实验 1　研究报告

课程名称：　Linux 应用技术基础　　实验类型：　　研究报告

实验项目名称：　　虚拟化技术在云计算数据中心的应用

学生姓名：　　　　专业：　信息安全　　学号：　　

电子邮件地址：　　

实验日期：　2020　年　4　月　20　日

虚拟化技术在云计算数据中心的应用

摘要： 目前，互联网以及分布式技术的快速发展，对云计算数据中心提出了更高的要求。虚拟化技术解决了电脑主机限制操作技术的问题，可以实现多个操作技术同时运行，给云平台带来了许多优势，但同时也给用户带来了许多新的安全风险。因此，本文主要研究了虚拟化技术在云计算数据中心中的应用以及存在的各种安全风险和应对方法。

关键词： 云计算；虚拟化；应用；安全

正文：

一、云计算与虚拟化的关系

云计算技术作为一种越来越成熟的商用计算模型，它将各种服务任务分布在大量计算机构成的网络资源池上，使用户能够根据需要获取存储空间、计算能力、带宽以及其它信息服务。它的主要优势在于低成本、高扩展性、管理方便、使用灵活、资费灵活。

由于云计算的运作范围极其之广,相应的在云计算数据中心方面也有很高的要求。旧有的数据中心具有不科学、不合理计划的性质，对于硬件的使用率不高，出现了资源不能够集中以及反复建立的现象，导致数据中心性能不高，损耗大以及管理难度加大，使得其跟不上云计算的发展。

虚拟化技术是提升云计算数据中心的前提，可以符合客户的要求以及提高服务水平。它有三层含义：虚拟化的对象是各种各样的资源；经过虚拟化后的逻辑资源对用户隐藏了不必要的细节；用户可以在虚拟环境中实现其在真实环境中的部分或者全部功能。借助它，一方面多台服务器可发生相互关联（即管理资源的优化），另一方面相关软件能朝着合理简化的方向得到重新配置（即相关程序的二次开发）。因此，将网络虚拟化技术应用到云计算平台，就能达成多个独立操作系统并行运行于同一网络环境的目标，从而大幅提升云计算平台的计算能力与运行质量。

二、云计算数据中心中虚拟化技术的分类

1、数据平面虚拟化

数据平面虚拟化是虚拟化技术衍生的周边技术，为虚拟化交换提供了一个新场所，提高了云计算数据中心的处理效率和运行速度，减少了人们的办公时间。数据平面虚拟化依托多路径转发模式，借助宽带与接入槽、核心层之间的“协作”，达成信息的交互，在一定程度上提高了计算机的运行效率和信息储存、转发的速度，拓展了计算机的运行空间。

但是，其存在一定运行缺陷，比如多路径转发会使计算机网络系统变得更为复杂化，带来运行安全的隐患，而且多路径转发的模式也会造成转发效率降低。因此，数据平面虚拟化技术实际运用中，对电脑主机运算能力的要求较高，对相关工作人员的解决问题能力要求也较高。因此相关工作人员需要不断创新改革，解决其运行中出现的问题，不断提高个人技术水平，促进云计算行业的快速发展。

2、控制平面虚拟化

控制平面虚拟化即用一个主板电脑控制多个操作系统，极大提高了云计算的数据调取能力。虚拟化数据信息交替分为横向和纵向两种情况。

对纵向控制平面虚拟化技术来说，其在运行过程中需要增加上一级接口的数量，减少下一级的技术要求。因此运行效率将下降，转发速度降低，且运行功能受到限制，仅能简单传送数据。横向控制平面虚拟化技术和纵向控制平面虚拟化技术的工作原理相似，都是运用一个主体控制多个操作系统，但数据传送口采用分布式的数据结构。

综上所述，平面虚拟化技术可以增加数据传送段的传送接口，可以统一管理庞大的数据信息，运用一个主机可以控制数万台操作系统。

三、云计算数据中心中虚拟化技术的特点

1、软件完成

虚拟化技术能够组成核算池,核算池拥有超级核算的能力。一个云核算中心含有几万台物理服务器。与此同时, 每一台服务器都会有虚拟机数目，有的可达到 100 个。由于不同的硬件虚拟化以及 CPU 功能的不断提升，物理服务器上出现了众多的运转虚拟机。此外，根据软件的模式模拟硬件,根据软件的分类方式分割服务器资源,塑造集中的虚拟资源池,建立一个环境以供虚拟机运行。

2、隔离操作、封装独特

在同一个物理服务器上操作虚拟机要彼此分离，确保虚拟机与虚拟机之间各司其职,其中包含核算分离、数据分离、储存分离以及网络分离等，要保证虚拟机彼此间不会透漏数据，程序要通信就要运用特定配备的网络。

虚拟机由运作系统以及应用封装而成，只有进行了封装，虚拟机才能自由移动。真实的软件经过封装后变成规范的虚拟硬件,所有的虚拟机都运用文件的方式进行储存，以利于备份、移动以及复制等操作。

3、硬件单独、接口准确

服务器的虚拟化使得虚拟机以及硬件相互分离，使得虚拟机能够自由移动，涉及范围广。同时虚拟机也包含多种硬件平台,可以使各种操作系统能够平稳的运行，其接口也比较精确,能够确保其兼容性质。

四、虚拟化技术在云计算数据中心中的应用

1、服务器虚拟化

虚拟化技术是很多个操作系统在同一台物理机方面上一起运作，但是操作系统就像是独立操作的,与不与其他系统相联系。按服务器结构划分，服务器虚拟

化可归为两类，寄居结构和原生结构。寄居结构指在已安装到位的传统操作系统中运行虚拟化操作系统，原生结构指将虚拟化操作系统在服务器硬件中进行部署，即通过硬件配置来实现服务器虚拟化控制。

在应用中，寄居结构不用考虑虚拟化操作系统与相关硬件的匹配度，应用起来较为方便，但同时易受原有操作系统的影响，一旦发生问题可能致使系统瘫痪。

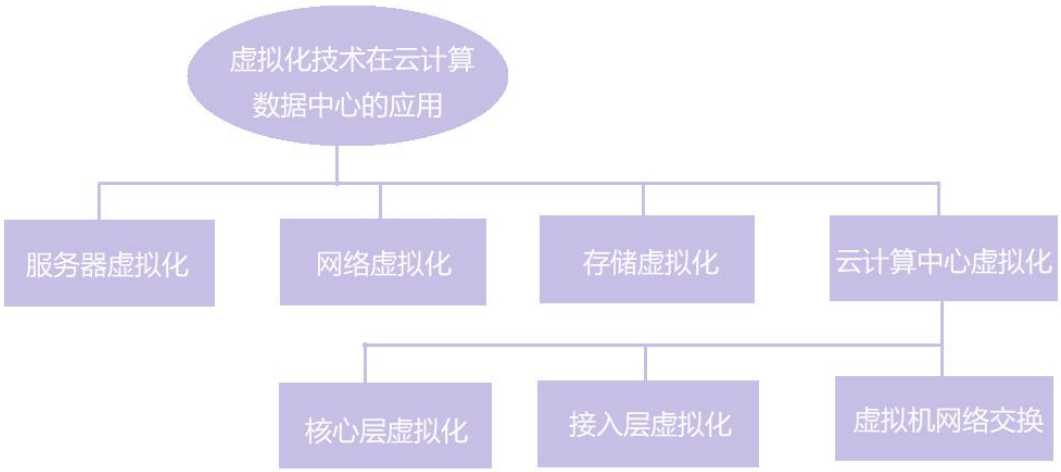
2、网络虚拟化

网络虚拟化是对同一个物理网络资源而言,运用独特的技术划出独立的虚拟网络资源。网络虚拟化当中的分权限访问以及自由掌控权等技术能够符合很多用户的需求，可以有效提升网络资源的利用效率。该项技术的应用可在多个具有明确结构与功能分配的层次之间展开，如核心层、访问层、交换层等等。因为云计算用户分散性大、规模大，故一般要考虑多种接入方式的采用。这样，必须借助技术手段来确保网络接入的适应性以及可扩展性。

3、储存虚拟化

储存虚拟化技术大致上就是要完成储存方面上的虚拟化操作，把多台物理储存器结合起来，以一台储存设备的方式提供服务，不同的用户可以依据自己的需求调用资源池中的资源储存。其主要的产品有网络储存协议的虚拟化，它的特征就是对网络性能有较高的要求，稳定性以及储存性有较低的要求。物理硬盘的分区也是虚拟化的，它的特征是难以修改储存空间容积的大小。

各类存储虚拟化的应用分析如下图所示：



图一 虚拟化技术在云计算平台的应用架构

4、计算中心虚拟化

（1）核心层虚拟化

核心层虚拟化是通过对系统资源的灵活调度与动态调整达成资源利用质和效的双双提升，从而加强了核心层网络的数据交换能力与数据接入规模。核心层虚拟化借助虚拟机箱技术简化设备管理流程、经由端口捆绑达成跨交换机的相互连接、经由以太网链路捆绑挖掘系统冗余能力实现。

（2）接入层虚拟化

接入层虚拟化是对接入层作科学分级。它要求基于以太网环境，对走线作分析，选择各种部署方式与相应交换机发生关联，适时发展以太网 DCE,以实现"拥塞通知”、“传输选择增强”、“优先级流量控制”等高级功能。

（3）虚拟机网络交换

虚拟机网络交换可分为物理网卡虚拟化和虚拟网络交换机。虚拟网络交换机是通过对交换机与网卡功能的虚拟，实现主机内部产生交换机，以及网卡与端口的一一连接。虚拟网卡拥有多个独立逻辑，可支撑流量灵活调度。此外，虚拟机网络交换应支撑深度包检测、端口镜像等方式对虚拟机的访问与监控；满足VLAN、QoS 等层面的必要属性；满足虚拟机迁移与业务连续性的不相关。

五、虚拟化的安全风险

1、虚拟化平台安全风险

（1）平台自身安全漏洞

虚拟化平台自身也存在安全漏洞，攻击者可能利用这些漏洞，通过虚拟化网络来攻击虚拟化平台的相关接口，可能导致基于虚拟化平台的各类业务均出现不可用或信息泄露。

（2）可控风险

虚拟化平台技术是从国外引进的，目前常见的主流商用虚拟化平台被几个大的国外厂商垄断，且不对外提供关键、核心接口，更不开源，导致在其上构建和部署安全措施困难，可控性差。再加上可能的利益驱使和网络战需要，无法判别是否留有控制“后门”，可信度有待商榷。

（3）虚拟资源池内恶意竞争风险

处于虚拟资源池内的多虚拟主机会共享统一硬件环境或软件环境，经常会出现恶意的抢占资源，影响了平台资源的可用性，进而影响虚拟化平台的服务水平，造成安全风险。

2、虚拟化网络安全风险

（1）虚拟化网络不可见风险

虚拟化的网络结构，使得传统的基于确定网络结构的安全防护变得困难。在云环境中，虚拟化资源会放在同一的资源池中，供各应用调配资源来实现业务的运行。在这种情况下，传统安全防护设备无法深入虚拟化平台内部进行安全防护，难以达到恶意代码的防护，流量监控，协议审计等安全要求。

（2） 网络边界动态化风险

为了实现虚拟化环境下的动态负载，出现了虚拟机动态漂移技术，导致虚拟化主机的真实位置也会随之改变，造成边界的安全策略也需要随之转移。若边界隔离、安全防护措施与策略不能跟随虚拟机漂移，会使得边界防护措施和防护策略难以起效，造成安全漏洞。

（3）多租户混用安全风险

云计算中的多租户架构通过共享系统或电脑运算资源的方式提升了资源利用率，同时云计算供应商根据租户对于共享资源使用量来进行计费。

多租户架构结合虚拟化技术形成了云计算的基础。在多租户的云计算环境里，由于云计算平台的开放性，平台上租户繁杂，租户间也可能存在一定的利益竞争关系，让云计算资源滥用、租户间的攻击等成为可能，传统安全防护措施在应付这些来自云环境内部的安全挑战时显得捉襟见肘。

（4）网络地址冲突风险

由于用户对虚拟机有完全控制权，所以可以随意修改虚拟机的 IP 或 MAC 地址，可能造成与其他虚拟机的地址冲突，从而影响虚拟机通信。

（5）恶意虚拟机实施攻击风险

虚拟机通信隔离机制不强，恶意虚拟机可能监听其他虚拟机的运行状态，实施 Dos 攻击，恶意占用内存、网络带宽等，影响其他虚拟机的运行。

3、虚拟化主机安全风险

（1）虚拟机恶意抢占资源风险

虚拟机完全由最终用户控制，恶意份子和被控制的虚拟机可能恶意抢占网络、存储和运算资源，导致整体云平台资源耗尽，从而影响其他关键业务系统的正常运行。

（2）虚拟机安全审计风险

在云平台构建完成后，将同时运转数量众多的虚拟机。并且，对虚拟机的操作人员各不相同，安全意识和安全防范措施也参差不齐。缺乏安全审计会导致某些虚拟机感染病毒 后进行非法操作，甚至可能利用已有漏洞，获 得更高权限，从而实施各种攻击。

（3）虚拟机镜像安全风险

比起物理主机，虚拟机镜像是以文件形式存在，因此，容易被复制和修改，同时，不同安全级别的版本镜像可能被替换。虚拟机镜像文件缺乏有效的安全控制措施，将给虚拟机的合法用户带来危险。

4、虚拟化存储安全风险

（1）数据隐私泄露风险

当终端用户把自己的数据通过虚拟化存储交付给云计算提供商后，数据的优先访问权已经发生了变化，即云计算提供商享有了优先访问权，因此如何保证数据的隐私变得很重要。但大部分敏感的，不宜公开的数据还会面临来自非法入侵后进行窃取或篡改，进而带来的数据保密性和完整性风险。

（2）数据可用性风险

当数据的完整性遭受破坏时，数据可用性也会遭受影响，数据失真，尤其是应用的关键参数失真最为严重。在虚拟化环境下，数据碎片化存储，在整合时出现问题，导致应用服务中断，进而造成应用可用性的风险，所以如何进行容灾、备份和恢复也是一个严峻的问题。

（3）数据审计风险

在云环境中，用户的数据不再保存在用户本地，大多依靠完整性验证的方式使用户确信他们的数据被正确的存储和处理。为了保证数据可恢复性及冗余性，在云计算环境中，必须要采用冗余存储的方式，但这就需要使用专门数据审计方法来验证和确保多个位置数据的一致性和完整性。同时，针对数据的使用者信息，也需要通过审计措施来进行记录。

（4）数据安全检测风险

在虚拟化存储环境下，数据往往是离散的分布在“云”中不同的位置，用户无法确定自己的数据究竟在哪里，具体是由哪个服务器进行管理，也因此造成当数据出现不可用，破坏，甚至泄露时，很难确定具体的问题点。

（5）数据库安全风险

数据库通常作为非结构化数据的索引，通过结构化表的表现形式，为前端应用和后方数据提供桥梁；同时，对于结构化的数据，数据库本身就进行了数据存储。恶意攻击通常会通过数据库漏洞或恶意代码的方式进行非法提权，从而通过数据库结构化语句窃取、篡改甚至破坏后台存储的数据，威胁到数据的保密性、完整性和可用性。

4、虚拟化应用安全风险

（1）身份鉴别风险

应用放置在云端，在实现资源共享的同时，会带来信息泄漏的风险。由于网络的不确定性，首要问题就是要确认使用者的身份、确保身份的合法性。由于工作需要，不同部门、不同职责的工作人员应用需求不同，信息使用权限不同，必须要对使用者身份进行统一的认证，统一授权，统一审计。

一旦攻击者获取使用者的身份验证信息，假冒合法用户，用户数据完全暴露在其面前，其他安全措施都将失效，攻击者将可以为所欲为，窃取或修改用户数据。

（2）应用服务可用性风险

任何形式的应用都存在可用性风险，而一旦可用性风险被威胁利用，进一步引发了安全事件，则会带来应用的不可用，进而导致业务受阻。缺乏对应用服务的审计也会带来可用性风险，如果通过审计和分析策略在故障或入侵之前可以察觉到异常信息，可能就避免了事故的发生。而在云计算环境下，因为应用的高度集中和边界模糊，可能一次单台主机的不可用，都会带来多种业务的不可用。

（3）WEB 攻击风险

WEB 攻击主要指针对 WEB 服务的各类应用恶意代码攻击，诸如 SQL 注入攻击、XSS 攻击、网页篡改等，通常是由于对 HTTP 表单的输入信息未做严格审查，或 WEB 应用在代码设计时存在的脆弱性导致的。

六、虚拟化安全风险的处理技术

1、同态加密技术

数据加密是保护数据安全的一个普遍采用的技术。在基于虚拟化的云平台环境下，可采用最新的同态加密技术。运用这种加密技术可以实现明文上执行指定的代数运算，结果等同于在密文上的另一个代数运算结果同态加密。其思想起源于私密同态，它允许在不知道解密函数的前提下对加密数据进行计算。它对数据的加解密可通过矩阵和向量的各种运算来实现，并支持对加密字符串的模糊检索和对密文数据的加减乘除。

2、基于加解密的数据安全存储技术

公有云中存储的数据一般属于外包数据，存在不少基于传统的加解密技术的研究来确保外包数据的安全。目前有基于代理重加密方法的数据分布式安全存储方案，但该方案存在恶意服务器和任意一个恶意用户勾结就能计算出所有密文数据的解密密钥的漏洞，严重威胁数据的安全；也可采用一种基于密钥导出方法的非可信服务器数据安全存储方案。这些存储方案的实际效果目前还有待于进一步研究和完善。

3、虚拟化软件安全技术

在虚拟化云平台中，软件完全由云服务商来管理和操作，用户不能直接接入虚拟化软件层。为了保障在计算机上多个操作系统并发运行的安全性，虚拟化软件必须要采用访问控制策略来管理虚拟化软件层的访问权限，这样才能同时保证虚拟化层次上的各用户数据安全。

七、结语

云计算平台与以往传统计算环境的一大区别在于其引入了虚拟化技术。从安全角度来说，攻击者可以从云计算平台本身、虚拟化的网络环境等多方面实施攻

击渗透，也正是虚拟化技术的引入使得传统的安全手段不能满足其安全需要，需要针对其特点重新定制。云计算平台的可用性、可靠性、数据安全性和运维管理能力是安全建设的重要指标，传统网络下的各项安全技术，如密码技术、边界防护技术、入侵检测技术、审计技术等在云计算环境下仍然需要，并需要针对云计算特别是虚拟化技术的应用给信息安全带来的新问题，需要重点解决。

当前，无论公有云还是私有云环境下，对用户来说一方面要对虚拟化带来的风险有充分的认识，引起足够的重视。另一方面不能因为有风险而因噎废食，要充分利用新的安全技术，合理运用云计算平台。

参考文献：

[1] Baroncelli, F., Martini, B. & Castoldi, P. Network virtualization for cloud computing. *Ann. Telecommun.* **65,** 713–721 (2010).
https://doi.org/10.1007/s12243-010-0194-y

[2] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: a survey," in *IEEE Communications Magazine*, vol. 51, no. 11, pp. 24-31, November 2013.
https://doi: 10.1109/MCOM.2013.6658648

[3] Du, Y., Zhang, R. & Li, M. Research on a security mechanism for cloud computing based on virtualization. *Telecommun Syst* 53, 19–24 (2013).
https://doi.org/10.1007/s11235-013-9672-7

[4] 莫建华. 基于虚拟化技术的云计算平台安全风险研究[J]. 信息技术与信息化, 2019(10):214-216.
doi：10.3969/j.issn.1672-9528.2019.10.068

[5] 褚辰琛. 虚拟化技术在新一代云计算数据中心的应用研究[J]. 信息与电脑, 2019(6):1-2.

[6] 闫鸿斌. 网络虚拟化技术在云计算数据中心的应用[J]. 电子技术与软件工程, 2019(14):3-4.

[7] 吕维体. 虚拟化技术在新一代云计算数据中心的应用研究[J]. 通讯世界, 2017(10):98-99.

[8] 柴立, 解建仓, 龚尚福. 大数据背景下金保数据中心建设关键技术研究[J]. 现代电子技术, 2019, 42(10):136-140.

[9] 肖锟, 袁俊. 云计算平台的数据安全技术分析[J]. 黔南民族师范学院学报, 2014, 34(6):102-105.

[10] 周立广.研究云计算环境下的存储虚拟化文档加密[J].通讯世界,2019,26(3):306-307.

[11] 王航.云计算中服务器虚拟化技术分析[J].信息系统工程,2019(2):38-38.

[12] 任新新.网络虚拟化映射综述[J].计算机产品与流通,2019(6):35-35.

[13] 侯俊芳.浅析云计算平台安全现状与解决方法研究[J].天津职业院校联合学报,2019,21(2):109-115.

[14] 宋杨.云计算网络安全策略的学习探讨[J].科学技术创新,2019(6):79-80.

[15] 钟原.基于云计算数据中心网络设计[J].微型电脑应用,2019(3):59-61.

[16] 杨继武.网络虚拟化在云计算领域应用[J].电子技术与软件工程,2019(3):1-1.

[17] 由海涌,姜达,侯昭宇.虚拟化技术在新一代云计算数据中心的应用研究[J].电子技术与软件工程,2014(12):221-221.

[18] 闫盛,石淼.基于云计算环境下的网络安全技术实现[J].计算机光盘软件与应用,2014,17(23):168-168.

[19] 王晓萌.网络虚拟化技术在云计算数据中心的应用分析[J].信息与电脑,2018(12):41-42.

[20] 黄泽星.虚拟化云计算管理平台升级解决方案[J].铁路通信信号工程技术,2019,16(2):50-54.

[21] 丁一军,于桂荣.云计算：安全技术问题探讨[J].科技创新导报,2015(7):58-59.