

Indo além do “sudo su”

Rodrigo Lira

eurodrigolira@gmail.com

<https://rodrigolira.eti.br>



/eurodrigolira

Tópicos



O que é o sudo?

História

Configurações do sudo

visudo

Configurações do `/etc/sudoers`

Usando o sudo

Logs

FreeIPA

Referências

Dúvidas

O que é o sudo?

É um programa que permite a execução de outro programa como outro usuário.

Normalmente esse usuário é o **root**.

Quando o usuário precisa executar um comando que requer permissões de outro usuário, ele pede ao **sudo** para executar o comando para ele, o **sudo** consulta sua lista de permissões, se o usuário tiver a permissão o comando será executado.

História

O projeto foi iniciado em **1980** no departamento de ciência da computação SUNY/Buffalo, criado por Bob Coggeshall e Cliff Spencer.

Em **1986**, é lançada uma versão melhorada do sudo. Nos cinco anos seguintes, o sudo foi desenvolvido por várias pessoas na Universidade do Colorado em Boulder.

Em **1991**, uma nova versão do sudo é escrita sob contrato para uma empresa de consultoria chamada "The Root Group".

Em **1994**, depois de manter o sudo CU-Boulder por algum tempo, **Todd C. Miller** fez uma versão pública do "CU sudo" com correções de bugs e suporte para mais sistemas operacionais.

História

Em **1995**, um novo analisador do arquivo sudoers foi contribuído por Chris Jepeway.

Em **1999**, o prefixo "CU" foi retirado do nome, a partir da versão 1.6, o Sudo não contém mais nenhum código da empresa "The Root Group".

Em **2003**, Aaron Spangler escreve o suporte para armazenar os dados dos sudoers no LDAP.

Em **2005**, **Todd C. Miller** reescreveu o sudoers para melhorar os recursos que foram adicionados nos últimos dez anos.

Em **2010**, a Quest Software começou a patrocinar o desenvolvimento do Sudo contratando **Todd C. Miller** para trabalhar no Sudo como parte de seu trabalho em tempo integral.

Configurações do sudo

Existem dois componentes chave na solução, o programa **sudo** e o arquivo de configuração **sudoers**, porém existem outros arquivos.

```
[root@com-sudo ~]# ls -l /etc/sudo*  
-rw-r-----. 1 root root 1786 Jun 26 15:07 /etc/sudo.conf  
-r--r-----. 1 root root 3938 Jun 26 15:07 /etc/sudoers  
-rw-r-----. 1 root root 3181 Jun 26 15:07 /etc/sudo-ldap.conf  
  
/etc/sudoers.d:  
total 0  
[root@com-sudo ~]# █
```

Configurações do sudo

/etc/sudo.conf - é usado para configurar o front end do sudo. Ele especifica a política de segurança e plug-ins, registros de E/S, sinalizadores de depuração, bem como nomes e configurações de caminhos independentes de plug-ins.

/etc/sudoers - determina os privilégios sudo dos usuários, é o plugin de política padrão do sudo.

/etc/sudo-ldap.conf - além do arquivo sudoers padrão, o sudo pode ser configurado via LDAP, normalmente utilizado em grandes ambientes.

Configurações do sudo

`/etc/sudoers.d` – este diretório nos dá a possibilidade de criarmos arquivos `sudoers` personalizados por usuário.

OBS: Para utilizarmos precisamos descomentar a seguinte linha no `/etc/sudoers`.

```
## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#include_dir /etc/sudoers.d
```


visudo

visudo - edita os arquivos sudoers de forma segura, ele bloqueia o arquivo sudoers contra várias edições simultâneas, fornece verificações básicas de integridade e verifica se há erros de análise.

Se o arquivo sudoers estiver sendo editado no momento, você receberá uma mensagem para tentar novamente mais tarde.

```
[root@com-sudo ~]# visudo
visudo: /etc/sudoers busy, try again later
[root@com-sudo ~]# █
```

visudo

Por padrão se executarmos apenas o **visudo** ele abrirá o arquivo **/etc/sudoers**, mas podemos especificar qual arquivos desejamos abrir passando o parâmetro **-f**.

```
# visudo /etc/sudo-ldap.conf
```

Dica: existe os comandos **vipw** e **vigr**, editam os arquivos **/etc/passwd** e **/etc/group**, respectivamente, tem o mesmo comportamento do visudo, bloqueando o arquivo.

Configurações do /etc/sudoers

O arquivo `/etc/sudoers` pode conter uma série de regras, uma por linha, o formato padrão das regras é a seguinte:

USUARIO **HOST** = **COMANDO**

```
##  
## The COMMANDS section may have other options added to it.  
##  
## Allow root to run any commands anywhere  
root    ALL=(ALL)    ALL
```

Configurações do /etc/sudoers

USUARIO - é o nome de usuário ao qual esta regra se aplica. O nome de usuário também pode ser um grupo de sistemas ou um alias definido dentro de sudoers.

HOST - é o nome do host do sistema ao qual esta regra se aplica.

= "sinal de igual" - separa o HOST dos comandos.

COMANDO - lista dos comandos a qual a regra se aplica, a configuração do sudo requer caminhos completos para os comandos.

rodrigo ALL = iptables != rodrigo ALL = /usr/sbin/iptables

Configurações do /etc/sudoers

O arquivo sudoers reconhece uma variedade de palavras-chave especiais. Um dos mais comumente visto é o ALL, que corresponde a todas as opções possíveis. Para permitir que todos os usuários executem qualquer comando, poderíamos escrever um arquivo sudoers como este:

```
ALL ALL = ALL
```

Isso equivale aproximadamente a dar acesso root a todos os usuários do sistema, mas usando suas próprias senhas ao invés da senha de root.

Por segurança não devemos fazer isso, devemos pelo menos restringir por usuário.

```
rodrigo ALL = ALL
```

Configurações do /etc/sudoers

Também conseguimos restringir o acesso sudo pelo host.

```
rodrigo www = ALL
```

Normalmente veremos o host como **ALL**, a maioria dos administradores de sistemas configuram o sudo por host.

Para não termos um arquivo sudoers muito grande, podemos ter várias regras na mesma linha, separadas por vírgulas.

```
rodrigo,lira www = ALL
```

```
rodrigo,lira www = /usr/sbin/iptables,/sbin/reboot
```

Configurações do /etc/sudoers

Também podemos utilizar grupos para definir as regras dentro do sudoers.

```
%wheel ALL = ALL
```

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

Podemos permitir a execução das regras sem solicitar senha ao usuário.

```
## Same thing without a password
# %wheel          ALL=(ALL)        NOPASSWD: ALL
```

Configurações do `/etc/sudoers`

Podemos trabalhar com aliases, caracteres conringas, expressões regulares e diversos outras possibilidades.

O sudo processa as regras em ordem e a última regra correspondente ganha, se duas regras entrarem em conflito, a última regra ganhará.

O ponto de exclamação (!) é o operador de negação, usado para excluir um item de uma lista, podemos dizer que uma regra se aplica a tudo, exceto a um usuário, host ou comando específico.

Um arquivo sudoers deve sempre terminar com umma linha em branco, se visudo indica um erro na última linha, mas a sintaxe parece correta, verifique se a última linha estará em branco.

Usando o sudo

Na primeira vez que executamos o **sudo** em qualquer sistema, o sudo exibe uma mensagem sobre a importância de pensar antes de executar comandos privilegiados.

```
Presumimos que você recebeu as instruções de sempre do administrador  
de sistema local. Basicamente, resume-se a estas três coisas:
```

- #1) Respeite a privacidade dos outros.
- #2) Pense antes de digitar.
- #3) Com grandes poderes vêm grandes responsabilidades.

```
Senha: █
```

Usando o sudo

Quando desejamos executar algo com o sudo, o primeiro comando a ser digitado é ele mesmo, seguido do comando que desejamos executar.

sudo iptables -L

```
rodrigo@s14:~$ sudo iptables -L
Senha:
rodrigo não está no arquivo sudoers. Este incidente será relatado.
rodrigo@s14:~$ █
```

Se o usuário não estiver no sudoers a mensagem acima é exibida.

Usando o sudo

Se o usuário estiver no arquivo sudoers e com as permissões corretas, o comando é executado.

```
rodrigo@sl4:~$ sudo /usr/sbin/iptables -L
Senha:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy DROP)
target     prot opt source                destination
DOCKER-USER all -- anywhere             anywhere
DOCKER-ISOLATION-STAGE-1 all -- anywhere             anywhere
ACCEPT     all -- anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all -- anywhere             anywhere
ACCEPT     all -- anywhere             anywhere
ACCEPT     all -- anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain DOCKER (1 references)
target     prot opt source                destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source                destination
DOCKER-ISOLATION-STAGE-2 all -- anywhere             anywhere
RETURN     all -- anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source                destination
DROP       all -- anywhere             anywhere
RETURN     all -- anywhere             anywhere

Chain DOCKER-USER (1 references)
target     prot opt source                destination
RETURN     all -- anywhere             anywhere
rodrigo@sl4:~$
```

Usando o sudo

Com o comando sudo também podemos verificar as permissões dos usuários sem ter a necessidade de verificar o arquivo de configuração, basta executarmos o sudo passando o parâmetro -l:

sudo -l

```
rodrigo@sl4:~$ sudo -l
Usuário rodrigo pode executar os seguintes comandos em sl4:
    (root) /usr/sbin/iptables
rodrigo@sl4:~$
```

sudo -U rodrigo -l

sudo -U root -l

```
root@sl4:~# sudo -U rodrigo -l
Usuário rodrigo pode executar os seguintes comandos em sl4:
    (root) /usr/sbin/iptables
root@sl4:~# sudo -U root -l
Usuário root pode executar os seguintes comandos em sl4:
    (ALL) ALL
root@sl4:~#
```

Usando o sudo

Também podemos executar um comando como um usuário específico adicionando o parâmetro `-u`.

```
# sudo -u rodrigo touch arquivo2
```

```
root@s14:/home/rodrigo/Documentos# touch arquivo1
root@s14:/home/rodrigo/Documentos# ls -l
total 0
-rw-r--r-- 1 root root 0 Nov  8 23:48 arquivo1
root@s14:/home/rodrigo/Documentos# sudo -u rodrigo touch arquivo2
root@s14:/home/rodrigo/Documentos# ls -l
total 0
-rw-r--r-- 1 root    root    0 Nov  8 23:48 arquivo1
-rw-r--r-- 1 rodrigo rodrigo 0 Nov  8 23:48 arquivo2
root@s14:/home/rodrigo/Documentos#
```

Usando o sudo

Também podemos executar o sudo passando o grupo como parâmetro, isso é necessário quando alguns programas precisam que o grupo principal do usuário seja seu grupo.

```
# sudo -g vboxusers virtualbox
```

Também podemos passar como parâmetro o ID do grupo.

```
# sudo -g #100 virtualbox
```

Logs

Todos os comandos que são executados, seja bem sucedido ou não, é gerado logs para os mesmos, esses logs podem variar de acordo com a distribuição Linux que vocês esteja utilizando, mas normalmente podem ser vistos no `/var/log/secure`.

```
Nov 9 00:41:12 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=iptables -L
Nov 9 00:41:23 s14 sudo: rodrigo : TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/iptables -L
Nov 9 00:41:25 s14 sudo: rodrigo : TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/iptables -L
Nov 9 00:41:31 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=touc
Nov 9 00:41:34 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/bin/touch
Nov 9 00:41:55 s14 sudo: rodrigo : TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=list
Nov 9 00:42:00 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/bin/su
Nov 9 00:42:50 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/bin/su
Nov 9 00:43:00 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=visudo
Nov 9 00:43:10 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/visudo
Nov 9 00:43:20 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/ip
Nov 9 00:43:24 s14 sudo: rodrigo : command not allowed ; TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/ip6tables
Nov 9 00:44:15 s14 sudo: rodrigo : TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/bin/docker run hello-world
Nov 9 00:44:22 s14 sudo: rodrigo : TTY=pts/4 ; PWD=/home/rodrigo ; USER=root ; COMMAND=/usr/sbin/iptables -L
```

FreeIPA



freelPA

Administrator

Identity

Policy

Authentication

Network Services

IPA Server

Users

User Groups

Hosts

Host Groups

Netgroups

Services

Automember

User categories

Active users

Stage users

Preserved users

Active users

Search

Refresh

Delete

Add

Disable

Enable

Actions

	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	admin		Administrator	Enabled	890200000			

Showing 1 to 1 of 1 entries.

FreeIPA

O FreeIPA é uma solução integrada de Identidade e Autenticação para ambientes de rede Linux/UNIX.

Um servidor FreeIPA fornece autenticação centralizada, níveis de permissões, gerenciamento de usuários, grupos, hosts e outros objetos necessários para gerenciar os aspectos de segurança de uma rede de computadores.

O FreeIPA é construído sobre componentes e protocolos padrão de código aberto bem conhecidos, com um foco muito forte na facilidade de gerenciamento e automação de tarefas.

Referências

Site oficial do sudo - <https://www.sudo.ws>

Livro de Michael W Lucas - **Sudo Mastery**

Site oficial do FreeIPA - <https://www.freeipa.org>



