虚拟机在反病毒实验中的应用

彭安杰
（西南科技大学计算机学院，四川绵阳 621010）

摘 要：为了适应反病毒实验的复杂性，本文利用IBM 刀片服务器和 VMware Lab Manager（以下简称 VLM） 搭建了反病毒实验平台。该平台既能虚拟出多种操作系统，也能构造复杂的网络环境。通过将虚拟机限制在隔绝的网络里，有效地降低了病毒的未知危害。

关键词：虚拟机；VLM；反病毒实验
中图分类号：TN918.1 **文献标识码：**A **文章编号：**1007-9599 （2010） 07-0025-01

Application of Virtual Machine in Anti-Virus Experiment

Peng Anjie
(School of Computer Science,Southwest University of Science and Technology,Mianyang 621010,China)

Abstract: Anti-virus tests need complicated conditions,such as the variety of operation system.We utilize IBM Blade Server and Vmware Lab Manager to construct a platform which can virtualized some operation systems.Since virtual machines are isolated, the platform can prevent virus's spread.

Keywords: Virtual machine;VLM;Anti-virus test

一、引言

反病毒实验具有复杂性和危害性等特点。其复杂性体现如下：（1）多操作系统的要求。例如 DOS，LINUX 等。学生有时需要在同一界面上使用多个操作系统。（2）复杂网络的需求。这主要体现在网络类病毒（如木马）方面。由于实验用的病毒样品具有未知的破坏性，还需要防止病毒样品的传播。

传统实验室的物理机采用了还原系统，不能满足反病毒实验的要求。虚拟机利用虚拟化技术，通过在硬件平台上添加虚拟机监视软件的中间层，进而虚拟出一台功能完善的计算机。[1]虚拟机技术能较好地满足反病毒实验的要求，它不仅能在一台物理机上部署多个虚拟机，也能在物理机上配置复杂网络。[1]现有的研究多数都采用 Vmware Workstation 对实验进行虚拟化改造[2]，其优势在于成本低，其劣势为：（1）对主机操作系统的依赖度高，因为其安装于主机操作系统上（2）不能实现集中管理（3）网络配置的局限性（4）无法限制用户拷贝虚拟机内的文件。VLM 架构于 VMware Infrastructure（以下简称 VI）之上，VI 既要将物理机进行虚拟化，也要管理 VLM。VLM 主要用于软件测试和实验室环境的搭建，其采用集中管理模式，它使得用户能轻松实现登录，克隆、创建系统快照等操作。VLM 的管理简便，其“存储租赁”通过回收过期的虚拟机空间消除空间剧增现象，其“角色和权限”功能实现了权限的分级管理。VLM 的可扩展性强，其创建的网络模板能虚拟复杂的网络环境。此外，它还支持 LDAP。鉴于反病毒实验的要求，我们选取 VLM 搭建反病毒实验平台。

二、实验基础平台的搭建

首先在刀片服务器上安装 VI。考虑到学生人数众多，添加了 H3C 的存储器作为附加存储。存储器和服务器之间通过 ISCSI 协议进行数据传输。

然后将 VLM 与域控制器集成，实现了权限的分级管理。为了体现不同权限，分别建立了学生组，教师组，实验室管理员组。当用户注册为域中的用户后，首先会拥有学生组的权限。如果用户需要提升权限，管理员通过域控制器为其提升权限。

三、利用Lab Manager开展实验

实验室管理员的工作包括：分配主机资源，创建网络模板和设置权限。为了有效地使用 VLM，管理员也可为其添加 VMware 平台的相关功能，如 VMotion，DRS 等。对于网络，管理员只需配置两种类型的模板：连接互联网和不连接互联网的模板。权限的设置通过配置“角色和权限”菜单实现，管理员只需为管理员组，教师组，学生组分配基本权限。若某个实验要求学生具有特殊的权限，管理员只需在学生组上添加相应的权限。 实验室管理员只需第一次配置实验平台，在以后的实验中，除非有特殊的需求，否则不必改变平台的配置。

教师的工作主要是部署实验模板。模板其实是一台虚拟机，包含了硬件配置，操作系统，网络配置以及软件配置。教师首先将模板设置为共享，然后将其复制到工作空间中生成一个虚拟机进行测试。教师最后将测试成功的虚拟机公布到“Library”中。此外，教师也可先利用 Workstation 配置好实验模板，然后再利用 VMware Converter 将模板转化为 VLM 中的模板。

学生通过以下步骤进行实验：

（一）学生利用自己的账号和密码通过Web登录VLM，点击“Library”，将实验用的虚拟机复制到工作空间中。

（二）学生配置虚拟机。为了防止学生恶意操作硬件资源，可以将学生组的权限设置为只能从默认配置中部署虚拟机。

（三）学生登录虚拟机进行实验。如果学生需要多台虚拟机，重复步骤（一），（二）即可。

复制的虚拟机在连接物理网络时，会发生IP地址冲突，原因在于复制虚拟机的IP都是模板虚拟机的IP，解决方法是在配置虚拟机的时候采用围栏技术。如果将虚拟机与物理网络隔离，学生便不能随意拷贝病毒样品。由于虚拟机完整地保留了实验痕迹，学生既可以在课堂上也可以在课后登陆虚拟机进行实验，这有利于学生复习实验，提高了实验的效益。

四、结语

本文以刀片服务器和VLM为基础构建了反病毒实验的平台。该平台不仅提升了实验的效果，也极大地降低了实验管理员和教师的工作量。该平台可与VPN结合形成远程实验室。实验平台在运行的过程中也出现了一些问题，当学生同时部署虚拟机时，服务器和存储的负载都很大。如何提高实验平台的运行速度是下一研究方向。

参考文献：

[1]董耀祖,周正伟.基于x86 架构的系统虚拟机技术与应用[J].计算机工程,2006,32(13):71-72。
[2]秦光.利用虚拟机搭建安全的木马及病毒测试系统[J].西昌学院学报.自然科学版,2007,21（1）:54-56

作者简介
彭安杰（1981-），男，硕士，研究方向为信息安全

虚拟机在反病毒实验中的应用

作者： 彭安杰， Peng Anjie
作者单位： 西南科技大学计算机学院,四川绵阳,621010
刊名： 计算机光盘软件与应用
英文刊名： COMPUTER CD SOFTWARE AND APPLICATIONS
年，卷(期)： 2010(7)

参考文献(2条)

1. 董耀祖;周正伟 基于x86架构的系统虚拟机技术与应用[期刊论文]-计算机工程 2006(13)

2. 秦光 利用虚拟机搭建安全的木马及病毒测试系统[期刊论文]-西昌学院学报(自然科学版) 2007(01)

本文读者也读过(10条)