CHMOD

Binary	Decimal	Representation
000	0	- - -
001	1	- - x
010	2	- w -
011	3	- w x
100	4	r - -
101	5	r - x
110	6	r w -
111	7	rwx

UOG Mode

1 - u = o dono do arquivo (user);
2 - g = os usuários que são membros do mesmo grupo do arquivo (group);
3 - o = os usuários que não membros do grupo do arquivo (others);

Permissionamento Especial

Peso - SUID	UGO
4	Usuário
2	Grupos
1	Outros

mkpasswd

mkpasswd generates passwords and can apply them automatically to users.
With no arguments, mkpasswd returns a new password.
mkpasswd
With a user name, mkpasswd assigns a new password to the user.
mkpasswd don
The passwords are randomly generated according to the flags below.
Flags
The -l flag defines the length of the password. The default is 9. The following example creates a 20 character password.
mkpasswd -l 20

mkpasswd (cont)

The -d flag defines the minimum number of digits that must be in the password. The default is 2. The following example creates a password with at least 3 digits.
mkpasswd -d 3
The -c flag defines the minimum number of lowercase alphabetic characters that must be in the password. The default is 2.
The -C flag defines the minimum number of uppercase alphabetic characters that must be in the password. The default is 2.
The -s flag defines the minimum number of special characters that must be in the password. The default is 1.
The -p flag names a program to set the password. By default, /etc/yppasswd is used if present, otherwise /bin/passwd is used.
The -2 flag causes characters to be chosen so that they alternate between right and left hands (qwerty-style), making it harder for anyone watching passwords being entered. This can also make it easier for a password-guessing program.
The -v flag causes the password-setting interaction to be visible. By default, it is suppressed.

RADIUS

Remote Authentication Dial In User Service (RADIUS) é um protocolo de rede que fornece gerenciamento centralizado de Autenticação, Autorização e Contabilização (Accounting em inglês) para usuários que conectam-se a e utilizam um serviço de rede.
RADIUS é um protocolo do tipo cliente/servidor que roda como um protocolo da camada de aplicação, usa como apoio o protocolo de transferência UDP.

RADIUS (cont)

Tanto Servidores de Acesso Remoto (RAS), como servidores de Redes Virtuais Privadas (VPNs) e Servidores de Acesso a Rede (NAS), e todos os gateways que controlam o acesso a rede possuem um componente cliente do protocolo RADIUS que se comunica com o servidor RADIUS. Este servidor normalmente é um processo de background rodando no UNIX ou Microsoft Windows server.[3]. O servidor RADIUS possui três funções básicas: autenticação de usuários ou dispositivos antes da concessão de acesso a rede. autorização de outros usuários ou dispositivos a usar determinados serviços providos pela rede.
para informar sobre o uso de outros serviços.
O protocolo RADIUS é resumidamente, um serviço baseado em UDP de pergunta e resposta. As requisições e respostas seguem uma padrão de tabelas (variável-=valor).

w

Show who is logged on and what they are doing.
-h, --no-header
Don't print the header.
-u, --no-current
Ignores the username while figuring out the current
process and cpu times. To demonstrate this, do a su and
do a w and a w -u.
-s, --short
Use the short format. Don't print the login time, JCPU or
PCPU times.
-f, --from
Toggle printing the from (remote hostname) field. The
default as released is for the from field to not be
printed, although your system administrator or

w (cont)

distribution maintainer may have compiled a version in
which the from field is shown by default.
--help Display help text and exit.
-i, --ip-addr
Display IP address instead of hostname for from field.
-p, --pids
Display pid of the login process/the "what" process in the
"what" field.
-V, --version
Display version information.
-o, --old-style
Old style output. Prints blank space for idle times less
than one minute.
user Show information about the specified user only.

mount

Option	Description
-a	Mounts all file systems listed in /etc/fstab.
-F	Forks a new incarnation of mount for each device. Must be used in combination with the -a option.
-h	Displays the help file with all command options.
-l	Lists all the file systems mounted and adds labels to each device.
-L [label]	Mounts the partition with the specified [label].
-M	Moves a subtree to another location.

mount (cont)

-O [opts]	Used in combination with -a, it limits the file system set that -a applies to.
-r	Mounts the file system in read-only mode
-R	Remounts a subtree in a different location, making its contents available in both places.
-t [type]	Indicates the file system type.
-T	Used to specify an alternative /etc/fstab file.
-v	Mounts verbosely, describing each operation.
-V	Displays the program version information.

touch

change file timestamps
-a change only the access time
-c, --no-create
do not create any files
-d, --date=STRING
parse STRING and use it instead of current time
-f (ignored)
-h, --no-dereference
affect each symbolic link instead of any referenced file
(useful only on systems that can change the timestamps of
a symlink)
-m change only the modification time
-r, --reference=FILE
use this file's times instead of current time
-t STAMP
use [[CC]YY]MMDDhhmm[.ss] instead of current time
--time=WORD
change the specified time: WORD is access, atime, or use:

touch (cont)

equivalent to -a WORD is modify or mtime: equivalent to -m

NSLOOKUP

nslookup é uma ferramenta comum ao Windows e ao Linux e utilizada para se obter informações sobre registros de DNS de um determinado domínio, host ou ip.
Ele pode trabalhar de duas formas: modo interativo ou não interativo
Modo interativo - o comando interage com vários servidores de domínios e com várias máquinas. O comando executa neste modo quando o primeiro argumento é o endereço ou o nome de um servidor de domínio do qual serão mostradas as informações.
Modo não interativo - o comando interage apenas com uma máquina específico. O comando entra nesse modo quando nenhum argumento de configuração é fornecido, ou quando o primeiro argumento é um sinal de menos (-) e o segundo argumento é o nome de uma máquina ou de um servidor de domínios.
Um conjunto de argumentos podem ser especificados no arquivo .nslookup, no diretório "home" do usuário.

IP E IF CONFIG

IPCONFIG - Windows - nao possibilita o gerenciamento, só consulta
IFCONFIG - Linux - gerenciamento, controle e consulta

Comandos

Comando	Descrição	Exemplo
newgrp	Muda, temporari-amente, o grupo do usuário	newgrp [nome_-do_grupo]
groupadd	cria um novo grupo de usuários	groupadd [nome_-do_grupo]

Comandos (cont)

groupdel	deleta um grupo de usuários do sistema	groupdel [nome_-do_grupo]
groupmod	modifica um grupo de usuário. -n para nome, -g altera gid, -o altera gid mesmo que outro grupo ja possua esse gidg paras do sistema	groupmod -n [nome_-novo] [nome_-antigo]
groups	exibe os nomes dos grupos aos quais um usuário pertence	-
chgrp	comando altera o nome de grupo de arquivos. -c : informa quais arquivos estão tendo o nome de grupo alterado, -v : informa quais arquivos estão sendo proces-sados (não necessariamente alterados), -R : altera, recursiva-mente, o nome de grupo dos arquivos.	chgrp [opções] [grupo] [arquivo]

Comandos (cont)

chown	permite alterar o nome do dono e/ou do grupo de arquivos. -c : informa quais arquivos estão sendo alterados, -h : altera o link, não o arquivo apontado pelo link, -v : informa quais arquivos estão sendo processados (não necessariamente alterados), -R : altera, recursiva-mente, dono e/ou grupo de arquivos.	chown [dono][:g-rupo] [arquivo]
chroot	muda o diretório root do processo corrente e de seus processos filhos.	chroot <diretóri-o> [comando]
usermod	utilizado para modificar parâmetros do usuário.	usermod [parâm-etro] [grupo] [usuário]

ssh

sshd_config - OpenSSH SSH daemon configuration file
sshd(8) reads configuration data from /etc/ssh/sshd_config (or the file specified with -f on the command line). The file contains keyword-argument pairs, one per line. Lines starting with '#' and empty lines are interpreted as comments. Arguments may optionally be enclosed in double quotes (") in order to represent arguments containing spaces.
ssh_config - OpenSSH SSH client config-uration files

TTL

TTL = TIME TO LIVE
UNIX 255
Linux 64
Windows 128

TACACS+

Em redes de computadores, o protocolo TACACS+ (Terminal Access Controller Access-Control System Plus) providencia acesso a roteadores, servidores de redes e outros equipamentos de rede. O TACACS+ providencia separadamente autenticação, autorização e serviços de contas. Com ele é possível realizar a autenticação do usuário de acesso junto a uma conta previamente cadastrada no AD(Active Directory)
Um cliente coleta o nome de usuário e a senha e então envia uma consulta a um servidor de autenticação TACACS, as vezes chamado de TACACS daemon ou simplesmente TACACSD. Baseado na resposta desta consulta, o acesso ao usuário e liberado ou não.
Outra versão do TACACS lançada em 1990 foi batizada de XTACACS (extended TACACS). Entretanto, estas duas versões vem sendo substituídas pelo TACACS+ e pelo RADIUS em redes mais novas. Apesar do nome, TACACS+ é um protocolo completamente novo e não é compatível com TACACS ou XTACACS.
TACACS é definido pela RFC 1492, usando tanto TCP como UDP e por padrão a porta 49

whodo

Prints information on all processes for a terminal, as well as the child processes. (who is doing what)
-h Suppress the heading that is printed on the output.
-l Produce a long form of output. A summary of the current activity on the system is printed. The summary includes the following:
User

whodo (cont)

Who is logged on.
tty
Name of the tty the user is on.
login@
Time of day the user logged on.
idle
Number of minutes since a program last attempted to read from the terminal.
JCPU
System unit time used by all processes and their children on that terminal.
PCPU
System unit time used by the currently active process.
what
Name and parameters of the current process.
The heading line of the summary shows the current time of day, how long the system has been up, the number of users logged into the system.
-X Prints all available characters of each user name instead of truncating to the first 8 characters. The user name is also moved to the last column of the output.

TAIL / HEAD

TAIL
Print the last 10 lines of each FILE to standard output. With
more than one FILE, precede each with a header giving the file
name.
With no FILE, or when FILE is -, read standard input.
Mandatory arguments to long options are mandatory for short
options too.
-c, --bytes=[+]NUM
output the last NUM bytes; or use -c +NUM to output

TAIL / HEAD (cont)

starting with byte NUM of each file
-f, --follow[={name|descriptor}]
output appended data as the file grows;
an absent option argument means 'descr-iptor'
-F same as --follow=name --retry
-n, --lines=[+]NUM
output the last NUM lines, instead of the last 10; or use
-n +NUM to skip NUM-1 lines at the start
--max-unchanged-stats=N
with --follow=name, reopen a FILE which has not
changed size after N (default 5) iterations to see if it
has been unlinked or renamed (this is the usual case of
rotated log files); with inotify, this option is rarely
useful
--pid=PID
with -f, terminate after process ID, PID dies
-q, --quiet, --silent
never output headers giving file names
--retry
keep trying to open a file if it is inaccessible
-s, --sleep-interval=N
with -f, sleep for approximately N seconds (default 1.0)
between iterations; with inotify and --pid=P, check
process P at least once every N seconds
-v, --verbose
always output headers giving file names
-z, --zero-terminated
line delimiter is NUL, not newline
HEAD
Print the first 10 lines of each FILE to standard output. With

TAIL / HEAD (cont)

more than one FILE, precede each with a header giving the file
name.
With no FILE, or when FILE is -, read standard input.
Mandatory arguments to long options are mandatory for short
options too.
-c, --bytes=[-]NUM
print the first NUM bytes of each file; with the leading
'-', print all but the last NUM bytes of each file
-n, --lines=[-]NUM
print the first NUM lines instead of the first 10; with
the leading '-', print all but the last NUM lines of each
file
-q, --quiet, --silent
never print headers giving file names
-v, --verbose
always print headers giving file names
-z, --zero-terminated
line delimiter is NUL, not newline

shred

Overwrite the specified FILE(s) repeatedly, in order to make it harder for even very expensive hardware probing to recover the data.
Mandatory arguments to long options are mandatory for short options too.
-f, --force
change permissions to allow writing if necessary
-n, --iterations=N
overwrite N times instead of the default (3)
--random-source=FILE
get random bytes from FILE
-s, --size=N

shred (cont)

shred this many bytes (suffixes like K, M, G accepted)
-u, --remove
truncate and remove file after overwriting
-v, --verbose
show progress
-x, --exact
do not round file sizes up to the next full block;
this is the default for non-regular files
-z, --zero
add a final overwrite with zeros to hide shredding

PASSWD

Altera as senhas dos usuários.
-d : deleta a senha de um usuário.
-e : passa a considerar a senha expirada. Isto significa que o usuário terá que alterar a senha no próximo login.
-u : a atualização só é efetuada após a data de expiração da senha atual.
As senhas dos usuários são armazenadas no arquivo /etc/passwd. Caso o sistema shadow esteja sendo usado, as senhas são criptografadas e armazenadas no arquivo /etc/shadow.
O comando vipw edita os arquivos /etc/passwd e /etc/shadow.

Shadow/GShadow

O sistema shadow consiste no uso do arquivo /etc/shadow para armazenar as senhas criptografadas das contas dos usuários.
O sistema gshadow consiste no uso do arquivo /etc/gshadow para armazenar as senhas criptografadas dos grupos do sistema.
O comando pwconv ativa o uso do sistema shadow.
O comando pwunconv desativa o uso do sistema shadow de proteção de senhas.
O comando vipw edita os arquivos /etc/passwd e /etc/shadow.

Shadow/GShadow (cont)

O comando grpconv ativa o sistema gshadow para proteger as senhas dos grupos.
O comando grpunconv elimina o uso do sistema gshadow de proteção de senhas.
O comando vigr edita os arquivos /etc/group e /etc/gshadow.

umask

Quando o usuário cria um arquivo (diretório), o sistema associa ao objeto criado um conjunto de permissões de acesso. Estas permissões indicam quem pode ler, alterar e/ou executar (acessar) o arquivo (diretório).
Por padrão,
as permissões iniciais de um arquivo são 0666 (leitura e gravação para todo e qualquer usuário do sistema);
as permissões iniciais de um diretório são 0777 (leitura, gravação e acesso para todo e qualquer usuário do sistema).
Quando um usuário cria um arquivo (ou diretório), o sistema associa a este arquivo (diretório) o resultado da operação "permissão padrão" – umask
onde umask tem as permissões não liberadas para os usuários.
O termo umask corresponde a "user mask", ou seja, máscara do usuário.
O comando chmod permite alterar as permissões de acesso de arquivos/diretórios.

Run Levels

Run Level	Description
0	System halt i.e., the system can be safely powered off with no activity.
1	Single user mode.

Run Levels (cont)

2	Multiple user mode with no NFS (network file system).
3	Multiple user modes under the command line interface and not under the graphical user interface.
4	User-definable.
5	Multiple user mode under GUI (graphical user interface) and this is the standard runlevel for most of the LINUX-based systems.
6	Reboot which is used to restart the system.

KILL

terminate a process
pid
Each pid can be expressed in one of the following ways:
n
where n is larger than 0. The process with PID n is
signaled.
0
All processes in the current process group are signaled.
-1
All processes with a PID larger than 1 are signaled.
-n
where n is larger than 1. All processes in process group
n are signaled. When an argument of the form '-n' is
given, and it is meant to denote a process group, either
a signal must be specified first, or the argument must be
preceded by a '--' option, otherwise it will be taken as

KILL (cont)

the signal to send.
name
All processes invoked using this name will be signaled.
OPTIONS top
-s, --signal signal
The signal to send. It may be given as a name or a number.
-l, --list [number]
Print a list of signal names, or convert the given signal
number to a name. The signals can be found in
/usr/include/linux/signal.h.
-L, --table
Similar to -l, but it will print signal names and their
corresponding numbers.
-a, --all
Do not restrict the command-name-to-PID conversion to
processes with the same UID as the present process.
-p, --pid
Only print the process ID (PID) of the named processes, do
not send any signals.
-r, --require-handler
Do not send the signal if it is not caught in userspace by
the signalled process.

ethtool

é possível verificar quais são as interfaces, mudar velocidade, alterar forma de negociação e é até mesmo verificar qual interface está localizada fisicamente.
Mostrar a velocidade da placa de rede, assim como a velocidade suportada para a interface:
ethtool [interface]

ethtool (cont)

Mostrar as estatísticas de rx e tx para a interface:
ethtool -S [interface]
Deixar a interface piscando para podermos descobrir qual é a interface fisicamente:
ethtool -p [interface] [tempo]
Manipular a velocidade da interface, assim como as formas de negociação:
ethtool -s [interface] speed [velocidade] duplex [half | full]

LASTB

exibe informações sobre as tentativas mal sucedidas de se logar ao sistema.
-a : exibe o nome da máquina onde foi efetuada a tentativa de login.
-d : exibe o número de IP da máquina remota onde foi efetuada a tentativa de login.
-f arquivo : define o nome do arquivo de onde serão extraídas as informações sobre as tentativas de login. Por padrão, o arquivo lido é o /var/log/btmp.
O comando lastb exige permissão de administrador (sudo) para ser executado.
Caso nenhum argumento seja passado, o comando lastb exibe todas as informações armazenadas no arquivo /var/log/btmp que possui todas as tentativas de login efetuadas no sistema.
Se não existirem registros de tentativas mal sucedidas de acessar o sistema, o comando fornecerá apenas a data de criação do arquivo /var/log/btmp (provavelmente, esta data corresponderá à data de instalação do sistema).
O comando last funciona da mesma forma do comando lastb. Entretanto, ele usa, por padrão, o arquivo /var/log/wtmp que possui informações referentes a entrada (login) e saída (logout) de usuários do sistema.

NICE / RENICE

NICE
run a program with modified scheduling priority
Run COMMAND with an adjusted niceness, which affects process scheduling. With no COMMAND, print the current niceness. Nicenesses range from -20 (most favorable scheduling) to 19 (least favorable).
-n, --adjustment=N
add integer N to the niceness (default 10)
RENICE
alter priority of running processes
-n priority
Specify the absolute or relative (depending on environment
variable POSIXLY_CORRECT) scheduling priority to be used for
the process, process group, or user. Use of the option -n is
optional, but when used, it must be the first argument. See
NOTES for more information.
--priority priority
Specify an absolute scheduling priority. Priority is set to
the given value. This is the default, when no option is
specified.
--relative priority
Specify a relative scheduling priority. Same as the standard
POSIX -n option. Priority gets incremented/-decremented by the
given value.
-g, --pgrp
Interpret the succeeding arguments as process group IDs.
-p, --pid
Interpret the succeeding arguments as process IDs (the

NICE / RENICE (cont)

default).

-u, --user

Interpret the succeeding arguments as usernames or UIDs.

By **xoulea**
cheatography.com/xoulea/

Published 8th January, 2024.
Last updated 8th January, 2024.