

# Install Dazuko for Red Hat Enterprise Linux (RHEL)

## Objective

Install Dazuko as a kernel module on a RHEL 4.6 machine. Dazuko provides a virtual device driver allowing ESET antivirus to execute online file access control. In other words, ESET can provide a On-access virus scanner at OS level. It is also required to use the same kernel version to compile the dazuko module.

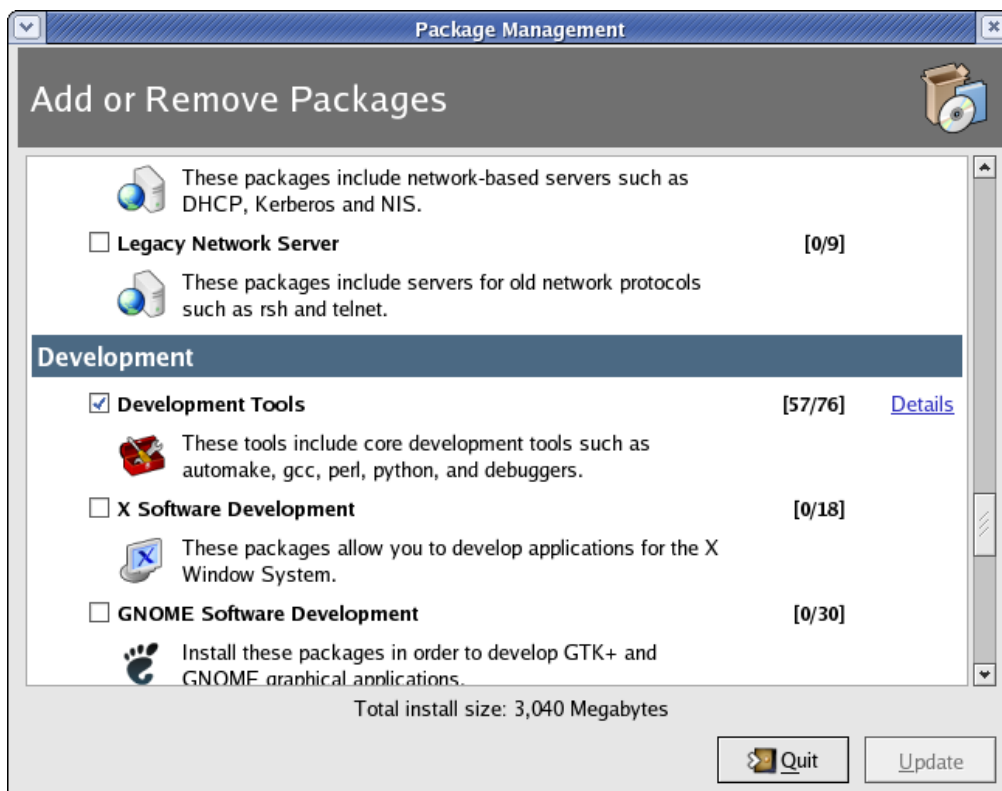
## Preparation

- 1) Find the existing kernel version and platform by typing “**uname -a**” command.

```
[barry@localhost ~]$ uname -a
Linux localhost.localdomain 2.6.9-67.0.4.EL_smp #1 SMP Sat Jul 12
16:28:55 HKT 2008 x86_64 x86_64 x86_64 GNU/Linux
```

That means the existing kernel version is **2.6.9-67.0.4** and using **x86\_64** arch and running **SMP** mode.

- 2) Download the corresponding kernel source RPM from Red Hat FTP server. E.g. For above kernel version, the kernel source RPM locate at <ftp://ftp.redhat.com/pub/redhat/linux/updates/enterprise/4ES/en/os/SRPMS/kernel-2.6.9-67.0.4.EL.src.rpm>
- 3) Download the latest dazuko source file from [www.dazuko.org](http://www.dazuko.org). The latest version, at the the of writing, is dazuko-2.3.5.tar.gz.



To compile the kernel, you need a lot of compile softwares/library for Linux. You can add “**Development Tools**” software from the installation CD.

## Recompile the kernel

All Red Hat Linux kernel have the “Linux Default Capabilities security” module compiled into the kernel itself rather than as a separate module. In order to make dazuko module running, we have to recompile the kernel so that “Linux Default Capabilities security” is a module.

- 1) Install the source kernel RPM

```
rpm -ivh kernel-2.6.9-67.0.4.EL.src.rpm
```

- 2) cd **/usr/src/redhat/SPECS** directory

```
cp kernel-2.6.spec kernel-2.6.spec.dazuko
```

Edit kernel-2.6.spec.dazuko file by vi, and change the following:

a) change %define release 67.0.20.EL.dazuko

b)

```
%define buildup 1
```

```
%define buildsmp 1
```

```
%define buildsource 0
```

```
%define buildhugemem 1
```

```
%define buildlargesmp 1
```

```
%define bulddoc 0
```

```
%define buildxen 1
```

```
%define kabi 1
```

0 means will not build the relevant kernel. Eg if you only need x86\_64 arch and running SMP mode. It will change to:

```
%define buildup 0
```

```
%define buildsmp 1
```

```
%define buildsource 0
```

```
%define buildhugemem 0
```

```
%define buildlargesmp 0
```

```
%define bulddoc 0
```

```
%define buildxen 0
```

```
%define kabi 1
```

- 3) cd **/usr/src/redhat/SOURCES** directory

Based on your kernel arch, select the .config file need to be change. Eg the example above, x86\_64 arch and running SMP mode. You need to change the following file:

```
kernel-2.6.9-x86_64-smp.config
```

change the line

```
CONFIG_SECURITY_CAPABILITIES=y
```

to

```
CONFIG_SECURITY_CAPABILITIES=m
```

To change the Security Capabilities as module.

- 4) cd back to `/usr/src/redhat/SPECS` directory

Type the following and start compiling:

```
rpmbuild -bb --target x86_64 kernel-2.6.spec.dazuko 2>/tmp/kernel-err.log
```

- 5) It take half an hour or so for compiling kernel (depending on your CPU speed and memory). After the build completes, the compiled RPM will locate at `/usr/src/redhat/RPMS/x86_64` directory.

Type

```
rpm -ivh kernel-smp-2.6.9-67.0.4.EL_dazuko.x86_64.rpm  
to install the new kernel without Security Capabilities build in.
```

- 6) Reboot the machine and make sure it use new kernel after reboot (by changing relevant lines in `/etc/grub.conf`).

## Build the dazuko kernel module

- 1) extract the tar ball source file (dazuko-2.3.5.tar.gz)  
**tar xvfz dazuko-2.3.5.tar.gz**
- 2) **cd dazuko-2.3.5**

Configure the Makefile

After we rebuild the kernel source as above procedure, we will leave the kernel source in the BUILD directory. Therefore, we set the parameter for `kernelsrc` as below:

```
[root@localhost dazuko-2.3.5]# ./configure  
--kernelsrcdir=/usr/src/redhat/BUILD/kernel-2.6  
.9/linux-2.6.9/
```

```
checking host system type... Linux  
checking for make utility... ok (make)  
checking for C compiler... ok (cc)  
kernel build source in /usr/src/redhat/BUILD/kernel-2.6.9/linux-2.6.9... yes  
acquiring Linux kernel code configuration... ok  
checking if Linux is RSBAC patched... no
```

```
checking if devfs is enabled... no
discovered host system... Linux (2.6.9)
checking if security module support is enabled... yes
verifying capabilities are not built-in... ok
locating LSM API header... ok
identifying LSM API (this can take a while)... ok
identifying device API... ok
inspecting class type... ok (class_simple)
inspecting suspend function... ok (suspend1)
inspecting task_struct structure... ok (using parent)
disabling ON_CLOSE events (not available for Linux 2.6 LSM/RedirFS)
configure: creating Makefile
configure: creating library/Makefile
configure: creating example_c/Makefile

./configure successful
```

---

---

#### Configuration summary

---

---

```
module events = ON_OPEN ON_EXEC
devfs support = no
rsbac support = no
stacking support = yes
path resolution = registered daemon context
module debug = no
library 1.x compatibility = yes
```

- 3) Type **make** and **make install** to compile and install the **dazuko.ko** module.
- 4) Test the module:

```
[root@localhost ~]# modprobe dazuko
[root@localhost ~]# lsmod | grep dazuko
```

You should see something like this:

```
dazuko          67344  8
commoncap      10305  1 dazuko
```

- 5) The installation for dazuko is completed.