
Base Lab Configuration For CentOS 7

Michael Pare <michael.pare@mymail.champlain.edu¹> version 0.1, 2020-04-12

1. Introduction

Terminology

A Records.
AAAA Records.
Active Directory (AD).
CNAME Records.
Domain Controller (DC).
Domain Name System (DNS).
Dynamic Host Configuration Protocol (DHCP).
Firewalld.
Google Public DNS.
GNU's Not Linux (GNU).
GNU nano.
IP Forwarding.
iptables.
Network Address Translation (NAT).
Network Interface Controller (NIC).
Network Manager (nmtui).
NS Records.
PTR Records.
Samba.
Xfce Desktop Environment.

1.1. Disclaimer

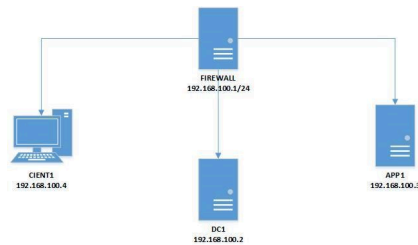
This website contains work created for informational purposes. Information may be out of date or changed or updated without notice. By using this website, you

¹ <mailto:michael.pare@mymail.champlain.edu>

recognize and agree that all information is provided “AS IS” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

The entire risk arising out of the use of these guides remains with you. IN NO EVENT SHALL CHAMPLAIN COLLEGE, ITS STUDENTS, FACULTY, OR ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE GUIDES BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES FOR ANY USE OF THE MATERIAL ON THIS WEBSITE. This includes, without limitation, damages for lost profits, business interruption, loss of data or business information, damage to computer equipment or networks, or other loss arising out of the use of any information in the guides

2. Network Design



Firewall

IP Address: 192.168.100.1/24

Hostname: firewall.college.com

The Firewall's purpose is to handle traffic between the Intranet and Internet. This means that it will act as a router directing traffic. There are two interfaces on Firewall, one is the external/Internet-facing called ens192 and the other is the internal/Intranet-facing called ens224.

DC1

IP Address: 192.168.100.2

Gateway: 192.168.100.1

DNS Server: 127.0.0.1

Hostname: dc1.college.com

This will be configured as the Intranet's Domain Name System (DNS) and the Dynamic Host Configuration Protocol (DHCP) server.

App1

IP Address: 192.168.100.3

Gateway: 192.168.100.1

DNS Server: 192.168.100.2

Hostname: app1.college.com

This is an internal web and application server.

Client1 IP Address: Dynamic

DNS Server: 192.168.100.2

Hostname: client1.college.com

Client1 is a workstation that has the ability to switch between the Intranet and Internet subnet.

3. I. Configure Firewall

The below instructions detail the installation and setup of Firewall. The last section, Troubleshooting, has some information on common problems that people come across.

3.1. Install the Operating System on Firewall

1. Start CentOS7 Firewall.
2. Hit Enter to select "Install CentOS 7."

3. On the “Welcome to CentOS Linux 7” page, select the appropriate language and region.
4. On “Installation Summary,” under “System,” select “Installation Destination.”
 - a. Check and click that the VMware Virtual disk has been selected. It will highlight in blue.
 - b. Click “Done” in the top left-hand corner to move back to the “Installation Summary” page.
5. To continue, click “Begin Installation.”
6. In “Configuration,” set the appropriate Root Password.
 - a. Recommended Root Password: Ch@mplain!18
7. On the same “Configuration” screen, Create a User.
 - a. Recommended Full Name: Champlain
 - b. Recommended User Name: champlain
 - c. Check box “Make this user administrator”
 - d. Recommended Password: S3cur1ty!18
8. Once installation is complete, click “Reboot.”
9. Logon to the credentials you just created.
 - a. User: root
 - Password: Ch@mplain!18
 - b. User: champlain
 - Password: S3cur1ty!18

3.2. Configure TCP/IP

1. Ensure that Network Manager is running. Type `systemctl status NetworkManager`.
 - a. You should see “Active: active (running)” in green if it is running.

- b. If it is not running, enter the command `sudo systemctl start NetworkManager.service`.
 - c. If the service fails to launch, check the logs by entering the command `sudo systemctl status NetworkManager.service -l`.
2. This is for the Internet-facing interface. Enter the command `nmtui` to enter the Network Manager.
 - a. Select "Edit a connection."
 - b. Select the Internet-facing interface, `ens192`, and use the arrow keys to select "<Edit...>"
 - c. Use the arrow keys to ensure that "IPv4 CONFIGURATION" is set to "<Automatic>"
 - d. At the very bottom, ensure that the brackets in front of "Automatically connect" have an X by hitting the spacebar while highlighting them.
 - e. Use the arrow keys to select "<OK>" then "<Back>" and press Enter to go back to the main menu of Network Manager.
 - f. Use the arrow keys to select "Quit" and press Enter to exit the editor.
3. Now, repeat for Intranet-facing interface.
 - a. Select "Edit a connection."
 - b. Select the Intranet-facing interface, `ens224`, and use the arrow keys to select "<Edit...>"
 - c. Use the arrow keys to ensure that "IPv4 CONFIGURATION" is set to "<Manual>"
 - d. Under "Addresses" add in "`192.168.100.1/24`"
 - e. At the very bottom, ensure that the brackets in front of "Automatically connect" have an X by hitting the spacebar while highlighting them.
 - f. Use the arrow keys to select "<OK>" then "<Back>" and press Enter to go back to the main menu of Network Manager.
 - g. Use the arrow keys to select "Quit" and press Enter to exit the editor.
4. Change the hostname. To change the hostname to `firewall.college.com` use the following command: `sudo hostnamectl set-hostname firewall.college.com`.

5. Restart the network using `sudo systemctl restart network`.

3.3. Install and Use of Nano

1. Run the command `sudo yum install nano -y`.

3.4. Configure NAT Rules

This will allow the system to act as a router and to allow traffic from the internal network out to the external network.

1. Enable IP forwarding by entering the command `sudo echo "net.ipv4.ip_forward = 1" >> /etc/sysctl.d/ip_forward.conf`.
 - a. You will need to be root to perform this task.
 - b. Switch back to champlain user afterwards using `su champlain`.
2. Add the external-facing NIC to FirewallD's "public" zone by typing: `sudo firewall-cmd --zone=public --add-interface=ens192 --permanent`
 - a. Where `ens192` is the name of the external interface
3. Add the internal-facing NIC to FirewallD's "internal" zone by typing: `sudo firewall-cmd --zone=internal --add-interface=ens224 --permanent`
 - a. Where "ens224" is the name of the internal interface
4. Apply masquerading to the external FirewallD zone by typing: `sudo firewall-cmd --zone=public --add-masquerade --permanent`
5. Save those changes by typing: `sudo firewall-cmd --complete-reload`
6. Enable NAT by entering the command `sudo firewall-cmd --permanent --direct --passthrough ipv4 -t nat -l POSTROUTING -o ens224 -j MASQUERADE -s 192.168.100.0/24`.
7. Restart the firewall to save using `sudo firewall-cmd --reload`.
8. Configure NAT rules on iptables. Enter the following commands. `sudo iptables -F` `sudo iptables -P INPUT ACCEPT` `sudo iptables -P OUTPUT ACCEPT`

9. Ensure NAT rules on iptables remains on boot. Add in the commands from earlier for NAT by entering the command `sudo nano /etc/rc.local`. This will open the file in Nano Editor.

a. Add in the following at the end:

```
# NAT Rules
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
```



```
GNU nano 2.3.1 File: /etc/rc.local
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.
touch /var/lock/subsys/local
#
# NAT Rules
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT_
```

- a. The above ensures that the NAT rules are still in place on reboot.
- b. Press Ctrl+X to exit the Nano Editor then hit Y to save the file and hit Enter to save it with the same name.

Congratulations, Firewall is now configured.

4. II. Configure DC1

The below instructions detail the installation and setup of DC1. The last section, Troubleshooting, has some information on common problems that people come across.

4.1. Install the Operating System on DC1

1. Start CentOS7 DC1.
2. Hit Enter to select “Install CentOS 7.”
3. On the “Welcome to CentOS Linux 7” page, select the appropriate language and region.
4. On “Installation Summary,” under “System,” select “Installation Destination.”

- a. Check and click that the VMware Virtual disk has been selected. It will highlight in blue.
 - b. Click “Done” in the top left-hand corner to move back to the “Installation Summary” page.
5. To continue, click “Begin Installation.”
6. In “Configuration,” set the appropriate Root Password.
 - a. Recommended Root Password: Ch@mplain!18
7. On the same “Configuration” screen, Create a User.
 - a. Recommended Full Name: Champlain
 - b. Recommended User Name: champlain
 - c. Check box “Make this user administrator”
 - d. Recommended Password: S3cur1ty!18
8. Once installation is complete, click “Reboot.”
9. Logon to the credentials you just created.
 - a. User: root
 - Password: Ch@mplain!18
 - b. User: champlain
 - Password: S3cur1ty!18

4.2. Configure TCP/IP on DC1

1. Ensure that Network Manager is running. Type `systemctl status NetworkManager`.
 - a. You should see “Active: active (running)” in green if it is running.
 - b. If it is not running, enter the command `sudo systemctl start NetworkManager.service`.
 - c. If the service fails to launch, check the logs by entering the command `sudo systemctl status NetworkManager.service -l`.

2. Enter the command `nmtui` to enter the Network Manager.
 - a. Select “Edit a connection.”
 - b. Select `ens192`, and use the arrow keys to select “<Edit...>”
 - c. Use the arrow keys to ensure that “IPv4 CONFIGURATION” is set to “<Manual>”
 - d. Under “Addresses” add in `192.168.100.2/24`.
 - e. Under “Gateway” add in the address of the router: `192.168.100.1`.
 - f. Under “DNS servers” add in the address of Google: `8.8.8.8`.
 - g. This is a temporary setting to ensure Internet connectivity while downloading the required packages to configure DNS and DHCP.
 - h. At the very bottom, ensure that the brackets in front of “Automatically connect” have an X by hitting the spacebar while highlighting them.
 - i. Use the arrow keys to select “<OK>” then “<Back>” and press Enter to go back to the main menu of Network Manager.
 - j. Use the arrow keys to select “Quit” and press Enter to exit the editor.
3. Change the hostname. To change the hostname to `dc1.college.com` use the following command: `sudo hostnamectl set-hostname dc1.college.com`.
4. Restart the network using `sudo systemctl restart network`.

4.3. Install and Use of Nano

1. Run the command `sudo yum install nano -y`.

4.4. Configure DC1 as DNS Server

1. Install DNS using the command `sudo yum install bind bind-utils -y`.
2. Configure bind by editing `named.conf`. Use the command `sudo nano /etc/named.conf` to do so. Make the following edits.
 - a. Edit this line to look like by adding in the IP address of the DNS server:

```
listen-on port 53 ( 127.0.0.1; 192.168.100.2; );
```
 - b. Comment out “listen-on-v6 port 53 { ::1; };” by adding a pound (#) sign:

```
# listen-on-v6 port 53 ( :::1 );
```

- c. Edit “allow-query” to add in the subnet to look like:

```
allow-query { localhost; 192.168.100.0/24; };
```

- d. Add in a section for “forwarders”:

```
forwarders {
    8.8.8.8;
    8.8.4.4;
};
```

- e. At the end add in “include “/etc/named/named.conf.local”;

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/named.conf.local";
```

3. Create and edit named.conf.local. Edit using: `sudo nano /etc/named/named.conf.local`. Fill in this new, blank file with the following information.

```
GNU nano 2.3.1 File: /etc/named/named.conf.local

zone "college.com" {
    type master;
    file "/etc/named/zones/db.college.com";
};

zone "100.168.192.in-addr.arpa" {
    type master;
    file "/etc/named/zones/db.100.168.192";
};
```

4. Now, you will need to create the two files referenced in “/etc/named/named.conf.local”

First, create the forwarder configuration.

- a. Make the zones directory in /etc/named, `sudo mkdir /etc/named/zones`.
- b. Create a file using `sudo nano /etc/named/zones/db.college.com`. In the end, it should look like the below screenshot.

```
GNU nano 2.3.1 File: /etc/named/zones/db.college.com

$TTL      604800
@         IN      SOA     dc1.college.com. champlain.college.com. (
                                2017030302; serial
                                604800 ; refresh
                                86400  ; retry
                                2419200 ; expire
                                604800 ); minimum

@         IN      NS      dc1.college.com.
@         IN      A       127.0.0.1
@         IN      AAAA    ::1

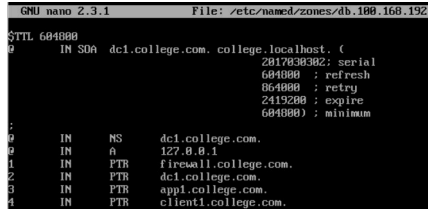
; Below are A Record Addresses

firewall  IN      A       192.168.100.1
dc1        IN      A       192.168.100.2
app1       IN      A       192.168.100.3
client1    IN      A       192.168.100.4

; Below are CNAME Record Addresses (aliases)
server1    IN      CNAME   dc1.college.com.
server2    IN      CNAME   app1.college.com.
```

5. Next, setup the reverse zone configuration file.

- a. Create a file using `sudo nano /etc/named/zones/db.100.168.192`. In the end, it should like the below screenshot.



```
GNU nano 2.3.1 File: /etc/named/zones/db.100.168.192
$TTL 604800
@ IN SOA dc1.college.com. college.localhost. (
                                2017030302 : serial
                                604800 : refresh
                                86400 : retry
                                2419200 : expire
                                604800) : minimum
;
;
@ IN NS dc1.college.com.
@ IN A 127.0.0.1
1 IN PTR firewall.college.com.
2 IN PTR dc1.college.com.
3 IN PTR appl.college.com.
4 IN PTR client1.college.com.
```

6. Start the DNS server.

- a. Enable the DNS server: `sudo systemctl enable named`
- b. Start the DNS server: `sudo systemctl start named`

7. Allow port 53 for DNS queries.

- a. Allow port 53/tcp and 53/udp through on the firewall: `sudo firewall-cmd --permanent --add-port={53/tcp,53/udp}`
- b. Reload the firewall: `sudo firewall-cmd --reload`

4.5. Reconfigure TCP/IP on DC1

1. Enter the command `nmtui` to enter the Network Manager.

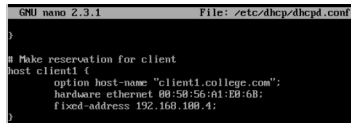
- a. Select “Edit a connection.”
- b. Select `ens192`, and use the arrow keys to select “<Edit...>”
- c. Under “DNS servers” remove `8.8.8.8` and add in the address: `127.0.0.1`
- d. Use the arrow keys to select “<OK>” then “<Back>” and press Enter to go back to the main menu of Network Manager.
- e. Use the arrow keys to select “Quit” and press Enter to exit the editor.

2. Restart the network: `sudo systemctl restart network`

4.6. Configure DHCP on DC1

1. Install DHCP: `sudo yum install dhcp -y`
2. Open the DHCP configuration file: `sudo nano /etc/dhcp/dhcpd.conf`

3. Edit the configuration file to look like the following:
 - a. Make sure to change the hardware ethernet address to your Client1's address .



```
GNU nano 2.3.1 File: /etc/dhcp/dhcpd.conf
}
# Make reservation for client
host client1 {
    option host-name "client1.college.com";
    hardware ethernet 08:50:56:a1:E8:68;
    fixed-address 192.168.108.4;
}
```

4. Start the DHCP server: `sudo systemctl start dhcpd`
5. Enable the DHCP server: `sudo systemctl enable dhcpd`

Congratulations, DC1 is now configured.

5. III. Configure App1

The below instructions detail the installation and setup of App1. The last section, Troubleshooting, has some information on common problems that people come across.

5.1. Install the Operating System on App1

1. Start CentOS7 App1.
2. Hit Enter to select "Install CentOS 7."
3. On the "Welcome to CentOS Linux 7" page, select the appropriate language and region.
4. On "Installation Summary," under "System," select "Installation Destination."
 - a. Check and click that the VMware Virtual disk has been selected. It will highlight in blue.
 - b. Click "Done" in the top left-hand corner to move back to the "Installation Summary" page.
5. To continue, click "Begin Installation."
6. In "Configuration," set the appropriate Root Password.

- a. Recommended Root Password: Ch@mplain!18
7. On the same “Configuration” screen, Create a User.
 - a. Recommended Full Name: Champlain
 - b. Recommended User Name: champlain
 - c. Check box “Make this user administrator”
 - d. Recommended Password: S3cur1ty!18
8. Once installation is complete, click “Reboot.”
9. Logon to the credentials you just created.
 - a. User: root
 - Password: Ch@mplain!18
 - b. User: champlain
 - Password: S3cur1ty!18

5.2. Configure TCP/IP on App1

1. Ensure that Network Manager is running. Type `systemctl status NetworkManager`.
 - a. You should see “Active: active (running)” in green if it is running.
 - b. If it is not running, enter the command `sudo systemctl start NetworkManager.service`.
 - c. If the service fails to launch, check the logs by entering the command `sudo systemctl status NetworkManager.service -l`.
2. Enter the command `nmtui` to enter the Network Manager.
 - a. Select “Edit a connection.”
 - b. Select `ens192`, and use the arrow keys to select “<Edit...>”
 - c. Use the arrow keys to ensure that “IPv4 CONFIGURATION” is set to “<Manual>”
 - d. Under “Addresses” add in `192.168.100.3/24`.

- e. Under “Gateway” add in the address of the router: 192.168.100.1.
 - f. Under “DNS servers” add in the address of the DNS Server: 192.168.100.2
 - g. At the very bottom, ensure that the brackets in front of “Automatically connect” have an X by hitting the spacebar while highlighting them.
 - h. Use the arrow keys to select “<OK>” then “<Back>” and press Enter to go back to the main menu of Network Manager.
 - i. Use the arrow keys to select “Quit” and press Enter to exit the editor.
 - j. Change the hostname. To change the hostname to app1.college.com use the following command: `sudo hostnamectl set-hostname app1.college.com`.
3. Restart the network using `sudo systemctl restart network`.

5.3. Install and Use of Nano

1. Run the command `sudo yum install nano -y`.

5.4. Install Web Server Role on App1

1. Install Apache: `sudo yum install httpd -y`
2. Enable Apache: `sudo systemctl enable httpd`
3. Start Apache: `sudo systemctl start httpd`
4. Allow Apache through the firewall: `sudo firewall-cmd --permanent --add-service=http`
5. Reload the firewall: `sudo firewall-cmd --reload`

5.5. Configure File Sharing on App1

1. Install Samba: `sudo yum install samba samba-client samba-common -y`
2. Create a backup of the default Samba configuration: `sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak`
3. Create a new Samba configuration file: `sudo nano /etc/samba/smb.conf`
4. Edit it to look like the following:



```
GNU nano 2.3.1 File: /etc/samba/smb.conf
[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = appl
security = user
map to guest = bad user
dns proxy = no
hosts allow = 192.168.100.0/24

[allaccess]
path = /samba/allaccess
browsable = yes
writable = yes
guest ok = yes
read only = no
```

5. Create the actual share: `sudo mkdir -p /samba/allaccess`
6. Allow Samba through the firewall: `sudo firewall-cmd --permanent --add-service=samba`
7. Reload the firewall: `sudo firewall-cmd --reload`
8. Move into Samba's directory: `cd /samba`
9. Change the permissions: `sudo chmod -R 0755 allaccess/`
10. Change the permissions: `sudo chown -R nobody:nobody allaccess/`
11. Configure SELinux to allow access to the Samba directory: `sudo chcon -t samba_share_t allaccess/`
12. Enable SMB and NMB: `sudo systemctl enable smb` and `sudo systemctl enable nmb`
13. Start SMB and NMB: `sudo systemctl start smb` and `sudo systemctl start nmb`
14. This finishes the creation of the Samba share that is accessible to all users on the LAN.
15. Set the specific SELinux Boolean values that you will need to install another package containing some utilities: `sudo yum install policycoreutils-python -y`
16. Create a group for users who will be allowed access to the share: `sudo groupadd samby`
17. Create some users: `sudo useradd user1` and `sudo useradd user2`
18. Add new users to the new group: `sudo usermod -a -G samby user1` and `sudo usermod -a -G samby user2`
19. Create passwords for the new users: `sudo smbpasswd -a user1` and `sudo smbpasswd -a user2`

20 May be beneficial to use the same password: Pr1vacy!

21 Make the directory that will be used for the share: `cd /` and `sudo mkdir /samby`

22 Modify the permissions of the /samby share: `sudo chmod 0770 /samby` and `sudo chgrp samby /samby`

23 Edit the SELinux settings for the /Samby share:

- `sudo setsebool -P samba_export_all_ro=1 samba_export_all_rw=1`
- `getsebool -a | grep samba_export`
- `sudo semanage fcontext -at samba_share_t '/samby(/.*)?'`
- `sudo restorecon /samby`

24 Edit the smb.conf file: `sudo nano /etc/samba/smb.conf`

25 Keep everything in there and add the following section to the smb.conf; that section should look like:

26 Restart the SMB services: `sudo systemctl restart nmb` and `sudo systemctl restart smb`

Congratulations, App1 is now configured.

6. IV. Configure Client1

The below instructions detail the installation and setup of the Client. The last section, Troubleshooting, has some information on common problems that people come across.

6.1. Install the Operating System on Client1

1. Start CentOS7 Client1.
2. Hit Enter to select "Install CentOS 7."
3. On the "Welcome to CentOS Linux 7" page, select the appropriate language and region.
4. On "Installation Summary," under "System," select "Installation Destination."
 - a. Check and click that the VMware Virtual disk has been selected. It will highlight in blue.

- b. Click “Done” in the top left-hand corner to move back to the “Installation Summary” page.
5. To continue, click “Begin Installation.”
6. In “Configuration,” set the appropriate Root Password.
 - a. Recommended Root Password: Ch@mplain!18
7. On the same “Configuration” screen, Create a User.
 - a. Recommended Full Name: Champlain
 - b. Recommended User Name: champlain
 - c. Check box “Make this user administrator”
 - d. Recommended Password: S3cur1ty!18
8. Once installation is complete, click “Reboot.”
9. Logon to the credentials you just created.
 - a. User: root
 - Password: Ch@mplain!18
 - b. User: champlain
 - Password: S3cur1ty!18

6.2. Configure TCP/IP on Client1

1. Ensure that Network Manager is running. Type `systemctl status NetworkManager`.
 - a. You should see “Active: active (running)” in green if it is running.
 - b. If it is not running, enter the command `sudo systemctl start NetworkManager.service`.
 - c. If the service fails to launch, check the logs by entering the command `sudo systemctl status NetworkManager.service -l`.
2. Enter the command `nmtui` to enter the Network Manager.

- a. Select “Edit a connection.”
 - b. Select ens192, and use the arrow keys to select “<Edit...>”
 - c. Under “DNS servers” add in the address of the DNS Server: 192.168.100.2
 - d. At the very bottom, ensure that the brackets in front of “Automatically connect” have an X by hitting the spacebar while highlighting them.
 - e. Use the arrow keys to select “<OK>” then “<Back>” and press Enter to go back to the main menu of Network Manager.
 - f. Use the arrow keys to select “Quit” and press Enter to exit the editor.
3. Change the hostname. To change the hostname to dc1.college.com use the following command: `sudo hostnamectl set-hostname client1.college.com`.
 4. Restart the network using `sudo systemctl restart network`.

6.3. Install GUI

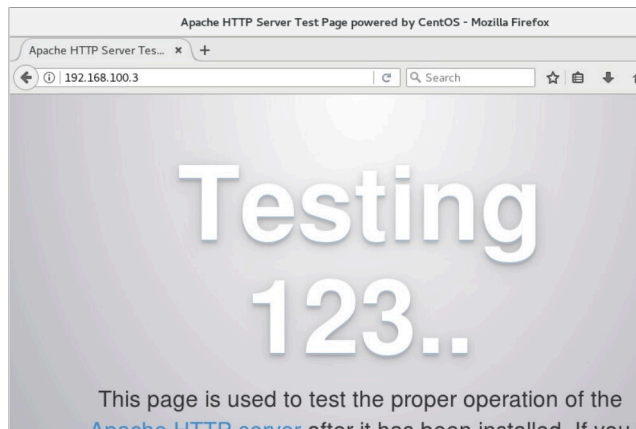
1. Install epel-release: `sudo yum install epel-release -y`
2. Install groupinstall: `sudo yum groupinstall "Server with GUI" -y`
 - a. This will be very time-intensive.
3. Install XFCE: `sudo yum groupinstall "XFCE" -y`
4. Tell the machine to boot to the GUI by default: `sudo systemctl set-default graphical.target`
5. Reboot the machine: `sudo reboot`
6. When the machine is rebooted, you may be taken to a screen that looks similar to the initial install screen.
 - a. Click “License Information”
 - b. Click the box next to “I accept the license agreement” and then click “Done”
 - c. Click “Finish Configuration”, which will take you to the login screen of the GUI
7. Login.
8. Click the gear icon and select “Xfce Session”
 - a. Enter your password and click “Sign In”

- b. When you first login, you will get a pop-up for the first start of the panel.
Click “Use default config”

6.4. Test Access to Resources on BUSNET Subnet

1. Test Access to the Web Server

- a. Under Applications, open Firefox Web Browser.
- b. Enter the IP address of App1 (192.168.100.3) into the URL bar.
- c. If it is configured correctly, you should see the Apache test page, shown below.

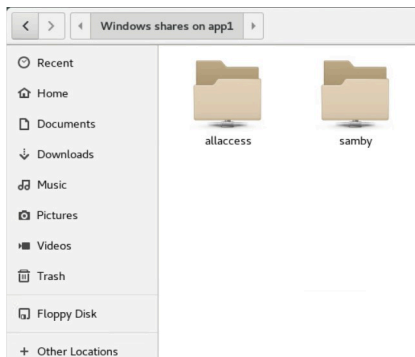


2. Test Access to the Samba Share

- a. Under Applications, open a Terminal.
- b. Install Samba: `sudo yum install samba-client samba-common cifs-utils -y`
- c. Allow Samba through the firewall: `sudo firewall-cmd --permanent --add-service=samba`
- d. Reload the firewall: `sudo firewall-cmd --reload`
- e. Log into the SMB share: `smbclient //app1.college.com/samby -U user1`

```
[champlain@client1 ~]$ smbclient //app1.college.com/samby -U user1
Enter SAMBA\user1's password:
Domain=[APP1] OS=[Windows 6.1] Server=[Samba 4.6.2]
smb: \>
```

- f. Alternatively, you should be able to access the “WORKGROUP” share through “File Manager” and then either browse to “allaccess” share, which allows all users or sign into the “samby” share.



Congratulations, Client1 is now configured.

Congratulations, the Base Lab Configuration is finished.

7. Troubleshooting

7.1. Location to Logs & Configuration Files

- General Logs: /var/log/messages
- Samba Configuration: /etc/samba/smb.conf

7.2. I. Firewall - Installing Nano - Cannot install nano

1. Check to see if you can ping out by using `ping 8.8.8.8`. If you can't then this should be a solution.
2. Sometimes, when interfaces are edited in Network Manager, there will be a second `ens192`. Delete it.
3. First check Network Manager by using `nmtui` to see if the interfaces are set up properly.
 - a. The external/Internet interface, `ens192`, should have:

- i. IPv4 Configuration set to Automatic
 - ii. Automatically connect check-boxed
- b. The internal/Intranet interface, ens224, should have:
 - i. IPv4 Configuration set to Manual
 - ii. IP Address: 192.168.100.1/24
 - iii. Automatically connect check-boxed
4. Restart your network by using `sudo systemctl restart network`.

7.3. II. Firewall - *systemctl restart network*

1. It's okay if network won't restart.

7.4. III. Firewall - *tcpdump*

1. Install tcpdump on your Firewall: `sudo yum install tcpdump -y`
2. Switches:
 - a. -D: Display available interfaces
 - Ex: `sudo tcpdump -D`
 - b. -i: Capture packets from a specific interface
 - Ex: `sudo tcpdump -i ens224`
 - c. -n: Capture IP address
 - Ex: `sudo tcpdump -n`
 - d. port: Captures from a specific port
 - Ex: `tcpdump -i ens224 port 22`
 - e. src: Captures packets from source IP
 - Ex: `tcpdump -i ens224 src 192.168.0.2`
 - f. tcp: Captures only TCP packets
 - Ex: `sudo tcpdump -i ens224 tcp`

