如何应对虚拟机蔓延？

如何应对虚拟机蔓延？

虚拟机易于创建，反应速度快，所消耗的硬件资源也非常有限，这必然会导致虚拟机的蔓延。该如何解决呢？本期虚拟化技术手册从虚拟机蔓延的原因入手，介绍能阻止虚拟机蔓延的部署方法与工具，并且从宏观方面描述高可用性架构与虚拟机蔓延之间的紧密关系。

虚拟机蔓延原因

当你需要对生产环境进行复制来测试一个新应用的部署时，你只需创建一个虚拟机即可，耗时仅仅几秒钟。但是，这项工作完成之后，那台虚拟机该如何处理？

- **虚拟机蔓延问题产生的根源及其影响**
- **虚拟化部署半途遇阻的三大原因**

预防虚拟机蔓延

虚拟化技术带来的蔓延对其所带来的优势大打折扣。如何知道环境中虚拟机蔓延的信号？那该如何抑制？使用什么的管理与工具？

- **分析：虚拟化技术蔓延的五大警告信号**
- **虚拟机蔓延如何抑制？**
- **虚拟机蔓延？使用服务器容量规划与生命周期管理**

虚拟机蔓延与高可用

如果你的架构中的高可用性部署得适当，那么就会对虚拟机蔓延问题有大大的缓解作用。高可用集群是什么？如何检查高可用计划以及部署时要考虑哪些问题？本部分为您做出解答。

- 数据中心高可用规划考虑的问题
- 虚拟数据中心中的高可用集群简介
- 虚拟化高可用检查清单

虚拟机蔓延问题产生的根源及其影响

虚拟机易于创建，反应速度快，所消耗的硬件资源也非常有限，这必然会导致虚拟机的蔓延。当你需要对生产环境进行复制来测试一个新应用的部署时，你只需创建一个虚拟机即可，耗时仅仅几秒钟。但是，这项工作完成之后，那台虚拟机该如何处理？它可能会处于你物理基础设施的某一个硬盘上，很容易会被遗忘，但它还会继续消耗相应的存储和计算资源，却没有产生任何回报，这也就是虚拟机的蔓延问题。不幸的是，广大管理人员并没有意识到这一问题的存在。

创建一个虚拟机很容易，这往往会导致虚拟机在系统内的泛滥。如果把这些虚拟机都加起来，对你所在企业或机构而言不是一个小数目。Embotics 发表的一份名为《详解虚拟机蔓延》的白皮书中介绍到，“在一个拥有 150 台虚拟机的环境中，会因为虚拟机的泛滥而浪费 50000 到 15000 美元的成本。”

事实上，虚拟机的泛滥是不可避免的。但问题的关键在于，管理人员会把过多的注意力放在一些独立系统的管理上，而忽略了整个 IT 环境的“健康”。此外，他们并没有意识到虚拟机蔓延这一问题的严重性。（《虚拟机蔓延如何抑制？》）

最为不幸的是，这已经形成了一种恶性循环。一旦关键关键任务完成之后，管理员们就有可能会对其管理任务进行重新排序，从而忽略一些边缘设备。他们会把更多的注意力放在仍在运行中的虚拟机上，而让那些旧的、不再使用的虚拟机陷入无人管理的局面。尽管说这样做可以减少他们的日常系统管理工作量，但旧的虚拟机仍然会消耗物理和财务资源。对于那些不再使用的虚拟机而言，即便是将其关闭，也或许还会有相应的软件许可、技术支持等成本产生。要知道，非生产性的计算资源和软件许可也会给企业带来很大的负担。

实际上，这种浪费状况很容易遭到恶化。管理人员提供的虚拟机数量经常会超出实际需求。不论面对什么业务需求和目的，他们提供的都是固定内存、存储和处理器核的虚拟机配置。此外，在进行快照备份时，他们也需要耗费过多的时间和存储资源来对多余的虚拟机进行保护。

（作者：Brian Proffit 译者：王霆 来源：TechTarget 中国）

原文标题：虚拟机蔓延问题产生的根源及其影响

原文链接：http://www.searchdatacenter.com.cn/showcontent_43026.htm

虚拟化部署半途遇阻的三大原因

随着组织越加深入他们的服务器虚拟化部署，许多人都遇到了常见的绊脚石。

一些应用厂商飞般逃离虚拟化。一些厂商仍当鸵鸟埋头沙里，不支持虚拟化。一些工作负载还难以被虚拟。

这种现象——当你实施虚拟化碰壁时——被称为“虚拟化拖延”或“VM stall”。

拖延会在任何时间袭击，并且会在虚拟化部署过程中发生多次。（在我的经验中，虚拟化拖延通常在组织达到 30%虚拟化时首次发生。）许多因素会导致其发生，我会在下面介绍几个常见的原因。

没有虚拟化实施计划

“如果你不知道目的地，那就算玩完了。”

但谈到虚拟化，就是说你要真正虚拟。但你开始部署虚拟化时，在哪设置目标？你的虚拟化项目会比计划走得更远么？

预先规划你的组织使用虚拟化想要走多远很关键。每个组织必须定义一个目标满足自身的唯一要求。一旦设置好目标，你必须经常测量进程，不要让日常工作阻碍目标。

虚拟化实施不受支持

组织不受支持也会导致虚拟化拖延。

许多组织努力开始有机增长，在 IT 部门的小团队内。随着技术的成成熟，发展加快并成为 IT 架构的一部分。

这种自下而上的模式在早期很有利，但自上而下的支持是任何大型虚拟化部署的关键因素。当 CIO 也参与此项目，许多难题就能迎刃而解。

虚拟机蔓延

虚拟机蔓延也是造成虚拟化拖延的常见因素。

虚拟化拖延并不意味着虚拟机创建停止。它意味着组织停止了虚拟物理服务器的进程。不需要虚拟任何物理服务器就能快速配置新虚拟机。事实上，这种不受控制的增长会消耗资源，不能让更多物理服务器工作负载转换成虚拟机。

如果你遇到虚拟化拖延，那么是时候重新审核你的虚拟化部署目标和策略。确保所有动作都是朝共同的、清晰的既定策略前进，高级管理层提供必需的方针和远见。最后，保护资源。它们不是免费的，项目的成功取决于对它们的成功管理。

(作者：Mark Vaughn 译者：唐琼瑶来源：TechTarget 中国)

原文标题：虚拟化部署半途遇阻的三大原因

原文链接：http://www.searchvirtual.com.cn/showcontent_44197.htm

分析：虚拟化技术蔓延的五大警告信号

虚拟化技术带来的蔓延对其所带来的优势（其中包括费用节省、高效运作和整合）大打折扣。虚拟化是对基础设施如何构架、提供、管理和运行的根本性改变，但是虚拟机（VM：Virtual Machine） 蔓延却在这些方面带来了更大的虚拟化基础架构问题。在本文中，TechTarget 中国的特约虚拟化专家 Rick Vanover 将解释虚拟化蔓延现象以及如何防止此类问题发生。

什么是虚拟化技术蔓延？

当一个网络上的虚拟机达到一定数量，管理员不能够有效地管理时，我们就称之为虚拟化蔓延。虽然虚拟机蔓延警告信号可以修改，但是仅仅一个故障现象并不能够足以标识出现蔓延。

但是标识出这些故障现象可以防止以后出现虚拟机蔓延问题，下面给出的是一些虚拟基础架构问题的常见警告信号。

虚拟蔓延故障现象 No. 1：缺少策略

在管理虚拟机配置方面一致性的不力是虚拟化蔓延的一个主要因素。在大多数情况下，很多操作系统在诸如管理的权限、加密设置、反病毒或者恶意软件保护以及网络设置方面都要求有一致性配置。简化这些问题会给物理基础架构带来问题，也会带来更大的虚拟化基础架构问题。

动态目录（AD：Active Directory）是辅助集中化这些配置的核心技术。AD 允许对计算机和用户账号进行粒度控制策略，也可以集中化管理如何在基础架构中部署一个操作系统（物理的或者是虚拟的）。

定义良好的 AD 准则可以防止以下的一些问题，如分散的管理权限制定、不一致的反病毒软件安装和配置、核心服务的非一致性加密设置和虚拟机中没有必要的运行程序等。

虚拟蔓延故障现象 No.2：无法管理的更新

如果每个月的第二个星期二都需要手忙脚乱地打微软补丁，那么如果先前没有规划，在虚拟基础架构中就无法顺利完成打补丁。

几乎所有的虚拟化技术部署都可以减少物理设备的数量，但增加的是操作系统的安装。因此，例如，这些情况在系统的数量加倍之后是是如何影响手动打补丁和更新系统的？在很多情况下，在一个快速增长的基础架构上手动完成 Windows 更新扫描和升级，这些问题很快地就变得无法管理。

然而一个经过良好规划的方法不会要求管理员时刻在线。诸如微软系统中心和 Symantec 的 Altiris 的工具都可以按照策略和进度集中化地在虚拟机（或者物理机）上进行更新。尽管这些产品不是免费的，但毕竟是便宜、并且不复杂的可用工具。

一个方案是通过组策略使 Windows 更新自动运行，其中包括定义检查自动更新的配置，如通过注册表或者计划任务。每一台虚拟机都可以配置为自动更新，但是这种方法缺少集中化配置推动。

虚拟蔓延故障现象 No.3：无法管理的清单

如果没有优化清单管理实施方案，虚拟化带来的必定是噩梦。例如购买物理服务器的场景，在实施虚拟化之前，很多 IT 组都用一到两个工作人员负责管理采购设备。然而部署虚拟化之后，通常情况下却需要更多的管理员许可才可以创建虚拟机，但是未必每一个人都采用同一种方式协调清单。如果在没有很好定义策略的情况下实施，最终可能就会被不断增加的清单所淹没。

有一些可用的免费工具可以辅助应对虚拟化清单问题，如 VMware 工作环境中有 Embotics 的 V-Scout 和 VKernel 的 SearchMyVM。虽然这些产品的功能各不相同，但是每一个都可以弥补动态增长虚拟基础架构中的可见性缺口。

虚拟蔓延故障现象 No.4：许可证符合性和费用

如果虚拟机增长的数量超过预期，许可和分配数字可能就会有风险。没有人希望在正常运行期间服务器的软件许可清单出现问题，或者是因为虚拟许可证超期而停止运行。虚拟机具有快速和容易的特性，但是并不免费。解决许可和分配问题最好的方案之一就是优化每台虚拟机的费用结构（或者是分配费用）。在很多情况下，就意味着会出现如下情况：

- **虚拟基础架构的一部分**：这表示目标整合率被主机费用切分。例如，如果起初的规划是 15：1 的整合率，并且一个虚拟化主机的存储费用是 30000 美元；服务器硬件和虚拟化管理部分的费用应该是 2000 美元；

- **操作系统许可**：虚拟机克隆、模板和其它特点可以快速地实现操作系统部署，但是许可证费用仍然存在，把平均操作系统的费用作为最常见的版本。当然也可以考虑为 Windows 数据中心版提供的无限的虚拟化授权。
- **管理软件**：如果在打补丁工具、反病毒软件、符合型协议、备份软件代理以及其它原因上存在相关的客户费用，则这些费用就需要增加在基础架构费用上。

虚拟化技术可以节省费用，但是需要优化费用模型。一个清晰定义的费用模型可以防止虚拟机蔓延（这个问题可以带来财务方面的影响）。另外利用这次机会也可以消除错误认识（虚拟基础架构中的虚拟机是免费的）。

虚拟蔓延故障现象 No.5：过多的系统需要备份

如果虚拟工作环境增长太快以至于备份基础设施无法保护工作负载的话，就可能带来潜在的灾难。在这样的情况下就需要标识出需要备份的数据。如果虚拟机上运行的是部署在企业内部的 Windows 服务，并且管理员非常熟悉安装流程，那么相对于浪费一定的时间存储空间保护该系统而言，从模板重建的方案要好一点。另外，如果需要备份系统，可能就会增加保护困难。一个可能的解决方案就是：一个供应许可程序和费用模型可以减小基础架构增长。

发现上述 5 个虚拟机蔓延故障现象后，最好马上采取行动。在规划阶段，尽量在虚拟化工作环境实施之前处理这些问题以及其它基础架构问题。采用全面的策略和良好定义的费用模型可以防止企业数据中心中出现虚拟化蔓延问题。

（作者：Rick Vanover 译者：王越 来源：TechTarget 中国）

原文标题：分析：虚拟化技术蔓延的五大警告信号
原文链接：http://www.searchvirtual.com.cn/showcontent_29652.htm

虚拟机蔓延如何抑制？

你做了许多准备，并计划通过虚拟化 40 台服务器节约大量资金，但几个月后，你只虚拟了其中的 20 台，就耗尽资源了。更糟的是，你没哟达到当初计划的节约。你的资源都去哪了呢？这其中出了什么问题呢？

因为发生了虚拟机蔓延。

向虚拟化的转变造成了戏剧性变化，很大程度上降低了采购新服务器资源的复杂性和精力。在没出现虚拟化之前，购买一台服务器如同在大商店里购买大型家用电器。很浪费钱，并且需要额外付费以运输与安装。而虚拟服务器，如同一包口香糖，廉价并且易于购买。

因此，服务器资源变成许多项目里后来添加的东西。人们在最后一刻才想到虚拟服务器，如同突然想到口香糖。有些人甚至需要第二包，因为他们后来还需要。

由于虚拟化使得服务器购买过程变得流线化，它是开放的。人们卸载了陈年以来压抑的想购买服务器的欲望，导致虚拟架构的规模超出了原先的设计，即虚拟机蔓延。

什么是虚拟机蔓延

起初你可能没注意到虚拟机蔓延。直到资源耗尽你才意识到存在这个现象。由于人们不用担心以前进行服务器购买需要担负的资金与运营责任，他们在虚拟环境似乎“肆无忌惮”了。

当然，你让上司了解到虚拟化的价值是件好事，但是必须对这项技术负责。否则，你要一直与虚拟机蔓延作斗争。要使原来的虚拟机项目回到正轨，让架构稳定，你必须保持理智，进行实践，鼓励合理规划的资源分配。

必须为运行着的项目预留资源，或者至少制作一个计划表在需要的使用进行资源补充。需要明白创建一台虚拟机的影响，事先能预测资源的使用率。问自己“将 X 那么多的资源分配给 Y 会对现有项目计划有何影响？”

当你重新掌控了资源消耗的权利，你的虚拟架构就能如愿成为有价值的资产。

（作者：Mark Vaughn 译者：唐琼瑶 来源：TechTarget 中国）

原文标题：虚拟机蔓延如何抑制？
原文链接：http://www.searchvirtual.com.cn/showcontent_42844.htm

虚拟机蔓延？使用服务器容量规划与生命周期管理

虚拟化并不是一蹴而就的，随着时间推移，虚拟化就会出现各种问题，就算看起来运行得很正常。

例如，虚拟机不受控制的增长就造成虚拟机蔓延，会逐步消耗来自服务器的剩余处理能力。虚拟机蔓延会降低其他虚拟机的性能，导致未知的崩溃，并阻止虚拟机从其他受影响的服务器进行正确的故障转移。给底层虚拟化平台升级或打补丁也会对性能和稳定性造成未知的结果。

因此，管理员必须积极主动地预防虚拟机蔓延，以及可能出现的其他问题。下面我们分享一些最佳实践。

虚拟化生命周期管理以及性能监控

虚拟化生命周期管理是有助于管理虚拟机的一种策略，确保只有授权的管理员能够创建所需的虚拟机，这些虚拟机能激活使用，并且最终能删除以释放计算资源给其他虚拟机。

性能监控能够根据有形因素计算资源利用率，比如网络带宽、磁盘 I/O 和 CPU 使用。追踪随着时间的推移，资源负载趋势能够标注出潜在的需要进行研究的故障点。几乎所有的性能监控工具都包括 email/SNMP 陷阱，当关键资源超出设置参数时会发生警报。识别资源使用里的瞬间警告转移能够较早发出警告，这对于快速做出决定是必要的，更能最小化产生环境的损失。

“在终端用户知道之前你应该发现问题，”First Flight Federal Credit Union 首席运营官 Todd Erickson 说。

服务器容量规划与归档

正在进行的性能监控对于实际的服务器容量规划也很必要。通过观察趋势，管理员能对未来升级做出预测，以适应业务的长期增长。

“在虚拟环境里作的容量规划越多，你就会发现这不是物理设置，”IBusiness Network LLC 技术服务经理 Ty Hacker 说。

服务器容量规划更好，花费也不贵，所以不过不做规划在达到危险级别时就会损失性能。

彻底预防虚拟化问题的最后一个元素是精确的、精心维护的存档。出现在虚拟设置里的大量细节非常容易忘记。所以要记录支持文档，确保你的修复、升级和提升进展顺利。

（作者：Stephen J. Bigelow 译者：唐琼瑶 来源：TechTarget 中国）

原文标题：虚拟机蔓延？使用服务器容量规划与生命周期管理
原文链接：http://www.searchvirtual.com.cn/showcontent_43272.htm

数据中心高可用规划考虑的问题

尽管服务器虚拟化已经在扩展性方面提供很多便利，但是在虚拟环境中部署高可用之前，还是很有必要对数据中心做一些规划。

通过使用如 Marathon Technologies 公司的 everRunVM 软件，虚拟机可以很快地部署高可用环境并从中获益，但是如果可以结合 VMware 的 DRS(Distributed Resource Scheduler)和 VMotion 来使用的话，第三方软件的功能可以获得极大的增强。

尽管大家都清楚部署高可用对企业而言一定是可以获益的，但是 IT 部门在进行部署之前，仍很有必要进行数据中心的相关规划。例如，考虑一下业务相关因素以及可能会遇到的一些技术方面的障碍。

“您需要明确您想如何建立高可用的系统环境，” Silverton Consulting Inc.公司（这是一家独立的，位于 Broomfield 的技术顾问公司）创建者及总裁 Ray Lucchesi 先生这样说，“这里涉及一些很复杂的问题可能会成为执行中的障碍。”

高可用数据中心规划流程

首先，应用程序本身需要衡量。很多企业自身的遗产或内部的开发程序都是非常关键的业务，但是他们并不支持传统的高可用集群方式。如果把这些应用迁移到虚拟化环境中，借助 everRunVM 或 VMware 的 DRS 就可以在容错性能方面获得大幅地提升。

在高可用数据中心规划过程中，管理者需要反复考虑到物理服务器的冗余问题。在传统的非虚拟化 HA 环境中，相对地两台普通物理服务器一般只运行相同的操作系统及应用程序。例如，在建设数据中心的时候，可能包含了两台冗余的 Exchange 2003 服务器。

在这种情况下，也可能我们虚拟化这两台服务器时，仍然采用 1：1 的配对方式。但是大多数情况不会这么做，一台虚拟主机通常会整合多台虚拟机。这样做的结果就是，物理服务器资源（如 CPU、内存、I/O 和网络资源等）都必须能够提供足够支持一定数量寄居虚拟机的运算能力。

对于运行有多个冗余虚拟机的集群服务器而言，保留适当的空间显得不是那么的重要，因为集群中还有另外一台服务器已经运行了一个或多个虚拟机的副本。不会有额外的需要从存储中装载的虚拟机。专家们注意到如果在可以满足相应的电源和散热方面需求的条件下，对于虚拟化而言，刀片服务器和独立的普通服务器效果是一样的。

高可用数据中心规划的考量

但是对于没有做集群的虚拟机而言，需要保留足够的空闲资源以满足从其他服务器上发生故障时切换过来的虚拟机运行需求。这部分保留资源确保了没有在 HA 工具管理下的虚拟机可以获得高可用性的保护，但是这个前提是 IT 管理员已经提前制定好故障切换计划。

“您需要同时保留硬件和 hypervisor 管理程序资源，以便于当某些特定的物理硬件失效后，hypervisor 管理工具可以知道把这些虚拟机安放到什么地方。”Evolve Technologies 公司 CEO Dave Sobel 这样说道。

管理员们经常忽略这种对数据中心的规划。而是通过允许虚拟化软件自动选择故障后可以切换到的目标地址，这种方式可能会引起未知的资源短缺问题。然后，这种短缺会导致接收了故障切换虚拟机的服务器上，所运行的虚拟机出现严重性能影响或者其应用崩溃的情况出现。避免这种潜在的资源短缺的方法之一，就是指定一台或多台传统服务器平台用于故障发生后的切换。

数据中心的管理员为了加强应用程序的高可用性（更多的是为了降低风险），通常考虑把虚拟机分发到不同的物理服务器上实现负载均衡。通常，他们会尽量避免把多个关键业务虚拟机放置到同一台物理服务器上。例如，假设我们在整合时把 Exchange 虚拟机和 SQL 虚拟机放在了一台物理服务器上。那么当这两台虚拟机需要迁移到集群中备用的服务器时，它们是不是仍然高可用就要取决于备用服务器资源是否可以支持他们的同时运行。

很多公司为了加强高可用性，如前例中，选择把 Exchange 虚拟机放到服务器 A 上，把 SQL 虚拟机放到服务器 B 上，然后选择集群中的第三台服务器作为这两台虚拟机的备用机。这种方式下，如果服务器 A 上的 Exchange 虚拟机宕机，Exchange 服务仍然可以在第三台服务器上启用，而且第二台服务器上 SQL 虚拟机运行不会受到任何影响。这样，所有的服务都可以继续正常运行。

数据中心高可用的趋势

虚拟化的引入使得数据中心高可用和容灾方案之间的界限越来越模糊。在虚拟化环境下，之前动辄花费数小时的数据保护和恢复任务现在只需要几分钟时间。

“之前需要通过 HA 来实现的，现在可能通过严格的容灾技术来实现，”Sobel 这样说，“HA 和容灾之间的界限是由每个单位自己来定义的，然而事实上它们可能是同一种东西，区别仅在于实现的时间长短上。”

Sobel 还补充道，HA 和容灾并不是互斥的，在虚拟化环境中它们甚至可以轻易地融合在一起。虚拟化同时也降低了 HA 和容灾的实现成本，使得数据中心管理员可以通过某种方式，为更多地应用提供低成本的数据保护方案，而这些在几年前可能是根本无法想象的。

短期看来，激烈的竞争似乎在不断推动虚拟化特性和功能的发展。微软在 Windows Server 2008 R2 操作系统中绑定了 Hyper-V R2 和更多的虚拟化特性，而 Citrix 则宣布其企业级产品 XenServer 5 开源。

从长期看，Lucchesi 指出，云计算和软件即服务应用的兴起使得高可用的实现更加地抽象化。

“这是一种对应用模式的重建，”他说，在加入云基础架构后，应用实现了从特定服务器上的脱离，“一旦应用被放到云里，那么它在 HA 方面的灵活性发生了难以想象的转变。”

把一个应用放到云里去并不容易，可能现有的某些应用也并不适合这么做。不过 Lucchesi 说，他希望高可用最终可以被云支持并成为现实。

（作者：Stephen J. Bigelow 译者：李哲贤 来源：TechTarget 中国）

原文标题：数据中心高可用规划考虑的问题
原文链接：http://www.searchvirtual.com.cn/showcontent_32822.htm

虚拟数据中心中的高可用集群简介

服务器虚拟化技术在数据中心内代替传统的高可用集群的方式如何？但是在实际工作中，典型的服务器集群架构和虚拟化的服务器工作性能相差不大，只有一些细微的差异。

高可用性集群给虚拟化带来的灵活性

首先，虚拟化技术可以在服务器的选择上提供更大的灵活性。这个软件抽象层（或者就是 Hypervisor）可以支持承载操作系统和应用程序的虚拟机实例（虚拟机实例可以从底层硬件资源相隔离），尽管功能强大、高可靠性的服务器在虚拟服务器工作环境中依然是必需的。两者并不需要完全相同，数据存储的方式也可以不同。非虚拟化的服务器可能通过 SAN——甚至是一个冗余的 SAN——读取数据，但是操作系统和应用程序却本地配置在每一个给定的服务器上。这样做给那些非虚拟化服务器带来了更多传统的备份需求。

相比而言，每一个虚拟机镜像实质上就是一个单独的数据文件，这个数据文件可以存储在本地，但是更多的情况下都是存储在 SAN 上。虚拟机在所运行的服务器上从 SAN 装载到内存中。通过定期的或者连续的虚拟机快照备份进程可以轻松地保护每一台虚拟机，该进程可以从服务器内存到 SAN 更新虚拟机镜像。

虚拟机可以从一个 SAN 备份到另外一个位置或者存储系统，不需要服务器 I/O 装载常规性的协助传统备份。一台意料之外运行在出现故障的服务器上的虚拟机可以在几分钟之内从一个 SAN 上装载到另外一个可用服务器上。这个新服务器可能是高可用性集群的一部分，但是也可能是一个常规服务器，只是有足够的计算资源才可以运行该虚拟机。

另外一个不同就是在虚拟机之间的安全通信，一般情况都是通过虚拟 LAN 或者 VLAN 技术进行处理。

高可用集群工具

当前的虚拟化工具可以很容易的配合传统的 HA 方法。在企业需要零宕机时间的要求中，虚拟服务器可以使用基于虚拟化的容错虚拟机工具（如 Marathon 技术公司的 everRunVM），该工具运行在服务器集群中每一成员服务器的虚拟化管理程序（如 Citrix XenServer）之上。HA 软件配置用来处理选择的虚拟机，这些虚拟机在高可用集群中可以很快地被复制到其它服务器上并且可以实时同步。在由于崩

溃或者服务器故障时虚拟机停止响应的情况下，虚拟机复制操作可以在另外一台服务器上继续进行。在原来的服务器恢复之后，应用程序控制重新指向原虚拟机。

例如，假设一台负载 SQL 服务器的虚拟机和一台负载企业资源规划（ERP：Enterprise Resource Planning）应用程序的虚拟机同时运行在服务器 A 上；在服务器 B 上运行三台虚拟机，其中一台承载 Exchange 服务器，另外一台作为域名服务器，在第三台上运行客户关系管理应用程序。
一般来说，这些服务器不能用来容错，因为每一台虚拟机都没有复制。但是 IT 管理员可以使用诸如 everRunVM 这样的工具在服务器 A 和服务器 B 之间复制 SQL 虚拟机。另外也可以在集群中新增第三台冗余服务器，只用来宿主从服务器 A 上复制的 SQL 备份，以及从服务器 B 上复制的 Exchanges 虚拟机备份等。

但是实际上虚拟化技术并没有使 HA 比使用传统的方法更高效。在虚拟机宕机备份中，使用诸如 everRunVM 这样的工具可以保证宕机时间是可以忽略不计的。但是可供虚拟化技术使用的软件工具的灵活性和功能不仅仅是对第二级应用程序的有效数据保护，这些应用程序如果在传统的工作环境中可能只是使用常规的磁带存储方法。

数据中心管理器并不需要复制每一台虚拟机，因为这是服务器虚拟化的主要优势之一。没有即时复制的虚拟机仍然可以通过持续快照，也可以使用一些工具（如 VMware 高可用性）从 SAN 移植到其它可用的服务器上而快速启动。

回顾上一个例子，只有服务器 A 上面的 SQL 应用程序为冗余备份复制到服务器 B 上。服务器 A 上的 ERP 应用程序并没有复制。通常来讲，这就意味着需要定期备份或者快照保护 ERP 虚拟机。相关的长恢复点对象（RPO：Recovery Point Objective，每两次备份之间的时间更长）在断电情况下将会给更多的数据带来风险。

中心化 SAN 上的 ERP 和其它虚拟机就有可能从服务器上维持每一台虚拟机的持续快照，把 RPO（以及潜在的数据损失）减小到几乎为零。如果服务器 A 出现故障，ERP 虚拟机可以从 SAN 恢复到另外一台有足够可用计算能力支持虚拟机的服务器上。大概只会引起几分钟的 ERP 应用程序不可访问，这对于一个企业来讲是完全可以接受的。因此在提升其它应用程序的可恢复性时，虚拟化可以继续支持高可用性。

高可用性下的虚拟服务器维护

虚拟化技术也可以支持常规维护这样的任务。在传统的高可用性集群中，常规维护通常就是指使集群中的一台服务器脱机服务，而让其它服务器处于高风险状

态，直到另外一台服务器启动并且重新同步。如果应用程序没有得到 HA 的保护，该服务器就会持续保持脱机状态一直到该服务器正常运行。

在虚拟化的工作环境中，底层硬件维护时可以使用工具，如 Windows Server 2008 R2 的部分组件 Microsoft Hyper-V 动态迁移，或者 VMware VMotion 和分布的资源调度器（DRS：Distributed Resource Schedule），把虚拟机导向其它可用的服务器上以维持应用程序的可用性。在从传统部署向虚拟化服务器部署转换的这个过程中，数据中心管理器最大的挑战就是为每一个应用程序实施最恰当的保护级别。

以公司内部使用的 FTP 服务器虚拟机为例：通常情况下使用 everRunVM 这样的工具复制虚拟机并不合适，因为这样做会因为非关键目标耗费大量的计算资源。考虑花几分钟时间在另外一台服务器上启动该虚拟机将会是更明智的选择。

（作者：Stephen J. Bigelow 译者：王越 来源：TechTarget 中国）

原文标题：虚拟数据中心中的高可用集群简介
原文链接：http://www.searchvirtual.com.cn/showcontent_32782.htm

虚拟化高可用检查清单

如果配置正确的话，虚拟化高可用（HA：High Availability）组合可以在数据中心的效率和可靠性方面发挥卓越的效果。

但是，如果规划不合理的话则将会导致一系列问题。高可用的数据中心规划和了解问题所在都可以很好地辅助解决问题。使用这个虚拟化高可用检查清单来确保数据中心高可用性成功部署：

确定准备做镜像的虚拟机：服务器集群的成员服务器很有可能会负载各种各样的虚拟机，因此应该确定这些服务器上需要通过镜像进行保护的虚拟机和那些非关键的、不需要保护的虚拟机。但是如果只需要两三分钟就可以在另外一台服务器上恢复虚拟机的话，复制虚拟机的价值就不是很大了。

考虑虚拟计算资源：每一台虚拟机都需要 CPU、RAM、I/O 和网络连接等资源，因此需要在每台服务器的可用计算能力之间指定和平衡这些工作负载。确保考虑到了因复制、镜像虚拟机或者宕机备份而需要的新增计算资源。

评估故障的单点：回顾虚拟机集群架构以及考察故障单点，比如一个存储区域网络、LAN 转换器或者单个存储系统。小型公司可能会因费用问题放弃新增冗余备份，但是大型公司需要尽量减小对关键应用程序可用性的任何威胁。

选择虚拟机镜像软件：镜像文件必须能够和每一台服务器上的虚拟化管理程序以及需要保护的应用程序进行无障碍交互。例如，Marathon 软件公司的 everRunVM 可以保护 Exchange、SQL、SharePoint 和 Blackberry 服务，并且与 Citrix 系统公司的 XenServer 完全兼容。

定期测试宕机备份和故障自动恢复：测试和部署之后，通过定期测试镜像虚拟机的宕机备份和故障自动恢复行为来验证 HA 的准备状态非常重要。触发方式非常简单，比如断开一台服务器的网线，验证镜像虚拟机是否会在另外一台服务器上运行以维持应用程序的可用性，而不带来任何中断。

在备份方案中维护虚拟化高可用：使用 HA 保护虚拟机通常被看作是一种数据恢复的形式，但是甚至镜像虚拟机也需要和非镜像虚拟机一同备份。使用各种各样的软件工具可以从 SAN 中备份到其它存储设备或者脱机的站点位置。

（作者：SearchServerVirtualization.com 译者：王越 来源：TechTarget 中国）

原文标题：虚拟化高可用检查清单
原文链接：http://www.searchvirtual.com.cn/showcontent_32932.htm