

Habilitando o Sudo no Slackware

Sudo, substitute user do (Substituição do usuário) ou Super user do (fazer como super usuário) tem um grande papel em sistemas UNIX Likes, o sudo permite que usuários comuns possam obter privilégios temporariamente de um outro usuário, em grande escala muito utilizada para os privilégios do super usuário root.

Há muitas vantagens e desvantagens em usar o sudo em relação ao su, por exemplo às vezes precisamos apenas realizar uma tarefa rapidamente, como atualizar o sistema com um único comando, como 'slackpkg update && slackpkg upgrade-all' ou simplesmente abrir um arquivo que tem permissão de escrita e leitura somente para o root, por exemplo.

Mas todo super herói paga seu preço, como o sudo permite que o usuário tenha super poderes temporariamente, qualquer pessoa que souber a senha do seu usuário comum pode ter estes super privilégios.

Por isto é de extrema importância você ter uma senha segura quanto para o root quanto para o seu usuário comum, assim podendo utilizar o sudo com tranquilidade.

Diferente de outras distribuições o Slackware vem por padrão com o sudo desabilitado, e vamos aprender a como habilitar.

O primeiro passo é criar um grupo chamado "sudo", para esta simples tarefa podemos fazer de dois modos. O primeiro é criando manualmente um grupo, e o segundo é utilizando o comando 'groupadd NOMEdoGRUPO'.

Vamos utilizar o modo manual para um melhor aprendizado e noção.

O primeiro passo é logar-se como root, para isto use o comando su, e logo após vamos abrir um arquivo de configuração dos grupos que fica localizado em /etc/group, abra com seu editor favorito:

```
$ su
# nano /etc/group
```

Vamos navegar até a última linha do arquivo 'group' e adicionar uma linha em especial para o sudo, a minha penúltima linha contém o grupo privoxy, o seu arquivo com toda certeza será diferente:

```
privoxy:x:206:
```

Neste mesmo formato vamos criar o grupo sudo, o formato deve ser o seguinte:

```
groupname:x:ID:USERNAME
```

Para conferir o ID do seu usuário rode o comando 'id -u', lembre-se de ser com o usuário que será habilitado o sudo.

```
$ id -u
1000
```

Adicionamos então na última linha do arquivo group:

```
sudo:x:1000:Username
```

Exemplo:

```
nobody:x:98:nobody
nogroup:x:99:
users:x:100:
console:x:101:
tor:x:220:
privoxy:x:206:
sudo:x:1000:slackjeff
```

Feito este processo, salve e feche. Agora vamos precisar editar o arquivo 'sudoers', para isto abra com seu editor favorito o arquivo /etc/sudoers.

```
# nano /etc/sudoers
```

Aberto o arquivo, localize a linha '# %sudo ALL=(ALL) ALL', esta linha está comentada com a tralha '#' na frente do %sudo, precisamos descomentar, retirar o '#' da frente do %sudo para ter efeito... caso você esteja utilizando o editor nano, pode utilizar as teclas simultaneamente CTRL + W, irá abrir um campo de pesquisa no canto esquerdo inferior, basta inserir '%sudo ALL=(ALL) ALL' para a localização ser feita.

Linha sudo comentada:

```
## Uncomment to allow members of group sudo to execute any command
# %sudo ALL=(ALL) ALL
```

Linha sudo descomentada:

```
## Uncomment to allow members of group sudo to execute any command
%sudo ALL=(ALL) ALL
```

Descomentado a linha do sudo, salve e feche, para colocar a cereja no bolo precisamos fazer uma última configuração que é muito importante. Sabemos que usuários comuns tem o UID 1000, e alguns comandos são especiais para o super usuário que contem a UID 0, quando rodamos um comando o sistema procura na variável de ambiente \$PATH a localização do comando que pedimos.

Existem diretórios como é o exemplo '/sbin' que é acessível somente com usuários de UID 0, um exemplo é o próprio root. O que acontece se tentarmos executar um comando como o slackpkg por exemplo que está dentro diretório? Vai falhar.

Por isso precisamos adicionar duas novas linhas em nosso PATH.

Para isto ainda como usuário root vamos abrir o arquivo 'profile' que está localizado em '/etc/profile' e localizar a linha:

```
# Set the default system $PATH:
PATH="/usr/local/bin:/usr/bin:/bin:/usr/games"
```

Note que há uma padrão estabelecido, os diretórios tem seu campo separado por ':'. Ao final do '/usr/games' adicionamos os ':' e adicionamos '/sbin' e após isto adicionamos ':' novamente e '/usr/sbin'. Salve e feche.

```
# Set the default system $PATH:  
PATH="/usr/local/bin:/usr/bin:/bin:/usr/games:/sbin:/usr/sbin"
```



observe que agora o seu usuário comum (UID 1000) consegue executar os comandos de manutenção que são encontrados em /sbin e /usr/sbin, sendo que antes estes comandos nestes diretórios nem sequer eram 'mostrados' para um usuário comum (UID 1000). Porém mesmo agora enxergando estes comandos vamos necessitar do super usuário para dar continuação.

Simplificando, é o mesmo que em um arquivo você dar permissão de leitura, para um determinado usuário, ele consegue ler mas não consegue escrever e nem executar, por exemplo.

Reinicie seu sistema com o comando shutdown com parâmetros -r now, ou simplesmente saia do seu usuário e retorne, para isto você poder executar o comando exit ou pressionar simultaneamente as teclas 'CTRL + D'.

Faça testes adicionando sudo na frente do(s) comando(s) desejado(s). Teste também atualizando sua lista e checksuns com o slackpkg.

```
$ sudo ls /root/  
$ sudo slackpkg update
```

Fontes

- Originally written by [Slackjeff](#)

[howtos](#), [template](#)

From:
<https://docs.slackware.com/> - **SlackDocs**

Permanent link:
https://docs.slackware.com/pt-br:howtos:misc:enabling_sudo_on_slackware

Last update: **2019/12/26 22:18 (UTC)**

