

Setting up Linux host

Preparing SSH Keys to Remote Hosts

To perform any deployment or management from the localhost to remote host first we need to create and copy the ssh keys to the remote host. In every remote host there will be a user account **user** (in your case may be different user).

First let us create a SSH key using below command and copy the key to remote hosts.

```
# ssh-keygen -t rsa -b 4096 -C "admin@novartis.com"
```

Terminal

```
tecmin@instructor ~ $
tecmin@instructor ~ $ ssh-keygen -t rsa -b 4096 -C "admin@tecminlocal.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/tecmin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tecmin/.ssh/id_rsa.
Your public key has been saved in /home/tecmin/.ssh/id_rsa.pub.
The key fingerprint is:
0a:b8:30:63:13:35:6a:3d:a9:ae:b2:a4:98:4d:fd:2a admin@tecminlocal.com
The key's randomart image is:
+--[ RSA 4096 ]-----+
|      o               |
|    + o               |
|  + +                |
| . o .               |
| ++. .   S          |
| 0+.0 . .           |
|  oo . .            |
| *+E .              |
| B.....            |
+-----+
tecmin@instructor ~ $
```

Create SSH Key

After creating SSH Key successfully, now copy the created key to all three remote server's.

```
# ssh-copy-id user@192.168.0.112
# ssh-copy-id user@192.168.0.113
# ssh-copy-id user@192.168.0.114
```

```
Terminal
tecmint@instructor ~ $
tecmint@instructor ~ $ ssh-copy-id tecmint@192.168.0.112
The authenticity of host '192.168.0.112 (192.168.0.112)' can't be established.
RSA key fingerprint is 51:62:55:81:60:00:e9:ec:2b:7e:9b:b1:83:77:15:e1.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
tecmint@192.168.0.112's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'tecmint@192.168.0.112'"
and check to make sure that only the key(s) you wanted were added.

tecmint@instructor ~ $
```

```
Terminal
tecmint@instructor ~ $
tecmint@instructor ~ $ ssh-copy-id tecmint@192.168.0.113
The authenticity of host '192.168.0.113 (192.168.0.113)' can't be established.
RSA key fingerprint is ff:1d:c0:e4:aa:ee:62:37:17:b4:86:16:73:46:88:06.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
tecmint@192.168.0.113's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'tecmint@192.168.0.113'"
and check to make sure that only the key(s) you wanted were added.

tecmint@instructor ~ $
```

After copying all SSH Keys to remote host, now perform a ssh key authentication on all remote hosts to check whether authentication working or not.

```
$ ssh user@192.168.0.112
$ ssh user@192.168.0.113
$ ssh user@192.168.0.114
```

```
tecmint@instructor ~ $  
tecmint@instructor ~ $ ssh tecmint@192.168.0.112  
[tecmint@srv1 ~]$ logout  
Connection to 192.168.0.112 closed.  
tecmint@instructor ~ $ ssh tecmint@192.168.0.113  
[tecmint@srv2 ~]$ logout  
Connection to 192.168.0.113 closed.  
tecmint@instructor ~ $ ssh tecmint@192.168.0.114  
[tecmint@srv3 ~]$ logout  
Connection to 192.168.0.114 closed.  
tecmint@instructor ~ $ █
```