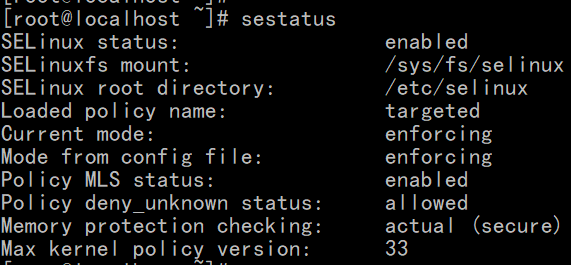
**任务一 使用SELinux 提升内核安全性**

1. **查看SELinux运行情况**

****

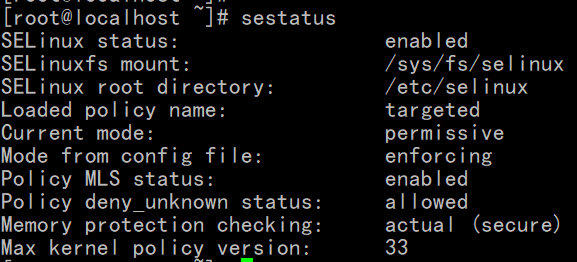
1. **查看SELinux服务自启动状态**

****

1. **配置SELinux运行模式为许可模式**

****

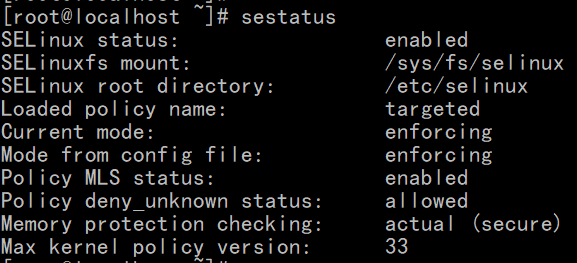
1. **查看SELinux运行信息**

****

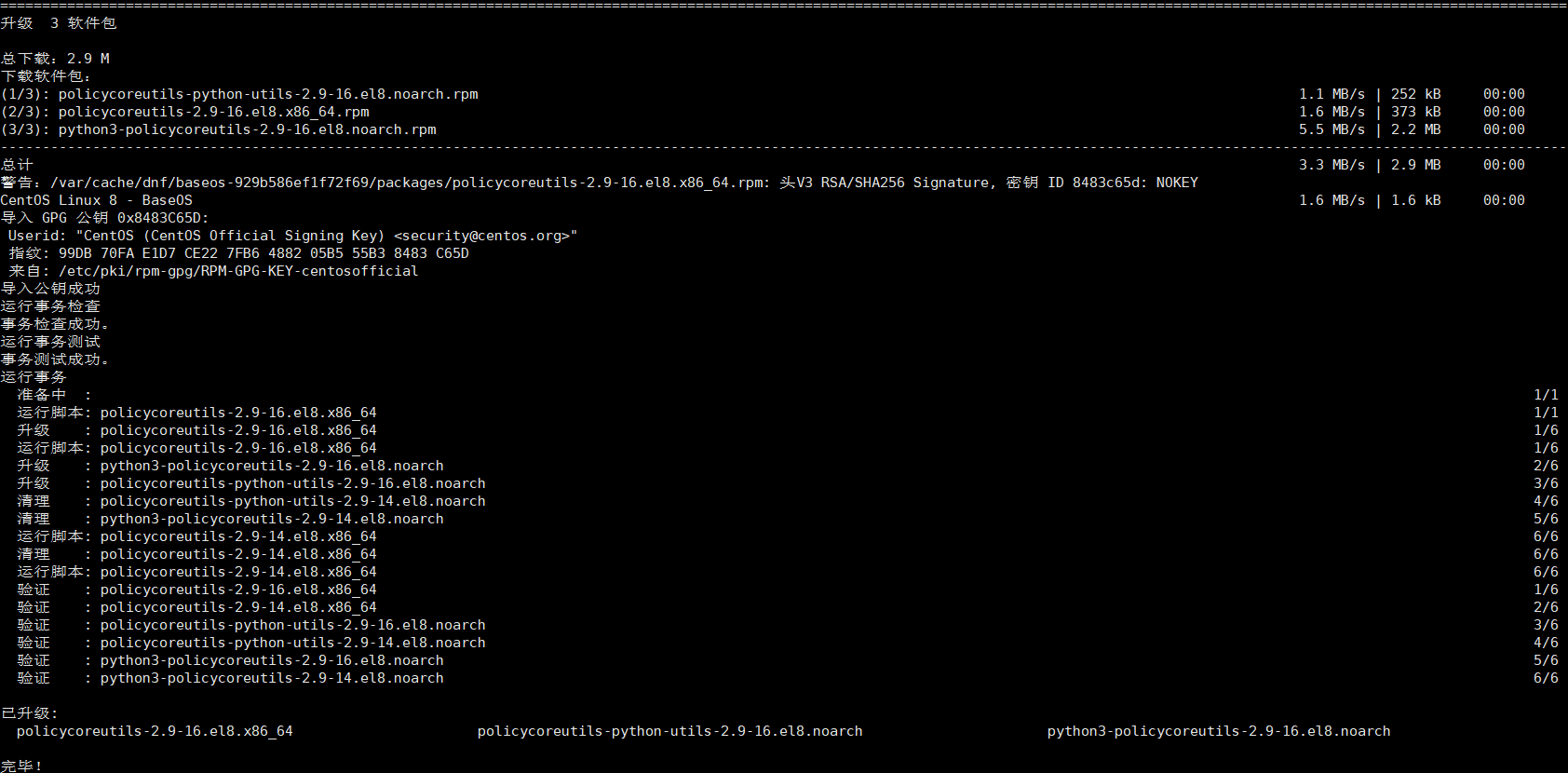
1. **恢复SELinux运行模式为强制模式**

****

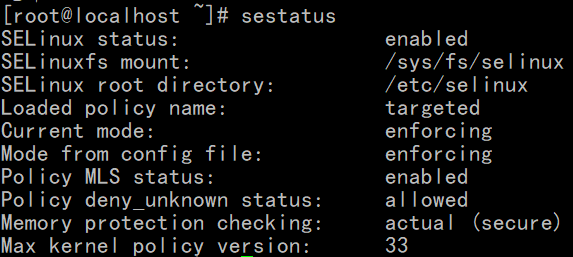
1. **查看SELinux运行信息**

****

1. **安装policycoreutils-python-utils**

****

1. **查看系统SELinux运行状态**

****

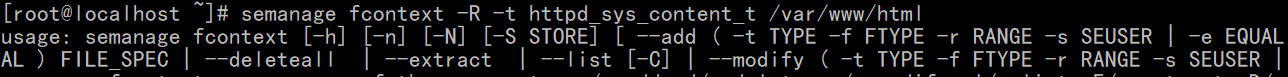
1. **增加82端口能够发布网站**

****

1. **查看SELinux允许提供服务的端口**

****

1. **设置网站发布目录**

****

1. **查看目录与文件的安全上下文信息**

****

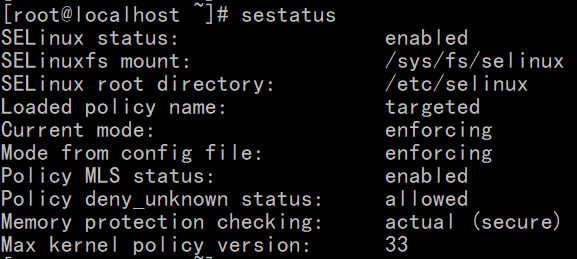
1. **禁止httpd服务允许目录浏览**

****

1. **禁止httpd服务发送电子邮件**

****

1. **查看系统SELinux运行状态**

****

1. **恢复SELinux默认运行模式**

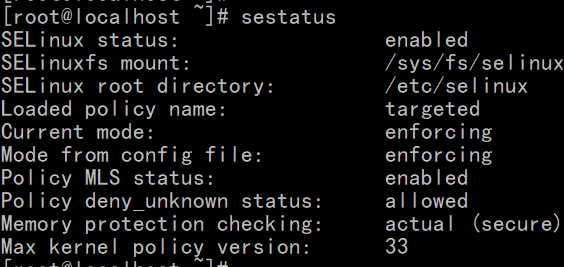
****

1. **禁止mysqld服务链接任意服务端口**

****

1. **禁止httpd服务远程链接mysqld服务**

****

1. **查看系统SELinux运行状态**
2. **禁止FTP服务允许匿名用户访问**

****

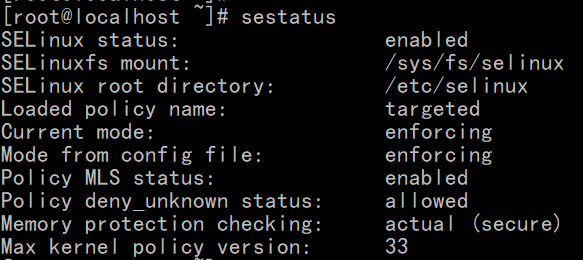
1. **禁止http服务远程链接FTP服务**

****

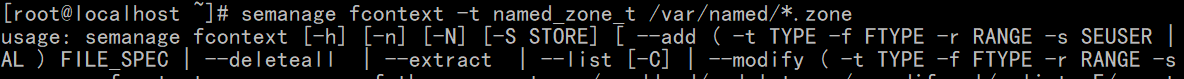
1. **禁止操作系统用户访问FTP服务目录**

****

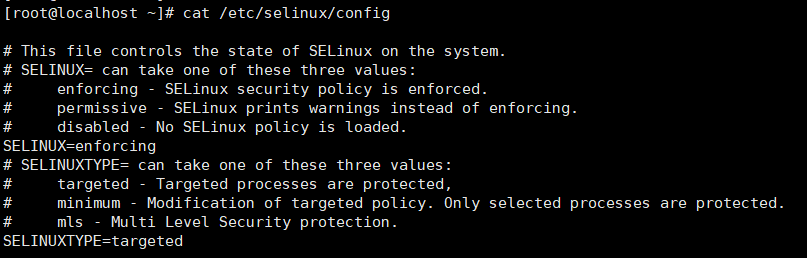
1. **查看系统SELinux运行状态**

****

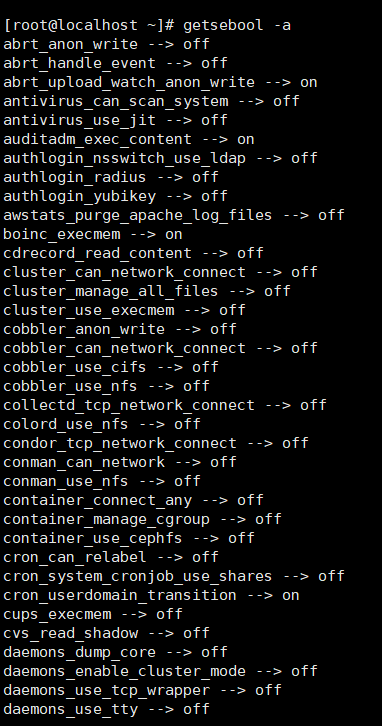
1. **设置域名纪录配置文件类型为named\_zone-t**

****

1. **查看域名配置文件信息**

****

1. **查看SELinux安全策略属性值**

****

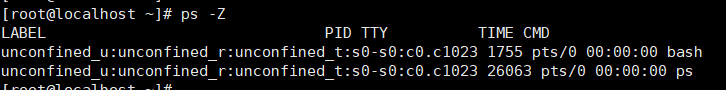
1. **设置SELinux安全策略属性值**

****

1. **查看当前目录与SELinux安全上下文**

****

1. **查看当前运行进程与SELinux安全上下文**

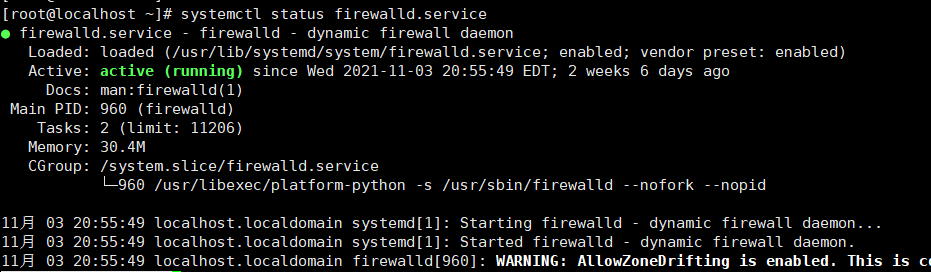
****

1. **查看当前系统用户的安全上下文**

****

**任务二 使用Firewalld提升系统安全性**

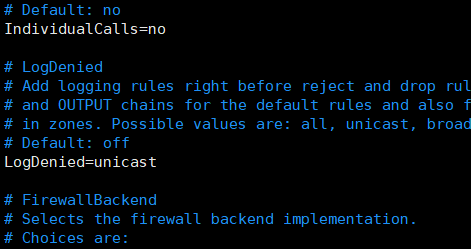
1. **查看防火墙Firewall服务状态**

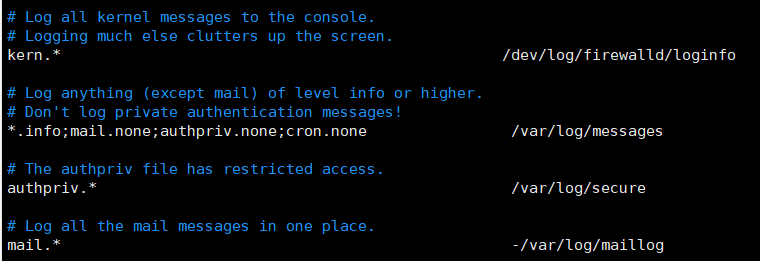
****

1. **查看Firewall服务是否为开机自启动**

****

1. **防火墙日志配置**

****

****

1. **创建防火墙存放目录**

****

1. **重新载入防火墙配置文件**

****

1. **重新启动系统日志服务**

****

1. **配置防火墙规则要求**

****

1. **重新载入配置文件**

****

1. **删除默认ssh服务规则**

****

1. **添加远程访问规则**

****

1. **重新加载防火墙**

****

1. **添加访问网站规则**

****

1. **添加指定主机访问规则**

****

1. **重新载入防火墙**

****

1. **添加本地客户端允许远程链接数据库**

****

1. **添加本地客户端允许访问**

****

1. **重新载入防火墙**

****

1. **允许DNS服务**

****

1. **重新载入防火墙**

****