



www.ez-admin.com

ศูนย์อบรมสำหรับผู้ต้องการก้าวสู่อาชีพผู้ดูแลระบบ
เครือข่ายคอมพิวเตอร์ โดยเรียนรู้จากการปฏิบัติงานจริง

“เราจะทำเรื่องยากให้เข้าใจง่ายด้วยสิ่งเหล่านี้”

- จัดอบรมเป็นกลุ่มเล็กๆ เพื่อให้การเรียนการสอนเกิดประสิทธิภาพสูงสุด
- เน้นเนื้อหาที่นำไปใช้งานได้จริง ถ่ายทอดให้ผู้เรียนเข้าใจได้ง่าย
- จัดทำคู่มือที่อ่านง่าย ทำตามได้ เพื่อให้ผู้เรียนนำไปต่อยอดหลังจากอบรม
- บริการอบรมซ้ำ เพื่อให้ผู้เรียนได้ทบทวนความรู้ให้เข้าใจได้ชัดเจนมากขึ้น

บริการเสริมที่น่าสนใจ : บริการติดตั้งระบบเครือข่ายคอมพิวเตอร์ ระบบ WiFi Hotspot ด้วย MikroTik บริการดูแลระบบ
เครือข่าย บริการติดตั้งระบบ Thin Client หรือ Zero Client คลินิกดูแลละเอียดได้ที่ service.ez-admin.com

บทที่ 3 กำหนดค่า Network Connection

RedHat จะติดต่อกับเครื่องอื่นๆ ที่อยู่ภายในระบบเครือข่ายเดียวกันได้ จะขึ้นอยู่กับค่า Network Connection ที่ได้กำหนดไว้ในส่วนของ `/etc/sysconfig/network-script` ซึ่งในบทนี้เราจะได้เรียนรู้เกี่ยวกับการเข้าไปกำหนดค่าในไฟล์หรือไดเรกทอรีต่างๆ ที่เกี่ยวข้องเกี่ยวกับค่า Network Connection กันอย่างละเอียด และในส่วนท้ายบท จะพูดถึงการรีโมทเข้ามาควบคุมเครื่อง RedHat โดยใช้โปรโตคอล SSH ด้วย

ใช้คำสั่ง `ifconfig`

`ifconfig` เป็นคำสั่งที่ใช้ในการจัดการค่าต่างๆ ของการ์ด LAN (Network Interface Card) ถือว่าเป็นคำสั่งสำคัญและมีการใช้งานบ่อย หากเรียกใช้คำสั่ง `ifconfig` โดยไม่มีการพิมพ์ค่าพารามิเตอร์ใดๆ ลงไป จะเป็นการสั่งให้แสดงผลค่าการทำงานของของการ์ด LAN ขึ้นมา

คำสั่ง `ifconfig` จะแสดงผลคำสั่งและค่าสำคัญต่างๆ ที่เกี่ยวข้องกับการทำงานของการ์ด LAN ดังนี้

- `inet` แสดงหมายเลข IP Address V4
- `netmask` แสดงหมายเลข Subnet Mask
- `broadcast` แสดงหมายเลข Broadcast Address
- `inet6` แสดงหมายเลข IP Address V6
- `ether` แสดงหมายเลข MAC Address
- `RX packets` และ `TX packets` แสดงจำนวนแพ็กเก็ต (Packet) และสถานะของการรับ (RX) และส่ง (TX)
- `RX bytes` และ `TX bytes` แสดงขนาดรวมของแพ็กเก็ตที่ใช้ในการรับและส่ง

Note

```
# nmcli dev status (ตรวจสอบสถานะของการ์ดแลน)
```

```
# nmcli dev show ens33 (ตรวจสอบค่าคอนฟิก (IP Address) ของการ์ดแลนชื่อ ens33)
```

กำหนดค่าของการ์ด LAN (Network Card)

การกำหนดค่าการ์ด LAN เป็นสิ่งสำคัญที่จะทำให้ RedHat เชื่อมต่อกับระบบเครือข่ายได้ โดยปกติในขั้นตอนการติดตั้งจะมี 2 ทางเลือก คือ ให้เครื่องรับหมายเลข IP จากเครื่อง DHCP Server ในที่นี้อาจเป็น ADSL Router หรือ Firewall ก็ได้ อีกทางเลือกหนึ่ง คือ กำหนดหมายเลข IP ของการ์ด LAN ด้วยตัวเอง ซึ่งในขั้นตอนการติดตั้ง เราได้เลือกแบบกำหนดเองไปแล้ว ซึ่งสามารถย้อนกลับไปแก้ไขค่าต่างๆ เหล่านี้ได้ภายหลัง แต่ก่อนอื่นเราต้องรู้จักไฟล์และไดเรกทอรีที่เกี่ยวข้องกับค่า Network Connection เหล่านี้กันก่อน

ทุกครั้งที่ RedHat บูตขึ้นมาทำงาน จะมีการเรียกใช้งานและอ่านค่าไฟล์ Networking ที่เก็บอยู่ใน /etc/sysconfig/network-scripts โดยในไดเรกทอรีนี้จะมีไฟล์สำคัญที่ชื่อ ifcfg-xxx ซึ่งค่าสำคัญของ Network Connection จะอยู่ในไฟล์นี้

1. เราสามารถเข้าไปกำหนดค่าต่างๆ ของไฟล์ ifcfg-eth0 ได้ โดยใช้คำสั่ง...

```
# gedit /etc/sysconfig/network-scripts/ifcfg-ens33
```

```
1 HWADDR=00:0C:29:D0:FF:91
2 TYPE=Ethernet
3 BOOTPROTO=static
4 DEFROUTE=yes
5 IPV4_FAILURE_FATAL=no
6 IPV6INIT=yes
7 IPV6_AUTOCONF=yes
8 IPV6_DEFROUTE=yes
9 IPV6_FAILURE_FATAL=no
10 NAME=ens33
11 UUID=c5555662-0eaa-4112-a6b5-4b19451952b1
12 DEVICE=ens33
13 ONBOOT=yes
14 DNS1=8.8.8.8
15 DNS2=8.8.4.4
16 IPADDR=192.168.0.10
17 PREFIX=24
18 GATEWAY=192.168.0.2
19 IPV6_PEERDNS=yes
20 IPV6_PEERROUTES=yes
21 IPV6_PRIVACY=no
```

2. หลังจากกำหนดค่าที่เกี่ยวข้องกับระบบเครือข่ายเสร็จแล้ว ให้รีสตาร์ทเซอวิสทุกครั้งด้วยคำสั่ง...

```
# systemctl restart network
```

```
# service network restart
```

ใช้คำสั่ง Ping ตรวจสอบการรับส่งข้อมูล

Ping ย่อมาจาก Package Internet Groper เป็นคำสั่งสำหรับตรวจสอบการรับส่งข้อมูลระหว่าง เครื่องต้นทางกับคอมพิวเตอร์หรืออุปกรณ์เน็ตเวิร์กปลาย

ตัวอย่าง หากต้องการตรวจสอบว่า RedHat จะสามารถติดต่อกับ Web Server ของ Google ได้หรือไม่ ให้พิมพ์คำสั่ง

```
# ping -c 5 www.google.com
```

หากมีการตอบกลับจากเครื่องปลายทางก็คือ Web Server ของ Google ก็แสดงว่า RedHat ในเครื่องของเราสามารถเชื่อมต่อกับ Web Server ของ Google ได้แล้ว

```
[root@server1 ~]# ping -c 5 www.google.com
PING www.google.com (74.125.130.106) 56(84) bytes of data:
64 bytes from sb-in-f106.1e100.net (74.125.130.106): icmp_seq=1 ttl=128 time=39.3 ms
64 bytes from sb-in-f106.1e100.net (74.125.130.106): icmp_seq=2 ttl=128 time=40.3 ms
64 bytes from sb-in-f106.1e100.net (74.125.130.106): icmp_seq=3 ttl=128 time=40.8 ms
64 bytes from sb-in-f106.1e100.net (74.125.130.106): icmp_seq=4 ttl=128 time=38.2 ms
64 bytes from sb-in-f106.1e100.net (74.125.130.106): icmp_seq=5 ttl=128 time=39.2 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 38.294/39.620/40.840/0.900 ms
```

กำหนด DNS Resolver

เพื่อให้ RedHat สามารถติดต่อไปยังเครื่องอื่นด้วยชื่อเครื่อง (Host name) ได้ เราจะต้องกำหนดหมายเลข IP ของเครื่องที่ทำหน้าที่เป็น DNS Resolver ลงในไฟล์ /etc/resolv.conf โดย...

1. เปิดไฟล์ /etc/resolv.conf ด้วยคำสั่ง...

```
# gedit /etc/resolv.conf
```

2. ตรวจสอบหมายเลข IP ของเครื่องที่จะทำหน้าที่เป็น DNS Resolver โดยหมายเลข IP ของ DNS Server ในไฟล์นี้จะถูกจัดการจากโปรแกรม Network Manager ซึ่งจะดึงค่ามาจากไฟล์ /etc/sysconfig/network-script/ifcfg-ens33

```
1 # Generated by NetworkManager
2 search localdomain
3 nameserver 8.8.8.8
4 nameserver 8.8.4.4
```

DNS ตัวแรกที่ถูกกำหนดไว้จะถูกเรียกใช้งานก่อน ก็คือหมายเลข 8.8.8.8 หากตัวแรกมีปัญหา DNS ในบรรทัดที่สองก็คือเครื่องหมายเลข 8.8.4.4 จะทำงานแทนตามลำดับลงไปเรื่อยๆ

ให้ทดสอบว่า DNS Server ที่กำหนด สามารถใช้งานได้หรือไม่ โดยใช้คำสั่ง ping ออกไปยังเครื่องที่อยู่เครือข่ายภายนอกด้วยชื่อเครื่อง เช่น

```
# ping -c5 www.google.com
```

หากมีการ Reply ตอบกลับจากเครื่องปลายทาง ก็แสดงว่าหมายเลข IP ของ DNS Resolver ที่กำหนดลงไปสามารถใช้งานได้จริง

หรือจะเลือกใช้คำสั่ง dig เพื่อ Query ฐานข้อมูล DNS ของ DNS Resolver ที่ต้องการตรวจสอบ เช่น ต้องการตรวจสอบ Record ใน DNS Server ของ google.com ให้พิมพ์คำสั่ง

```
# dig www.google.com
```

กำหนดชื่อเครื่อง (Host)

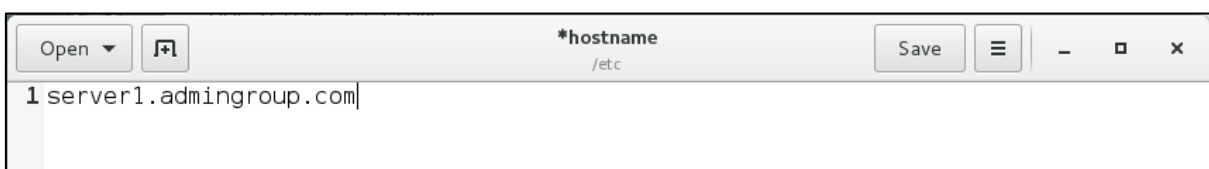
หลังจากกำหนด DNS Server ที่ต้องการใช้งานแล้ว หากต้องการให้เครื่องอื่นๆ ติดต่อมาที่เครื่อง RedHat ด้วยชื่อเครื่อง จะต้องเข้าไปกำหนดค่าของ hostname ดังนี้

1. เปิดไฟล์ /etc/hostname โดยพิมพ์คำสั่ง...

```
# gedit /etc/hostname
```

2. แก้ไขชื่อเครื่องเป็น...

```
server1.admingroup.com
```

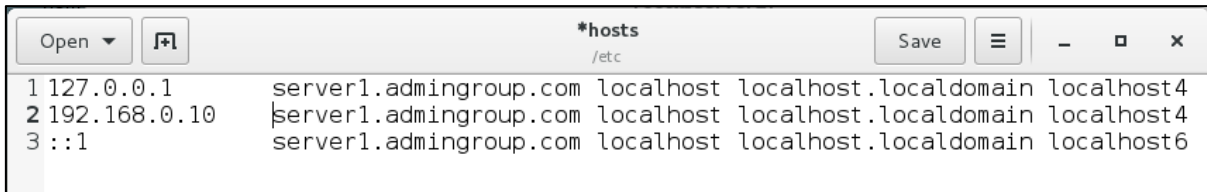


3. เปิดไฟล์ /etc/hosts โดยพิมพ์คำสั่ง...

```
# gedit /etc/hosts
```

4. แก้ไขชื่อเครื่องเป็น...

```
127.0.0.1      server1.admingroup.com
192.168.0.10  server1.admingroup.com
::1           server1.admingorup.com
```



```
*hosts
/etc
1 127.0.0.1      server1.admingroup.com localhost localhost.localdomain localhost4
2 192.168.0.10  server1.admingroup.com localhost localhost.localdomain localhost4
3 ::1           server1.admingroup.com localhost localhost.localdomain localhost6
```

5. รีสตาร์ท Service ของ Network โดยพิมพ์คำสั่ง...

```
# systemctl restart network
```

6. ทดสอบการแก้ไขชื่อเครื่อง โดยพิมพ์คำสั่ง

```
# hostname -f          (สำหรับแสดงชื่อเครื่องแบบเต็ม)
หรือคำสั่ง...
# hostname -s          (สำหรับแสดงชื่อเครื่องแบบสั้น)
```

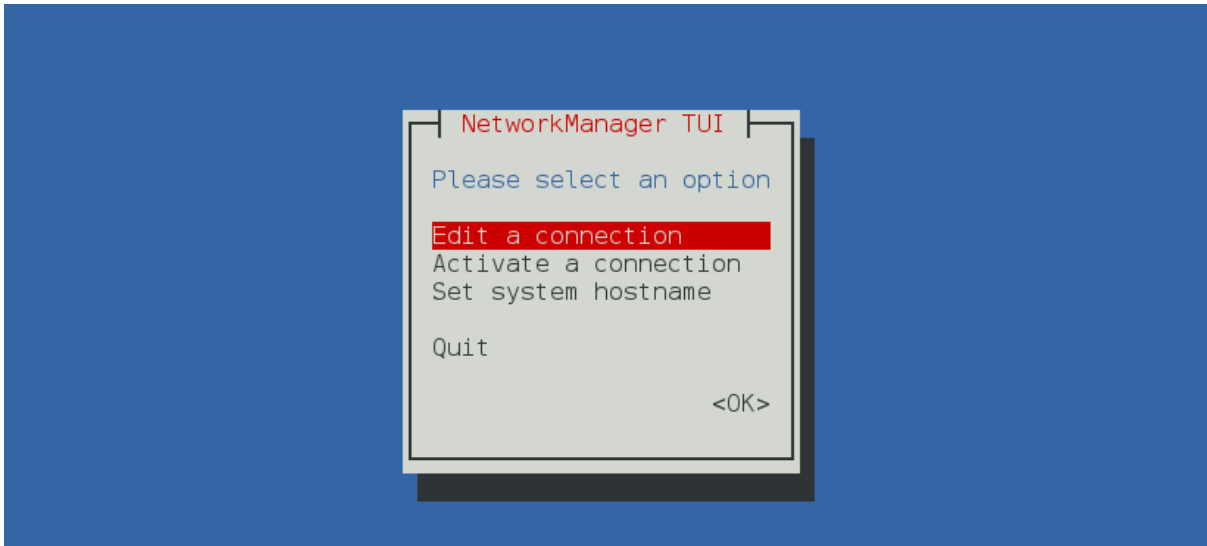
ใช้เมนู Text GUI กำหนดค่า Network ทั้งหมด

เราสามารถกำหนดค่า Network อย่างสะดวกรวดเร็วแทนการเข้าไปกำหนดค่าทีละไฟล์ได้ด้วยคำสั่ง nmtui ซึ่งเป็นการใช้งานแบบ Text GUI ของโปรแกรม Network Manager

1. เรียกหน้าต่าง Text GUI ขึ้นมา โดยพิมพ์คำสั่ง...

```
# nmtui
```

2. จะปรากฏเมนู NetorkManager TUI ขึ้นมา ซึ่งเราสามารถกำหนดค่าการทำงาน Network ทั้งหมดของ RedHat ได้จากเมนูเหล่านี้



การติดตั้ง SSH Server

หลังจากกำหนดค่าการทำงานของระบบเครือข่ายให้กับ RedHat แล้ว ปัจจุบันการเข้าไปกำหนดค่าการทำงานต่างๆ ที่เครื่องเซิร์ฟเวอร์ เรามักจะใช้เครื่องไคลเอนต์ Log in เข้าไปมากกว่าที่จะไปทำงานที่หน้าเครื่องเซิร์ฟเวอร์โดยตรง เพราะเหตุผลด้านความปลอดภัยและความสะดวกนั่นเอง

ปัจจุบันโปรแกรมที่นิยมใช้ในการ Remote Log in จะใช้โปรแกรมประเภท Open SSH หรือ SSH (Secure Shell) ซึ่งคล้ายกับโปรแกรมประเภท Telnet แต่ SSH จะมีความปลอดภัยมากกว่า เพราะมีการเข้ารหัสไว้ด้วย โดยปกติ Open SSH จะติดตั้งมากับ RedHat โดยสามารถตรวจสอบได้จากคำสั่ง

```
# systemctl status sshd
```

(ตรวจสอบว่า ssh ทำงานอยู่หรือไม่)

```
# systemctl is-enabled sshd
```

(ตรวจสอบว่า ssh ถูกเปิดใช้ตอนบูตเครื่อง)

หากตรวจสอบด้วยคำสั่ง `service sshd status` แล้วไม่พบ SSH กำลังทำงานอยู่ ให้ติดตั้งลงไปใหม่ ใช้คำสั่ง

```
# yum install openssh-server
```

หรือถ้าตรวจสอบแล้วพบว่า SSH ถูกปิดการทำงานอยู่ ให้เปิดขึ้นมาทำงานอีกครั้งด้วยคำสั่ง

```
# systemctl start sshd
```

```
# systemctl status sshd
```

ถ้าต้องการให้ SSH ถูกเรียกใช้ตอนบูตเครื่องขึ้นมาใหม่ ให้พิมพ์คำสั่ง

```
# systemctl enable sshd
```

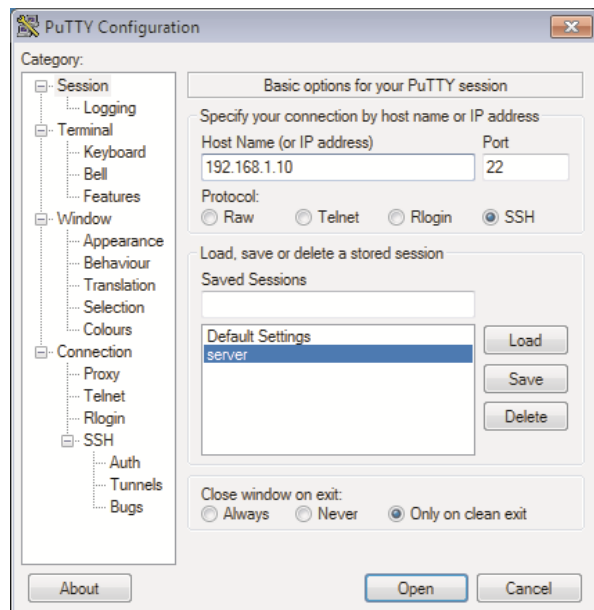
รีโมทด้วย SSH Client

ที่เครื่องไคลเอนต์ (อาจเป็น Linux หรือ Windows 7/10) จะต้องติดตั้งโปรแกรมประเภท SSH Client ลงไป เพื่อใช้เป็นหน้าต่าง Console ในการเข้ามาควบคุมเครื่องเซิร์ฟเวอร์ เช่น โปรแกรม putty, SecureCRT หรือ SSHSecureShellClient

ตัวอย่างนี้จะใช้โปรแกรม putty เนื่องจากใช้เป็น Open Source และใช้งานง่าย โดยดาวน์โหลดได้ที่

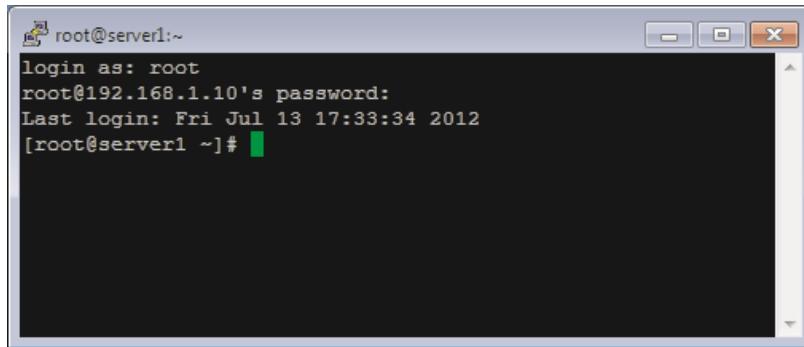
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> เมื่อเปิดโปรแกรม

Putty ขึ้นมา ให้พิมพ์หมายเลข IP ของ RedHat ลงในช่อง Host Name และคลิกเลือกช่อง SSH ทำให้ที่ช่อง Port โปรแกรมจะกำหนดเป็น 22 เพราะเป็นพอร์ตทำงานของ SSH จากนั้นหากต้องการเซฟชื่อเก็บไว้เพื่อวันหลังจะได้ไม่ต้องใส่หมายเลข IP ของ



เครื่อง RedHat อีกให้กำหนดชื่อเครื่องที่ช่อง Saved Session แล้วคลิกปุ่ม Save แล้วคลิกปุ่ม Open เพื่อรีโมท Log in เข้าสู่เครื่อง RedHat

เมื่อปรากฏหน้าต่าง Log in ขึ้นมา ให้พิมพ์ชื่อยูสเซอร์และรหัสผ่านที่ต้องการ Log in ลงไป หากข้อมูลทุกอย่างถูกต้อง ก็จะสามารถรีโมทเข้าไปที่เครื่อง RedHat ได้



เพิ่มความปลอดภัยให้การรีโมทผ่าน SSH

ถ้าต้องการให้การรีโมท SSH มีความปลอดภัยมากขึ้น เราอาจกำหนดให้ยูสเซอร์ที่จะรีโมทห้ามใช้ Root เข้ามา หรือให้ใช้เฉพาะยูสเซอร์บางคนหรือเฉพาะบางเครื่องเท่านั้นที่เข้ามาได้ โดยเข้าไปแก้ไขค่าในไฟล์ /etc/ssh/sshd_config

1. เปิดไฟล์ /etc/ssh/sshd_config ด้วยคำสั่ง...

```
# gedit /etc/ssh/sshd_config
```

2. เลื่อนเคอร์เซอร์ไปบรรทัดที่ 17 จะพบคำสั่ง Port (ค่าปกติ คือ 22) เราสามารถแก้ไขเป็นพอร์ตอื่นๆ ที่ไม่ใช่พอร์ตมาตรฐานของ SSH (22) ทำให้นอกจากคนที่เข้ามาจะต้องใส่ชื่อ User และ Password ให้ถูกแล้ว ต้องใส่หมายเลขพอร์ตที่เรากำหนดไว้ด้วย จึงจะรีโมทเข้ามาได้

```
Port <หมายเลขพอร์ต>
```

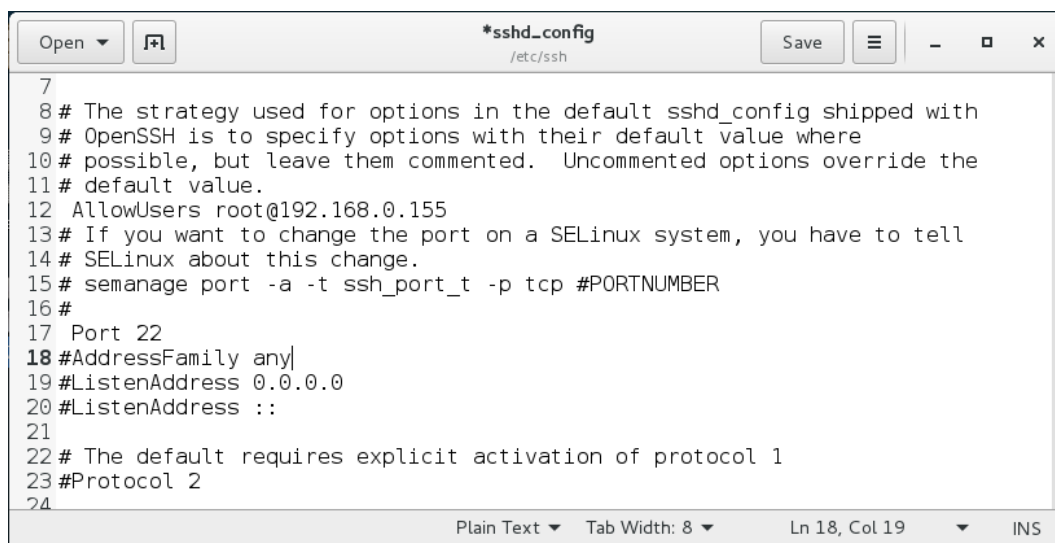
3. เลื่อนเคอร์เซอร์ไปบรรทัดที่ 49 จะพบคำสั่ง PermitRootLogin (ค่าปกติ คือ yes) แก้ไขคำสั่งนี้ให้เป็น no เพื่อห้ามไม่ให้ Root สามารถรีโมทผ่านทาง SSH ได้

```
PermitRootLogin no
```

4. หากต้องการให้รีโมทเข้ามาเฉพาะยูสเซอร์และเครื่องที่มีหมายเลข IP ที่ได้รับอนุญาตเท่านั้นให้เพิ่มคำสั่งด้านล่างนี้ไว้ด้านบนของไฟล์

```
AllowUsers root@192.168.1.105
```

คำสั่งนี้หมายความว่าอนุญาตให้ยูสเซอร์ root ที่ใช้เครื่องหมายเลข IP คือ 192.168.1.105 เท่านั้นจึงจะสามารถรีโมทเข้ามาได้



```

7
8 # The strategy used for options in the default sshd_config shipped with
9 # OpenSSH is to specify options with their default value where
10 # possible, but leave them commented. Uncommented options override the
11 # default value.
12 AllowUsers root@192.168.0.155
13 # If you want to change the port on a SELinux system, you have to tell
14 # SELinux about this change.
15 # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
16 #
17 Port 22
18 #AddressFamily any|
19 #ListenAddress 0.0.0.0
20 #ListenAddress ::
21
22 # The default requires explicit activation of protocol 1
23 #Protocol 2
24

```

5. ทุกครั้งที่มีการเปลี่ยนแปลงค่าใหม่ให้สั่งรีสตาร์ทเซอร์วิสของ SSH ด้วย โดยพิมพ์คำสั่ง...

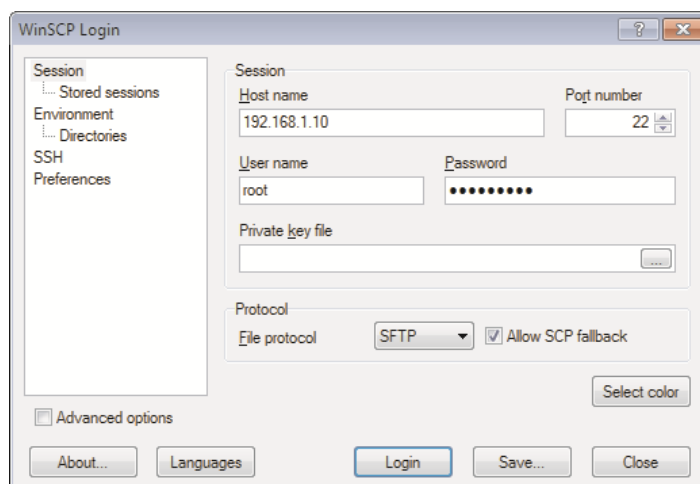
```
# systemctl restart sshd
```

การใช้ SFTP ในการรับส่งไฟล์ไปที่ RedHat

หลังจากที่ติดตั้ง SSH แล้ว จะมีการติดตั้ง Protocol ชื่อ SFTP ลงไปด้วย โดย SFTP จะเป็น Protocol ที่ทำงานคล้ายกับ FTP (File Transfer Protocol) เพื่อใช้ในการรับส่งไฟล์ระหว่างเครื่อง RedHat กับเครื่องอื่นๆ

สำหรับเครื่องไคลเอนต์ที่ต้องการโอนไฟล์ไปเก็บไว้ที่เครื่อง RedHat จะต้องติดตั้งโปรแกรมประเภท SFTP Client เช่น WinSCP หรือ SSHSecureFileTransferClient

ตัวอย่างนี้จะทดสอบการใช้งานโปรแกรม WinSCP โดยที่เครื่องไคลเอนต์เรียกหน้าต่างโปรแกรมขึ้นมา ที่ช่อง Hostname กำหนดหมายเลข IP ของเครื่อง RedHat และที่ช่อง Port Number ให้ใส่หมายเลขพอร์ตของ SFTP ลงไป (จะใช้พอร์ตเดียวกับ SSH) แล้วที่พิมพ์ชื่อยูสเซอร์และรหัสผ่านลงในช่อง User name และ Password ตามลำดับ จากนั้นคลิกปุ่ม Login



หากข้อมูลถูกต้อง เครื่องไคลเอนต์จะสามารถรับส่งไฟล์ไปที่เครื่อง RedHat ได้ ผ่านหน้าต่างโปรแกรม WinSCP