(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117940900 A
(43)申请公布日 2024.04.26

(21)申请号 202280062038.4
(22)申请日 2022.09.12
(30)优先权数据
17/474,220 2021.09.14 US
(85)PCT国际申请进入国家阶段日
2024.03.13
(86)PCT国际申请的申请数据
PCT/EP2022/075220 2022.09.12
(87)PCT国际申请的公布数据
WO2023/041462 EN 2023.03.23
(71)申请人 国际商业机器公司
地址 美国
(72)发明人 J·布拉德伯里 T·亨德尔
R·宾德根 C·伊布伦达
C·博尔特雷格 J·A·弗兰克
(74)专利代理机构 北京市中咨律师事务所 11247
专利代理师 于静 刘薇
(51)Int.Cl.
G06F 9/455(2006.01)
G06F 21/53(2006.01)

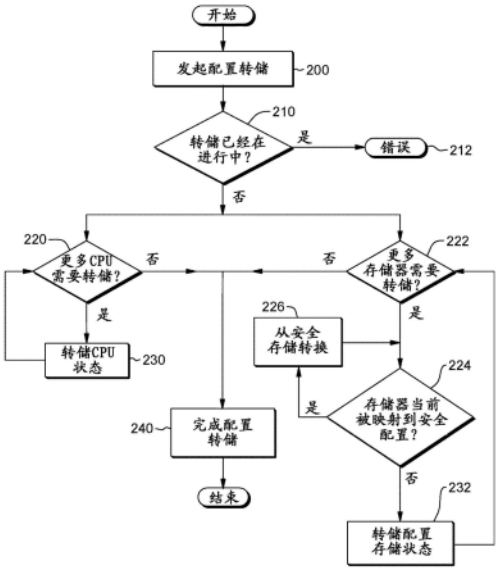
权利要求书3页 说明书20页 附图11页

(54)发明名称

存储安全虚拟机的诊断状态

(57)摘要

获得存储虚拟机的诊断状态的至少一个请求。基于获得至少一个请求,执行对虚拟机的诊断状态的存储以提供虚拟机的所存储的诊断状态。执行存储包括加密虚拟机的未被加密的且正在被存储的诊断状态,以防止在加密虚拟机的未被加密的且正在被存储的诊断状态之前由不可信实体读取虚拟机的诊断状态。



CN 117940900 A

1.一种用于促进计算环境内的处理的计算机程序产品,所述计算机程序产品包括:

一个或多个计算机可读存储介质和共同存储在所述一个或多个计算机可读存储介质上的程序指令,所述程序指令用于执行一种方法,所述方法包括:

获得存储虚拟机的诊断状态的至少一个请求;以及

基于获得所述至少一个请求,执行所述虚拟机的诊断状态的存储以提供所述虚拟机的所存储的诊断状态,其中,执行所述存储包括:加密所述虚拟机的未被加密且正在被存储的诊断状态,以防止在加密所述虚拟机的未被加密且正在被存储的诊断状态之前由不可信实体读取所述虚拟机的所述诊断状态。

2.根据权利要求1所述的计算机程序产品,其中,所述虚拟机的所存储的诊断状态包括:所述虚拟机的存储器内容。

3.根据权利要求1或2所述的计算机程序产品,其中,所述虚拟机的所存储的诊断状态包括:所述虚拟机的一个或多个处理器寄存器的内容。

4.根据前述权利要求中的任一项所述的计算机程序产品,其中,所述方法还包括:获得发起所述虚拟机的诊断状态的存储的发起存储诊断状态请求,所述发起存储诊断状态请求将被用于获得第一加密密钥,所述第一加密密钥将被用于加密所述虚拟机的未被加密且正在被存储的诊断状态的至少一部分。

5.根据权利要求4所述的计算机程序产品,其中,获得所述至少一个请求包括获得存储诊断处理器状态请求,并且其中,基于获得所述存储诊断处理器状态请求,执行所述诊断状态的存储包括:

使用所述第一加密密钥对所述虚拟机的至少一个处理器的至少选择内容进行加密,以提供经加密的处理器内容;以及

存储经加密的处理器内容。

6.根据前述权利要求中的任一项所述的计算机程序产品,其中,获得所述至少一个请求包括获得从安全存储器转换请求,并且其中,基于获得所述从安全存储器转换请求,执行所述诊断状态的存储包括:

使用第二加密密钥对所述虚拟机的未被加密的至少选择存储器内容进行加密以提供经加密的存储器内容;以及

存储经加密的存储器内容。

7.根据权利要求6所述的计算机程序产品,其中,基于获得所述从安全存储器转换请求,执行所述诊断状态的存储包括:

确定其内容将被存储的存储器单元是否被加密;以及

基于确定所述存储器单元未被加密,使用所述第二加密密钥来加密所述存储器单元,其中,被加密的存储器单元不被重新加密。

8.根据前述权利要求中的任一项所述的计算机程序产品,其中,所存储的诊断状态包括经加密的存储器内容,并且其中,所述方法还包括:

获得存储诊断存储器状态请求;以及

基于获得所述存储诊断存储器状态请求,存储将用于解密经加密的存储器内容的元数据。

9.根据权利要求8所述的计算机程序产品,其中,所述元数据包括将要用于创建将要用

于解密经加密的存储器内容的一个或多个选择值的一个或多个选择分量值。

10.根据前述权利要求中的任一项所述的计算机程序产品,其中,所述方法还包括:

获得完成诊断状态的存储的完成请求;以及

基于获得所述完成请求,提供将要用于解密所述虚拟机的经加密的所存储的诊断状态的数据。

11.根据权利要求10所述的计算机程序产品,其中,所述数据包括在对经加密的存储器内容进行解密时所使用的第二加密密钥和将被用于创建将要在加密时所使用的一个或多个选择值的随机数值,并且其中,所述数据的至少一部分被加密。

12.一种用于促进计算环境内的处理的计算机系统,所述计算机系统包括:

存储器;以及

与所述存储器通信的至少一个处理器,其中,所述计算机系统被配置为执行一种方法,所述方法包括:

获得存储虚拟机的诊断状态的至少一个请求;以及

基于获得所述至少一个请求,执行所述虚拟机的诊断状态的存储以提供所述虚拟机的所存储的诊断状态,其中,执行所述存储包括:加密所述虚拟机的未被加密且正在被存储的诊断状态,以防止在加密所述虚拟机的未被加密且正在被存储的诊断状态之前由不可信实体读取所述虚拟机的所述诊断状态。

13.根据权利要求12所述的计算机系统,其中,所述方法还包括:获得发起所述虚拟机的诊断状态的存储的发起存储诊断状态请求,所述发起存储诊断状态请求将被用于获得第一加密密钥,所述第一加密密钥将被用于加密所述虚拟机的未被加密且正在被存储的诊断状态的至少一部分。

14.根据权利要求13所述的计算机系统,其中,获得所述至少一个请求包括获得存储诊断处理器状态请求,并且其中,基于获得所述存储诊断处理器状态请求,执行所述诊断状态的存储包括:

使用所述第一加密密钥对所述虚拟机的至少一个处理器的至少选择内容进行加密,以提供经加密的处理器内容;以及

存储经加密的处理器内容。

15.根据权利要求12至14中的任一项所述的计算机系统,其中,获得所述至少一个请求包括获得从安全存储器转换请求,并且其中,基于获得所述从安全存储器转换请求,执行所述诊断状态的存储包括:

使用第二加密密钥对所述虚拟机的未被加密的至少选择存储器内容进行加密以提供经加密的存储器内容;以及

存储经加密的存储器内容。

16.根据权利要求12至15中的任一项所述的计算机系统,其中,所存储的诊断状态包括经加密的存储器内容,并且其中,所述方法还包括:

获得存储诊断存储器状态请求;以及

基于获得所述存储诊断存储器状态请求,存储将用于解密经加密的存储器内容的元数据。

17.一种促进计算环境内的处理的计算机实现的方法,所述计算机实现的方法包括:

获得存储虚拟机的诊断状态的至少一个请求;以及

基于获得所述至少一个请求,执行所述虚拟机的诊断状态的存储以提供所述虚拟机的所存储的诊断状态,其中,执行所述存储包括:加密所述虚拟机的未被加密且正在被存储的诊断状态,以防止在加密所述虚拟机的未被加密且正在被存储的诊断状态之前由不可信实体读取所述虚拟机的所述诊断状态。

18.根据权利要求17所述的计算机实现的方法,其中,所述方法还包括:获得发起所述虚拟机的诊断状态的存储的发起存储诊断状态请求,所述发起存储诊断状态请求将被用于获得第一加密密钥,所述第一加密密钥将被用于加密所述虚拟机的未被加密且正在被存储的诊断状态的至少一部分。

19.根据权利要求18所述的计算机实现的方法,其中,获得所述至少一个请求包括获得存储诊断处理器状态请求,并且其中,基于获得所述存储诊断处理器状态请求,执行所述诊断状态的存储包括:

使用所述第一加密密钥对所述虚拟机的至少一个处理器的至少选择内容进行加密,以提供经加密的处理器内容;以及

存储经加密的处理器内容。

20.根据权利要求17至19中的任一项所述的计算机实现的方法,其中,获得所述至少一个请求包括获得从安全存储器转换请求,并且其中,基于获得所述从安全存储器转换请求,执行所述诊断状态的存储包括:

使用第二加密密钥对所述虚拟机的未被加密的至少选择存储器内容进行加密以提供经加密的存储器内容;以及

存储经加密的存储器内容。

存储安全虚拟机的诊断状态

背景技术

[0001] 一个或多个方面一般涉及促进计算环境内的处理,尤其涉及改进这样的处理。

[0002] 虚拟机的诊断状态的存储(也称为虚拟机转储(dump))在文件中提供虚拟机的状态以供稍后分析。它通常用于查找虚拟机故障的根本原因。虚拟机的状态包括例如虚拟机的存储器的副本,以及虚拟机的一个或多个中央处理单元的选择寄存器的副本。

[0003] 一些虚拟机是安全虚拟机,其中计算机系统的硬件和固件拒绝对安全虚拟机的状态的访问,除了虚拟机主动指定为共享的特殊存储器区域之外。这种虚拟机不能被托管虚拟机的操作系统的管理程序或管理员访问,如通常可能的那样。对虚拟机状态的访问意味着主机系统上的授权实体可以从虚拟机存储器读取敏感信息,如加密密钥或机密文档,这是安全风险。

[0004] 将促进与虚拟机相关联的处理,包括存储诸如安全虚拟机之类的虚拟机的诊断状态。

发明内容

[0005] 通过提供一种用于促进计算环境内的处理的计算机程序产品,克服了现有技术的缺点,并且提供了附加的优点。该计算机程序产品包括一个或多个计算机可读存储介质和共同存储在该一个或多个计算机可读存储介质上以执行方法的程序指令。该方法包括获得存储虚拟机的诊断状态的至少一个请求。基于获得至少一个请求,执行对虚拟机的诊断状态的存储以提供虚拟机的存储的诊断状态。执行存储包括加密虚拟机的未被加密的且正在被存储的诊断状态,以防止在加密虚拟机的未被加密的且正在被存储的诊断状态之前由不可信实体读取虚拟机的诊断状态。

[0006] 可以存储虚拟机(例如,安全虚拟机)的诊断状态,同时保持正被存储用于诊断目的虚拟机的状态的安全性。

[0007] 作为示例,虚拟机的所存储的诊断状态包括虚拟机的存储器内容和/或虚拟机的所存储的诊断状态包括虚拟机的一个或多个处理器寄存器的内容。

[0008] 在一个示例中,获得发起虚拟机的诊断状态的存储的发起存储诊断状态请求。发起存储诊断状态请求将用于获得第一加密密钥,该第一加密密钥将用于加密虚拟机的未被加密且正在被存储的诊断状态的至少一部分。

[0009] 在一个示例中,获得至少一个请求包括获得存储诊断处理器状态请求。基于获得存储诊断处理器状态请求,执行诊断状态的存储包括例如使用第一加密密钥对虚拟机的至少一个处理器的至少选择内容进行加密,以提供经加密的处理器内容,以及存储经加密的处理器内容。

[0010] 在一个示例中,获得至少一个请求包括获得从安全存储器转换请求。基于获得从安全存储器转换请求,执行诊断状态的存储包括例如使用第二加密密钥对虚拟机的未被加密的至少选择存储器内容进行加密以提供经加密的存储器内容,并且存储经加密的存储器内容。

[0011] 作为示例,基于获得从安全存储器转换请求来执行诊断状态的存储包括例如确定其内容将被存储的存储器单元是否被加密,以及基于确定存储器单元未被加密,使用第二加密密钥来加密存储器单元,其中被加密的存储器单元不被重新加密。

[0012] 通过加密未被加密的内容(而不是重新加密经加密的状态),减少了处理周期和复杂度,提高了系统性能。

[0013] 在一个示例中,所存储的诊断状态包括经加密的存储器内容。此外,在一个示例中,获得存储诊断存储器状态请求,并且基于获得存储诊断存储器状态请求,存储用于解密经加密的存储器内容的元数据。

[0014] 作为示例,元数据包括将要用于创建将要用于解密经加密的存储器内容的一个或多个选择值的一个或多个选择分量值。

[0015] 在一个示例中,获得完成诊断状态的存储的完成请求,并且基于获得完成请求,提供要用于解密虚拟机的经加密的存储的诊断状态的数据。

[0016] 作为示例,数据包括在对经加密的存储器内容进行解密时所使用的第二加密密钥和将被用于创建将要在加密时所使用的一个或多个选择值的随机数值。此外,在一个示例中,数据的至少一部分被加密。

[0017] 本文还描述并要求保护与一个或多个方面相关的计算机实现的方法和系统。此外,本文还描述并要求保护与一个或多个方面相关的服务。

[0018] 通过本文所述的技术实现了额外的特征和优点。其它实施例和方面在本文中详细描述,且被视为所主张的方面的一部分。

附图说明

[0019] 在说明书结尾处的权利要求中作为示例特别指出并清楚地要求了一个或多个方面。从结合附图的以下详细描述中,一个或多个方面的前述和目的、特征和优点将变得显而易见,在附图中:

[0020] 图1描绘了包含和使用本发明的一个或多个方面的计算环境的一个示例;

[0021] 图2描绘了根据本发明的一个或多个方面的存储配置(例如,虚拟机)的诊断状态的一个示例,也称为执行配置转储;

[0022] 图3描绘了根据本发明的一个或多个方面的发起配置转储控制块的一个示例;

[0023] 图4A描绘了根据本发明的一个或多个方面的转储中央处理单元(CPU)状态控制块的一个示例;

[0024] 图4B描绘了根据本发明的一个或多个方面的安全中央处理单元转储区域的一个示例;

[0025] 图4C描绘了根据本发明的一个或多个方面所使用的从安全存储转换控制块的一个示例;

[0026] 图5描绘了根据本发明的一个或多个方面的转储配置存储状态控制块的一个示例;

[0027] 图6描绘了根据本发明的一个或多个方面的完成配置转储控制块的一个示例;

[0028] 图7A-7C描绘了根据本发明的一个或多个方面的促进计算环境内的处理的一个示例;

[0029] 图8A描绘了用于结合和使用本发明的一个或多个方面的计算环境的另一示例;

[0030] 图8B描绘了根据本发明一个或多个方面的图8A的存储器的进一步细节;

[0031] 图9描绘了根据本发明的一个或多个方面的云计算环境的一个实施例;以及

[0032] 图10描绘了根据本发明的一个或多个方面的抽象模型层的一个示例。

具体实施方式

[0033] 根据本发明的一个或多个方面,提供了一种能力以便于在计算环境中进行处理。作为示例,该能力包括一种技术,其中虚拟机(例如,安全虚拟机)的诊断状态可被存储(也称为转储),同时维持正被存储的虚拟机的状态的安全性。作为示例,诊断状态在其可由不可信实体(例如,管理程序)读取之前被加密。

[0034] 在一个示例中,要被存储以用于诊断分析(即,转储)的虚拟机的存储器内容可以通过例如使用被称为转储密钥(也被称为第一加密密钥)的所选择密钥来加密。例如,被页调出并且当前用分页(paging)密钥(也称为第二加密密钥)加密的存储器被解密并且用所选择密钥重新加密。作为另一示例,根据本发明的一方面,为了降低复杂性和所使用的中央处理单元循环的数量,代替重新加密经加密的存储器(使用分页密钥来加密),提供存储器单元(例如,存储器页)的选择唯一值(例如,调整(tweak)值)并用所选择密钥来加密分页密钥。因此,被页调出的页不需要为了转储而被重新加密,并且仅未被加密的页被加密以用于转储。为了进一步解释,每个存储器单元被给予一个值,该值例如是无符号整数,其被称为调整值或选择唯一值。这些值从任意整数开始并且被连续地分配。该值可以被转换为例如小端字节数组,其中可以使用例如AES(高级加密标准)算法来执行对该值的加密。

[0035] 在一个或多个方面,为了安全地促进虚拟机(例如,安全虚拟机)的转储或诊断存储,提供并使用应用编程接口,该应用编程接口采用被称为超管理程序(Ultravisor)调用(call)的指令。超管理程序调用指令用于发起要用于存储安全虚拟机的诊断状态的一个或多个命令。这些命令包括例如发起配置转储命令、转储中央处理单元状态命令、从安全存储转换命令、转储配置存储状态命令、和完成配置转储命令,下面进一步描述它们中的每一个。

[0036] 参考图1描述了用于结合和使用本发明的一个或多个方面的计算环境的一个实施例。作为示例,计算环境基于由纽约Armonk的国际商业机器公司提供的**z/Architecture®**指令集架构。z/Architecture指令集架构的一个实施例在题为“z/Architecture Principles of Operation”的出版物中描述,IBM出版物No.SA22-7832-12,第十三版,2019年9月,其通过引用整体并入本文。然而,z/Architecture指令集架构仅是一个示例架构;国际商业机器公司和/或其他实体的其他架构和/或其他类型的计算环境可以包括和/或使用本发明的一个或多个方面。z/Architecture和IBM是国际商业机器公司在至少一个司法管辖区的商标或注册商标。

[0037] 参考图1,在一个示例中,计算环境100包括中央处理器复合体(CPC)102。中央处理器复合体102例如是IBM**Z®**服务器(或由国际商业机器公司或其他实体提供的其他服务器或机器),并且包括多个组件,例如耦合到一个或多个处理器单元(也称为处理器)110和输入/输出(I/O)子系统111的存储器104(也称为系统存储器、主存储器、中央存储、存储)。示

例处理器单元110包括一个或多个通用处理器(也称为中央处理器或中央处理单元(CPU))和/或一个或多个其他处理器。IBM Z是国际商业机器公司在至少一个管辖权内的商标或注册商标。

[0038] I/O子系统111可以是中央处理器复合体的一部分或与其分离。它引导主存储104和耦合到中央处理器复合体的输入/输出控制单元108以及输入/输出(I/O)设备106之间的信息流。

[0039] 可以使用许多类型的I/O设备。一种特定类型是数据存储设备140。数据存储设备140可以存储一个或多个程序142、一个或多个计算机可读程序指令144、和/或数据等。计算机可读程序指令可以被配置为执行本发明的各方面的实施例的功能。

[0040] 中央处理器复合体102可以包括和/或耦合到可移动/不可移动、易失性/非易失性计算机系统存储介质。例如,它可以包括和/或耦合到不可移动的、非易失性磁介质(通常称为“硬盘驱动器”)、用于从可移动的、非易失性磁盘(例如,“软盘”)读取和向其写入的磁盘驱动器、和/或用于从可移动的、非易失性光盘(诸如CD-ROM、DVD-ROM或其它光学介质)读取或向其写入的光盘驱动器。应当理解,其它硬件和/或软件组件可以与中央处理器复合体102结合使用。示例包括但不限于:微码或毫码、设备驱动器、冗余处理单元、外部磁盘驱动器阵列、RAID系统、磁带驱动器和数据档案存储系统等。

[0041] 此外,中央处理器复合体102可以与许多其它通用或专用计算系统环境或配置一起操作。适合与中央处理器复合体102一起使用的公知的计算系统、环境和/或配置的示例包括但不限于个人计算机(PC)系统、服务器计算机系统、瘦客户端、胖客户端、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络PC、小型计算机系统、大型计算机系统、以及包括任何上述系统或设备的分布式云计算环境等。

[0042] 在一个或多个实施例中,中央处理器复合体102提供虚拟化支持,其中存储器104包括例如一个或多个虚拟机112(也称为访客)、管理虚拟机的虚拟机管理器(诸如管理程序114)、可信执行环境115和处理器固件116。管理程序114的一个示例是由纽约Armonk的国际商业机器公司提供的z/VM®管理程序。管理程序有时被称为主机(host)。z/VM是国际商业机器公司在至少一个管辖权内的商标或注册商标。

[0043] 在一个或多个实施例中,可信执行环境115可以至少部分地在被配置成执行例如诸如本文所描述的过程的硬件和/或固件中实现。可信执行环境是利用存储器保护硬件来实施存储器保护的可信固件(称为超管理程序)和/或硬件。访客的所有者可以通过使用嵌入在主机密钥文档中的公共主机密钥来安全地将信息传递(例如使用IBM安全执行)到可信执行环境。为了处理机密信息,可信执行环境使用匹配的私有主机密钥。私有主机密钥是服务器(例如IBM Z®服务器)专用的,并且是硬件保护的。

[0044] 处理器固件116包括例如处理器的微码或毫码。它包括例如在实现更高级的机器代码时使用的硬件级指令和/或数据结构。在一个实施例中,它包括例如通常作为微码或毫码传送的专有代码,其包括可信软件、特定于底层硬件的微码或毫码、并且控制操作系统对系统硬件的访问。

[0045] 中央处理器复合体的虚拟机支持提供了操作大量虚拟机(也称为访客)112的能力,每个虚拟机能够与不同的程序120一起操作并且运行客户操作系统122,诸如Linux®

操作系统。每个虚拟机112能够用作单独的系统。也就是说,每个虚拟机可以被独立地重置,运行客户操作系统,并且利用不同的程序来操作。在虚拟机中运行的操作系统或应用程序看起来可以访问整个且完整的系统,但是实际上,仅有一部分是可用的。尽管z/VM和Linux作为示例提供,但是根据本发明的一个或多个方面,可以使用其他虚拟机管理器和/或操作系统。注册商标**Linux®**是按照来自Linus Torvalds的专有被许可人Linux基金会的分许可人在全球范围内使用的。

[0046] 在一个实施例中,一个或多个虚拟机112是安全虚拟机。安全虚拟机由管理程序(例如,管理程序114)以管理程序不能观察安全虚拟机的状态(例如,存储器、寄存器等)的方式发起。例如,在机密计算的一个实施例中,管理程序可以启动/停止安全虚拟机,并且管理程序知道用于启动安全虚拟机的数据位于何处,但是它不能查看运行的安全虚拟机。用于加载/启动安全虚拟机的数据可以以管理程序不能看到安全机器的方式被加密。安全虚拟机映像的所有者将机密数据置于安全访客元数据中,然后生成安全虚拟机映像以及安全访客元数据。在加载安全虚拟机之后,与安全虚拟机的状态的任何交互由诸如可信执行环境115等可信执行环境来处理。

[0047] 根据本发明的一方面,可存储安全虚拟机的诊断状态(即,可转储安全虚拟机),同时维持虚拟机状态的安全性。在一个示例中,诊断状态在其可由不可信实体(例如,管理程序)读取之前被加密。为了安全地促进安全虚拟机的转储,根据一个或多个方面,使用到硬件和固件的应用编程接口。应用编程接口允许管理程序访问虚拟机状态的加密版本,该加密版本可以被传递到虚拟机的所有者。所有者(例如,排他地)然后可以解密状态并获得未被加密的虚拟机转储以供分析,因为所有者是具有用于加密转储的解密密钥的实例(例如,仅有实例)。例如,用于启动虚拟机的元数据包括机密密钥,在此称为所有者密钥或通信密钥,其被保护以使得例如仅可信固件可获得机密所有者密钥。该密钥例如专门用于解密经加密的诊断数据。

[0048] 作为一个例子,应用编程接口被分成多个Ultravisor调用,用于多个命令,包括例如发起配置转储命令、转储中央处理单元状态命令、从安全存储转换命令、转储配置存储状态命令和完成配置转储命令。例如,在执行Ultravisor调用指令时指定每个命令,在一个实施例中,该指令包括指定超管理程序调用操作和多个操作数的操作码。作为示例,当指令的第三操作数(例如,直接(immediate)字段)指定零时,指定正常命令,并且指令的第二操作数(例如寄存器)指向存储器中指定要由超管理程序(或其它可信实体)执行的命令的超管理程序控制块。

[0049] 将参照图2-6描述用于存储可由超管理程序调用指令指定的诊断状态的示例命令和控制块。例如,根据本发明的一个或多个方面,图2描绘了采用命令的处理流程,并且图3-6描绘了由命令使用的各种控制块/信息。

[0050] 首先参考图2,发起配置转储命令(也称为发起存储诊断请求)被调用200。例如,超管理程序调用指令由例如管理程序(例如,管理程序114)发出,它指定指向控制块的指针,该控制块包括要由例如可信实体(例如超管理程序)执行的发起配置转储命令。参考图3描述了这种控制块的示例。

[0051] 在一个示例中,发起配置转储超管理程序控制块300包括例如以下字段:

[0052] 长度302:该字段(例如,字节0-1)包括例如无符号二进制整数(例如,16位),其值

以字节为单位指定控制块(也称为参数块)的长度。长度用于指定选择值(例如,40十六进制);否则,应用选择响应代码(例如,0005十六进制)。

[0053] 命令代码304:该字段(例如,字节2-3)包括无符号二进制整数(例如,16位),其值指定用于发起配置转储超管理程序调用命令的命令代码。

[0054] 响应代码306:该字段(例如,字节4-5)包括指定响应码的无符号二进制整数(例如,16位)。当操作完成时存储该值。

[0055] 返回原因代码308:该字段(例如,字节6-7)包括返回原因代码。

[0056] 安全配置上下文句柄310:该字段(例如,字节24-31)包括标识要初始化转储过程的安全配置(例如,虚拟机)的值(例如,64位值)。

[0057] 如果存在特殊条件,则将除了选择代码之外的响应代码(例如,十六进制0001)存储在超管理程序调用控制块中。用于发起配置转储超管理程序调用的特殊条件包括,例如:

[0058] 0003十六进制:在没有发出成功执行的发起超管理程序调用命令的配置中发出发起配置转储超管理程序调用命令。

[0059] 0005十六进制:发出发起配置转储超管理程序调用命令,其长度不等于选择值(例如,40十六进制)。

[0060] 0020十六进制:安全配置上下文句柄不是用于已定义安全配置的有效句柄。

[0061] 0101十六进制:配置未被授权转储。

[0062] 0102十六进制:针对指定的配置,验证未打包的映像Ultravisor调用没有成功完成。

[0063] 0103十六进制:转储已经在进行中以用于配置。

[0064] 发起配置转储超管理程序调用被用于针对指定的安全配置(例如,安全虚拟机)发起转储过程。作为初始化的一部分,导出唯一转储密钥(例如,加密密钥,为了清楚起见,这里称为第一加密密钥)用于转储选择安全配置数据(例如,经加密的处理器状态)。作为示例,命令从保存的客户通信密钥(例如,所有者密钥)和密钥派生种子导出转储密钥。该密钥被保存,并且稍后可以用于加密经由其他命令提供的数据。

[0065] 在一个示例中,以指定配置为目标的验证未打包(unpack)映像Ultravisor调用(用于验证未打包的映像-安全和破译的映像的完整性)将已经成功完成;否则,不执行任何操作,并且存储所选择的响应代码(例如,0101十六进制)。如果对于指定的配置,另一个发起配置转储超管理程序调用已经成功完成,而没有成功完成的完成配置转储超管理程序调用,则不执行任何操作,并且存储所选择的响应代码(例如,0102十六进制)。

[0066] 在一个示例中,如果安全虚拟机仍在设置过程中,则不发起转储过程,因为虚拟机的状态对于所有者是已知的,直到执行第一指令的点。此外,如所指示的,该命令发起转储过程,这使得其它应用编程接口命令能够被管理程序调用。在发起转储过程之后,直到当前过程完成,才针对该安全虚拟机发起第二转储过程。因此,在一个示例中,基于执行发起配置转储命令,确定对于选择的配置(例如,虚拟机)转储(也称为存储诊断状态)是否已经在进行中210。如果配置的转储已经在进行中,则在一个示例中,对于该处理指示错误212。然而,如果对于配置转储还未在进行中,则处理继续,如本文所述。

[0067] 例如,基于发起配置转储,做出关于虚拟机的状态是否要被转储的确定。返回图2,进行关于是否要转储一个或多个中央处理单元的状态的询问220。如果一个或多个中央处

理单元的状态要被转储,则发起转储中央处理单元状态命令(也称为存储诊断处理器状态请求)230。例如,超管理程序调用指令由例如管理程序发出,其指定指向控制块的指针,该控制块包括将由例如可信实体执行的转储中央处理单元状态命令。参考图4A描述了这种调用控制块的示例。

[0068] 在一个示例中,转储中央处理单元状态超管理程序调用控制块400包括例如以下字段:

[0069] 长度402:该字段(例如,字节0-1)包括例如无符号二进制整数(例如,16位),其值以字节为单位指定控制块的长度。长度用于指定选择值(例如,50十六进制);否则,应用选择响应代码(例如0005十六进制)。

[0070] 命令代码404:该字段(例如字节2-3)包括无符号二进制整数(例如16位),其值指定用于转储中央处理单元状态超管理程序调用命令的命令代码。

[0071] 响应代码406:该字段(例如,字节4-5)包括指定响应代码的无符号二进制整数(例如,16位)。当操作完成时存储该值。

[0072] 返回原因代码408:该字段(例如,字节6-7)包括返回原因代码。对于转储中央处理单元状态超管理程序调用命令,该字段例如为零。

[0073] 安全中央处理单元上下文句柄410:该字段(例如,字节24-31)包括标识其状态将被转储的安全中央处理单元的值(例如,64位值)。

[0074] 安全中央处理单元转储区域源412:附加了选择数量(例如12)的零的该字段(例如字节32-39的位0-51)包括安全中央处理单元转储区域的逻辑地址(例如64位逻辑地址)。

[0075] 如果存在特殊条件,则将除了选择代码之外的响应代码(例如,十六进制0001)存储在超管理程序调用控制块中。用于转储中央处理单元状态Ultravisor调用的特殊条件包括,例如:

[0076] 0003十六进制:在没有发出成功执行的初始化超管理程序调用命令的配置中发出转储中央处理单元状态超管理程序调用命令。

[0077] 0005十六进制:转储中央处理单元状态超管理程序调用命令以不等于选择值(例如,50十六进制)的长度发出。

[0078] 0021十六进制:安全中央处理单元上下文句柄不是用于所定义的安全中央处理单元的有效句柄。

[0079] 0101十六进制:在包含指定的安全中央处理单元的安全配置上还没有完成发起配置转储Ultravisor调用。

[0080] 0102十六进制:用于指定中央处理单元的中央处理单元状态已被转储。

[0081] 0103十六进制:当前正在执行指定的安全中央处理单元。

[0082] 0104十六进制:当试图访问安全中央处理单元转储区域时识别出访问异常。

[0083] 参考图4B描述了安全中央处理单元转储区域的格式的一个示例。作为示例,安全中央处理单元转储区域420包括:

[0084] 安全中央处理单元转储区域版本422:该字段(例如,字节0-3)包括无符号二进制整数(例如,32位),其值指定由超管理程序写入的安全中央处理单元转储区域的版本。版本号定义了安全中央处理单元转储区域中的其他字段的布局。

[0085] 安全中央处理单元转储区域长度424:该字段(例如字节4-7)包括无符号二进制整

数(例如32位),其值指定由超管理程序写入安全中央处理单元转储区域的数据的字节数。

[0086] 初始化向量426:该字段(例如字节8-19)包括当执行例如安全中央处理单元转储区域的AES256-GCM(Galois/Counter模式)加密时由超管理程序使用的唯一初始化向量。

[0087] 通用寄存器428:该字段(例如,字节32-159)包括用于指定的安全中央处理单元的选择通用寄存器(例如,通用寄存器0至15)的内容。

[0088] 当前程序状态字430:该字段(例如字节160-175)包括用于指定安全中央处理单元的当前程序状态字的内容。

[0089] 前缀432:该字段(例如,字节184-187)包括用于指定安全中央处理单元的前缀寄存器的选择位(例如,位32至63)。

[0090] 浮点控制寄存器434:该字段(例如,字节188-191)包括用于指定安全中央处理单元的浮点控制寄存器。

[0091] 时刻(TOD)可编程寄存器436:该字段(例如,字节196-199)包括用于指定安全中央处理单元的时刻可编程寄存器。

[0092] 中央处理单元定时器438:该字段(例如,字节200-207)包括用于指定的安全中央处理单元的中央处理单元定时器。

[0093] 时钟比较器440:该字段(例如,字节209-215)包括用于指定安全中央处理单元的时钟比较器的选择位(例如,位0-55)。

[0094] 存取寄存器442:该字段(例如,字节224-287)包括用于指定安全中央处理单元的选择存取寄存器(例如,存取寄存器0至15)的内容。

[0095] 控制寄存器444:该字段(例如字节288-415)包括用于指定安全中央处理单元的选择控制寄存器(例如控制寄存器0到15)的内容。

[0096] 向量寄存器446:该字段(例如,字节416-927)包括用于指定安全中央处理单元的选择向量寄存器(例如,向量寄存器0至31)的内容。

[0097] 保护存储指定寄存器448:该字段(例如,字节1448-1455)包括用于指定安全中央处理单元的保护存储指定寄存器的内容。

[0098] 保护存储部分掩码(mask)寄存器450:该字段(例如,字节1456-1463)包括用于指定安全中央处理单元的保护存储部分掩码寄存器的内容。

[0099] 保护存储事件参数列表地址寄存器452:该字段(例如,字节1464-1471)包括用于指定安全中央处理单元的保护存储事件参数列表地址寄存器的内容。

[0100] 转储标志(flag)454:该字段(例如,字节1536-1537)包括传达关于转储的中央处理单元内容的信息的标志。示例标志(例如,位0)包括未完成(outstanding)的安全指令拦截处理指示符。当设置了该标志时,部分指令结果可以包含在转储的中央处理单元状态中。

[0101] 安全中央处理单元转储区域标签(tag)456:该字段(例如,安全中央处理单元转储区域的最后16字节)包括用于验证该区域的内容的真实性的认证标签。

[0102] 在一个示例中,字段422-426被认证并且字段428-454被加密。

[0103] 转储中央处理单元超管理程序命令可对虚拟机的每个中央处理单元(或其子集)执行,并且它产生中央处理单元的经加密的状态。虚拟机的状态的加密是用例如转储密钥来执行的。经加密的中央处理状态可以包括但不限于通用寄存器、控制寄存器、浮点寄存器、向量寄存器以及定时器、浮点控制寄存器和/或当前指令地址的内容。此外,在一个示例

中,它包括未被加密的区域。在该区域中,作为示例,保存了用于数据加密的初始化向量,以及便于转储数据的稍后解密和解释的长度和版本指示。

[0104] 该命令用于转储指定的安全中央处理单元(或另一处理器单元)的经加密的内容。安全中央处理单元转储区域包括例如纯文本头部(header),该纯文本头部包括版本信息、加密数据的大小、和用于中央处理单元状态的加密的初始化向量。使用例如AES-GCM利用256位转储密钥对中央处理单元状态进行加密。用于经加密的中央处理单元转储区域的认证标签被直接存储在经加密的区域之后。安全中央处理单元转储区域的长度例如小于或等于例如通过查询超管理程序调用命令返回的安全中央处理单元存储长度。

[0105] 在发布转储中央处理单元状态超管理程序调用命令之前,发起配置转储超管理程序调用命令已经成功完成;否则,存储选择响应代码(例如,0101十六进制)。如果在发起配置转储超管理程序调用命令和完成配置转储超管理程序调用命令之间对于指定安全中央处理单元上下文句柄,不止一次地发出转储中央处理单元状态超管理程序调用命令,则存储选择响应代码(例如,0102十六进制)。如果指定的安全中央处理单元当前正在执行,则存储选择响应代码(例如,0103十六进制)。

[0106] 返回图2,在一个示例中,基于发起配置转储200,还确定虚拟机的存储器是否要被转储222。在一个示例中,如果要转储存储器,则在页调出过程期间发生转储。例如,确定正被转储的存储器当前是否被映射到安全配置(例如,安全虚拟机)224。如果正被转储的存储器被映射到安全配置,则在一个示例中,发起从安全存储转换命令226。例如,超管理程序调用指令由例如指定从安全存储转换控制块的管理程序发出,该从安全存储转换控制块指定要由例如超管理程序执行的从安全存储转换命令。参考图4C描述了这种控制块的一个示例。

[0107] 在一个示例中,从安全存储转换超管理程序调用控制块470包括例如以下字段:

[0108] 长度472:该字段(例如,字节0-1)包括例如无符号二进制整数(例如,16位),其值以字节为单位指定控制块的长度。长度用于指定选择值(例如,20十六进制);否则,应用选择响应代码(例如0005十六进制)。

[0109] 命令代码474:该字段(例如,字节2-3)包括无符号二进制整数(例如,16位),其值指定用于从安全存储转换的超管理程序调用命令的命令代码。

[0110] 响应代码476:该字段(例如,字节4-5)包括指定响应代码的无符号二进制整数(例如,16位)。当操作完成时存储该值。

[0111] 返回原因代码478:该字段(例如,字节6-7)包括返回原因代码。当存储例如'0001'十六进制的响应代码时,当修改存储器的指定单元(例如,存储块)的安全属性时,存储例如'0000'十六进制的返回原因代码。如果存储器的指定单元的安全属性已经被设置为期望状态,则存储返回原因代码,例如'0001'。

[0112] 主机绝对地址480:具有附加至右边的选择数量(例如,12个零)位的该字段(例如,字节32到39的位0到51)形成存储器单元(例如,4K字节的存储块)的绝对地址以转换为非安全存储。

[0113] 如果存在特殊条件,则将除了选择代码之外的响应代码(例如,十六进制0001)存储在超管理程序调用控制块中。对于从安全存储转换超管理程序调用的特殊条件包括例如:

[0114] 0003十六进制:在没有发出成功执行的初始化超管理程序调用命令的配置中发出从安全存储转换超管理程序调用命令。

[0115] 0005十六进制:发出具有不等于选择值(例如,20十六进制)的长度的从安全存储转换超管理程序调用命令。

[0116] 0030十六进制:归属(home)地址空间控制元素具有被设置为例如1的R位(例如,位58)。

[0117] 0031十六进制:试图访问配置变量存储区域时发生转换异常。

[0118] 0032十六进制:安全访客机变量存储区域包含转换成区域帧绝对地址或段帧绝对地址的虚拟地址。

[0119] 0103十六进制:主机绝对地址在主机配置中不可用。

[0120] 0104十六进制:主机绝对地址是超管理程序存储。

[0121] 0105十六进制:相应的主机虚拟地址已经从安全存储转换了太多次。

[0122] 作为一个示例,从安全存储转换超管理程序命令被用来转储安全存储器,其中被转储的存储器单元(例如,存储器页)使用例如分页密钥来加密并被存储。从安全存储转换的命令将与安全配置相关联的存储器单元(例如,4K字节的存储块)的安全属性修改为非安全存储。如果指定的存储器单元已经被定义为非安全存储,则操作完成而无需进一步的动作,并且存储选择响应代码(例如,“0001”十六进制)和选择返回原因代码(例如,“0001”十六进制)。如果存储器单元不是定义共享存储,则从存储器单元的内容创建摘要(digest)。在一个示例中,该摘要由可信实体(例如,超管理程序)保存。存储器单元的内容被加密(例如,使用分页密钥),然后使存储器单元不安全。如果存储器单元被定义为共享存储,则在不修改存储器单元的内容的情况下,使存储器单元不安全。

[0123] 如果指定的主机绝对地址由可信实体拥有,则指定的存储器单元不变,并且存储所选择的响应代码(例如,“0104”十六进制)。

[0124] 在从安全存储转换之后,参考图2,处理继续到查询224。如果要转储的存储器当前没有被映射到安全配置,则发起转储配置存储状态命令(也称为存储诊断存储器状态请求)232。例如,由例如管理程序发出超管理程序调用指令,该管理程序指定指向转储配置存储状态控制块的指针,该转储配置存储状态控制块指定将要由例如超管理程序执行的转储配置存储状态命令。参考图5描述了这种控制块的一个示例。

[0125] 在一个示例中,转储配置存储状态超管理程序调用控制块500包括例如以下字段:

[0126] 长度502:该字段(例如,字节0-1)包括例如无符号二进制整数(例如,16位),其值以字节为单位指定控制块的长度。长度用于指定选择值(例如,58十六进制);否则,应用选择响应代码(例如,0005十六进制)。

[0127] 命令代码504:该字段(例如,字节2-3)包括无符号二进制整数(例如,16位),其值指定用于转储配置存储状态超管理程序调用命令的命令代码。

[0128] 响应代码506:该字段(例如,字节4-5)包括指定响应代码的无符号二进制整数(例如,16位)。当操作完成时存储该值。

[0129] 返回原因代码508:该字段(例如,字节6-7)包括返回原因代码。对于转储配置存储状态超管理程序调用命令,该字段例如为零。

[0130] 安全配置上下文句柄510:该字段(例如,字节24-31)包括标识其状态应当被转储

的安全配置的值(例如,64位值)。

[0131] 安全配置存储转储区域源512:附加了选择数量(例如12个)零的该字段(例如,字节32-39的位0-51)包括安全配置存储转储区域的逻辑地址(例如,64位逻辑地址)。

[0132] 安全配置绝对地址514:附加了选择数量(例如,20个)零的该字段(例如字节40-47的位0-43)包括例如256个存储帧的第一帧的安全配置绝对地址(例如64位地址),以存储选择唯一分量(例如调整分量)。

[0133] 如果存在特殊条件,则将除了选择代码之外的响应代码(例如,0001十六进制)存储在超管理程序调用控制块中。用于转储配置存储状态超管理程序调用的特殊条件包括,例如:

[0134] 0003十六进制:在尚未发出成功执行的初始化超管理程序调用命令的配置中发出转储配置存储状态超管理程序调用命令。

[0135] 0005十六进制:转储配置存储状态超管理程序调用命令以不等于选择值(例如,50十六进制)的长度发出。

[0136] 0020十六进制:安全配置上下文句柄不是用于定义的安全配置的有效句柄。

[0137] 0031十六进制:尝试访问配置虚拟存储区域时发生转换异常。

[0138] 0101十六进制:在指定的安全配置上,发起配置转储超管理程序调用还没有完成。

[0139] 0102十六进制:当访问安全配置存储转储区域时识别访问异常。

[0140] 0103十六进制:安全配置绝对地址例如大于安全配置存储长度。

[0141] 当存储特殊选择唯一分量(例如,特殊调整分量)时,选择字节(例如,字节14到15)包括提供关于如何解译对应的存储器单元(例如,4K字节存储块)的信息的标志。示例性的标志包括:

[0142]

位	描述
15	零页 对应的存储器单元(4K 字节存储块)尚未被安全配置存储,并且其内容可以被假定为零(或另一个选择值)。
14	共享页 对应的存储器单元(4K 字节存储块)被定义为共享存储并且不被加密。
13	页映射 对应的存储器单元(4K 字节存储块)具有到安全页的有效映射。

[0143] 转储配置存储状态命令转储针对给定量的访客存储器的每页的选择唯一分量值(例如,调整分量值)和状态标志。

[0144] 在一个示例中,转储配置存储状态超管理程序调用命令将例如256选择唯一分量值(例如,调整分量值)存储到安全配置转储区域,从用于由安全配置绝对地址指定的存储器单元(例如,4K字节存储块)的选择唯一值(例如,调整)开始。指定的配置转储区域的大小

可以从例如查询超管理程序信息超管理程序调用命令中获得。

[0145] 转储配置存储状态超管理程序调用用于转储例如16字节选择唯一分量值(例如,调整分量值),该选择唯一分量值用于导出在加密或解密安全配置存储的存储器单元(例如,4K字节块)的内容时所使用的选择唯一值(例如,调整值)。从对应于存储器单元的值开始,按顺序输出选择唯一分量值,该存储器单元在例如安全配置内的绝对地址零处开始。如果例如选择唯一分量值的字节0-3是例如“FFFFFFFF”十六进制,则存储器单元没有指定的选择唯一值,并且例如选择唯一分量值的字节14-15包含提供关于应当如何解释相应的存储器单元的更多信息的标志。如果选择唯一分量值是任何其它值,则从例如完成配置转储超管理程序调用中获得的选择唯一分量值和解密的选择唯一值随机数(例如,调整随机数)的OR将被用作用于AES-XTS操作的选择唯一值。

[0146] 返回图2,并且特别地,查询220、222,如果没有更多的中央处理单元要转储或者如果没有更多的存储器要转储,则进行240完成配置转储调用(也称为完成请求)。例如,超管理程序调用指令由例如指定完成配置转储控制块的管理程序发出,该控制块指定要由超管理程序执行的完成配置转储命令。参考图6描述了这种控制块的一个示例。

[0147] 在一个示例中,完成配置转储超管理程序调用控制块600包括例如以下字段:

[0148] 长度602:该字段(例如,字节0-1)包括例如无符号二进制整数(例如,16位),其值以字节为单位指定控制块的长度。长度用于指定选择值(例如,64+N字节的值);否则,应用选择响应代码(例如,0005十六进制)。值N可以从例如由查询超管理程序信息超管理程序调用命令返回的配置最终化转储长度中获得。

[0149] 命令代码604:该字段(例如字节2-3)包括无符号二进制整数(例如16位),其值指定用于完成配置状态转储超管理程序调用命令的命令代码。

[0150] 响应代码606:该字段(例如,字节4-5)包括指定响应代码的无符号二进制整数(例如,16位)。当操作完成时存储该值。

[0151] 返回原因代码608:该字段(例如,字节6-7)包括返回原因代码。对于完成配置转储超管理程序调用命令,该字段例如为零。

[0152] 安全配置上下文句柄609:该字段(例如,字节24-31)包括标识其转储将被完成的安全配置的值(例如,64位值)。

[0153] 密钥派生(derivation)种子(seed)610:该字段(例如,字节64-127)包括用于导出转储密钥的种子以及该控制块中的数据,其中转储密钥用于加密中央处理单元状态。

[0154] 初始化向量612:该字段(例如,字节128-143)包括在加密由该超管理程序调用存储的数据时所使用的初始化向量。

[0155] 调整随机数(又名,选择唯一随机数)614:该字段(例如,字节144-159)包括用于选择唯一值(例如,调整值)的随机数值。该值将与每个非专用选择唯一分量(例如,调整分量)进行“或”运算,以创建用于加密存储器单元(例如,4K字节存储块)的选择唯一值。

[0156] 存储加密密钥1(616):该字段(例如,字节160-191)包括用于加密选择唯一值(例如,调整值)的第一AES-256XTS密钥,该选择唯一值随后被用于解密转储的存储器单元(例如,4K字节的存储块)。

[0157] 存储加密密钥2(618):该字段(例如,字节192-223)包括与经加密的选择唯一值(例如,调整值)一起使用来对存储器单元(例如,4K字节的存储块)进行解密的第二AES-

256XTS密钥。在一个示例中,与存储加密密钥2组合的存储加密密钥1是分页密钥。

[0158] 认证标签620:该字段(例如,字节256-271)包括AES-GCM认证标签,该AES-GCM认证标签是通过使用认证值(例如,字节64-143)作为附加认证数据、然后根据加密字段(例如,字节144-255)计算标签的剩余部分而得到的。

[0159] 如果存在特殊条件,则将除了选择代码之外的响应代码(例如,十六进制0001)存储在超管理程序调用控制块中。用于完成配置转储超管理程序调用的特殊条件包括例如:

[0160] 0003十六进制:在没有发出成功执行的初始化超管理程序调用命令的配置中,发出完成配置转储超管理程序调用命令。

[0161] 0005十六进制:发出具有不等于选择值(例如,130十六进制)的长度的完成配置转储超管理程序调用命令。

[0162] 0020十六进制:安全配置上下文句柄不是用于定义的安全配置的有效句柄。

[0163] 0101十六进制:在指定的安全配置上,发起配置转储超管理程序调用还没有完成。

[0164] 使用完成配置转储超管理程序调用来完成用于指定安全配置的转储处理。该调用返回由客户用来解密转储并检查其完整性的数据。它还完成转储过程,因此允许经由发起配置转储调用发起新的转储过程。它包括例如用于创建转储密钥的密钥派生种子,从而虚拟机的所有者可以自己计算转储密钥。此外,它包括用于加密返回数据的加密部分的初始化向量和应当用于验证经认证和加密的数据的内容的认证标签。加密部分包括例如所选择的唯一值随机数,其将被"或"运算到来自转储存储器状态调用的每个选择唯一值中,以及包括用于加密那些选择唯一值的AES XTS(高级加密标准XEX可调整的块密码,具有密文窃取)密钥。

[0165] 如本文所述,可以转储安全虚拟机,同时通过在转储由不可信实体可读之前加密转储来保持转储的虚拟机的状态的安全性。为了安全地促进安全虚拟机的转储,采用转储应用程序编程接口。接口使用多个调用,并且每个调用指向控制块,这里描述了其示例。在一个或多个实施例中,本文描述的每个控制块/区域可以包括附加的、更少的和/或其他字段。此外,每个字段可以在控制块/区域内的不同位置和/或具有不同的大小或数据类型。此外,控制块/区域可以包括一个或多个保留字段。许多变化是可能的。

[0166] 在一个或多个方面,可以使用多种技术来转储虚拟机的存储器。例如,一种技术包括用转储密钥直接加密存储器。利用被称为中央处理单元存储器加密的这种技术,安全虚拟机的页面被加密。安全虚拟机的密钥和管理程序的密钥不同,因此如果管理程序读取或写入结果,则它是随机数据。为了最佳安全性,加密密钥从不离开中央处理单元的存储器控制器,并且因此它不能用于转储安全虚拟机的存储器,因为只有虚拟机当前运行的中央处理单元可以解密页面。另外,当安全虚拟机停止时清除密钥。

[0167] 该保护机制留下了一种转储安全虚拟机存储器的技术,因为用于访问安全虚拟机存储器的密钥通常不能被输出:用可以被输出以替换不可输出的访问密钥的特殊转储密钥对其进行加密。如果页面已经被交换到磁盘(disk),则它将被带回到访客的存储器中以便对其进行解密和重新加密。这产生了额外的存储器压力,并且花费处理器周期来加密/解密。

[0168] 根据一个或多个方面,用于转储安全虚拟机的存储器的另一种技术被称为存储器保护,其拒绝访问除了页面所属的安全虚拟机和可信固件(例如,超管理程序)之外的安全

虚拟机的页面,直到在管理程序向固件请求之后它被加密。在加密之后,页面不再对安全虚拟机可用,但是可以由管理程序写入磁盘。类似地,对固件的请求用于解密、完整性检查和将加密页面映射回到安全虚拟机中,使得其可再次访问安全虚拟机。

[0169] 这种保护机制能够使用在加密页面以交换用于转储时所使用的相同密钥。这意味着一旦页面被加密,如果访客想再次访问它们,则只需要将它们带回访客。尚未被加密的页面将被加密,但是已经加密的页面,无论它们是否仍然在存储器中或已经在磁盘上,都可以直接被写入到转储。如果页面已经被分页到磁盘,则这导致转储所需的CPU周期的显著减少。加密专用数据将被输出,以便在稍后检查转储时解密页面。此类数据例如可包含针对存储器的每一页的选择唯一值(例如,调整值)。

[0170] 与由虚拟机内的故障内核所写入的诊断状态的存储相比,如本文在一个或多个方面中所述的诊断状态的存储由管理程序在虚拟机外部生成。它由虚拟机的所有者触发,或者在管理程序已经确定虚拟机已经发生故障并且没有正常执行代码时自动触发。

[0171] 本发明的一个或多个方面不可分地依赖于计算机技术,并便于计算机内的处理,从而提高其性能。通过以较不复杂的方式安全地存储虚拟机(例如,安全虚拟机)的诊断状态来促进处理,使用较少的处理周期并提高性能,同时维持安全性。

[0172] 参考图7A-7C描述了与本发明的一个或多个方面相关的便于计算环境内的处理的一个实施例的进一步细节。

[0173] 参考图7A,在一个实施例中,获得存储虚拟机的诊断状态的至少一个请求700。基于获得至少一个请求,执行虚拟机的诊断状态的存储,以提供虚拟机的存储的诊断状态702。执行存储包括例如加密虚拟机的未被加密且正在被存储的诊断状态,以防止在加密虚拟机的未被加密且正在被存储的诊断状态之前由不可信实体读取虚拟机的诊断状态704。

[0174] 可以存储虚拟机(例如,安全虚拟机)的诊断状态,同时保持正在被存储用于诊断目的虚拟机的状态的安全性。

[0175] 作为示例,虚拟机的所存储的诊断状态包括虚拟机的存储器内容706和/或虚拟机的所存储的诊断状态包括虚拟机的一个或多个处理器寄存器的内容708。

[0176] 在一个示例中,获得用于发起虚拟机的诊断状态的存储的发起存储诊断状态请求710。发起存储诊断状态请求被用于获得第一加密密钥,该第一加密密钥将用于加密虚拟机的未被加密且正在被存储的诊断状态的至少一部分712。

[0177] 在一个示例中,参照图7B,获得至少一个请求包括获得存储诊断处理器状态请求720。基于获得存储诊断处理器状态请求,执行诊断状态的存储包括例如使用第一加密密钥对虚拟机的至少一个处理器的至少选择内容进行加密以提供经加密的处理器内容722,以及存储经加密的处理器内容724。

[0178] 在一个示例中,获得至少一个请求包括获得从安全存储器转换请求726。基于获得从安全存储器转换请求,执行诊断状态的存储包括例如使用第二加密密钥对虚拟机的未被加密的至少选择存储器内容进行加密以提供经加密的存储器内容730,并且存储经加密的存储器内容732。

[0179] 作为示例,基于获得从安全存储器转换请求来执行诊断状态的存储包括例如确定其内容将被存储的存储器单元是否被加密736,以及基于确定存储器单元未被加密来使用第二加密密钥对存储器单元进行加密,其中被加密的存储器单元不被重新加密738。

[0180] 通过加密未被加密的内容(而不是重新加密的状态),减少了处理周期和复杂度,提高了系统性能。

[0181] 在一个示例中,参考图7C,所存储的诊断状态包括经加密的存储器内容750。此外,在一个示例中,获得存储诊断存储器状态请求752,并且基于获得存储诊断存储器状态请求,存储要用于解密经加密的存储器内容的元数据754。

[0182] 作为示例,元数据包括用于创建用于对经加密的存储器内容进行解密一个或多个选择值的一个或多个选择分量值756。

[0183] 在一个示例中,获得完成诊断状态的存储的完成请求760,并且基于获得完成请求,提供要用于解密虚拟机的经加密的存储的诊断状态的数据762。

[0184] 作为一个示例,数据包括在对经加密的存储器内容进行解密时所使用的第二加密密钥和将被用于创建将要在加密时所使用的一个或多个选择值的随机数值770。此外,在一个示例中,数据的至少一部分被加密772。

[0185] 其它变化和实施例是可能的。

[0186] 本发明的各方面可由许多类型的计算环境使用。参考图8A描述了用于结合和使用本发明的一个或多个方面的计算环境的另一实施例。在该示例中,计算环境36包括经由例如一个或多个总线40和/或其它连接彼此耦合的例如本机中央处理单元(CPU)37、存储器38、以及一个或多个输入/输出设备和/或接口39。作为示例,计算环境36可包括纽约Armonk的国际商业机器公司提供的**PowerPC®**处理器;加利福尼亚州Palo Alto的惠普公司提供的具有**Intel® Itanium®**II处理器的HP Superdome;和/或基于由国际商业机器公司、惠普、英特尔公司、甲骨文和/或其它公司提供的架构的其它机器。PowerPC是国际商业机器公司在至少一个管辖区内的商标或注册商标。Intel和Itanium是英特尔公司或其子公司在美国和其它国家的商标或注册商标。

[0187] 本机中央处理单元37包括一个或多个本机寄存器41,诸如在环境内的处理期间使用的一个或多个通用寄存器和/或一个或多个专用寄存器。这些寄存器包括表示在任何特定时间点的环境状态的信息。

[0188] 此外,本机中央处理单元37执行存储在存储器38中的指令和代码。在一个特定示例中,中央处理单元执行存储在存储器38中的仿真器代码42。该代码使得在一个架构中配置的计算环境能够仿真另一架构。例如,仿真器代码42允许基于z/Architecture指令集架构之外的架构的机器(诸如PowerPC处理器、HP Superdome服务器或其它)来仿真z/Architecture指令集架构,并且执行基于z/Architecture指令集架构开发的软件和指令。

[0189] 参考图8B描述了与仿真器代码42有关的进一步细节。存储在存储器38中的访客指令43包括软件指令(例如,与机器指令相关),其被开发为在不同于本机CPU37的架构中执行。例如,访客指令43可以被设计为基于z/Architecture指令集架构在处理器上执行,但是替代地,在本机CPU37上被仿真,其可以是例如Intel Itanium II处理器。在一个示例中,仿真器代码42包括指令获取例程44,以从存储器38获得一个或多个访客指令43,并且可选地为所获得的指令提供本地缓冲。它还包括指令转译例程45,以确定所获得的访客指令的类型,并且将访客指令转译成一个或多个对应的本机指令46。该转译包括例如标识要由访客指令执行的功能以及选择(一个或多个)本机指令来执行该功能。

[0190] 此外,仿真器代码42包括仿真控制例程47以使得执行本机指令。仿真控制例程47可以使本机CPU37执行仿真一个或多个先前获得的访客指令的本机指令的例程,并且在该执行结束时,将控制返回到指令获取例程以仿真下一个访客指令或一组访客指令的获得。本机指令46的执行可包括将数据从存储器38加载到寄存器中;将数据从寄存器存储回存储器;或者执行由转换例程确定的某种类型的算术或逻辑操作。

[0191] 例如,每个例程以软件实现,该软件存储在存储器中并由本机中央处理单元37执行。在其它示例中,例程或操作中的一个或多个以固件、硬件、软件或其某种组合实现。被仿真的处理器的寄存器可使用本机CPU的寄存器41或通过使用存储器38中的位置来仿真,在实施例中,访客指令43、本机指令46和仿真器代码42可驻留在相同的存储器中,或者可分配在不同的存储器设备之间。

[0192] 根据本发明的一个或多个方面,可被仿真的指令、命令或者调用包括本文描述的超管理程序调用。此外,根据本发明的一个或多个方面,可以仿真本发明的其他指令、命令、功能、操作、调用和/或一个或多个方面。

[0193] 上述计算环境仅是可以使用的计算环境的示例。可以使用其它环境,包括但不限于,非分区环境、分区环境、云环境和/或仿真环境;实施例不限于任何一种环境。尽管在此描述了计算环境的各种示例,但是本发明的一个或多个方面可以与许多类型的环境一起使用。这里提供的计算环境仅仅是示例。

[0194] 每个计算环境能够被配置为包括本发明的一个或多个方面。

[0195] 一个或多个方面可以涉及云计算。

[0196] 可理解,尽管本公开包括关于云计算的详细描述,但是本文所陈述的教导的实现不限于云计算环境。相反,本发明的实施例能够结合现在已知或以后开发的任何其它类型的计算环境来实现。

[0197] 云计算是一种服务递送模型,用于实现对可配置计算资源(例如,网络、网络带宽、服务器、处理、存储器、存储、应用、虚拟机和服务)的共享池的方便的按需网络访问,该可配置计算资源可以以最小的管理努力或与服务的提供者的交互来快速供应和释放。该云模型可以包括至少五个特性、至少三个服务模型和至少四个部署模型。

[0198] 特征如下:

[0199] 按需自助:云消费者可以单方面地自动地根据需要提供计算能力,诸如服务器时间和网络存储,而不需要与服务的提供者进行人工交互。

[0200] 广域网接入:能力在网络上可用,并且通过促进由异构的薄或厚客户端平台(例如,移动电话、膝上型计算机和PDA)使用的标准机制来访问。

[0201] 资源池化:供应商的计算资源被集中以使用多租户模型来服务多个消费者,其中不同的物理和虚拟资源根据需求被动态地分配和重新分配。存在位置无关的意义,因为消费者通常不控制或不知道所提供的资源的确切位置,但是能够在较高抽象级别(例如国家、州或数据中心)指定位置。

[0202] 快速弹性:在一些情况下,可以快速且弹性地提供快速向外扩展的能力和快速向内扩展的能力。对于消费者,可用于提供的能力通常看起来不受限制,并且可以在任何时间以任何数量购买。

[0203] 测量服务:云系统通过利用在适合于服务类型(例如,存储、处理、带宽和活动用户

账户)的某一抽象级别的计量能力来自动地控制和优化资源使用。可以监视、控制和报告资源使用,从而为所利用服务的提供者和消费者两者提供透明性。

[0204] 服务模型如下:

[0205] 软件即服务(SaaS):提供给消费者的能力是使用在云基础设施上运行的提供者的应用。应用可通过诸如web浏览器(例如,基于web的电子邮件)等瘦客户机界面从各种客户机设备访问。消费者不管理或控制包括网络、服务器、操作系统、存储、或甚至个别应用能力的底层云基础结构,可能的例外是有限的用户专用应用配置设置。

[0206] 平台即服务(PaaS):提供给消费者的能力是将消费者创建或获取的应用部署到云基础设施上,该消费者创建或获取的应用是使用由提供商支持的编程语言和工具创建的。消费者不管理或控制包括网络、服务器、操作系统或存储的底层云基础设施,但具有对部署的应用和可能的应用托管环境配置的控制。

[0207] 基础设施即服务(IaaS):提供给消费者的能力是提供处理、存储、网络和消费者能够部署和运行任意软件的其它基本计算资源,该软件可包括操作系统和应用。消费者不管理或控制底层云基础设施,但具有对操作系统、存储、部署的应用的控制,以及可能对选择的联网组件(例如,主机防火墙)的有限控制。

[0208] 部署模型如下:

[0209] 私有云:云基础设施仅为组织操作。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0210] 社区云:云基础设施由若干组织共享,并且支持具有共享关注(例如,任务、安全要求、策略和合规性考虑)的特定社区。它可以由组织或第三方管理,并且可以存在于场所内或场所外。

[0211] 公有云:云基础设施可用于一般公众或大型工业群体,并且由销售云服务的组织拥有。

[0212] 混合云:云基础设施是两个或更多云(私有、共同体或公共)的组合,所述云保持唯一实体,但是通过使数据和应用能够移植的标准化或私有技术(例如,用于云之间的负载平衡的云突发)绑定在一起。

[0213] 云计算环境是面向服务的,其焦点在于无状态、低耦合、模块性和语义互操作性。在云计算的核心是包括互连节点的网络的基础设施。

[0214] 现在参考图9,描述了说明性的云计算环境50。如图所示,云计算环境50包括云消费者使用的本地计算设备可以与其通信的一个或多个云计算节点52,本地计算设备例如个人数字助理(PDA)或蜂窝电话54A、台式计算机54B、膝上型计算机54C和/或汽车计算机系统54N。节点52可以彼此通信。它们可以被物理地或虚拟地分组(未示出)在一个或多个网络中,诸如如上文描述的私有云、社区云、公共云或混合云或其组合。这允许云计算环境50提供基础设施、平台和/或软件作为服务,云消费者不需要为其维护本地计算设备上的资源。可理解,图9中所示的计算设备54A-N的类型仅旨在说明,并且计算节点52和云计算环境50可以在任何类型的网络和/或网络可寻址连接上(例如,使用web浏览器)与任何类型的计算机化设备通信。

[0215] 现在参考图10,示出了由云计算环境50(图9)提供的一组功能抽象层。可预先理解,图10中所示的组件、层和功能仅旨在说明,并且本发明的实施例不限于此。如所描绘的,

提供了以下层和相应的功能：

[0216] 硬件和软件层60包括硬件和软件组件。硬件组件的示例包括：主机61；基于RISC(精简指令集计算机)架构的服务器62；服务器63；刀片服务器64；存储装置65；以及网络和网络组件66。在一些实施例中，软件组件包括网络应用服务器软件67和数据库软件68。

[0217] 虚拟化层70提供抽象层，从该抽象层可以提供虚拟实体的以下示例：虚拟服务器71；虚拟存储器72；虚拟网络73，包括虚拟专用网络；虚拟应用和操作系统74；以及虚拟客户机75。

[0218] 在一个示例中，管理层80可以提供以下描述的功能。资源供应81提供用于在云计算环境内执行任务的计算资源和其它资源的动态采购。计量和定价82提供了在云计算环境中利用资源时的成本跟踪，以及用于消耗这些资源的计帐单或开发票。在一个示例中，这些资源可包括应用软件许可证。安全性为云消费者和任务提供身份验证，以及为数据和其它资源提供保护。用户门户83为消费者和系统管理员提供对云计算环境的访问。服务级别管理84提供云计算资源分配和管理，使得满足所需的服务级别。服务水平协议(SLA)规划和履行85提供对云计算资源的预安排和采购，其中根据SLA预期未来需求。

[0219] 工作负载层90提供了可以利用云计算环境的功能的示例。可从该层提供的工作负载和功能的示例包括：绘图和导航91；软件开发和生命周期管理92；虚拟教室教育传送93；数据分析处理94；交易处理95；以及安全虚拟机转储处理96。

[0220] 本发明的各方面可以是处于任何可能的技术细节集成水平的系统、方法和/或计算机程序产品。计算机程序产品可以包括其上具有计算机可读程序指令的计算机可读存储介质(或多个介质)，该计算机可读程序指令用于使处理器执行本发明的各方面。

[0221] 计算机可读存储介质可以是能够保留和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质可以是例如但不限于电子存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或前述的任何合适的组合。计算机可读存储介质的更具体示例的非穷举列表包括以下：便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式光盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、诸如上面记录有指令的打孔卡或凹槽中的凸起结构的机械编码装置，以及上述的任何适当组合。如本文所使用的计算机可读存储介质不应被解释为暂时性信号本身，诸如无线电波或其它自由传播的电磁波、通过波导或其它传输介质传播的电磁波(例如，通过光纤线缆的光脉冲)、或通过导线传输的电信号。

[0222] 本文描述的计算机可读程序指令可以从计算机可读存储介质下载到相应的计算/处理设备，或者经由网络(例如因特网、局域网、广域网和/或无线网络)下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光传输光纤、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或网络接口从网络接收计算机可读程序指令，并转发计算机可读程序指令以存储在相应计算/处理设备内的计算机可读存储介质中。

[0223] 用于执行本发明的操作的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、集成电路的配置数据，或者以一种或多种编程语言(包括面向对象的编程语言，例如Smalltalk、C++等)和过程

编程语言(例如“C”编程语言或类似的编程语言)的任意组合编写的源代码或目标代码。计算机可读程序指令可以完全在用户的计算机上执行,部分在用户的计算机上执行,作为独立的软件包执行,部分在用户的计算机上并且部分在远程计算机上执行,或者完全在远程计算机或服务器上执行。在后一种情况下,远程计算机可以通过任何类型的网络连接到用户的计算机,包括局域网(LAN)或广域网(WAN),或者可以连接到外部计算机(例如,使用因特网服务提供商通过因特网)。在一些实施例中,为了执行本发明的各方面,包括例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)的电子电路可以通过利用计算机可读程序指令的状态信息来执行计算机可读程序指令以使电子电路个性化。

[0224] 在此参考根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明的各方面。将理解,流程图和/或框图的每个框以及流程图和/或框图中的框的组合可以由计算机可读程序指令来实现。

[0225] 这些计算机可读程序指令可被提供给计算机或其它可编程数据处理装置的处理器以产生机器,使得经由计算机或其它可编程数据处理装置的处理器执行的指令创建用于实现流程图和/或框图的一个或多个框中指定的功能/动作的装置。这些计算机可读程序指令还可以存储在计算机可读存储介质中,其可以引导计算机、可编程数据处理装置和/或其它设备以特定方式工作,使得其中存储有指令的计算机可读存储介质包括制品,该制品包括实现流程图和/或框图的一个或多个框中指定的功能/动作的方面的指令。

[0226] 计算机可读程序指令还可以被加载到计算机、其它可编程数据处理装置或其它设备上,以使得在计算机、其它可编程装置或其它设备上执行一系列操作步骤,以产生计算机实现的过程,使得在计算机、其它可编程装置或其它设备上执行的指令实现流程图和/或框图的一个或多个框中指定的功能/动作。

[0227] 附图中的流程图和框图示出了根据本发明的各种实施例的系统、方法和计算机程序产品的可能实现的架构、功能和操作。在这点上,流程图或框图中的每个框可以表示指令的模块、段或部分,其包括用于实现指定的逻辑功能的一个或多个可执行指令。在一些替代实施方案中,框中所注明的功能可不按图中所注明的顺序发生。例如,连续示出的两个框实际上可以作为一个步骤来实现,同时、基本同时、以部分或全部时间重叠的方式执行,或者这些框有时可以以相反的顺序执行,这取决于所涉及的功能。还将注意,框图和/或流程图图示的每个框以及框图和/或流程图图示中的框的组合可以由执行指定功能或动作或执行专用硬件和计算机指令的组合的专用的基于硬件的系统来实现。

[0228] 除了上述之外,可以由提供客户环境管理的服务提供商来提供、部署、管理、服务等一个或多个方面。例如,服务提供商可以创建、维护、支持等执行一个或多个客户的一个或多个方面的计算机代码和/或计算机基础设施。作为回报,服务提供商可以例如在订阅和/或费用协议下从客户接收支付。另外或替代地,服务提供商可以从向一个或多个第三方销售广告内容接收支付。

[0229] 在一个方面,可以部署应用以执行一个或多个实施例。作为一个示例,应用的部署包括提供可操作以执行一个或多个实施例的计算机基础结构。

[0230] 作为另一方面,可以部署计算基础设施,包括将计算机可读代码集成到计算系统中,其中与计算系统结合的代码能够执行一个或多个实施例。

[0231] 作为又一方面,可以提供一种用于集成计算基础设施的过程,包括将计算机可读

代码集成到计算机系统中。计算机系统包括计算机可读介质,其中计算机介质包括一个或多个实施例。与计算机系统结合的代码能够执行一个或多个实施例。

[0232] 尽管上文描述了各种实施例,但这些仅是实例。例如,其它架构的计算环境可用于结合和/或使用一个或多个方面。此外,可以使用不同的指令、命令、功能、调用和/或操作。许多变化是可能的。

[0233] 本文描述了各个方面。此外,在不背离本发明的各方面的精神的情况下,许多变化是可能的。应当注意,除非另外不一致,否则本文所述的每个方面或特征及其变型可与任何其它方面或特征组合。

[0234] 此外,其它类型的计算环境也可以受益并被使用。作为示例,适于存储和/或执行程序代码的数据处理系统是可用的,其包括通过系统总线直接或间接耦合到存储器元件的至少两个处理器。存储器元件包括例如在程序代码的实际执行期间采用的本地存储器、大容量存储装置和缓冲存储器,其提供至少一些程序代码的临时存储以减少在执行期间必须从大容量存储装置取得代码的次数。

[0235] 输入/输出或I/O设备(包括但不限于键盘、显示器、定点设备、DASD、磁带、CD、DVD、拇指驱动器和其它存储介质等)可以直接或通过中间I/O控制器耦合到系统。网络适配器也可耦合到系统,以使数据处理系统能够通过中间专用或公共网络耦合到其它数据处理系统或远程打印机或存储设备。调制解调器、电缆调制解调器和以太网卡只是几种可用的网络适配器类型。

[0236] 本文所用的术语仅是为了描述特定实施例的目的,而不是旨在进行限制。如本文所用,单数形式“一”、“一个”和“该”旨在也包括复数形式,除非上下文另有明确指示。还将理解,在本说明书中使用术语“包括”和/或“包含”时,指定所描述的特征、整数、步骤、操作、元件和/或组件的存在,但不排除一个或多个其它特征、整数、步骤、操作、元件、组件和/或其群组的存在或添加。

[0237] 如果存在,下面的权利要求中的所有装置或步骤加功能元件的对应结构、材料、动作和等同物旨在包括用于与具体要求保护的其它要求保护的元件组合执行功能的任何结构、材料或动作。出于说明和描述的目的呈现了对一个或多个实施例的描述,但是该描述不旨在是穷尽的或者限于所公开的形式。许多修改和变化对于本领域普通技术人员来说是显而易见的。选择和描述实施例是为了最好地解释各个方面和实际应用,并且使本领域的其它普通技术人员能够理解具有适合于所设想的特定用途的各种修改的各种实施例。

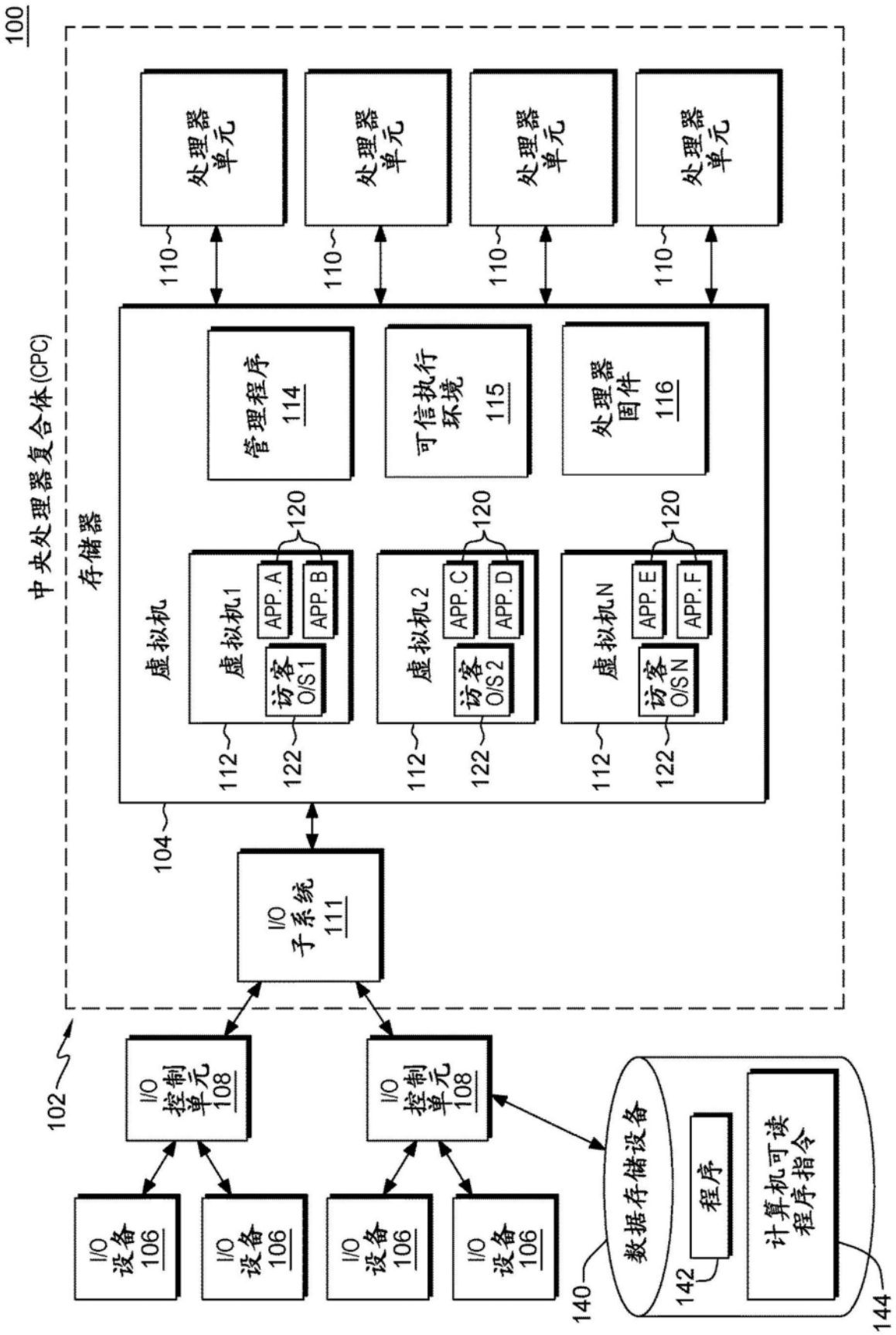

100
中央处理器复合体(CPC)
存储器
处理器单元
处理器单元
处理器单元
处理器单元
110
110
110
110
虚拟机
管理程序 114
可信执行环境 115
处理器固件 116
虚拟机1
APP.A
APP.B
访客O/S1
虚拟机2
APP.C
APP.D
访客O/S2
虚拟机N
APP.E
APP.F
访客O/S N
120
120
120
112
122
112
122
112
122
104
I/O子系统 111
102
I/O控制单元 108
I/O控制单元 108
I/O设备 106
I/O设备 106
I/O设备 106
I/O设备 106
数据存储设备
程序
计算机可读程序指令
140
142
144

图1

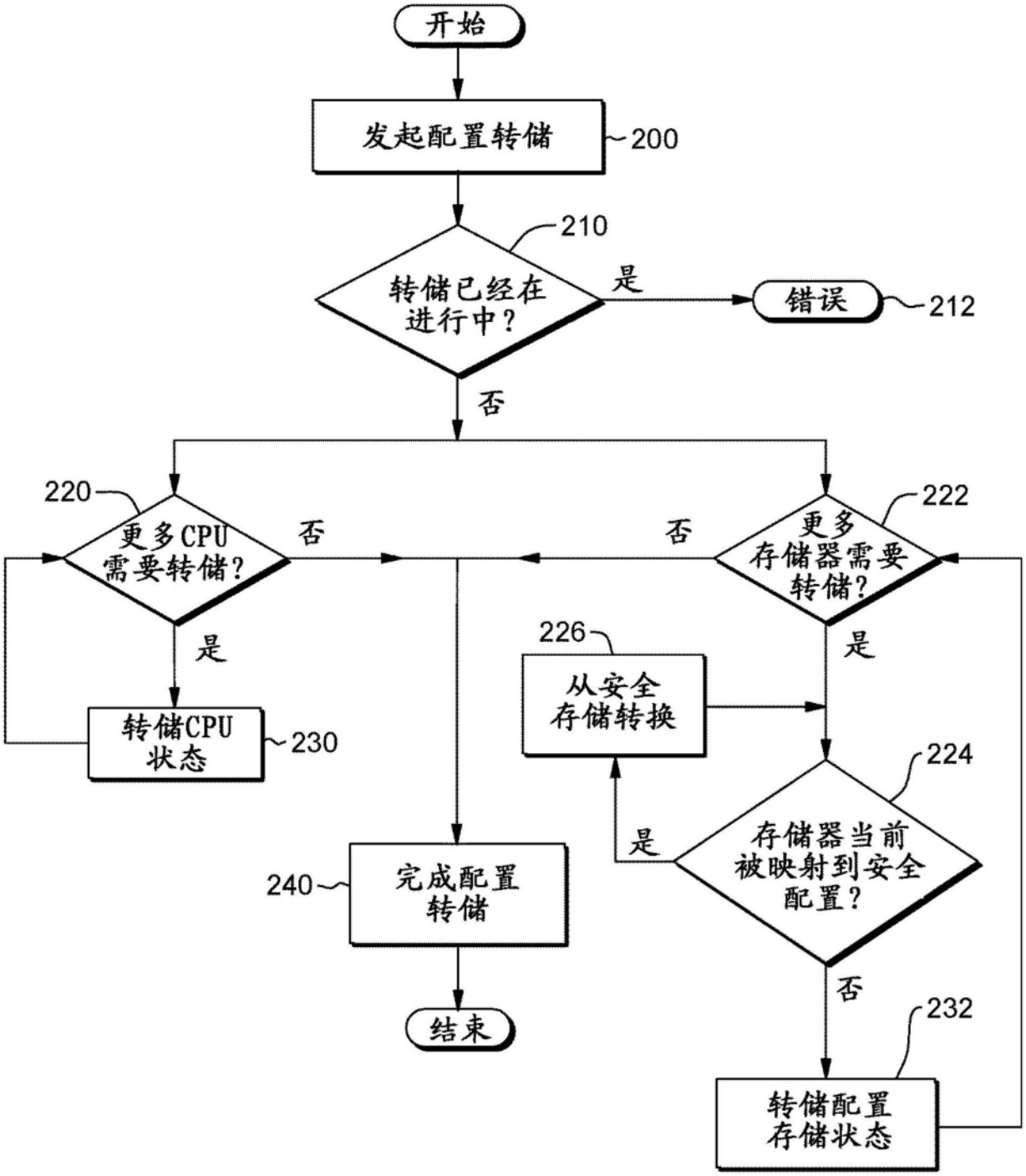

开始
发起配置转储
200
210
转储已经在进行中？
是
错误
212
否
220
更多CPU需要转储？
否
否
222
更多存储器需要转储？
是
是
转储CPU状态
230
226
从安全存储转换
224
存储器当前被映射到安全配置？
是
否
240
完成配置转储
结束
232
转储配置存储状态

图2


300
发起配置转储控制块
长度
命令代码
响应代码
返回原因代码
302
304
306
308
安全配置上下文句柄
310

图3

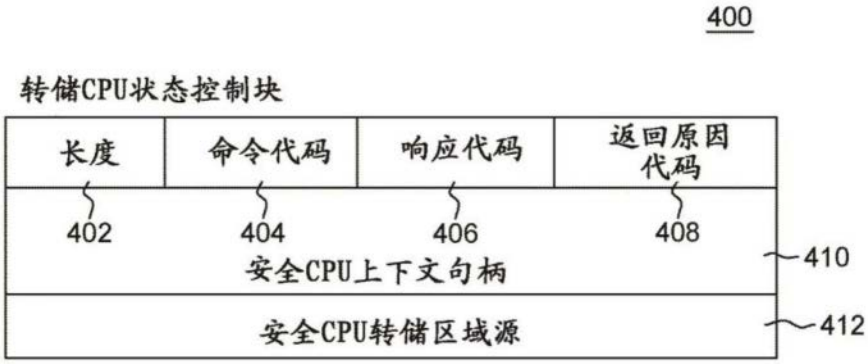

400
转储CPU状态控制块
长度
命令代码
响应代码
返回原因代码
402
404
406
408
安全CPU上下文句柄
410
安全CPU转储区域源
412

图4A

420

安全CPU转储区域

安全CPU转储区域版本 ～422	安全CPU转储区域长度 ～424
初始化向量 ～426	
通用寄存器～428	
当前程序状态字 ～430	
前缀～432	浮点控制寄存器 ～434
时刻(TOD)可编程寄存器 ～436	
CPU定时器 ～438	
时钟比较器 ～440	
存取寄存器～442	
控制寄存器 ～444	
向量寄存器～446	
保护存储指定寄存器 ～448	
保护存储部分掩码寄存器 ～450	
保护存储事件参数列表地址寄存器 ～452	
...	
转储标志 ～454	
安全CPU转储区域标签 ～456	

图4B

470

从安全存储转换控制块

长度	命令代码	响应代码	返回原因代码
472	474	476	478
主机绝对地址 ～480			

图4C


500
转储配置存储状态控制块
长度
命令代码
响应代码
返回原因代码
502
504
506
508
安全配置上下文句柄
510
安全配置存储转储区域源
512
安全配置绝对地址
514

图5

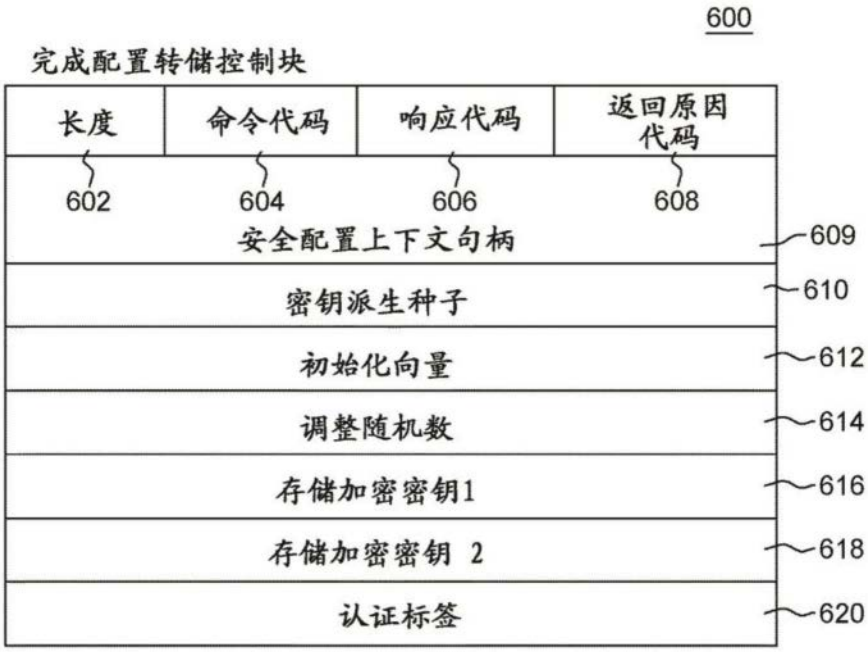

600
完成配置转储控制块
长度
命令代码
响应代码
返回原因代码
602
604
606
608
安全配置上下文句柄
609
密钥派生种子
610
初始化向量
612
调整随机数
614
存储加密密钥1
616
存储加密密钥 2
618
认证标签
620

图6

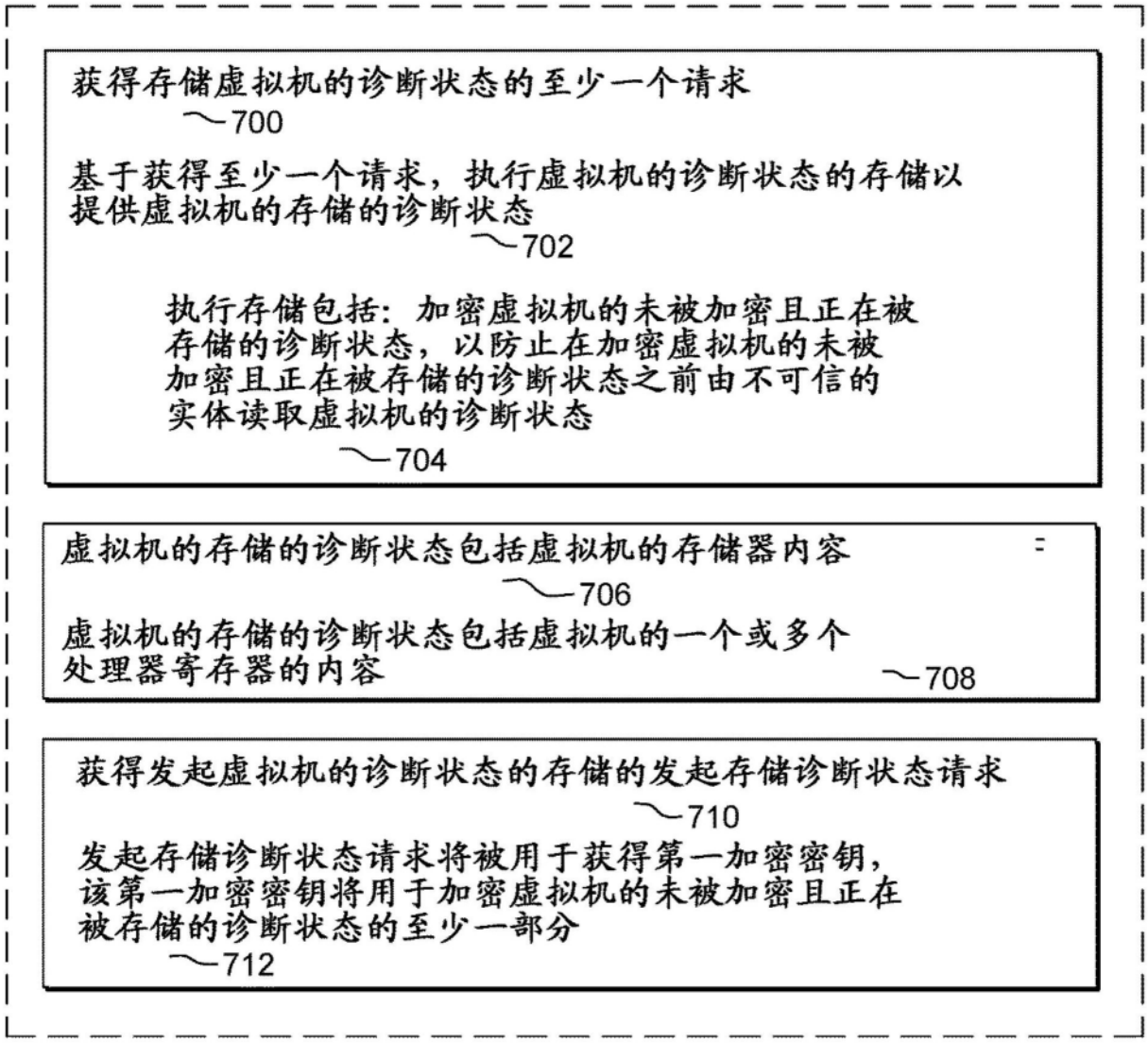

获得存储虚拟机的诊断状态的至少一个请求
700
基于获得至少一个请求，执行虚拟机的诊断状态的存储以提供虚拟机的存储的诊断状态
702
执行存储包括：加密虚拟机的未被加密且正在被存储的诊断状态，以防止在加密虚拟机的未被加密且正在被存储的诊断状态之前由不可信的实体读取虚拟机的诊断状态
704
虚拟机的存储的诊断状态包括虚拟机的存储器内容
706
虚拟机的存储的诊断状态包括虚拟机的一个或多个处理器寄存器的内容
708
获得发起虚拟机的诊断状态的存储的发起存储诊断状态请求
710
发起存储诊断状态请求将被用于获得第一加密密钥，该第一加密密钥将用于加密虚拟机的未被加密且正在被存储的诊断状态的至少一部分
712

图7A

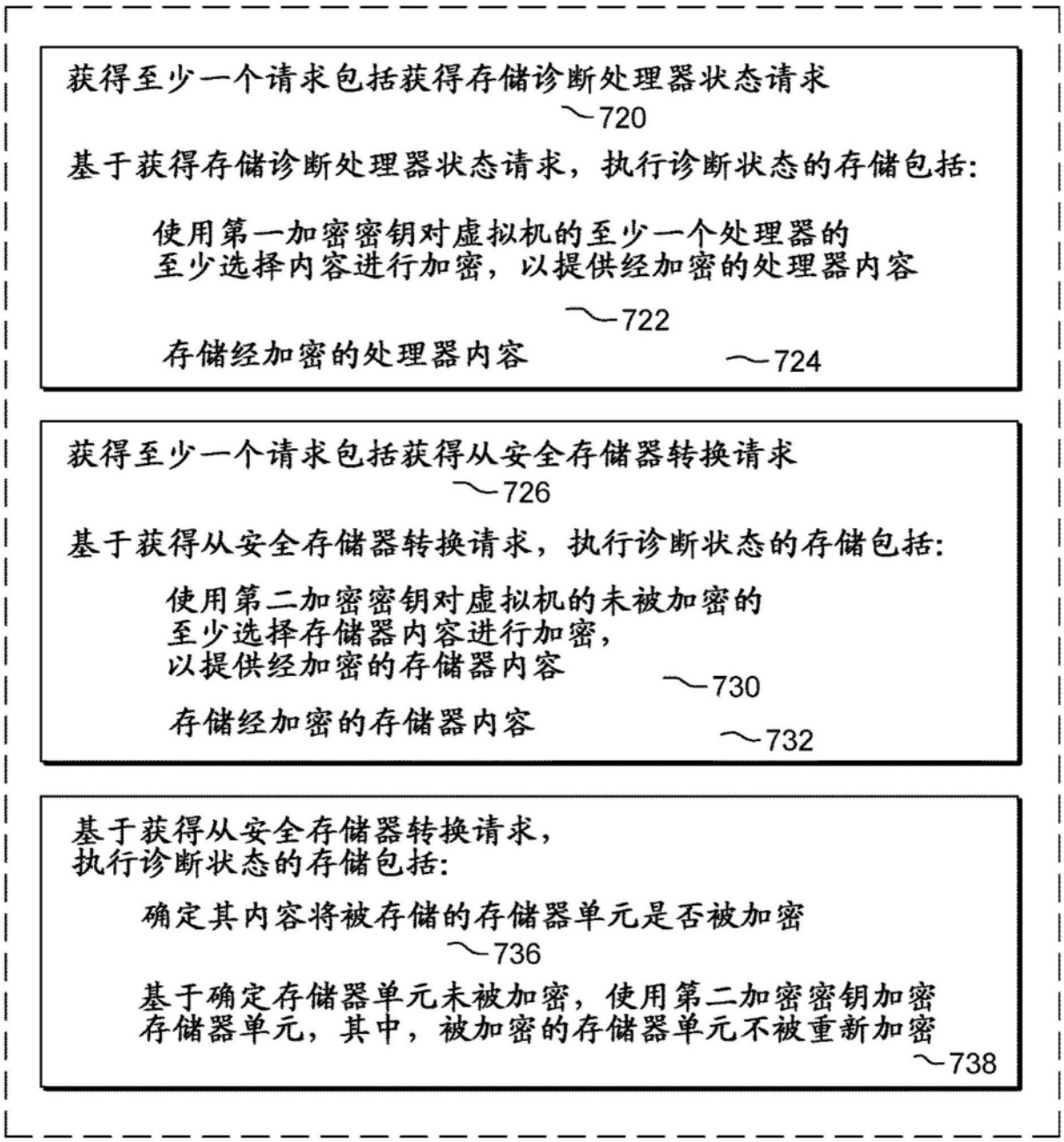

获得至少一个请求包括获得存储诊断处理器状态请求
720
基于获得存储诊断处理器状态请求，执行诊断状态的存储包括:
使用第一加密密钥对虚拟机的至少一个处理器的
至少选择内容进行加密，以提供经加密的处理器内容
722
存储经加密的处理器内容
724
获得至少一个请求包括获得从安全存储器转换请求
726
基于获得从安全存储器转换请求，执行诊断状态的存储包括:
使用第二加密密钥对虚拟机的未被加密的
至少选择存储器内容进行加密，
以提供经加密的存储器内容
730
存储经加密的存储器内容
732
基于获得从安全存储器转换请求，
执行诊断状态的存储包括:
确定其内容将被存储的存储器单元是否被加密
736
基于确定存储器单元未被加密，使用第二加密密钥加密
存储器单元，其中，被加密的存储器单元不被重新加密
738

图7B

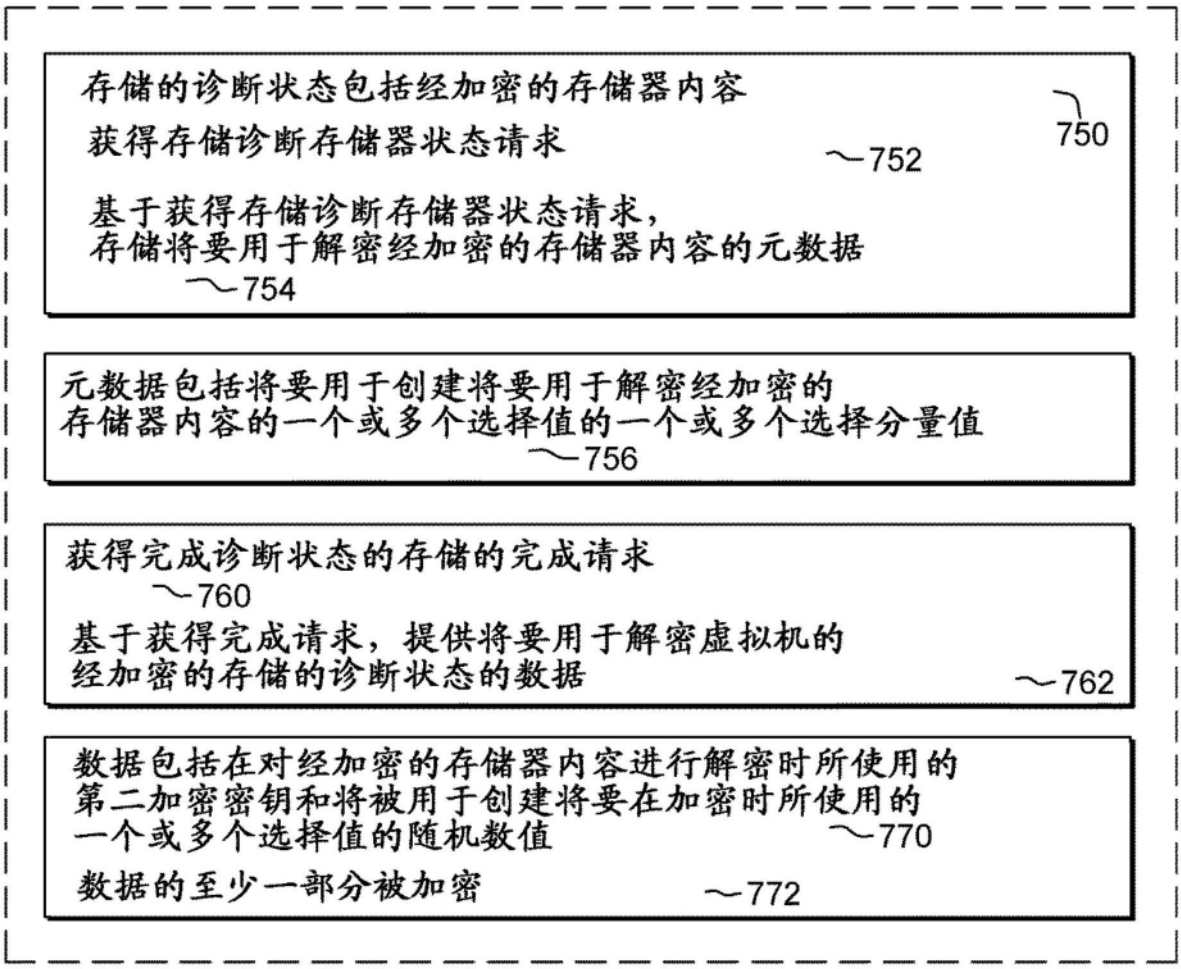

存储的诊断状态包括经加密的存储器内容
750
获得存储诊断存储器状态请求
752
基于获得存储诊断存储器状态请求，
存储将要用于解密经加密的存储器内容的元数据
754
元数据包括将要用于创建将要用于解密经加密的
存储器内容的一个或多个选择值的一个或多个选择分量值
756
获得完成诊断状态的存储的完成请求
760
基于获得完成请求，提供将要用于解密虚拟机的
经加密的存储的诊断状态的数据
762
数据包括在对经加密的存储器内容进行解密时所使用的
第二加密密钥和将被用于创建将要在加密时所使用的
一个或多个选择值的随机数值
770
数据的至少一部分被加密
772

图7C

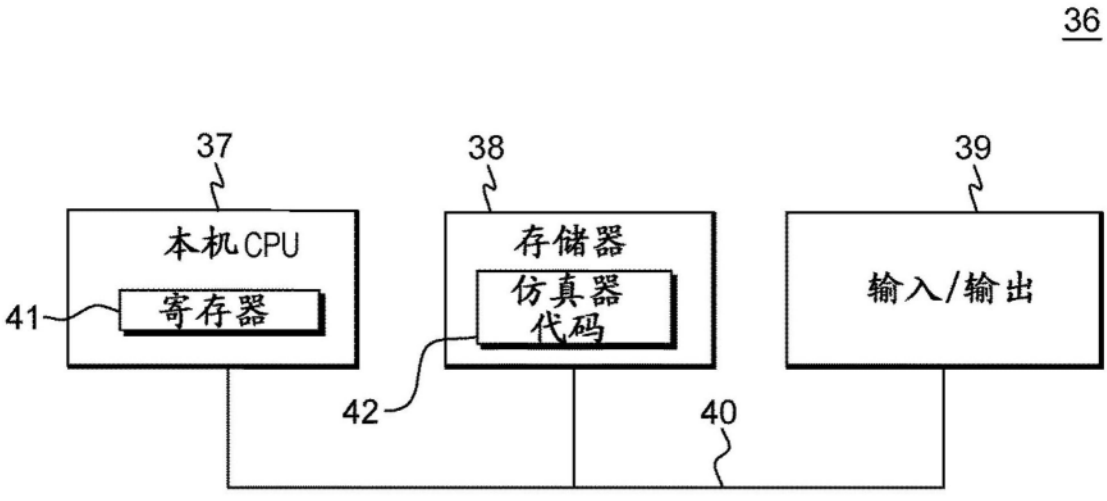

36
37
38
39
本机CPU
寄存器
41
存储器
仿真器
代码
42
输入/输出
40

图8A

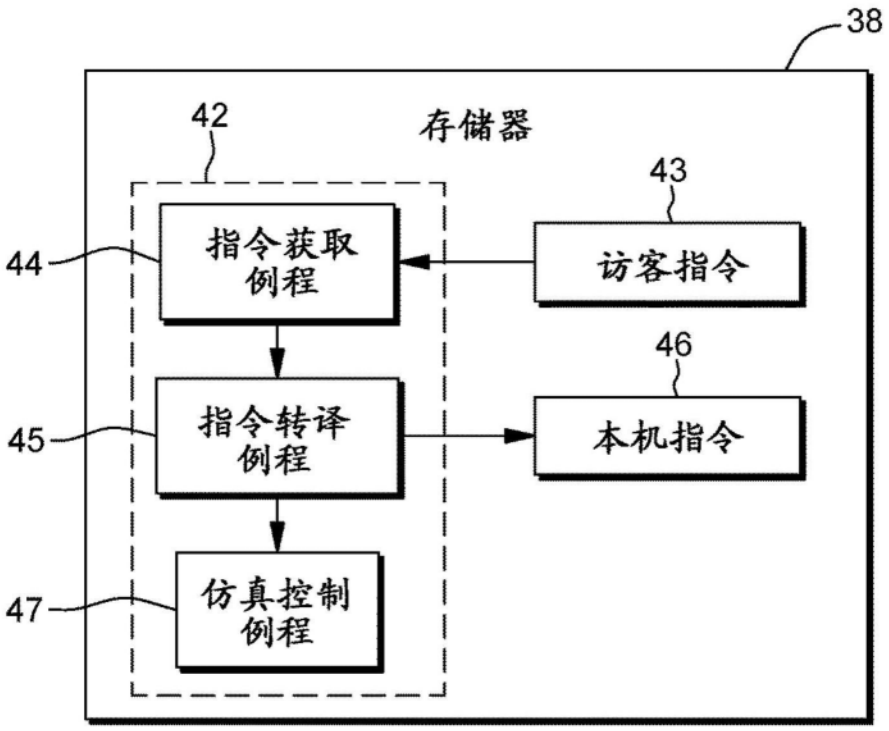


图8B

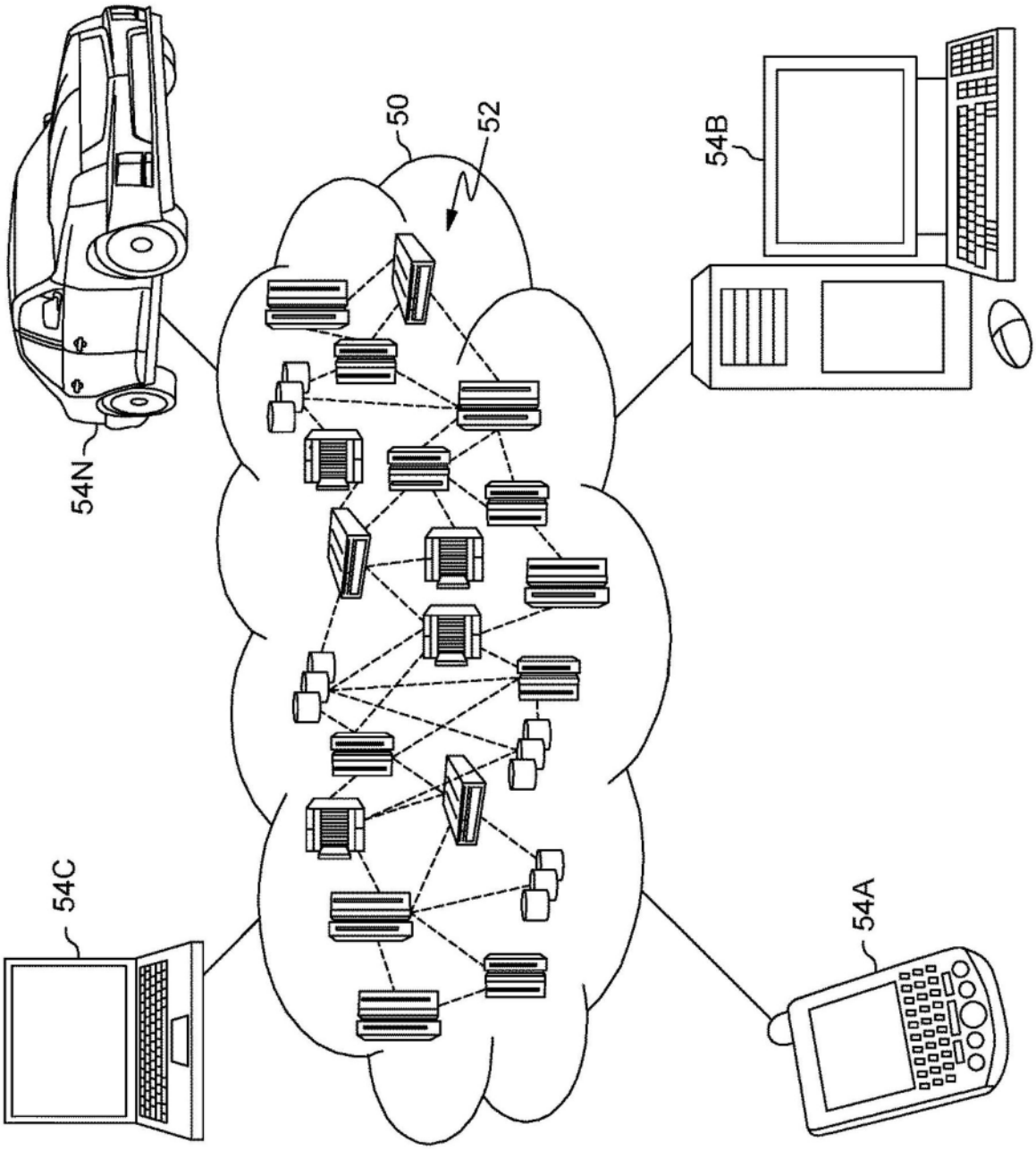


图9

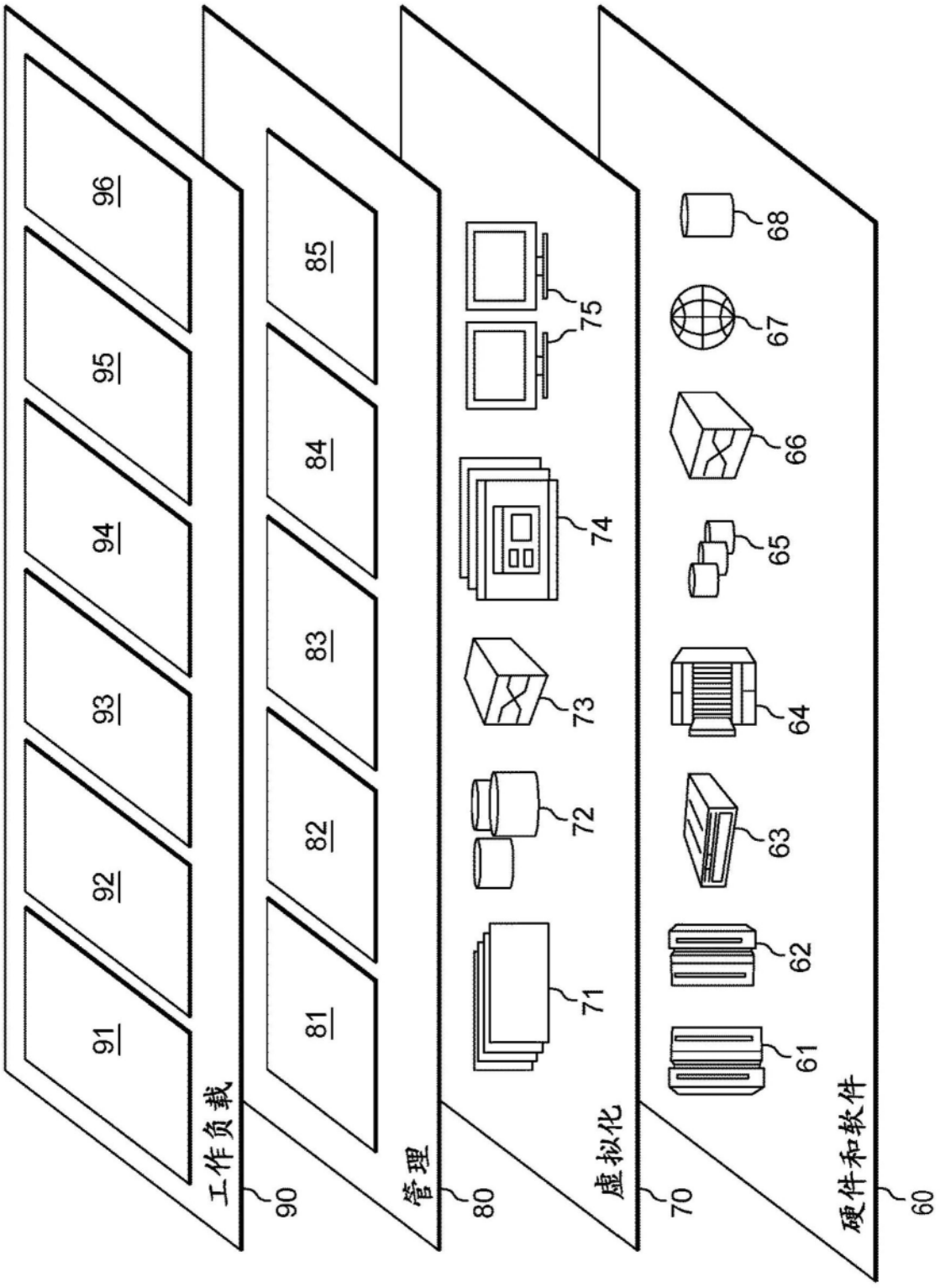

工作负载
90
91
92
93
94
95
96
管理
80
81
82
83
84
85
虚拟化
70
71
72
73
74
75
硬件和软件
60
61
62
63
64
65
66
67
68

图10