Network Administration 2

**Environment Setup**

The first steps to implementing the tasks is to download the virtual box and install on the computer.

The next step is to download and install vagrant.

1. Create the Project Directory on my computer.

I used my existing repo and created my directory from the existing location.

mkdir network-setup

cd network-setup

mkdir main-office branch-office client

1. Create Vagrantfile:

I created my Vagrantfile in my network-setup directory

A screenshot of a computer program

Description automatically generated

**Create Provision Scripts**

1. Create the main-office/provision.sh file

A computer screen shot of a black screen

Description automatically generated

1. Create the branch-office /provision.sh file

A screenshot of a computer program

Description automatically generated

1. Create the client /provision.sh file

A screenshot of a computer program

Description automatically generated

After creating the files, the next step is to bring up the Virtual machines

vagrant up

I got the message below indicating that one of the IPs is in use already so I have to modify my config files. However, the main-office VM was created already as I can see it in my Virtual box.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

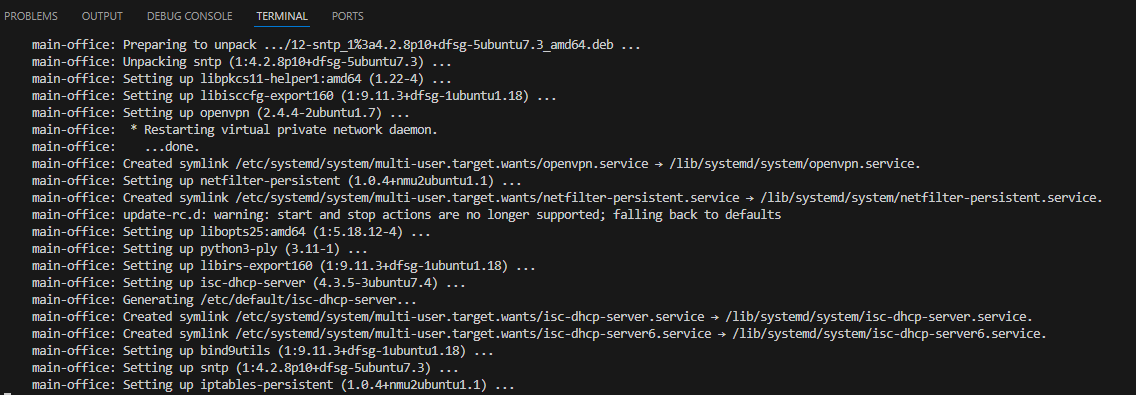
After modifying my vagrant file and the three provision files, I proceeded to run the “vagrant up” command.

The main virtual machine has been created and is running but other VMs have not been created yet and the process is taking to long.

A screenshot of a computer

Description automatically generated

Main office VM created



A screenshot of a computer

Description automatically generated

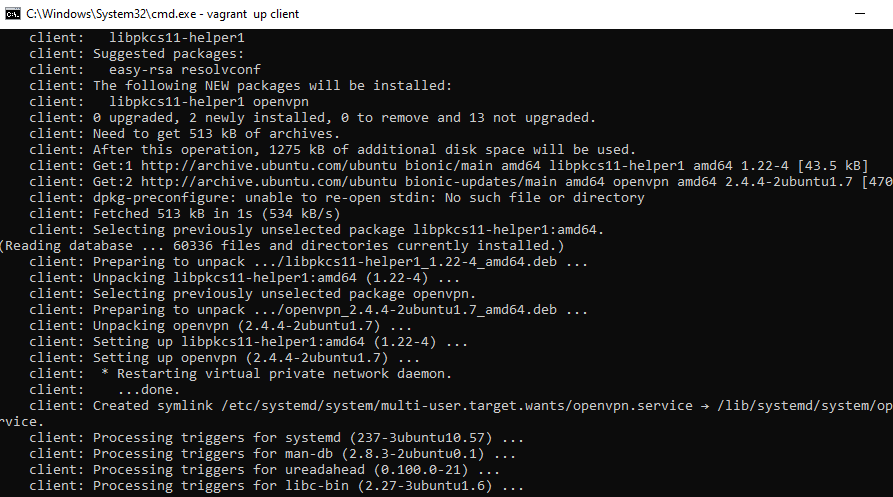
Branch office VM created

A computer screen with white text

Description automatically generated



Client VM created



A screenshot of a computer

Description automatically generated

The virtual box manager displays all virtual machines and a summary of their status

A screenshot of a computer

Description automatically generated

**Network Configuration:**

To login to the VMs from the virtual box manager we use the default vagrant credentials

 **Username:** vagrant

 **Password:** vagrant

A screenshot of a computer

Description automatically generated

However, I will SSH into the VMs

**Main Office Server:**

1. **Network Configuration File:**

vagrant ssh main-office

A screenshot of a computer

Description automatically generated

Next I will open the network config file

sudo nano /etc/netplan/01-netcfg.yaml

I will paste this into the file:

A screenshot of a computer

Description automatically generated

 **network:** - Defines the network configuration.

 **version: 2** - Specifies the version of the network configuration format.

 **ethernets:** - Indicates that you are configuring Ethernet interfaces.

 **enp0s3:** - Refers to the first network interface.

* **addresses:** - Specifies the IP addresses assigned to this interface.
* **gateway4:** - Sets the default gateway for IPv4 traffic.
* **nameservers:** - Lists the DNS servers to use for resolving domain names.

 **enp0s8:** - Refers to the second network interface.

* **addresses:** - Specifies the IP addresses for this interface.

I will then apply the config changes: sudo netplan apply

To verify the config I will run: ip a

A screenshot of a computer program

Description automatically generated

1. DNS Configuration (BIND9):

**Install BIND9:** sudo apt install bind9 bind9utils bind9-doc

A screenshot of a computer program

Description automatically generated

**Edit Configuration File::** sudo nano /etc/bind/named.conf.options

A screenshot of a computer

Description automatically generated

**Create Internal Zone:**

sudo nano /etc/bind/named.conf.local

A computer screen with white text

Description automatically generated

**Configure Zone File:**

A computer screen with a black background

Description automatically generated

**Verify Zone Data File: sudo nano /etc/bind/db.company.local**

A computer screen shot of a computer program

Description automatically generated

**The one displayed is a reverse file, so I will create my own**

**sudo nano /etc/bind/db.company.local**

A computer screen shot of white text

Description automatically generated

** SOA Record: Specifies the primary DNS server and administrative contact.**

** NS Record: Specifies the authoritative name server for the zone.**

** A Record: Maps the domain name to an IP address.**

**Then Restart BIND: sudo systemctl restart bind9**

**Verify DNS Resolution : nslookup internal.company.local**

A screen shot of a computer

Description automatically generated

**The SERVFAIL error indicates that the DNS server is failing to process the query. This can happen due to various issues in DNS configuration.**

To resolve, I verified my BIND Configuration : sudo nano named.conf.local

A screen shot of a computer code

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

Verify BIND Configuration: sudo nano /etc/bind/named.conf.local

A computer screen with a white tab

Description automatically generated

Ensure /etc/bind/named.conf.options is correctly configured. To confirm that the forwarders are there

Sudo nano /etc/bind/named.conf.options

Then we Verify DNS Resolution

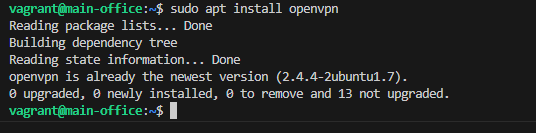
dig @localhost internal.company.local

A computer screen with white text

Description automatically generated

1. **VPN Server Configuration:**

Install Vpn: sudo apt install openvpn



1. **Routing Configuration:**

**Enable IP Forwarding: sudo nano /etc/sysctl.conf**

A screen shot of a computer

Description automatically generated

**Apply changes: sudo sysctl -p**

A screenshot of a computer

Description automatically generated

**Client VM Configuration**

The steps for connecting will be repeated for the client vm

A screenshot of a computer

Description automatically generated

Verify DHCP Lease: ip a

A computer screen with a black background

Description automatically generated

**Check DHCP Lease:** sudo dhclient -v enp0s8

A screenshot of a computer

Description automatically generated

**Verify DNS Resolution:** Check if DNS resolution is working correctly:

nslookup internal.company.local

nslookup google.com

A computer screen shot of a black screen

Description automatically generated

A computer screen with text on it

Description automatically generated

**Check NTP Synchronization: Verify if the time is synchronized with the NTP server:**

Timedatectl

A screenshot of a computer program

Description automatically generated

**Test Access to Resources:** **Ensure that you can access resources on the Main Office network.**

**ping 192.168.1.1**

A screenshot of a computer

Description automatically generated

**Branch Office Server:**

* 1. **Network Configuration File**

**sudo nano /etc/netplan/01-netcfg.yaml**

A screenshot of a computer

Description automatically generated

**Save the changes and apply the changes: sudo netplan apply**

* 1. **DHCP Configuration (isc-dhcp-server):**

**Configure the branch-office VM as a DHCP Server**

The branch-office VM is set up to act as a DHCP server for the BranchOfficeNet. I will install and configure a DHCP server on the branch-office VM.

sudo apt update

sudo apt install isc-dhcp-server

A computer screen with white text

Description automatically generated

A screen shot of a computer

Description automatically generated

The DHCP config file has been updated. Then we restart

* 1. DNS Configuration (BIND9):
* **Set Up as a Slave:**

sudo nano /etc/bind/named.conf.local

A computer screen with white text

Description automatically generated

1. NTP Configuration:

Install NTP and update the config:

sudo apt install ntp

sudo nano /etc/ntp.conf

A computer screen with white text

Description automatically generated

Allow NTP clients: sudo nano /etc/ntp.conf

Add: restrict 192.168.2.0 mask 255.255.255.0 nomodify notrap

A screen shot of a computer

Description automatically generated

1. VPN Client Configuration:

Install VPN Client: Openvpn

sudo apt install openvpn

Configure the VPN client

1. Firewall Configuration (iptables or nftables):

**Configure iptables:**

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT

sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT

sudo iptables -A INPUT -p udp --dport 1194 -j ACCEPT

sudo iptables -A INPUT -j DROP

Save iptables

sudo netfilter-persistent save

A screenshot of a computer screen

Description automatically generated

IDS/IPS Setup (Snort ): sudo apt install snort

I have updated the configuration files.

**Main Office**

To check DNS, DHCP, NTP, and VPN services

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

A computer screen with white text

Description automatically generated

Client

 **Install OpenVPN on the Client VM**:

sh

Copy code

sudo apt-get update

sudo apt-get install openvpn

 **Copy the Transferred Files to the OpenVPN Directory**:

sh

Copy code

sudo cp /home/vagrant/ca.crt /etc/openvpn/

sudo cp /home/vagrant/client1.crt /etc/openvpn/

sudo cp /home/vagrant/client1.key /etc/openvpn/

 **Create an OpenVPN Configuration File**: Create a configuration file for the client, for example, client1.conf:

sh

Copy code

sudo nano /etc/openvpn/client1.conf

Add the following configuration to client1.conf:

conf

Copy code

client

dev tun

proto udp

remote [YOUR\_SERVER\_IP] [PORT] # Replace with your server IP and port

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert client1.crt

key client1.key

remote-cert-tls server

comp-lzo

verb 3

 **Start the OpenVPN Client**:

sh

Copy code

sudo systemctl start openvpn@client1

 **Check the Status of the OpenVPN Client**:

sh

Copy code

sudo systemctl status openvpn@client1

systemctl status openvpn@client1

A computer screen shot of a program

Description automatically generated

A screen shot of a computer

Description automatically generated

Branch

A computer screen shot of a computer

Description automatically generated

A computer screen shot of a computer program

Description automatically generated

**Network Analysis and Troubleshooting**

* 1. Perform Network Scanning

**Install nmap** on both the Main Office and Branch Office servers if not already installed:

sudo apt-get update

sudo apt-get install nmap

Main VM:

A screen shot of a computer program

Description automatically generated

Branch VM

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

* 1. **Scan the Main Office network** from the Branch Office server to check for open ports and services:

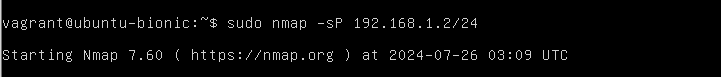
sudo nmap -sP 192.168.2.2/24

A computer screen shot of a computer

Description automatically generated

* 1. **Scan the Branch Office network** from the Main Office server:

sudo nmap -sP 192.168.1.2/24



A screenshot of a computer

Description automatically generated

**Capture and Analyze Network Traffic**

Install tcpdump on the Main and Branch VMs

sudo apt-get install tcpdump

**Main VM**

A screenshot of a computer

Description automatically generated

**Branch**

A black screen with white text

Description automatically generated

1. Capture traffic on the Main Office and Branch Office servers

sudo tcpdump -i eth0 -w main-office.pcap

sudo tcpdump -i eth0 -w branch-office.pcap

1. Analyze captured traffic using Wireshark:

 Transfer the .pcap files to a local machine where Wireshark is installed.

 Open the files in Wireshark to inspect network packets, verify VPN traffic, and troubleshoot any issues.

**Automation**

Develop Ansible Playbooks

DHCP Configuration

A screenshot of a computer

Description automatically generated

Dhcpd.conf

A computer screen shot of a computer program

Description automatically generated

DNS Configuration

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

NTP Configuration

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Firewall Configuration

A screenshot of a computer program

Description automatically generated

The playbooks can be run using the following commands:

ansible-playbook -i inventory dhcp.yml

ansible-playbook -i inventory dns.yml

ansible-playbook -i inventory ntp.yml

ansible-playbook -i inventory firewall.yml

A black background with white text

Description automatically generated

**Terraform to provision a cloud VM simulating an additional branch office**

A computer screen shot of a computer code

Description automatically generated**s**