服务器虚拟化在网络信息体系中的应用和安全防护

李　超[1],党增江[2]

(1.中国人民解放军92728部队,上海 200040;2.中国航天科工集团第二研究院七〇六所,北京 100854)

摘　要:针对服务器虚拟化技术在网络信息体系应用过程中存在的安全隐患和风险,提出了一种服务器虚拟化在网络信息体系应用中的安全防护设计方案,实现了服务器虚拟化在部署环境、宿主机、虚拟机、系统运行和运维管理等方面的安全防护,并搭建试验环境进行了安全防护验证,有助于推动服务器虚拟化在企事业单位信息化和数字化转型中的落地应用。

关键词:虚拟化技术;服务器虚拟化;安全防护

中图分类号:TP309　　文献标识码:A　　DOI:10.19358/j.issn.2097-1788.2023.01.010

引用格式:李超,党增江.服务器虚拟化在网络信息体系中的应用和安全防护[J].网络安全与数据治理,2023,42(1):72-78.

Application and security protection of server virtualization in network information system

Li Chao[1], Dang Zengjiang[2]

(1.The Chinese People Liberation Army 92728 Army, Shanghai 200040, China;
2.Institute 706, Second Academy of China Aerospace Science and Industry Corporation, Beijing 100854, China)

Abstract: In view of the potential security problems and risks of server virtualization technology in the application network information system, this paper proposes a security protection design scheme of server virtualization in the application of network information system, which realizes the security protection of server virtualization in deployment environment, host, virtual machine, system operation, operation and maintenance management, etc., and built a test environment to verify security protection effect, helping to promote the application of server virtualization in the informatization and digital transformation of enterprises and institutions.

Key words: virtualization technology; server virtualization; security protection

0 引言

随着虚拟化技术的快速发展,服务器虚拟化作为最常用的虚拟化技术已经在各行各业得到了广泛应用。服务器虚拟化通过运用相应的虚拟化软件将服务器中的资源进行整合转换,实现对资源的均衡分配,并且还能实现对网络资源的合理利用,进而达到提高工作效率的目的[1-4]。

目前,服务器虚拟化有“一虚多”“多虚一”和“多虚多”三种方式[5]。“一虚多”是传统的虚拟化方式,实现把一台物理服务器虚拟为多台逻辑服务器,虚拟出的逻辑服务器彼此独立、互不干扰,每个逻辑服务器单独运行一个操作系统的副本,并且应用程序都可以在相互独立的空间内运行而不相互影响。“多虚一”实现把多台物理服务器虚拟成一台逻辑服务器,多台物理服务器之间使用高速网络或专用总线连接,在虚拟出的这台逻辑服务器上运行单一的操作系统副本,应用程序运行在逻辑服务器中可以同时使用多台物理服务器中的硬件资源,构成一个大节点服务器。“多虚多”是在“多虚一”的技术上,再将虚拟出的逻辑服务器划分为多台虚拟服务器,且性能都能根据资源池中实际资源情况进行灵活配置和调度。无论那种服务器虚拟化方式,都存在虚拟机逃逸、跳跃、蔓延,虚拟机镜像被非法拷贝,虚拟机间流量难以被审计等安全风险,这

些安全风险一旦被黑客利用进行网络攻击，容易造成关键数据被窃取，甚至虚拟机被完全控制，这对服务器虚拟化在军工等特殊行业的应用带来了巨大挑战[6]。

本文重点分析了常用的“一虚多”服务器虚拟化在网络信息体系应用中面临的安全风险，从部署环境、宿主机、虚拟机、系统运行和运维管理等方面的采取安全防护措施，形成一套服务器虚拟化安全防护解决方案，推动服务器虚拟化在企事业单位网络信息体系中的落地应用。

1 服务器虚拟化安全风险分析

服务器虚拟化技术的应用提升了计算机服务器的应用效率及价值，但在实际的技术应用过程中，尤其在军工企业等敏感网络信息体系中，还存在一定的安全风险[7-8]，这在一定程度上影响了服务器虚拟化在军工等特殊行业的应用效果。下面对虚拟化技术的安全风险进行分析和总结。

1.1 技术架构安全风险

在服务器“一虚多”的虚拟化方式下，所有的虚拟机共享宿主机上的硬件资源并彼此逻辑隔离，依靠虚拟机管理器进行统一管理和调度。目前，在 X86 架构下，常用的虚拟化软件大多都是国外产品，如 VMware Station、Virtual Box 等，若这些国外虚拟机产品存在后门，将会影响整个虚拟化系统的安全运行。

同时，虚拟化技术存在虚拟机逃逸、跳跃、蔓延等技术缺陷，非法用户可以利用虚拟化软件的漏洞发起攻击，获取宿主机的管理员权限，控制虚拟机管理器，或者以某一个虚拟机为跳板，获得同一宿主机上其他虚拟机的访问权限，最终实现越权访问、拒绝服务，甚至对虚拟机进行完全控制[9]。

1.2 系统运行安全风险

在虚拟化环境中，同一台宿主机上一般运行着多个虚拟机，这些虚拟机共享宿主机上的处理器、内存、存储和网络资源。所有虚拟机都连接到宿主机的同一张网卡或虚拟交换机上，虚拟机之间的通信流量可以不经过外部网络，传统的基于交换机镜像端口的网络流量入侵检测技术将会失效，如果一台虚拟机发生安全问题，将可能会扩散到同一宿主机的其他虚拟机[6]。

虚拟化环境下的端口由物理服务器映射到虚拟机，如果端口没有设置安全规则，虚拟机的端口有可能连接到外部网络，有可能会受到攻击者的非法访问。

在进行服务器虚拟化时，为了部署快捷方便，管理员可能使用同一镜像文件批量创建多个虚拟机，如果虚拟机的镜像文件本身存在漏洞或携带病毒，虚拟机运行时这种漏洞和病毒会影响到整个网络，带来极大的安全隐患。

虚拟机在使用过程中需要对物理服务器中的资源进行竞争，包括处理器、内存和带宽等，在实际的建设过程中，一旦虚拟出的服务器过多或者同一虚拟机中出现过多应用程序，就会导致整个服务器工作负载过重，使服务器的工作效率降低，影响整个虚拟化系统的运行质量。

1.3 配置管理安全风险

在虚拟化环境中，物理资源高度集中，管理员在配置过程中若因规划或设计不当，可能导致虚拟机存在配置缺陷而留下安全隐患。配置缺陷主要包括：管理流量和业务流量共用网络链路，可能在管理流量中混入攻击流量而不被监管，造成业务系统正常访问受到影响；不同密级的虚拟机共用一台宿主机或存储设备未进行有效的安全隔离，网络边界模糊，一些敏感信息可能会被其他虚拟机非法读取；虚拟磁盘中的文件明文存储，虚拟机在迁移过程中文件被非法复制，可能造成重要数据外泄；安全产品缺失或者安全策略配置不合理，虚拟机中的流量无法被监管和审计，都会导致安全风险[10]。

1.4 运维管理安全风险

在虚拟化环境中，对服务器硬件维修、软件维护、虚拟机迁移和删除等运维过程缺少相应的安全监管，极易发生运维安全事件。如虚拟机管理员权限过大，宿主机的管理员账号随意使用，运维操作缺乏安全审计导致随意创建虚拟机和修改虚拟机配置，不能及时更新病毒库和系统补丁，非授权人员随意接触虚拟机管理器，运维过程中移动存储介质随意接入虚拟机等，都会对虚拟化系统带来恶意攻击和数据泄密等安全隐患，更有甚者造成整个虚拟化系统瘫痪和业务中断。

2 服务器虚拟化安全防护设计

为推动服务器虚拟化在企事业单位网络信息体系中的落地应用，保证虚拟化系统的安全运行，本文提出了一种服务器虚拟化的安全防护设计方案，从部署环境安全、宿主机安全、虚拟机安全、系统运行安全和运维安全管理方面进行了详细阐述。

2.1 安全防护架构

本文提出的安全防护设计总体架构如图 1 所示,该安全防护架构的设计思路如下:

(1)分级分域设计,将整个网络划分为高密级应用服务域、低密级应用服务域、高密级用户终端域、低密级用户终端域、安全监管域、运维管理域和核心交换域,对服务器宿主机、虚拟机、存储资源、用户终端等进行安全分级管理。

(2)安全域访问控制,各安全域之间的通信通过核心交换域进行安全防护控制,严禁低密级终端访问高密级的虚拟机和存储资源。

(3)“三网设计”,将整个网络中按照流量类型设计为业务网、存储网和管理网,业务交换机、管理交换机和存储交换机独立设置,在服务器虚拟化宿主机上配置 3 块不同的网卡承载相应的数据流量,避免流量交叉[10]。

(4)加密存储,各虚拟机的系统文件和数据文件均存储在磁盘阵列中,并使用存储密码机进行透明加密存放,保证虚拟机的文件和数据安全[7]。

(5)在服务器虚拟化宿主机上部署服务器审计系统,对宿主机的操作和运行状态进行安全审计,在网络中部署入侵检测设备,对服务器交换机和核心交换机上的流量进行安全分析和异常检测。

(6)设置专用的运维管理终端,对虚拟化系统和其他设备进行日常运维管理。

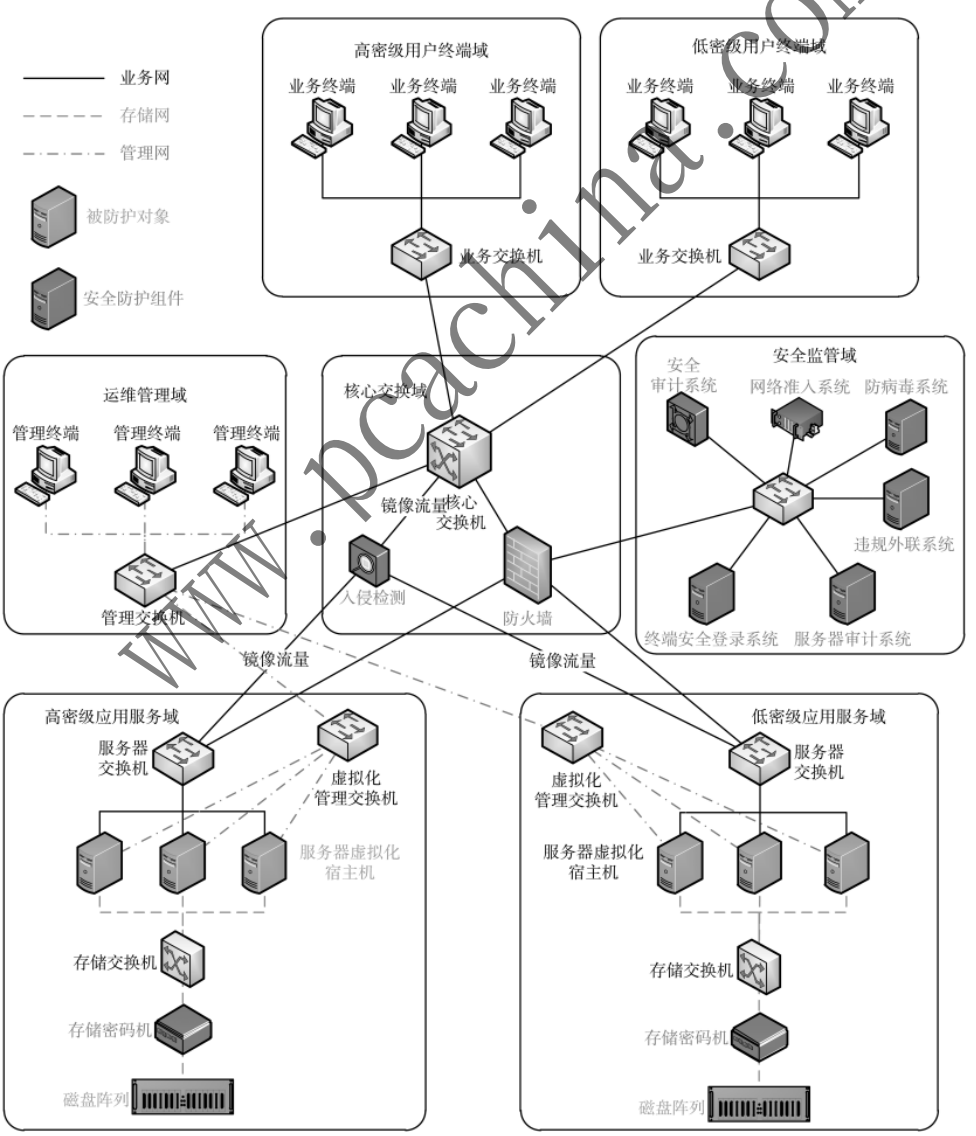

图 1 安全防护总体架构

2.2 部署环境安全

服务器虚拟化系统的服务器、存储设备及相关网络设备等要放置在机房进行集中管理，并对机房进行安全防护和访问控制：

(1)机房配置电子门禁系统，通过身份认证后方可进入，控制、鉴别和记录出入人员。

(2)机房配置视频监控和红外入侵监控，及时发现非法人员进入，防止对机房设备进行破坏。

(3)机房配置动环监控系统，实时调节机房的温湿度环境，监控机房的供电状态，防止对技术设备造成损坏，保障机房环境运行安全。

(4)机房内业务网、存储网和管理网使用不同颜色的线缆，并设置相应标志，防止不同网络之间交叉使用。

(5)对服务器、交换机等设备上不使用的接口进行物理关闭。

2.3 宿主机安全

宿主机的安全是整个服务器虚拟化系统的前提，宿主机一旦被控制，其上运行的虚拟机都有可能被攻击，可以从以下几方面对宿主机进行安全加固：

(1)设置宿主机 BIOS 密码，设置默认从本地硬盘启动，禁止从网络或 USB 口启动，确保宿主机的启动安全。

(2)宿主机优先使用国产服务器，并安装配套的融合系统，对外设端口进行管控，控制开放的网络服务和端口，安装服务器审计系统，对宿主机的登录、运行状态和指令操作进行审计，保障宿主机的运行安全。

(3)在宿主机中安装相应的安全管理软件，定期对宿主机进行病毒和恶意代码查杀、漏洞修复。

(4)设置高强度的宿主机操作系统登录密码，密码由字母、数字和特殊字符混合组成，并定期进行密码更换。

(5)宿主机配置不同的网口和 HBA 卡，分别用于连接业务网、管理网和存储网。

(6)按照设备密级，对宿主机进行分机柜放置，严禁在低密级的宿主机上创建高密级的虚拟机。

2.4 虚拟机安全

虚拟机中承载着网络中各业务系统的运行，虚拟机的安全是保障业务系统安全的关键所在，虚拟机一旦被攻击，业务系统将会受到破坏或直接瘫痪。可以从以下几方面对虚拟机进行安全防护：

(1)优先使用国产化虚拟化软件，防止非国产化虚拟化软件存在后门，对业务系统带来潜在的安全威胁。

(2)对 KVM、QEMU 等虚拟化软件已知的漏洞进行修复和加固，持续追踪和修复最新发现的虚拟机漏洞。

(3)虚拟机的系统文件和数据文件存放在磁盘阵列中，磁盘阵列设置 RAID 进行冗余，并经存储加密机进行文件存储加密，防止硬盘损坏或丢失带来的数据损坏或泄密，同时保证虚拟机迁移过程的安全性。

(4)在虚拟机中开启虚拟化防火墙，对进出虚拟机的流量进行访问控制，及时阻断非法网络连接。

(5)定期对虚拟机进行快照操作，防止虚拟机因意外情况无法正常运行，可对状态异常的虚拟机进行及时恢复。

(6)对虚拟机的操作系统设置高强度登录密码，密码由字母、数字和特殊字符混合组成，并定期进行密码更换。

2.5 系统运行安全

为进一步加强整个虚拟化系统的安全防护，应部署防火墙、网络接入控制系统、违规外联系统、终端安全登录系统、网络防病毒系统、入侵检测系统和安全审计系统等，提升虚拟化系统的整体安全防护能力。

(1)访问策略控制

在网络中部署防火墙，可以在虚拟化服务器与用户终端、不同级别的安全域之间提供网络安全隔离服务，提供基于 IP、协议、端口等要素的安全访问策略，通过制定合理的访问规则防止各安全域设备之间的非法网络访问。

(2)网络接入控制

在网络中部署网络接入控制系统，对接入交换机上的端口进行入网管控，并在计算机终端上安装网络接入控制客户端，计算机入网时校验 IP 地址、MAC 地址、交换机管理 IP、交换机端口和用户名密码等信息。同时，网络接入控制客户端可以对计算机终端进行健康检查，如检测是否安装了防病毒软件、主机监控和审计软件、终端安全登录软件等，只有通过终端健康检查后才能通过网络准入认证，确保只有授权的计算机终端可以接入网络中，访问业务服务。

(3)违规外联管控

在计算机终端上安装违规外联软件，制定违规外联策略，对计算机中的外设接口进行有限管控，

防止移动存储介质交叉使用带来数据外泄风险。实时检测计算机是否连接到互联网,发现外联后立即阻断网络通信,避免受到外部网络的攻击。

(4)终端登录管控和身份认证

在网络中建立统一的身份认证体系,结合 USB Key 等物理硬件,保证各用户身份的唯一性,部署终端安全登录系统和身份认证网关,实现计算机终端安全登录管控和应用认证,记录终端登录和应用认证日志,方便管理员进行日常审计。

(5)网络防病毒

在网络中部署网络防病毒系统,服务器和终端上安装防病毒客户端,在防病毒系统的控制中心制定病毒和恶意代码查杀策略,对各客户端进行升级管理,通过控制中心可以查看整个网络中的病毒查杀和主动防御信息。

(6)网络入侵检测

在网络中部署入侵检测系统,实时检测核心交换机、服务器交换机上的网络流量,及时发现网络中的异常流量并进行报警。将虚拟化宿主机连接的服务器交换机的镜像流量接入到入侵检测系统,可以监控宿主机之间、虚拟机之间的非法网络访问,通过分析服务器交换机上的网络流量,可以对应用服务的访问事件进行记录和分析,及时发现网络中的潜在攻击行为。

(7)安全审计

在网络中部署安全审计系统,可以接收来自其他安全设备的审计日志,实现对审计日志的集中存储、统一管理、关联分析,可以对安全事件进行溯源和定位。

2.6 运维安全管理

任何系统的安全防护仅仅依靠技术措施是不够的,必须辅助管理手段,做到人防和技防相结合。针对服务虚拟化所在的网络,可以从以下几个方面进行日常运维和安全管理:

(1)设置专用的运维管理终端,对虚拟化系统宿主机和虚拟机进行日常运维,做到管理信息和业务信息安全隔离。

(2)设置系统“三员”,即系统管理员、安全管理员和安全审计员,三员相互独立,彼此监督,明确各管理员的权限和职责,禁止权限交叉,严禁越权操作。

(3)建立与服务器虚拟化日常运行相适应的安全管理制度,对虚拟机的创建、修改、删除、迁移以及开机、重启、关机、快照等日常操作制定操作规程,必要时进行审批流程,做好日常操作记录。

(4)定期对虚拟化系统的运维日志和安全防护设备日志进行安全审计,及时发现违规操作,并采取针对性的补救措施。

3 试验验证

本节对上文中提出的服务虚拟化安全防护设计方案进行了试验验证。

3.1 试验设备

试验验证需要用到的主要设备如表 1~表 3 所示。

试验中使用的管理终端和业务终端使用普通的 X86 电脑,高密级业务终端配置 2 台,低密级业务终端配置 2 台,管理终端配置 3 台。

3.2 试验过程

3.2.1 搭建试验环境

将试验设备按照图 1 进行组网,搭建试验环境。网络 VLAN 划分如表 4 所示,服务器的 IP 地址分配如表 5 所示,其他设备按照 VLAN 划分分配相应的 IP 地址。

表 1 服务器列表

物理服务器	虚拟服务器	应用服务
天玥 SR124212 服务器 1	公文服务器	电子公文系统(高密级应用)
	邮件服务器	电子邮件系统(高密级应用)
天玥 SR124212 服务器 2	OA 服务器	OA 系统(高密级应用)
	文件服务器	FTP Server(高密级应用)
浪潮 NF5280M5 服务器 1	所网服务器	所网主页(低密级应用)
	电子图书服务器	电子图书馆(低密级应用)
浪潮 NF5280M5 服务器 2	打印服务器	集中打印系统(低密级应用)
	财务服务器	财务预算系统(低密级应用)

注:天玥 SR124212 服务器是国产服务器,飞腾 FT2000+/64 处理器,银河麒麟 V4 操作系统,使用银河麒麟系统自带的 QEMU 虚拟化软件。浪潮 NF5280M5 服务器是 X86 服务器,英特尔 Xeon 4210 处理器,Windows Server 2019 操作系统,使用 VMware Station 虚拟化软件。

表 2 交换机及存储设备列表

交换机类别	设备型号	数量
核心交换机	锐捷 S5670C	1
服务器交换机	H3C S5560X	2
虚拟化管理交换机	H3C S5560X	2
运维管理交换机	华为 S5328C	1
终端及安全产品接入交换机	华为 S5328C	3
存储交换机	NetStor MDS 9148S	2
磁盘阵列	NetStor iSUM A1600	2

表 3 安全防护设备列表

产品名称	设备型号	数量
防火墙	天融信 NG-51138	1
入侵检测	绿盟 IDSNX5-8210-BM	1
安全审计系统	绿盟 SASNX3-HD310	1
网络准入系统	天融信 TSM-21128-TopNAC	1
终端安全管理系统	奇安信天擎终端安全管理系统 V6	1
服务器审计系统	中孚服务器审计系统	1
终端安全登录系统	锐尔终端安全登录系统	1
存储密码机	数盾科技 SJJ1608	2

注：防火墙、入侵检测、安全审计系统、网络准入系统和存储密码机是专用硬件设备，终端安全管理系统、服务器审计系统、终端安全登录系统是安全防护软件，需要配置相应的硬件服务器，服务器审计系统配置 1 台天玥 SR124212 服务器进行安装，终端安全管理系统和终端安全登录系统配置 1 台普通的 X86 服务器进行安装。

表 4 VLAN 划分

VLAN 名称	VLAN 地址	网关
高密级服务器 vlan10	192.168.10.0	192.168.10.254
低密级服务器 vlan20	192.168.20.0	192.168.20.254
设备管理 vlan30	192.168.30.0	192.168.30.254
安全产品 vlan40	192.168.40.0	192.168.40.254
高密级业务终端 vlan50	192.168.50.0	192.168.50.254
低密级业务终端 vlan60	192.168.60.0	192.168.60.254
管理终端 vlan70	192.168.70.0	192.168.70.254

3.2.2 防护策略配置

(1)宿主机安全配置

2 台天玥服务器和 2 台浪潮服务器均设置BIOS 启动密码，安装天擎终端安全管理系统客户端软件，并在天擎系统控制中心设置违规外联和外设管控措施。同时，在物理服务器中加装 HBA 卡，使用光纤通过存储密码机连接到相应的磁盘阵列，磁盘阵列配置的硬盘组建 RAID5，并为相应的服务器提供存储空间。

表 5 服务器 IP 地址分配

设备	IP 地址	网关
公文服务器(业务地址)	192.168.10.10	192.168.10.254
邮件服务器(业务地址)	192.168.10.11	192.168.10.254
OA 服务器(业务地址)	192.168.10.12	192.168.10.254
文件服务器(业务地址)	192.168.10.13	192.168.10.254
所网服务器(业务地址)	192.168.20.10	192.168.20.254
电子图书服务器(业务地址)	192.168.20.11	192.168.20.254
打印服务器(业务地址)	192.168.20.12	192.168.20.254
财务服务器(业务地址)	192.168.20.13	192.168.20.254
天玥 SR124212 服务器 1(管理地址)	192.168.30.10	192.168.30.254
天玥 SR124212 服务器 2(管理地址)	192.168.30.11	192.168.30.254
浪潮 NF5280M5 服务器 1(管理地址)	192.168.30.12	192.168.30.254
浪潮 NF5280M5 服务器 2(管理地址)	192.168.30.13	192.168.30.254

2 台天玥国产服务器中安装服务器审计代理软件，进行服务器状态监控和操作审计。

(2)虚拟机安全配置

在天玥服务器中使用 QEMU 创建虚拟机，浪潮服务器使用 VMware Station 创建虚拟机，将虚拟机的系统文件保存到磁盘阵列提供的存储空间中，确保虚拟机中的文件通过存储密码机进行安全加密。在虚拟机中开启系统自带的防火墙，并设置复杂的登录口令。

(3)系统运行安全配置

在核心交换机中配置 ACL 列表，控制各 VLAN 之间的网络通信，在防火墙中设置访问控制策略保证业务终端只能访问授权的业务资源。在网络准入控制系统中配置 802.1X 准入模式，同时在接入交换机中启用 802.1X 认证，确保只有授权的设备才可以接入网络。利用天擎终端安全管理系统对服务器、终端电脑进行外设使用控制和违规外联控制，违反外联控制策略时及时断开主机网络。

使用网络安全审计系统和服务器审计系统对网络中的异常事件、违规操作以及服务器的状态和操作进行安全审计。

(4)运维安全配置

设置系统管理员、安全管理员和安全审计员，并配置专用的管理终端，对整个系统进行配置和维护，

虚拟机的创建、修改、删除、迁移操作由系统管理员负责,安全管理员对系统管理员和安全审计员的操作进行安全审计,安全审计员对安全管理员的操作进行安全审计。

3.3 防护效果

通过试验验证,本文提出的服务器虚拟化安全防护方案能够达到以下防护效果:

(1)做到业务数据流和管理数据流分离,降低内部人员或外部恶意人员通过业务终端攻击虚拟化服务器的安全风险;

(2)实现虚拟机系统文件和数据文件的透明加密存储,在保障业务正常运行的同时,防止因硬盘丢失造成虚拟机中的数据泄密风险;

(3)高密级虚拟机和低密级虚拟机严格逻辑隔离,分域使用,杜绝数据高密低用;

(4)在国产服务器中安装服务器审计系统客户端,对服务器的系统状态、系统登录、操作行为、网络配置等进行审计,能够追溯登录用户对虚拟机的创建、删除、修改等操作行为;

(5)通过入侵检测系统和安全审计系统对网络中的业务流量进行检测和审计,及时发现网络中的异常行为,识别可能的虚拟机攻击行为;

(6)通过网络准入控制系统、终端安全登录系统确保只有授权的用户可以接入网络并访问虚拟出的业务应用,有效防止非法用户的接入和访问。

3.4 功能性能提升

以本文的试验为例,在保持业务应用系统部署需求不变的情况下,使用服务器虚拟化方案可以达到以下提升效果:

(1)物理服务器需求数量减少 50%,服务器资源利用率可以提升 1 倍;

(2)在模拟 100 人同时访问业务系统的情况下,服务器的网络带宽实际利用率可以提高近 30%;

(3)可扩展性较好,在物理服务器硬件性能满足的情况下,新增业务系统可以通过创建新的虚拟机快捷部署,业务系统停用可以通过删除虚拟机快速停用,释放硬件资源,在一定程度上减少业务系统安装维护工作量;

(4)虚拟机均存储在磁盘阵列中,当物理服务器发生故障时,可以将对应的分区挂载到新的服务器中,实现虚拟机的快速迁移,并可以保证业务数据不丢失。

4 结论

本文针对服务器虚拟化的技术特点,从技术架构、系统运行、配置管理和运维管理四方面分析了服务器虚拟化在网络信息体系应用中面临的安全风险,提出了一种服务器虚拟化的安全防护设计方案,介绍了设计方案的安全防护总体架构,在部署环境安全、宿主机安全、虚拟机安全、系统运行安全和运维安全管理等方面进行了详细的技术防护措施设计和安全管理设计,为服务虚拟化的应用提供了一种可行的安全解决方案,并搭建试验环境进行了安全防护试验验证,有助于推动服务器虚拟化在企事业单位信息化和数字化转型中的落地应用。

参考文献

[1] 罗喆帅.基于虚拟化技术构建安全集中式应用平台[J].金融科技时代,2022,30(5):60-64.

[2] 金俊玲,王昕.基于服务器虚拟化技术的数据中心网络安全设计[J].网络安全技术与应用,2022(5):5-7.

[3] 林世城.虚拟化技术在计算机技术中的运用研究[J].信息与电脑(理论版),2022,34(1):26-28.

[4] 王嘉鹏.计算机技术中虚拟化技术的运用探讨[J].电脑知识与技术,2021,17(33):148-150.

[5] 洪亚玲.服务器虚拟化技术与安全研究[J].电脑知识与技术,2022,18(8):34-35.

[6] 孟思明.服务器虚拟化技术及安全分析[J].中国设备工程,2021(16):190-191.

[7] 于兆鑫.计算机信息技术中虚拟化技术的运用[J].信息记录材料,2021,22(11):146-147.

[8] 刘怡生,韩春霞.基于超融合技术的服务器虚拟化平台创新建设与应用[J].现代工业经济和信息化,2021,11(5):109-111.

[9] 李辉强,姜正涛,林珊珊.虚拟化安全技术分析[J].保密科学技术,2020(10):4-8.

[10] 熊明俊,杨景茂.虚拟化安全防护与应用研究[J].保密科学技术,2020(10):15-20.

(收稿日期:2022-11-08)

作者简介:

李超(1984-),男,硕士,工程师,主要研究方向:电子信息系统、信息化、射频识别、标准化。

党增江(1989-),通信作者,男,硕士,高级工程师,主要研究方向:网络安全、工控系统安全。E-mail:dangzjiang@163.com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部