

Gerenciamento de Usuários e Grupos



Rodrigo Vieira

Oct 16, 2016 · 6 min read

O Linux executa diversos processos simultaneamente e cada processo em execução pertence a um usuário do sistema. De acordo com esse usuário é que o processo terá permissões para acessar recursos específicos do sistema.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1	root	20	0	30196	1728	1424	S	0.0	0.1	0:00.11	avahi-daemon: running [server1.local]
716	avahi	20	0	30072	240	0	S	0.0	0.0	0:00.00	avahi-daemon: chroot helper
674	chrony	20	0	113M	1844	1476	S	0.0	0.1	0:00.04	/usr/sbin/chronyd
1712	colord	20	0	394M	5988	4408	S	0.0	0.3	0:00.00	/usr/libexec/colord
1716	colord	20	0	394M	5988	4408	S	0.0	0.3	0:00.00	/usr/libexec/colord
1782	colord	20	0	394M	5988	4408	S	0.0	0.3	0:00.09	/usr/libexec/colord
697	dbus	20	0	101M	3420	1472	S	0.0	0.2	0:00.00	/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
669	dbus	20	0	101M	3420	1472	S	0.0	0.2	0:03.45	/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
652	libstorag	20	0	8532	800	656	S	0.0	0.0	0:00.10	/usr/bin/lsm -d
1597	nobody	20	0	15552	860	676	S	0.0	0.0	0:00.06	/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/usr/libexec/libvirt_leas
761	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:00.10	/usr/lib/polkit-1/polkitd --no-debug
762	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:00.56	/usr/lib/polkit-1/polkitd --no-debug
763	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:00.00	/usr/lib/polkit-1/polkitd --no-debug
766	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:00.02	/usr/lib/polkit-1/polkitd --no-debug
770	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:00.56	/usr/lib/polkit-1/polkitd --no-debug
750	polkitd	20	0	522M	18068	5008	S	0.0	0.9	0:09.41	/usr/lib/polkit-1/polkitd --no-debug
1600	postfix	20	0	93396	3940	2936	S	0.0	0.2	0:00.02	qmgr -l -t unix -u
9888	postfix	20	0	93328	3916	2912	S	0.0	0.2	0:00.01	pickup -l -t unix -u
1	root	20	0	122M	6520	3912	S	0.0	0.3	0:02.98	/usr/lib/systemd/systemd --switched-root --system --deserialize 21
476	root	20	0	36944	4140	3776	S	0.0	0.2	0:01.24	/usr/lib/systemd/systemd-journald
503	root	20	0	126M	5632	2504	S	0.0	0.3	0:00.00	/usr/sbin/lvmtool -f
508	root	20	0	46404	4972	2728	S	0.0	0.2	0:00.23	/usr/lib/systemd/systemd-udev
629	root	16	-4	51212	1612	1232	S	0.0	0.1	0:00.12	/sbin/auditd -n

htop

Na imagem acima podemos ver diversos processos em execução, cada um rodando sob diferentes usuários do sistema (coluna USER): *avahi*, *chrony*, *colord*, *dbus*, *libstrogage*, *nobody*, *root*, ...

Visão Geral

Os comandos abaixo são utilizados para gerenciar usuários:

- **useradd**: possibilita que usuários privilegiados criem novos usuários ou definam atributos para novos usuários.
- **usermod**: modifica contas existentes.
- **userdel**: remove um usuário.

- **passwd:** utilitário para definir senhas, bloquear uma conta ou expirar uma senha.
- **chage:** utilitário para definir atributos de expiração de senha.

Os seguintes **arquivos** estão envolvidos no gerenciamento de usuários:

- **/etc/passwd:** contém informações sobre a conta do usuário.
- **/etc/shadow:** contém a senha e informações sobre a senha.
- **/etc/group:** informações sobre os grupos de usuários.
- **/etc/gshadow:** armazena senhas para grupos, raramente utilizado.
- **/etc/login.defs:** padrões utilizados pelos comandos acima.
- **/etc/default/useradd:** padrões utilizados pelo comando useradd.

. . .

Tipos de usuários

No Linux podemos classificar os usuários em privilegiados e não-privilegiados. Por padrão, o único usuário privilegiado do sistema é o *root*.

O usuário *root* tem acesso total e pode acessar todos os recursos do sistema sem restrição alguma. Por isso essa conta só deve ser utilizada para administrar o sistema. O melhor é sempre utilizar uma conta não-privilegiada e somente quando necessário escalar os privilégios do usuário para uma conta privilegiada.

. . .

id [user]

Para obter informações da conta de um usuário, use o comando **id**. Se não for informado um usuário como parâmetro, o comando irá devolver informações sobre a conta do usuário que está executando o comando.

```
[syscop@server1 ~]$ id
uid=1000(syscop) gid=1000(syscop) groups=1000(syscop),10(wheel)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Neste caso o usuário **syscop** possui:

- **uid:** possui o uid ou user identification de número 1000.
- **gid:** possui o gid ou group identification 1000, que representa o grupo primário *syscop*.
- **groups:** O usuário *syscop* está no seu grupo primário e também no grupo *wheel*.
- **context:** informações utilizadas pelo SELinux para isolar os recursos do usuário. No entanto, este usuário não está confinado, podendo utilizar todos os recursos disponíveis, respeitando suas permissões de acesso.

O comando **whoami** retorna o seu nome de usuário.

. . .

Escalando privilégios

Há três maneiras básicas de sair de um acesso não-privilegiado para um privilegiado:

su

O comando **su** - switch user pode ser usado para alternar para qualquer conta, no entanto o mais comum é seu uso para obter acesso a conta root. Podendo se dar de duas formas, **su** ou **su -**:

```
$ su
# alterna para conta root iniciando um sub-shell
# somente os arquivos /etc/bashrc e ~/.bashrc são executados.
```

```
$ su -
# alterna para a conta root iniciando um login-shell
# os arquivos /etc/profile, /etc/bashrc, ~/.bashrc e
~/.bash_profile são executados, nessa ordem.
```

sudo

O comando **sudo** possibilita que um usuário execute tarefas como um usuário privilegiado, sem a necessidade de usar uma conta privilegiada.

O CentOS 7 já vem preparado para utilizar o grupo wheel como sendo o grupo de usuários com privilégios administrativos. Qualquer usuário pertencente a este grupo

poderá executar comandos de root, simplesmente confirmando sua própria senha.

O comando **visudo** é usado para gerenciar o arquivo de configuração do sudo. Repare no padrão de configuração do CentOS:

visudo

```
## Allows people in group wheel to run all commands
%wheel    ALL=(ALL)        ALL
```

Dessa forma, o usuário que estiver no grupo *wheel* poderá a partir da sua própria conta executar comandos que requerem privilégios:

```
[syscop@server1 ~]$ sudo useradd ada
[sudo] password for syscop:
```

Ao invés de

```
[syscop@server1 ~]$ su -
Password:
[root@server1 ~]# useradd
```

Uma grande vantagem do sudo é o registro de suas operações. Todo comando executado através dele fica registrado nos logs do sistema:

```
Oct 16 16:43:55 server1.umbrella.corp sudo[8417]: syscop :
TTY=pts/1 ; PWD=/home/syscop ; USER=root ; COMMAND=/sbin/useradd
ada
Oct 16 16:43:55 server1.umbrella.corp useradd[8422]: new user:
name=ada, UID=1005, GID=100, home=/home/ada, shell=/bin/bash
```

PoliciKit

Utilizado por programas gráficos que requerem privilégios administrativos. Para saber mais consulte as páginas de manual do **pkexec** e do **polkit**.

. . .

Gerenciando Usuários

Quando criamos um usuário com o comando **adduser** o usuário será cadastrado no arquivo **/etc/passwd**, sua senha criptografada e os dados de expiração da senha ficarão no arquivo **/etc/shadow**, o grupo primário do usuário será cadastrado em **/etc/group**, e os grupos suplementares que porventura o usuário seja colocado receberão este novo usuário neste mesmo arquivo, o **/etc/group**.

```
useradd ada
```

```
tail /etc/passwd
```

```
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
syscop:x:1000:1000:syscop:/home/syscop:/bin/bash
vboxadd:x:988:1::/var/run/vboxadd:/bin/false
lisa:x:1001:1001::/home/lisa:/bin/bash
lori:x:1002:1002::/home/lori:/sbin/nologin
linda2:x:1003:100::/home/linda2:/bin/bash
bob:x:1004:100::/home/bob:/bin/bash
ada:x:1005:1005::/home/ada:/bin/bash
```

Repare na última linha do arquivo:

```
ada:x:1005:1005::/home/ada:/bin/bash
```

O registro do usuário é dividido em campos através do caractere ":", sendo:

- **username (ada):** o nome do usuário. Deve ser único e o mesmo utilizado em **/etc/shadow**.
- **password (x):** antigamente armazenava o hash da senha que hoje fica no **/etc/shadow**.
- **UID (1005):** o número de identificação único deste usuário. O sistema sempre utiliza o próximo UID disponível, iniciando pelo que estiver definido em **/etc/login.defs** no parâmetro **UID_MIN**.
- **GID (1005):** todo usuário deve fazer parte de pelo menos um grupo, dito grupo primário.
- **Comment ():** geralmente contém o nome completo do usuário.

- **Directory (/home/ada):** o diretório inicial do usuário ou *home directory*. Onde um usuário armazena seus arquivos pessoais ou um usuário do sistema armazena os arquivos necessários para sua execução.
- **Shell (/bin/bash):** O comando que será executado logo após o usuário se autenticar no Linux. Geralmente **/bin/bash**, mas alguns usuário não precisam ou não devem ter acesso ao shell, recebendo **/sbin/nologin** neste campo. Você pode colocar um texto em */etc/nologin.txt* que será exibido para usuários que possuem */sbin/nologin* neste campo e tentarem usar um shell de login no sistema.

*O CentOS, a partir da versão 7, utiliza **UID menores que 1000 para usuários do sistema** e de 1000 em diante para usuários comuns.*

```
$ sudo tail /etc/shadow
[sudo] password for syscop:
postfix:!!:17071::::::
ntp:!!:17071::::::
tcpdump:!!:17071::::::
syscop:$6$ON8w6Io7hFZVO8uY$39loAqUwfJeSQX.K.HtQHSeBu/GJHiA4UAULzv
YqnFiu.RpNgkepeVi8HunAEkdcq2slavDpRWPQUTt4JrT6L/::0:99999:7:::
vboxadd:!!:17071::::::
lisa:$6$dtG3joiF$453wh/poueznSj2vuu3Ou/gvBmsZdUfTgjajojrQHNEI11cI
HHBCjtVSpI79zzU8XIPxq8pbKATqe9LMQOJgL1:17087:0:99999:7:::
lori:!!:17087:0:99999:7:::
linda2:$6$3yqCyCkp$LH5/JHkkIMbHehvhGOyVxn/GCQGJDx6WdxCtUpSLzNwWD1
IUN4rdmgoLJYTnCrFLY26fqP3hGR9DJtAR5z9O91:17087:30:90:3:::
bob:!!:17087:0:99999:7:::
ada:!!:17090:0:99999:7:::
```

Repare na última linha que faz referência ao usuário **ada**. Os campos neste arquivo também são separados por ":" e são eles:

- **Login name (ada):** login do usuário, repare que não é utilizado o UID.
- **Encrypted password (!!):** senha criptografada.
- **Dias desde 1970-01-01 até o dia em que a senha foi alterada pela última vez(17090).**
- **Mínimo de dias que o usuário deve permanecer com a nova senha (0):** padrão 0.

- **Número de dias após o qual a senha deve ser alterada (99999):** padrão 99999 (cerca de 273 anos).
- **Dias antes de vencer em que usuário começará a receber alertas (7):** padrão 7.
- **Dias após vencer em que a conta será bloqueada ().**
- **Dias após 1970-01-01 em que a conta será bloqueada ().**
- **Campo reservado para uso futuro ().**

Veja que não há senha definida para o usuário **ada**, vamos criá-la agora:

```
[syscop@server1]$ sudo passwd ada
[sudo] password for syscop:
Changing password for user ada.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

[syscop@server1]$ sudo tail -1 /etc/shadow
ada:$6$8dlc1QFS$8bt5gi35fZMrOgWlmxmjyo6M61NmV7PlhuyCA8rim2LKjnKiF
Dx1QvrS6am2eqBcRuua9t5K0L0b1JrveDaY81:17090:0:99999:7:::
```

Agora **ada** tem uma senha e já pode usar o sistema.

O comando **chage** pode ser utilizado para visualizar e alterar os dados de expiração da senha:

```
$ sudo chage -l ada
Last password change                : Oct 16, 2016
Password expires                    : never
Password inactive                   : never
Account expires                     : never
Minimum number of days between password change : 0
Maximum number of days between password change  : 99999
Number of days of warning before password expires: 7
```

Podemos criar outros grupos através do groupadd

```
sudo groupadd marketing
```

Podemos adicionar ada em outros grupos:

```
sudo usermod -aG marketing ada
```

Define uma nova senha para usuário ada que:

- expira após 90 dias.
- só permite uma nova alteração após 30 dias.
- avisa o usuário sobre a expiração da senha 3 dias antes.

```
passwd -n 30 -w 3 -x 90 ada
```

A maioria das tarefas feitas com passwd podem ser realizadas com chage. Consulte suas páginas de manual.

Remove o usuário ada:

```
# -r remove o diretório home do usuário ada também.  
sudo userdel -r ada
```

Obsevações finais:

- Ao criar um novo usuário através do comando useradd, o diretório home conterá alguns arquivos padrões, estes arquivos são copiados a partir do diretório `/etc/skel`. Experimente criar um arquivo nesta pasta e depois criar um novo usuário.
- O arquivo `/etc/group` possui os seguintes campos:

```
nomeDoGrupo:senhaDoGrupo:GID:usuarios,do,grupo
```

Atualmente criamos somente usuários de sistema para os serviços instalados no servidor e um ou dois usuários administrativos. Usuários comuns são autenticados de maneira

centralizado utilizando um servidor LDAP, como o Fedora 389 ou Red Hat Identity Manager.

• • •

Gostou? Então recomende.

Obrigado!

Some rights reserved 

[Linux](#) [Sysadmin](#) [Centos](#)

[About](#) [Help](#) [Legal](#)