

RE: sudoers

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2007-10/msg00263.html>

- *From:* "Mertens, Bram" <mertensb@xxxxxxxxxxxxx>
 - *Date:* Thu, 25 Oct 2007 12:38:45 +0200
-

I don't believe any restrictions you'll make to this setup will have much effect.

No matter what commands you'll disallow for these users to execute in /usr/local/bin there's tons of ways they can circumvent it:

Sudo visudo + remove the restrictions

Sudo bash + and do whatever they want as root WITHOUT any logging

Create a symbolic link to /usr/local/bin will probably also circumvent any restrictions

..

It is probably safer to allow only those commands they really need rather than trying to open everything and then close some things again.

If you want to add restrictions look into the su and passwd commands in the sudoers man page:

```
pete HPPA = /usr/bin/passwd [A-z]*, !/usr/bin/passwd root
```

The user pete is allowed to change anyone's password except for root on the HPPA machines. Note that this assumes passwd(1) does not take multiple usernames on the command line.

```
john ALPHA = /usr/bin/su [!-]*, !/usr/bin/su *root*
```

On the ALPHA machines, user john may su to anyone except root but he is not allowed to give su(1) any flags.

Regards

Bram

—

Bram Mertens

Web application Administrator / Red Hat Certified Technician

Mazda Motor Logistics Europe N.V.

Tel.: +32 3 860 12 61

RE: sudoers

Mazda Motor Logistics Europe NV, Blaasveldstraat 162, B-2830 Willebroek
VAT BE 406.024.281, RPR Mechelen, ING 310-0092504-52, IBAN : BE64 3100 0925 0452, SWIFT :
BBRUBEBB

-----Original Message-----

From: redhat-list-bounces@xxxxxxxxxx
[mailto:redhat-list-bounces@xxxxxxxxxx] On Behalf Of Johan Booyen
Sent: donderdag 25 oktober 2007 10:34
To: General Red Hat Linux discussion list
Subject: sudoers

On one of our development servers, we have a number of developers
specified in /etc/sudoers:

```
abc ALL=(ALL) ALL
def ALL=(ALL) ALL
ghi ALL=(ALL) ALL
jkl ALL=(ALL) ALL
```

Now I need to restrict access to /usr/local/bin, so that only the root
user can make changes to that directory. Even the people in
/etc/sudoers should not be able to make changes to /usr/local/bin.

How can I adapt /etc/sudoers to achieve this? I've already
read the man
page and will investigate, but any quick pointers will be appreciated.

Thanks.

Johan

--

redhat-list mailing list
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>

--

redhat-list mailing list
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>

RE: sudoers