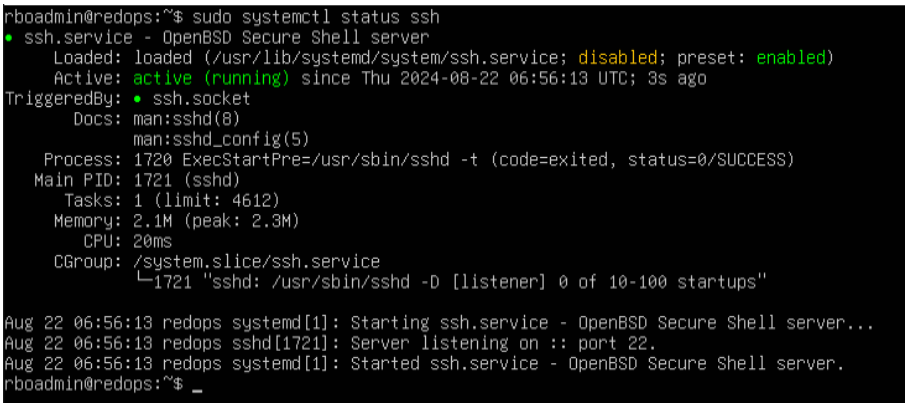
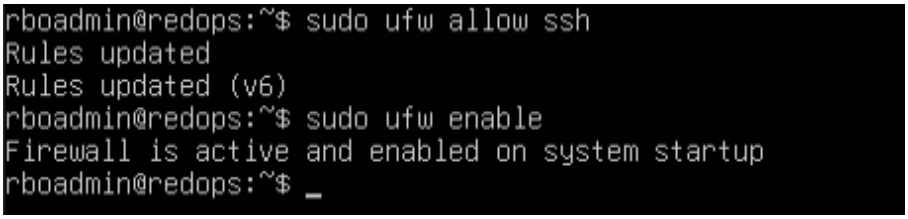
SSH Service (OpenSSH)

The OpenSSH package, responsible for the SSH service, was installed and configured. SSH (Secure Shell) is essential for secure remote access to the server, allowing administrators and users to connect, execute commands, and manage files over an encrypted connection.

- Commands Used:
    - sudo systemctl status ssh



    - sudo ufw allow ssh



Once installed, SSH allows secure remote access to the server for administrative tasks such as installing software, managing files, or configuring network services.

net-tools

The net-tools package was installed to provide the ifconfig command. ifconfig is an essential network management tool that displays the current state of network interfaces. It's used to view and manage the IP addresses, network configurations, and connection details of the server.

- Commands Used:
    - sudo apt install net-tools

```
rboadmin@redops:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python3-acme python3-certbot python3-configargparse python3-icu python3-josepy python3-parsedatetime python3-rfc3339
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 204 kB of archives.
After this operation, 811 kB of additional disk space will be used.
Get:1 http://au.archive.ubuntu.com/ubuntu noble/main amd64 net-tools amd64 2.10-0.1ubuntu4 [204 kB]
Fetched 204 kB in 0s (3,363 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 83999 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1ubuntu4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4) ...
Setting up net-tools (2.10-0.1ubuntu4) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
rboadmin@redops:~$
```

- ifconfig

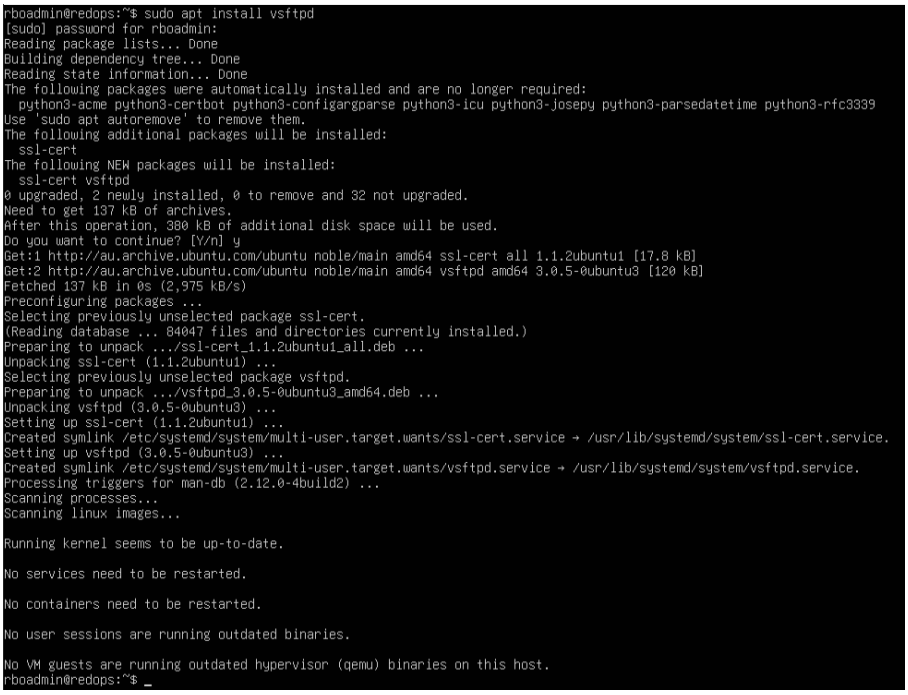
```
rboadmin@redops:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.68.108  netmask 255.255.255.0  broadcast 192.168.68.255
        inet6 fe80::a00:27ff:fecd:dba1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cd:db:a1  txqueuelen 1000  (Ethernet)
        RX packets 1731  bytes 155943 (155.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 283  bytes 17964 (17.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 84  bytes 6352 (6.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 6352 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

rboadmin@redops:~$
```

This tool is useful for configuring networking services on the server, especially when working with virtual machines, setting up network adapters, or troubleshooting network connections.

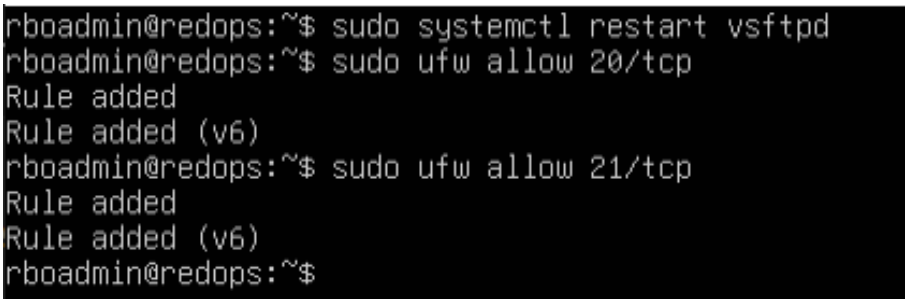
FTP Service (vsftpd)

The vsftpd package, which stands for "Very Secure FTP Daemon," was installed to provide FTP services on the server. FTP (File Transfer Protocol) allows users to upload and download files between the server and remote clients. The configuration steps also included setting up SSL certificates for secure FTP (FTPS), ensuring that file transfers are encrypted.

- Commands Used:
    - sudo apt install vsftpd



- sudo ufw allow 20/tcp && sudo ufw allow 21/tcp



Once installed, the vsftpd service provides secure, encrypted file transfer capabilities, which are essential for remote users who need to upload or download files to/from the server.

SSL Certificates

During the installation process, the ssl-cert package was installed to enable SSL for secure communications. SSL certificates are essential for encrypting sensitive data exchanged over the network, such as FTP credentials and file transfers.

- Commands Used:
    - sudo apt install ssl-cert

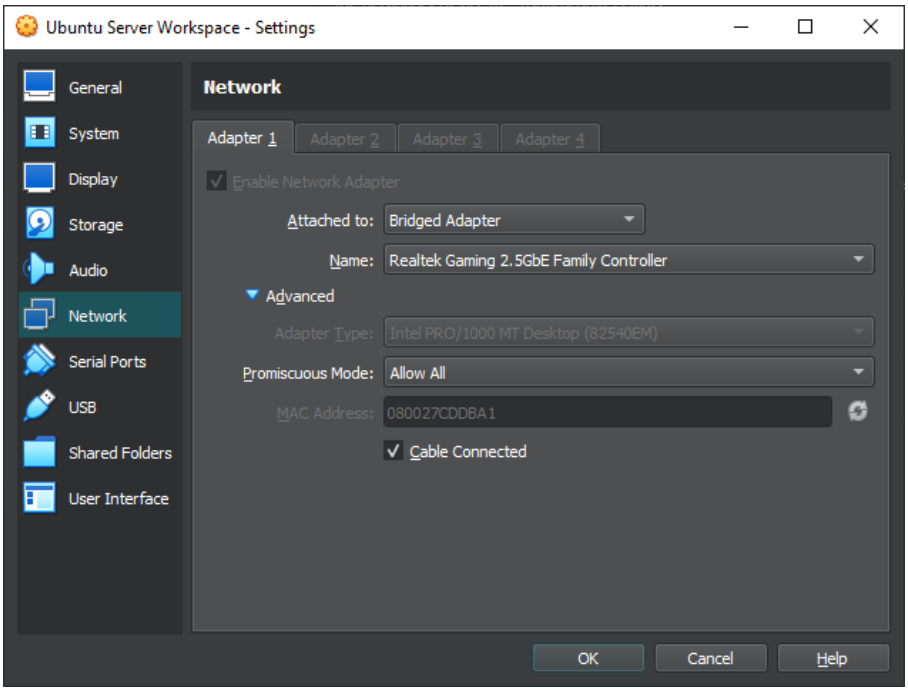
SSL/TLS certificates are crucial for ensuring that services like FTP or web servers can encrypt traffic between the server and remote clients, preventing eavesdropping or data tampering.

VirtualBox Network Configuration

Though not a software package, the VirtualBox network settings were adjusted for the Ubuntu Server Workspace. The network adapter was set to Bridged Mode, allowing the virtual machine to connect directly to the network and obtain an IP address like any other physical machine on

the same network. The Promiscuous Mode was also set to Allow All to enable packet capturing or network monitoring within the VM.

- Configuration Used:



This configuration is vital for setting up services that need external access, such as SSH or FTP, on a virtual machine.

Checking LDAP Ports with lsof

```
rboadmin@redops:~$ sudo lsof -i -P -n |grep slapd
slapd       957         openldap    8u  IPv4   6959      0t0  TCP *:389 (LISTEN)
slapd       957         openldap    9u  IPv6   6960      0t0  TCP *:389 (LISTEN)
```

- lsof: Lists open files and the processes that opened them. This tool is useful for seeing which processes are using which ports.
- -i: Displays network files (i.e., files that involve TCP/IP communication).
- -P: Shows the actual port numbers rather than trying to resolve service names.
- -n: Prevents lsof from attempting to resolve hostnames (keeps the output in numeric form).
- grep slapd: Filters the output to only show lines related to slapd, the LDAP daemon.

The output shows that slapd is listening on port 389, which is the default LDAP port for both IPv4 (TCP *:389) and IPv6 (TCP *:389). This indicates that the LDAP server is actively running and listening for connections over both IP versions.

Checking Open Ports with netstat

```
rboadmin@redops:~$ sudo netstat -tuln | grep :389
[sudo] password for rboadmin:
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
tcp6       0      0 :::389                  :::*                    LISTEN
```

- netstat: Displays network connections, routing tables, interface statistics, and open ports.
- -tuln: Options used:
    - -t: Show TCP connections.
    - -u: Show UDP connections.
    - -l: Show listening ports.
    - -n: Show numerical addresses rather than resolving names.
- grep :389: Filters the output to show only the lines involving port 389, which is the standard port for LDAP.

The output confirms that port 389 is open and listening for both IPv4 and IPv6 connections. This means that the LDAP service is actively awaiting incoming connections on the specified port, which is crucial for LDAP communication.

Summary

The installations and configurations performed play a pivotal role in making the Ubuntu Server functional, secure, and easily manageable from remote locations. Key services such as SSH allow for encrypted command-line access, while vsftpd enables secure file transfers, both critical for remote server management. The use of SSL certificates ensures encrypted communication for services like FTP, safeguarding sensitive data during transmission. The UFW firewall further enhances security by managing which services are exposed to the network, ensuring only authorized traffic can pass through.

Additionally, tools like net-tools and the VirtualBox network configuration provide essential network management and monitoring capabilities, ensuring the server's connectivity and performance are optimized. The configuration of slapd (LDAP server) to listen on port 389 for both IPv4 and IPv6 connections confirms that the LDAP service is running properly and ready to handle directory service tasks. Together, these installations and configurations establish a robust and secure environment, making the system ready for production use and remote management.