系统监控原理：这里的系统监控不止指os的，也可以指邮件服务器，web服务器等；

为什么需要监控：

发现故障和bug，监控系统及应用的安全性，分析性能瓶颈，发现系统规律------修复完善系统应用，防御保护，优化速度，提高稳定性，大数据分析；

监控什么：系统及应用层的错误，攻击行为，性能参数，用户行为规则；

如何进行监控-获取数据：监控就是获取想要的数据并进行分析（snmp与日志系统），分析之后数据经过处理以直观的方式展示。数据可视化，统计分析日志。

SNMP协议：简单网络管理协议，这是一个标准协议，用来获取或设置系统上的数据与参数，分为监控设备与被监控设备，snmp是跑在被监控设备上的，snmp使用的是udp，端口号：161,162，被监控设备上拥有一个snmp agent的服务，监控设备称为nms，只要支持snmp的监控软件；snmp使用MIB数据库来存储信息，mib使用树状结构组织管理数据，mib使用oid定位资源。

Snmp的方法：get，get next，get bulk，set，traps，inform。

获取数据：监控设备主动向被监控设备发送的：get，get next，get bulk，set。

触发性接收数据：traps，inform，被监控设备发生故障后主动向监控设备发送信息。

Snmp三个版本：主要是snmpv1与v2，版本之间提高安全性，snmp的开源实现，net-snmp，yum install –y net-snmp net-snmp-devel, net-snmp-libs, net-snmp-utils;

安装好之后启动服务配置文件在/etc/snmp/snmp.conf，snmp的community的概念我们community等价于password；先配置在使用，配置snmp.conf文件，



使用snmpget获取一个在指定的oid的值：

Snmpget –v1 –c public 127.0.0.1 1.3.6.1.2.1.1.1.0

使用snmpwalk命令获取从某个节点开始后的所有信息：

Snmpwalk –v1 c public 127.0.0.1 .1;

日志分析：日志一纯文本的形式记录程序运行的相关信息，内容由相关程序决定，日志比snmp更灵活，记录的信息也更多，但分析起来比较麻烦/var/log/\*；每个服务，大型程序都会有日志，但是不同的日志的格式大不相同，通常用专用的工具或脚本进行分析，日志以行为单位，grep，wc，sort，awk。

Cacti的使用：安装apache，php，mysql，net-snmp，然后查看iptables，selinux，然后启动服务httpd，mysqld，配置snmpd.Conf文件，设置权限systemview---all，将all的#去掉，重启snmp服务并查看；php对snmp模块的支持，从pkgs上下载php-snmp的软件包，安装完成后使用php –m查看有没有该模块，然后可以下载cacti的压缩包，将cacti的文件放到html下，修改用户apache，为cacti创建数据库，然后从源包下导入cacti.sql，然后进入include/config.php改变用户名与密码，去掉url的注释，安装rrdtool，之后就可以登陆了。使用定时任务crond（在安装文档里面找），vim /etc/crontab，重启crond的服务。