CNIT 34210: Storage Area Networking

CNIT34210-004

Group 09

Ethan Hammond

Julio Navarro

Aadi Jain

Submitted To: Justin Anderson

Date Submitted: 05/05/23

Date Due: 05/05/23

Table of Contents

Table of Contents 2
Executive Summary 3
Business Case 4
Procedures 5
    Phase 1: 5
    Phase 2: 7
    Phase 3 11
CONCLUSION AND RECOMMENDATIONS 14
RECOMMENDATIONS 14
RESULTS 16
BIBLIOGRAPHY 19
APPENDIX A: PROBLEM SOLVING 22
    Problem 1: PXE Boot issues 22
    Problem 2: DHCP 22
    Problem 3: CHAP Authentication Issues 22
APPENDIX B: TABLES 24
APPENDIX C: DHCP Configuration Page 25

Executive Summary

This report covers the procedures completed to install and configure a network storage server using multiple different technologies for the ACME corporation. This report will be covered in several main sections including the Executive Summary, Business Case, Procedures, Conclusion, Recommendations, and Results. First, the Executive Summary provides a general overview of the contents contained within this report. The Business Case details the goals and objectives required to meet the needs of ACME corporation as well as the technologies needed to be implemented. The Procedures section covers the steps needed in order to successfully implement each component necessary to provide block storage across the network. Next, the Conclusion provides an overall summary of the devices and software used and required in order to meet the needs and expectations of the business. Following the Conclusion, Recommendations were provided relating to steps that could be taken when initially configuring the network. Finally, the Results portion covers the final outcome including what was created that led to the final architecture and how the logical and physical diagram demonstrates the final results expected from ACME.

Business Case

The objective of this project was to show a network to ACME Inc., showing a display of what is needed for the company's growing storage needs. The overall end goal for this project was to show a small network with many services as an example that could be used for ACME Inc. for their storage problems and as something that could be implemented into their network.

The first service that was shown was one of the first services that was implemented, iSCSI SAN. iSCSI is a protocol that talks about how SCSI packets, or information, should be transported using TCP or IP, while a SAN is a block level storage letting multiple users or clients access it. An iSCSI SAN would allow for the company to access data quickly since Ethernet is used as the connection. The second service that was implemented was the implementation of CHAP to authenticate the initiator or both the target and the initiator. This service would be an effective solution as an authentication method to ensure that the right target and/or initiator is being connected to. The third key service was DHCP and TFTP as these services are needed in order to implement PXE booting. DHCP assigns IP addresses, while TFTP saves device configurations. These two services give redundancy along with reduced network administration for ACME Inc. Finally, the last key service that was implemented was PXE, which allows a machine to be booted without the OS being on the machine. This service lets devices on the network be more efficient by letting them not have to store the OS along with providing a centralized place for network administration.

All of these services demonstrated throughout the network were configured so that ACME Inc. would get a clear idea about the potential of implementing these services on their own network.

Procedures

The procedures section was broken up into groups of steps that were completed. In the steps, the buttons pressed were **bolded**, options were *italicized*, text entered into console/terminal was typed in `Courier New`, menu navigation and repeated actions were shown with the | pipe | symbol.

Phase 1:

Installation of host OS VMs

Host VMs needed to be installed to demonstrate how SANs work off of the TrueNAS server. All machines were created with minimal specifications for ease of creation. TrueNAS was installed with the special necessary media.

1. Opened a browser and typed https://studentvc.cit.lcl to get to the Heavilon Cluster.
2. Created VMs with minimal specifications for the following operating systems:
    a. Almalinux Server 9
    b. Windows 2019 Server
    c. Windows 2022 Server
    d. Windows 11 Client
3. Installed a client for ESXi 8.0 and booted the machine.
4. Added the attached hard drive as a 20 GB VMFS datastore and pressed enter.

TrueNAS Install

5. Right clicked the *vSwitch0* under the *networking* tab and created a new port group named iSCSI.

6. Created a VM with a TrueNAS ISO disc image, 16GB HDD, 16GB of RAM, 1 public CIT NIC, 1 iSCSI private NIC, and 2 RDM disks 1TB.
7. Entered `1` to configure network interfaces and set the following IP address information on the management public NIC:
    a. IP Address: 10.20.9.10
    b. Subnet mask: 255.255.255.0

TrueNAS Configuration

TrueNAS was the operating system chosen to house the Storage Area Network service. This OS contains a web configurator accessed via a management network. This can be used for networking configurations, and service configurations.

1. Logged into the management portal at 10.20.9.10.
2. Clicked *Global Configuration* on the left pane and set nameservers, a hostname, and a gateway.
3. Selected *Interfaces* on the left pane and created a new interface for the iSCSI network.
4. Set the interface IP to 192.168.1.10 | 255.255.255.0.
5. Selected *Static Routes* on the left pane and changed the iSCSI network gateway to 192.168.1.1.
6. Clicked *Storage* | *Pools* on the left pane and clicked *Add*.
7. Created a new disk pool using RAID 1 from the two RDM disks added to the machine on install.
8. Clicked *Next* | *Next* to finish the creation wizard.
9. Clicked the three dots to the right of the new disk pool and selected *add Zvol*.

10. Created a Zvol for all three windows server machines, linux machine, and ESXi machine of 150 GiB each.
11. Selected Services in the left pane and checked the boxes next to iSCSI services.

Phase 2:

TrueNAS Target Configuration

TrueNAS can be used to create extents out of connected hard disks, targets associated with these extents, and targets to be connected to by clients. The clients access the targets and can input and output data onto the underlying hard disk.

1. Navigated to the TrueNAS web configurator at 10.20.9.10.
2. Clicked *Sharing | Block Shares (iSCSI)* on the left hand pane.
3. Set the Base Name to iqn.truenas and clicked *Portals*.
4. Clicked Add to add a new portal with an IP address of 192.168.1.10 on port 3260.
5. Clicked *Initiators Groups* and added new initiator groups with new group IDs for all client machines.
6. Selected *Targets* and created a new target for every Zvol created.
7. Set a target name to the name of the Zvol created, the portal group ID as the portal, and initiator group ID to the group that was created for its client.
8. Selected *Extents* and created a new extent for each client and named it the same name as its Zvol.
9. Added the *Device* as the Zvol that was created for each extent's client.
10. Clicked *Associated Targets* and created a new entry for each target.

11. Selected the target and added its corresponding extent, mapping it over LUN ID 0.

CHAP Configuration

CHAP is the method used to secure Storage Area networks. CHAP can be implemented for discovery or connection. It can also be configured for one-way or mutual CHAP with targets authenticating initiators and both authenticating each other.

Discovery One-Way CHAP

1. Logged into the TrueNAS web configurator at 10.20.9.10.
2. Clicked *Sharing | Block Shares (iSCSI)* on the left hand pane.
3. Selected *Authorized Access* and created a new group with an ID of 1.
4. Added a user name of CNIT342group9 and set a secret password.
5. Navigated to the *Portals* tab and edited the current portal.
6. Changed *Discovery Auth Method* to 'CHAP' and the group to ID 1.

Mutual CHAP

7. Clicked *Authorized Access* and added a group of ID 2.
8. Added a user name and peer user name of CNIT342group9 and set secret passwords.
9. Clicked on *Targets* and added authentication methods of Mutual CHAP, and added Authentication Group Number 2.
10. Selected *Initiators Groups* and edited every group ID, setting only the specific initiator IQNs and IP addresses to be allowed in each group.

Windows Initiator Configuration

Windows machines can function as iSCSI initiators with the built-in Microsoft software MS iSCSI Initiator. This is done through a GUI with an IP to the target server, and CHAP authentication credentials.

1. Opened the Windows start menu and entered iSCSI initiator.
2. Clicked the *Discovery* tab | *Discover Portal* and entered 192.168.1.10:3260.
3. Clicked *Advanced* and set the local adapter and initiator IP to the iSCSI NIC.
4. Checked 'Enable CHAP log on' and entered the target secret from the auth group.
5. Clicked OK to discover the share and clicked the *Configuration* tab.
6. Selected *CHAP…* and set the peer secret set in the auth group.
7. Selected the *Targets* tab and clicked the target discovered | Connect.
8. Clicked Advanced and set the local adapter, initiator IP, target portal IP.
9. Checked 'Enable CHAP log on' and 'Perform mutual authentication'.
10. Entered the peer username and the user secret from the auth group.
11. Clicked connect to connect to the share.
12. Opened the Windows start menu and typed disk partition and clicked enter to open disk management.
13. Right clicked the iSCSI share to partition the share.

AlmaLinux 9 Initiator Configuration

Linux iSCSI initiator functionality can be configured with iSNS servers or Sendtargets. Sendtargets can be used to directly connect to an iSCSI share or discover an iSCSI share.

1. Opened up a terminal and entered `sudo yum install iscsi-initiator-utils`.

2. Used `sudo nano /etc/iscsi/iscsid.conf` to edit the iscsi initiator configuration.
3. Uncommented the lines for username and passwords for the discovery CHAP and entered in the user name and user password.
4. Uncommented the lines for username and passwords for the mutual CHAP and entered in the peer username and peer passwords.
5. Used `iscsiadm -m discovery -t sendtargets -p 192.168.1.10` to discover the share.
6. Used `iscsiadm -m login` to log into the share to access it.
7. Used `parted --script /dev/sdb "mklabel gpt"` to part the partition.
8. Entered `parted --script /dev/sdb "mkpart primary 0% 100%"` to partition the drive.
9. Used `mkfs.xfs /dev/sdb1` to make the share in dev.
10. Entered `mount /dev/sdb1 /mnt` to mount the share and `df -hT` to show the connected filesystems.

ESXi Initiator Configuration

ESXi initiators are configured through the management interface by adding a vmkernel and a vmnic and adding it to a vswitch. NIC Teaming is then used to configure a port group and vmkernel to just use one NIC for iSCSI functionality.

1. Logged into the management portal at 10.20.9.15 and selected *networking* on the left pane.
2. Created a new VMkernel NIC for the iSCSI port group and attached it to vSwitch0.

3. Opened the vSwitch0 and configured NIC teaming to use vmnic0 for the uplink only, and the iSCSI port group to just use the iSCSI vmkernel NIC.
4. Clicked *Storage* in the left pane and navigated to *Adapters* | *Software iSCSI*.
5. Selected use CHAP for CHAP authentication and entered the username and password to discover the share.
6. Added a port binding and selected the vmk1 and iSCSI port group.
7. Added a dynamic target of 192.168.1.10 and refreshed the page.
8. Selected *Datastores* and partitioned the iSCSI shared drive.

Phase 3

TFTP and DHCP Installation

PXE booting can be achieved through using a TFTP server to transfer an undionly.kpxe file to the clients. A DHCP server needed to be installed for static IP and PXE reservations for booting.

1. Created a new Almalinux 9 VM on the Heavilon Cluster and used `sudo yum install tftp-server.`
2. Copied directories into /etc with `sudo cp -v /usr/lib/systemd/system/tftp.service /etc/systemd/system/tftp-server.service.`
3. Used `sudo cp -v /usr/lib/systemd/system/tftp.socket /etc/systemd/system/tftp-server.socket.`

4. Edited the service config with sudo nano /etc/systemd/system/tftp-server.service and added the lines:
    a. Requires=tftp-server.socket
    b. ExecStart=/usr/sbin/in.tftpd -c -p -s /var/lib/tftpboot
    c. WantedBy=multi-user.target.
5. Edited the socket config page and added `BindIPv6Only=both` under the socket config.
6. Downloaded the undionly.kpxe file from Brightspace and placed it inside /var/lib/tftpboot.
7. Used `sudo chmod 777 /var/lib/tftpboot` to allow TFTP access to the folder.
8. Used `sudo systemctl enable tftp-server.service | sudo systemctl start tftp-server.service` to start TFTP.
9. Used `sudo yum install dhcp-server` to install DHCP server service.
10. Used `sudo systemctl enable dhcp-server` and `sudo systemctl start dhcp-server` to start the service.
11. Wrote the following config page for IP and PXE distribution (See Appendix C for config page.
12. Removed the firewall with `sudo` systemctl disable firewalld and `sudo systemctl stop firewalld.`

BIOS Boot Order Changes

BIOSes for all machines needed to be configured to boot off of the iSCSI NIC, and then the installation media second to allow PXE booting to work effectively. This was configured in vSphere.

1. Logged into vSphere at https://studentvc.cit.lcl.
2. Turned all VMs off and right clicked | edit settings | VM Options | Boot options, and turned it to BIOS mode with Force BIOS Setup.
3. Added a CD/DVD drive with the desired machine ISO file and connected it.
4. Booted the machines and changed the boot order to boot off of the iSCSI NIC, and then the CD/DVD drive.
5. Booted the machine and booted into the new OS and installed it onto the iSCSI drive.
6. Took the CD/DVD drive off of the machine after it installed the OS and restarted the VMs.

CONCLUSION AND RECOMMENDATIONS

CONCLUSION

Storage Area Networks can be used to host storage volumes for clients to connect to and can be managed with operating systems such as TrueNAS. These shares can be connected by multiple operating systems as demonstrated by using Windows Client OS, Windows Server OS, Linux Server OS, and ESXi OS. When SANs are implemented, they can be secured by using methods like CHAP authentication. Authorization was managed by using One-way CHAP for discovery, and mutual CHAP for connection. SANs can also be used for PXE booting for efficiency, management, and ease of NIC Boot ROM versions. This was implemented with DHCP static reservations as well as an undionly.kpxe over TFTP on the same Almalinux 9 server. PXE booting can cause issues if not configured correctly but can be very effective in minimizing issues with many computer operating systems.

RECOMMENDATIONS

Recommendation 1: When setting up DHCP, make sure that the syntax is correct since the syntax needs to be correct in order for DHCP services to be provided. One way to easily check this is to use the DHCP syntax checker that checks the syntax for the dhcp config file. If DHCP is still not working after fixing the changes listed as an error, redo the DHCP configurations since it could be one issue that you are not noticing currently.

Recommendation 2: When setting up the infrastructure initially when setting everything up, be sure to add a second NIC to the devices for iSCSI connections to work. This is necessary

since there will be two networks created, one for the public and another for iSCSI. Failure to do this will result in the initiator not being able to connect to the TrueNAS and access the data there. Setting up this early makes the setup process quicker since one will not have to go back and change the settings on all the machines, wasting time in the process.

Recommendation 3: If a problem arises and forces one to troubleshoot, attempt to trace the steps in the process and troubleshoot each step. The reason for this is that attempting to "hail mary" the problem is not the best troubleshooting method since it does not help. Troubleshooting each step in the process will ensure that the problem will be fixed if done correctly since all the steps in the process must be correct for the whole process to work properly.

RESULTS

The results for this lab were a big success with some success and struggles along the way. Some of the evidence of success is that all the infrastructure and services required to be completed in the lab were eventually completed and fully operational. The struggle however was found in Phase 3 of the lab in which PXE booting was meant to work, but it would not properly function and load the image file into the machines. This problem was eventually resolved, making the issue nonexistent. All the IP information for all the devices in the network can be found in Appendix B Table 1.

One of the first results was found when setting up the iSCSI and the authentication protocol (CHAP) working properly. Both one-way and mutual CHAP were set up properly, letting either the target authenticate the initiator or for both devices to authenticate each other for security. On top of this, all four VMs (AlmaLinux and all Windows VMs) were able to connect to their respective targets on the target server, letting them access whatever contents exist on there. The next major result that happened was for Phase 3 and involved PXE booting.

Another major result was when the PXE booting was properly set up, letting the images of all the machines be saved and loaded up at boot time by the TFTP server to the machine. PXE required that a TFTP Server and DHCP server be created with the DHCP Server assigning IP addresses and the TFTP server holding and sending image files to be booted. One server having both functions was created instead of two separate ones to make it simpler and more efficient. The benefit of PXE booting is that it allows devices to use less storage since the OS image file does not have to be stored locally, saving space that would be otherwise occupied by it. This also makes devices on the network and the network as a whole more efficient as well since less resources are devoted to the OS.

Overall, the results of this lab showed the potential of all of the services that were done in the network. Below are the final diagrams of the completed network. The first diagram is the logical diagram, showing how data moves through the network. The second diagram is the physical diagram, showing all the devices, the interfaces they are connected to, and the addresses attached to them.

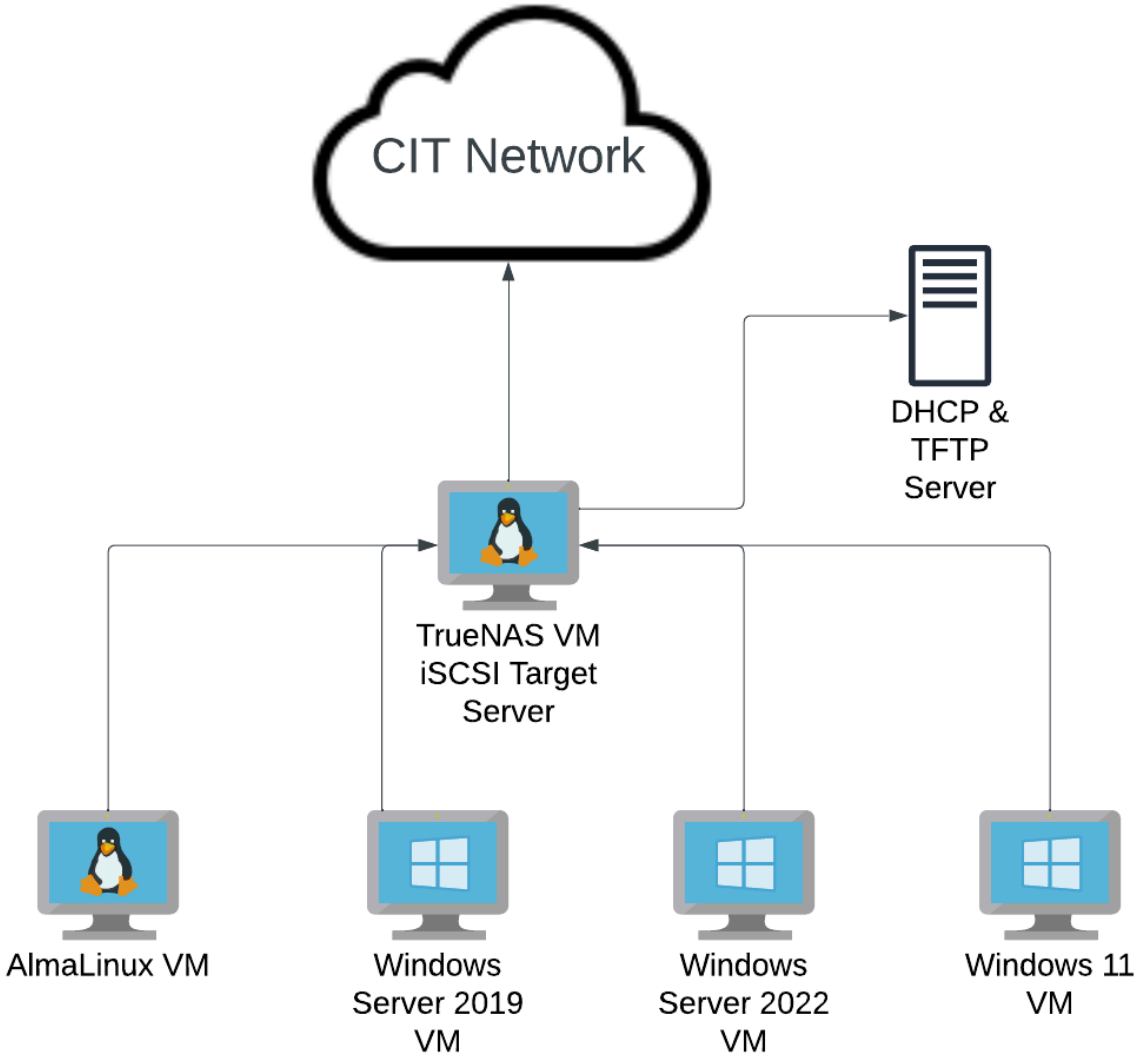

Figure 1: Logical Diagram for the network created in this lab.

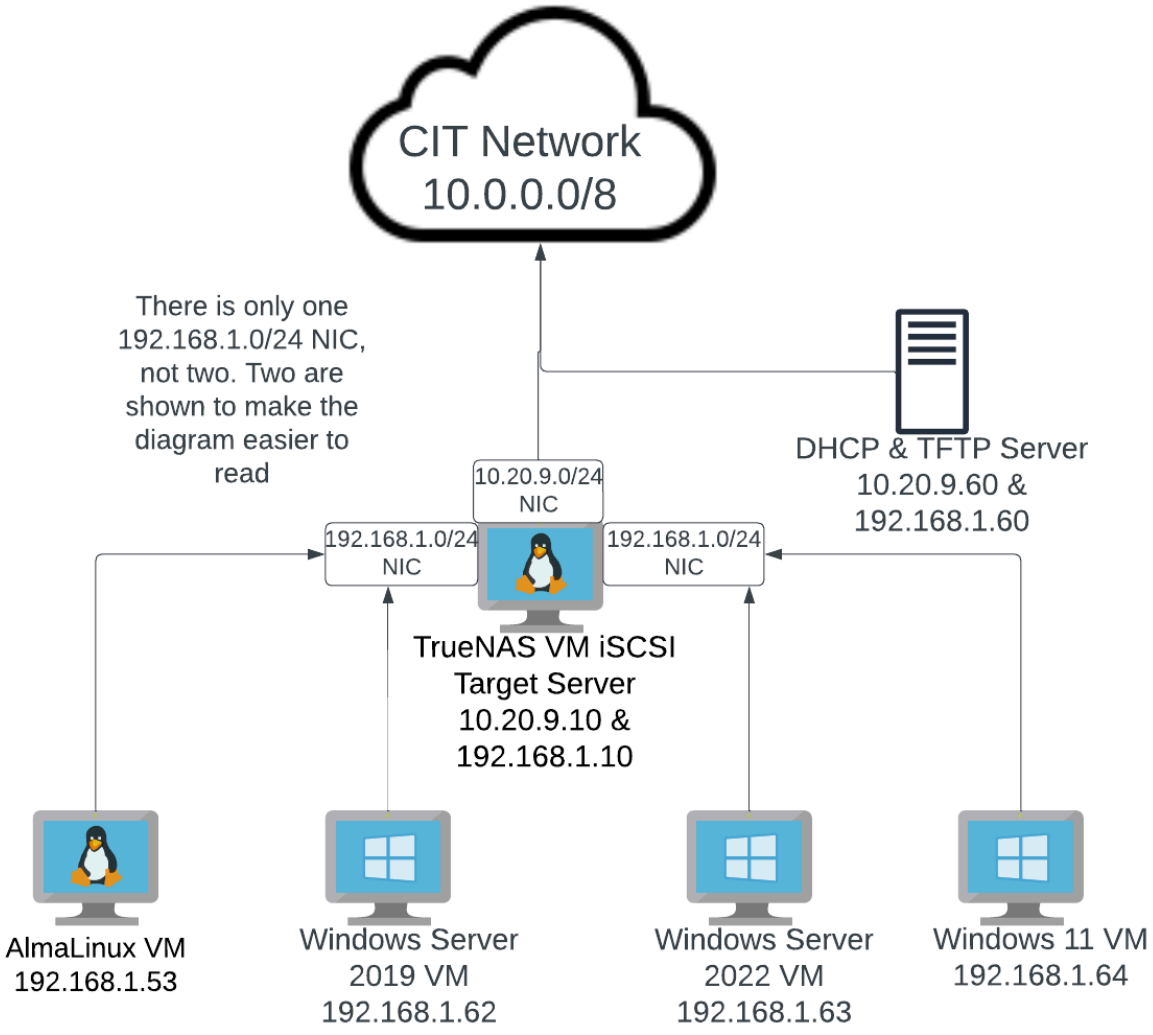

Figure 2: Physical Diagram for the network created in this lab.

BIBLIOGRAPHY

Anderson, J., personal communication, 27 April 2023

Bishun, R. (2020, January 26). *How to configure vmware esxi 6.7 to use iscsi NAS storage*. Ray's Notebook. Retrieved May 4, 2023, from https://raybishun.com/2020/01/26/how-to-configure-vmware-esxi-6-7-to-use-iscsi-nas-storage/

Daisy. (2023, April 2). *How to use the PXE (Preboot Execution Environment) boot?* MiniTool. Retrieved May 4, 2023, from https://www.minitool.com/backup-tips/pxe-boot.html

Firth, M. (2013, January 4). *How can I check dhcpd.conf against syntax error without running dhcpd?* Stack Overflow. Retrieved May 4, 2023, from https://stackoverflow.com/questions/13878706/how-can-i-check-dhcpd-conf-against-syntax-error-without-running-dhcpd

Gite, V. (2023, March 4). *How to make disk image with DD on linux or unix - nixcraft*. HowTo Linux. Retrieved May 4, 2023, from https://www.cyberciti.biz/faq/unix-linux-dd-create-make-disk-image-commands/

Microsoft Corporation. (2015). *Windows 10*. Microsoft. Retrieved April 26, 2022 from https://www.microsoft.com/en-us/windows/get-windows-10

Microsoft Corporation. (2019). Windows Server 2019 (Windows 10, version 1809). Retrieved from https://microsoft.com/windowsserver

Microsoft Corporation. (2019). Windows Server 2022 (Windows 10, version 1809). Retrieved from https://microsoft.com/windowsserver

Odondon, L. (1962, February 1). *ISCSI login failed with error 24 - could not log in to all portals*. Unix & Linux Stack Exchange. Retrieved May 4, 2023, from https://unix.stackexchange.com/questions/207534/iscsi-login-failed-with-error-24-could-not-log-in-to-all-portals

Purdue University CIT. (2019, January 2). *CIT Networking Laboratories Laboratory Manual*. Purdue University

Purdue University CIT. (2022, 1 15). *Lab Report Template*. Purdue University

Rawles, P., personal communication, 24 April 2023

Rawles, P. (2023). *Lab 1- Storage*. Purdue University CIT

Reynolds, L. (2022, February 6). *PXE network boot on linux*. Linux Tutorials - Learn Linux Configuration. Retrieved May 4, 2023, from https://linuxconfig.org/network-booting-with-linux-pxe

SUSE. (n.d.). *Preparing network boot environment: SLES 15 SP1*. documentation.suse.com. Retrieved May 4, 2023, from https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-deployment-prep-pxe.html

Vladan, S. (2017, February 10). *How to configure esxi 6.5 for iscsi shared storage*. 4sysops. Retrieved May 4, 2023, from https://4sysops.com/archives/how-to-configure-esxi-6-5-for-iscsi-shared-storage/

VMware, Inc. (2021). VMware ESXI (version 7). Retrieved from https://www.vmware.com/products/esxi-and-esx.html

VMware (n.d.). *vSphere*. VMware Inc. Retrieved April 26, 2022, from https://www.vmware.com/products/vsphere.html

APPENDIX A: PROBLEM SOLVING

Problem 1: PXE Boot issues

Problem Description: On boot, the machine would launch an iPXE session, loading in the undionly.kpxe file, lose connection, and time out. This would then continuously repeat.

Solutions Attempted: It was attempted to change the networking information and IPs, repair the DHCPd config file, and re-evaluate TFTP functionality.

Final Solution: The final solution was to reinstall the DHCP and TFTP server and reconfigure it from scratch. This solved the issue of not being able to PXE boot.

Problem 2: DHCP

Problem Description: DHCP was not able to give out IPs to the machines on the 192.168.1.0/24 network. This caused issues for PXE booting as the machines could not connect to the TFTP server to obtain undionly.kpxe

Solutions Attempted: It was attempted to reconfigure the dhcpd.conf file and TFTP files.

Final Solution: The issue was fixed by removing the public NIC from all machines and changing all entries of 10.20.9.0/24 networks and IP addresses to 192.168.1.0/24 networks which solved the issue.

Problem 3: CHAP Authentication Issues

Problem Description: CHAP authentication was causing the Alma machine to not be able to connect to the iSCSI shares.

Solutions Attempted: It was attempted to turn off CHAP and see if it worked, which it did. Then it was attempted to reconfigure the iscsi.conf file to attempt to get it to connect.

Final Solution: The solution to the issue was to turn off CHAP, turn on one-way CHAP, then turn on mutual CHAP. One by one, security was enhanced and solved one by one until the issue was resolved.

APPENDIX B: TABLES

Table 1

All the machines connected created for all three phases and their respective IP Addresses

Machine Description	IP Address
AlmaLinux1 VM	192.168.1.53
AlmaLinux2 VM	192.168.1.20
AlmaLinux DHCP Server	10.20.9.60
	192.168.1.60
ESXI	10.20.9.15
	192.168.1.15
TrueNAS	10.20.9.10
	192.168.1.10
Windows Server 2019	192.168.1.62
Windows Server 2022	192.168.1.63
Windows 11	192.169.1.64

Note. All the IP Addresses of all the machines located in the network that are connected along with a description for each machine.

APPENDIX C: DHCP Configuration Page

```
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

ddns-update-style interim;
option domain-name-servers 10.2.1.11, 10.2.1.12;
authoritative;
option time-offset      -18000;

subnet 192.168.1.0 netmask 255.255.255.0 {
range dynamic-bootp 192.168.1.50 192.168.1.100;
option broadcast-address 192.168.1.255;
option routers 192.168.1.1;
}

#PXE option definitions
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.keep-san code 8 = unsigned integer 8;
option gpxe.bus-id code 177 = string;
option domain-name "g9.iscsi";

        group {
          host alma {
            option host-name "alma.iscsi.group9.lcl";
            hardware ethernet 00:50:56:91:43:E4;
            fixed-address       192.168.1.61;
            if not exists gpxe.bus-id {
                next-server 192.168.1.60;
                filename "undionly.kpxe";
            }
           else
           {
            filename "";
            option root-path "iscsi:192.168.1.10::::iqn.truenas:alma3";
            option gpxe.keep-san 1;
           }
          }


          host win19 {
            option host-name "win19.iscsi.group9.lcl";
            hardware ethernet 00:50:56:91:78:C5;
            fixed-address       192.168.1.62;
            if not exists gpxe.bus-id {
                next-server 192.168.1.60;
                filename "undionly.kpxe";
            }
           else
           {
            filename "";
```

Figure 1: First page of /etc/dhcp/dhcpd.conf.

```
  option root-path "iscsi:192.168.1.10::::iqn.truenas:win19";
  option gpxe.keep-san 1;
 }
}

host win22 {
  option host-name "win22.iscsi.group9.lcl";
  hardware ethernet 00:50:56:91:14:8C;
  fixed-address       192.168.1.63;
  if not exists gpxe.bus-id {
      next-server 192.168.1.60;
      filename "undionly.kpxe";
  }
 else
 {
  filename "";
  option root-path "iscsi:192.168.1.10::::iqn.truenas:win22";
  option gpxe.keep-san 1;
 }
}

host win11 {
  option host-name "win11.iscsi.group9.lcl";
  hardware ethernet 00:50:56:91:6E:56;
  fixed-address       192.168.1.64;
  if not exists gpxe.bus-id {
      next-server 192.168.1.60;
      filename "undionly.kpxe";
  }
 else
 {
  filename "";
  option root-path "iscsi:192.168.1.10::::iqn.truenas:win11a";
  option gpxe.keep-san 1;
 }
}









#Group bracket
}
```

Figure 2: Second page of /etc/dhcp/dhcpd.conf