The xFusionCorp Industries security team recently did a security audit of their infrastructure and came up with ideas to improve the application and server security. They decided to use SElinux for an additional security layer. They are still planning how they will implement it; however, they have decided to start testing with app servers, so based on the recommendations they have the following requirements:

Install the required packages of SElinux on App server 3 in Stratos Datacenter and disable it permanently for now; it will be enabled after making some required configuration changes on this host. Don't worry about rebooting the server as there is already a reboot scheduled for tonight's maintenance window. Also ignore the status of SElinux command line right now; the final status after reboot should be disabled.

Soln

1. thor@jump\_host ~$ ssh banner@stapp03

[banner@stapp03 ~]$ sudo su

2.

[root@stapp03 banner]# sestatus

bash: sestatus: command not found

[root@stapp03 banner]# sudo apt install selinux-utils

sudo: apt: command not found

[root@stapp03 banner]# yum install selinux -y

3.

[root@stapp03 banner]# sestatus

SELinux status: disabled

[root@stapp03 banner]# cat /etc/selinux/config | grep SELINUX

# SELINUX= can take one of these three values:

SELINUX=enforcing

# SELINUXTYPE= can take one of these three values:

SELINUXTYPE=targeted

[root@stapp03 banner]# vi /etc/selinux/config | grep SELINUX

Vim: Warning: Output is not to a terminal

# SELINUX= can take one of these three values:

SELINUX=enforcing

# SELINUXTYPE= can take one of these three values:

SELINUXTYPE=targeted

[root@stapp03 banner]# vi /etc/selinux/config

[root@stapp03 banner]# cat /etc/selinux/config | grep SELINUX

# SELINUX= can take one of these three values:

SELINUX=disabled

# SELINUXTYPE= can take one of these three values:

SELINUXTYPE=targeted

[root@stapp03 banner]# ^C

[root@stapp03 banner]# ^C

[root@stapp03 banner]# sestatus

SELinux status: disabled