服务器日常维护工作要点

Web服务器的日常维护是网管的一项重要工作，主要工作有：入侵检测、数据备份、服务器优化、常见故障处理以及日志安排等一系统日常维护，服务器管理工作必须规范严谨。

一、入侵检测和数据备份

（一）入侵检测工作

作为服务器的日常管理，入侵检测是一项非常重要的工作，在平常的检测过程中，主要包含日常的服务器安全例行检查和遭到入侵时的入侵检查，也就是分为在入侵进行时的安全检查和在入侵前后的安全检查。系统的安全性遵循木桶原理，木桶原理指的是：一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么这个木桶的最大容量不取决于长的木板，而取决于最短的那块木板。应用到安全方面也就是说系统的安全性取决于系统中最脆弱的地方，这些地方是日常的安全检测的重点所在。

日常的安全检测

日常安全检测主要针对系统的安全性，工作主要按照以下步骤进行：

1、查看服务器状态：

打开进程管理器，查看服务器性能，观察 CPU和内存使用状况。查看是否有CPU和内存占用过高等异常情况。

2、检查当前进程情况

切换 任务管理器 到进程，查找有无可疑的应用程序或后台进程在运行。用进程管理器查看进程时里面会有一项 taskmgr，这个是进程管理器自身的进程。如果正在运行 windows更新会有一项 wuauclt.exe进程。对于拿不准的进程或者说不知道是服务器上哪个应用程序开启的进程，可以在网络上搜索一下该进程名加以确定 [进程知识库：http://www.dofile.com/]。通常的后门如果有进程的话，一般会取一个与系统进程类似的名称，如 svch0st.exe，此时要仔细辨别 [通常迷惑手段是变字母 o为数字 0，变字母 l为数字 1]

3、检查系统帐号

打开计算机管理，展开本地用户和组选项，查看组选项，查看administrators组是否添加有新帐号，检查是否有克隆帐号。

4、查看当前端口开放情况

使用 activeport，查看当前的端口连接情况，尤其是注意与外部连接着的端口情况，看是否有未经允许的端口与外界在通信。如有，立即关闭该端口并记录下该端口对应的程序并记录，将该程序转移到其他目录下存放以便后来分析。

打开计算机管理 ⇒ 软件环境 ⇒ 正在运行任务 [在此处可以查看进程管理器中看不到的隐藏进程]，查看当前运行的程序，如果有不明程序，记录下该程序的位置，打开任务管理器结束该进程，对于采用了守护进程的后门等程序可尝试结束进程树，如仍然无法结束，在注册表中搜索该程序名，删除掉相关键值，切换到安全模式下删除掉相关的程序文件。

5. 检查系统服务

运行 services.msc，检查处于已启动状态的服务，查看是否有新加的未知服务并确定服务的用途。对于不清楚的服务打开该服务的属性，查看该服务所对应的可执行文件是什么，如果确定该文件是系统内的正常使用的文件，可粗略放过。查看是否有其他正常开放服务依存在该服务上，如果有，可以粗略的放过。如果无法确定该执行文件是否是系统内正常文件并且没有其他正常开放服务依存在该服务上，可暂时停止掉该服务，然后测试下各种应用是否正常。对于一些后门由于采用了 hook系统 API技术，添加的服务项目在服务管理器中是无法看到的，这时需要打开注册表中的 HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Services项进行查找，通过查看各服务的名称、对应的执行文件来确定是否是后门、木马程序等。

6. 查看相关日志

运行 eventvwr.msc，粗略检查系统中的相关日志记录。在查看时在对应的日志记录上点右键选 属性 ，在 筛选器 中设置一个日志筛选器，只选择错误、警告，查看日志的来源和具体描述信息。对于出现的错误如能在服务器常见故障排除中找到解决办法则依照该办法处理该问题，如果无解决办法则记录下该问题，详细记录下事件来源、 ID号和具体描述信息，以便找到问题解决的办法。

7. 检查系统文件

主要检查系统盘的 exe和 dll文件，建议系统安装完毕之后用 dir *.exe /s >1.txt将 C盘所有的 exe文件列表保存下来，然后每次检查的时候再用该命令生成一份当时的列表，用 fc比较两个文件，同样如此针对 dll文件做相关检查。需要注意的是打补丁或者安装软件后重新生成一次原始列表。检查相关系统文件是否被替换或系统中是否被安装了木马后门等恶意程序。必要时可运行一次杀毒程序对系统盘进行一次扫描处理。

8. 检查安全策略是否更改

打开本地连接的属性，查看 常规 中是否只勾选了 TCP/IP协议 ，打开 TCP/IP 协议设置，点 高级 ⇒ 选项 ，查看 IP安全机制 是否是设定的 IP策略，查看 TCP/IP 筛选允许的端口有没有被更改。打开 管理工具 ⇒ 本地安全策略 ，查看目前使用的 IP安全策略是否发生更改。

9. 检查目录权限

重点查看系统目录和重要的应用程序权限是否被更改。需要查看的目录有 c:; c:winnt; C:winntsystem32; c:winntsystem32/inetsrv;

c:winntsystem32/inetsrvdata; c:documents and Settings,然后再检查 serv-u 安装目录，查看这些目录的权限是否做过变动。检查 system32

下的一些重要文件是否更改过权限，包括：cmd, net, ftp, tftp, cacls等文件。

10、检查启动项

主要检查当前的开机自启动程序。可以使用 AReporter来检查开机自启动的程序。

发现入侵时的应对措施

对于即时发现的入侵事件，以下情况针对系统已遭受到破坏情况下的处理，系统未遭受到破坏或暂时无法察觉到破坏，先按照上述的检查步骤检查一遍后再酌情考虑以下措施。系统遭受到破坏后应立即采取以下措施：

视情况严重决定处理的方式，是通过远程处理还是通过实地处理。如情况严重建议采用实地处理。如采用实地处理，在发现入侵的第一时间通知机房关闭服务器，待处理人员赶到机房时断开网线，再进入系统进行检查。如采用远程处理，如情况严重第一时间停止所有应用服务，更改 IP策略为只允许远程管理端口进行连接然后重新启动服务器，重新启动之后再远程连接上去进行处理，重启前先用 AReporter检查开机自启动的程序。然后再进行安全检查。

以下处理措施针对用户站点被入侵但未危及系统的情况，如果用户要求加强自己站点的安全性，可按如下方式加固用户站点的安全：

站点根目录 ---只给 administrator读取权限，权限继承下去。

wwwroot -----给 web用户读取、写入权限。高级里面有删除子文件夹和文件权限

logfiles-----给 system写入权限。

database-----给 web用户读取、写入权限。高级里面没有删除子文件夹和文件权限

如需要进一步修改，可针对用户站点的特性对于普通文件存放目录如 html、js、图片文件夹只给读取权限，对 asp等脚本文件给予上表中的权限。另外查看该用户站点对应的安全日志，找出漏洞原因，协助用户修补程序漏洞。

（二）数据备份和数据恢复

数据备份工作大致如下：

1、每月备份一次系统数据。

2、备份系统后的两周单独备份一次应用程序数据，主要包括 IIS、serv-u 数据库等数据。

3、确保备份数据的安全，并分类放置这些数据备份。因基本上采用的都是全备份方法，对于数据的保留周期可以只保留该次备份和上次备份数据两份即可。

数据恢复工作：

1、系统崩溃或遇到其他不可恢复系统正常状态情况时，先对上次系统备份后发生的一些更改事件如应用程序、安全策略等的设置做好备份，恢复完系统后再恢复这些更改。

2、应用程序等出错采用最近一次的备份数据恢复相关内容。

二、服务器性能优化

1、整理系统空间：

删除系统备份文件，删除驱动备份，删除不用的输入法，删除系统的帮助文件，卸载不常用的组件。最小化 C盘文件。

2、性能优化：

删除多余的开机自动运行程序；
减少预读取，减少进度条等待时间；
让系统自动关闭停止响应的程序；
禁用错误报告 ,但在发生严重错误时通知；
关闭自动更新 ,改为手动更新计算机；
启用硬件和 DirectX加速；
禁用关机事件跟踪；
禁用配置服务器向导；
减少开机磁盘扫描等待时间；
将处理器计划和内存使用都调到应用程序上；
调整虚拟内存；
内存优化；
修改 cpu的二级缓存；
修改磁盘缓存。

IIS性能优化

1、调整 IIS高速缓存

HKEY_LOCAL_MACHINE SystemCurrentControlSetServicesInetInfoParametersMemoryCacheSize MemoryCacheSize的范围是从 0道 4GB, 缺省值为 3072000（3MB）。一般来说此

值最小应设为服务器内存的 10%。IIS通过高速缓存系统句柄、目录列表以及其他常用数据的值来提高系统的性能。这个参数指明了分配给高速缓存的内存大小。如果该值为 0，那就意味着 不进行任何高速缓存 。在这种情况下系统的性能可能会降低。如果你的服务器网络通讯繁忙，并且有足够的内存空间，可以考虑增大该值。必须注意的是修改注册表后，需要重新启动才能使新值生效。

2. 不要关闭系统服务： Protected Storage

3. 对访问流量进行限制

（1）对站点访问人数进行限制
（2）站点带宽限制。保持 HTTP连接。
（3）进程限制，输入 CPU的耗用百分比

4. 提高 IIS的处理效率

应用程序设置 处的 应用程序保护 下拉按钮，从弹出的下拉列表中，选中 低（IIS进程） 选项，IIS服务器处理程序的效率可以提高 20%左右。但此设置会带来严重的安全问题，不值得推荐。

5. 将 IIS服务器设置为独立的服务器

（1）提高硬件配置来优化 IIS性能
硬盘：硬盘空间被 NT和 IIS服务以如下两种方式使用：一种是简单地存储数据；另一种是作为虚拟内存使用。如果使用 Ultra2的 SCSI硬盘，可以显著提高 IIS的性能
（2）可以把 NT服务器的页交换文件分布到多个物理磁盘上，注意是多个 物理磁盘 ，分布在多个分区上是无效的。另外，不要将页交换文件放在与 Windows NT引导区相同的分区中
（3）使用磁盘镜像或磁盘带区集可以提高磁盘的读取性能
（4）最好把所有的数据都储存在一个单独的分区里。然后定期运行磁盘碎片整理程序以保证在存储 Web服务器数据的分区中没有碎片。使用 NTFS有助于减少碎片。推荐使用 Norton的 Speeddisk，可以很快的整理 NTFS分区。

6. 起用 HTTP压缩

HTTP压缩是在 Web服务器和浏览器间传输压缩文本内容的方法。HTTP压缩采用通用的压缩算法如 gzip等压缩 HTML、Javas cript或 CSS文件。可使用 pipeboost进行设置。

7. 起用资源回收

使用 IIS5 Recycle定时回收进程资源。

三、服务器常见故障排除

1、ASP 请求的资源正在使用中 的解决办法：

该问题一般与杀毒软件有关，在服务器上安装个人版杀毒软件所致。出现这种错误可以通过卸载杀毒软件解决，也可尝试重新注册 vbs cript.dll和 jscript.dll来解决，在命令行下运行： regsvr32 vbscript.dll 和 regsvr32 jscript.dll即可。

2、ASP500错误解决办法：

首先确定该问题是否是单一站点存在还是所有站点存在，如果是单一站点存在该问题，则是网站程序的问题，可打开该站点的错误提示，把 IE的 显示友好 HTTP错误 信息取消，查看具体错误信息，然后对应修改相关程序。如是所有站点存在该问题，并且 HTML页面没有出现该问题，相关日志出现 服务器无法加载应用程序 /LM/W3SVC/1/ROOT 。错误是 不支持此接口 。那十有八九是服务器系统中的 ASP相关组件出现了问题，重新启动 IIS服务，尝试是否可以解决该问题，无法解决重新启动系统尝试是否可解决该问题，如无法解决可重新修复一下 ASP组件：首先删除 com组件中的关于 IIS的三个东西，需要先将属性里的高级中 禁止删除 的勾选取消。

命令行中，输入 cdwinntsystem32inetsrv 字符串命令，单击回车键后，再执行 rundll32 wamreg.dll,CreateIISPackage 命令，接着再依次执行 regsvr32 asptxn.dll 命令、 iisreset 命令，最后重新启动一下计算机操作系统，这样 IIS服务器就能重新正确响应 ASP脚本页面了。

3、IIS出现 105错误：

在系统日志中 服务器无法注册管理工具发现信息。管理工具可能无法看到此服务器 来源：w3svc ID：105

解决办法：在网络连接中重新安装 netbios协议即可，安装完成之后取消掉勾选。

4、MySQL服务无法启动【错误代码 1067】的解决方法

启动 MySQL服务时都会在中途报错 !内容为 :在 本地计算机 无法启动 MySQL服务 错误 1067：进程意外中止。

解决方法：查找 Windows目录下的 my.ini文件，编辑内容（如果没有该文件，则新建一个），至少包含 basedir, datadir这两个基本的配置。

```
[mysqld]
# set basedir to installation path, e.g., c:/mysql
#设置为 MYSQL的安装目录
basedir=D:/www/WebServer/MySQL
# set datadir to location of data directory,
```

e.g., c:/mysql/data or d:/mydata/data
#设置为 MYSQL的数据目录
datadir=D:/www/WebServer/MySQL/data
注意，我在更改系统的 temp目录之后没有对更改后的目录给予 system用户的权限也出现过该问题。

5、 DllHotst进程消耗 cpu 100%的问题

服务器正常 CPU消耗应该在 75%以下，而且 CPU消耗应该是上下起伏的，出现这种问题的服务器，CPU会突然一直处 100%的水平，而且不会下降。查看任务管理器，可以发现是 DLLHOST.EXE消耗了所有的 CPU空闲时间，管理员在这种情况下，只好重新启动 IIS服务，奇怪的是，重新启动 IIS服务后一切正常，但可能过了一段时间后，问题又再次出现了。
直接原因：
有一个或多个 ACCESS数据库在多次读写过程中损坏， MDAC系统在写入这个损坏的 ACCESS文件时， ASP线程处于 BLOCK状态，结果其他线程只能等待， IIS被死锁了，全部的 CPU时间都消耗在 DLLHOST中。
解决办法：
把数据库下载到本地，然后用 ACCESS打开，进行修复操作。再上传到网站。如果还不行，只有新建一个 ACCESS数据库，再从原来的数据库中导入所有表和记录。然后把新数据库上传到服务器上。

6、 Windows installer出错：

在安装软件的时候出现 不能访问 windows installer 服务。可能你在安全模式下运行 windows，或者 windows installer 没有正确的安装。请和你的支持人员联系以获得帮助 如果试图重新安装 InstMsiW.exe，提示： 指定的服务已存在 。
解决办法：
关于 installer的错误，可能还有其他错误提示，可尝试以下解决办法：
首先确认是否是权限方面的问题，提示信息会提供相关信息，如果是权限问题，给予 winnt目录 everyone权限即可 [安装完把权限改回来即可]。如果提示的是上述信息，可以尝试以下解决方法：运行 msiexec /unregserver 卸载 Windows Installer服务，如果无法卸载可使用

SRVINSTW进行卸载，然后下载 windows installer的安装程序 [地址：http://www.newhua.com/cfan/200410/instmsiw.exe]，用 winrar解压该文件，在解压缩出来的文件夹里面找到 msi.inf文件，右键单击选择 安装 ，重新启动系统后运行 msiexec /regserver 重新注册 Windows Installer服务。

四、服务器管理

（一）服务器日常管理安排

仙居县求是文化传播有限公司

服务器管理工作必须规范严谨，尤其在不是只有一位管理员的时候，日常管理工作包括：

1. 服务器的定时重启。每台服务器保证每周重新启动一次。重新启动之后要进行复查，确认服务器已经启动了，确认服务器上的各项服务均恢复正常。对于没有启动起来或服务未能及时恢复的情况要采取相应措施。前者可请求托管商的相关工作人员帮忙手工重新启动，必要时可要求让连接上显示器确认是否已启动起来；后者需要远程登陆上服务器进行原因查找并根据原因尝试恢复服务。

2. 服务器的安全、性能检查，每服务器至少保证每周登陆两次粗略检查两次。每次检查的结果要求进行登记在册。如需要使用一些工具进行检查，可直接在 e:tools中查找到相关工具。对于临时需要从网络上找的工具，首先将 IE的安全级别调整到高，然后在网络上进行查找，不要去任何不明站点下载，尽量选择如华军、天空等大型网站进行下载，下载后确保当前杀毒软件已升级到最新版本，升级完毕后对下载的软件进行一次杀毒，确认正常后方能使用。对于下载的新工具对以后维护需要使用的话，将该工具保存到 e:tools下，并在该目录中的 readme.txt文件中做好相应记录，记录该工具的名称，功能，使用方法。并且在该文件夹中的 rar文件夹中保留一份该工具的 winrar压缩文件备份，设置解压密码。

3. 服务器的数据备份工作，每服务器至少保证每月备份一次系统数据，系统备份采用 ghost方式，对于 ghost文件固定存放在 e:ghost文件目录下，文件名以备份的日期命名，如 0824.gho，每服务器至少保证每两周备份一次应用程序数据，每服务器至少保证每月备份一次用户数据，备份的数据固定存放在 e:databak文件夹，针对各种数据再建立对应的子文件夹，如 serv-u用户数据放在该文件夹下的 servu文件夹下， iis站点数据存放在该文件夹下的 iis文件夹下。

4. 服务器的监控工作，每天正常工作期间必须保证监视所有服务器状态，一旦发现服务停止要及时采取相应措施。对于发现服务停止，首先检查该服务器上同类型的服务是否中断，如所有同类型的服务都已中断及时登陆服务器查看相关原因并针对该原因尝试重新开启对应服务。

5. 服务器的相关日志操作，每服务器保证每月对相关日志进行一次清理，清理前对应的各项日志如应用程序日志、安全日志、系统日志等都应选择 保存日志 。所有的日志文件统一保存在 e:logs下，应用程序日志保存在 e:logsapp中，系统程序日志保存在 e:logssys中，安全日志保存在 e:logssec中。对于另外其他一些应用程序的日志，也按照这个方式进行处理，如 ftp的日志保存在 e:logsftp中。所有的备份日志文件都以备份的日期命名，如 20050824.evt。对于不是单文件形式的日志，在对应的记录位置下建立一个以日期命名的文件夹，将这些文件存放在该文件夹中。

6、服务器的补丁修补、应用程序更新工作，对于新出的漏洞补丁，应用程序方面的安全更新一定要在发现的第一时间给每服务器打上应用程序的补丁。

7、服务器的隐患检查工作，主要包括安全隐患、性能等方面。每服务器必须保证每月重点的单独检查一次。每次的检查结果必须做好记录。

8、不定时的相关工作，每服务器由于应用软件更改或其他某原因需要安装新的应用程序或卸载应用程序等操作必须知会所有管理员。

9、定期的管理密码更改工作，每服务器保证至少每两个月更改一次密码，对于 SQL服务器由于如果 SQL采用混合验证更改系统管理员密码会影响数据库的使用则不予修改。

相关建议：对每服务器设立一个服务器管理记载，管理员每次登陆系统都应该在此中进行详细的记录，共需要记录以下几项：登入时间，退出时间，登入时服务器状态 [包含不明进程记录，端口连接状态，系统帐号状态，内存 /CPU状态]，详细操作情况记录 [详细记录下管理员登陆系统后的每一步操作]。无论是远程登陆操作还是物理接触操作都要进行记录，然后将这些记录按照各服务器归档，按时间顺序整理好文档。

对于数据备份、服务器定时重启等操作建议将服务器分组，例如分成四组，每月的周六晚备份一组服务器的数据，每周的某一天定时去重启一组的服务器，这样对于工作的开展比较方便，这些属于固定性的工作。另外有些工作可以同步进行，如每月一次的数据备份、安全检查和管理员密码修改工作，先进行数据备份，然后进行安全检查，再修改密码。对于需要的即时操作如服务器补丁程序的安装、服务器不定时的故障维护等工作，这些属于即时性的工作，但是原则上即时性的工作不能影响固定工作的安排。

（二）管理员日常注意事项

在服务器管理过程中，管理员需要注意以下事项：

1、对自己的每一次操作应做好详细记录，具体见上述建议，以便于后来检查。

2、努力提高自身水平，加强学习

硬件维护

1、储存设备的扩充

当资源不断扩展的时候，服务器就需要更多的内存和硬盘容量来储存这些资源。所以，内存和硬盘的扩充是很常见的。增加内存前需要认定与服务器原有的内存的兼容性，最好是同一品牌的规格的内存。如果是服务器专用的 ECC内存，则必须选用相同的内存，普通的 SDRAM内存与 ECC内存在同一台服务器上使用很可能会引起统严重出错。在增加硬盘以前，需要认定服务器是否有空余的硬盘支架、硬盘接口和电源接口，还有主板是否支持这种容量的硬盘。尤其需要注意，防止买来了设备却无法使用。

2、设备的卸载和更换

卸载和更换设备时的问题不大，需要注意的是有许多品牌服务器机箱的设计比较特殊，需要特殊的工具或机关才能打开，在卸机箱盖的时候，需要仔细看说明书，不要强行拆卸。另外，必须在完全断电、服务器接地良好的情况下进行，即使是支持热插拔的设备也是如此，以防止静电对设备造成损坏。

3、除尘

尘土是服务器最大的杀手，因此需要定期给服务器除尘。对于服务器来说，灰尘甚至是致命的。除尘方法与普通 PC除尘方法相同，尤其要注意的是电源的除尘。

软件维护

1、操作系统的维护

操作系统是服务器运行的软件基础，其重要性不言自明。多数服务器操作系统使用Windows NT或 Windows 2000 Server作为操作系统，维护起来还是比较容易的。

在 Windows NT或 Windows 2000 Server打开事件查看器，在系统日志、安全日志和应用程序日志中查看有没有特别异常的记录。现在网上的黑客越来越多了，因此需要到微软的网站上下载最新的 Service Pack(升级服务包)安装上，将安全漏洞及时补上。

2、网络服务的维护

网络服务有很多，如 WWW服务、 DNS服务、 DHCP服务、 SMTP服务、 FTP服务等，随着服务器提供的服务越来越多，系统也容易混乱，此时可能需要重新设定各个服务的参数，使之正常运行。

3、数据库服务

数据库经过长期的运行，需要调整数据库性能，使之进入最优化状态。数据库中的数据是最重要的，这些数据库如果丢失，损失是巨大的，因此需要定期来备份数据库，以防万一。

4、用户数据

经过频繁使用，服务器可能存放了大量的数据。这些数据是非常宝贵的资源，所以需要加以整理，并刻成光盘永久保存起来，即使服务器有故障，也能恢复数据。