Cloud Computing Lab

PRODUCTION ENVIRONMENT SETUP GUIDE

1ST EDITION: JOHN KRIVICH 2ND EDITION: ERIC EALES, ALEX LLOYD
DURHAM TECHNICAL COMMUNITY COLLEGE 1637 LAWSON STREET DURHAM, NC 27703

You can find regularly updated CCL information and documentation on the Durham Tech. Web site at:

durhamtech.edu/durham-tech-foundation/grants/cloud-computing-lab-ccl

The Durham Tech. Web site also includes information on project history and participation.

This material is based upon work supported by the National Science Foundation under Grant Number 1104251. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Durham Technical Community College
1637 Lawson St.
Durham, NC 27703
Durham Tech Website

Contents

Chapter 3. vCenter Server Appliance

About This Document

The *Cloud Computing Lab: Production Environment Setup Guide* is intended to familiarize administrators with the components and configurations that are needed to build and deploy a complete, functional version of the CCL as it is implemented at Durham Technical Community College (DTCC). DTCC obtains all necessary software and license keys through an Academic License with VMware.

Based on the same core configurations that were detailed in the *Cloud Computing Lab: Test Environment Setup Guide*, this environment was developed to be put into production on the DTCC network and includes technologies and configurations that were not covered in the previous guide. Much of the initial configuration is similar or the same, so you will be familiar with portions of this process if you have completed the test environment setup. Refer to your small-scale model for any difference in configuration that is specific to your hardware environment.

The CCL system at DTCC uses NDG NETLAB+® hardware and software (Link to NetLab Website) to provide the front end/user interface. This requires the upfront expense of purchasing Network Development Group™ hardware, as well as the ongoing cost of an annual license fee for NETLAB Academy Edition™. Alternative front end solutions exist, including free and open-source options. This guide describes the back end configurations that would be used for any of these options.

The operating systems, software, hardware, and services described herein are those that were chosen or available for this system at Durham Technical Community College. If you choose to make alterations, or utilize different hardware or software components, this document may no longer be accurate for your setup.

Included at the end of this document is an appendix section providing reference images that may be helpful during configuration of the CCL. The images shown are to be used as examples only, and are not intended to replace the step-by-step directions of the following chapters.

Chapter 1. Configuring the Physical / Network Environment

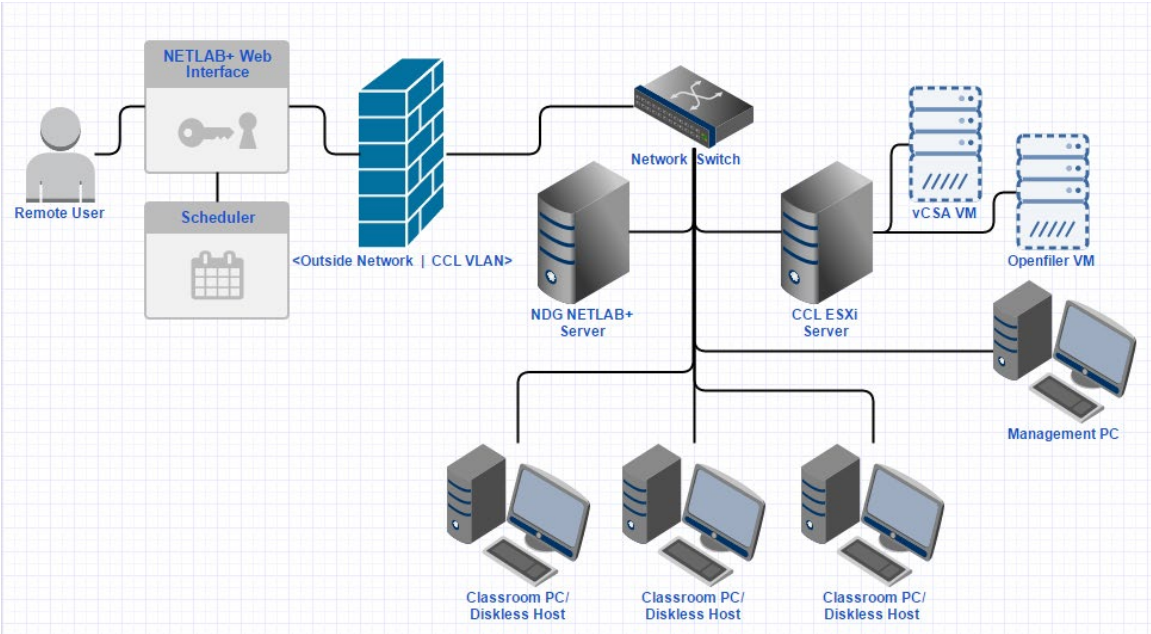
This chapter describes how to set up all required physical equipment (up to and including the selection of operating systems) needed to replicate the production environment used at DTCC for full-scale rollout. Further software and services configuration will be detailed in later chapters.

This chapter also describes some initial configurations that will have to be made on the network switch in order to ensure proper and safe communication within the CCL system.

The CCL environment at DTCC consists of a Dell™ PowerEdge™ R710 server, Cisco® Catalyst® 2960-s switch, and twenty (20) Dell Optiplex™ 790 desktop PCs. The desktop machines will require no less than 4GB accessible RAM and Wake-on-LAN (WoL) and Preboot Execution Environment (PXE) capable NICs.

Other necessary items include a Windows® PC for system management, cabling, and input/output devices.

The following image is a representation of the hardware and systems at work in the CCL system.



Hardware

This section describes all of the various hardware that is needed to complete the CCL build, and explains the role of each component. Any specific hardware or software requirements are also detailed below. Information regarding how to install or configure components will be laid out in subsequent chapters.

Server Host

For the CCL server, use the most up to date equipment available to you, as this machine will house and manage the entire CCL system. This server will run VMware ESXi™ 5.5 as the native operating system, within which your virtual environment will be built. Key virtual components are described below.

VMware vCenter™ Server Appliance™

This virtual server provides DHCP, TFTP, and HTTP services to the CCL network. It is used for WoL and PXE to wake and boot host machines, as well as managing the entire virtual environment. The vCenter Server Appliance (vCSA) is packaged with vSphere® Auto Deploy™, syslog collector, ESXi dump collector and vSphere Web Client services. Not included, but necessary for this system, is an ESXi 5.5 Offline Bundle zip repository.

Openfiler 2.99

This virtual server provides storage for the CCL system. It holds all virtual machine configuration files, as well as remote host syslog data and profiles, providing on demand availability to any ESXi host on the network.

Network Switch

In order to ensure that communication within the CCL environment is reliable and not affected by outside traffic (also, to avoid interfering with the greater network), use a dedicated switch with, at minimum, enough available ports to connect each of your hosts as well as a line out to the greater network.

Cisco Catalyst 2960-s (or similar)

This layer 2 network switch provides all connectivity for the CCL system. It enables the diskless hosts to communicate normally with the greater network, as well as facilitating segregated communication within the CCL system by leveraging VLANs and SNMP protocols. Administrative access is required on this switch.

Desktop PCs

The CCL system requires at least one Windows PC, in addition to the classroom hosts, that is connected to the CCL network for management purposes. Software / hardware requirements for each are listed below.

Management PC (Windows 7 or 8)
This machine is used for centralized management of the CCL environment. It will have VMware vSphere Client installed, as well as vSphere PowerCLI™. This machine must also have an up-to-date web browser (preferably Mozilla® Firefox®, as it provides the most consistent performance with the vSphere Web Client) to perform web-based administration of the Openfiler server as well as the VMware vCenter Server Appliance.

Classroom / Lab PCs
These are your current lab machines that are to be used as diskless hosts running ESXi 5.5. They may normally run any operating system, so long as they meet the hardware requirements. As stated earlier in this document, they must have no less than 4 GB usable RAM and NICs that are WoL and PXE capable.

Physical Topology

This section describes the physical configuration of the production CCL environment. The CCL system is designed to be integrated into your existing physical environment, with the addition of a single physical server. As such, it requires very minimal changes to the existing physical and network setup.

All devices are connected via Ethernet cables through a central switching device. If the switch that your classroom PCs are already connected to supports VLANs and SNMP protocols, and has open ports to connect the server host as well as the management PC, your physical environment is ready. If this is the case, you will may use all current cables and connections.

You also need a detailed network topology to refer to. This helps you to minimize the risk of interrupting normal traffic over the current network. Prior to making any changes to the network, ensure that the topology you are using is complete and accurate. With this as a reference, you can make changes with confidence that you may revert to prior configurations if necessary.

Initial Network / Switch Setup

This section describes the network / switch configurations that are necessary for the CCL network to work as intended. These changes enable the CCL system to operate as needed while remaining segregated from the greater network. This ensures that normal network traffic is unaffected by the services that will be running within the CCL network.

Depending upon the type of switch that you have access to, the commands used may be different, but the basic steps that you must take will remain the same.

The following sections describe the process of preparing the CCL network on a Cisco Catalyst 2960-s layer 2 switch. Any other switch running an up-to-date version of Cisco IOS will take similar commands; for all others, refer to manufacturer documentation.

As stated in the previous section, be sure to start this process with a thorough understanding of the current network and switch topology. Work with your network administrator to obtain this.

Create a New VLAN for the CCL Network

Creating a separate VLAN for CCL network traffic allows you to maintain all current, working network settings while ensuring that CCL traffic remains unimpeded and that there is no conflict between the two.

1. At the terminal, enter Privileged EXEC mode with the following command and enter your admin password if prompted:
   ```
   #enable
   ```
2. Enter Global Configuration mode with this command:
   ```
   #configure terminal
   ```
3. Once in Global Configuration mode, enter the following command to create your new VLAN for use by the CCL network:
   ```
   #vlan <vlan ID>
   ```
4. Exit Global Configuration and save changes to memory by entering the following commands:
   ```
   #end
   #write memory
   ```

Add Switch Ports to CCL VLAN

Now that you've created the CCL VLAN, you must add switch ports to it before it will become active. Add the switch ports that your server host and management PC are connected to first; you can wait until you are ready to test the system before adding the classroom PC connected switch ports if you wish.

1. At the terminal, enter Privileged EXEC mode with the following command and enter your admin password if prompted:
   ```
   #enable
   ```
2. Enter Global Configuration mode with this command:
   ```
   #configure terminal
   ```

3. Once in Global Configuration mode, use the following command to specify the interface / port that you wish to configure:
   ```
   #interface <interface/port number>
   ```
4. Now that you are ready to configure a specific port, enter the following commands to set that interface to access mode with the proper VLAN:
   ```
   #switchport mode access
   #switchport access vlan <vlan ID>
   ```
5. Ensure that portfast is enabled on the switch to avoid issues with DHCP on host machines.
6. Exit Configuration mode and save changes to memory by entering the following commands:
   ```
   #end
   #write memory
   ```

Repeat this procedure for each interface that you wish to add to the CCL VLAN at this time.

Configure SNMP Agent on the Switch

As this switch will be communicating with your lab workstations using two separate VLANs at different times, the CCL system needs a method of changing switch ports between the two.

The following steps get this switch ready to run the SNMP commands that you will write scripts for in Chapter 6.

1. At the terminal, enter Privileged EXEC mode with the following command and enter your admin password if prompted:
   ```
   #enable
   ```
2. Enter Global Configuration mode with this command:
   ```
   #configure terminal
   ```
3. Set private and public community strings with the proper permissions using these commands:
   ```
   #snmp-server community <public string> RO
   #snmp-server community <private string> RW
   ```
4. Enable SNMP notifications using the following command:
   ```
   #snmp-server enable traps
   ```
5. Exit Configuration mode and save changes to memory by entering the following commands:
   ```
   #end
   #write memory
   ```

Chapter 2. Initial Operating System/Software Configuration

This chapter describes how to configure each component in the CCL environment immediately after installing the desired operating system (OS). If you require instruction on how to install a specific operating system, refer to the documentation supplied with that particular OS.

Topics covered in this chapter include BIOS settings (boot priority, WoL w/ PXE), static IP address assignment, and any additional software applications that need to be installed and available. This chapter is organized by individual components, giving all information necessary for one before advancing to the next. Following the sequence used in this chapter is not required, but configuring components in this order will make management tasks more convenient.

Server Host: VMware ESXi 5.5

This section describes how to begin configurations on the ESXi server host. This machine is a hypervisor, exclusively, and therefore requires very little initial configuration.

Install ESXi 5.5

Before beginning this process, make certain that there is nothing important stored on the host machine, as the hard drive will be overwritten by the new operating system. For further instruction on installing ESXi, refer to VMware documentation.

Change ESXi root Password

To change the default root password on the ESXi host, use the following procedure:

1. At the terminal, press **f2** to enter configuration mode. You are prompted for a root password; it is blank on new installations by default.
2. Select **Configure Password**.
3. Enter the new root password in the provided field, confirm, and press **Enter**.

Assign Static IP Address

To assign a static IP address on the ESXi host, use the following procedure:

1. At the terminal, press **f2** to enter configuration mode. You are prompted for a root password; enter the password that you assigned to the account.
2. Select **Configure Management Network**, then select **IP Configuration**.

3. Select **Set Static IP Address and Network Configuration**, and set your desired IP address.
4. Save and log out.

Remote Management PC: Windows Desktop OS

This section describes how to configure the PC that you will use to manage your CCL environment. Once all components are running and have undergone initial configuration, this PC will be used to access the system for the purpose of completing all further configuration.

Set Boot Priority in BIOS

Since this PC is used to manage the CCL environment, you do not want it to network boot. To avoid this, set the correct boot priority in BIOS. To enter BIOS, follow the on-screen prompts during the boot process. Hardware manufacturers use different options, but it usually requires pressing either a Function key (such as F2, F8, or F10), the Esc key, or the Delete key. In BIOS, set the local hard drive as the first priority. For further instruction on how to navigate BIOS, refer to documentation for your specific hardware.

Assign Static IP Address

To assign a static IP address in Windows, use the following procedure:

1. To open Control Panel, click the **Start** button, and then click **Control Panel**.
2. Select **Network and Sharing Center**.
3. In the left pane, click **Change adapter settings**.
4. Right-click **Local Area Connection**, and select **Properties**.
5. Under the Networking tab, select **Internet Protocol Version 4 (TCP/IPv4)**, and click **Properties**.
6. Under the General tab, click the radio button to select the option **Use the following IP address**. Enter your desired IP address, subnet mask, and default gateway as well as a preferred DNS server in the provided fields.
7. Click **OK** to save your settings and exit the Properties window.
8. Click **Close** to exit the Local Area Connection Properties window.

Install and Update Web Browser

In order to take advantage of all the new features included in vSphere 5.5, you are required to use the vSphere Web Client. It is recommended that you access the vSphere Web Client with Mozilla Firefox, as there are known issues when using Internet Explorer® and Google Chrome™.

1. From your management (Windows) machine, open Internet Explorer.
2. Navigate to the FireFox Website, and click **Free Download**.

3. Select a location, and click **Save**.
4. Launch the installer and follow prompts to complete installation.

Install VMware vSphere Client 5.5

The vSphere Client can be downloaded directly from any ESXi host. This method ensures that you get the correct version for your version of ESXi. In order to do so, the host and management machines must be on the same network and have internet access.

1. From your management (Windows) machine, open a Web browser.
2. Enter the IP address that you have assigned to the ESXi server host. For example, `http://xxx.xxx.xxx.xxx` .
3. Click **Download the vSphere Client** under the heading titled **Getting Started**.
4. Select a location and click **Save** to begin the installer download.
5. Launch the vSphere Client installer and follow the prompts to complete installation.

Install VMware vSphere Auto Deploy GUI Fling

The vSphere Auto Deploy GUI Fling will not be configured until later in this process but it should be installed now, as it provides a critical service. This is an experimental plugin from VMware that allows you to manage and configure your Deploy Image without the need for PowerCLI.

1. Download the Auto Deploy GUI Fling from VMware, for vSphere 5.5 at VMware Download Link.
2. Save the downloaded executable to the same directory that houses your vSphere files. Likely to be the following: `C:\Program Files (x86)\VMware\Infrastructure`
3. Run the executable installation file, accepting all defaults.

Install VMware vSphere Web Client 5.5

To install the vSphere Web Client, mount the vCenter Server 5.5 installation ISO file. Use the same ISO that you used to install ESXi on your host machine/server.

1. When the installation wizard opens, click **vSphere Web Client** in the left pane, then click **Install**.
2. Select the desired language, and click **OK**.
3. Review the EULA and select **I accept the terms in the license agreement**. Click **Next**.
4. Accept defaults, or choose alternatives for installation location and TCP port for vSphere Web Client Service, and click **Next**.
5. Enter administrator username and password. Click **Next**.
6. Review certificate information and click **Install Certificates**. When prompted, click **Install**, then click **Finish**.

File Server: Openfiler 2.99

This section describes the creation and initial configurations on the Openfiler file server. Items covered include virtual machine creation and the assignment of a static IP address. Also covered is the process for configuring network and service options as well as creating and configuring your CCL network share.

Create Openfiler 2.99 Virtual Machine

Before beginning this process, take time to consider the storage location for your virtual machine and the share that you will create. Configure hard drives/RAID arrays as appropriate for your setup.

In the vSphere Client interface, right-click the ESXi server host icon and select **Create New Virtual Machine**. Choose to build a VM with custom options. Configure the following:

1. Add a second hard drive and configure it to map to your desired SAN storage array.
2. Set the VM's CD-ROM to connect at power on to the media that your Openfiler ISO is on.
3. Complete virtual machine build.

For further instruction on installing Openfiler, refer to their website at `Openfiler Website` for documentation. For help with creating or customizing a virtual machine in vSphere, refer to VMware documentation at the VMware Documentation Site.

Assign Static IP Address

To assign a static IP address on the Openfiler file server, use the following procedure:

1. Working from the vSphere Client, power on the Openfiler VM and open a console connection.
2. At the terminal, you are prompted for login. Log in as root using the credentials you supplied during installation.
3. Change to the correct directory using the following command:
   ```
   #cd /etc/sysconfig/network-scripts
   ```
4. Open the configuration file for the network adapter in the vi editor with the following command:
   ```
   #vi ifcfg-eth0
   ```
5. Edit the configuration file to reflect the following, replacing all `xxx` with your desired network settings:
   ```
   DEVICE=eth0
   BOOTPROTO=static
   IPADDR=xxx.xxx.xxx.xxx
   BROADCAST=xxx.xxx.xxx.xxx
   GATEWAY=xxx.xxx.xxx.xxx
   HWADDR=xx:xx:xx:xx:xx:xx
   ONBOOT=yes
   ```

6. Save the altered file and quit vi editor:
   ```
   #:wq
   ```
7. Reboot the VM and confirm that your changes hold.

Configure Network and Services

In order to make the necessary changes to your Openfiler file server, log in to the Openfiler Web Interface.

Launch a Web browser and navigate to the IP address associated with the Openfiler file server (`https://xxx.xxx.xxx.xxx:446`). Log in to the Web Interface using **openfiler** as the username, and **password** as the password, and make the following changes:

1. Navigate to the **Accounts** tab, and click **Admin Password** on the right side of the screen.
2. Enter the default password (password) and your new admin password. Click **Submit**.
3. After changing the password, you must re-authenticate.
4. Navigate to the **System** tab.
5. Enter **Network Interface Configuration** settings to reflect your network.
6. Under **Network Access Configuration**, add a connection to your desired Network with the type set to **Share**.
7. Navigate to the **Services** tab and enable the necessary services:
   ```
   CIFS Server           Enabled - Running
   NFS Server            Enabled - Running
   HTTP/Dav Server       Enabled - Running
   ACPI Daemon           Enabled - Running
   SCST Target (FC)      Enabled - Running
   ```

Create and Configure Share

Still working in the Web Interface, make the following changes:

1. Create new volume by first navigating to the **Volumes** tab.
2. In the right pane, click **Volume Groups**, then click the link labeled **create new physical volumes**.
3. If issues arise when creating the physical volumes, change the cylinders to 80 more than its default value.
4. Select the hardware on which you are to create the volume.
5. In the right pane, click **Add Volume**. When prompted, enter the desired name, size & file system type (**XFS**), select **Share** and click **Create**.
6. Navigate to the **Shares** tab.
7. Click selected volume, and name the new share folder.
8. Click the share folder icon, and under the **Share Access Control Mode** heading select **Public Guest Access**. This setting allows Windows sharing without credentials. Note that using this setting can result in security issues in some systems, but it is a requirement for Openfiler to work as intended for this system.

9. Under the **Host access configuration (/mnt/*volume*/*share*/*folder*/)** heading, select the option **Restart services**, and set **RW** permissions for both **SMB/CIFS** and **NFS**.
10. Under **NFS** > **Options**, click **Edit** and select **no_root_squash** from the **UID/GID Mapping** drop-down.

Set Openfiler VM to Start when the Server Host Boots

1. In the vSphere client, from the **Home** tab, select **Hosts and Clusters** under the heading **Inventory**.
2. Select the IP address of the server host in the left pane, then select the **Configuration** tab in the right pane.
3. Under **Software**, click **Virtual Machine Startup/Shutdown**.
4. In the upper right of the screen, click **Properties**. The **Virtual Machine Startup and Shutdown** window will open.
5. Check the box labeled **Allow virtual machines to start and stop automatically with the system**.
6. Set **Default Startup Delay** time. For this setup, the vCSA must be running before this VM can start, so set the default delay to 60 seconds to ensure full boot.
7. Under the heading **Startup Order**, select the VM(s) you wish to have start automatically, and click the **Move Up** button until the VM(s) are arranged under the **Automatic Startup** heading.
8. Click **OK**.

Lab Workstations: Current Service Machine

This section describes the configurations that must be completed in order for your lab workstations to properly work as remote ESXi hosts. It is necessary to make changes to settings both in BIOS and Windows. Remember, these PCs require no less than 4 GB available RAM as well as a NIC that is WoL w/PXE capable.

BIOS Configurations

Enter BIOS and confirm/set the following configurations:

System Configuration:

```
Integrated NIC: Enabled w/PXE
```

Power Management:

```
Wake on LAN: LAN with PXE Boot
Deep Sleep Control: Disabled
Fast Boot: Thorough
```

Windows Configurations

Make the following changes inside Windows:

1. Right-click the **Start** button and select **Device Manager**.

2. Expand **Network Adapters**, and right-click the **integrated NIC**. Select **Properties**.
3. Under the **Driver** tab, click **Update Driver**. In the pop-up, select **Search automatically for updated driver software** and follow prompts to complete the update.
4. Under the **Power Management** tab, ensure that all three available boxes are checked.
5. Under the **Advanced** tab, ensure that **Wake on Magic Packet** and **Wake on Pattern Match** are enabled. Save and exit.
6. Right-click the **Start** button and select **Power Options**.
7. In the left pane, select **Choose what the power buttons do**.
8. Using Administrative privileges, uncheck the radio button beside **Turn on fast startup**.

Chapter 3. vCenter Server Appliance

This chapter describes how to deploy the vCenter Server Appliance (vCSA) virtual machine, as well as how to configure services and software that are utilized within the vCSA.

Contained in this chapter is in-depth configuration information for setting up services needed for the CCL environment. The services covered include DHCP, ATFTP, Net-SNMP, and a WoL client.

vCenter Server Appliance Deployment

This section describes the process of deploying the vCSA from within the vSphere Desktop Client. If you choose to use the vSphere Web Client, the process may vary slightly.

Launch the vSphere Client and Deploy the vCSA

Log in to your ESXi Server Host from Windows via the vSphere Client using the ESXi Server's IP address and root password, then deploy the vCenter Server Appliance VM.

1. Click **File** in the navigation menu and select **Deploy OVF Template.**
2. Select OVF file from either your local storage, or a networked share that you have access to.
3. Accept defaults in creating the VM.
4. Log in to the vCSA and accept user agreements.

vCenter Server Appliance Initial Configuration

Once it has been deployed and is running, perform these initial changes to the vCSA virtual machine before you begin advanced configurations.

Change the vCSA Hostname

1. Launch the vCSA Web Interface by navigating to the IP address that is displayed on the terminal of the VM in a Web browser.
2. Navigate to the **Network** tab and enter the desired hostname.
3. Confirm changes and save.

Set a Static IP Address

1. Remaining in the vCSA Web Interface, navigate to the **Network** tab.
2. In the **Address** field, enter desired settings and save.

3. If you are unable to access the web interface, the IP can be set by running the following command:
   /opt/vmware/share/vami/vami_config_net

Reset the vCSA root Password

1. Launch the Web Interface, navigate to the **Admin** tab.
2. Enter default password **vmware** and desired new password and submit changes.

Ready the vCSA for System Management

From this point, all CCL system management and configuration tasks will be completed within the vCSA. Logged in to the vCSA in the vSphere desktop client, you must first add the physical server as a host.

1. Open vCSA through vSphere Client application, and log in using root credentials.
2. From the vCSA **Home** directory, select **Hosts and Clusters** under the **Inventory** sub header.
3. In the left pane, you will see your vCSA virtual machine. Right click the top node, localhost or the hostname of the machine.
4. Select **New Datacenter**, and set a name.
5. Right click the Datacenter that you created, and select **Add Host**.
6. Enter the IP address and root credentials for your server, and click **Next**.
7. Complete this wizard accepting all defaults.

Set the NIC to Work with Large MTU Transmissions

1. In the vCSA terminal, enter the following command to open the `ifcfg-eth0` configuration file with the vi editor.
   ```
   #vi /etc/sysconfig/network/ifcfg-eth0
   ```
2. Make the following adjustment:
   ```
   MTU=9000
   ```
3. Save and exit by entering the following command:
   ```
   #:wq
   ```

Virtual Network Configuration

In order for the CCL system to work as designed, without interfering with normal classroom network operation, it must run on the separate VLAN that you created. When the time comes to move the PCs into the CCL VLAN, however, the vCSA also needs to be able to communicate with the switch via the normal classroom VLAN. The following sections describe the steps necessary to achieve this communication.

Configure additional vSwitch to handle traffic to the Classroom VLAN

In order for the vCSA to be able to communicate with the switch (on the classroom VLAN) and run the necessary SNMP scripts, you need a

virtual switch set up to communicate on that VLAN. Follow these steps to complete this configuration:

1. From the **Home** directory, select **Hosts and Clusters** under **Inventory**.
2. In the left pane, select the icon that represents your Server Host.
3. Under the **Configuration** tab, select **Networking** from the **Hardware** menu.
4. In the upper right of the window, click **Add Networking…**
5. Select **Virtual Machine** as the connection type, click **Next**.
6. Choose **Create a vSphere standard switch**, and select the physical interface that you wish to utilize for this connection. Click **Next**.
7. Enter a name for this network, and a VLAN ID. Click **Next**.
8. Review configurations, and click **Finish**.

Add second NIC to the vCSA Virtual Machine

As the vCSA needs to be able to communicate with two separate VLANs (your CCL VLAN, and the normal classroom VLAN), a second NIC is needed on the virtual machine. Log in via the vSphere Client using the IP address and your root password, and complete the following configurations:

1. From the **Home** directory, select **Hosts and Clusters** under **Inventory**.
2. In the left pane, right-click the icon that represents your vCSA VM, select **Edit Settings**.
3. Under the **Hardware** tab, click **Add**.
4. Select **Ethernet Adapter**, click **Next**.
5. Enter your network information and click **Next**.
6. Review your configurations, and click **Finish**.

Configure the second NIC within the vCSA terminal

1. In the CLI, enter the following command to copy the ifcfg-eth0 configuration file:
   ```
   #cp -a
   /etc/sysconfig/networking/devices/ifcfg-
   eth0
   /etc/sysconfig/networking/devices/ifcfg-
   eth1
   ```
2. Use the vi editor to alter this new file to work on the correct VLAN. Set a static IP, Netmask, and Broadcast Address in the file.
3. Save and exit by entering the following command:
   ```
   #:wq
   ```
4. Create a symbolic link to this file using the following command:
   ```
   #ln -s
   /etc/sysconfig/networking/devices/ifcfg-
   eth1 /etc/sysconfig/network/ifcfg-eth1
   ```

5. In order for this new configuration to work properly, restart the network service:
```
#service network restart
```

Add Required Packages to the vCSA

There are additional software packages that you need to install in the vCSA in order to perform tasks necessary to the CCL. This section details how to install each of them.

In order to access and download these packages, the vCSA needs temporary access to the internet. This can be achieved by several different methods, such as via a trunk line that has access to a VLAN with DHCP/DNS. Giving internet access to the vCSA creates the possibility of security issues, so this access should be removed after completing all necessary downloads.

Note: Some installation steps require files to be uploaded to the datacenter. Use the following steps to upload the needed files.

1. From vCSA home screen click hosts and clusters
2. Right click data store in left pane and click browse datastore.
3. Click upload files to datastore icon in top bar
4. Click **upload file**.
5. Browse to file and click open.

Add net-snmp to the vCSA

This service is required in order to switch hosts between the standard classroom VLAN and the VLAN that is used by ESXi/Netlab.

1. Obtain and upload a copy of the **SLES™ 11 SP2 ISO** to a Datastore accessible from the vCSA.
2. In the vSphere Client, click the **CD/DVD icon** in the toolbar and select **Connect to ISO image on a datastore** and select the ISO.
3. Mount the ISO in the vCSA command line with the following command:
```
#mount /dev/cdrom /media
```
4. Enter the command `#yast` to enter yaST2 GUI.
5. Select **Software Repositories** from the list and press **Enter**.
6. Press **F3** to add a repository.
7. Select **Local Directory**, then select **Next** and press **Enter**.
8. Select **Browse** and press **Enter**.
9. Under the **/root** directory, select **..** under **Directory Name** and press **Enter**.
10. Select **media** and press **Enter**.
11. Select **OK** and press **Enter**.
12. On the main Yast2 screen, select **Next** and press **Enter**.
13. Read the User Agreement, select **Yes** to agree to the terms of use, select **Next** and press **Enter**.
14. Select **OK** and press **Enter**.

15. Select **Software Management** and press **Enter**.
16. In the **Search Phrase** field, enter **net-snmp** and press **Enter**.
17. Select **net-snmp** along with any additional dependency items, select **Accept** and press **Enter**.

Add WoL Client to the vCSA

This service is necessary to wake the host machines for the CCL system.

1. Connect to online SLES 11 repository using the following command:
   ```
   #zypper addrepo -f
   http://download.opensuse.org/distribution/1
   1.2/repo/oss/ opensuse1
   ```
2. Issue the following command to confirm that the repository is available:
   ```
   #zypper repos -d
   ```
3. Issue the following command to connect to the repository:
   ```
   #zypper refresh
   ```
4. Search for, and install, wol client using the following commands:
   ```
   #zypper search wol
   #zypper install wol
   ```

Add sshpass Package to the vCSA

In order to be able to automate virtual machine shutdown as well as host power off, the vCSA must use SSH to log in to the diskless hosts. For this process to be completed without intervention, this software package must be used to read host root passwords from a directory and enter them when prompted.

1. Connect to the online SLES 11 repository that contains sshpass software using the following command:
   ```
   #zypper addrepo -f
   http://download.opensuse.org/repositories/h
   ome:Strahlex/SLE_11_SP2/home:Strahlex.repo
   ```
2. Issue the following command to confirm that the repository is available:
   ```
   #zypper repos -d
   ```
3. Issue the following command to connect to the repository.
   ```
   #zypper refresh
   ```
   Enter `t` to temporarily trust the key associated with this repository.
4. Search for, and install, sshpass using the following commands:
   ```
   #zypper search sshpass
   #zypper install sshpass
   ```
   Enter `y` to continue download/install.

Configure vCSA VM Startup/Shutdown Options

In the event that the server power cycles due to outage or maintenance, you will want the vCSA VM to restart automatically to reduce CCL

downtime. Also, it is a good idea to set the VM to shutdown gracefully before the server is powered off. This section details how to achieve that.

Set vCSA to Start when the Server Host Boots

1. In the vSphere client, from the **Home** tab, select **Hosts and Clusters** under the **Inventory** heading.
2. Select the IP address of the server host in the left pane, then select the **Configuration** tab in the right pane.
3. Under **Software**, click **Virtual Machine Startup/Shutdown**.
4. In the upper right of the screen, click **Properties**. The **Virtual Machine Startup and Shutdown** window will open.
5. Check the box labeled **Allow virtual machines to start and stop automatically with the system**.
6. Set **Default Startup Delay** time. For this setup, the vCSA must be running before some of the other VMs can start, so set the default delay to 60 seconds to ensure full boot.
7. Under the heading **Startup Order**, select the VM(s) you wish to have start automatically, and click the **Move Up** button until the VM(s) are arranged under the **Automatic Startup** heading.

Set vCSA to Shutdown Gracefully on Host Shutdown

Remaining in the **Virtual Machine Startup and Shutdown** window, complete the following steps before exiting.

1. Set **Default Shutdown Delay** time. Enter a value of 0 (zero) seconds to ensure that this VM begins shutdown as soon as the server is given the shutdown command.
2. Click **OK** to save the changes and exit.

Utilize the Openfiler Share as a Datastore

This section covers the procedure of adding your Openfiler share as a Datastore that can be used as storage to house virtual machines, ISO files, and other necessary packages.

Configure a Datastore for use by VMs

As with other tasks performed in the setup of the CCL environment, this can be achieved in the vSphere Web Client. If you choose to use the Web Client, some details of this process may differ from what is laid out here.

To ensure that the Datastore is always available for use, the first host it is connected to should be the ESXi server. This will keep the Datastore available even when the other (diskless) hosts are offline.

1. In vSphere Desktop Client, select **Home** in the navigation bar, then select **Datastores and Datastore Clusters** from the **Inventory** sub header.
2. Right-click your Datacenter and select **Add Datastore**.
3. Select the Host you wish to apply the Datastore to, click **Next**.
4. Select **Network File System**, click **Next**.
5. Type in the IP of your SAN server, in this case the Openfiler machine, the desired file path (/*mnt*/*volume*/*share*/*folder*/), and a name for this Datastore. Click **Next**.
6. Review, and click **Finish**.

Configure DHCP

This section describes the process of setting up DHCP in the vCSA as it is needed in order for the CCL to work as desired. After completing DHCP configurations, save all altered files to chroot, as some services may not work properly otherwise.

You may remove chroot requirements from DHCP if you desire by altering the `/etc/sysconfig/dhcpd` file to reflect the following:

```
DHCP_RUN_CHROOTED="no"
```

Alter DHCP for the Proper Network Interface

In most cases when using a single NIC, the interface will be **`eth0`**. Your system may differ.

1. In the vCSA CLI, enter the command to open the file in the vi file editor:
   ```
   #vi /etc/sysconfig/dhcpd
   ```
2. Change `DHCPD INTERFACE` value to `eth0`.
3. Save changes and exit the vi editor:
   ```
   #wq
   ```

Set up DHCP Deploy Configuration File

This file does not exist by default in some versions of the vCSA. Create, or open, it by entering the command `#vi /etc/dhcpd.deploy.conf` before making the following configurations:

```
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate
gpxe;
option gpxe.priority code 1 = signed integer 8;
option gpxe.keep-san code 8 = unsigned integer 8;
option gpxe.no-pxedhcp code 176 = unsigned
integer 8;
option gpxe.bus-id code 177 = string;
option gpxe.bios-drive code 189 = unsigned
integer 8;
```

```
option gpxe.username code 190 = string;
option gpxe.password code 191 = string;
option gpxe.reverse-username code 192 = string;
option gpxe.reverse-password code 193 = string;
option gpxe.version code 235 = string;
```

Enter `#:wq` to save the file and exit the vi text editor.

Alter DHCP Configuration File

Prior to making any changes to this file, it is recommended that you make a copy of the original in case issues arise. You can do so by issuing the command `#cp -a /etc/dhcpd.conf /etc/dhcpd.conf.orig`.

1. In the vCSA CLI, open the `dhcpd.conf` file in the vi editor.
2. In the vi editor, alter the file to reflect the following:

```
allow booting;
allow bootp;
deny duplicates;
ddns-update-style none;
include "/etc/dhcpd.deploy.conf";

subnet <your subnet> netmask <your netmask> {
option domain-name "your.domain";

option domain-name-servers <IP of your vCSA>;
option subnet-mask <SM of your vCSA>;
option routers <IP of your vCSA>;
range <first.IP.address last.IP.address>;
allow unknown-clients;
option gpxe.no-pxedhcp 1;

   **The following portion is necessary in
   order to assign each host the same IP
   consistently based on MAC address, and must
   be repeated for each individual host**

host hostname {
hardware ethernet xx:xx:xx:xx:xx:xx;
fixed-address xxx.xxx.xxx.xxx;
option host-name hostname;
}

next-server <IP of your vCSA>;

filename "undionly.kpxe.vmw-hardwired";
}
```

3. Save changes and exit the vi editor:

```
#:wq
```

Set DHCP Service Startup Level

In order for the service to work as you have configured it to, ensure that it will start with the vCSA at the proper levels. Also, you initially have to start the service as it may not yet be running.

1. Enter the command `#service dhcpd start` to bring the DHCP daemon online.
2. Check the service startup level by entering:
   `#chkconfig --list dhcpd`
   Make sure that `3` and `5` are set to `on`, under chkconfig – level x [service name]
3. To set DHCP to run at startup, enter the command:
4. `#chkconfig dhcpd on.`
5. If any configuration changes are required, you must restart the DHCP service.

Configure ATFTP

This section details all necessary configurations that are related to the ATFTP service. SYSLINUX, PXELINUX, and ESXi installation materials are included in this section due to their close relation to the ATFTP service and directories.

Make Initial Changes to ATFTP

Prior to making any changes, make a backup copy of the `atftpd` file in the `/etc/sysconfig` directory. To do this, change to the `/etc/sysconfig` directory and enter the command `#cp –a atftpd atftpd.orig`.

1. Enter `atftpd` file with the vi editor.
2. Make the following alteration:
   Adjust `ATFTP_OPTIONS` line to read:
   `"--daemon --user root"`
   This will allow the service to run with root privileges.

Put the Necessary SYSLINUX Package on the vCSA

After you download and install this package, move the `pxelinux.0` file into the root of the `/tftpboot` directory.

1. Change to the `/tmp` directory (`#cd /tmp`).
2. Issue the following command to download the required files:
   `#wget http://www.kernel.org/pub/linux/utils/boot/syslinux/3.xx/syslinux-3.86.tar.gz`
3. De-compress and make the file available for use:
   `#gunzip syslinux-3.86.tar.gz`
   `#tar xvf syslinux-3.86.tar`

4. Now, you copy the file `pxelinux.0` to the root of the `/tftpboot` directory:
   `#cp /tmp/syslinux-3.86/core/pxelinux.0 /tftpboot`

Create Directory Structure in /tftpboot to Support PXE

Create and configure the proper file structure needed to support PXE. These steps also cover the configuration of the tramp file, as well as preparing for and loading the ESXi ISO that will be deployed to the remote hosts.

1. Enter `#cd /tftpboot` to change to the correct directory.
2. Copy `menu.c32`, `mboot.c32`, and `chain.c32` from `/syslinux` directly to `/tftpboot` root using the following commands:

```
#cp -a /tmp/syslinux-3.86/com32/menu/menu.c32 /tftpboot
#cp -a /tmp/syslinux-3.86/com32/mboot/mboot.c32 /tftpboot
#cp -a /tmp/syslinux-3.86/com32/modules/chain.c32 /tftpboot
```

3. Use the command `#vi /tftpboot/tramp` to open the tramp file in the vi editor.
4. In both lines (set filename, and chain), change the entry from vCenterServerAppliance to your vCSA IP address. This is how it should look:
   `set filename https://` ***<IP of your vCSA>***`:6501/vmw/rbd/tramp`
   `chain https://` ***<IP of your vCSA>***`:6501/vmw/rbd/tramp`
5. Enter `#:wq` to save the file and exit the vi text editor.
6. Issue the command `#mkdir esxi` to create the `/esxi` directory under `/tftpboot.`
7. Insert the ESXi installation disc into the server. Opening the tray will sometimes cause vSphere errors; to fix, log in to the server host in vSphere and answer any questions found under the **Summary** tab for the vCSA.
8. Mount the ESXi CD. Be sure to go into the VM settings and set the cd-rom to **Connect to Host**, then use the following command:
   `#mount /dev/cdrom /media`
9. Issue the command `#cp -a /dev/cdrom /media* /tftpboot/esxi` to copy the contents of the CD to the proper directory. Be sure to adjust this command to copy from where your CD is mounted.

Configure PXELINUX

Create the structure that makes linking PXELINUX, ATFTPD, and the ESXi ISO possible.

1. Create the directory structure that pxelinux.0 will be looking for by issuing the following commands:
   `#cd /tftpboot`

```
#mkdir pxelinux.cfg
```

2. Issue the following commands to load default configurations to this directory:

```
#cd /pxelinux.cfg
#cp -a /tftpboot/esxi/media/isolinux.cfg
default
```

3. Ensure correct configuration of this file by issuing the following commands:

```
#chmod a+w default
#vi default
```

Alter the file to look like this:

```
   DEFAULT /esxi/media/menu.c32
   KERNEL /esxi/media/mboot.c32
   APPEND -c /esxi/media/boot.cfg
#:wq
```

Configure ESXi Installation Files

Since the ESXi installation files have been copied into a new directory (/tftpboot/esxi/media), we need to change the path referred to within those files.

1. First, make a copy (.orig) of the boot.cfg file, then make the necessary changes to boot.cfg:

```
#cd /tftpboot/esxi/media
#cp -a boot.cfg boot.cfg.orig
```

2. Now, open the file in the vi editor (`#vi boot.cfg`) and make the following changes:

   Add `/esxi/media` to the kernel path, as well as all of the modules (***each and every path*** **in "modules" will need to have this added**)

3. To save from the vi editor, use the command **:wq!** to override read only

   .

Set ATFTP Service Auto Start

For the service to work as intended, ensure that it starts with the vCSA virtual machine. Also, you will initially have to start the service as it is not running by default.

1. Enter the command `#service atftpd start` to bring the ATFTP daemon online.
2. To set ATFTP to run at startup, enter the command `#chkconfig atftpd on`.

Chapter 4. VMware vSphere Auto Deploy

This chapter describes how to install and configure the vSphere Auto Deploy service used to push the ESXi operating system out to the hosts that are to be used as hypervisors.

Topics covered include how to enable the Auto Deploy service, installing the Auto Deploy GUI, and in-depth instructions on configuring Auto Deploy.

Install and Enable Auto Deploy Components

This section covers the enabling of Auto Deploy via the web admin GUI, installation of the Auto Deploy GUI Fling, and some initial configurations necessary to this process.

Enable Auto Deploy in the vCSA

Enable service through vCenter Server Appliance (via web admin GUI) and start the service.

1. Navigate to vCSA in Web browser at `https://` ***`<IP of your vCSA>`***`:5480`
2. Log in as root.
3. Navigate to the **vCenter Server** tab, sub-heading **Summary**.
4. Click the **Start** button to enable vSphere Auto Deploy Service.

Configure Auto Deploy for Use by the CCL

This section details, in full, the configurations necessary for Auto Deploy to work in the CCL environment. Included in this section is a specific example of a customization needed for the CCL to work with the lab workstations at Durham Technical Community College. You may not be required to make this particular alteration, but the process described will guide you through any similar customizations that you may require.

vSphere Desktop Client Auto Deploy Setup

These configurations are also possible using the vSphere Web Client, but the details and steps may differ slightly.

1. Click **Home** in the navigation bar.
2. Under **Solutions and Applications**, click the **VMware Auto Deploy** icon.
3. Under the **Software Depot** tab, right-click the blank area under the **Depot Url** heading and select **Add Zip Repository**.

4. Browse to and select the ESXi offline depot Zip file from your storage. The Zip you use may be stored either in a Datastore or a network share to which you have access.
5. Allow the vCSA a few minutes (at least) to download and unzip this file.
6. To confirm the import, select the **Image Profile** tab. You should see several ESXi 5.5 profiles. In this case, for example, there are four different versions:

   ```
   esxi-5.5.0-20140901001s-standard
   esxi-5.5.0-20140902001-standard
   esxi-5.5.0-20140901001s-no-tools
   esxi-5.5.0-20140902001-no-tools
   ```

   The "`s-`" options refer to security related updates only, with no other bugfixes. The "`no-tools`" options do not include VMware Tools™ as standard.

Auto Deploy Image Customization

In some instances, it may be necessary to add software packages to your ESXi Image Profile; The lab workstations at DTCC, for example, would not work properly due to the onboard NIC not having a compatible driver built into the ESXi Depot. In order to remedy this, or issues like it, follow these steps:

1. First, you must find or create a Zip Repository containing the required driver. In our case, there was one available for download that contained the proper driver.
2. Repeat the steps listed in the previous section to add this file as a Zip Repository.
3. Click the **Image Profile** tab
4. Right-click the Profile that you wish to use, and select **Clone**.
5. From the drop-down labeled **Acceptance**, select **CommunitySupported**, as this will allow you to edit the Profile to include files that are not directly supported by VMware.
6. Click **Next**, then **Finish**.
7. Once completed, click the **Image Profile** tab.
8. Locate and right-click your copied version of the Profile, and select **Add Software Packages**. Select the desired file (in our case, the driver for our NIC), and click **Next**, then **Finish**.
9. Now, with all files successfully copied into the Software Depot, you select the **Deploy Rule** tab.
10. Right-click in the blank area below the **Active** and **Editable** subheadings and select **Add.**
11. Name the rule, and click **Next**.
12. Select from the list your desired Image Profile, choosing the -standard (not s-standard) option. Click **Next**.
13. Select the folder/Datacenter where you would like to house this rule, click **Next**.
14. Select a Host Profile (we have not created one yet, so skip), and click **Next**.

15. Select Host Rules (none configured yet), or choose to **Apply to any hosts**. Click **Next**.
16. Review selections and click **Finish**. Expect this process to take a few minutes.
17. Right-click your new rule, select **Active**. If all configurations are correct, you are now able to test the process of PXE booting one of your service workstations as a diskless ESXi host.

Chapter 5. vCSA Host Configuration

This chapter describes the configuration of hosts once they are running ESXi and have been connected to the vCSA and vSphere.

After the hosts have been successfully PXE booted and are showing in the Hosts and Clusters section in vSphere, complete the following changes in either the vSphere Desktop Client or the vSphere Web Client.

Repeat the following steps for each host. All of your hosts will then retain persistent access to configurations and storage. This will hold even after rebooting the hosts.

Link the Diskless Hosts to Persistent Storage

This section covers how to connect the host machines to a datastore for VM storage and access, as well as how to configure the host to store syslogs and configuration data remotely.

Connect Hosts to Datastore

In the vSphere Client, make the following configurations:

1. In the navigation bar, click **Home** and select **Hosts and Clusters**.
2. Click the IP address to select one of your diskless hosts, and in the right pane, navigate to the **Configuration** tab.
3. Select **Storage** from the **Hardware** list on the left side. Click **Add Storage** on the upper right.
4. Select **Network File System** and click **Next**.
5. Enter the IP address of your file server, the path to the share folder, and the Datastore name. Click **Next**, then **Finish**.

Set Host syslogs to be Stored on the Server

1. Remaining in the **Configuration** tab, select **Advanced Settings** from the **Software** list in the left pane.
2. Expand **syslog**, and select **global.** In the **Syslog.global.logDir** field, enter the Datastore path of your desired log output location. It should look like this: `[Name_of_Datastore] Name_of_folder`
3. Click **OK**. Configure Diskless Hosts

Assign Admin Password to Hosts

In the vSphere Client, follow these steps to assign an admin password to the hosts:

1. In the Navigation Bar, select **Home**. Under the **Management** sub header, select **Host Profiles**.

2. In the left pane, right-click the Host Profile that you wish to edit and select **Edit Profile**.
3. In the left pane, expand **Security configuration** and select **Administrator password**.
4. Select **Configure a fixed administrator password** from the drop-down menu in the right pane.
5. Enter and confirm your password, click **OK**.

Alter the Host Security Settings to Allow Network Connection to VM Serial Port

Setting this configuration within the vSphere Client allows the end user to connect to and see a running virtual machine's console through the Netlab web interface. If this step is not completed properly, remote interaction with the virtual machines will be limited to startup and shutdown via Netlab.

1. In the navigation bar, click **Home** and select **Hosts and Clusters**.
2. Click the IP address to select one of your diskless hosts, and in the right pane, navigate to the **Configuration** tab.
3. Select **Security Profile** from the **Software** list in the left pane.
4. Click **Properties** in the upper right of the **Firewall** section of the page.
5. Select the option called **VM serial port connected over network**.
6. Click **OK** to save and exit.

Enable SSH on the Host

The CCL system utilizes an SSH session between the vCSA and each host to gracefully shutdown VMs that may be left running at the end of CCL hours. This connection is also used to send the power off command to each host at that time.

1. Remaining in the **Configuration** tab, select **Security Profile** from the **Software** list in the left pane.
2. Under **Services**, select **Properties**.
3. Select **SSH**, then click **Options.**
4. Click **Start and Stop with host**. This change will not take effect until the next time that the workstation reboots.
5. Click **OK** and finish.

In order for the vCSA to be able to SSH into the hosts when you schedule it to do so, you will first have to do it manually and accept the option of saving the SSH key. This will then allow the vCSA to enter an SSH session later without requiring this type of user input.

Enable the Host to Automatically Startup and Shut Down Virtual Machines

For these hosts, you will not need to start any VMs automatically; these steps are for enabling VM shutdown. In order for this to work, you will

have to install VMware Tools on all of your virtual machines. VMs that do not have VMware Tools installed will not shut down, and may be corrupted when the host is powered off.

1. Remaining in the **Configuration** tab, select **Virtual Machine Startup/Shutdown** from the **Software** list in the left pane.
2. Click **Properties** in the upper right corner of the window.
3. Select **Allow virtual machines to start and stop automatically with the system.**
4. In the field marked **Default Shutdown Delay**, enter a value of **0**, as you want the VMs to begin shutdown as soon as they receive the command.
5. From the drop-down menu, select **Guest Shutdown**.
6. Click **OK** to save and exit.

Add SAFETY NET vSwitch to Host for Virtual Machines

When creating virtual machines in the CCL system, you must choose a vSwitch for them to connect to. In order to better control your virtual environment, you will want this vSwitch to exist without connection to a physical adapter.

1. Remaining in the **Configuration** tab, select **Networking** from the **Hardware** list in the left pane.
2. Click **Add Networking…** in the upper right corner of the window.
3. Select **Virtual Machine** as the connection type, click **Next**.
4. Choose **Create a vSphere standard switch**, *do not select a physical interface for this connection*. Click **Next**.
5. Enter a name for this network, such as SAFETY NET. Click **Next**. Review configurations, and click **Finish**.

NOTE: The following configuration allows the use of larger packet sizes in the network in order to speed up file transfer. However, testing in some environments has shown this setting to cause errors.

Set Hosts to Work with Large MTU Sizes

There have been some issues with ESXi 5.5 and large MTU sizes, this step may or may not work depending on your setup.
Remaining in the vSphere Client, follow these steps to ensure that the hosts will accept large-sized MTU transmissions across the network:

1. In the Navigation Bar, select **Home**. Under the **Management** sub header, select **Host Profiles**.
2. In the left pane, right-click the Host Profile that you wish to edit and select **Edit Profile**.
3. Expand **Network configuration**, **vSwitch**, **vSwitch0** and select **MTU Policy**.
4. Select **Assign the specified MTU** from the drop-down menu in the right pane.

5. Enter and your desired MTU size.
6. Remaining under **Network configuration**, expand **Host port group** and **Management Network**.
7. Select **MTU policy**.
8. Select **Assign the specified MTU** from the drop-down menu in the right pane.
9. Enter and your desired MTU size. Click **OK**.

Create and Apply Host Profiles

This section covers the process of creating and applying Host Profiles to individual hosts. This ensures consistent performance from the diskless hosts upon each boot.

Create Host Profiles

Remaining in the vSphere Client, follow these steps to create Host Profiles:

1. Right-click the IP address representing the host in the left pane, mouse over **Host Profile**, and select **Create Profile From Host**.
2. Enter a unique name for each host profile, click **Next**. Click **Finish**.

Attach Host Profiles

Remaining in the vSphere Client, follow these steps to assign specific Host Profiles to each host:

1. In the Navigation Bar, select **Home**. Under the **Management** sub header, select **Host Profiles**.
2. In the left pane, right-click the Host Profile that you wish to work with and select **Attach Host / Cluster**.
3. Navigate to the Host IP that you wish to attach, and select it.
4. Click **Attach**, then **OK**.

Apply Host Profiles

Remaining in the vSphere Client, follow these steps to apply the Host Profiles that have been assigned:

1. In the Navigation Bar, select **Home**. Under the **Inventory** sub header, select **Hosts and Clusters**.
2. Right-click the IP of the desired Host and select **Enter Maintenance Mode**. Click **OK** to confirm.
3. When the Host has entered Maintenance Mode, right-click the Host IP.
4. Mouse over **Host Profile** and select **Apply Profile**. Click **Finish** to apply changes.
5. After the task has completed, right-click the Host and select **Exit Maintenance Mode**.

Chapter 6. Automating the CCL Environment

In this Chapter, the processes involved in the automation of the CCL system are described. Once completed, these steps allow the CCL to run as desired without regular human intervention.

These tasks require that the vCSA be configured exactly as described in Chapter 3. If the vCSA is not configured correctly, or does not have the proper packages installed, these automation methods will not work as designed.

Topics in this chapter include creating SNMP scripts to change CCL connected switch ports from one VLAN to another, scripts for using WoL packets to wake multiple hosts simultaneously, and scripts that utilize an SSH connection to hosts in order to gracefully shut down running virtual machines before powering off the host. Also covered in this chapter is how to utilize Crontab to schedule these scripts to run exactly when you want them to.

SNMP Scripts

This section covers the process of creating and configuring your SNMP scripts. These will be used by the vCSA to alter network switch settings, placing CCL connected switch ports in the correct VLAN based on system status. For normal classroom operation, the ports will be in what we will refer to as CLASSROOM VLAN. During CCL hours, those ports will be in what we will refer to as CCL VLAN.

In order to perform this portion of CCL configurations, you must first identify the OID associated with your switch/interfaces. These will be necessary for implementation of this setup.

All tasks described in this chapter are completed from within the vCSA command line interface.

Replace CCL VLAN and CLASSROOM VLAN with the number of the VLAN that you are using. Change the script file names (.sh) to reflect your organization's naming conventions.

Configure SNMP Script to Change Ports to CCL VLAN

1. In the vCSA console, enter the following commands at the root level to create your script file and make it executable:
   ```
   #touch CCLnet.sh
   #chmod 777 CCLnet.sh
   ```
2. Issue the command `#vi CCLnet.sh` to enter the script file in the vi editor.

3. The following string is designed to move switch port g1/0/2 on the 192.168.1.1 switch into CCL VLAN:

```
snmpset -v 1 -c <private snmp string>
192.168.1.1
1.3.6.1.4.1.9.9.68.1.2.2.1.2.10102 integer
<CCL VLAN>
```

4. Repeat this line for each switch port that you wish to include when changing VLANs, altering the string only to account for the identity of each port.

Configure SNMP Script to Change Ports to CLASSROOM VLAN

1. In the vCSA console, enter the following commands at the root level to create your script file and make it executable:

```
#touch Windowsnet.sh
#chmod 777 Windowsnet.sh
```

2. Issue the command `#vi Windowset.sh` to enter the script file in the vi editor.
3. The following string is designed to move switch port g1/0/2 on the 192.168.1.1 switch into CLASSROOM VLAN:

```
snmpset -v 1 -c <private snmp string>
192.168.1.1
1.3.6.1.4.1.9.9.68.1.2.2.1.2.10102 integer
<CLASSROOM VLAN>
```

4. Repeat this line for each switch port that you wish to include when changing VLANs, altering the string only to account for the identity of each port.

Wake on LAN Scripts

This section covers the process of creating and configuring your WoL scripts. These will be used by the vCSA to send a WoL packet to powered-off hosts. This will wake the host and instruct it to begin the PXE boot process.

Hosts must be shut down completely in order for this process to work. Hosts that are in “Sleep” or “Hibernation” modes will simply wake to their normal operating systems, failing to enter the PXE process and will not be available as CCL resources. The settings described in the “Lab Workstations” section of Chapter 2 are necessary to ensure that your hosts will perform as desired for this section.

To ensure that all hosts wake when they are needed you should only wake half at a time (depending on the number of machines involved), and run each script in Crontab more than once. This section includes only a single example of the script that will be used for this process. Depending on the size of your lab, you may need to break it into several sections, each of which would need a separate version of this script.

Configure Wake on LAN Script(s)

The `-i` option used in the wol commands is used to ensure that the packet will be sent out through the correct network interface on the vCSA.

1. In the vCSA console, enter the following commands at the root level to create your script file and make it executable:
   ```
   #touch CCLwakeup.sh
   #chmod 777 CCLwakeup.sh
   ```
2. Issue the command `#vi CCLwakeup.sh` to open the script file in the vi text editor.
3. In the text editor, enter the following string for each host MAC address in your lab, each on a separate line:
   ```
   wol -i <CCLnet broadcast address> <host MAC address>
   ```
4. Repeat this line for each host that you wish to wake, altering the string only to account for the MAC address of each host.

SSH / Host Control Scripts

This section describes the steps necessary to create scripts that will open and use an SSH connection with each host. This connection will be used for two tasks; gracefully shutting down all running VMs, and powering off the host itself.

In order for the vCSA to be able to establish an SSH connection with the hosts without manual intervention, the *sshpass* software package must be installed in the vCSA. If you have not done so, refer to the "Add Required Packages to the vCSA" section of Chapter 3.

Before any of the SSH tasks can be automated, you must first manually initiate an SSH connection with each host from the vCSA command line in order to accept and save the SSH keys that will be generated.

As with the WoL scripts, you may want to break your lab into smaller groups for this process. For example; if you are waking the hosts in two groups, you should use those same two groups for the SSH scripts.

Configure SSH Script to Shut Down VMs

1. In the vCSA console, enter the following commands at the root level to create a file that this script will be looking to for the needed SSH password:
   ```
   #touch /etc/hostpw
   ```
2. Issue the command `#vi /etc/hostpw` to enter the file in the vi editor.

3. In the text editor, enter the password to be used on the first line. Nothing else should be in this file.
4. Remaining in the vCSA console, enter the following commands at the root level to create your script file and make it executable:
   ```
   #touch VMshutdown.sh
   #chmod 777 VMshutdown.sh
   ```
5. Issue the command `#vi VMshutdown.sh` to enter the script file in the vi editor.
6. In the text editor, enter the following string for each host on a new line:
   ```
   sshpass -f /etc/hostpw ssh -l root <host IP> /sbin/vmware-autostart.sh stop
   ```
7. Repeat this line for each host in your CCL lab, altering the string only to account for the IP address of each host.

Configure SSH Script to Power off Hosts

1. In the vCSA console, enter the following commands at the root level to create your script file and make it executable:
   ```
   #touch HostPowerOff.sh
   #chmod 777 HostPowerOff.sh
   ```
2. Issue the command `#vi HostPowerOff.sh` to enter the script file in the vi editor.
3. In the text editor, enter the following string for each host on a new line:
   ```
   sshpass -f /etc/hostpw ssh -l root <hostIP> /sbin/poweroff
   ```
4. Repeat this line for each host in your CCL lab, altering the string only to account for the IP address of each host.

Crontab

This section describes the process of setting up Crontab in the vCSA to create a schedule for running the automation scripts. Before completing this section, be sure that your vCSA time and date are configured correctly.

As a matter of course, it is a good idea to run multiple iterations of each of your scripts, about a minute apart from one another. That way, if one fails for any reason, the repeat command should pick up any hosts left out.

The following example includes only one entry for each of the required automation tasks. Your CCL setup may require additional entries, as well as redundant executions of each.

Configure Crontab to run CCL Automation Tasks

1. Enter the following command in the vCSA console with root privileges to enter the crontab file and begin configurations:
   ```
   #crontab -e
   ```
2. The required syntax for crontab follows:
   ```
   * * * * * command
   | | | | |
   | | | | |
   | | | | |--- day of week (0 - 7)
   | | | |------- month (1 - 12)
   | | |----------- day of month (1 - 31)
   | |--------------- hour (0 - 23)
   |------------------- minute (0 - 59)
   ```
3. First, enter the job for changing switch ports into the CCL VLAN:
   ```
   00 21 * * 1-5 ./CCLnet.sh
   ```
   This will execute the `CCLnet.sh` script Monday through Friday at 9:00 PM.
4. Skip a line, then enter the job for sending the WoL packet to the host machines:
   ```
   01 21 * * 1-5 ./CCLwakeup.sh
   ```
   This will send a wol packet to the listed MAC addresses Monday through Friday at 9:01 PM.
5. Skipping another line, the next job to enter will gracefully shut down all running VMs at the end of CCL hours:
   ```
   00 05 * * 1-5 ./VMshutdown.sh
   ```
   This will execute the command to shutdown VMs Monday through Friday at 5:00 AM.
6. The next job will power off the host at the end of CCL hours:
   ```
   10 05 * * 1-5 ./HostPowerOff.sh
   ```
   This will execute the poweroff command and shut down the host Monday through Friday at 5:10 AM. This allows time for the VMs to shutdown prior to cutting power to the host.
7. Next, enter the job that will change switch ports back into the normal classroom VLAN:
   ```
   00 06 * * 1-5 ./Windowsnet.sh
   ```
   This will execute the `Windowsnet.sh` script Monday through Friday at 6:00 AM, returning the lab network to normal classroom operations.

Conclusion/Next Steps

Now that the back end of the Cloud Computing Lab is configured, the CCL system is ready for testing and implementation. The system may be tested in-place and as-is without further configuration or being tied in to a front end/user portal.

As stated in the beginning of this document, the CCL system at DTCC uses NDG NETLAB+ hardware and software (NetLab Website) to provide the front end/user interface. This requires the upfront expense of purchasing Network Development Group hardware, as well as the ongoing cost of an annual license fee for NETLAB Academy Edition.

Alternative front end solutions do exist, including free and open-source options. At this point, the CCL system is fully configured and ready to begin integration with the front end of your choosing. If your institution has a license with NDG, refer to their documentation at NetLab Documentation to begin. If you choose to use a different front end option, refer to the documentation supplied with that specific solution.

Appendix: Reference Images and Screenshots

This appendix is intended to serve as a basic reference and contains images of the different interfaces that are used in the configuration of the Cloud Computing Lab. Software versions may differ slightly, resulting in an appearance different from what is depicted in these images.

Images included in this section include basic screenshots of the various software components, more focused shots of specific directories, and examples of various configuration files used in the CCL system.

Configuration Interfaces

Images in this section are of the various interfaces used in configuring the CCL system. These images are intended to help familiarize you with the different software components.

vSphere Desktop Client

The vSphere Desktop Client is where the vast majority of CCL configuration takes place. It is a good idea to get to know this software and be able to navigate comfortably within it. Also shown is an image of the vSphere Web Client for comparison.

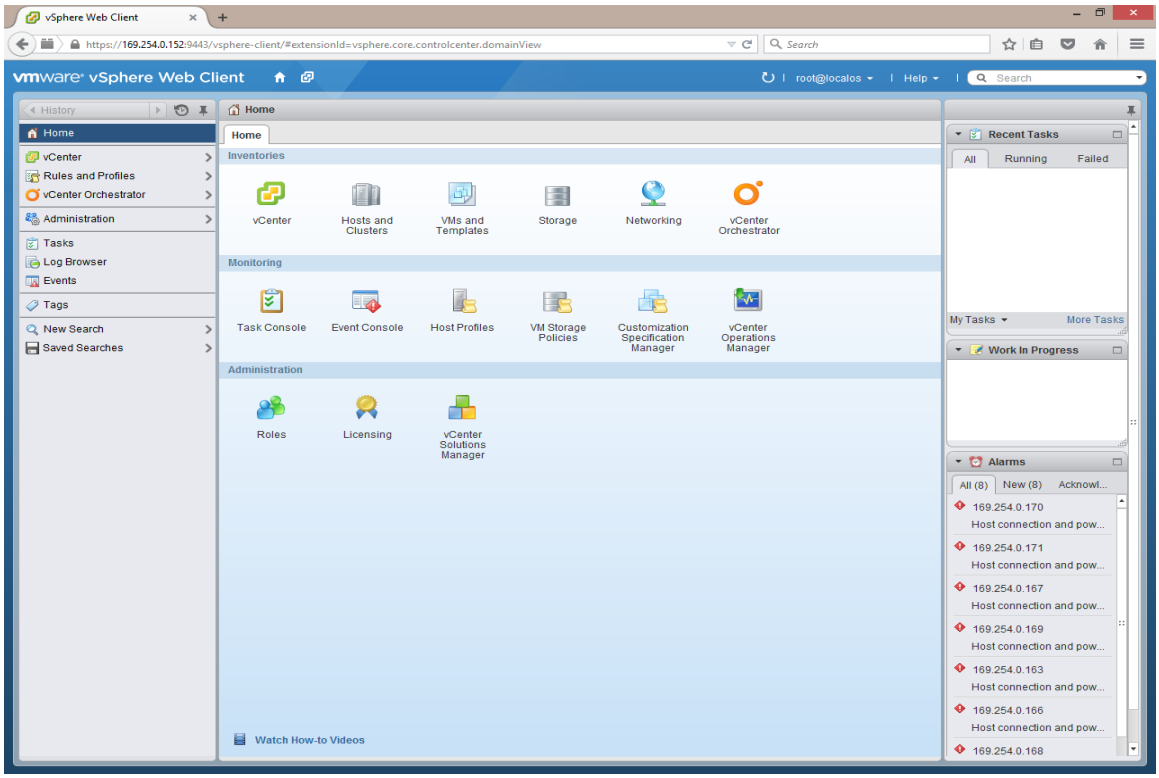


Figure: Image of vSphere Web Client "Home" menu.

Openfiler Web Admin Interface

Aside from the initial setting of a static IP address, all Openfiler configurations are completed through this interface. Included here are images of the Openfiler Web Admin Interface home screen, as well as views of the other main areas where CCL configuration takes place.

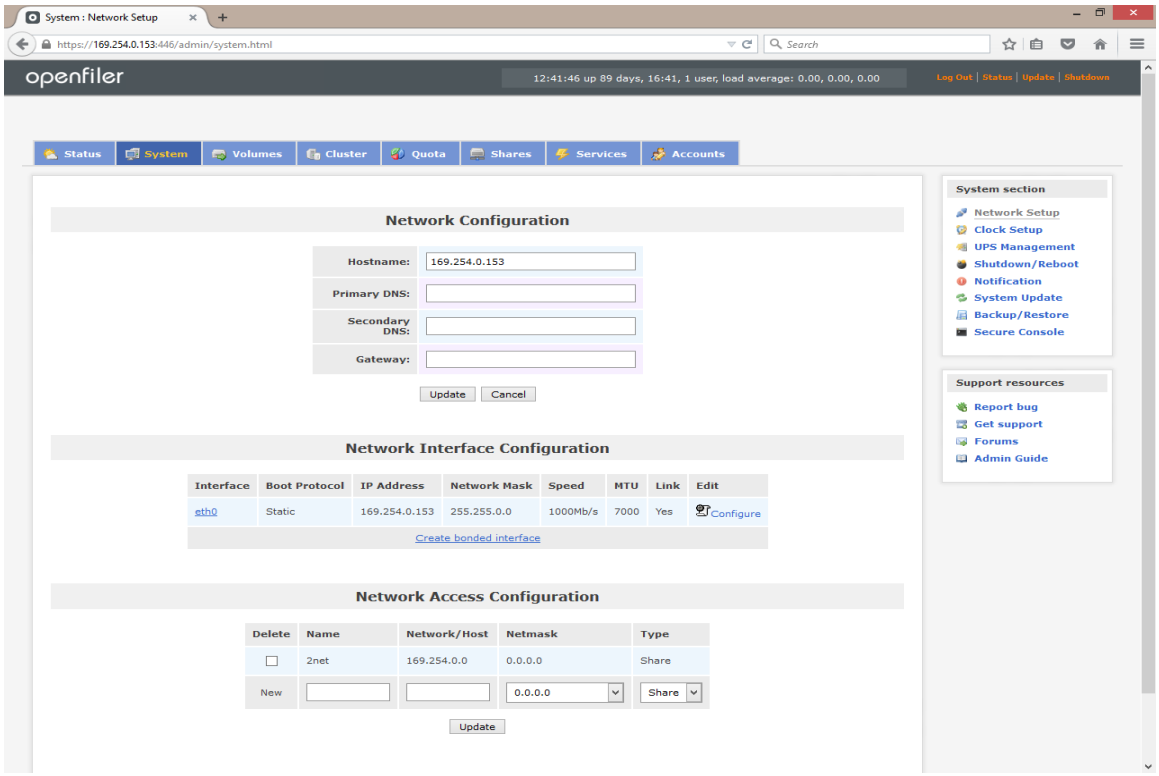


Figure: Image of Openfiler Web Admin Interface "System" tab.

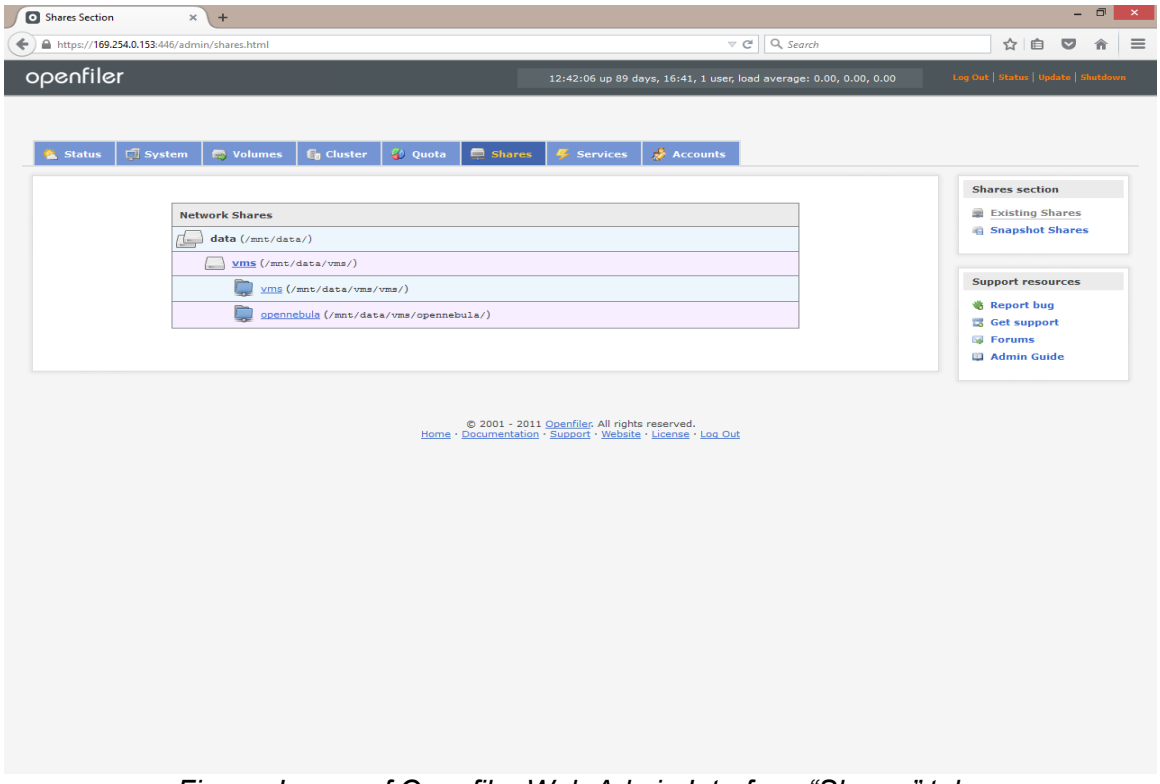


Figure: Image of Openfiler Web Admin Interface "Shares" tab.

vCenter Server Appliance Web Admin Interface

Once the vCSA is deployed, some initial configurations must be made in the Web Admin Interface. This section provides a view of the home screen and the menu tabs available.

Configuration File Examples

Images in this section depict some of the key configuration files that are altered in the creation of the CCL system. These images are intended to be used as a supplemental reference, not to replace the step-by-step instructions of previous chapters.

DHCP Configuration Files

Completed within the command line of the vCSA, these images are examples of properly configured DHCP files.

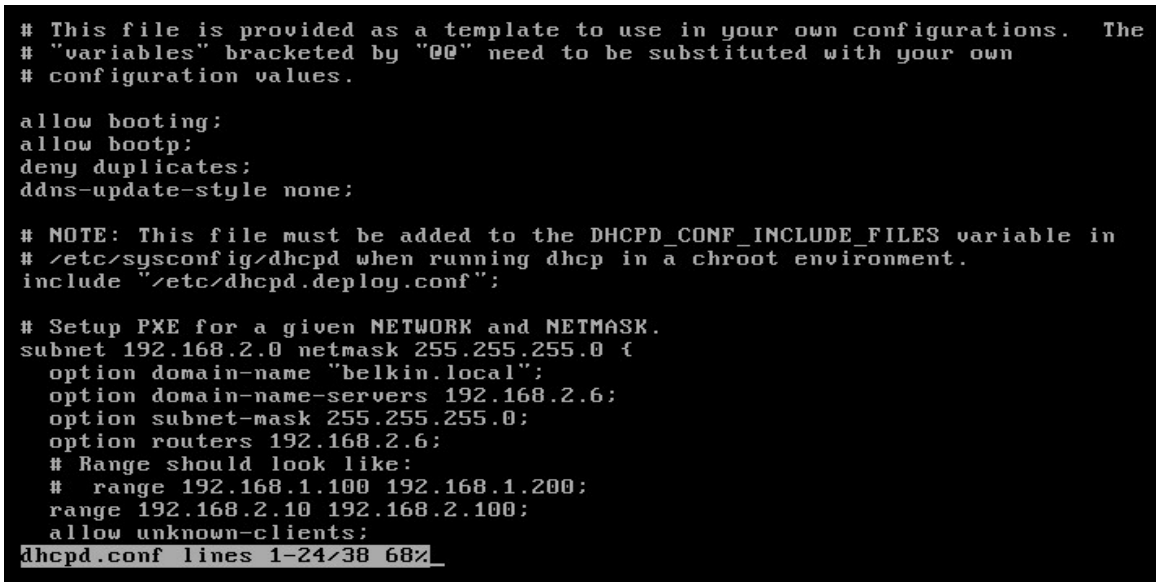


Figure: Image of /etc/dhcpd.conf configured without static IP assignments.

ATFTP Configuration Files

Completed within the command line of the vCSA, these images are examples of properly configured ATFTP related files.

```
## Path:     Network/FTP/Atftpd
## Description: ATFTP Configuration
## Type:     string
## Default: "--daemon "
#
# atftpd options
#
ATFTPD_OPTIONS="--daemon --user root "

## Type:     yesno
## Default: no
#
# Use inetd instead of daemon
#
ATFTPD_USE_INETD="no"

## Type:     string
## Default: "/srv/tftpboot"
#
#  TFTP directory must be a world readable/writable directory.
#  By default /srv/tftpboot is assumed.
#
ATFTPD_DIRECTORY="/srv/tftpboot"

atftpd lines 1-24/32 62%
```

Figure: Image of /etc/sysconfig/atftpd file properly configured.

```
vCenterServerAppliance:/tftpboot # cd pxelinux.cfg/
vCenterServerAppliance:/tftpboot/pxelinux.cfg # ls
default
vCenterServerAppliance:/tftpboot/pxelinux.cfg # less default
DEFAULT /esxi/media/menu.c32
MENU TITLE ESXi-5.5.0-20140902001-standard Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL /esxi/media/mboot.c32
  APPEND -c /esxi/media/boot.cfg
  MENU LABEL ESXi-5.5.0-20140902001-standard ^Installer
LABEL hddboot
  LOCALBOOT 0x80
  MENU LABEL ^Boot from local disk
default lines 1-12/12 (END)
```

Figure: Image of /tftpboot/pxelinux.cfg file configured properly.

CCL Automation Files

Completed within the command line of the vCSA, these images are examples of files that are necessary for the automation of tasks in the CCL. Included are examples of the scripts described in Chapter 6, as well as an image of a properly configured crontab file.

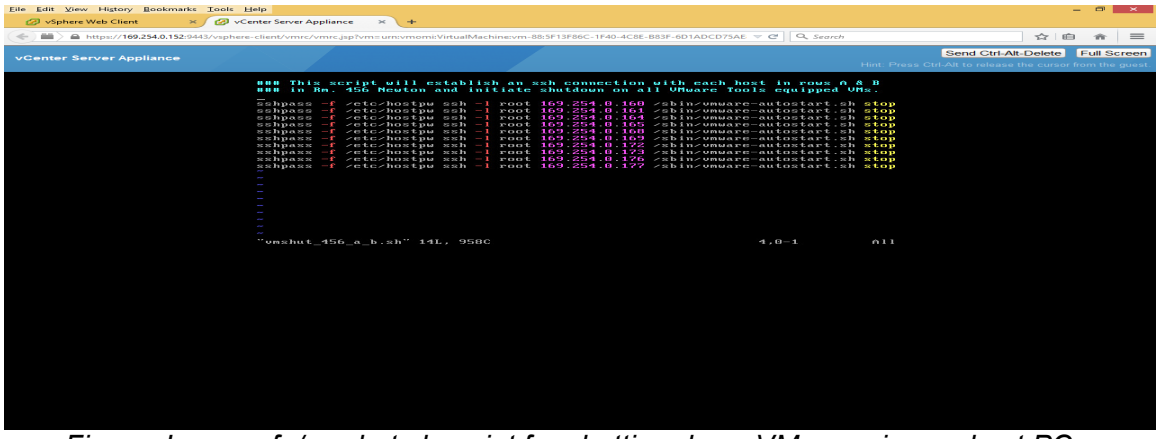


Figure: Image of ./vmshut.sh script for shutting down VMs running on host PCs.

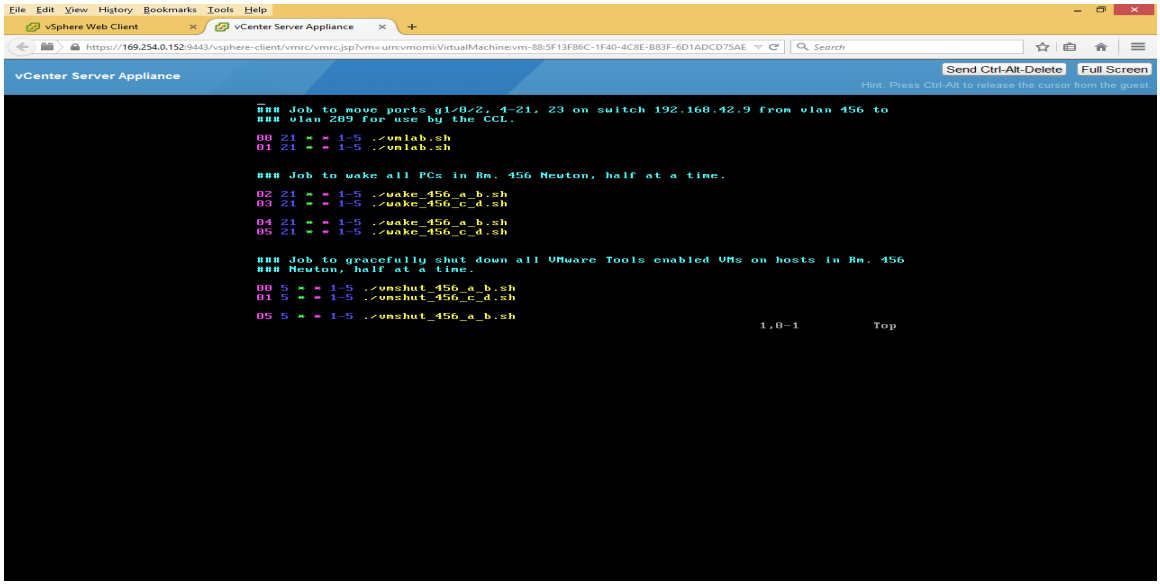


Figure: Image of crontab -e configured to work as needed for the CCL system.