文章编号:1001 - 4179(2013)S1 - 0194 - 03

红帽企业虚拟化在网站服务器上的应用初探

张 雷

(长江水利委员会 长江水利网站,湖北 武汉 430010)

摘要:长江水利网站已建多年,许多业务系统相继上线,服务器数量逐年增多,故障率和维修成本也越来越高。为降低运营成本,提高资源利用率和集约化管理水平,采用虚拟化技术对机房的服务器和应用系统进行整合,充分利用服务器的有效资源,提高各系统的速度和可靠性,同时降低能耗,提高对机房资源的集中管理能力。根据实际情况,对比了几种较成熟的虚拟化软件功能,由于 RHEL6 具有占用资源较少、使用方便,故选用红帽企业 RHEL6 架构结合 iSCSI 存储搭建了小型虚拟化系统。该系统可以提高服务器性能,同时保证业务数据的安全。目前虚拟化技术正在长江水利网升级改造中得到运用。

关 键 词:虚拟化技术; 存储空间; 数据安全; RHEL6

中图法分类号: TP391 **文献标志码**: A

服务器升级换代后,高性能的物理设备不能充分利用,政务网站高安全性要求多个应用服务必须独立运行,这样一来,增加物理服务器势必增加财政投入,而且后续使用的电费也会成倍增加。为解决这一矛盾,本文通过应用服务器虚拟化技术,并对比几种比较成熟的虚拟化软件,结合红帽企业虚拟化 KVM 架构优势,指出具体实践过程中遇到的问题和解决方法。

1 虚拟化软件的选择

1.1 主流虚拟化软件的比较

可选择的主流虚拟化产品有:红帽 KVM、VMware、Citrix 的 Xen 和微软的 Hyper - V。早期应用的 Citrix 的 Xen 由于不能实现基于内核的虚拟化逐渐被淘汰,2011 年,随着新版操作系统 Red Hat Enterprise Linux 6 的发布,红帽也完全放弃了以开源 Xen 为虚拟化平台的思路,开始支持 KVM 作为 hypervisor。VMware 发展的较早,也很成功,有多个版本。企业级的应用需要复杂的管理工具,且不开源,价格不菲。微软的 Hyper - V 依赖庞大的 Windows 操作系统,性能有限价格不低。据红帽官方描述,相比其他虚拟化应用,红帽 KVM 性能优异,不仅可以实现 VMware 的所有功能,甚至可以节约 60% ~80% 的使用费用。

1.2 RHEL 与 RHEV 的取舍

红帽企业的 Red Hat Enterprise Linux (RHEL) 与 Red Hat Enterprise Virtualization (RHEV) 都提供 KVM 虚拟化,但这两者在 KVM 管理、功能与实施中有重大区别。

RHEV 包含 RHEV Manager (RHEV - M),这是个集中的 KVM 管理平台,能同时管理物理与虚拟资源。RHEV - M 能够从 Web 界面完成管理虚拟机与其磁盘镜像,安装 ISO,进行高可用性设置,创建虚拟机模板等工作,也可使用 RHEV - M 管理物理机和虚拟机两种不同类型的 hypervisor。但是由于 RHEV 2.2 虚拟化管理软件 RHEV - M 依赖微软. NET 与 SQL Server,迫使管理员在 Windows Server 下,利用 PowerShell 通过脚本来自动更新任务。

作者曾经在 RHEV2.2 测试安装中,意外损坏数据库文件,造成整个虚拟机配置文件丢失,无法恢复,故此没有使用 RHEV2.2,而是直接使用 RHEL6.0。RHEL 是款具有 KVM 虚拟化功能的普通 Linux 服务器产品,由 Linux 内核与大量的包组成,包括一些 KVM 桌面管理工具,更适合小型环境。使用 RHEL6 可以安装并管理少量的虚拟机,性能与 RHEV2.2 相当,都是基于裸金属内核虚拟化,在小型环境中,RHEL6 能满

收稿日期:2013 - 04 - 20

作者简介:张 雷,男,馆员,主要从事网站技术服务工作。E - mail:zl2826@ qq. com

足用户对开源虚拟化的所有要求。

1.3　RHEL6 的使用

由于 RHEL 管理系统不是图形化的管理系统,运行中占用的资源较少,挂载的图形管理界面在使用自带的 KVM 管理工具时也很方便,巧妙地使用惠普服务器提供的 Intergrated Light - Out(iLO)可以实现远程管理。作者使用的是惠普公司的 ProLiant DL380 G7,由于 iLO3 是集成在服务器主板上的硬件 ASIC 芯片,有自己独立的 CPU、内存,因此,它的使用方式与软件无关,可在远程操作服务器开机、关机,进而实现对服务器完全的远程管理,安装相应的 java 或. net 框架插件后,可以通过任何浏览器进行远程物理机桌面甚至对物理机内部的虚拟机桌面进行 KVM 管理,非常方便[1-2]。

2　虚拟机存储的使用

2.1　本地存储与 iSCSI 网络存储使用

作者在采购惠普 DL380 G7 服务器的同时采购了惠普 LeftHand P4500 存储,它属于 iSCSI 区域网络存储(IP SAN),iSCSI 拥有与光纤存储(FC SAN)无法比拟的价格优势,1 G 的 IP SAN 网络带宽拥有与 10 G 的 FC SAN 光纤带宽相当的性能,实际使用中也证明其完全能够满足现有应用的需求。

应用 iSCSI 后,几乎所有的客户在购买服务器时都有一些内部的存储(也就是直接式存储 DAS)是不用的,有时候这部分的容量可以达到每台服务器 1TB 的存储空间之大,占惠普 P4500 存储空间的 1/5,但是 P4500 价格却是 G7 服务器 3 倍,因此充分使用这部分 DAS 存储就显得非常的必要。

除了以上成本的考虑外,通过外部的网线和交换机链接的物理存储相对于服务器内部的本地存储 DAS 产生故障的因素更多,比如网卡、网线、交换机甚至 iSCSI 物理机本身。故此,作者在实际应用中将重要的数据库应用和内部管理系统安装在本地存储上。

2.2　虚拟机与存储结合的应用

RHEL6 作为物理机的核心管理平台,在其上除了提供 KVM 虚拟机服务之外不安装任何其他的应用服务。

RHEL6 为其下的虚拟机提供的存储类型很多,其中包括 DAS 和 IP SAN,DAS 可以是一个子目录或是一个文件,作者将除操作系统必要的分区之外全部格式化为逻辑卷,为将来扩容提供方便,在逻辑卷基础上创建独立的虚拟机的分区。对于 IP SAN 红帽 RHEL6 已默认提供 iSCSI 服务,主要步骤如下。

(1) 在 P4500 存储上创建指向 DL380 G7 服务器 IP 地址的 Server。

(2) 在 DL380 G7 上配置存储环境。使用搜寻 iSCSI 盘阵命令:

#iscsiadm - - mode discovery - - type sendtargets - - portal 192.168.1.110 (示例存储的 IP 地址)

返回结果:

192.168.1.110:3260,1

iqn. 2003 - 10. com. leftheandnetworks: cjw - p4300:abc:123

测试 iqn 设备是否可以连接(这是关键,否则无法挂载成功!)

#isisadm - d2 - m node - - login

(3) 进入 KVM 在创建新的虚拟机时,选择"托管或现有的存储——存储池"将会发现新的存储空间。

3　操作系统的选择与应用

作者所在单位网站原系统下生成的大量以 asp 后缀的静态文件必须依赖 IIS 环境,需要安装 Windows 服务器,除此之外,其他应用都是 Liunx 服务器环境,包括 NTP 时间服务、DNS 域名服务、DHCP 地址服务、SAMBA 文件服务、Email 邮件服务、APACHE 网页服务等。由于 RHEL6 的 KVM 虚拟化对 Windows 及 Linux 有着良好的兼容性,实践证明也非常稳定,没有出现过任何服务意外中断的情况。

正如作者前面提到的,为了保证各项应用程序安全稳定,需要安装多个虚拟机,往往 1 台虚拟机上只运行 1,2 个服务,这样简单设置可以避免某项服务的故障对其他服务的影响,也更便于系统日志的分析和故障的排除。KVM 还有一个最大的优势是虚拟机中安装相同的 OS 操作系统,可以实现内核同页合并(kernel samepage merging ,KSM),允许有限物理内存安装尽可能多的虚拟机,实现硬件使用效率最大化[3-5]。

4　虚拟化安全问题

4.1　系统安全与数据备份

RHEL6 提供了基于内核的强大的 Security - Enhanced Linux(SELinux)强制访问控制,SELinux 系统比起通常的 Linux 系统来,安全性能要高的多,它通过对于用户,进程权限的最小化,即使受到攻击,进程或者用户权限被夺去,也不会对整个系统造成重大影响。将各种服务独立开来也是提高安全性手段之一。

Linux 的数据备份也是很方便的,可以使用 rsync 镜像保存整个目录树和文件系统数据,而且利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

需要注意的是必须在服务器 A 和 B 上都安装 rsync,其中 A 服务器上是以服务器模式运行 rsync,而 B 上则以客户端方式运行 rsync。这样在 Web 服务器 A 上运行 rsync 守护进程,在 B 上定时运行客户程序来备份 Web 服务器 A 上需要备份的内容。

#rsync - avzP nemo@192.168.10.1:/nemo/backup

程序 rsync 不同于 ftp 传递协议,除首次备份实行完全备份之外,之后的备份可以实现自动增量备份,程序会自动识别修改或增加的文档,实现备份数据与源数据的版本同步。

容易忽略的是,由于虚拟机的 IP 易于变更,会造成不能联机的情况,可以修改 root 家目录下的隐含目录.ssh 中的文件 known_hosts,删除其中对应故障主机的那条记录,故障即可恢复。

在备份机上执行以下命令,可以动态查看备份增量变化情况。

watch -n 60 "du -sh"(每分钟刷新一次动态信息)

4.2 虚拟化实践中应注意的问题

KVM 开源虚拟化技术可以最大程度保障单位对自身解决方案和服务的弹性定制,并可有效实现后期按需扩展性。尤其重要的是,开源的 RHEL 没有强硬的许可证限,这使单位在今后横向扩展新的虚拟化服务器时不会再产生额外成本。正是这种高效率和低成本的虚拟化应用也带来如下一些负面影响。

(1) 过于集中地部署密集型应用程序到虚拟机,造成这些应用程序争夺同一硬件服务器的带宽、内存、处理器和存储等资源,可能会遇到网络瓶颈和性能问题,引起服务器负载过重。最为明显的压力来自于内存,一般情况内存使用不要超过物理内存的 90% 为宜,应用上文提及的 KSM 内存调优也可以改善性能,前提是控制虚拟机总数,往往可以提高虚拟机 10% 的性能。

(2) 多个系统整合在 1 台服务器中,节约资源的同时,也面临一个严重的问题,即一旦服务器出现硬件故障,其上运行的多个系统都将停止运行。虚拟化的服务器合并的程度越高,此风险越大。可以使用异地备份的方式定期备份重要数据;严格控制服务器机房的温度,避免物理机升温过快,造成硬件的不稳定甚至宕机。最终的解决方案是通过双机双存储集群方案提高动态高可用性。

(3) 虽然 RHEL 系统安全性极高,但是超级管理员 root 账号具有至高无上的权限,严格管理账号密码至关重要,严格控制硬件防火墙的的端口,对外仅开放有限的端口号,服务器的 IP 地址使用专有网段,限定超级管理员访问地址,严禁非管理员接近物理机甚至上机操作等,都是很必要的安全措施。

5 结 语

服务器虚拟化已经成为主流技术,并非只有在大型的数据中心才可以应用,上例说明了小型的服务器环境也可以成功应用。服务器虚拟化技术可以帮助单位整合服务器资源,并在一定程度上解决了数据中心空间、电力、制冷不足的问题,具有良好的应用效果。随着虚拟化技术的日益完善,会有越来越多的应用逐渐迁移到虚拟化环境中,各种各样的安全威胁也会不断出现,对政务网站的数据安全及基础架构的安全提出了新的要求。因此,在部署服务器虚拟化的同时,必须完善安全管理策略,严格执行安全措施,从根本上预防虚拟化安全问题,真正实现政务网站安全高效节约成本的最终目标。

参考文献:

[1] 刘亚军,刘延军,李涛.服务器虚拟化技术在报业的应用初探[J].中国传媒科技,2011,(11).

[2] 金天昕.服务器虚拟化管理问题与对策[J].中小企业管理与科技(下旬刊),2010,(12).

[3] 秦学东.开源虚拟化——KVM 的构建[J].现代图书情报技术,2011,(11).

[4] 宋欣.图书馆服务器虚拟化存在的安全风险与防范措施[J].现代信息技术,2011,(4).

[5] 宋晓光,杨晒晒,吕渊鸣.虚拟化技术在数字化校园建设中的应用[J].中国教育网络,2011,(3).

(编辑:邓 玲)

(上接第 184 页)

(4) 管理与数据的安全。水利水电云 GIS 平台中异构网络环境中透明的协同或融合,需要具有良好的可扩展性并能进行网络组件化的即插即用自主管理,减少甚至排除人为的配置与干预,尤其以大规模自组织工作模式的泛在节点与终端自主管理为突出需求。同时还应能针对网络及业务环境的变化做出迅速的反应,保证水利水电云 GIS 平台中传感采集、网络传输、业务认证端到端的信息安全,构建以用户为中心面向水利水电应用的可管可控可信的网络支撑体系。

(编辑:郑 毅)