Pc Server日常巡检总结

1. 巡检介绍
2. 目的

巡检就是通过人工的定期检查工作，来提高对服务器安全、稳定的管理措施。定期的巡检工作不但可以及时发现一些安全漏洞和异常，还可以及时发现一些日常管理的问题，为服务器的安全和管理措施的整改做好基础。巡检可以做为一项例行的工作来做，具有非常重要的作用。

1. 方式

PC机的巡检有初检和日常巡检，初检是整个环境的一个摸底，日常巡检只需要查看硬件状态和资源使用率及日志，没有特殊情况无需收集设备信息。

二、日常巡检的工作：

１、环境巡检

温、湿度以及环境清洁程度。

２、硬件设备巡检

主要通过外观（指示灯和光通路诊断面板）来判读设备是否正常工作，如果设有管理口可以登录，最好通过管理口查看硬件状态。

３、OS巡检

1. 查看资源使用率，包括内存/交换空间、CPU、Disk、NIC等(建议不能超过80%）。
2. 查看日志是否有告警或报错，可以通过第三方软件，也可以查看ＯＳ的Event 。
3. OS补丁是否有更新。
4. 进程，是否有僵尸进程（Linux用top命令查看）

三、初检的工作

在日常巡检的基础上增加一下工作：

１、设备信息收集

硬件信息收集的目的除了统计服务器的配置设备，最主要是能在生产服务器的某个部件坏了后快速的找到备件，也就是找到备件号(PN/FRU等)这里以HP为例总结了三种方法：

1. 没工作的服务器：可以直接取出查看各硬件的标签，标签一般有硬件的SN号和备件号。
2. 使用第三方（如HP的HP Insight Diagnostics Onlin Edition）工具。

选区_012

1. 这是最不推荐，但却不得不知道的一种方法，当客户的生产服务器上没有装第三方管理工具时：
2. 我们只有通过OS查看主机的SN号(确认主板未更换或换了主板后改了主板的SN)和硬件信息（如CPU的型号、主频等信息），具体命令见附件。
3. 在http://partsurfer.hpe.com网站通过主机ＳＮ号查到该系列该型号的主机支持的所有硬件信息和ＰＮ号。
4. 通过对比网站上的信息和ＯＳ里查到的信息，确认出该主机使用的硬件，获得备件号。（同系列同型号的主机的配置是不一样的，所以必须进行匹配）。

２、查看整个环境的脆弱点，尤其是设备是否有冗余。

３、许可证。

４、防火墙状态。

５、网卡工作状态，建议不使用的网卡disable掉。

６、OS的例行性工作（执行计划）

最后引用一段互联网上某位工程师的心得吧：

　　做安全巡检，需要有计划的去进行，数据至关重要。经验可以有效提高你的管理效率，但经验也容易造成惯性思维，导致故障延误。故，应根据现象的表现和出现的具体情况给予谨慎的判断，同时做好记录和分析笔记。

附件１：