

ENGENHARIA DA COMPUTAÇÃO
UNIVERSIDADE FEDERAL DO MARANHÃO



Estudo Analítico de um Sistema Operacional Real: UBUNTU 24.04.2 LTS

Aluno : Juan Pablo Furtado

1

Gerência de Processos



Como o sistema cria e gerencia processos

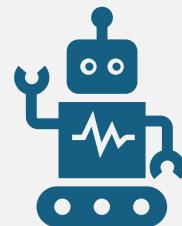
Main	I/O	PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
		2601	eryk	20	0	3768M	303M	135M	S	20.1	4.0	0:31.77	/usr/bin/gn
		805	avahi	20	0	14496	10296	4024	S	14.9	0.1	4:31.33	avahi-daemon
		6303	eryk	20	0	2795M	101M	83692	S	11.0	1.3	0:00.17	/usr/bin/gjs
		6306	eryk	20	0	707M	84836	69860	S	7.1	1.1	0:00.11	/usr/bin/gn
		6307	eryk	20	0	422M	28924	23036	R	7.1	0.4	0:00.11	/usr/bin/sea
		6016	eryk	20	0	9464	5864	3816	R	4.5	0.1	0:04.93	htop
		842	root	20	0	327M	21236	17140	S	1.3	0.3	0:13.55	/usr/sbin/N
		2402	eryk	20	0	11048	6716	4668	S	1.3	0.1	0:00.57	/usr/bin/dbu
		2624	eryk	-21	0	3768M	303M	135M	S	1.3	4.0	0:03.86	/usr/bin/gn
		6336	eryk	20	0	707M	84836	69860	R	1.3	1.1	0:00.02	/usr/bin/gn
		2411	eryk	20	0	306M	10460	9436	S	0.6	0.1	0:00.04	/usr/bin/gn
		2436	eryk	20	0	738M	7856	7088	S	0.6	0.1	0:00.03	/usr/libexec
		2615	eryk	20	0	9480	5232	4720	S	0.6	0.1	0:00.02	/usr/bin/dbu
		2620	eryk	20	0	3768M	303M	135M	S	0.6	4.0	0:00.96	/usr/bin/gn
		2747	eryk	20	0	377M	12768	7540	S	0.6	0.2	0:01.41	/usr/bin/ib
		2784	eryk	20	0	377M	12768	7540	S	0.6	0.2	0:02.20	/usr/bin/ib
		3255	eryk	20	0	2663M	55292	41140	S	0.6	0.7	0:00.60	gjs /usr/sha
		4250	eryk	20	0	692M	62728	49312	S	0.6	0.8	0:01.55	/usr/libexec
		5667	eryk	20	0	1462M	127M	71160	S	0.6	1.7	0:02.27	/usr/bin/rhy
		5669	eryk	20	0	1462M	127M	71160	S	0.6	1.7	0:04.07	/usr/bin/rhy
		6129	eryk	20	0	1079M	99.2M	80264	S	0.6	1.3	0:00.29	/usr/bin/nau
		6302	eryk	20	0	512M	17736	15816	S	0.6	0.2	0:00.01	/usr/libexec

Execução da chamada de sistema fork():

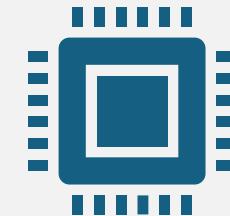
```
[11:26] ~ Bash
[~]
> ps -ef | grep bash
eryk      3991  2601  0 10:51 ?        00:00:00 /bin/bash /usr/bin/brave-browser-stable
eryk      4259  4250  0 10:52 pts/0    00:00:00 bash
eryk      7071  4259  0 11:26 pts/0    00:00:00 grep --color=auto bash
```

- Assim que um programa é aberto o sistema executa a função fork que cria um clone exatamente igual do programa que está sendo executado, porém com um PID diferentes, pois é tratado como uma instância separada.

Execução da função exec():



A FUNÇÃO EXEC() NÃO CRIA UM NOVO PROCESSO; ELA TRANSFORMA O PROCESSO ATUAL. EM TERMOS DE SISTEMA OPERACIONAL, ELA REALIZA UMA **SUBSTITUIÇÃO SUBSTITUIÇÃO DA IMAGEM DO PROCESSO.**



NO LINUX (E, PORTANTO, NO UBUNTU), QUANDO UM PROGRAMA CHAMA EXECVE() (A SYSCALL BASE PARA TODAS AS VARIANTES EXECL, EXECP, ETC.)

Usa o Init ou systemd como “pai de todos”:

```
[12:06] ✘ Bash
└─
  └── pstree -p
    systemd(1) ── ModemManager(1859) ── {ModemManager}(1072)
    └── {ModemManager}(1073)
    └── {ModemManager}(1075)
    NetworkManager(842) ── {NetworkManager}(979)
    └── {NetworkManager}(984)
    └── {NetworkManager}(988)
    accounts-daemon(825) ── {accounts-daemon}(1011)
    └── {accounts-daemon}(1012)
    └── {accounts-daemon}(1023)
    auditd(515) ── {auditd}(516)
    avahi-daemon(805) ── avahi-daemon(844)
    bluetoothd(806)
    colord(1452) ── {colord}(1471)
    └── {colord}(1472)
    └── {colord}(1475)
    containerd(1214) ── {containerd}(1223)
    └── {containerd}(1224)
    └── {containerd}(1225)
    └── {containerd}(1226)
    └── {containerd}(1236)
    └── {containerd}(1237)
    └── {containerd}(3969)
    containerd-shim(2121) ── gunicorn(2145) ── gunicorn(2320) ── {gunicorn}(8857)
    └── {containerd-shim}(2122)
    └── {containerd-shim}(2123)
    └── master(2304) ── pickup(2305)
    └── qmgr(2306)
```

```
[11:26] ✘ Bash
└─
  └── ps -p 1 -o pid,comm,etime
      PID COMMAND          ELAPSED
      1  systemd            01:19:49
```

top - 14:59:42 up 4:12, 1 user, load average: 0,98, 0,94, 0,96										
Tarefas: 250 total, 1 em exec., 249 dormindo, 0 parado, 0 zumbi										
%CPU(s): 5,9 us, 2,2 sy, 0,0 ni, 91,0 id, 0,7 wa, 0,0 hi, 0,2 si, 0,0 st										
MB mem : 7665,4 total, 664,9 free, 3627,6 used, 4215,0 buff/cache										
MB swap: 12288,8 total, 12287,7 free, 0,2 used. 4037,8 avail mem										
PID	USUARIO	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TEMPO+ COMANDO
2601	eryk	20	0	3951948	329992	140236	S	8,3	4,2	4:33.42 gnome-shell
805	avahi	20	0	14640	10424	4024	S	3,0	0,1	21:31.50 avahi-daemon
5649	eryk	20	0	1500660	134648	71416	S	1,3	1,7	1:37.08 rhythmbox
160	root	-51	0	0	0	0	S	1,0	0,0	1:08.30 irq/133-ELAN0B00:00
2386	eryk	20	0	405980	20864	15488	S	0,7	0,3	0:45.13 wireplumber
4000	eryk	20	0	33,0g	509668	275000	S	0,7	6,5	4:45.81 brave
4049	eryk	20	0	32,6g	190424	155184	S	0,7	2,4	1:28.70 brave
5509	eryk	20	0	1410,2g	357968	155052	S	0,7	4,6	7:12.07 brave
10848	root	0	-20	0	0	0	D	0,7	0,0	0:01.20 kworker/u9:0+i915_flip
11058	root	20	0	0	0	0	I	0,7	0,0	0:01.16 kworker/0:1-events
2388	eryk	20	0	125516	29292	10352	S	0,3	0,4	0:26.75 pipewire-pulse
11137	root	20	0	0	0	0	I	0,3	0,0	0:00.74 kworker/1:0-i915-unordered
11439	eryk	20	0	12128	6140	3964	R	0,3	0,1	0:00.20 top
1	root	20	0	23464	14752	9632	S	0,0	0,2	0:04.29 systemd
2	root	20	0	0	0	0	S	0,0	0,0	0:00.00 kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:00.00 pool_workqueue_release
4	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/R-rcu_gp
5	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/R-sync_wq
6	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/R-slub_flushwq
7	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/R-netns
9	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/0:0H-events_highpri
12	root	0	-20	0	0	0	I	0,0	0,0	0:00.00 kworker/R-mm_percpu_wq
13	root	20	0	0	0	0	I	0,0	0,0	0:00.00 rcu_tasks_kthread
14	root	20	0	0	0	0	I	0,0	0,0	0:00.00 rcu_tasks_rude_kthread

adicionar mais núcleos na CPU

```
[15:35] ✘ Bash
└─~
  > lscpu
Arquitetura:          x86_64
  Modo(s) operacional da CPU: 32-bit, 64-bit
  Address sizes:           39 bits physical, 48 bits virtual
  Ordem dos bytes:         Little Endian
CPU(s):                2
  Lista de CPU(s) on-line: 0,1
ID de fornecedor:      GenuineIntel
  Nome do modelo:         Intel(R) Celeron(R) 6305 @ 1.80GHz
  Família da CPU:        6
  Modelo:                 140
  Thread(s) per núcleo:  1
  Núcleo(s) por soquete: 2
  Soquete(s):            1
  Step:                  1
  CPU(s) scaling MHz:    76%
  CPU MHz máx.:          1800,0000
  CPU MHz min.:          400,0000
  BogoMIPS:               3609,60
```

Barras de utilização da CPU via terminal htop



Como o usuário ou o administrador pode visualizar, controlar ou encerrar processos



Monitor do Sistema Ubuntu



Comando	Função
kill -STOP <PID>	Pausa temporariamente a execução de um processo
kill -CONT <PID>	Retoma um processo pausado anteriormente
pkill <nome>	Encerra processos pelo nome
xkill	Modo gráfico: clique em uma janela para encerrá-la
stress -c <n>	Simula carga de CPU com n processos paralelos
lscpu	Exibe informações sobre núcleos e threads da CPU
fg %<número>	Retorna um processo do segundo para primeiro plano

2

Gerência de Memória

Swap do sistema Ubuntu.

```
[18:05] ✘ Bash
└─~
  ↳ free -h
      total        used        free      shared  buff/cache   available
Mem:       7.6Gi     668Mi     6.7Gi      3.8Mi     350Mi     6.9Gi
Swap:      2.0Gi          0B     2.0Gi
```

Tabela com lista de processos

Top - 2023-06-20 10:45:40												
	Main	I/O		Mem			Swap			CPU% ▷ MEM%	TIME+	Command
		PID	USER	PRI	NI	VIRT	RES	SHR	S			
	1	root	20	0	21940	12656	9456	S	0.0	0.2	0:00.47	/sbin/init
	2	root	20	0	3060	1664	1664	S	0.0	0.0	0:00.00	/init
	7	root	20	0	3076	1792	1792	S	0.0	0.0	0:00.00	plan9 --control-so
	8	root	20	0	3076	1792	1792	S	0.0	0.0	0:00.00	plan9 --control-so
	9	root	20	0	3060	1664	1664	S	0.0	0.0	0:00.00	/init

ferramentas para monitoramento

Comando	Descrição
<code>free -h</code>	Mostra o uso atual da memória RAM e da área de swap, com valores legíveis (em MB/GB).
<code>htop</code>	Interface interativa que mostra o uso de CPU, RAM, swap e detalhes de cada processo.
<code>top</code>	Similar ao <code>htop</code> , exibe o uso da CPU e da memória em tempo real, mas de forma mais simples.
<code>vmstat</code>	Mostra estatísticas de memória virtual, processos, E/S e uso da CPU.
<code>cat /proc/meminfo</code>	Exibe detalhes técnicos da memória do sistema, incluindo buffers, cache, <code>swap</code> , etc.
<code>cat /proc/<PID>/status</code>	Mostra o consumo de memória de um processo específico, incluindo <code>VmSize</code> , <code>VmRSS</code> e <code>VmSwap</code> .
<code>cat /proc/vmstat</code>	<code>grep -E 'pg</code>
<code>cat /proc/<PID>/oom_score</code>	Exibe a pontuação de um processo para o OOM Killer (quanto mais alto, maior a chance de ser morto).

3

Gerência de Arquivos

“ext4” como sistema de arquivos montado

```
ls@JuanPablo484806:~$ df -T -x tmpfs -x devtmpfs
Filesystem      Type      1K-blocks      Used   Available  Use% Mounted on
none            overlay       1924712          0    1924712   0% /usr/lib/modules/6.6.87.2-microsoft-standard-WSL2
drivers          9p        498406724  219991728  278414996  45% /usr/lib/wsl/drivers
/dev/sdd         ext4       1055762868  3237412  998821984  1% /
none            overlay       1924712          0    1924712   0% /usr/lib/wsl/lib
rootfs           rootfs      1919700        2664    1917036   1% /init
none            overlay       1924712          76    1924636   1% /mnt/wslg/versions.txt
none            overlay       1924712          76    1924636   1% /mnt/wslg/doc
C:\             9p        498406724  219991728  278414996  45% /mnt/c
```

diretórios

/bin e /sbin:	Comandos essenciais para todos os usuários e para operações em modo de usuário único
/etc	Arquivos de configuração do sistema, com lógica de "tudo que não é binário" que permanece estático;
/usr	Hierarquia secundária, destinada a utilitários e aplicações de múltiplos usuários, geralmente em modo somente-leitura;
/var	Dados variáveis (logs, caches, spools), cujo conteúdo muda continuamente em tempo de execução;
/home	Diretórios pessoais dos usuários, onde residem documentos e configurações individuais;
/tmp	Área para arquivos temporários, frequentemente limpa a cada reinicialização.

nível da hierarquia de diretórios

```
bin -> usr/bin
bin usr-is-merged
boot
dev
etc
home
init
lib -> usr/lib
lib usr-is-merged
lib64 -> usr/lib64
lost+found
media
mnt
opt
proc
root
run
sbin -> usr/sbin
sbin usr-is-merged
snap
srv
sys
```

permissões

```
ls@JuanPablo484806:~$ sudo apt update && sudo apt install acl
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1391 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1684 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [225 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [9504 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [916 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [207 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [71.5 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.4 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [2286 kB]
Get:15 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [311 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [523 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:20 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [15.8 kB]
Get:21 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1506 kB]
Get:22 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [306 kB]
Get:23 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [378 kB]
Get:24 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [31.4 kB]
Get:25 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2413 kB]
Get:26 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [550 kB]
Get:27 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:28 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [516 B]
Get:29 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [30.3 kB]
Get:30 http://archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [6048 B]
Get:31 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:32 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [488 B]
Get:33 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Packages [40.4 kB]
Get:34 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7288 B]
Get:35 http://archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [368 B]
Get:36 http://archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [29.5 kB]
```

```
Get:40 http://archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:41 http://archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 13.6 MB in 5s (2627 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
59 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  acl
0 upgraded, 1 newly installed, 0 to remove and 59 not upgraded.
Need to get 39.4 kB of archives.
After this operation, 197 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 acl amd64 2.3.2-1build1.1 [39.4 kB]
Fetched 39.4 kB in 1s (44.7 kB/s)
Selecting previously unselected package acl.
(Reading database ... 47774 files and directories currently installed.)
Preparing to unpack .../acl_2.3.2-1build1.1_amd64.deb ...
Unpacking acl (2.3.2-1build1.1) ...
Setting up acl (2.3.2-1build1.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
ls@JuanPablo484806:~$ getfacl /home
getfacl: Removing leading '/' from absolute path names
# file: home
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

entradas estendidas de ACL

Exemplos de operações básicas

```
ls@JuanPablo484806:~$ # 1. Preparar o ambiente (criar arquivos que faltam)
mkdir -p backup entrega
touch documento.pdf relatório.docx arquivo_antigo.tmp

# 2. Executar as operações da imagem
touch novo_arquivo.txt
mkdir -p projeto_exemplo
cp documento.pdf backup/documento.pdf
mv relatório.docx entrega/relatorio.docx
rm -i arquivo_antigo.tmp # Responda 'y' se pedir confirmação
ls -lah
rm: remove regular empty file 'arquivo_antigo.tmp'?
total 72K
drwxr-x--- 13 ls  ls  4.0K Dec 24 11:52 .
drwxr-xr-x  3 root root 4.0K Nov 24 18:19 ..
-rw-------  1 ls  ls   841 Nov 26 17:04 .bash_history
-rw-r--r--  1 ls  ls   220 Nov 24 18:19 .bash_logout
-rw-r--r--  1 ls  ls   3.7K Nov 24 18:19 .bashrc
drwx-----  4 ls  ls  4.0K Nov 26 15:05 .cache
drwxr-xr-x  3 ls  ls  4.0K Nov 26 15:05 .dotnet
drwxr-xr-x  3 ls  ls  4.0K Nov 26 15:59 .ipython
drwxr-xr-x  2 ls  ls  4.0K Nov 26 15:01 .landscape
-rw-r--r--  1 ls  ls     0 Dec 24 11:26 .motd_shown
-rw-r--r--  1 ls  ls   807 Nov 24 18:19 .profile
-rw-r--r--  1 ls  ls     0 Nov 24 18:51 .sudo_as_admin_successful
drwxr-xr-x  4 ls  ls  4.0K Nov 26 15:03 .vscode-remote-containers
drwxr-xr-x  5 ls  ls  4.0K Nov 26 15:05 .vscode-server
-rw-r--r--  1 ls  ls   268 Nov 26 15:05 .wget-hsts
drwxr-xr-x  3 ls  ls  4.0K Nov 24 18:28 Documentos
-rw-r--r--  1 ls  ls     0 Dec 24 11:52 arquivo_antigo.tmp
drwxr-xr-x  2 ls  ls  4.0K Dec 24 11:52 backup
-rw-r--r--  1 ls  ls     0 Dec 24 11:52 documento.pdf
drwxr-xr-x  2 ls  ls  4.0K Dec 24 11:52 entrega
-rw-r--r--  1 ls  ls     0 Dec 24 11:52 novo_arquivo.txt
drwxr-xr-x  3 ls  ls  4.0K Nov 26 15:55 pipeline_dados
drwxr-xr-x  2 ls  ls  4.0K Dec 24 11:51 projeto_exemplo
```

Saída do comando

```
ls@JuanPablo484806:~$ echo '#!/bin/bash' > script.sh
echo 'echo Olá, mundo!' >> script.sh
chmod 750 script.sh
ls -l script.sh
-rwxr-x--- 1 ls ls 30 Dec 24 11:56 script.sh
ls@JuanPablo484806:~$ ./script.sh
Olá, mundo!
```



4 Proteção e Segurança

Configuração típica de autenticação PAM em Ubuntu

```
ls@JuanPablo484806:~$ cat /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok
# here's the fallback if no module succeeds
auth    requisite                  pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                   pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                  pam_cap.so
# end of pam-auth-update config
```

Partições em Ubuntu 24.04.2 LTS.

```
ls@JuanPablo484806:~$ lsblk -o NAME,FSTYPE,SIZE,TYPE,MOUNTPOINT | grep crypt
cryptsetup status /dev/mapper/ubuntu--vg-root
Command 'cryptsetup' not found, but can be installed with:
sudo apt install cryptsetup-bin
```

Usuários com Permissão para Sudo

```
ls@JuanPablo484806:~$ getent group sudo
```

```
sudo:x:27:ls
```

verificação do SELinux com sestatus.

```
ls@JuanPablo484806:~$ aa-status  
sestatus  
apparmor module is loaded.  
apparmor filesystem is not mounted.  
Command 'sestatus' not found, but can be installed with:  
sudo apt install policycoreutils
```