

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	1 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



Creating virtual networking of ubuntu servers using VirtualBox

Contents

1	Networking.....	2
2	Virtual Network Topologies (VM)	2
2.1	Example of VN topologies.....	2
2.2	Default VN network topology.....	3
2.3	Topology used in this Manual	3
3	Requirements.....	4
3.1	VirtualBox.....	4
3.2	Ubuntu server 18.04 LTS	4
3.3	Cygwin	4
3.4	PuTTY and PuTTYgen	4
4	Create a cloneable base server	4
4.1	Install	5
4.2	Configure.....	9
5	Cloning the base server into network nodes	13
5.1	Create a snapshot of the base virtual machine	13
5.2	Clone Virtual Machine (base)	13
5.3	Configure each node	16
6	Using the virtual network.....	18
6.1	Cygwin	18
6.2	PuTTY and PuTTYgen	21
7	What's next?	26
8	References	26

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	2 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	

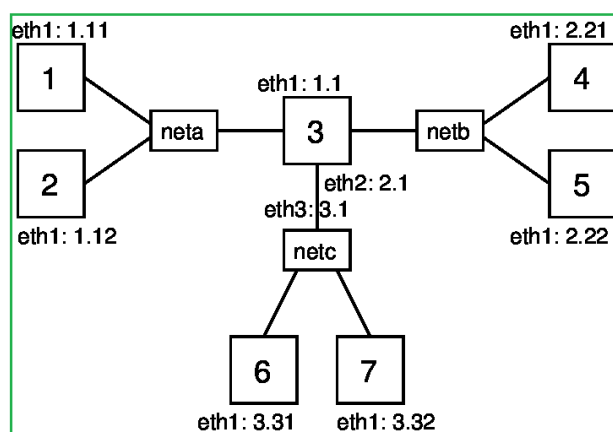
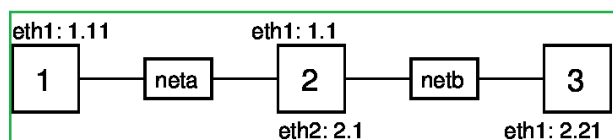
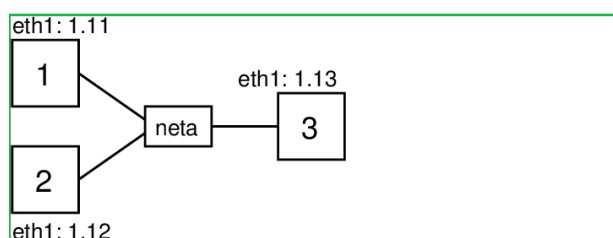


1 Networking

Often, it is necessary to create virtual networking labs to simulate, practice different environments and testing scenarios. Cloud platforms such as GCP, AWS and Azure already offer easy configurations at some cost (\$\$). This document presents an open source solution to setup virtual networking environments of ubuntu servers using VirtualBox. Although Virtual Machines use hypervisor for virtualization, it is still a great open source solution for a limited range of applications.

2 Virtual Network Topologies (VM)

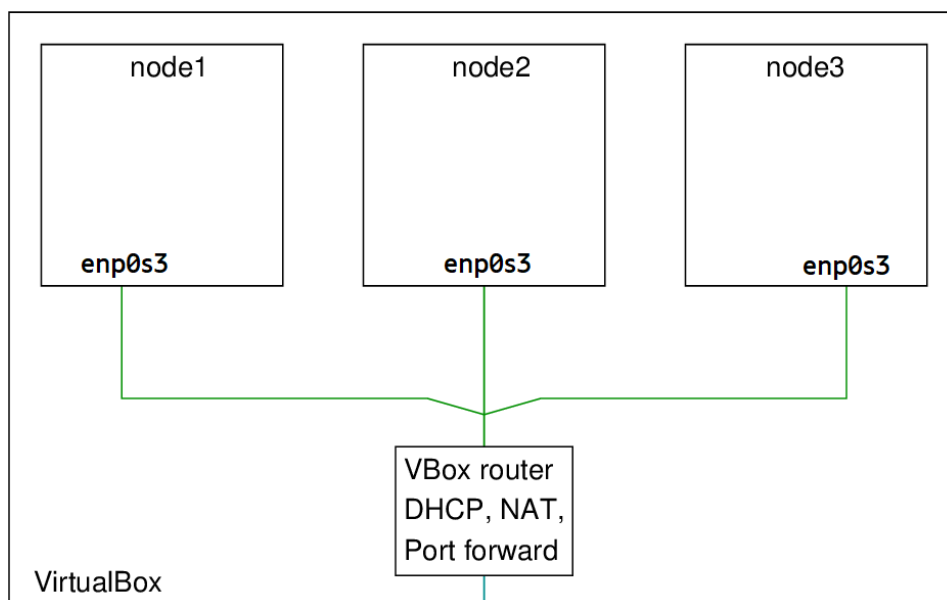
2.1 Example of VN topologies



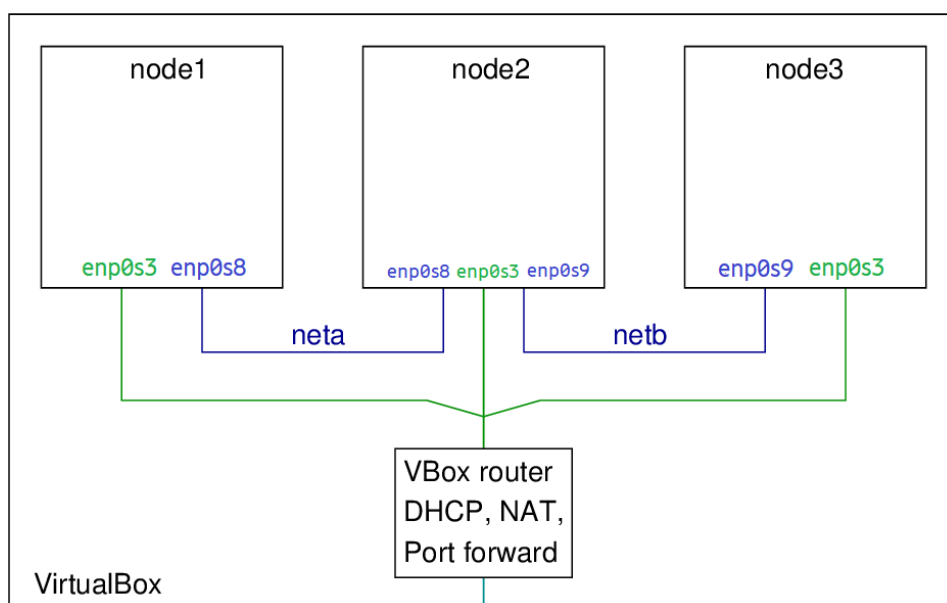
Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	3 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



2.2 Default VM NAT Adapter



2.3 Topology used in this Manual



Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	4 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



3 Requirements

This manual assumes you are using Windows OS. In case a different OS is used, please find alternative or appropriate tools whenever applicable.

3.1 VirtualBox

Download VirtualBox for Windows hosts in the following link: [Download VirtualBox > VirtualBox platform packages > Windows hosts](#)

3.2 Ubuntu server 18.04 LTS

Download Ubuntu server 18.04, this document uses [Ubuntu 18.04.5 LTS \(Bionic Beaver\)](#), which can be found in <http://releases.ubuntu.com/18.04/> website next to the ***“Server install image”*** tab.

3.3 Cygwin

This manual assumes you have Cygwin installed, in case you do not have, you can follow the guide to install Cygwin in Moshell website, <http://newtran01.au.ao.ericsson.se/moshell/content.php?content.9>, refer to the section ***Installation for Cygwin***, that should work.

3.4 PuTTY and PuTTYgen

Go to [Download PuTTY: latest release](#) website, and download PuTTY and PuTTYgen.

1. PuTTY

Download and install the PuTTY software from the ***MSI (‘Windows Installer’)*** section, most windows are 64bit x86, so you can go ahead and download the ***64-bit x86*** version.

2. PuTTYgen

Using the same website, scroll down to the ***puttygen.exe (a RSA and DSA key generation utility)*** section and download and install the ***64-bit x86*** version.

4 Create a (cloneable) base server

Table 1. Virtual Machine Specifications

OS (Linux)	Memory	Processor	Hard disk
Ubuntu server (64-bit)	7.5 GB	3	10GB

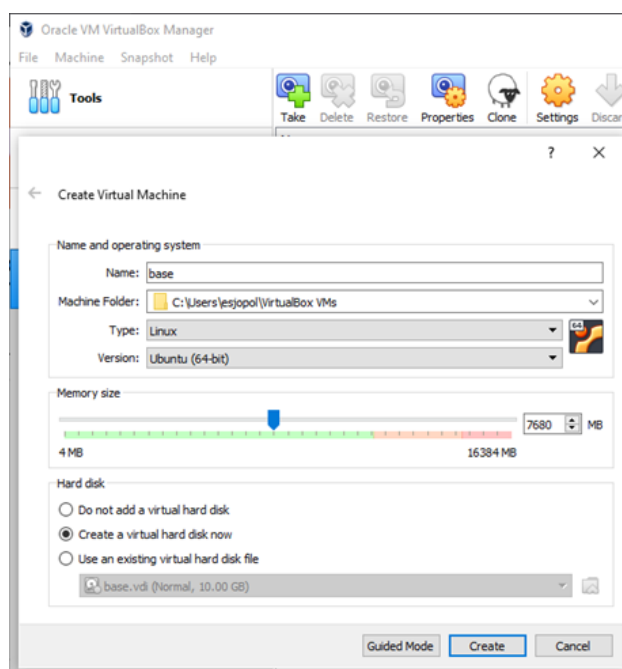
Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	5 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



4.1 Install

- A) Open VirtualBox, click on the **Machine > New**, and fill in as shown in the Figure below. Press **Create**, and on the next screen "Create Virtual Hard Disk", press **Create** again.

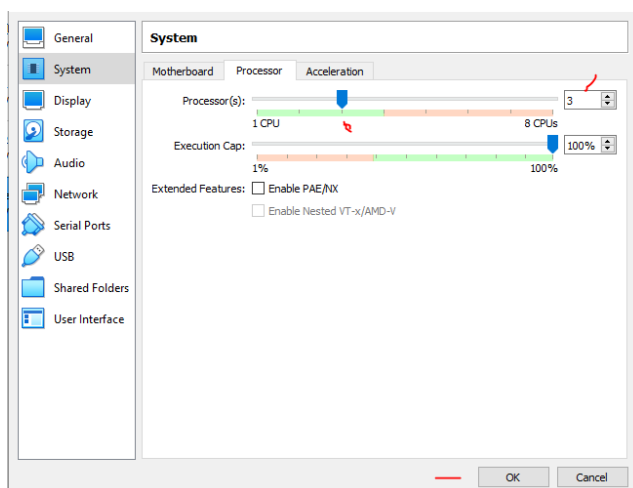
Figure 1. Create Virtual Machine



Name: **base**
Type: **Linux**
Version: **Ubuntu (64-bit)**
Memory size: **7680 MB**

- B) Change the System's processor to 3 CPUs. Right click on the **base** machine and select **settings...** option. Click on the **System** tab, then click on the **Processor** tab on the right. Set the Processor slider to 3 CPUs.

Figure 2. System CPUs



Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	6 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



- C) Before starting the machine, let's configure the network adapter settings.
- By default, VirtualBox enables only the first adapter, but allows up to four network adapters. We will configure most of them, even though some will not be used in this manual, but this allows flexibility in case you want to expand your own network configurations.

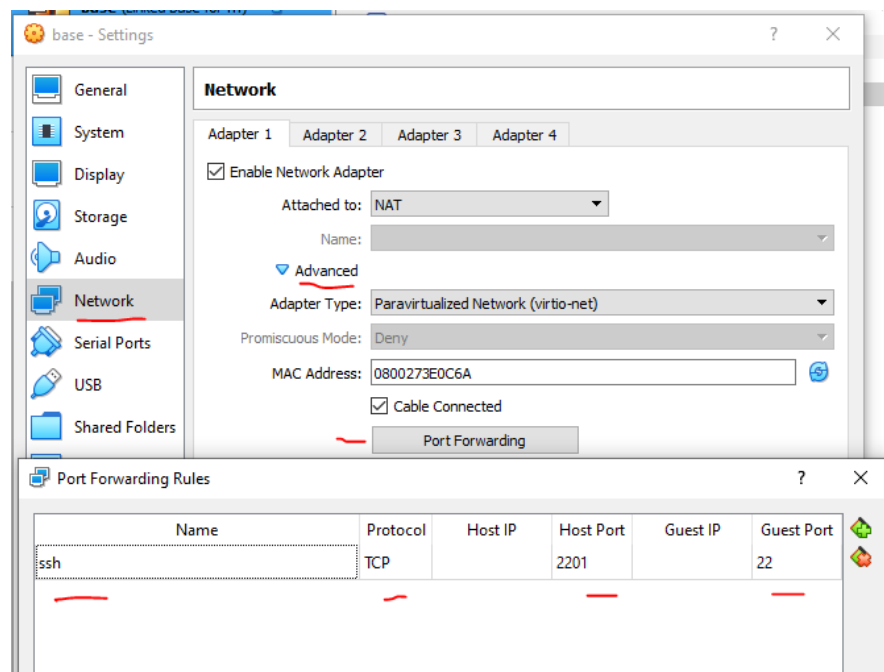
Right click on the **base** machine and select **settings...** option. Click on **Network** tab, next we will configure the network adapters one by one.

- **Adapter 1**, this adapter is configured by default to use NAT. It allows the virtual machine to have Internet access. This means that this adapter can communicate with the Host OS.

Go ahead and press the **Advanced** options. Here we need to change two things:

1. Press the **Port Forwarding** button and add a new rule with the following parameters:
 - Name: *ssh*
 - Protocol: *TCP*
 - Host IP:
 - Host Port: *2201*
 - Guest IP:
 - Guest Port: *22*

Figure 3. Port Forwarding



Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	7 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	

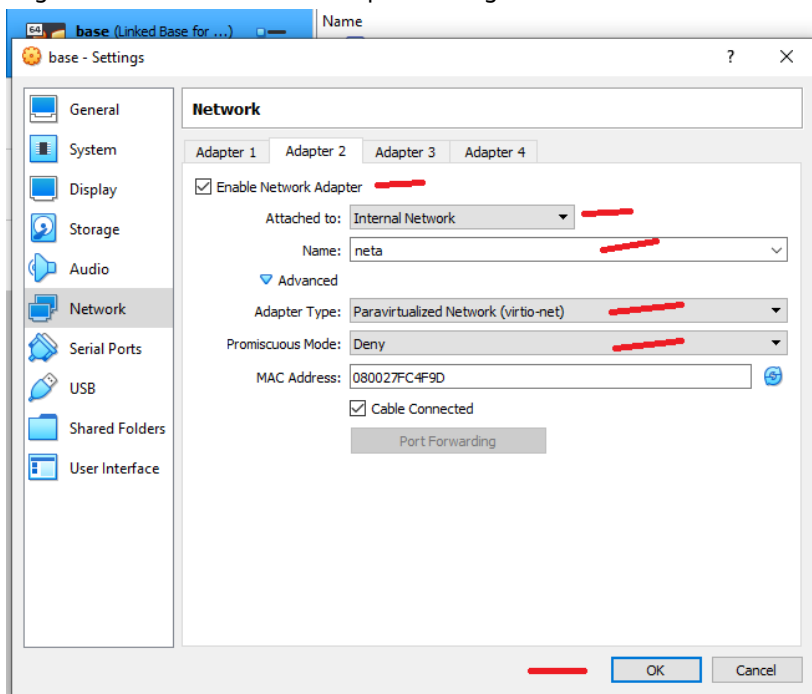


2. The **Adapter Type** may optionally be changed to **Paravirtualized Network (virtio-net)**. This option improves slightly the network performance. (This step is optional, the default type should still work fine).

- **Adapter 2, Adapter 3 and Adapter 4**, We going to use these adapters for the internal network of the Virtual machines, so that our ubuntu servers can communicate internally with each other. For each adapter, use the following configurations:
- Attached to: Internal Network
 - Name: *neta* (for Adapter 2), *netb* (Adapter 3), *netc* (Adapter 4)
 - Adapter Type: *Paravirtualized Network (virtio-net)*
 - Promiscuous Mode: *Deny*
 - MAC Address: *default value* (All adapters should have different values)
 - Cable Connection: *yes (checked)* for Adapter 2; *no (unchecked)* for Adapters 3 and 4. (You can enable this two adapters later according to your networking requirements)
 - Port Forwarding: no rules

You can refer to the Figure below. Click **OK** button to save configurations and close the *settings* window.

Figure 4. Internal Network Adapter settings

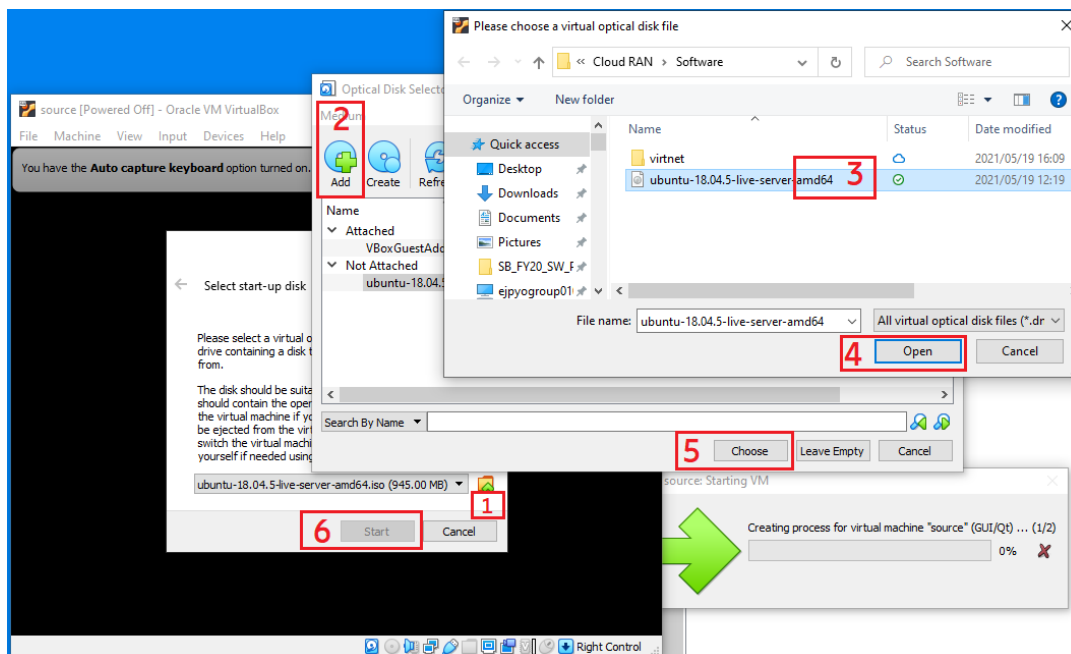


Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	8 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



- D) **Start** the **base** VM. Select your base VM and press Start. Virtualbox will prompt for a disc (iso) to boot from. Select the downloaded Ubuntu .iso image.
- Please refer to the figure below.

Figure 5. Boot from Ubuntu iso image



- E) **Continue with installation of the Ubuntu server.** As following:
- Use **UP**, **DOWN** and **ENTER** keys to select your language.
 - [English]
 - Installer update available
 - [Continue without updating]
 - Keyboard configuration
 - [Done]
 - (You can change the keyboard if you want, this installation uses English Keyboard)
 - Network connections
 - [Done]
 - (Confirm that the one interface was configured automatically with *DHCPv4*)
 - Configure proxy
 - [Done]
 - (No proxy setting required for this installation)
 - Configure Ubuntu archive mirror
 - [Done]
 - Guided storage configuration
 - (X) Use an entire disk
 - [X] Set up this disk as an LVM group
 - [Done]
 - (Default selection is okay)

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	9 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



- h) *Storage configuration*
 - *[Done]*
 - *Confirm destructive action*
 - *[continue]*
- i) *Profile setup*
 - *Your name: **ericsson***
 - *Your server's name: **base***
 - *Pick a username: **ericsson***
 - *Choose a password: **ericsson***
 - *Confirm your password: **ericsson***
- j) *SSH Setup*
 - *[X] Install OpenSSH server*
 - *[Done]*
- k) *Featured Server Snaps*
 - *[Done]*

(If you need any software from the list, you can select it. This installation does not select any software. If needed, it will be installed later using *sudo taskel* or *apt*)
- l) *Installing system -> Installation complete!*
 - *[cancel update and reboot]*

(We do not need new software updates, simply use the software in the .iso image)
- m) *Please remove the installation medium, then press ENTER:*

4.2 Configure

1. After reboot is complete, login to the server. As following:

```
base login: ericsson
Password: ericsson

ericsson@base:~$
```

2. Add Root Password

```
ericsson@base:~$ sudo su
root@base:/home/ericsson# passwd
Enter new UNIX password: ericsson
Retype new UNIX password: ericsson
passwd: password updated successfully
root@base:/home/ericsson# exit
exit
```

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	10 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



3. Network interface configuration

Check current networking interfaces, some (example) commands are:

```
ericsson@base:~$ ip link show [<interface_name>]
```

- List networking interfaces

```
ericsson@base:~$ ip address show [<interface_name>]
```

- List networking interfaces with IP addresses

```
ericsson@base:~$ ip link set enp3s0 down
```

- Bring an interface down

```
ericsson@base:~$ ip link set enp3s0 up
```

- Bring an interface up

In Ubuntu 18.04, network interface configuration has been migrated from `/etc/network/interfaces` in favor of [netplan](#) *.yaml based config.

The netplan network configuration *.yaml files are located inside the `/etc/netplan/` directory. Let's backup the current configuration and create a new virtual machine network configuration.

1. Backup

```
ericsson@base:~$ sudo mv /etc/netplan/00-installer-config.yaml  
/etc/netplan/00-installer-config.yaml.old_bak20210607
```

- Root password: **ericsson**

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	11 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



2. Create "vm-adapters-config.yaml" file with contents below: (fix)

```
ericsson@base:~$ cd /etc/netplan/
ericsson@base:/etc/netplan/$ sudo vi vm-adapters-config.yaml
ericsson@base:/etc/netplan/$ cat vm-adapters-config.yaml
network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses:
        - 192.168.1.11/24
      gateway4: 192.168.1.1
      optional: true
#   enp0s9:
#     addresses:
#       - 192.168.2.21/24
#     gateway4: 192.168.2.1
#     optional: true
#   enp0s10:
#     addresses:
#       - 192.168.3.31/24
#     gateway4: 192.168.3.1
#     optional: true
```

3. Apply network configuration

```
ericsson@base:~$ sudo netplan apply
```

- [netplan configuration](#)

```
ericsson@base:~$ ip address show
```

- Confirm interfaces 'enp0s3' and 'enp0s8' are up.

```
ericsson@base:~$ ip route
```

- Check ip routing table (route -n)

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	12 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



4. Password-less Logins

1. Create ssh keys

```
ericsson@base:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key
(/home/ericsson/.ssh/id_rsa): ENTER
Enter passphrase (empty for no passphrase): ENTER
Enter same passphrase again: ENTER
Your identification has been saved in
/home/ericsson/.ssh/id_rsa.
Your public key has been saved in
/home/ericsson/.ssh/id_rsa.pub.
The key fingerprint is:
4d:5f:66:33:21:bf:85:a4:8b:70:b2:ea:5b:da:ed:32 ericsson@base
The key's randomart image is:
+--[ RSA 2048 ]-----+
|           . o  |
|            = o  |
|         o o . 0 .|
|          B o = =|
|         S o o . |
|           .    |
|          . .   |
|         . +E.  |
|          +. . +o|
+-----+

```

- Default file location is ok (just press ENTER), and no passphrase is needed (press ENTER twice)

2. Copy the public key (id_rsa.pub) into **authorized_keys** file

```
ericsson@base:~$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

- This will allow us to login between cloned VM without password.

5. Other software configuration phase (Optional)

- mysql, postgresql
- server applications (scripts)
- etc...

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	13 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



6. Power off the VM

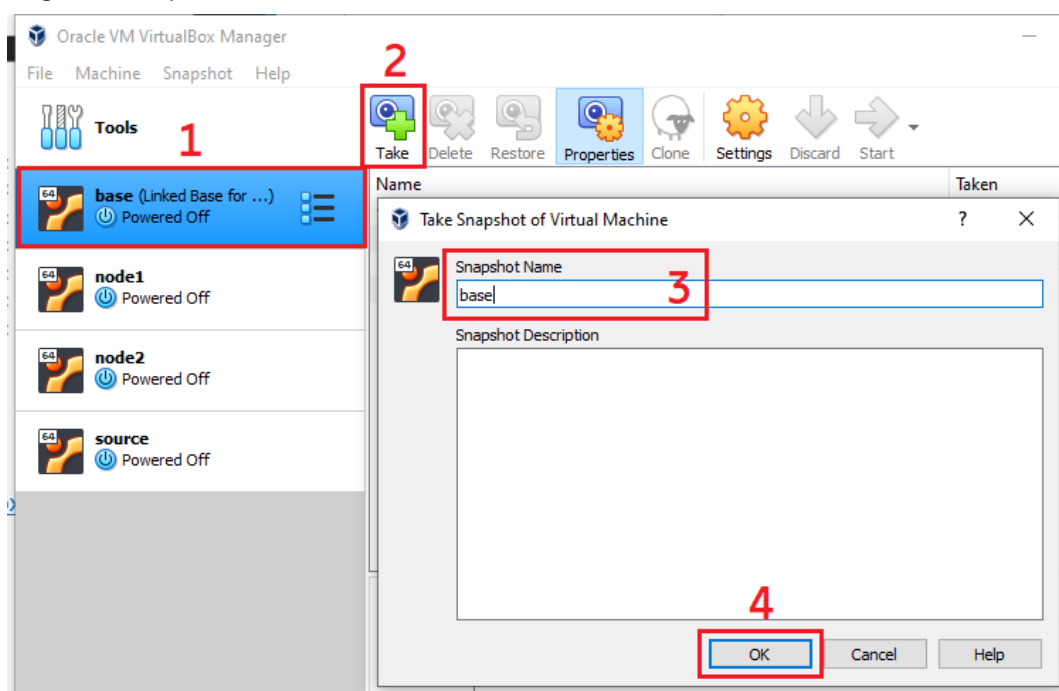
```
ericsson@base:~$ poweroff
```

5 Cloning the base server into network nodes

5.1 Create a snapshot of the base virtual machine

Before cloning the virtual machine, we need to create a snapshot of the current state of base VM, so that cloned machines can link to the current version. Refer to the Figure below:

Figure 6. Snapshot of the base VM

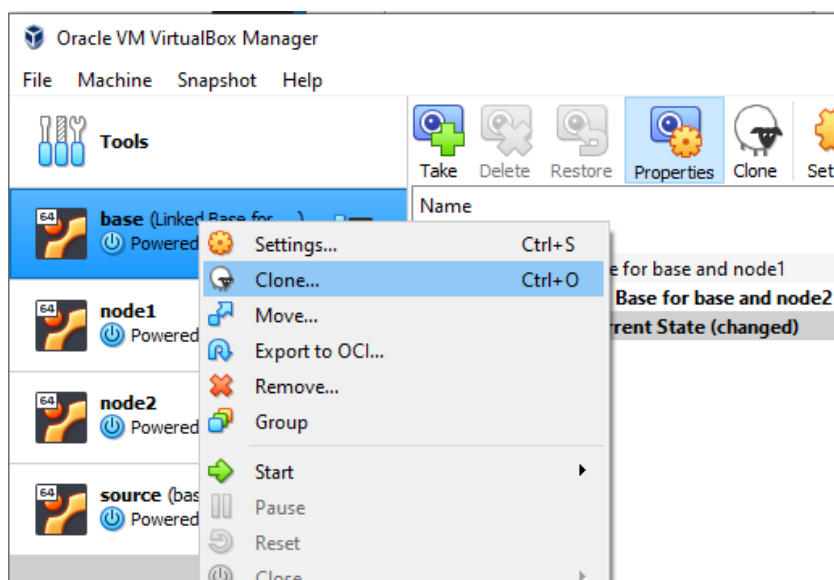


5.2 Clone Virtual Machine (base)

1. Right click on the base VM, and select Clone...

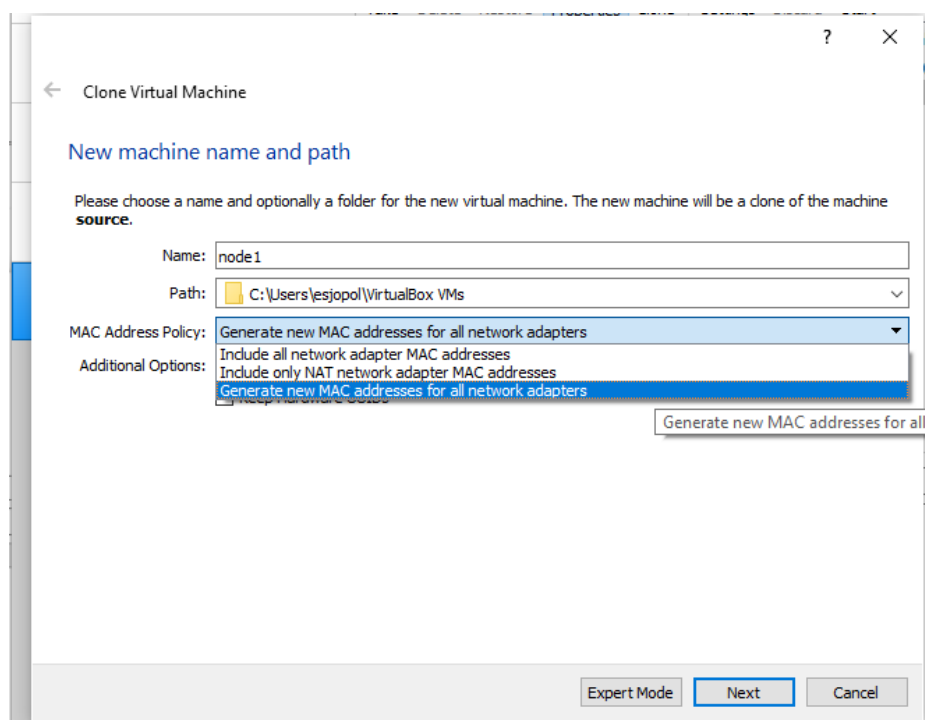
Figure 7. Select clone option

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	14 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



2. New machine name and path, as following:
 - *Name: **node1***
 - *Mac Address Policy: **Generate new MAC addresses for all network adapters***
 - *[Next]*

Figure 8. New machine configuration step 1



- We need to make sure that every adapter has a different MAC address.

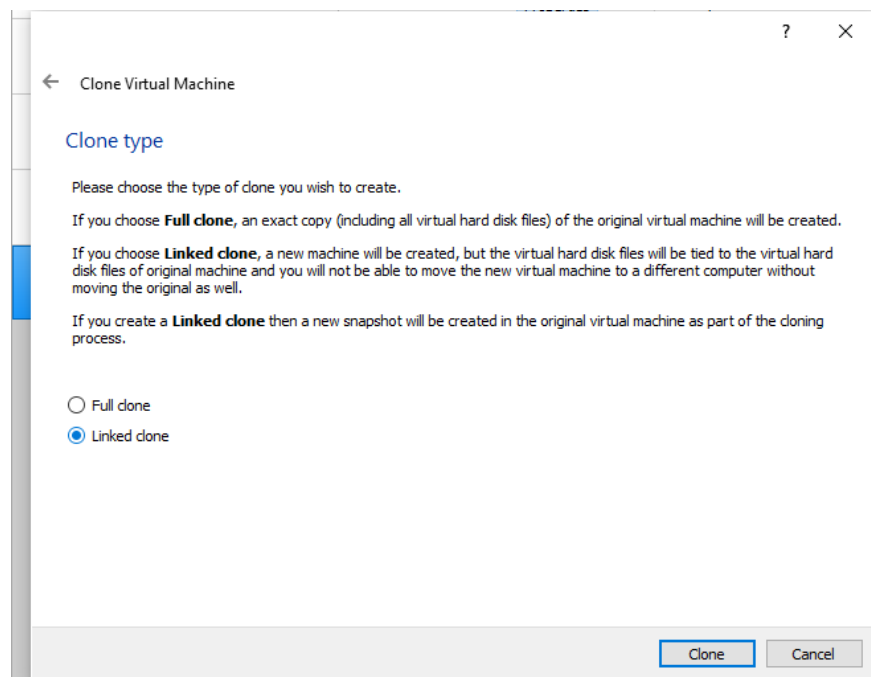
Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	15 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



3. Clone type

- Select **Linked clone** as the clone type. We are going to select a linked clone so that only the differences between the *base VM* and *cloned VMs* are saved to the hard disks. This saves us a lot of hard disk space on our host Machine.
- If you are confident about your setup, you can choose whichever clone type suits you. In this lab, a Linked clone is enough.

Figure 9. New machine configuration step 2



4. Configure network adapters on the cloned node

Right click on the **base** machine and select **settings...** option. Click on **Network** tab. Check adapters configuration.

- The newly cloned virtual machine is created with all the default settings from base VM.
- The network Adapters default settings are:
 - **Adapter 1:** NAT, used for connection to host and internet.
 - **Adapter 2:** internal network, used for connecting to other nodes. Initially configured to use internal network neta.
 - **Adapter 3:** internal network, used for connecting to other nodes. Initially configured to use internal network netb but with the cable disconnected.
 - **Adapter 4:** internal network, used for connecting to other nodes. Initially configured to use internal network netc but with the cable disconnected.
- You can change which adapters are connected or disconnected, depending on the type of network topology you are creating. For this Lab, Adapter 1 and Adapter 2 are connected.

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	16 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



5. Port Forwarding configuration for each cloned nodes

Right click on the **base** machine and select **settings...** option. Click on **Network** tab, on **Adapter 1**, expand the **Advanced** label, and click on **Port Forwarding**.

- The default **Host Port** is 2201, this port should be changed so that it is unique for each of the cloned nodes. For example:
 - On node1 use host port 2201
 - On node2 use host port 2202
 - On node3 use host port 2203
 - And so on...

- The Host Port can be any port number you want (excluding [reserved ports](#)), as long as it is unique among your nodes.

6. Repeat "Clone Virtual Machine (base)" steps 1 to 5 for any number of nodes you want to create.

- This Lab makes usage of node1 and node2. The number of nodes depends on your topology. So create nodes appropriately.

5.3 Configure each node

For each of the nodes we created, we need to change the host name and configure a different IP address.

1. Change host name

```
ericsson@base:~$ sudo sed -i 's/base/node1/' /etc/hostname
ericsson@base:~$ sudo sed -i 's/base/node1/' /etc/hosts
```

- Default host name is **base**, we replace it with VM node name, i.e. **node1** or **node2**, etc...
- So we change the host name in both **/etc/hostname** and **/etc/hosts** files.

2. Change internal network interface IP address

- We will change ip configuration in "vm-adapters-config.yaml"
- In this Lab, we will only change and confirm the ip address of **enp0s8** interface:
 - For node1, the default ip address **192.168.1.11** is okay.
 - For node2, we change the ip address to **192.168.1.12**.
 - In case there is a node3, the ip address should be changed to **192.168.1.13**.
- Again, you are free to use any ip address strategy. We keep it simple here by matching the last digit of the ip address same as the node number sequence (1, 2, 3, etc...)

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	17 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



```
ericsson@base:~$ cd /etc/netplan/
ericsson@base:/etc/netplan/$ sudo vi vm-adapters-config.yaml
ericsson@base: /etc/netplan/$ cat vm-adapters-config.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses:
        - 192.168.1.11/24
      gateway4: 192.168.1.1
      optional: true
#   enp0s9:
#     addresses:
#       - 192.168.2.21/24
#     gateway4: 192.168.2.1
#     optional: true
#   enp0s10:
#     addresses:
#       - 192.168.3.31/24
#     gateway4: 192.168.3.1
#     optional: true
```

- An example of node1 ip address configuration

```
ericsson@base:~$ sudo netplan apply
```

- [netplan configuration](#)
- Apply the network interface configuration

3. Power off all nodes and start VM in headless mode

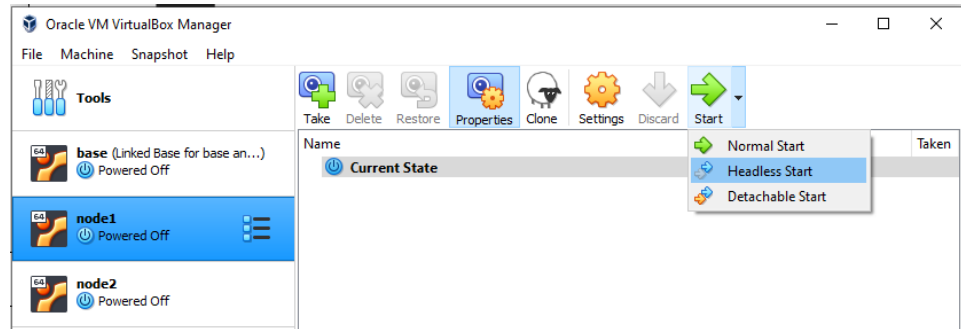
```
ericsson@base:~$ poweroff
```

- all nodes should be powered off

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	18 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



Figure 10. Start nodes in headless mode



- Start all nodes in headless mode

6 Using the virtual network

6.1 Cygwin

1. Connect to VM nodes via ssh using password

```
[~]$ ssh -p 2201 ericsson@127.0.0.1
The authenticity of host '[127.0.0.1]:2201 ([127.0.0.1]:2201)'
can't be established.
ECDSA key fingerprint is
SHA256:jtowm+hNeZAJ+ugYoyfWogBQ1pG/g1CNjB9c8QPMNq8.
Are you sure you want to continue connecting
(yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:2201' (ECDSA) to the
list of known hosts.
ericsson@127.0.0.1's password: ericsson
...
...
Last login: Wed Jun  9 02:19:47 2021 from ...
ericsson@node1:~$
```

- Example shows login to node1 via ssh on cygwin

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	19 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



```
ericsson@node1:~$ ssh ericsson@192.168.1.12
...
Last login: Wed Jun  9 07:07:56 2021 from 192.168.1.11
ericsson@node2:~$ ssh ericsson@192.168.1.12
```

- Example shows ssh login to node2 from node2

```
ericsson@node1:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 node1
192.168.1.12 node2
...
ericsson@node1:~$ ssh ericsson@node2
...
ericsson@node2:~$
```

- In case you do not want to use ip address every time

2. Connect to VM nodes via **ssh without password**

- In cygwin, confirm that ssh keys are available.

```
[~]$ ls -l ~/.ssh/
...
-rw----- 1 esjopol Domain Users 2610 May 25 13:17 id_rsa
-rw-r--r-- 1 esjopol Domain Users  573 May 25 13:17 id_rsa.pub
```

- Create new key in case there is no ssh keys. (Optional)

```
[~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/esjopol/.ssh/id_rsa):
ENTER
Enter passphrase (empty for no passphrase): ENTER
Enter same passphrase again: ENTER
Your identification has been saved in /home/esjopol/.ssh/id_rsa.
Your public key has been saved in /home/esjopol/.ssh/id_rsa.pub.
The key fingerprint is:
...
```

- Default is ok (press ENTER), no passphrase is needed (press ENTER twice)

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	20 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



c) Copy ssh keys to remove VM nodes

```
[~]$ ssh-copy-id -i ~/.ssh/id_rsa.pub -p 2201 ericsson@127.0.0.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/home/esjopol/.ssh/id_rsa.pub"
/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 prompted now it is to install the new keys
ericsson@127.0.0.1's password: ericsson
```

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p '2201' 'ericsson@127.0.0.1'"
and check to make sure that only the key(s) you wanted were added.

- Example of copying ssh public key to node1
- For node2, execute the same command with port number as **2202**
 - You can do this for any number of nodes, simply change the port number.

d) ssh to remote VM

```
[~]$ ssh -p 2201 ericsson@127.0.0.1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic
x86_64)
...
...
...
Last login: Wed Jun  9 02:19:47 2021 from ...
ericsson@node1:~$
```

- Example of ssh to remote node1 VM
 - No password prompt displayed!

3. Common errors section

- Host key verification failed!
 - Remove the cached key with the [127.0.0.1]:22xx ip address
 - The the host keys will be stored in the /home/<username>/.ssh/known_hosts file.

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	21 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



A) Check the cached keys in ~/.ssh/known_hosts file

```
[~]$ cat ~/.ssh/known_hosts
seroiuts00093. sero. gic. ericsson. se, 10. 210. 132. 54 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDBYgXY1Jg19qXNP3RVi5+...
[127. 0. 0. 1]:2201 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJR50R0EPVgw
oJ4HV3bjX0CIC7Zi9Ftp4C8yMwn5de36uZanwrSLe7DCzanYmj6XanaVoBVHoazv
sgdT/y8YvU=
[127. 0. 0. 1]:2202 ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJR50R0EPVgw
oJ4HV3bjX0CIC7Zi9Ftp4C8yMwn5de36uZanwrSLe7DCzanYmj6XanaVoBVHoazv
sgdT/y8YvU=
```

- This examples shows that 127.0.0.1 has caches for ports 2201 and 2202; Which correspond to node1 and node2 in our lab.
- B) Fix this error by removing the corresponding key, note that ip is 127.0.0.1 but the port number is different for each known host key.

```
[~]$ ssh-keygen -R [127.0.0.1]:2202
```

- Example shows how to remove cached key of node2 from known_hosts file
- You can remove any cached key for other ports that show errors when doing ssh.

6.2 PuTTY and PuTTYgen

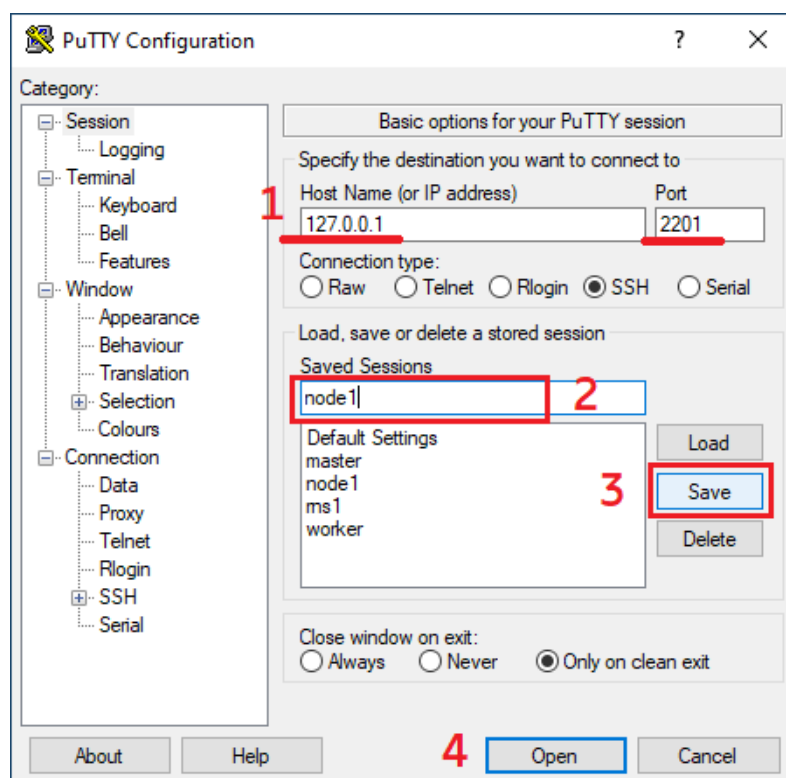
Use the following information whenever necessary for remote connection using PuTTY:

- Host name: **127.0.0.1**
- Port: **2201** (node1), **2202** (node2), etc... depending on the node you want to connect.
- Username: **ericsson**
- Password: **ericsson**

1. Connect to VM nodes via PuTTY using password

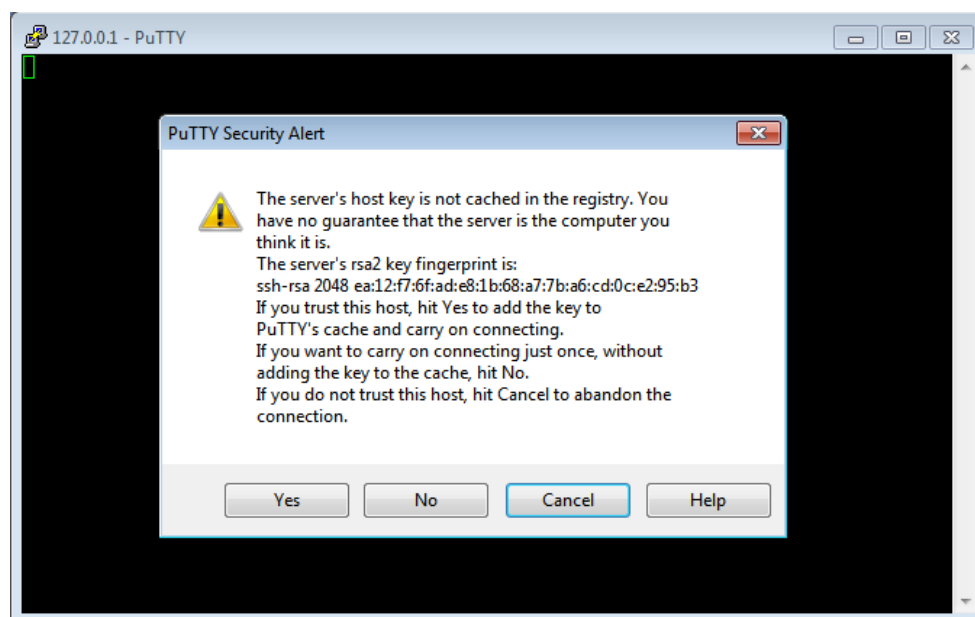
Figure 11. PuTTY configuration window

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	22 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



- Notice port is **2201**, referring to the port forwarding to **node1** VM.

Figure 12. PuTTY Security Alert

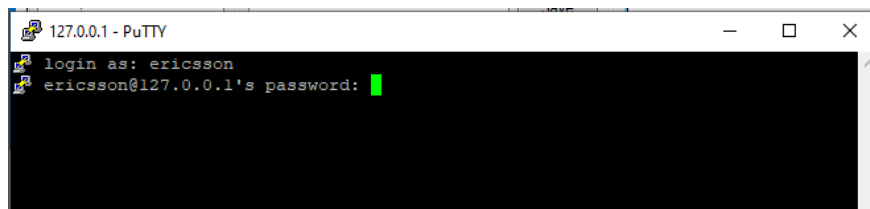


- Click **[Yes]** and ignore the security alert, connection is internal and chance of an attack is little.

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	23 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)		Checked
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



Figure 13. PuTTY remote login



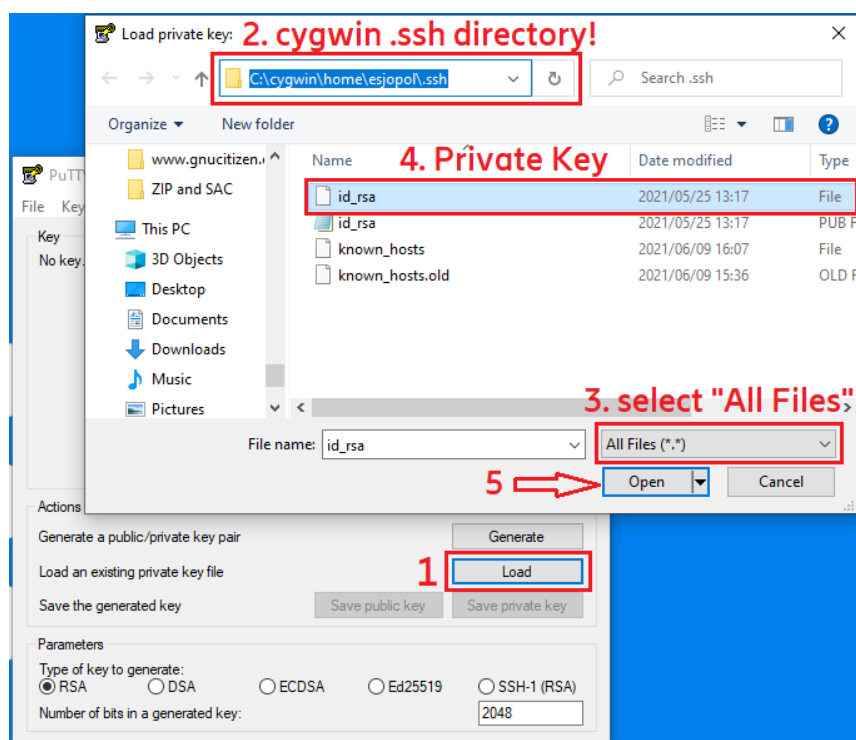
- login/password: ericsson/ericsson

2. Connect to VM nodes via PuTTY without password

a) Open PuTTYgen

- Load the Cygwin ssh private key file into PuTTYgen

Figure 14. PuTTYgen loading an existing private key file



- Click [OK] on the "Successfully imported foreign key" message.

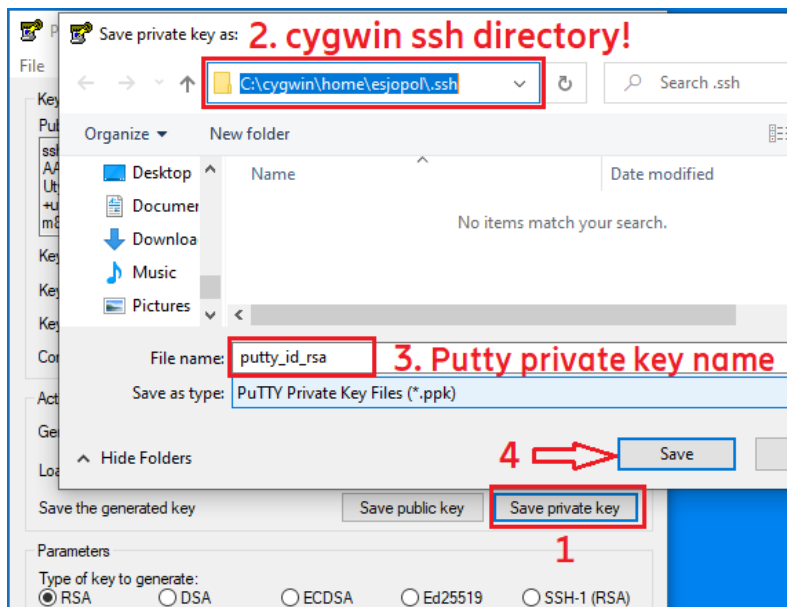
b) Save private key

- Click on [Save private key] button, then Click [Yes], Save as: *putty_id_rsa*, Close PuTTYgen.

Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	24 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	

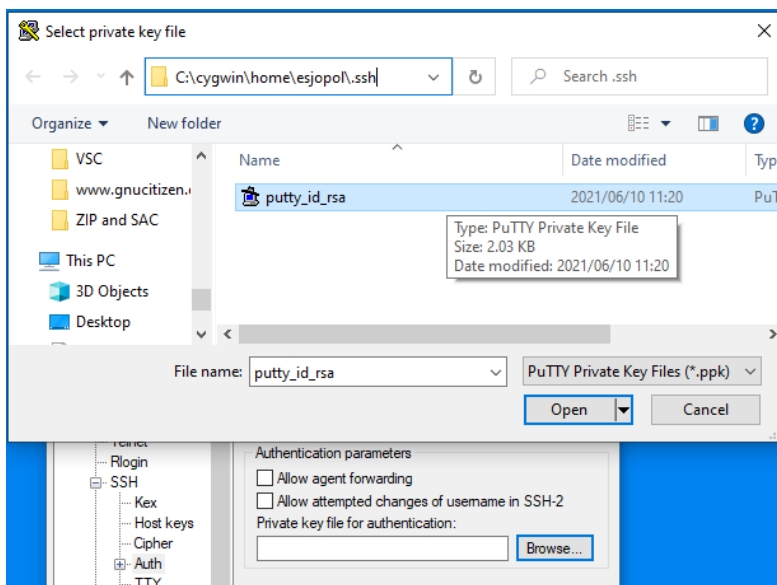


Figure 15. PuTTYgen Save private key



- c) Open PuTTY
- Under **Saved Sessions**, select and Load [node1]
 - On the left Sidebar, Click on Connection > SSH > Auth.
 - Click **Browse** the [Private key file for authentication] as shown in Figure.
 - Refer to previous step, putty private key is saved as **putty id rsa**

Figure 16. PuTTY Select private key file

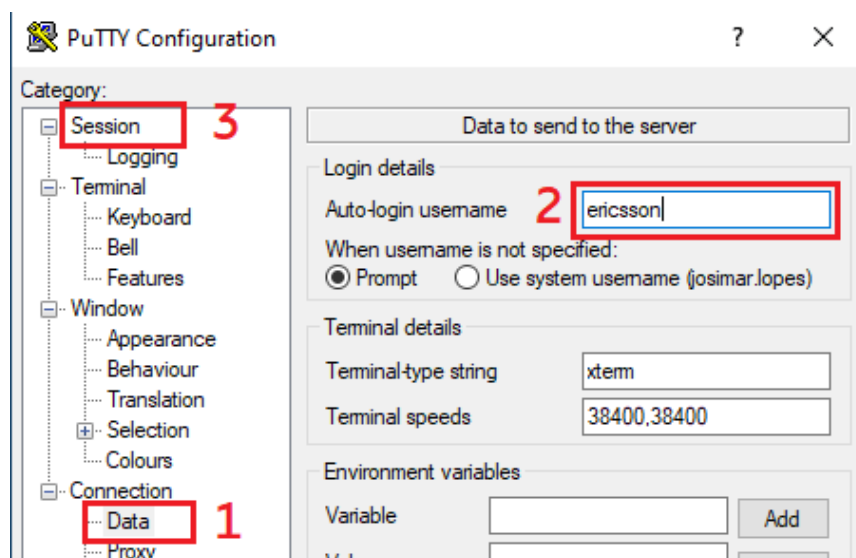


Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	25 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



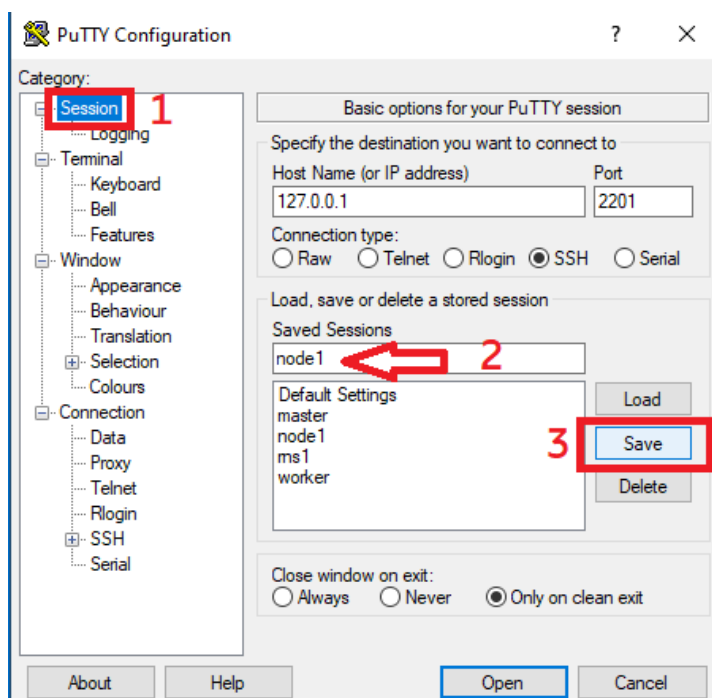
- Click on [Connection > Data], Under Auto-login username, type **ericsson**. Refer to Figure below:

Figure 17. PuTTY Auto-login username



- Click on [Session] and Under Sessions, Save updated *node1* configuration. As shown below:

Figure 18. PuTTY configuration [save] updated configuration

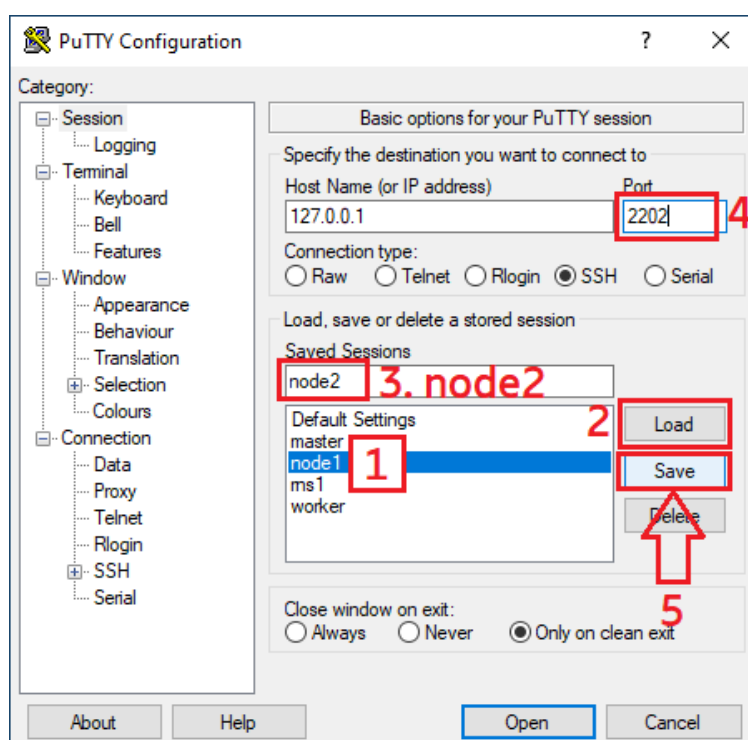


Confidentiality Class	External Confidentiality Label	Document Type	Page
Ericsson Internal		Manual	26 (26)
Prepared By (Subject Responsible)	Approved By (Document Responsible)	Checked	
ESJOPOL Josimar Lopes			
Document Number	Revision	Date	Reference
	A	2021-06-03	



- d) Click on **[Open]**
 - Notice that no username/password prompt is displayed
3. Add node2 session to PuTTY
 - Open PuTTY, in **Session**, then Under **Saved Sessions**, load **node1** session
 - Rename session name to **node2** and change port to **2202** and **Save node2** session.

Figure 19. PuTTY configuration [Save] new session



7 What's next?

- Configure node as a router
 - DHCP
 - Firewall
 - `/etc/sysctl.conf, #net.ipv4.ip_forward=1`
- Try different topology types
- Use VBoxManage command to automate VM node creation

8 References

- <https://netplan.io/>
- <http://releases.ubuntu.com/18.04/>
- <https://en.wikipedia.org/wiki/VirtualBox>