全基线上的企业服务迁移机制①

凌斯齐, 谭成翔

(同济大学 计算机科学与技术系, 上海 201804)

摘 要: 以大型企业服务器运维管理为背景, 基于安全体系中的“基线”概念, 提出了一种新的服务迁移机制. 将原有迁移过程分为两步: 先环境迁移, 再服务迁移. 环境迁移的过程依赖安全基线来完成, 其中包括基线的定制、转换、分发与部署几个步骤. 该迁移的优势在于业务与服务的前提条件不易遗漏, 运行环境得以保障. 同时, 可由一台计算机远程统一管理多台服务器的迁移, 操作简便. 在文章最后, 以微软安全基线为例, 详细介绍了本人实现的系统和基线转换的算法. 最终的实验结果证明是高效的、令人满意的.

关键词: 服务迁移; 环境迁移; 安全基线; 基线转换; 组策略对象

Mechanism of Enterprise’s Services Migration Based on Security Baselines

LING Si-Qi, TAN Cheng-Xiang

(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)

Abstract: This paper proposes a mechanism of services migration in the background of the operation management of large enterprises using the notion of “security baseline”. It splits the original migration into two parts. First, transport the environment on the server, which includes the custom, transform, distribution and deploy of baselines, and then the running services. By this way, the preconditions of the businesses and the services will not be omitted and the environment is guaranteed. Furthermore, it is of convenience that one can control multiple servers from one terminal. Finally, this paper introduces the realized system and the baseline transform algorithm in detail. The experiment result shows that the mechanism is high efficient and satisfactory.

Key words: services migration; environment migration; security baseline; baseline transform; GPO

服务迁移是将原服务器上的服务、应用、业务等迁移到目标服务器的过程. 企业的 IT 部门所面临的挑战是即要完成服务迁移又不会缺失、降低整个业务系统的数据与功能. 如何应对这种两难状况成为了企业运维管理的一大挑战. 随着信息化进程加速, 企业越来越向着面向服务的架构(Service-Oriented Architecture)发展[1], 特别是大型企业内包含大量服务器、工作站、业务站等基础设施, 几乎成为了服务的储藏库. 复杂的业务逻辑使这些高耦合的系统变得更加难以维护. 稍有不慎则可造成不良的安全事件, 影响甚至瘫痪整个业务流程. 因此, 需要有更高级、自动化的手段来管理服务的迁移, 保障前后的一致性、连续性和安全性等高标准需求.

虚拟化技术是管理服务器有利的手段之一, 通过在实体机上分割虚拟服务器, 分别管理不同的服务. 在迁移时, 可以将操作系统随服务一起拷贝. 文献[2]提出了一种针对高内存负荷的大型服务的跨网迁移方法, 着重于服务的连续性与独立性. 文献[3]介绍了服务在线迁移系统, 通过层次化请求过滤驱动模块产生与该时刻系统服务一致的即时快照, 并将其作为数据源发送给虚拟设备. 该方法着重于迁移状态一致性以及生产活动的独立性. 文献[4]提出了一种基于动态自适应模糊控制的调度方法, 自主调度资源来侦察或修复诸如负荷超载、低响应、失败等问题, 从而保证了服务迁移时的质量.

① 收稿时间:2012-09-24;收到修改稿时间:2012-11-10

但虚拟化技术并不是企业唯一的选择，仍有相当多的服务运行于真机之上，此时上述方法都无法解决问题. 文献[5]提出了一种以服务为中心，自上而下过程与自下而上过程相结合的面向服务架构迁移方法，将面向服务设计与分析方法和传统的软件再工程方法有机地结合. 该方法忽略的一点是：迁移前后系统运行环境并不一定是相同的，这可能会给服务器正常运行带来困难. 针对这一问题，本文借鉴虚拟化技术，将服务环境与服务同等对待. 以基线(Baseline)代表环境，通过基线中安全策略的统一部署和安全状态的实时监测，来保障环境的合规性和服务的有效性，提供标准支撑和自主可控的服务运行[6].

1 迁移方法总体设计

实施迁移时的企业环境如图 1 所示，为了减少管理复杂度，我们的迁移机制采用第三台服务器(迁移管理服务器)统一管理企业中所用服务器的迁移工作. 此时，内网中有以下三类服务器：原机、目标机和管理机. 管理机同时也可以是原机或者目标机.

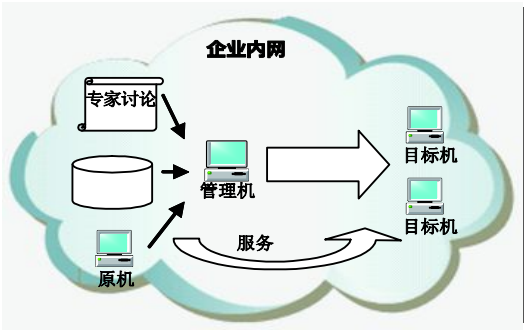

图 1 基于安全基线的迁移机制

方法中，将原始迁移分为两步. 第一步，迁移环境，将正确的环境设置导入到目标机上；第二步，原有服务迁移，这时可以结合其它现有的机制. 所谓的环境，特指用基线文件描述的安全配置项(CLS)和安全策略. 诸如：系统服务设置、网络的认证类型与相关协议配置、最小功能集与最小权限集设置、系统的完整性与默认设置、事件记录等等. 如何决定这些设置项的值，这需要 IT 管理人员了解系统之间的从属关系，根据实际情况，明确哪些是必须迁移的组件、哪些是系统中不需要的. 可以看到，新的方法需要额外的对于基线的操作，包括以下几个步骤：

① 定制：根据需求制定目标机应有的安全配置项. 其来源为三类：企业运营管理人员等专家讨论后的最终决定、知识库中存储的针对特定服务的历史记录、原机上直接导出的安全策略. 当来源出现矛盾时应该以专家的决定为准；

② 转换：基线文件往往是一类可读性比较强的初始配置清单，根据它来生成操作系统可识别的配置文件；

③ 分发：管理机将准备就绪的配置文件发送至目标机，文件与目标机是多对多的关系，一个文件可作用于多台计算机，一台计算机可配置多个文件；

④ 部署：将环境配置文件导入到目标机中，目标机重启后策略生效. 定制和分发工作都由管理机完成.

环境的迁移看似使整个过程变得复杂，但统一的远程管理带给我们诸多便利. 更重要的是，目标机上安全隐患可大大降低，保证了目标机的安全运行环境至少与原机相同甚至优于原机. 环境的迁移是本文的重点，将在下一章里作详细介绍.

2 环境迁移设计与实现

以微软操作系统为例，文献[6]详细介绍了对于 Windows Xp 系统的安全评估后得到其安全基线的过程. 本文中设计的系统针对更多的操作系统版本，包括 Server 2008、Server 2008 R2、Server 2003 以及其它非服务器版本. 各类基线包来自微软的官方下载，它是一类 cab 格式的数据压缩文件，包含一些说明文档、链接地址和 Xml 规则文件，并不能直接应用到计算机中. 关于配置项的核心内容存放于 Package.xml 文件中. 经转换后，可成为微软系统可识别的组策略对象(GPO)备份文件夹.

2.1 基线到组策略

首先介绍下配置文件的格式. 根据微软安全基线中不同的配置项，组策略对象备份文件夹可包含以下三类文件：

① Registry.pol 文件：该文件详细定义了用户或用户组的设置，包含了所有计算机、用户、用户组使用到的注册表中的信息；

② GptTmpl.inf 文件：该文件为 window 安全模板文件,功能包括：复制文件、删除文件、或重新命名文件、新增或删除注册表中的项目、修改重要的系统设置文件；

③ Audit.csv 文件：是一种通用的以逗号分隔的数据文件格式，该文件包含开启审计子系统的策略，包括哪些活动必须受到监视，哪些必须记录在安全事件日志当中.

图 2 为转换算法 SCMcabToGPO 的程序流程图(以下引号中的值均为 Xml 节点). 函数的输入为 Package.xml 文档地址和需要解析的基线名称, 输出为三种自定义的结构体. 循环遍历文件, 其根节点下包含多个“baseline”, 其下包含多个“settinggroup”, 这是一类设置的集合, 再其下又包含多条“setting”.

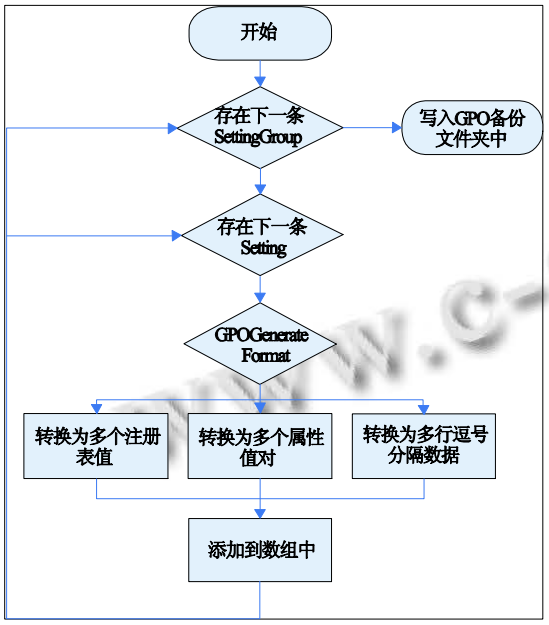

图 2　转换算法流程图

“setting”的 GPOGenerateFormat 属性值表明了该条设置的导出后的文件类型. 对该值进行判断, 分别对应不同的转换函数: SCMcabToPol、SCMcabToInf、SCMcabToCsv. 下面以转换注册表策略文件为例, 大致地介绍下 SCMcabToPol 算法:

① 以“setting”的 Id 属性为索引, 在“settinggroups”下找到相应的“check”, “check”由一条“settingrule”和可能的多条“optionrule”或“listoptionrule”组成, 每一条规则都与一条“注册表值”相对应. “注册表值”的主体包括: 注册表路径、注册表名称、数据类型、数据长度和数据本身.

② 转换“settingrule”, 关键在于得到数据. “setting”中的“valuemappingtable”是一个取值映射表, 记录着数据的名称与对应的值, 其中的 SelectedFriendlyName 属性表示当前选择的值, 与“check”中“value”的 ValueA 属性对应. 判断该值, “not configured”或“not defined”, 表示此条设置未被定义, 直接忽略; “disabled”, 在注册表名称前加上“**del.”, 表示删除该项设置; “enabled”, 获取该值.

③ 每当有一条“optionrule”或者一条“listoptionrule”时, 同样将其转换. 方法大致相同.

SCMcabToInf 与 SCMcabToCsv 实现另两种格式的转换, 将得到的三类数据结构写入到文件夹中指定的路径, 文件的名称和格式固定, 分别为: Registry.pol, GptTmpl.inf 和 Audit.csv. GPO 备份文件夹就形成了.

2.2 部署组策略

部署方法有两种: 一是自行部署三类策略文件. 打开 C:\Windows\System32\GroupPolicy 目录, 将子目录中的原始文件进行备份, 然后将生成的 Registry.pol 替换原文件, 使用 dos 命令行工具输入 gpupdate 命令进行策略刷新. 该命令的具体用法可以在 msdn 上获得. 部署 inf 文件, 可以在 MMC 控制台里添加“安全模板”和“安全配置分析”或者直接执行 secedit 命令, 将 inf 定义好的安全模板应用于计算机中. csv 文件需要使用域控制器进行部署.

另一种方式是使用微软提供的 LocalGPO 工具部署整个文件夹. LocalGPO 提供导入、导出 GPO 备份文件夹的命令. 本文的系统就是调用 LocalGPO 命令来完成策略部署的.

2.3 系统实现

图 3 为本人参与开发的安全基线管理系统. 采用 C/S 架构开发, 左图为服务器端主界面, 客户端为 Windows 服务, 不设界面. 主要的工作流程如下: 服务器端将安全基线转换为 GPO 并通过 Socket 分发给各客户端, 然后在客户端上进行部署, 最后把执行结果返回给服务端. 用户可以使用微软提供的各操作系统版本的标准模板, 也可以根据模板自定义基线. 定制模块如右图所示. 通过在企业内网中架设本系统, 可以顺利完成安全基线的迁移工作.

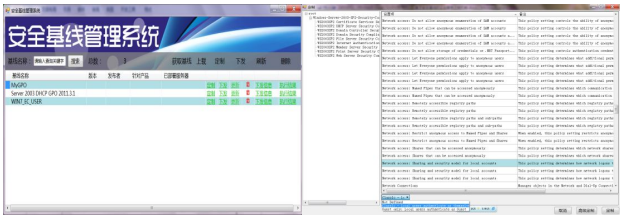

图 3　安全基线管理系统

3　文件服务实验与结果

本实验选取最为简单的文件服务进行迁移, 实验

对象为两台 Server 2003 服务器镜像(192.168.1.111 原机和 192.168.1.117 目标机)和一台 Server 2008 真机(192.168.1.102, 装有安全基线管理系统), 第三方工具 XCOPY. 实验开始前, 在原始文件服务器上“管理工具”的“管理您的服务器”中设置向导成功设置目录 C:\DocPool 为共享文件夹, 在其中添加共享文件.

先尝试直接服务迁移, 打开命令行工具, 输入命令: net uset: \\192.168.1.111\DocPool “key” /user: “name”. 将远程 ip 地址共享目录映射成本地 t 盘: Xcopy t:\ C:\SharedFiles /o /e /h /k. 将 t 盘上文件夹和其中子文件夹内所有文件复制到本地 C 盘 SharedFiles 共享文件夹下, 包括其属性、所有权和 ACL 信息(需要写权限). 尝试访问新的共享文件夹, 提示没有权限, 如图 4 所示. 经查证, 原因是目标机上的 guest 账号未开启访问权限. 事实上, 必须完成以下配置才能达到预期的效果:

① Server、Workstation 服务已开启(点击“开始”→运行→输入“services.msc”后回车打开服务管理窗口, 开启服务);

② 开启 guest 账号(电脑右键→管理→本地用户和组→用户→双击 Guest, 将“账户已停用”钩去掉确定);

③ 允许 guest 用户访问本机(控制面板→管理工具→本地安全策略→本地策略→用户权利指派里, “从网络访问此计算机”中加入 guest 账号, 而“拒绝从网络访问这台计算机”中删除 guest 账号);

④ 设置共享模式(控制面板→管理工具→本地安全策略→本地策略→安全选项里, 把“网络访问: 本地账号的共享和安全模式”设为“仅来宾-本地用户以来宾的身份验证”或者“经典-本地用户以自己的身份验证”).

而这些配置都可以在安全基线中找到对应的设置项, 如图 5 所示. 因此, 完全可以用本文的方法来完成文件迁移. 下面将控制权托付给管理机, 定制好图中的安全基线并下发, 返回部署完成. 目标机重启, 按上述过程迁移共享文件夹后, 成功进入并未发生异常.

图 4 访问共享文件夹出错

企业级服务器有强大的数据处理能力, 往往身兼数职. 其上运行的服务可以分为两类, 一类是操作系统自身提供的服务, 如: 文件服务、DNS 服务、域控服务等; 另一类是基于系统服务的应用服务, 如: OA 服务, 财务服务、数据库等. 对于企业级服务器而言, 环境配置的要求更庞大、严格, 环境迁移也显得更加重要. 对于不同的服务与应用, 读者可以自行试验, 这里不再一一举例.

```
<Setting ID="{7c18bc01-f889-4ead-9ff0-ba9d44f11e19}" Name="Server"
<Setting ID="{d1ebfdbd-94b8-42ac-b990-be964d46daf7}" Name="Workstation"
<Setting ID="{93ecb18c-a5e3-4a87-84d4-5398a37fe855}" Name="Accounts: Guest account status"
<Setting ID="{97b4ca68-163f-4b5b-83f8-e4a579af9c21}" Name="Access this computer from the network"
<Setting ID="{b19cf8db-0f8f-4f6a-9722-31e6837c67f6}" Name="Deny access to this computer from the network"
<Setting ID="{c619d762-fd2b-476c-838e-857cd15985e2}" Name="Network access: Sharing and security model for local accounts"
```

图 5 Server 2003 上对应的安全基线设置

4 总结

本文探讨了企业安全运营管理中复杂而繁琐的环节: 服务迁移. 旨在通过安全基线解决服务与环境共同迁移这一难题. 用户当然可以先迁移服务, 再针对出错的原因查找、更改环境设置, 但提前预防出错始终是更好的选择. 在新环境中, 先由安全基线铺设道路, 服务与应用程序在其上可靠运行. 一对多的迁移控制, 无须为每台计算机手动配置每一个设置项, 这大大降低了管理的困难度. 简洁也意味着更加安全, 业务应用与服务的前提条件不会遗漏, 同时不需要的服务则可以配置关闭, 减少安全隐患. 可谓一箭双雕. 在非完全虚拟化的管理模式中, 本机制可以与其它机制相结合, 共同维护企业的运营安全.

参考文献

1 张彬彬.面向服务架构的应用迁移方法及其应用研究[硕士学位].武汉:华中科技大学,2006.

2 Hacking S, Hudzia B. Improving the live migration process of large enterprise applications. VTDC’09 Proc. of the 3rd International Workshop on Virtualization Technologies in Distributed Computing. New York: ACM, 2009:51–58.

3 张仲敏,宋凭,许鲁.服务在线迁移系统研究与实现.计算机科学,2007:34(12).

4 Gmach D. Adaptive quality of service management for enterprise services. ACM Trans. on the Web, 2008,2(1).

5 许涛,吴亚非,刘蓓,李新友.我国政务终端安全桌面核心配置标准研究.计算机安全,2010,11:71–74.

6 位华.Windows Xp 安全基线评估技术研究[硕士学位论文].上海:复旦大学,2008.