SSH-Remote System Management

To access the remote machine using ssh, the syntax is

```
[root@vivek p]# ssh 192.168.254.136
The authenticity of host '192.168.254.136 (192.168.254.136)' can't be established.
ECDSA key fingerprint is SHA256:ME+V3zHU3ORB1pBL5Re7GFVgax/FD1bW1MIpcRc6Ojg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.254.136' (ECDSA) to the list of known hosts.
root@192.168.254.136's password:
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Wed Feb 16 08:17:05 2022
[root@localhost ~]#
```

to generate the SSH key pair

```
[root@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:KHlVdC1Qtjr5WZkKTiUccrxkI4nJXg+Ybgy4sfO+e2M root@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]----+
|    . . =.+*o+.   |
|   o . * ===+...  |
|    + = ..*ooo.   |
|   +  .=o  o=   o |
|   oo.o S *   +   |
|    .o   o + +    |
|   .       . +    |
|    . E           |
|    o= .          |
+----[SHA256]-----+
[root@localhost ~]#
```

HIDEDEN FILES SHOW

```
[root@localhost ~]# ls -la
total 32
dr-xr-x---.  6 root root  213 Feb 16 02:53 .
dr-xr-xr-x. 17 root root  224 Feb 16  2022 ..
-rw-------.  1 root root 1404 Feb 16  2022 anaconda-ks.cfg
-rw-r--r--.  1 root root   18 Aug 12  2018 .bash_logout
-rw-r--r--.  1 root root  176 Aug 12  2018 .bash_profile
-rw-r--r--.  1 root root  176 Aug 12  2018 .bashrc
drwx------.  3 root root   19 Feb 16  2022 .cache
drwx------.  4 root root   31 Feb 16 02:50 .config
-rw-r--r--.  1 root root  100 Aug 12  2018 .cshrc
drwx------.  3 root root   25 Feb 16  2022 .dbus
-rw-------.  1 root root   16 Feb 16 02:50 .esd_auth
-rw-r--r--.  1 root root 1559 Feb 16  2022 initial-setup-ks.cfg
drwx------.  2 root root   38 Feb 16 02:53 .ssh
-rw-r--r--.  1 root root  129 Aug 12  2018 .tcshrc
```

CHECK FILE

```
[root@localhost ~]# cd .ssh
[root@localhost .ssh]# ls
id_rsa  id_rsa.pub
[root@localhost .ssh]#
```

CREATED BY:- VIVEK GANDHI

SSH-Remote System Management

2 SERVER SSH KEYGEN

```
┌──(root☠kali)-[~]
└─# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:kZ8pPdbDLbG1SgCDhP66hzG6vitrBwOdWp98Vo51Z3Y root@kali
The key's randomart image is:
+---[RSA 3072]----+
|     o..o        |
|    . . +        |
|  . o   o . . .  |
| . + .   o+.*+=E.|
|.o o o =S.B+B.o  |
|.o  * = .o o +   |
|  o. B      .    |
|....o .          |
|o+*+.o           |
+------[SHA256]-----+
```

```
[root@localhost ~]# ls -la
total 36
dr-xr-x---.  6 root root  234 Feb 16 03:05 .
dr-xr-xr-x. 17 root root  224 Feb 16  2022 ..
-rw-------.  1 root root 1404 Feb 16  2022 anaconda-ks.cfg
-rw-------.  1 root root  154 Feb 16 03:01 .bash_history
-rw-r--r--.  1 root root   18 Aug 12  2018 .bash_logout
-rw-r--r--.  1 root root  176 Aug 12  2018 .bash_profile
-rw-r--r--.  1 root root  176 Aug 12  2018 .bashrc
drwx------.  3 root root   19 Feb 16  2022 .cache
drwx------.  4 root root   31 Feb 16 02:50 .config
-rw-r--r--.  1 root root  100 Aug 12  2018 .cshrc
drwx------.  3 root root   25 Feb 16  2022 .dbus
-rw-------.  1 root root   16 Feb 16 02:50 .esd_auth
-rw-r--r--.  1 root root 1559 Feb 16  2022 initial-setup-ks.cfg
drwx------.  2 root root   38 Feb 16 03:05 .ssh
-rw-r--r--.  1 root root  129 Aug 12  2018 .tcshrc
```

```
┌──(root☠kali)-[~/.ssh]
└─# ls
authorized_keys  id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

Id_rsa -> private file

Id_rsa.pub -> public file

Authorized_keys -> new acess file created

VIM FILE CREATED

```
┌──(root☠kali)-[~/.ssh]
└─# vim authorized_keys
^[[C
```

SSH-Remote System Management

File Actions Edit View Help

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDTmjiMMDHG5jGu5e9fNnBFN7ilNwyg+xH529eEswC1vLsudH9Oqk9q23rttp4OPFZQoOjF1jBHvGnFotKPdwkmOxunxqwWbJxP
oj6y0XInriBhWEHpD3N5xqu2gMP5fFQ/FhsRgYS+7/JaXeRvPbvKuUSQoWB4KGKM/sw8wqidH9We686THrM4Rf5uMPiNfFRrB2CikSC13VXbxzrJ7ypRGKkQ3wzFzCEUegLT7QcR
uF1VE9QORGbsVaEiltasCFDn/UFtkGqpabTo87vhfccjYi2uUc9mP+tqMpHxwJDvNIlKGkHst6+Ndjc= root@vivek.gandhi.com
~
~

NO PASSWORD REQUIRED

```
┌──(root💀kali)-[~/.ssh]
└─# ssh root@192.168.254.135
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Wed Feb 16 03:21:09 2022
[root@vivek ~]#
```