

面向云环境的虚拟机可信迁移方案

张建标^{1,2}, 朱元曦^{1,2}, 胡俊^{1,2}, 王晓^{1,2}

(1. 北京工业大学信息学部, 北京 100124;

2. 可信计算北京市重点实验室, 北京 100124)

摘要: 现今云计算技术迅猛发展, 虚拟机迁移技术作为云服务的一项优势, 受到了广泛的关注和应用。然而, 虚拟机动态迁移过程中存在平台认证复杂、数据传输安全性差等问题有待解决。为此, 首先分析了现有的基于可信计算技术的虚拟机迁移方案, 提出了云环境下基于可信计算技术的虚拟机动态迁移方案的3项安全要求: 平台认证、数据传输保护和虚拟可信根原子性保护。然后提出了面向云环境的虚拟机可信迁移方案, 其中引入了虚拟机中央迁移引擎和可信迁移代理, 实现了迁移过程的虚拟可信根的原子性保护。最后给出了具体的方案实现与验证。

关键词: 可信计算; 云计算; vTPCM; 虚拟机迁移

中图分类号: TP302.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018009

Scheme of virtual machine trusted migration in cloud environment

ZHANG Jianbiao^{1,2}, ZHU Yuanxi^{1,2}, HU Jun^{1,2}, WANG Xiao^{1,2}

1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

Abstract: With the rapid development of cloud computing, as an advantage of cloud services, virtual machine migration technology has been widely noticed and applied. However, there are some problems about VMs migration which should be solved, such as the complication of authentication of platform and the security issues of data transmission, etc. For these problems, firstly, the existing virtual machine migration scheme based on trusted computing technology was analyzed. Secondly, three secure needs that the virtual machine migration scheme which based on trusted computing technology should meet were proposed: the authenticated platform, confidentiality and integrity preserving transfer and atomicity of the vTPCM. Thirdly, a trusted migration scheme of virtual machines for cloud environment was proposed, in which the virtual machine central migration engine and trusted migration agent were introduced to solve the atomicity protection of vTPCM during the migration process. Finally, the concrete scheme was given with verification.

Key words: trusted computing, cloud computing, vTPCM, virtual machine migration

收稿日期: 2017-12-05; 修回日期: 2018-01-03

通信作者: 张建标, zjb@bjut.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61671030, No.U1405254); 国家高技术研究发展计划 (“863”计划) 基金资助项目 (No.2015AA016002)

Foundation Items: The National Natural Science Foundation of China (No.61671030, No.U1405254), The National High-Tech R&D Program of China (863 Program) (No.2015AA016002)

1 引言

现今云计算技术^[1]迅猛发展,已经成为国内外互联网行业的研究热点,知名的有谷歌云、亚马逊云、阿里云和腾讯云,也吸引了许多行业精英创立以云服务为核心的公司,国内较为成熟的有七牛云、青云等。云计算作为一种新型计算模式,它以资源租用、应用托管、服务外包为核心,把IT资源、数据、应用作为服务^[2]通过互联网提供给云租户,为互联网公司带来巨大利益的同时,也为云租户节约了生产成本。

虚拟机动态迁移技术^[3]是云计算技术的重要组成部分,可以实现服务器的动态负载均衡和在线维护,并提供了一种前瞻性灾备容错方案。虚拟机动态迁移具体指:将一台虚拟机从源服务器迁移至目标服务器,迁移过程中的宕机时间极短,使用户的正常使用时不受迁移过程宕机的影响,保证迁移过程对用户是透明的。

可信计算作为一项革命性技术,已经成为信息安全发展的新方向之一。如今,可信计算进入3.0时代,已经由被动防御变为主动免疫计算模式。可信3.0的双系统体系结构应用可信平台控制模块(TPCM, trusted platform control model)可以实现主动监控和主动度量,不仅可以对实体(如软、硬件的启动,网络接入等)的初始状态进行度量,还可以在系统运行中,对实体的状态及行为进行动态度量,增强了系统的安全性。针对云计算自身的技术特点、服务模式严重影响传统信息安全解决方案有效性,应用可信计算技术可以有效降低云计算安全风险。将vTPCM与云平台、虚拟化结合起来,解决VM-vTPCM的迁移问题。

目前,针对虚拟机动态迁移技术的研究大多是对迁移效率的研究,如缩短迁移时间、快速迁移、减少迁移量等,对迁移过程中存在安全问题研究较少。而在实际的云计算环境中,存在大量迁移过程中的安全威胁有待解决。现有基于可信计算技术^[4]的虚拟机迁移方案对虚拟机迁移过程的数据安全和平台可信证明^[5]有所考虑。但对于虚拟可信根的原子性问题,现有的方案绝大多数没有考虑,很少一部分有所提及,但是也没有给出具体解决方案。没有针对性的具体解决方案,

会造成云环境中出现虚拟可信根的副本存在,云环境的可信状态无法保障,使云环境的安全受到严重威胁。同时,现有基于可信计算技术的虚拟机迁移方案没有给出详细具体的虚拟机动态迁移框架设计,没有明确的功能模块设计方案。所以,本文提出了一种面向云环境的虚拟机可信迁移方案,以解决迁移过程的虚拟可信根的原子的保护为出发点,提出了相应的解决方案。

2 相关技术

2.1 可信软件基框架 Cube

可信软件基是可信机制的核心,其在可信计算平台中的作用类似于操作系统对信息系统的作用。北京工业大学可信计算实验室提出并设计实现了可信软件基框架Cube^[6]。Cube之间互连接,构成一个分布式的可信计算子系统来管理信息系统。用户可以开发可信处理机制,以插件的形式挂载到可信计算子系统特定节点的Cube进程中,通过Cube汇总到可信管理中心统一管理,Cube也可以提供针对特定安全机制定制的可信插件,将安全机制作为可信对象进行统一管理。

Cube提供了如下一些核心功能。

1) 策略格式的定义与解析功能:用来让Cube能够解读不同格式的策略。

2) 内存键值数据库维护功能:可以为Cube所定义的数据格式建立内存数据库,持久化存储这些数据格式,必要时还可以导出。

3) 可扩展消息处理功能:可以定义特定格式策略的消息,通过可信协议保护策略的传输和处理,并可利用消息驱动各模块协同执行可信功能。

4) 子模块载入功能:框架可以载入不同的可信功能子模块,以实现不同的可信处理机制。

5) 消息路由定义功能:可以定义消息在子模块之间以及不同节点可信软件基之间的传输途径,通过定义消息的传输途径实现子模块之间的数据对接和节点间可信协议协作过程。

Cube的具体架构如图1所示。

2.2 VM-vTPM 迁移过程的安全威胁

在现有的VM-vTPM迁移方案中,Hong等^[7]和Danev等^[8]都只提出了迁移过程的平台认证、数据传输的机密性和完整性保护要求,设计了相

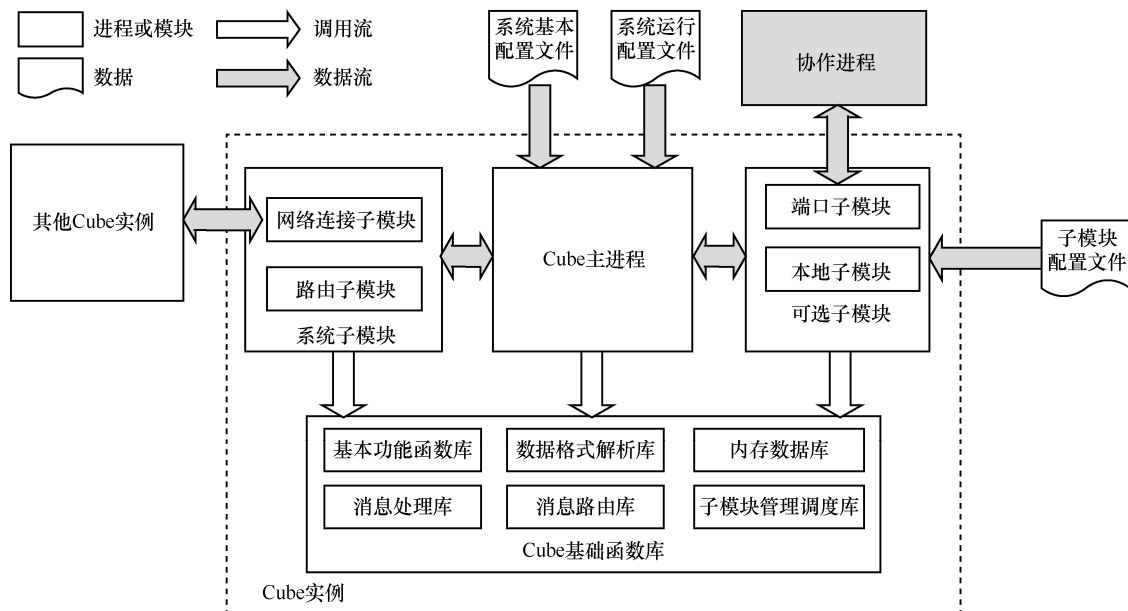


图 1 可信软件基框架 Cube

应的协议。然而，其安全需求完全没有考虑虚拟可信根的原子性保护要求，无法保证平台的可信状态不被破坏。Liang 等^[9]提到了虚拟可信根的原子性保护需求，然而描述不足，不够具体，并且缺乏详细的安全机制设计来解决虚拟可信根的原子性保护。

综上，VM-vTPM 迁移过程的安全问题主要有如下几点。

1) 平台间完整性证明。虚拟机可能被迁移到不可信平台中，攻击者在虚拟机迁移前，通过某种手段控制了目的平台，一旦虚拟机被迁移过来，攻击者就会对其进行攻击破坏，获取虚拟机权限。

2) 通信通道安全。迁移的数据可能遭到监听甚至修改。一方面，攻击者通过监听源宿主机与目标宿主机之间的网络，获得迁移过程中传送的全部数据，从而可以确定迁移虚拟机的大小、迁移时间，甚至虚拟机操作系统的用户口令、应用数据等敏感信息。另一方面，攻击者通过修改迁移的内存数据为特定数据，进而控制虚拟机。

3) 虚拟可信根的原子性问题。云环境中不可以出现一个虚拟可信根的多个副本，或者迁移失败时虚拟可信根无法恢复的问题。无法恢复虚拟可信根可能会导致租户遭受 DoS，无法正常使用服务。

现有的虚拟机迁移方案实现了平台认证、数

据传输的机密性和完整性保护要求，然而对迁移过程的原子性保护问题考虑不足，缺少具体的解决方案。同时，现有的 VM-vTPM 迁移方案主要是迁移协议的设计，有些对安全需求考虑不周全，有些虽然有考虑，但是没有详细具体的迁移机制和功能模块的设计。而且使用 TPM 也只是进行被动的防御，无法在复杂的云环境中对各种安全威胁主动免疫，降低安全风险。使用 TPCM 保证平台进行主动控制和主动度量，达到主动免疫的效果则是更为合适的选择。

3 云环境下基于 vTPCM 的虚拟机安全迁移方案

3.1 云环境下基于 vTPCM 的虚拟机安全迁移框架

本节针对云环境下 VM-vTPCM 迁移过程中的原子性保护问题提出云环境下基于 vTPCM 的虚拟机安全迁移框架，旨在防止云环境中出现 vTPCM 副本，保护虚拟可信根的原子性。

底层硬件环境的硬件 TPCM 芯片为系统提供了可信计算的密码服务，而且 TPCM 与宿主机系统构成可信 3.0 提出的双系统体系结构，为系统提供主动监控和主动度量机制，优先于系统进行加电启动，监控系统运行环境，保障系统的安全性。

宿主机系统包含可信迁移代理和 vTPCM 管

理器。vTPCM 管理器作为一个服务程序,管理上层对 vTPCM 实例的访问,根据上层对 vTPCM 的访问情况,调度底层硬件环境的 TPCM 的可信计算资源,管理 vTPCM 上下文的导入导出,并提供新的 vTPCM 实例创建和 vTPCM 迁移功能。可信迁移代理与控制节点的虚拟机中央迁移引擎对接,接收中央迁移引擎发起的虚拟机迁移指令,二者协作实现 VM-vTPCM 的迁移功能,并提供虚拟可信根的原子性保护。

最上层是由 VMM 统一管理的虚拟机实例,每个虚拟机实例中都包含一个虚拟机的 TSB,提供虚拟机的可信管理支撑。

云环境下基于 vTPCM 的虚拟机安全迁移框架的具体设计如图 2 所示。

Xen^[10]中的 vTPM 是一个 miniOS,作为一个小型的虚拟域,通过 vTPM Manager 前端驱动和

vTPM 建立连接通路,通过 vTPM 后端驱动与指定虚拟机绑定连接,形成完整的 VM-vTPM 系统结构。因此,在 VM-vTPM 迁移的过程中,对 vTPM 的迁移要求迁移 vTPM 虚拟域,所以传输过程中网络带宽的占用率较高。

而本文 VM-vTPCM 的迁移方案中,采用了 Cube 模型实现 vTPCM Manager 和 vTPCM。因此,vTPCM 上下文均是以文件形式存储的。当系统需要进行相应操作的时候,会进行相应的读写操作。所以,迁移过程中只需对相应的 PCR 值、密钥句柄、会话等数据进行迁移。

3.2 虚拟机中央迁移引擎

如图 3 所示,虚拟机中央迁移引擎由 5 个模块构成:状态信息报告生成模块、信息收集模块、迁移流程控制模块、迁移信号传输模块和迁移回滚日志模块。

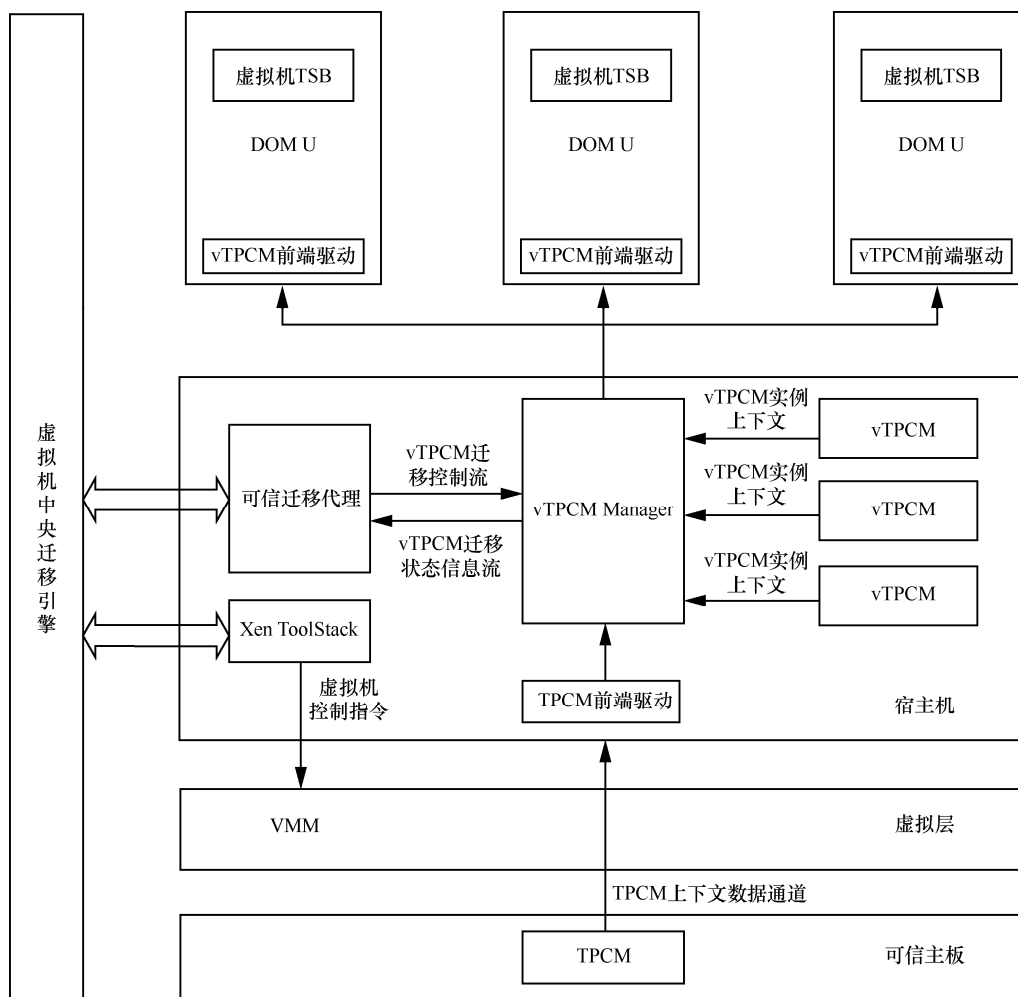


图2 云环境下基于 vTPCM 的虚拟机安全迁移框架

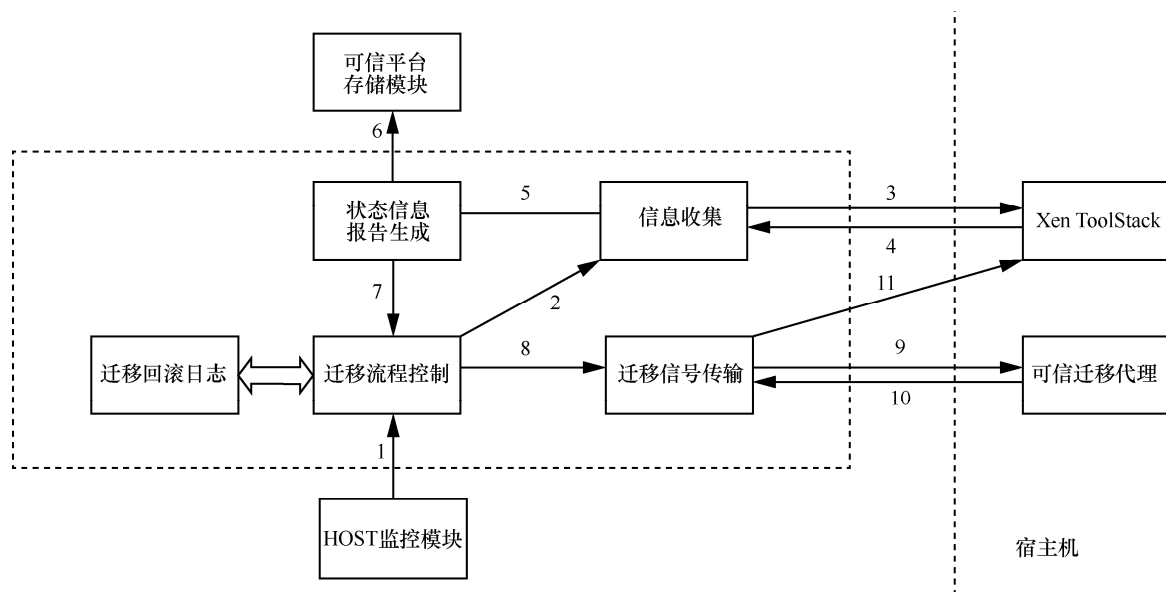


图3 虚拟机中央迁移引擎

迁移流程控制模块作为核心，调度其他4个模块协作完成 VM-vTPCM 迁移过程。主要功能包括接收控制节点的资源监控模块发出的 VM-vTPCM 迁移指令，初始化生成可信迁移报告；发送信息收集指令，调度信息收集模块进行 VM-vTPCM 迁移的预处理；接收状态信息报告生成模块的可信迁移报告，判断是否符合迁移策略基准库的迁移策略，确定是否发起迁移操作；对迁移信号传输模块发起正式迁移指令。当迁移过程出现 VM 或者 vTPCM 迁移失败时，迁移流程控制模块会通过迁移回滚日志获取系统需要执行的恢复操作。

信息收集模块用于对 VM-vTPCM 迁移进行预处理，收集源服务器和目标服务器的信息，用于判断源服务器的 VM-vTPCM 状态是否可以迁移，目标服务器的剩余资源是否满足迁移策略要求。

状态信息报告生成模块对信息收集模块获得的信息进行筛选，如内存、CPU 信息，获得必要的信息填入可信迁移报告中。

迁移信号传输模块与服务器的可信迁移代理以及 Xen ToolStack 对接，分别控制 vTPCM 的迁移和 VM 的迁移。

迁移回滚日志是保证迁移过程的虚拟可信根原子性的核心机制。迁移回滚日志包括 Redo^[11]（重做信息）和 Undo（撤销信息）2 个部分。Redo

记录了迁移引擎执行的每条操作，如 VM 迁移、vTPCM 迁移等，当某一项操作失败的时候，可以读取 Redo 记录再次执行相应操作。Undo 记录了迁移引擎执行的每条操作的逆向操作，如 VM 从 A→B 的迁移，逆向操作则是由 B→A 的迁移操作，一旦系统某项操作的多次执行均失败超时，便不再读取 Redo 记录进行操作重做，而是读取 Undo 记录，将某一迁移过程恢复到初始状态，即撤回 VM-vTPCM 的迁移操作。

在整个 VM-vTPCM 迁移的生命周期内，控制节点的虚拟机中央迁移引擎需要生成一份可信迁移报文。可信迁移报文随着迁移控制流在模块间传递，记录迁移状态，通过对报文中 VM-vTPCM 迁移状态的判断，一旦发生迁移失败的情况，则调用迁移回滚日志，进行迁移的回滚操作，保证 vTPCM 不在源服务器和目标服务器出现相同的副本，确保迁移过程的虚拟可信根的原子性。

虚拟机中央迁移引擎的主要工作流程如下。

1) Host 监控模块实时监控服务器的资源使用情况，监控到资源负载过高的服务器时，确定 VM-vTPCM 迁移的源服务器和目标服务器以及待迁移虚拟机，对迁移流程控制模块发出迁移指令。

2) 迁移流程控制模块将生成可信迁移报文，填充源服务器和目标服务器以及待迁移虚拟机等相关的数据，发送到信息收集模块。

3)、4) 信息收集模块通过 Host 的 UUID 获取

对应的服务器连接，获取源服务器和目标服务器的状态信息、虚拟机的状态、是否可以发起迁移的相关信息。

5)~7) 信息收集模块将收集到的状态信息发送给状态信息报告生成模块，相应地填充到可信迁移报文中，发送到迁移流程控制模块，并存储到可信平台的存储模块。

8) 迁移流程控制模块对可信迁移报告进行判断，如果符合迁移要求，则发出迁移指令给迁移信号传输模块。

9)、10) 迁移信号传输模块接收到迁移指令后，对可信迁移代理发起 vTPCM 迁移的操作，并根据迁移结果对可信迁移报告中的 vTPCM 迁移状态进行更改。

11) 完成 vTPCM 迁移后，对 Xen ToolStack 发起 VM 的迁移指令，并在迁移完成后进行 VM-vTPCM 的恢复绑定操作。

3.3 可信迁移代理

VM-vTPCM 迁移过程中，为了保证虚拟可信根的原子性，防止 vTPCM 副本的产生以及数据的丢失，除了控制节点的虚拟机中央迁移引擎外，服务器端必须有控制迁移过程中 vTPCM 的创建、副本销毁以及灾备恢复工作的相应模块。为了实现 vTPCM 迁移过程的原子性保护功能，本文设计了运行于服务器的宿主机上的可信迁移代理。该模块作为 VM-vTPCM 的核心模块之一，负责调度 vTPCM Manager 完成 vTPCM 的迁移工作。

可信迁移代理主要功能是接收并解析虚拟机中央迁移引擎发送的可信迁移报告，调用目标服务器 vTPCM Manager 生成 vTPCM 的容器，用于接收迁移的 vTPCM 实例。vTPCM 迁移成功与否将返回状态信息给可信迁移代理，由可信迁移代理对可信迁移报告的 vTPCM 迁移状态进行修改，确保 vTPCM_migration_status 和 vTPCM_reset_status 互斥，保证 vTPCM 在源服务器和目标服务器不产生副本。

当 vTPCM_migration_status 为 0 时，表示 vTPCM 迁移失败，系统将删除目标服务器的 vTPCM 相关信息，同时恢复 vTPCM 在源服务器的运行，此时即 vTPCM 复位状态，vTPCM_reset_status 设置为 1。

4 方案实现及实验分析

4.1 方案实现

本文方案基于 Xen 的云平台实现 VM-vTPCM 的动态迁移过程，迁移过程的原子性保护的关键是对可信迁移报告的数据结构设计。下面给出具体设计方案。

1) Host 监控模块—>迁移流程控制模块的过程中，必要的参数用于确定 VM-vTPCM 迁移的源服务器、目标服务器以及待迁移虚拟机，具体参数如表 1 所示。

表 1 迁移启动参数

参数	类型	意义
SourceHost	UUID	源服务器唯一标志
TargetHost	UUID	目标服务器唯一标志
TargetVm	UUID	待迁移虚拟机

2) Xen ToolStack—>信息收集模块的数据传输过程中，主要收集服务器的状态以及资源使用情况，用于下一步确定是否满足迁移条件，是否可以执行迁移操作。具体参数有 VM 和 Host 这两部分的相关参数，如表 2 和表 3 所示。

表 2 VM 参数

参数	类型	意义
Vm_uuid	String	虚拟机唯一标识
Domin_id	Long	虚拟机域标识
Bios_string	Map<String,String>	BIOS 信息
Sr_uuid	String	虚拟机 SR 的唯一标识

表 3 Host 参数

参数	类型	意义
Cpu_info	Map<String,String>	CPU 信息
Host_uuid	String	主机唯一标志
Bios_string	Map<String,String>	BIOS 信息
Software_version	Map<String,String>	软件信息
migrationReceive	Map<String,String>	迁移 token,是否准备好接收迁移虚拟机

3) 迁移信号传输模块实时监控 VM 以及 vTPCM 的迁移状态，结构如表 4 所示。

表4 迁移状态参数

参数	类型	意义
VM_power_status	VM	虚拟机电源状态
vTPCM_migration_status	int	vTPCM 迁移进度状态
vTPCM_reset_status	int	vTPCM 复位状态

迁移过程中的信息收集主要函数是 `host_info_collect` (Connection connection, Uuid host, Uuid vm), 通过调用 XAPI 与 Xen 建立 Https 连接, 获取相关数据, 并加密返回给控制节点。

vTPCM 的迁移以及恢复主要函数包括以下 2 个。

`vTPCM_migrate` (Connection connection, Uuid sourceHost, Uuid targetHost, Uuid vm);

`vTPCM_restore` (Connection connection, Uuid sourceHost, Uuid targetHost, Uuid vm)

第一个函数通过迁移的虚拟机获得相应的源服务器 vTPCM 数据, 通过 Host UUID 以及 VM UUID 确定目标服务器需要绑定的虚拟机, 完成 vTPCM 数据的加密传输, 以及 VM-vTPCM 绑定操作。

第二个函数用于在第一个函数返回 vTPCM 迁移失败的时候, 对迁移的原子性进行保护。在恢复源服务器 vTPCM 的同时, 将迁移失败的目标服务器的 vTPCM 副本删除, 防止云环境内出现 vTPCM 的复制。

4.2 功能测试

实验环境如下。每一台服务器均搭载 TPM 芯片, 搭建 XenServer 私有云环境, 对 VM-vTPM 虚拟机动态迁移方案进行测试。具体配置如表 5 所示。

表5 实验节点信息

节点类型	数量	CPU	磁盘	内存
计算节点	2	Intel (R) Core i5-4590	1 TB	8 GB
控制节点	1	Intel (R) Core i5-4590	1 TB	8 GB
存储节点	1	Intel (R) Core i5-4590	1 TB	8 GB

迁移实验拓扑如图 4 所示。通过控制节点的虚拟机迁移引擎手动发起虚拟机迁移操作, 指定源服务器 (test1) 和目标服务器 (test2) 以及待迁移虚拟机 (vm_test), 系统迁移过程中收集到了 VM、vTPM 和迁移状态的相关信息。程序中强制设置 vTPM_migration_status 状态为 0, vTPM_reset_status 状态为 1, 使迁移过程失败。系统执行 Undo 日志生成的迁移过程的逆向操作内容, 恢复了源服务器的虚拟可信根, 删除了目标服务器的虚拟可信根副本, 从而保证了迁移过程的虚拟可信根的原子性, 如图 5 所示。

4.3 系统性能分析

本节对 VM-vTPM 虚拟机动态迁移和常规虚拟机动态迁移的系统性能进行实验和分析。实验中待迁移虚拟机为 CentOS 7.0 版本, 为虚拟机分配不同大小的内存, 记录虚拟机动态迁移所使用的时间。然后在虚拟机和 vTPM 绑定之后, 为虚拟机分配不同大小的内存, 记录 VM-vTPM 动态迁移使用的时间。实验的性能指标是虚拟机动态迁移的总时间。

具体的实验结果如图 6 所示。迁移虚拟机的总迁移时间和虚拟机的内存成正比。相比常规的虚拟机迁移, 基于 vTPCM 虚拟机动态方案在虚拟机内存为 128 MB 时, 迁移总时间增加了 19.2%, 当虚拟机内存为 1 024 MB 时, 迁移总时

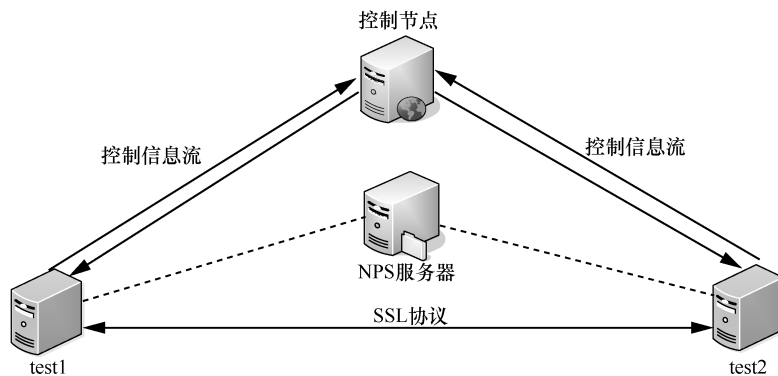


图4 迁移实验拓扑



图5 虚拟可信根原子性保护测试

间增加了 2.1%，总平均花费时间增加了 5.2%。可见随着虚拟机内存的增大，基于 vTPCM 虚拟机动态方案影响的迁移时间占比越来越低。现今云计算行业中，云服务器最低是 1 GB 内存，很多企业的需求更高。所以，迁移过程中增加的耗时是可以接受的。

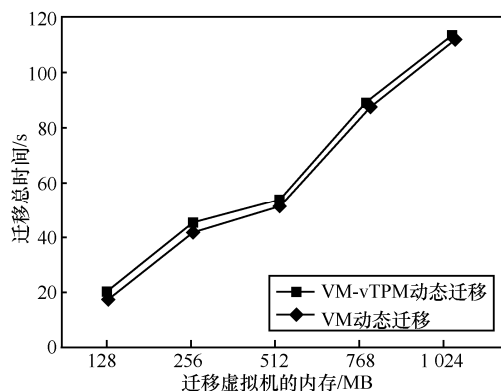


图6 迁移时间对比

5 结束语

本文首先对可信软件基框架 Cube 进行了介绍，对 VM-vTPM 的虚拟机迁移方案进行了分析，总结了云环境虚拟机迁移过程中存在的安全问题，提出了迁移过程中的 3 点安全需求：平台间认证、传输数据的保护和虚拟可信根原子性的保护。根据安全需求，提出了面向云环境的虚拟机可信迁移方案，详细说明了总体设计方案和各个

模块功能说明，最后给出了方案实现与验证。通过设计面向云环境的虚拟机可信迁移方案，解决了迁移过程中虚拟可信根的原生性保护问题，保证了云环境的可信状态不被破坏，使云环境免于受到迁移过程带来的安全威胁。

参考文献：

- [1] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(6): 1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. The review of cloud computing environment security[J]. Journal of Software, 2016, 27(6): 1328-1348.
- [2] WANG C, WANG Q, REN K, et al. Toward secure and dependable storage services in cloud computing[J]. IEEE Transactions on Services Computing, 2012, 5(2): 220-232.
- [3] LI W, TORDSSON J, ELMROTH E. Modeling for dynamic cloud scheduling via migration of virtual machines[C]//IEEE Third International Conference on Cloud Computing Technology and Science. 2011:163-171.
- [4] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学:信息科学, 2010(2):139-166.
SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing[J]. SCIENTIA China: Information Sciences, 2010, (2): 139-166.
- [5] 冯登国. 可信计算:理论与实践[M]. 北京: 清华大学出版社, 2013.
FENG D G. Trusted computing: theory and practice[M]. Beijing: Tsinghua University Press, 2013.
- [6] 胡俊, 沈昌祥, 公备. 可信计算 3.0 工程初步[M]. 北京: 人民邮电出版社, 2017.
HU J, SHEN C X, GONG B. Trusted Computing 3.0, Preliminary Project[M]. Beijing: Posts & Telecom Press, 2017.

- [7] HONG Z, WANG J, ZHANG H G. A trusted VM-vTPM live migration protocol in clouds[C]// The International Workshop on Cloud Computing & Information Security. 2013: 299-302.
- [8] DANEV B, MASTI R J, KARAME G O, et al. Enabling secure VM-vTPM migration in private clouds[C]//The 27th Computer Security Applications Conference(ACSAC 2011). 2011:187-196.
- [9] LIANG X, JIANG R, KONG H. Secure and reliable VM-vTPM migration in private cloud[C]//The International Symposium on Instrumentation and Measurement, Sensor Network and Automation. 2014:510-514.
- [10] SUN M, REN W. Improvement on dynamic migration technology of virtual machine based on Xen[C]//The International Forum on Strategic Technology. 2013:124-127.
- [11] JOSHI A, NAGARAJAN V, VIGLAS S, et al. ATOM: atomic durability in non-volatile memory through hardware logging[C]// IEEE International Symposium on High Performance Computer Architecture. 2017:361-372.



朱元曦（1993-），男，北京人，北京工业大学硕士生，主要研究方向为云计算、可信计算。



胡俊（1972-），男，湖南湘阴人，博士，北京工业大学讲师，主要研究方向为信息安全和可信计算。

[作者简介]



张建标（1969-），男，江苏海门人，博士，北京工业大学教授、博士生导师，主要研究方向为网络与信息安全、可信计算。



王晓（1983-），女，河北石家庄人，北京工业大学博士生，主要研究方向为信息安全、可信计算。