

(19) 中华人民共和国国家知识产权局



## (12) 发明专利申请

(10) 申请公布号 CN 103810422 A

(43) 申请公布日 2014. 05. 21

(21) 申请号 201410058594. 1

(22) 申请日 2014. 02. 20

(71) 申请人 东莞中国科学院云计算产业技术创新与育成中心

地址 523808 广东省东莞市松山湖高新技术  
产业开发区松科苑 14 号楼

申请人 中国科学院自动化研究所

(72) 发明人 王飞跃 孔庆杰 邹哲峰 熊刚  
朱凤华

(74) 专利代理机构 北京科亿知识产权代理事务  
所（普通合伙） 11350

代理人 汤东凤

(51) Int. Cl.

G06F 21/53 (2013. 01)

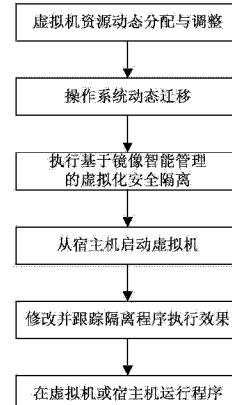
权利要求书2页 说明书6页 附图3页

### (54) 发明名称

一种基于镜像智能管理的安全虚拟化隔离方  
法

### (57) 摘要

本发明涉及云计算虚拟化安全技术领域，尤其是一种基于镜像智能管理的安全虚拟化隔离方法。包括下列步骤：1. 虚拟机资源动态分配与调整；2. 操作系统动态迁移；3. 执行基于镜像智能管理的虚拟化安全隔离；4. 从宿主机启动虚拟机；5. 修改并跟踪隔离程序执行效果；6. 在虚拟机或宿主机运行程序。本发明方法能够平衡虚拟化系统安全隔离性、功能完整性、性能适应性和行为可监控性等；可用于云计算虚拟化安全中。



1. 一种基于镜像智能管理的安全虚拟化隔离方法,其特征在于 :包括下列步骤 :

步骤 1 :在宿主机上预留虚拟机或物理机,启动定时器和电源管理器,将每个虚拟机部署在不同的磁盘区域或空间 ;

步骤 2 :操作系统动态迁移管理器在虚拟层标识客户操作系统中的进程,将进程日志自动记录到不兼容服务数据库 ;

步骤 3 :制作虚拟机所需要运行的镜像文件,创建引导文件、内核文件和镜像文件,通过镜像管理,将镜像文件和数据复制到特定的存储空间或其他存储服务器 ;

步骤 4 :启动 SVIS 虚拟机,运行系统服务和开机自动运行的软件 ;

步骤 5 :运行修改跟踪过滤驱动来监视 Local-Booted OS 中的数据修改信息和隔离程序执行效果 ;

步骤 6 :在虚拟机或宿主机上运行应用程序。

2. 根据权利要求 1 所述的安全虚拟化隔离方法,其特征在于 :步骤 1 具体包括 :

步骤 11 :客户远程申请虚拟机或物理机预留 ;

步骤 12 :宿主系统根据用户的权限和预留情况跳转到预留模块 ;

步骤 13 :如果是物理机预留,系统判断用户是否具有物理机预留权限,如果有,则将预留物理机 IP 地址、启动、关闭时间等信息放入数据库进行保存 ;否则,提示权限不足,不能预留 ;

步骤 14 :定时器进行事件处理,当到达预留结束时间的前 10 分钟,启动物理机 ;当到达预留的开始时间时,锁定或者关闭计算机 ;

步骤 15 :如果是虚拟机预留,系统判断用户是否具有虚拟机或 CPU 预留权限,如果有,则将虚拟机类型、预留的虚拟机硬盘大小、CPU、内存、启动和关闭时间等放入数据库进行保存 ;否则,提示权限不足,不能预留 ;

步骤 16 :定时器进行事件处理,当到达预留开始时间的前 30 分钟时,系统执行虚拟机启动程序进行启动 ;当到达预留结束时间,系统关闭或者终止虚拟机的运行。

3. 根据权利要求 1 所述的安全虚拟化隔离方法,其特征在于 :步骤 3 具体包括 :

步骤 31 :制作虚拟机镜像文件,包括制作引导文件、内核文件、以及利用操作系统打包并合成镜像文件,并将上述三个文件放到指定位置 ;

步骤 32 :将镜像文件纳入服务数据库和文件系统进行管理,包括镜像的修改、镜像中的安装软件和程序动态增加或减少,镜像文件的属性调整,引导文件的配置和管理、内核文件的调整和硬件的拔插管理等 ;

步骤 33 :物理机磁盘管理,包括对磁盘进行监控、磁盘的动态分区、磁盘之间通信的管理和配置等 ;

步骤 34 :根据磁盘信息在宿主机上创建 SVIS 虚拟机实例 ;

步骤 35 :利用 SVIS 虚拟机监视器,对虚拟机和虚拟机上的数据进行虚拟化管理 ;

步骤 36 :对于 Local-Booted OS 中访问的目录、文件等敏感数据,将在被修改前复制到特定的磁盘分区实现数据隔离。

4. 根据权利要求 2 所述的安全虚拟化隔离方法,其特征在于 :步骤 3 具体包括 :

步骤 31 :制作虚拟机镜像文件,包括制作引导文件、内核文件、以及利用操作系统打包并合成镜像文件,并将上述三个文件放到指定位置 ;

步骤 32 :将镜像文件纳入服务数据库和文件系统进行管理,包括镜像的修改、镜像中的安装软件和程序动态增加或减少,镜像文件的属性调整,引导文件的配置和管理、内核文件的调整和硬件的拔插管理等;

步骤 33 :物理机磁盘管理,包括对磁盘进行监控、磁盘的动态分区、磁盘之间通信的管理和配置等;

步骤 34 :根据磁盘信息在宿主机上创建 SVIS 虚拟机实例;

步骤 35 :利用 SVIS 虚拟机监视器,对虚拟机和虚拟机上的数据进行虚拟化管理;

步骤 36 :对于 Local-Booted OS 中访问的目录、文件等敏感数据,将在被修改前复制到特定的磁盘分区实现数据隔离。

5. 根据权利要求 1 至 4 任一项所述的安全虚拟化隔离方法,其特征在于:步骤 5 具体包括:

步骤 51 :在宿主机和虚拟机同时部署修改跟踪过滤驱动;

步骤 52 :开启 SVIS 虚拟机监视器,跟踪隔离程序执行效果,监视虚拟机和数据的修改信息;

步骤 53 :运行结束时向用户提供三种操作:放弃 SVIS 内隔离程序的执行结果、保留执行结果和提交执行结果到宿主操作系统。

6. 根据权利要求 1 至 4 任一项所述的安全虚拟化隔离方法,其特征在于:所述的方法还包括:执行虚拟机安全隔离后,SVIS VMM 采用“动态指令转换技术”,使得 SVIS VMM 通过运行时指令转换将原本不产生自陷的非特权敏感指令替换为具有通知 VMM 功能的指令。被隔离的非可信软件在由 SVIS 虚拟机启动的 Local-Booted OS 中运行,而可信程序则直接在宿主操作系统上运行。

7. 根据权利要求 5 所述的安全虚拟化隔离方法,其特征在于:所述的方法还包括:执行虚拟机安全隔离后,SVIS VMM 采用“动态指令转换技术”,使得 SVIS VMM 通过运行时指令转换将原本不产生自陷的非特权敏感指令替换为具有通知 VMM 功能的指令。被隔离的非可信软件在由 SVIS 虚拟机启动的 Local-Booted OS 中运行,而可信程序则直接在宿主操作系统上运行。

## 一种基于镜像智能管理的安全虚拟化隔离方法

### 技术领域

[0001] 本发明涉及云计算虚拟化安全技术领域,尤其是一种基于镜像智能管理的安全虚拟化隔离方法。

### 背景技术

[0002] 虚拟化是当前云计算技术中发展十分迅速的新兴产业,具有广阔的发展前景和应用领域;但同时在互联网环境下虚拟化用户和虚拟化平台面临的安全威胁和挑战也是前所未有的。在典型的云计算服务平台中,资源以虚拟化按需租用的使目模式提供给用户,虚拟化可以减少操作成本,允许用户按需快速地调配资源;但这种灵活性也会使虚拟机安全隐患在云计算平台快速扩展。如果云计算平台中的虚拟化软件存在安全漏洞,用户的数据就可能被其它共用云平台的用户非法访问。而且,由于云计算规模的巨大性、开放性和复杂性等特点,一旦其遭受恶意攻击,将会带来严重的信息安全事故,这就有必要采取虚拟化隔离方法。

[0003] 云计算中用户使用的是虚拟化资源,同一计算机上的虚拟机之间的通信是通过本地硬件进行的,因而传统基于网络通信的安全控制机制无法进行有效的监测和过滤,需要新的方法来解决这个问题。同时虚拟机是承接底层硬件和上层服务应用的关键层次,建立安全可信的虚拟化环境是对上层管理应用安全的基本支持。虚拟机可信、隔离、迁移等技术都需要有针对应硬件层的解决方法,以解决虚拟化给云计算和大数据存储带来的新风险。

[0004] 当前的虚拟化隔离技术无法使得各个虚拟机平等地共享磁盘带宽、保证虚拟机间的I/O性能隔离问题,往往造成文件系统数据与本地磁盘数据的冲突,操作系统关键文件的一致性将会导致虚拟化系统的崩溃。由于虚拟机与宿主硬件环境的差异,依赖于硬件系统的本地服务很可能导致虚拟机启动时挂起甚至崩溃。此外,现有的隔离程序仅执行虚拟机隔离操作,而缺少隔离执行效果的跟踪,无法监控运行环境由于外界攻击而导致的数据删改行为。对于隔离运行非可信软件的运行环境而言,为了实现操作系统应用程序透明的目标,同时能够重现已有的软件运行环境并支持操作系统信息重构,就需要在保证安全隔离性的前提下提升隔离运行环境的功能完整性、性能适应性与行为可监控性。

### 发明内容

[0005] 本发明解决的技术问题在于提出一种基于镜像智能管理的安全虚拟化隔离方法;用来保护虚拟机运行过程中的虚拟机文件和存储资源。

[0006] 本发明解决上述技术问题的技术方案是:

[0007] 包括下列步骤:

[0008] 步骤1:在宿主机上预留虚拟机或物理机,启动定时器和电源管理器,将每个虚拟机部署在不同的磁盘区域或空间;

[0009] 步骤2:操作系统动态迁移管理器在虚拟层标识客户操作系统中的进程,将进程日志自动记录到不兼容服务数据库;

- [0010] 步骤 3 :制作虚拟机所需要运行的镜像文件,创建引导文件、内核文件和镜像文件,通过镜像管理,将镜像文件和数据复制到特定的存储空间或其他存储服务器;
- [0011] 步骤 4 :启动 SVIS 虚拟机,运行系统服务和开机自动运行的软件;
- [0012] 步骤 5 :运行修改跟踪过滤驱动来监视 Local-Booted OS(本地启动系统)中的数据修改信息和隔离程序执行效果;
- [0013] 步骤 6 :在虚拟机或宿主机上运行应用程序。
- [0014] 步骤 1 具体包括:
- [0015] 步骤 11 :客户远程申请虚拟机或物理机预留;
- [0016] 步骤 12 :宿主系统根据用户的权限和预留情况跳转到预留模块;
- [0017] 步骤 13 :如果是物理机预留,系统判断用户是否具有物理机预留权限,如果有,则将预留物理机 IP 地址、启动、关闭时间等信息放入数据库进行保存;否则,提示权限不足,不能预留;
- [0018] 步骤 14 :定时器进行事件处理,当到达预留结束时间的前 10 分钟,启动物理机;当到达预留的开始时间时,锁定或者关闭计算机;
- [0019] 步骤 15 :如果是虚拟机预留,系统判断用户是否具有虚拟机或 CPU 预留权限,如果有,则将虚拟机类型、预留的虚拟机硬盘大小、CPU、内存、启动和关闭时间等放入数据库进行保存;否则,提示权限不足,不能预留;
- [0020] 步骤 16 :定时器进行事件处理,当到达预留开始时间的前 30 分钟时,系统执行虚拟机启动程序进行启动;当到达预留结束时间,系统关闭或者终止虚拟机的运行。
- [0021] 步骤 3 具体包括:
- [0022] 步骤 31 :制作虚拟机镜像文件,包括制作引导文件、内核文件、以及利用操作系统打包并合成镜像文件,并将上述三个文件放到指定位置;
- [0023] 步骤 32 :将镜像文件纳入服务数据库和文件系统进行管理,包括镜像的修改、镜像中的安装软件和程序动态增加或减少,镜像文件的属性调整,引导文件的配置和管理、内核文件的调整和硬件的拔插管理等;
- [0024] 步骤 33 :物理机磁盘管理,包括对磁盘进行监控、磁盘的动态分区、磁盘之间通信的管理和配置等;
- [0025] 步骤 34 :根据磁盘信息在宿主机上创建 SVIS 虚拟机实例;
- [0026] 步骤 35 :利用 SVIS 虚拟机监视器,对虚拟机和虚拟机上的数据进行虚拟化管理;
- [0027] 步骤 36 :对于 Local-Booted OS 中访问的目录、文件等敏感数据,将在被修改前复制到特定的磁盘分区实现数据隔离。
- [0028] 步骤 5 具体包括:
- [0029] 步骤 51 :在宿主机和虚拟机同时部署修改跟踪过滤驱动;
- [0030] 步骤 52 :开启 SVIS 虚拟机监视器,跟踪隔离程序执行效果,监视虚拟机和数据的修改信息;
- [0031] 步骤 53 :运行结束时向用户提供三种操作:放弃 SVIS 内隔离程序的执行结果、保留执行结果和提交执行结果到宿主操作系统。
- [0032] 方法还包括:执行虚拟机安全隔离后,SVIS VMM 采用“动态指令转换技术”,使得 SVIS VMM 通过运行时指令转换将原本不产生自陷的非特权敏感指令替换为具有通知 VMM

功能的指令。被隔离的非可信软件在由 SVIS 虚拟机启动的 Local-Booted OS 中运行,而可信程序则直接在宿主操作系统上运行。

[0033] 本发明的有益效果有:

[0034] 本发明借助基于镜像智能管理的虚拟化安全隔离和操作系统动态迁移管理器,实现了本地虚拟化技术,解决了 SVIS 虚拟机与宿主硬件环境之间冲突,用户可以安全删除不允许在本地操作系统中访问的目录、文件等敏感数据,实现了 SVIS 虚拟机和数据的安全隔离。

[0035] 通过修改跟踪管理器,能够跟踪和记录被隔离软件对数据的修改操作,从而为分析程序行为与提交相应程序的执行效果到宿主环境提供依据,实现了系统隔离运行环境的行为监控。而且,镜像智能管理能够保证虚拟机位于不同的磁盘区域,保证虚拟机资源的不重叠。由此,非可信软件可以运行在一个与宿主操作系统隔离的虚拟计算机系统中,实现了操作系统隔离。

[0036] 本发明方法是在安全虚拟化隔离系统 (Safe Virtualization Isolation System, SVIS) 上实现的,构造出以本地虚拟化技术为核心的满足隔离运行模型的方法,该方法独立于操作系统实现,具有很好的可移植性。同时,该方法能够平衡虚拟化系统安全隔离性、功能完整性、性能适应性和行为可监控性,被保护的宿主环境的容侵能力也将得到有效提升。

## 附图说明

[0037] 下面结合附图对发明进一步说明:

[0038] 图 1 是本发明的基于镜像智能管理的安全虚拟化隔离系统架构图;

[0039] 图 2 是本发明的基于镜像智能管理的安全虚拟化隔离方法流程图;

[0040] 图 3 是本发明的虚拟机资源预留流程图;

[0041] 图 4 是本发明的镜像智能管理流程图;

[0042] 图 5 是本发明的修改跟踪记录器流程图。

## 具体实施方式

[0043] 如图 1 所示,是本发明的基于镜像智能管理的安全虚拟化隔离系统架构图。安全虚拟化隔离系统 (Safe Virtualization Isolation System, SVIS) 体系结构由五个核心组件构成:SVIS 虚拟机监视器 (SVIS Virtual Machine Monitor, 简称 SVISVMM)、基于镜像智能管理的虚拟化安全隔离、操作系统动态迁移管理器、修改跟踪管理器和虚拟层系统信息组件。根据隔离运行模型,SVIS VMM 需要以 VMM 的形式实现,即在宿主操作系统之上运行。SVIS VMM 负责创建非可信软件的隔离运行环境—SVIS 虚拟机 (SVIS Virtual Machine, 简称 SVIS VM)。借助基于镜像智能管理的虚拟化安全隔离和操作系统动态迁移管理器,SVIS 实现了本地虚拟化技术,即 SVIS 虚拟机中无需重新安装操作系统 (这是现有虚拟机软件的运行模式),而是直接从宿主操作系统启动,启动后的操作系统即为“本地启动操作系统”(Local-Booted OS)。修改跟踪管理器则记录 Local-Booted OS 和宿主操作系统 (宿主 OS) 内的资源 (如文件、注册表等) 变化信息,为进一步分析被隔离软件的行为或之后将 Local-Booted OS 的数据变化合并到宿主操作系统提供支持。虚拟层系统信息组件不依赖

于操作系统提供的接口,能够利用硬件层的数据(如处理器寄存器信息、存储器管理单元、磁盘信息等)重构出具有应用层语义的客户操作系统信息。

[0044] 如图2所示,是本发明的基于镜像智能管理的安全虚拟化隔离方法流程图。本发明所述的基于镜像智能管理的安全虚拟化隔离方法,包括下列步骤:

[0045] (1) 虚拟机资源动态分配与调整。

[0046] 虚拟机资源的动态分配和调整是使用虚拟机的必要准备,本发明通过实现物理机和虚拟机的有效预留,可以动态启动和关闭物理机,也可以动态创建和销毁虚拟机。虚拟机资源动态分配与调整主要是在宿主机上设置虚拟机或物理机的预留权限,启动定时器和电源管理器,准备对预留事件进行处理,使得每个虚拟机位于不同的磁盘区域或空间,进而分配或调整虚拟机资源。

[0047] (2) 操作系统动态迁移

[0048] 由于SVIS虚拟机与宿主硬件环境的差异,依赖于硬件系统的系统服务可能会导致SVIS虚拟机启动时挂起甚至崩溃。为了解决这个问题,操作系统动态迁移管理器在虚拟层标识客户操作系统中的进程(包括当前进程),结合此技术与SVIS VMM获取的Local-Booted OS的内存信息,就能够确定导致Local-Booted OS挂起或崩溃的进程,进而将这些信息自动记录到不兼容服务数据库。此后,在启动SVIS虚拟机前,操作系统动态迁移管理器将在Local-Booted OS中自动禁用所有不兼容服务数据库中的服务。

[0049] 系统启动过程中关键一步就是由服务控制管理器启动各个系统服务。如果有系统服务依赖于硬件平台且与SVIS虚拟设备不兼容,也会导致Local-Booted OS不能正常启动甚至使系统崩溃。针对这一问题,本发明通过操作系统动态迁移技术,在任一时刻标识出SVIS虚拟机中运行的当前进程,这样就能发现导致操作系统死锁或崩溃的进程,进而在之后的启动过程中禁用相应的服务。成功启动了Local-Booted OS之后,仍有一些软件的正常运行需要依赖于硬件信息。为了解决这个问题,SVIS引入了硬件标识迁移方法,将宿主计算机系统的各类硬件标识导出到SVIS虚拟机的相应虚拟设备上从而解决了依赖于硬件信息的软件迁移问题。

[0050] (3) 执行基于镜像智能管理的虚拟化安全隔离

[0051] 由于SVIS虚拟机或外界应用程序需要访问系统卷,而此时宿主操作系统也在修改系统卷,前者对数据的修改并没有使用宿主操作系统提供的访问接口,后者的修改信息也无法及时被SVIS虚拟机内的文件系统感知,这就造成了文件系统数据与磁盘数据的冲突,操作系统关键文件的不一致将会导致系统的崩溃。为了解决这个问题,本文提出了基于镜像智能管理的虚拟化安全隔离技术。执行镜像智能管理是指通过制作虚拟机所需要的镜像文件,将镜像文件纳入数据库和文件系统进行管理。它提供了文件系统标准卷相同的访问接口,镜像文件以存储设备的形式导出到SVIS虚拟机,形成虚拟机虚拟磁盘。通过镜像管理,将镜像文件在原始卷的数据被修改前复制该数据到特定的存储空间或其他存储服务器。虚拟机和宿主机之间有严格的权限级别,不能随意进行文件共享,虚拟机不能通过宿主机再访问另一个虚拟机。之后,用户可以安全删除不允许在Local-Booted OS中访问的目录、文件等敏感数据,从而实现SVIS虚拟机和数据的安全隔离。

[0052] (4) 从宿主机启动虚拟机

[0053] 从宿主机上的操作系统直接启动SVIS虚拟机,之后在SVIS虚拟机上运行启用的

系统服务和开机自动运行的软件。SVIS 虚拟机在第一次启动时,虚拟设备会重用原有的设备驱动程序或重新安装新的设备驱动。

[0054] (5) 修改并跟踪隔离程序执行效果

[0055] 为了跟踪隔离程序执行效果并监视 Local-Booted OS 中的数据修改信息,需要运行修改跟踪过滤驱动以监视和记录文件的修改操作。

[0056] (6) 在虚拟机或宿主机运行程序

[0057] 在实现的应用程序或数据在虚拟机上的安全隔离后,即可从虚拟机或宿主机运行程序。SVIS VMM 采用“动态指令转换技术”,使得 SVIS VMM 通过运行时指令转换将原本不产生自陷的非特权敏感指令替换为具有通知 VMM 功能的指令。由此,被隔离的非可信软件在由 SVIS 虚拟机启动的 Local-Booted OS 中运行,而可信程序则直接在宿主操作系统上运行。

[0058] 图 3 是本发明的虚拟机资源预留流程图。图 3 进一步解释了图 2 虚拟机资源动态分配与调整中的虚拟机资源预留流程。虚拟机资源的动态预留和调整包括如下功能:资源预留的管理与分配、预留权限的设置、预留信息的管理和配置、定时器的管理、物理机的电源管理等。图 3 具体流程为:

[0059] (1) 客户远程申请虚拟机或物理机预留。

[0060] (2) 宿主系统根据用户的权限和预留情况跳转到物理机预留或虚拟机预留功能模块;

[0061] (3) 如果是物理机预留,系统判断用户是否具有物理机预留权限,如果有,则将预留物理机 IP 地址、启动、关闭时间等信息放入数据库进行保存;否则,提示权限不足,不能预留。

[0062] (4) 定时器进行事件处理,当到达预留结束时间的前 10 分钟,启动物理机;当到达预留的开始时间时,锁定或者关闭计算机。

[0063] (5) 如果是虚拟机预留,系统判断用户是否具有虚拟机或 CPU 预留权限,如果有,则将虚拟机类型、预留的虚拟机硬盘大小、CPU、内存、启动和关闭时间等放入数据库进行保存;否则,提示权限不足,不能预留。

[0064] (6) 定时器进行事件处理,当到达预留开始时间的前 30 分钟时,系统执行虚拟机启动程序进行启动;当到达预留结束时间,系统关闭或者终止虚拟机的运行。

[0065] 图 4 是本发明的镜像智能管理流程图。操作步骤如下:

[0066] (1) 制作虚拟机所需要的镜像文件,包括制作引导文件、内核文件、以及利用操作系统打包并合成镜像文件,并将上述三个文件放到指定位置。

[0067] (2) 将镜像文件纳入服务数据库和文件系统进行管理,包括镜像的修改、镜像中的安装软件和程序动态增加或减少,镜像文件的属性调整,引导文件的配置和管理、内核文件的调整和硬件的拔插管理等。

[0068] (3) 物理机磁盘管理,包括对磁盘进行监控、磁盘的动态分区、磁盘之间通信的管理和配置等。

[0069] (4) 根据磁盘信息在宿主机上创建 SVIS 虚拟机实例。

[0070] (5) 利用 SVIS 虚拟机监视器,对虚拟机和虚拟机上的数据进行虚拟化管理。

[0071] (6) 通过 SVIS 虚拟机镜像管理,实现虚拟机隔离,对于 Local-Booted OS 中访问的

目录、文件等敏感数据，将在被修改前复制到特定的磁盘分区实现数据隔离。

[0072] 图 5 是本发明的修改跟踪记录器流程图。如图 5 进一步解释了图 2 修改并跟踪隔离程序执行效果中的修改跟踪记录器处理方法。具体步骤如下：

[0073] (1) 在宿主机和虚拟机同时部署修改跟踪过滤驱动，从而提交 Local-Booted OS 中的修改结果到宿主操作系统。

[0074] (2) 开启 SVIS 虚拟机监视器，跟踪隔离程序执行效果，监视虚拟机和数据的修改信息。

[0075] (3) SVIS 运行结束时，可以向用户提供三种操作：放弃 SVIS 内隔离程序的执行结果、保留执行结果和提交执行结果到宿主操作系统。对于第一种情况，SVIS 虚拟机的整个运行环境将被销毁，之后启动的 SVIS 虚拟机均需要重新创建新的虚拟简单磁盘；若保留执行结果，则仅关闭 SVIS 虚拟机，而不销毁虚拟简单磁盘；对于第三种情况，需要利用修改跟踪管理器来分析和比较 SVIS 虚拟机从创建到结束整个过程中 Local-Booted OS 和宿主操作系统的数据变化，进而修改合并数据。

[0076] 以上是对本发明具体实施例的描述，并非对本发明保护范围的限制；凡在本发明公开的方案之内，所做的任何无需过多创造性劳动的修改、等同替换、改进等，均应包含在本发明的保护范围之内。

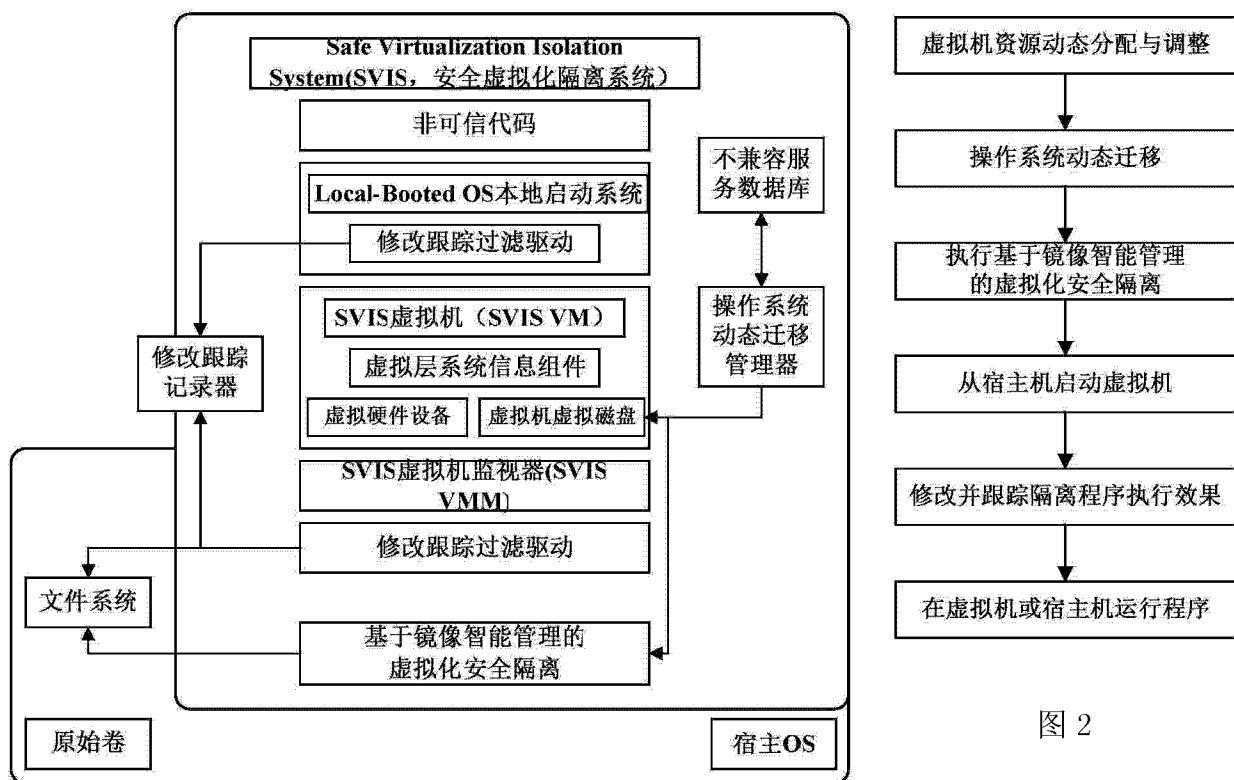


图 1

图 2

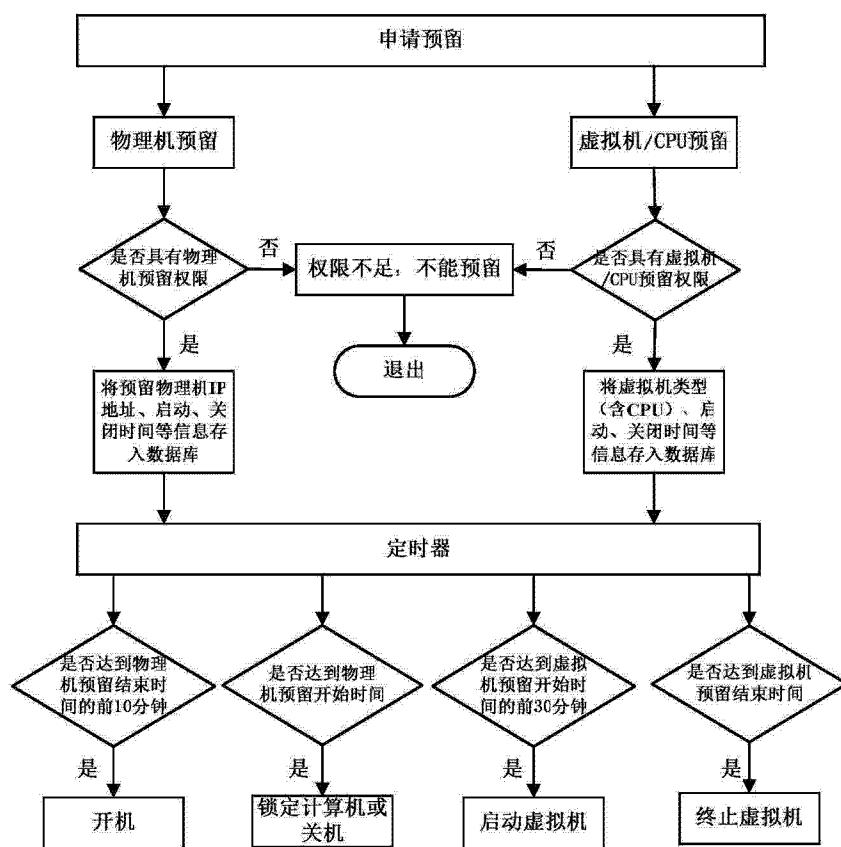


图 3

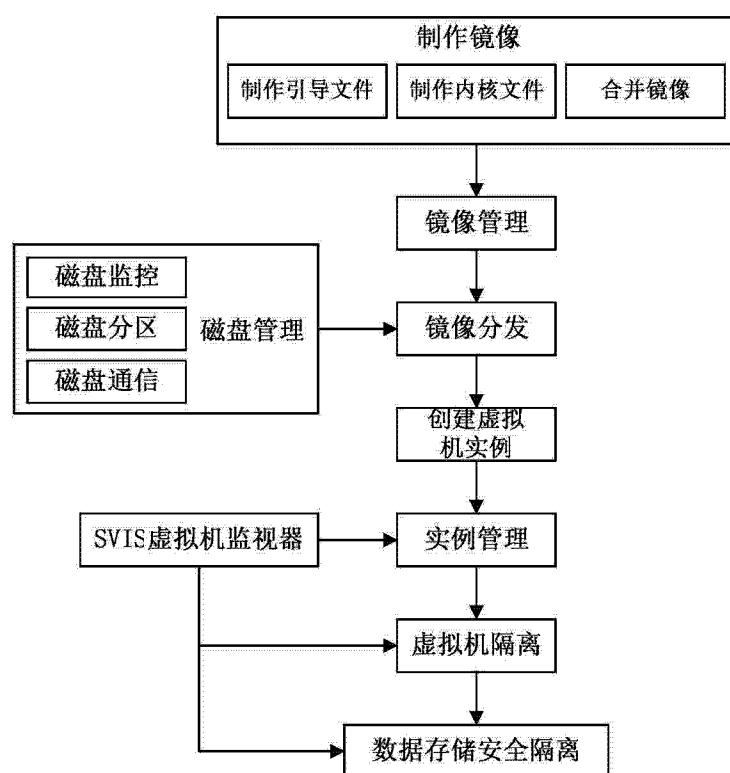


图 4

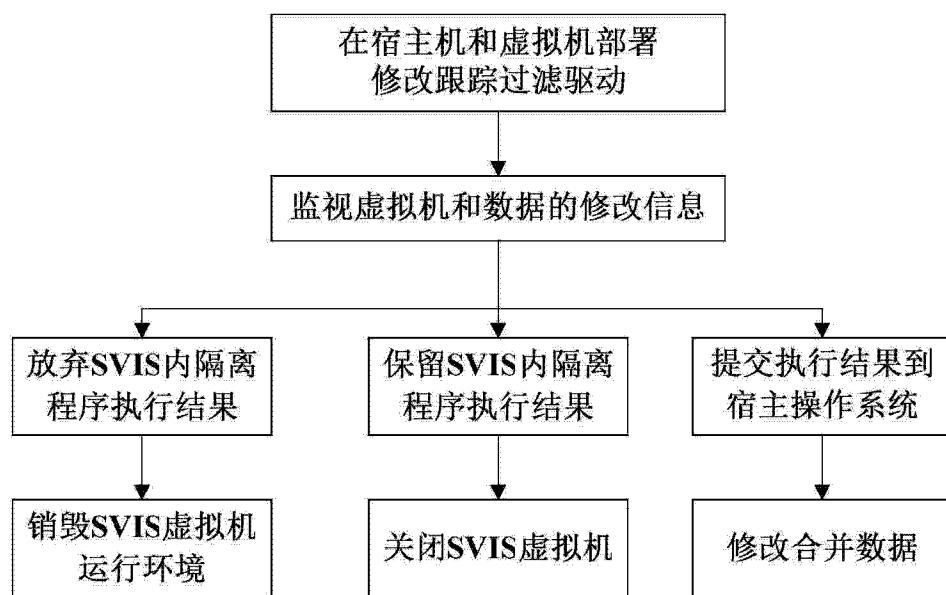


图 5