OS Installation: CentOS 5.8

OpenTUSK Training
University of Nairobi

Mike Prentice
michael.prentice@tufts.edu

Tufts University
Technology for Learning in the Health Sciences

July 2013

Outline

1. OS Install
2. SELinux
3. Firewall
4. Yum Packages
5. Time
6. System Accounts
7. OpenTUSK Software
8. Database

Resources

- Official website:
  `http://opentusk.org/`
- Wiki documentation:
  `https://wikis.uit.tufts.edu/confluence/display/TUSKpub/Home`
- Source code:
  `https://github.com/opentusk/Opentusk`

Coming Up...

1. OS Install
2. SELinux
3. Firewall
4. Yum Packages
5. Time
6. System Accounts
7. OpenTUSK Software
8. Database

CentOS 5.8

- OpenTUSK requires CentOS 5.8
- Web servers on CentOS 5.8 virtual machines
- Database server: MySQL
  - Version 5 or higher
- Installation prerequisites:
  - Dedicated IP address
  - hostname in DNS
  - root account password
  - SSH access to hardware or virtual machine

OpenTUSK Repository

Configure the OpenTUSK repository for RHEL/CentOS 5.8:

```
# curl --output /etc/yum.repos.d/opentusk.repo
    https://raw.github.com/opentusk/Opentusk/master/install/
        centos-5.8/opentusk.repo
```

Note: If you copy and paste these commands, be careful of spaces.

Coming Up...

1. OS Install
2. SELinux
3. Firewall
4. Yum Packages
5. Time
6. System Accounts
7. OpenTUSK Software
8. Database

Disable SELinux

SELinux, or security-enhanced Linux, is on by default in CentOS.

SELinux interferes with the operation of OpenTUSK.

We set SELinux to run in permissive mode:

```
# sed -i 's/^SELINUX.*/SELINUX=permissive/g'
    /etc/selinux/config

# /usr/sbin/setenforce Permissive
```

Coming Up...

1 OS Install
2 SELinux
3 Firewall
4 Yum Packages
5 Time
6 System Accounts
7 OpenTUSK Software
8 Database

Configure the Firewall

Allow connections to http (port 80) and https (port 443):

/etc/sysconfig/iptables

```
...
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --
    dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --
    dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --
    dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-
    prohibited
COMMIT
```

Restart the firewall:

```
# /sbin/service iptables restart
```

Coming Up...

1 OS Install
2 SELinux
3 Firewall
4 Yum Packages
5 Time
6 System Accounts
7 OpenTUSK Software
8 Database

Install Packages

Install services and Perl packages needed for OpenTUSK:

```
# cd /tmp

# curl -O
    https://raw.github.com/opentusk/Opentusk/master/install/
        centos-5.8/install_yum_packages.bash

# bash install_yum_packages.bash
```

Coming Up...

1 OS Install
2 SELinux
3 Firewall
4 Yum Packages
5 Time
6 System Accounts
7 OpenTUSK Software
8 Database

Set the Timezone

Set your local timezone from `/usr/share/zoneinfo`. For example, to set Nairobi time:

```
# rm /etc/localtime

# ln -s /usr/share/zoneinfo/Africa/Nairobi /etc/localtime
```

Update Time

Note: The network time (NTP) steps may not be necessary depending on your virtual machine setup.

Set the network time using NTP:

```
# /usr/sbin/ntpdate 0.africa.pool.ntp.org
```

Fix NTP

Edit `/etc/ntp.conf` to comment out the local clock and add African NTP servers to the pool:

/etc/ntp.conf

```
...
server 0.africa.pool.ntp.org
server 1.africa.pool.ntp.org
server 2.africa.pool.ntp.org
server 3.africa.pool.ntp.org

...
# Undisciplined Local Clock. This is a fake driver ...
# server   127.127.1.0     # local clock
# fudge    127.127.1.0 stratum 10
```

Start NTP

Start/restart the NTP time service:

```
# /sbin/service ntpd restart

# /sbin/chkconfig ntpd on
```

Coming Up...

1 OS Install
2 SELinux
3 Firewall
4 Yum Packages
5 Time
6 System Accounts
7 OpenTUSK Software
8 Database

tusk

Create tusk user account:

```
# /usr/sbin/groupadd -g 1100 tusk

# /usr/sbin/useradd -c 'Tusk' -u 1100 -g tusk
    -d /usr/local/tusk tusk

# /usr/sbin/usermod -a -G tusk apache

# chmod 755 /usr/local/tusk
```

tuskoper

Create a tuskoper account with system privileges:

```
# /usr/sbin/useradd tuskoper

# /usr/sbin/usermod -a -G tuskoper wheel,apache,tusk

# passwd tuskoper
```

Note: Creating a tusk operator account is optional but recommended.

sudo

- Setup sudo for tuskoper and the wheel group with `visudo`
- Add tuskoper line below root
- Uncomment wheel line
- No spaces, only tabs

/etc/sudoers

```
...
## Allow root to run any commands anywhere
root        ALL=(ALL)         ALL
tuskoper    ALL=(ALL)         ALL
...

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

Coming Up...

1 OS Install
2 SELinux
3 Firewall
4 Yum Packages
5 Time
6 System Accounts
7 OpenTUSK Software
8 Database

Download OpenTUSK

Download OpenTUSK from Github:

```
# cd /usr/local/tusk

# git clone https://github.com/opentusk/Opentusk.git

# ln -s Opentusk current
```

Coming Up...

1. OS Install
2. SELinux
3. Firewall
4. Yum Packages
5. Time
6. System Accounts
7. OpenTUSK Software
8. Database

Start MySQL

Recommended: Secure MySQL root user with the `mysql_secure_installation` command.

Start the MySQL database and add an administrative user:

```
# /sbin/chkconfig mysqld on

# /sbin/service mysqld start

# mysql -u root

mysql> grant all on *.* to 'tuskoper'@'localhost'
    -> identified by '<password>' with grant option;

mysql> flush privileges;
```

Optional: Setup `.my.cnf` file for `tuskoper`

Resources

- Official website:
  `http://opentusk.org/`
- Wiki documentation:
  `https://wikis.uit.tufts.edu/confluence/display/TUSKpub/Home`
- Source code:
  `https://github.com/opentusk/Opentusk`