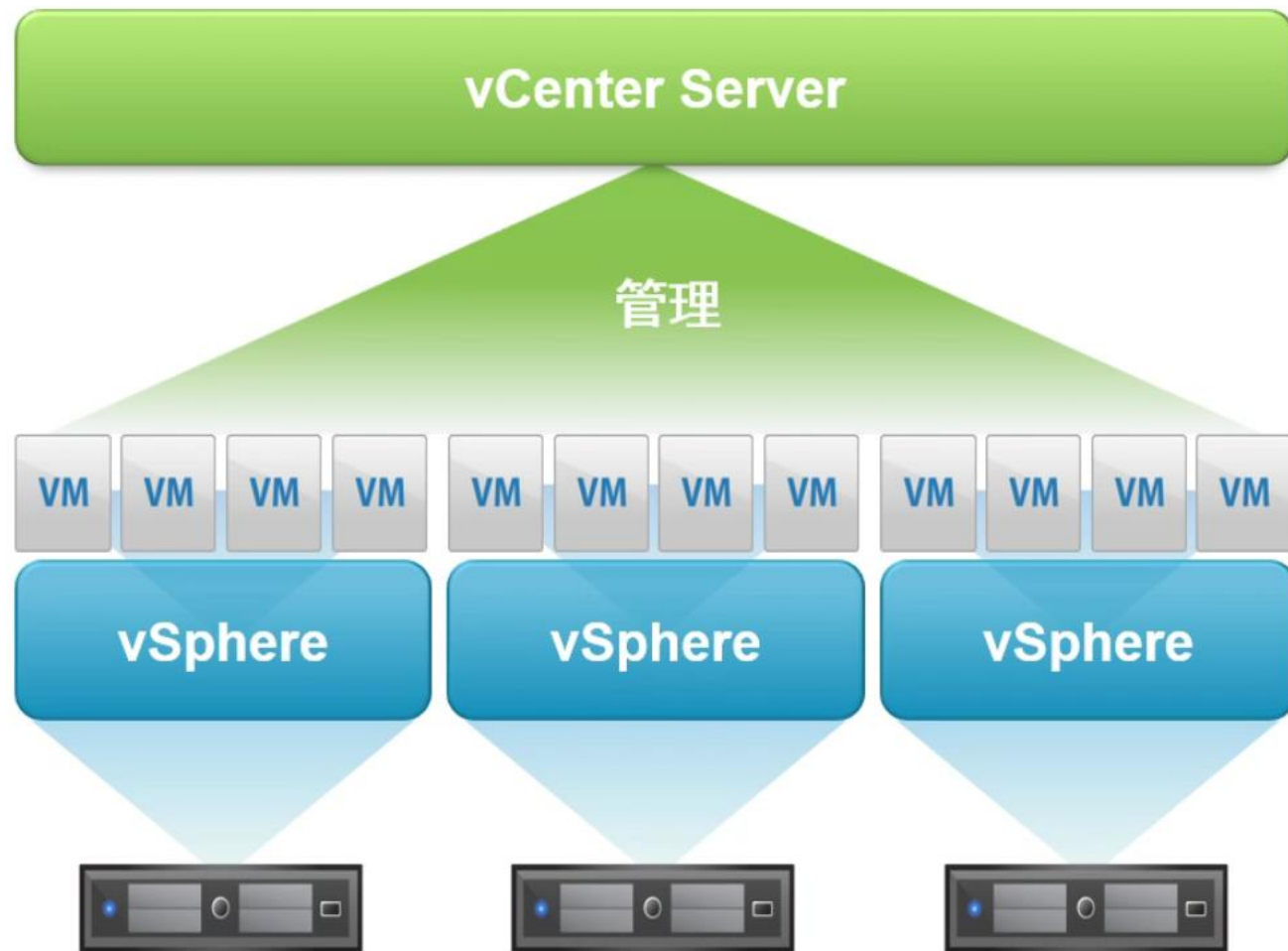
- VMware ESXi是VMware的裸机虚拟机管理程序。
- VMware vCenter是帮助用户集中管理整个VMware虚拟化基础架构的软件。
- VMware Workstation是一款基于OS的虚拟化软件。
- VMware vSphere则是一个具体的虚拟化方案。



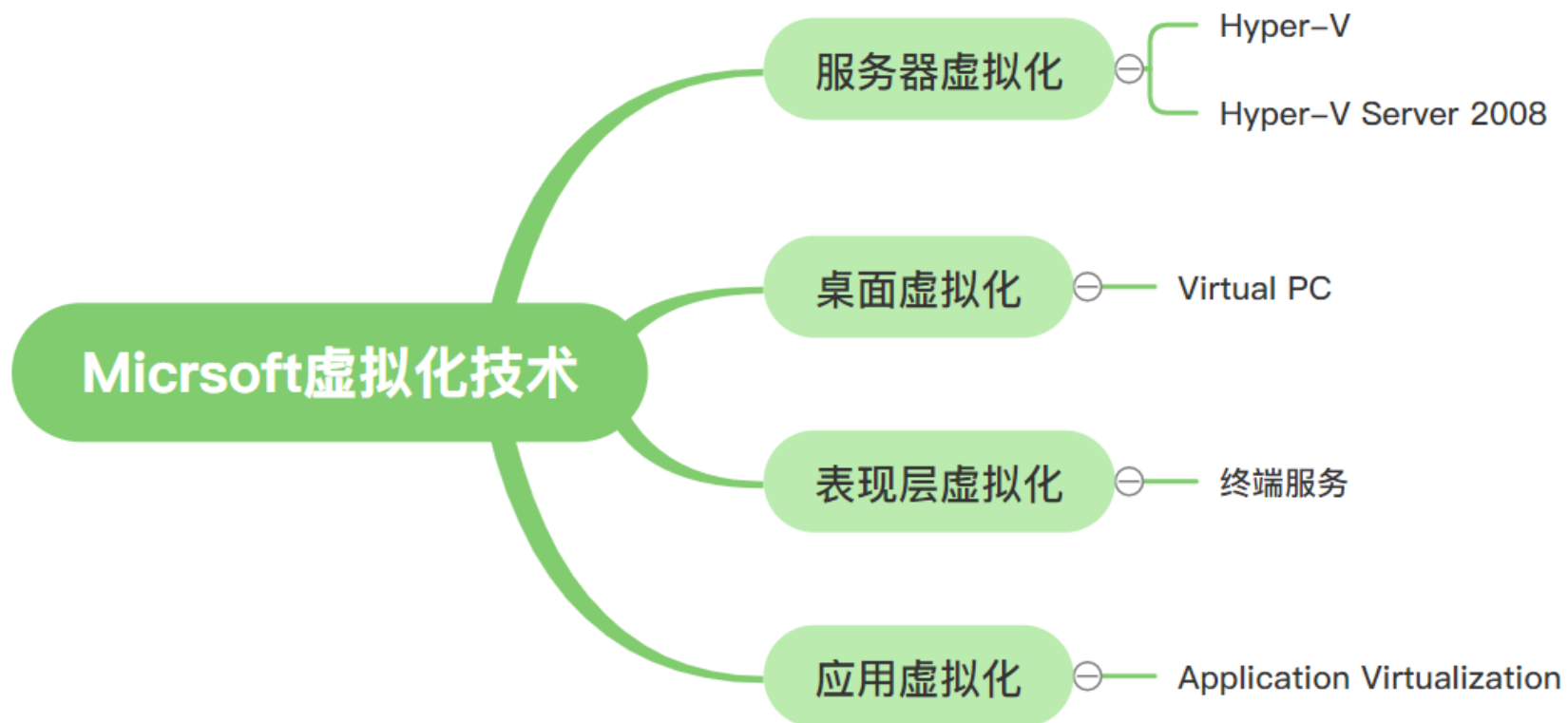
# VMware ESXi介绍



# 关于vCenter Server管理平台



# Microsoft

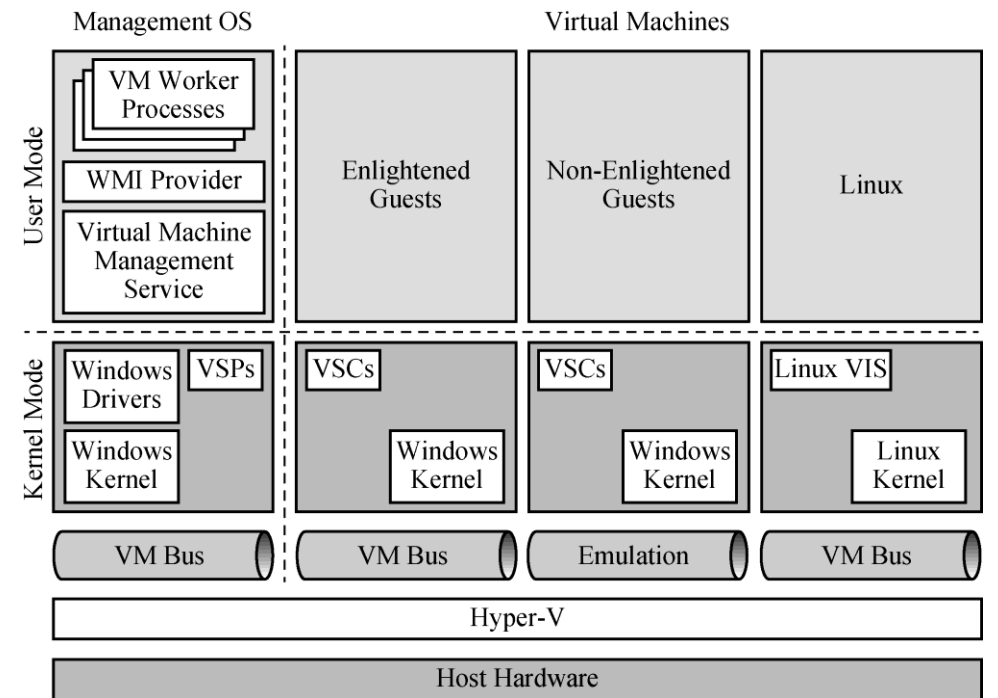


# Microsoft

- Hyper-V是微软提出的一种系统管理程序虚拟化技术，采用微内核的架构，兼顾了安全性和其他性能要求。
- Hyper-V 底层的Hypervisor运行在最高的特权级别下，微软将其称为Ring 1(Intel将其称为rootmode)，而虚拟机的OS内核和驱动运行在Ring 0下，应用程序运行在Ring 3下，这种架构不需要采用复杂的一进制特权指令翻译技术，可以进一步提高安全性。
- 从架构上讲，Hyper-V只有“硬件—Hyper-V—虚拟机”三层，本身非常小巧，代码简单，且不包含任何第三方驱动，因此安全可靠、执行效率高，能充分利用硬件资源，使虚拟机系统性能更接近真实系统性能。

# Microsoft

- Hyper-V支持分区层面的隔离。分区是逻辑隔离单位,受虚拟机监控程序支持,并且操作系统在其中执行。Microsoft 虚拟机监控程序必须至少有一个父/根分区,用于运行64位版本的Windows Server 2008操作系统。虚拟化堆栈在父分区中运行,并且可以直接访问硬件设备。随后,根分区会创建子分区用于承载来宾操作系统。根分区使用虚拟化调用应用程序编程接口来创建子分区。



# Microsoft

- 分区对物理处理器没有访问权限，也不能处理处理器中断。它们具有处理器的虚拟视图，并运行于每个来宾分区专用的虚拟内存地址区域。虚拟机监控程序负责处理处理器中断，并将其重定向到相应的分区。

# Hyper-V介绍

/10

Windows 10 的虚拟机Hyper-V

4



# Xen

- Xen是由剑桥大学计算机实验室开发的一个开源项目,是一个直接运行在计算机硬件之上的用以替代操作系统的软件层,它能够在计算机硬件上并发地运行多个客户操作系统(Guest OS)。目前已经在开源社区中得到了极大的推动。
- Xen支持x86、x86-64、安腾(Itanium)、PowerPC和ARM多种处理器,因此可以在大量的计算设备上运行。目前, Xen支持Linux、NetBSD、FreeBSD、Solaris、Windows和其他常用的操作系统作为客户操作系统在其管理程序上运行。
- Xen对虚拟机的虚拟化分为两大类:半虚拟化( paravirtualization)和完全虚拟化(fullvirtualization)。



# Xen-半虚拟化

- 半虚拟化简称PV, 是Xen主导的虚拟化技术。这种技术允许虚拟机操作系统感知到自己运行在Xen Hypervisor上而不是直接运行在硬件上, 同时也可以识别出其他运行在相同环境中的客户虚拟机。
- 在Xen Hypervisor上运行的半虚拟化的操作系统, 为了调用系统管理程序(Xen Hypervisor), 要有选择地修改操作系统, 然而却不需要修改操作系统上运行的应用程序。由于Xen需要修改操作系统内核, 因而不能直接让当前的Linux内核在Xen系统管理程序中运行, 除非它已经移植到了Xen架构。不过, 如果当前系统可以使用新的已经移植到Xen架构的Linux内核, 那么可以不加修改地运行现有系统。

# Xen-完全虚拟化

- 完全虚拟化又称硬件虚拟化, 简称HVM, 是指运行在虚拟环境上的虚拟机在运行过程中始终感觉自己是在直接运行在硬件之上的, 并且感知不到在相同硬件环境下运行着其他虚拟机的虚拟技术。
- 在Xen Hypervisor上运行的完全虚拟化虚拟机, 所运行的操作系统都是标准的操作系统, 即无须任何修改的操作系统版本, 同时也需要提供特殊的硬件设备。需要注意的是, 在Xen上虚拟的Windows虚拟机必须采用完全虚拟化技术。

# CPU完全虚拟化， I/O半虚拟化(PVHVM)

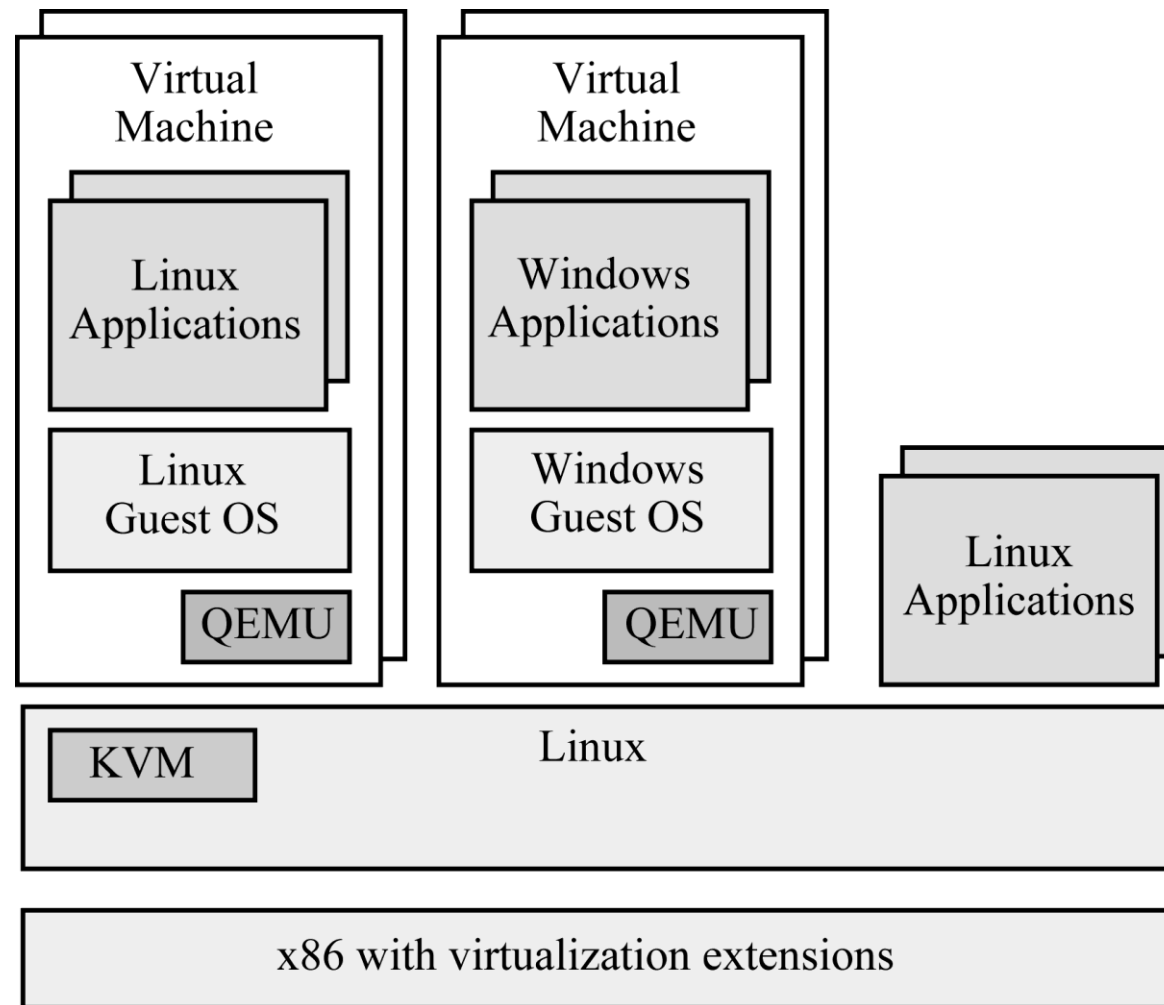
(1) Xen Hypervisor: 直接运行于硬件之上, 是Xen客户操作系统与硬件资源之间的访问接口。通过将客户操作系统与硬件进行分类, Xen管理系统可以允许客户操作系统安全独立地运行在相同硬件环境之上。

(2) Domain 0: 运行在Xen管理程序之上, 具有直接访问硬件和管理其他客户操作系统的特权的客户操作系统。

(3) Domain U: 运行在Xen管理程序之上的普通客户操作系统或业务操作系统, 不能直接访问硬件资源(如内存、硬盘等), 但可以独立并行地存在多个。

# KVM

- KVM是与Xen类似的一个开源项目, 全称是 Kernel-based Virtual Machine, 即基于内核的虚拟机。KVM是集成到Linux内核的 Hypervisor, 是x86架构且硬件支持虚拟化技术 (Intel VT或AMD-V) 的Linux全虚拟化解决方案。它是Linux的一个很小的模块, 将利用Linux做大量的工作, 如任务调度、内存管理与硬件设备交互等。
- Linux内核集成管理程序加载KVM内核模块, 管理Linux的虚拟化功能。在这种模式下, 每个虚拟机都是一个常规的Linux 进程, 通过Linux程序进行调度。

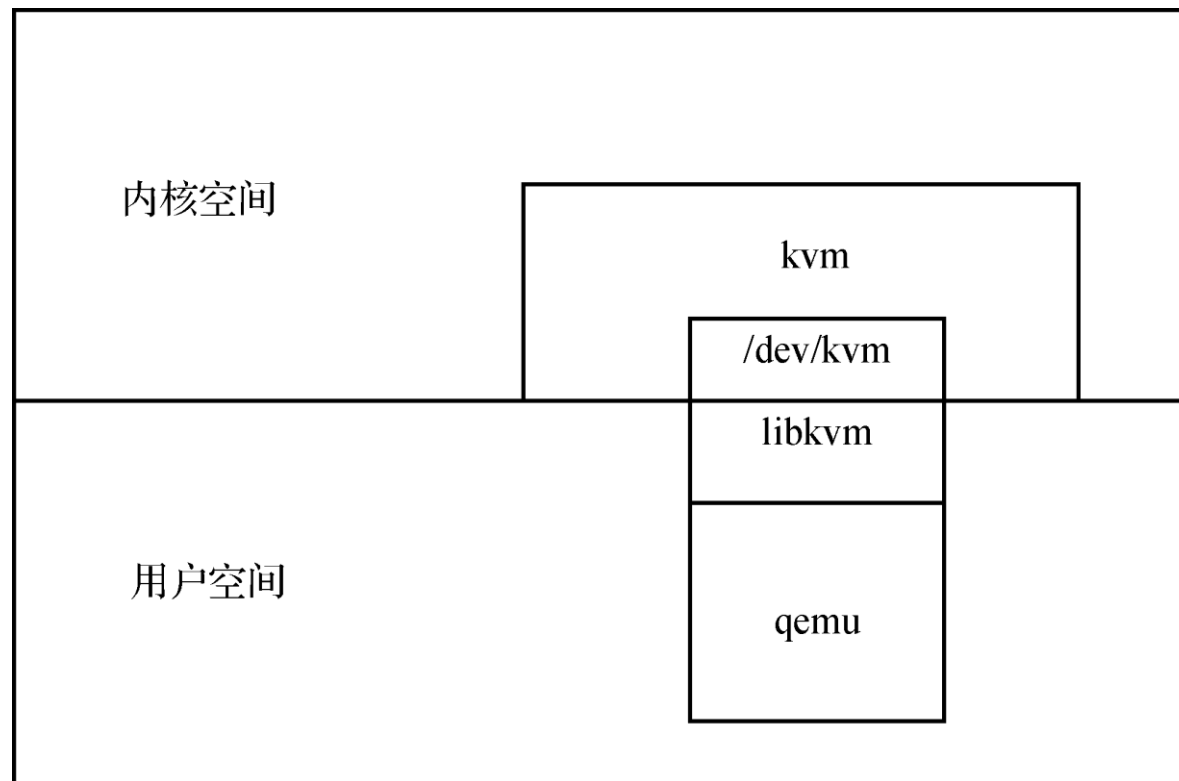


# KVM

- KVM是Linux Kernel的一个模块。加载了该模块后，才能进一步通过其他工具创建虚拟机。但仅有KVM模块是不够的，因为用户无法直接控制内核模块去执行任务，还必须有一个运行在用户空间的工具才可以，KVM开发者选择了已经成熟的开源虚拟化软件QEMU。
- QEMU是一个虚拟化软件，它可以虚拟不同的CPU。KVM使用了QEMU的一部分，并稍加改造，就变成了可控制KVM的用户空间工具。

# KVM

- QEMU将KVM整合进来, 通过ioctl函数调用/dev/kvm接口, 将有关CPU指令的部分交由内核模块来做。KVM负责CPU虚拟化和内存虚拟化, 但KVM不能模拟其他设备。QEMU模拟I/O设备(网卡、磁盘等), KVM加上QEMU之后就能实现真正意义上的服务器虚拟化, 所以称之为QEMU-KVM。QEMU模拟其他硬件, 同样会影响这些设备的性能, 于是又产生了pass through半虚拟化设备virtio\_blk、virtio\_net, 以提高设备性能。



## 4.4 用户交互技术

# 用户交互技术

- 随着云计算的逐步普及,浏览器已经不仅仅是一个客户端的软件,而逐步演变为承载着互联网的平台。浏览器与云计算的整合技术主要体现在两个方面:浏览器网络化与浏览器云服务。
- 国内各家浏览器都将网络化作为其功能的标配之一,主要功能体现在用户可以登录浏览器,并通过账号将个性化数据同步到服务端。用户在任何地方,只需要登录自己的账号,就能够同步更新所有的个性内容,包括浏览器选项配置、收藏夹、网址记录、智能填表和密码保存等。
- 目前的浏览器云服务主要体现在P2P下载、视频加速等单独的客户端软件中,主要的应用研究方向包括基于浏览器的P2P下载、视频加速、分布式计算和多任务协同工作等。在多任务协同工作方面,AJAX(Asynchronous JavaScript and XML,异步JavaScript和XML)是一种创建交互式网页应用的网页开发技术,改变了传统网页的交互方式,改进了交互体验。



## 4.5 安全管理技术

# 安全管理技术

- (1) 数据存储及访问控制。数据存储及访问控制包括如何有效存储数据以避免数据丢失或损坏, 如何避免数据被非法访问和篡改, 如何对多租户应用进行数据隔离, 如何避免数据服务被阻塞, 如何确保云端退役 (atrest) 数据的妥善保管或销毁, 等等。
- (2) 数据传输保护。数据传输保护包括如何避免数据被窃取或攻击, 如何保证数据在分布式应用中有效传递等。
- (3) 数据隐私及敏感信息保护。数据隐私及敏感信息保护包括如何保护数据所有权, 并可根据需要提供给受信方使用, 如何将个人身份信息及第三方数据移动到云端使用等
- (4) 数据可用性。数据可用性包括如何提供稳定可靠的数据服务以保证业务的持续性, 如何进行有效的数据容灾及恢复等。
- (5) 依从性管理。依从性管理包括如何保证数据服务及管理符合法律及政策的要求等。