

1 Audit配置文件是什么？

参考答案

/etc/audit/auditd.conf。

2 Auditctl命令的常用选项有哪些？

参考答案

```
01. [root@svr7 ~] # auditctl -s      //查询状态
02. [root@svr7 ~] # auditctl -l      //查看规则
03. [root@svr7 ~] # auditctl -D      //删除所有规则
```

3 设置规则所有对passwd文件的写、属性修改操作都会被记录审计日志

参考答案

```
01. [root@svr7 ~] # audit -w /etc/passwd -p wa -k passwd_change
```

4 如何通过key搜索审计日志？

参考答案

01. [roo@svr7 ~] # ausearch - k sshd_config - i

5 简述ngx_http_limit_req_module模块的用法？

参考答案

01. limit_req_zone \$binary_remote_addr zone=one:10m rate=1r/s;
02. limit_req zone=one burst=5;
03. 语法：limit_req_zone key zone=name: size rate=rate;
04. 将客户端IP信息存储名称为one的共享内存，空间为10M
05. 1M可以存储8千个IP的信息，10M存8万个主机状态
06. 每秒中仅接受1个请求，多余的放入漏斗
07. 漏斗超过5个则报错

6 备份与还原MySQL数据库的方法？

参考答案

01. [roo@svr7 ~] # mysqldump - uroot - predhat my db table > table.sql
02. //备份my db数据库中的table表

```
03. [ roo@svr7 ~] # mysqldump -uroot -predhat my db > my db.sql
04. //备份my db数据库中的所有数据表
05. [ roo@svr7 ~] # mysqldump -uroot -predhat -- all- databases > all.sql
06. //备份所有数据库
07. [ roo@svr7 ~] # mysql -uroot -predhat my db < table.sql //还原表
08. [ roo@svr7 ~] # mysql -uroot -predhat my db < my db.sql //还原数据库
09. [ roo@svr7 ~] # mysql -uroot -predhat < all.sql //还原所有
```

7 Linux系统中生成补丁与打补丁的命令是什么？

参考答案

生成补丁的命令是diff，打补丁的命令是patch。