**Prova 101 - Tópico 104: Dispositivos, Sistemas de arquivos Linux, Filesystem Hierarchy Standard**

**Sub-Tópico: 104,5 Gerenciar permissões de arquivo e propriedades   
  
Peso 3**

**Descrição**: Os candidatos devem ser capazes de controlar o acesso a ficheiros através do uso correto de permissões e posses. **Principais Áreas de Conhecimento**:

* Gerenciar permissões de acesso em arquivos regulares e especiais, bem como diretórios;
* Use os modos de acesso, como SUID, SGID e sticky bit para manter a segurança;
* Saiba como mudar a máscara de criação de arquivo;
* Use o campo de grupo para conceder acesso a arquivos para os membros do grupo.

**Prova 102 - Tópico 107: Tarefas Administrativas**

**Sub-Tópico: 107,1 gerenciar usuários, contas de grupo e sistema de arquivos   
  
Peso 5**  
  
**Descrição**: Os candidatos devem ser capazes de adicionar, remover, suspender e alterar contas de usuários.  
  
**Principais Áreas de Conhecimento**:

* Adicionar, modificar e remover usuários e grupos;
* Criar usuário, senha em bases de dados, grupos;
* Criar e gerenciar contas específicas e limitadas.

**Prova 101 e 102**

**1) Com a umask 007, quais as permissões para diretórios e arquivos respectivamente?  
R: 770 e 660.**  
  
Vamos a conta:   
777 - Permissão total   
-007 - Valor de Umask  
====   
770 - Permissão equivalente ao valor de umask 007 para diretórios  
-111 - Tirando o x (1) pois ele pediu arquivo simples  
====   
660 - Permissão para um arquivo simples!  
  
**2) Qual permissão especial faz com que arquivos criados em determinado diretório pertençam ao mesmo grupo do diretório?  
R: sgid bit**  
  
Essa permissão especial força todos os arquivos de um determinado diretório a serem criados com o grupo do diretório e não do usuário que criou.  
  
Comandos e arquivos que podem ser cobrados na prova:

* chmod
* umask
* chown
* chgrp

**3) Qual permissão especial permite que um usuário comum consiga executar algum comando como se tivesse poderes de root sobre o mesmo?  
R: SUID bit**  
  
Vamos usar como exemplo o shutwdown. Mesmo se você der permissão através do "chmod 755 /sbin/shutdown", o usuário comum não vai conseguir realizar a execução deste, somente o root.  
  
**4) Exemplo prático:  
  
Vou criar um grupo no qual os usuários que poderão reiniciar ou desligar o sistema estarão:**  **# groupadd shutdown  
  
No meu caso, o usuário comum leo estará nesse grupo:**  **# gpasswd -a leo shutdown  
  
Precisamos mudar o grupo do arquivo executável /sbin/shutdown:**  **# chown root.shutdown /sbin/shutdown  
  
Aplicando a permissão especial SUID em modo octal, apenas o root terá poder de escrita nesse arquivo:**  **# chmod 4750 /sbin/shutdown  
  
Agora, vamos criar um link do arquivo para o /bin. Lembrem-se que o usuário comum só executa arquivos que estão em /bin, por isso a necessidade do link. Criando o link:**  **# ln -s /sbin/shutdown /bin/shutdown**   
  
Comandos e arquivos que podem ser cobrados na prova:

* /etc/passwd
* /etc/shadow
* /etc/group
* /etc / skel
* chage
* groupadd
* groupdel
* groupmod
* passwd
* useradd
* userdel
* usermod

**5) Quais comandos podemos usar para trocar o grupo de um determinado arquivo?  
R: chgrp e chown**  
  
Exemplo:  
# chown root.diretoria arquivo\_publico.txt  
ou  
# chgrp diretoria arquivo\_publico.txt   
  
A diferença é que o comando chown permite que você modifique o dono e o grupo ao mesmo tempo.