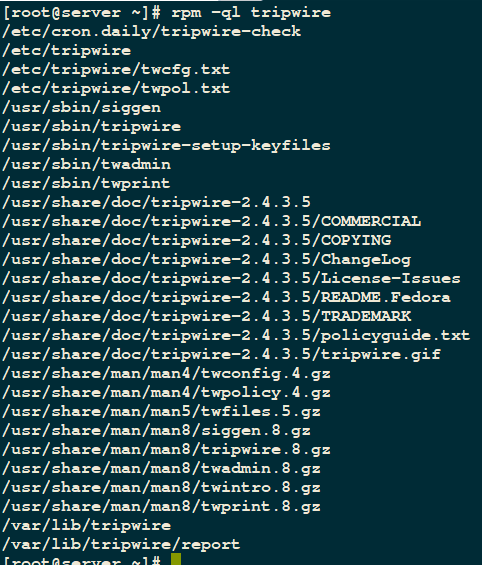
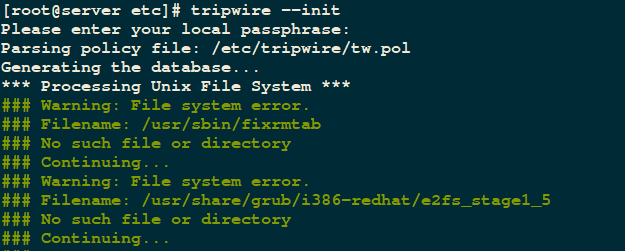
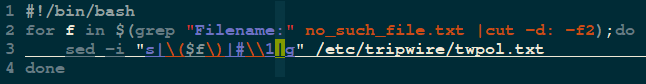
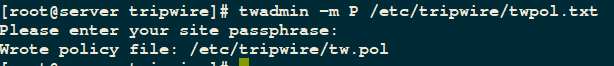
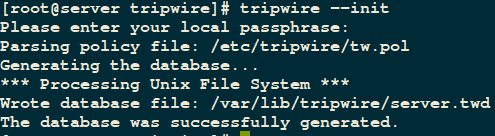
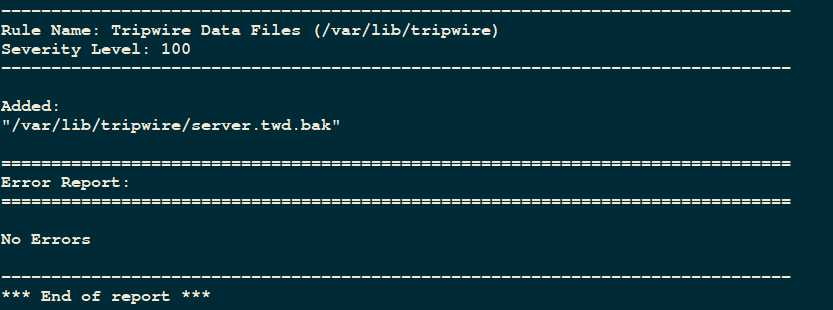
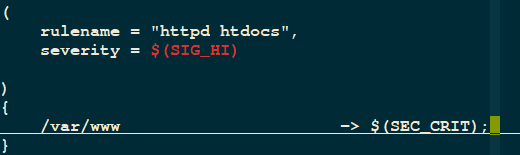
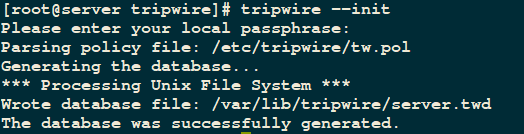
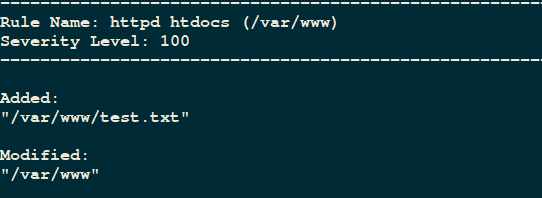
**使用tripwire保护系统敏感文件**  
https://www.howtoing.com/monitoring-and-detecting-modified-files-using-tripwire-on-centos-7

1. **简介**  
   tripwire可以监控指定系统文件，并在文件被改变时给出警报信息
2. **安装**
   1. Yum install tripwire
   2. 使用rpm -ql 可以查看安装了哪些文件  
      
3. **配置tripwire**
   1. 生成密钥文件tripwire-setup-keyfiles(site-key用于保护配置文件，local-key用于验证tripwire二进制文件)  
      期间会提示输入密码，按提示输入即可
   2. 初始化基线数据库  
        
      得到如图所示的警告，默认tripwire配置文件监控了一些本机不存在的文件，所以tripwire给出警报，数据库已经成功生成，如果不想看到类似警报，可以删除配置文件中的条目，由于数量众多，使用脚本完成更为方便，先得到不存在的文件列表  
        
      编写如下脚本（执行前先备份原配置文件）  
        
      在不存在的文件前加上注释#，执行该脚本后，重新签署tripwire配置  
        
      重新初始化基线数据库  
      
4. **验证tripwire配置、检查系统**
   1. 检测文件异常tripwire --check  
        
      由于我们刚才备份了twpol.txt文件，所以提示有新加文件
5. **向配置文件添加新策略**
   1. 编辑策略文件twpol.txt  
      可参考原配置文件格式，添加内容如下（包括用（）括起来的规则名称，严重等级，以及用｛｝括起来的目录和文件，报警等级）  
      更多细节参照帮助手册  
      
   2. 重新签署生成配置  
      
   3. 重新生成基线数据库  
      
   4. 尝试在/var/www下新建文件后进行检查可以发现警告  
        
      结果如下  
      
6. **邮件和cron配置（参照给出的网址，随后测试）**