

Gerenciamento Linux (básico)

Primeiros Passos:
Gerenciamento de contas e grupos
de usuários

Programa de Formação Tecnológica DELL-UFRGS
<http://www.inf.ufrgs.br/~asc/linux>



Roteiro

- Comandos básicos de administração
- Gerenciamento de contas
 - Usuários e grupos

Hot line do Linux

- Comando `man`
 - Fornece a descrição de um comando (sintaxe + funcionalidade)
 - Possibilita a pesquisa por palavra chave
- Talvez o mais importante a saber utilizar
 - e.g: `man ls`
- Pode-se optar por não instalar
 - Não recomendável
- Outros comandos de ajuda:
 - `apropos`: equivale a `man -k`
 - `info`

Funcionamento do `man`

- Procura pela descrição de um comando em uma ordem pré-definida
 - Comandos
 - Chamadas de sistema
 - Funções da biblioteca

Conectores (*Pipe*)

- Permite que a saída de um comando seja fornecido como entrada a outro comando
 - Representado pelo símbolo `|`
- Exemplo:
 - `%ps -aux | grep chavez`

Verificação do conteúdo de um arquivo

- Comando `cat`
- Comandos `less` e `more`
- Comando `tail`
 - Mostra as últimas linhas de um arquivo

Ferramenta para localização de arquivos

- Comando `find`
 - Sintaxe e opções riquíssimas
 - `man find`
 - Permite localizar arquivos que possuem uma característica em comum
 - `find diretório critérios-opções`
 - Exemplo:
 - `find . -name *.c -print`
- Outro comando de localização: `locate`
 - Depende de uma base de dados gerado pelo sistema (`updatedb`)

Outros usos do `find`

- Sob o ponto de vista da administração do sistema `find` serve:
 - Vigiar a utilização de espaço em disco
 - Localizar arquivos que podem representar problemas de segurança
 - Efetuar operações sobre arquivos
- Exemplos:
 - `find /chem -size +2048 -mtime +30 -exec ls -l {} \;`
 - `find / -type -f \(-perm -2000 -o -perm -4000 \) -print`
 - `find /chem -name *.c` -exec mv {} /chem1/src \;`

Roteiro

- Comandos básicos de administração
- Gerenciamento de contas
 - Usuários e grupos

Contas e usuários

- Para utilizar um sistema UNIX é necessário uma conta de usuário
 - Não necessariamente uma pessoa física
 - Usuário é uma "entidade" que pode executar programas e possuir arquivos
- Contas são gerenciadas pelo administrador do sistema
- Existem três tipos de contas:
 - Contas "normais": contas de usuários em geral
 - Conta do super-usuário (root): conta de administração do sistema
 - Contas especiais: associadas a certas tarefas do sistema

Conta de super-usuário (*root*)

- Conta com todos privilégios de acesso
 - Possível destruir o sistema operacional
 - Remover dados importantes
- Criada automaticamente no momento da instalação do sistema
- O Ministério da saúde adverte: "A conta de root é prejudicial a saúde do administrador de rede. Utilizar com moderação."
 - Utilizar APENAS quando for realmente necessário
 - Não utilizar essa conta para realizar trabalhos cotidianos
 - Todo administrador de redes deve ter sua conta pessoal

Contas de usuários (1)

- Cada usuário do sistema deve ter sua própria conta
 - Questão de segurança do sistema e dos dados do usuário
 - Possibilita identificar quem faz o que no sistema
- Uma conta de usuário é caracterizada por:
 - Possuir o nome (*login name*) e senha próprios
 - Associa um UID (*user identifier*)
 - Pertencer a um grupo
 - Cada grupo tem seu GID (*group identifier*)
 - O *uid* e o *gid* determinam os direitos de acesso de um usuário a arquivos e recursos de sistema

Contas de usuários (2)

- Cada usuário possui associado :
 - Um diretório (*home*)
 - Um interpretador de comandos (*shell*)
- Informações sobre contas são mantidas no arquivo `/etc/passwd`

Exemplo de `/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
named:x:25:25:Bind User:/var/named:
ftp:x:14:50:FTP User:/var/ftp:
apache:x:48:233:Apache:/var/www:/bin/bash
asc:x:2222:200:Alexandre Carissimi:/home/asc:/bin/tcsh
```

Entendendo o arquivo `/etc/passwd`

asc:x:2222:200:Alexandre Carissimi:/home/asc:/bin/tcsh

Nome da conta uid gid comentário Diretório shell

senha

- Alguns detalhes:
 - Letras maiúsculas e minúsculas são caracteres diferentes em UNIX
 - Caracteres especiais no campo senha:
 - * : proíbe o acesso a uma determinada conta
 - vazio : permite o *login* no sistema sem necessitar senha
 - x : senha é criptografada e armazenada no arquivo (`/etc/shadow`)

Arquivo `shadow`

- Na maioria dos sistemas UNIX o `/etc/passwd` deve ser “visível”
 - Permitir a conversão do “nome” de um usuário no uid correspondente
 - “Furo” de segurança
- O arquivo `/etc/shadow` possui as senhas criptografadas e permite a leitura apenas pelo *root*
- Comandos `pwconv`
 - Permite de criar/modificar a senha de um usuário

Criando contas de usuários

- Procedimento para criação de uma conta é:
 - Inserir uma entrada em `/etc/passwd`
 - Criar um diretório para o usuário (colocá-lo como proprietário)
 - Copiar os arquivos de inicialização do interpretador de comandos (*shell*) para esse diretório e atualizar as permissões de acesso ao novo usuário

- Exemplo:

```
marceau:x:103:5:Sophie Marceau:/home/marceau:/bin/sh

mkdir /home/marceau
chown marceau /home/marceau
cp /etc/skel/profile /home/marceau/.profile
chown marceau /home/marceau/.profile
```

Removendo contas de usuários

- Procedimento para remoção de uma conta:
 - Retirar a entrada correspondente a conta em `/etc/passwd` e as referências a essa conta em `/etc/group`
 - Remover o diretório associado a essa conta (usuário)
 - Eliminar as referências a essa conta em atividades diárias, arquivos de contabilização, mailbox, etc...
- Conselho:
 - Não remover diretamente os arquivos relacionados com uma conta
 - Cancelar o direito de login dessa conta e após um tempo remove-la
 - Inserir o caractere * no campo senha

Mais sobre criação e remoção de contas de usuários

- Existem *scripts* e programas gráficos para o gerenciamento de contas de usuários:
 - Criação:
 - e.g.: `adduser`
 - Remoção:
 - e.g.: `deluser`, `userdel`
- É possível determinar um período de validade para cada conta

Grupo de usuários

- Todo usuário pertence a pelo menos um grupo
- O conceito de grupo pode ser utilizado para limitar acesso a recursos dos sistema à um certo número de usuários
 - e.g.: uso de periféricos, arquivos de dados, sistemas de arquivos, máquinas
- Informações sobre os grupos são armazenadas em `/etc/group`
 - Uma linha para cada grupo
 - Existem grupos sistema que servem para controlar acesso a arquivos de configuração e *daemons* sistema
- Um grupo pode ser criado diretamente através do campo *gid* do arquivo `/etc/passwd`
 - Se perde o "tradução" entre o "nome fantasia do grupo" e o *gid*

Exemplo de */etc/group*

■ Formato de */etc/group*

nome_do_grupo:senha:gid:membros

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
named:x:25:
wheel:x:10:root
postgres:x:234:
prof:x:200:
```

Funcionamento de grupos

- Um dos mecanismos de segurança em UNIX
- Cada usuário pertence a um grupo primário (*/etc/passwd*) e a um ou mais grupos secundários (*/etc/group*)
 - Usuário tem direito de acesso a recursos pertencentes a seus grupos
 - Tipo de acesso é fornecido através dos bit *rwx*
- Alguns comandos associados a grupos e conta corrente:
 - *groups*: lista os grupos aos quais um usuário pertence
 - *newgrp*: trocar de um grupo (desde que pertença)
 - *id*: lista *uid* e *gid* corrente

Criando e removendo grupos

- De forma análoga a gerência de contas:
 - Manualmente através da edição do arquivo */etc/group*
 - Automaticamente através de programas e/ou *scripts*
 - e.g.: *addgroup* ou *groupadd*, *delgroup* ou *groupdel*
- Sempre que um grupo for removido é necessário “re-classificar” todos os usuários que pertenciam a esse grupo.