平台虚拟化和软件许可：

软件供应商最佳实践

白皮书

“目前仍未解决如何在虚拟环境下管理其应用程序许可的软件发布商有些落后了。策略不仅包括为虚拟环境下许可提供支持，也包括一旦在虚拟机上部署应用程序后强化实施许可条件的能力。如果不能实施的话，软件发布商对许可没有控制力，从而也就不能控制他们的收益。”

——Amy Konary，IDC1 研究总监

执行摘要

关于互联网上的虚拟化（Virtualization），有很多相关但不同的定义。如果更细致地梳理检查的话，我们会发现多数定义都是关注于设计一套让数据中心更高效的程序和方法。虚拟化在测试和开发领域已经存在的很多年。但是，在当今的经济环境下，虚拟化日益流行开来，IT 业界通过虚拟化来降低成本并提高运行效率。

对于那些被软件许可合规性难题所困扰的终端用户机构，以及那些想要强化软件合规性并确保收益同时不会限制客户部署的独立软件供应商（ISV）来说，平台虚拟化是一个重要方法。本文介绍了虚拟化概念，探讨了其所具有的优点，以及它之所以成为软件许可业界炙手可热话题的原因。最后，本文重点介绍了独立软件供应商（ISV）可用的产品选择并提供了在虚拟环境下处理软件许可的最佳实践。

什么是虚拟化？

如果使用互联网搜索引擎搜索的话，马上就可以搜到诸多有关“虚拟化”的定义。在计算领域，虚拟化已经从一个“专门术语（buzz word）”变成一个主流 IT 术语，就像 PC 或服务器一样平常。对于当今那些涉及计算机行业的人士来说，如果没遇到过“虚拟机”、“VM”甚或是“超级监督程序（Hypervisor）”术语的话，的确是一件非常不可思议的事情。

如果继续搜索一下的话，搜索引擎会提供诸多提供虚拟化解决方案的供应商信息，产品名称诸如 VMware、XEN、VirtualBox、KVM 和 Microsoft（业界领先者）。术语“虚拟化”被广泛使用，可以是指平台、应用程序、网络、存储、内存和其他领域。最终，它是这样一个概念：在软件中模拟或人工重新创建一个或多个物理环境情境。虽然，术语“虚拟化”涵盖了不同的领域，但是本文主要关注于平台虚拟化领域，以及其对软件许可和自动软件许可实施领域的影响情况。

虚拟化

- 通过更有效地使用硬件资源节省资本并降低运行成本。
- 通过绿色 IT（Green IT）进一步降低成本和环境影响。
- 更高效地测试/开发和更高的安全性。
- 改进的可扩展性和部署灵活性。
- 高可用性/冗余度。

为什么虚拟化成为一个如此炙手可热的话题？

有很多原因可以说明虚拟化现在的发展情况，虚拟化是 IT 行业内最有用的技术改进之一。虚拟化可以提供如下诸多显著益处。

通过更高效地使用硬件资源节省资本并降低运行成本。通常来说，支持公司每天业务运行的系统（如电子邮件服务器和数据库服务器）大约只会消耗物理机器可用资源的 10%到 30%。换句话说，如果不采用虚拟化技术，一台机器多达 90%的资源实际都用不上而被白白浪费。

考虑到高性能服务器的平均采购成本，显而易见地这是一个多么大的浪费。通过在一台物理机器上创建多个虚拟服务器，公司可以更高效地使用它们的硬件设备，因此，可以降低采购并维护多台物理机器所带来的成本。

通过绿色 IT（Green IT）进一步减少成本和环境影响。通过虚拟化减少服务器数量不仅可以通过更高效地使用硬件节省资金，同时也可以减少电能消耗，从而降低公司的碳排放量。

更高效地测试/开发和更高的安全性。虚拟化的另一项明显益处就是提高测试效率和安全性。可以轻松地使用'干净的'虚拟镜像轻松地再生系统以创建新的测试和部署环境，或者快速替换一个受到恶意软件破坏的系统。

改进的可扩展性和部署灵活性。可扩展性是推动虚拟化应用的另一个重要因素。当公司需要更多带宽或更高可用性时，可以在短时间内相对简单地创建一个新的虚拟化系统情境，无需花钱采购新硬件，也无需用户重新熟悉新设备。

高可用性/冗余度。虚拟化服务常常被安装在集群环境中。动态加速虚拟镜像'克隆'的内在概念可以显著地降低管理集群基础架构相关的复杂度和成本。

为什么虚拟化成为许可领域日益关注的一个话题？

上面所述原因已经表明公司不能忽视虚拟化的存在，有诸多简单但非常合理的理由支持公司采用虚拟化技术。但是，当考虑到软件供应商利益时，这些支持理由也会带来一种利益冲突。

按照 IDC1 研究总监 Amy Konary 的说法，"目前仍未解决如何在虚拟环境下管理其应用程序许可的软件发布商有些落后了。策略不仅包括为虚拟环境下许可提供支持，也包括一旦在虚拟机上部署应用程序后强化实施许可条件的能力。如果不能实施的话，软件发布商对许可没有控制力，从而也就不能控制他们的收益。"

今天，并非所有第三方许可实施技术都是基于一种名为基于主机的许可实施的概念的。简而言之，这是一个将许可政策束缚到一个已知且授权的主机或机器的概念。

典型地，会通过一种被称为硬件指纹识别或节点锁定的机制将一份软件许可紧密连接到指定或授权计算机、指纹识别的目的是通过独一地将一份许可与机器结合起来保护许可免遭非法复制或共享。指纹识别最常见的例子是将许可与独特的硬件属性（如磁盘识别符或以太网（MAC）地址等）结合在一起。

自动许可实施选项

- 硬件密钥
- 虚拟机检测
- 虚拟机指纹识别

虚拟化已经为许可复制保护的基本组件带来了一个重大挑战。创建虚拟硬件的概念意味着同样可以创建虚拟指纹识别信息。一个复制的虚拟机常常会导致有一个复制的指纹识别信息，许可实施技术常常会将虚拟指纹识别信息与实际（物理）机器的指纹识别信息一视同仁。传统的看似可靠并且安全的反盗版技术不再有效，软件供应商也不能接受这种技术了。

这里要指出的最重要一点并不是虚拟化带来了更高的恶意软件或故意软件许可滥用的威胁。软件供应商所要面临的一个更重要问题是虚拟化带来了一个新问题，传统的"诚实"用户现在可以通过正常的每日操作疏忽而复制许可。换句话说，如果虚拟化成为部署应用程序的常用方式的话，这就会导致不经意地复制软件许可。这就带来了另外一个问题，供应商很难避免这种情况的出现，从而不能有效地保护其软件不被盗版或滥用。

软件供应商如何在今天处理虚拟化？

历史上来讲，提供给关注虚拟化的软件许可持有人的建议是围绕具体变化情况为他们提供指导，指导其如何对其软件应用程序进行定价和打包。例如，互联网上提供有很多免费文章建议供应商将其许可模式从常规的基于"坐席"的模式转到基于度量标准的模式，如基于交易的框架或基于消费使用的框架等。

对于很多供应商来说，实施这类重大运行和商业变化的预期常常也会带来一个大障碍。很容易理解，他们在寻求'解决'虚拟化所带来难题同时保留其现有商业模式的办法。对变化有抵触的主要原因是公司内诸多部门都会受到影响。许可模式的变更会对销售和销售模式带来直接影响，而这又关系到财务和审计流程。但是，受影响最大的就是业务运行部门，该部门负责产品和相关许可的实施。以服务为导向的职位，如客户维护和技术支持部门也会受到影响。多数软件供应商发现很容易预见如果将应用程序许可方式做出重大变化的话会给公司里那些独立但又相互联系的部门带来诸多的问题。

缺乏适当的技术解决方案首先会推动供应商创建协议条款内容，该内容不允许将其应用程序安装到虚拟环境。一些基本的'虚拟机检测'解决方案在许可技术（允许供应商技术性并且合法地实施其政策）中可用。这些政策已在短时间内进行了应用，但是在虚拟化成为更常见技术时变得不太有效。这给供应商留下了两个简单但困难的选择。

i. 他们不允许将其应用程序安装在虚拟机上，从而可以避免潜在的许可滥用情况。但是这种策略会限制其软件的部署范围，从而影响销售量。

ii. 更常见的做法是选择对虚拟化无动于衷，保持开放态度，提高销售业绩，强制用户接受许可实施政策的做法被显著弱化。

自动许可实施选项说明

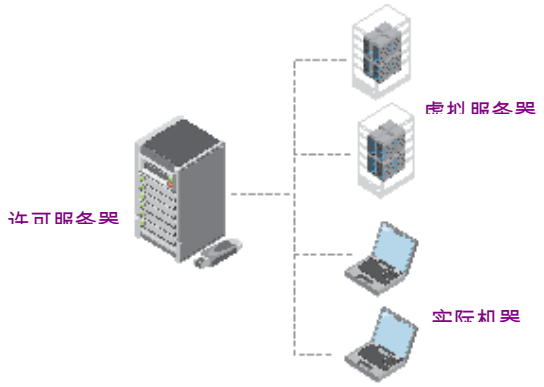
1. 硬件密钥

通过虚拟化针对许可复制最佳的保护是将负责实施许可政策的信息保存在一个可靠或受保护的位置或者在虚拟环境之外的一个位置。当今最常见的做法是软件供应商选择用硬件密钥（也被称为加密狗，dongle）来保护其应用程序。如果使用加密狗对应用程序进行保护的话，虚拟化和软件许可之间的矛盾就可以迎刃而解。

根据 IDC 报告，虚拟机数量会超过物理服务器数量，比例为 2：1。

这个概念相对简单。软件的使用依赖于特定硬件密钥的存在。虽然安装软件的系统可以被虚拟化（因此软件也被复制），但是一次只能使用一个加密狗访问一台机器，其他机器对加密狗的访问会被拒绝。这意味着在一台物理机器上，只能由一台虚拟机器访问加密狗，而无论在该物理机器上实际运行有多少台虚拟机。

硬件密钥的扩展应用是将密钥与并行网络许可组合起来。在这种情境下，通过将许可与硬件密钥连接起来保护许可服务器或许可管理程序免遭虚拟化。受保护的应用程序是否安装在一个实际客户端或虚拟化客户端上都没什么影响，因为许可管理程序会保留许可位置数量。这种情境就为软件供应商提供了一个很高的保证水平，确保保持许可数量不变，同时为客户提供了部署灵活性，而客户之所以选择虚拟化技术往往就是因为需要获得灵活性。



但是，也有一些原因导致人们认为硬件密钥并非是针对许可实施和虚拟化的最普遍的解决方案。其一，许多虚拟化技术不能充分支持外部 USB 设备，这意味着虚拟机不能发现硬件密钥。

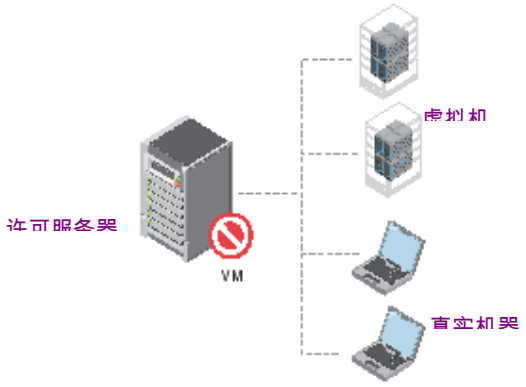
其二，很多供应商很不愿意给他们的客户发放硬件密钥，他们更倾向于选择一种基于软件的电子化解决方案。如上所述，围绕虚拟化的整个争论并不是在硬件密钥环境下出现的，它在那些只采用电子许可实施方式的供应商身上表现得更显著。

2. 虚拟机检测

借助此方法，许可系统使用内部检查来检测它（和受保护软件）是否运行在一台虚拟机上。供应商随后可以选择允许或不允许在虚拟环境下使用其软件并强制将应用程序部署在实际机器上。这种方法最大的问题是有短保质期的风险。如上所述，虚拟化越来越常见了，选择不准其客户将应用程序安装到虚拟环境的供应商会发现能部署他们软件的客户量会逐渐减少，相应地销售量也会减少。

接近 50%的企业机构都对其所有或部分地*IT 基础架构进行了虚拟化，另外 33%的企业计划在未来 12 月内实施虚拟化。*

但是，如果将此方法与并行网络许可部署组合使用的话（就像与硬件密钥组合一样），可以提供一个更可让人接受的解决方案。通过强制许可管理程序选择真实硬件，终端用户就可以自由地将受保护的应用程序部署到任何一组真实和虚拟机器上。这也可以满足很多软件供应商保持部署电子许可的想法。



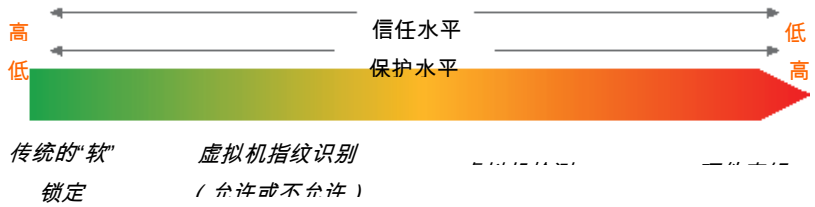
3. 虚拟机指纹识别

软件供应商希望继续以从前的方式部署并实施其软件，受这一想法推动，将一份许可独特地结合到一个虚拟机的能力是对他们来说可用的最新工具。这又回到前面所讨论的情况：多数软件供应商希望能够获得一套能够允许他们保持现有许可和部署模式的解决方案。虚拟机指纹识别（VM 指纹识别）概念允许软件供应商像对待真实机器一样对待虚拟机，虚拟化的整个争论也就不再那么重要了。

通过提供一个指纹识别机制（该机制包含设计时就考虑到的虚拟化属性），可以将一份许可锁定到一台虚拟计算机，同时提供高保证水平，保证虚拟机复制不会导致复制一份有效许可。

用可用选项创建最佳实践

目前对软件供应商来说有很多可用的方法，当考虑如何解决虚拟化和自动许可实施时可以创建一个有效的最佳实践方式。要考虑的首要因素就是软件供应商对其客户的信任水平。一般来说，软件供应对客户的信任水平和他们能提供给客户的灵活性水平之间有直接关系。当供应商对客户的信任水平较高时，他们就能够实施更为柔和的政策，给终端客户提供更少的部署限制。



90%的 ENT 机构都希望截止 2011 年底将其软件运行在虚拟机上。*

传统的软锁定对终端客户的限制最少，终端客户几乎有全部自由确定供应商应用程序的安装时间和安装方式。但是这一般只适用于那些自身有很高许可合规意识的终端客户。

一般情况下，终端用户都会寻求从其软件供应商处获得更多帮助，帮助他们'保持诚实'，供应商也倾向于实施帮助客户保持合规性的措施。虚拟机指纹识别方式就很适合这种情况，因为它可以提供高水平的保护，避免软件许可被意外滥用。

如果供应商要求实施更严苛的政策的话，那么可以选择检测虚拟机和拒绝虚拟环境使用软件这种方式。更常见的做法是将这种功能与并行网络许可组合起来（如前所述）以创建一个更可行的解决方案。

最后，如果想获得最高的保证水平，那么硬件密钥就是最佳选择，许可实施相关的信息会被保存在一个可信并且有保证的虚拟环境之外的位置。

结语

很显然虚拟化并非是一个短期跟风行为。目前虚拟化技术正处于发展初期。随着虚拟化技术的不断发展，想要分辨虚拟环境和真实环境之间的差异会日益困难。自动软件许可实施必须随虚拟化发展而发展，远程许可实施苗头的出现导致的虚拟化威胁让问题变得更加棘手。

幸运的是，目前有一些可供软件发布商使用的选项，通过使用这些选项，让虚拟化不再成为是收益损失或影响销售的原因，而是将其转变为一个机会。那些利用可用工具最快拥抱虚拟化的供应商会获得一个显著的区分优势，从竞争对手中脱颖而出。

在虚拟环境下许可的赛孚耐方式

赛孚耐意识到在企业机构内虚拟机（VM）的日益流行让软件供应商有能力在任何（对业务增长和持久发展来说重要的）虚拟环境内许可并控制其应用程序。

成功的软件管理不仅要求在虚拟环境下做出许可，也需要在应用程序部署到一台虚拟机之时就实施许可条款。如果没有这种实施的话，软件发布商对许可就没有控制力，从而也就不能保证其收益。

在任何虚拟环境下为应用程序提供许可的赛孚耐选项帮您实现以下功能：

- 通过避免虚拟环境下应用程序复制保护收益。
- 通过支持在虚拟环境下使用您的应用程序来减少混乱、确保新业务安全并提升竞争力。
- 通过虚拟环境许可和定价模型提高利润。

虽然硬件密钥仍然是避免软件在虚拟环境下被非法使用和分配的最有效方式，但是在某些情况下，这种方式是缺乏可操作性的。在赛孚耐发布虚拟机指纹识别解决方案之前，那些希望扩展其基于软件的许可实施以支持虚拟环境的软件供应商所能采用的方法是有限的：检测的虚拟机（VM）存在性，确定是否允许在虚拟环境下运行软件。而这是一套不完善的解决方案，授权后对应用程序没有任何控制力。

赛孚耐为他们提供了新的选择——通过业界第一个也是唯一一个技术不可知的虚拟机指纹识别解决方案让他们可以在任何虚拟环境下许可并控制软件。通过让软件供应商唯一锁定一个许可到一个虚拟机（就像其在传统许可情境的做法一样），赛孚耐技术可以保护其许可也就是其应用程序在任何终端用户环境（无论是否是虚拟环境）下免受复制或滥用。

赛孚耐是业界唯一一个为软件供应商提供基于软件和基于硬件的选项（以在任何虚拟化环境下许可应用程序）的软件许可和管理技术供应商。

- 通过避免虚拟环境下应用程序复制保护收益。
- 通过支持在虚拟环境下使用您的应用程序来减少混乱、确保新业务安全并提升竞争力。
- 通过虚拟环境许可和定价模型提高利润。

赛孚耐软件版权管理解决方案

Sentinel HASP®

Sentinel HASP（原名 Aladdin HASP SRM）是业界第一个也是唯一一个软件许可和安全解决方案，该方案可以使用基于软件或基于硬件的保护密钥实施软件保护和许可授权。

借助 Sentinel HASP，您可以通过保护您的软件免遭盗版和知识产权偷窃从而提高您的收益，应用富有创造性的商业模式来提高价值并让您的产品从市场上脱颖而出。

Sentinel HASP 能够与您现有的软件产品生命周期完全整合在一起以最大程度减少对开发和商业流程的干扰。Sentinel HASP 具有适合开发人员、产品经理、订单处理和生产的易用的基于角色的工具，可以确保员工快速上手，优化员工工作时间，提高核心竞争力，确保产品快速上市并及时响应不断变化的市场需求。

要下载一份免费的 Sentinel HASP 开发员套件，请访问：
http://www3.safenet-inc.com/Special/hasp/safenet-hasp-srm-order/default/asp。

Sentinel RMS®

Sentinel RMS 是一套强效许可应用和实施解决方案，该方案可以为软件供应商和技术供应商提供对其应用程序部署和使用方式的控制力和可见性。Sentinel RMS 关注于可扩展且灵活的许可管理，是在中型和大型企业环境下部署应用程序的理想选择。

Sentinel RMS 的部署可以提供对软件许可协议的固定连接，从而实施条款和条件，通过这些条款和条件您可以管理您的产品。除了可以降低盗版风险之外，Sentinel RMS 让您可以提供多种许可模式，灵活地定价并打包您的产品。

当与 Sentinel EMS（赛孚耐公司导向型基于网络的管理系统产品）组合使用时，Sentinel RMS 可以提供一个许可管理和实施的完整解决方案。Sentinel RMS 是由业界领先的企业软件供应商和高技术设备制造商共同部署的。

LicensingLive!™ (lahy'sun sing lahyv'), adj. n. [SAFENET, INTERACTIVE] 1.立即方案与软件打包、定价、实施、交付和管理相关的最佳实践和新兴挑战。2. 一个将软件供应商、行业分析师、许可顾问和技术供应商组织在一起的论坛。

赛孚耐 Sentinel 软件货币化解决方案

赛孚耐在为全球的软件和技术供应商提供创新且稳定的软件许可和版权管理解决方案方面拥有 25 年之多的从业经验。公司的 Sentinel®软件货币化解决方案易于整合和使用，具有创新性并且是专注于功能的，该方案设计用于满足任何公司（机构）的独特许可实施、强化和管理需求，而无论公司（机构）有怎样的规模、技术要求或组织结构，均能满足其需求。只有选择赛孚耐产品，客户才能解决其所有的反盗版、IP 保护、许可实施和许可管理难题，同时提高整体盈利性、改善内部运行、保持具有竞争力的市场位置，同时改进其与客户和终端用户的关系。赛孚耐一直以来都不断适应新要求并不断推出新技术以满足不断发展的市场需求。赛孚耐遍及全球的 25,000 多名客户都深知选择了 Sentinel 就等于选择了在当今和未来不断实现业务成长的自由。

欲了解有关赛孚耐的软件货币化解决方案完整产品组合的安装、内置和云应用程序的详细信息或要下载一份我们屡获奖励产品的免费评估版，请访问：www.safenet-inc.com/sentinel。

加入对话

Sentinel Online
www.Safenet-inc.com/sentinel

LicensingLive!
www.LicensingLive.com

Twitter
http://twitter.com/#!/LicensingLive

LinkedIn
http://bit.ly/LinkedInLicensingLive

YouTube
http://www.youtube.com/user/LicensingLive

BrightTalk
http://www.brighttalk.com/channel/5572

*企业终端用户调查 2010 年 9 月 ,赛孚耐委托一家第三方公司 Vanson Bourne 在美国调查了 300 名高级 IT 决策者（一般是首席技术官或相当职位）, 通常是公司（机构）内 IT 部门的领导。受访者行业分布在金融业、RDT（零售、分销和运输）、公共部门、制造业和其他商业部门。Vanson Bourne 于 2010 年 4 月在欧洲和亚洲地区完成了相同的调查。

联系我们：欲了解所有办事处地址和联系人信息，请访问：www.safenet-inc.com。
关注我们：www.safenet-inc.com/connected。