

Overview

This project seeks to demonstrate the implementation of internal networked services for a commercial enterprise. Specifically, we will set up a Windows Server VM that will provide several services, such as NTP, DNS, NFS, and Active Directory. We will also set up a Debian VM server with DNS and OpenSSH. These services provide valuable functions to a business such as accessing shared documents, maintaining consistent logins across workstations, and allowing easier remote management of workstations while increasing overall security. Since many of the above aspects have been done this semester on Linux-based systems, our goal is to duplicate these services on a Windows server that is integrated with a Linux-based platform to demonstrate real world applicability.

Implementation

Create the Infrastructure

Note: Text in Courier New font and highlighted in gray are to be typed as commands.

Information Tables

Description	IP Address	DNS Names	Services
Windows Server VM	192.168.1.10	winkoi-2012.fantom.koi dns.fantom.koi time.fantom.koi	AD, Master DNS NTP NFS
Debian Server VM	192.168.1.20	debian.fantom.koi	Slave DNS
Windows 7 VM	192.168.1.101		AD client

Windows 2012 Server

Background Information: Windows Server 2008 vs. 2012

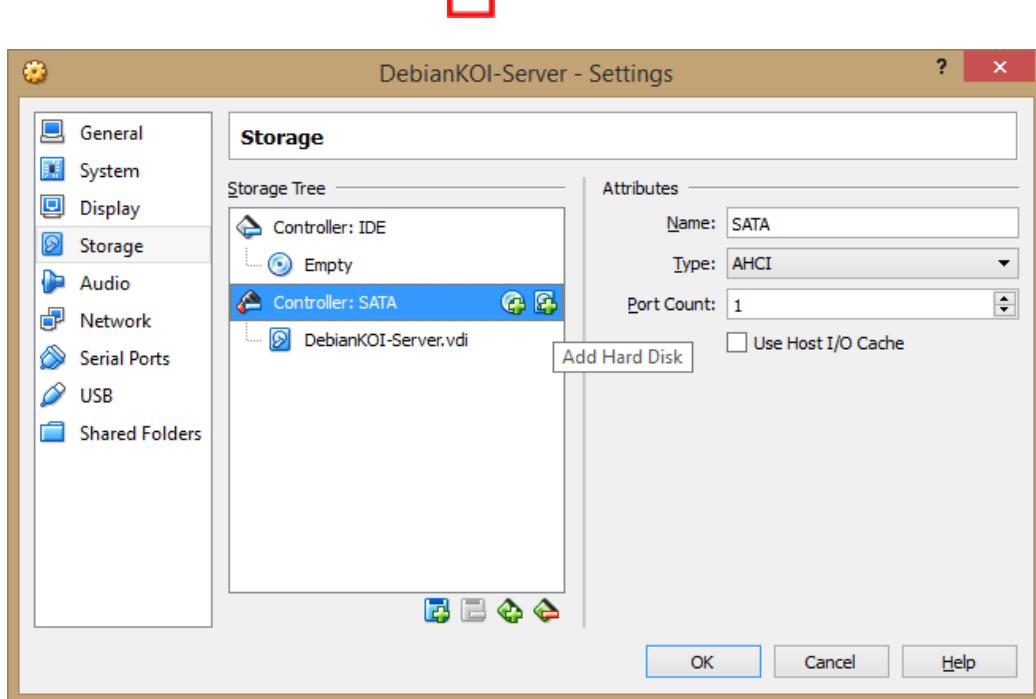
When compared to Windows Server 2008 the most noticeable difference in Windows Server 2012 is the GUI. The 2008 version is Vista based and uses IIS7, while the 2012 version is Windows 8 based and uses IIS8.5. The GUI in the 2012 Virtual Machine acts and looks very much like Windows 8, while the 2008 looks and feels like Windows XP. There are also updates to services such as Active Directory and includes a new version of Hyper-V. There are also many security-related features in the 2012 version.

Virtual Machine Setup

In this section, MS Windows Server 2012 R2 Datacenter with 64-bit Update is used.

1. Set the Memory Size to 4096 MB (4 GB).
2. Set the size of the VM to 25 GB.
3. From the list, select the Windows Server VM and choose Settings.
4. Select System from the left panel.
 - a. Make sure network is checked.
 - b. Under the Processor tab, set Processor(s) to 2.
5. Select Network from the left panel.
 - a. Check Enable Network Adapter.
 - b. For Attached to, select Bridged Adapter.
6. Select Shared Folders from the left panel.
 - a. Click on the folder with the green plus icon.
 - b. Browse to a desired folder.
 - c. Select Auto-mount.

7. Next, highlight Controller: SATA and select the Add Hard Disk icon.



Adding a Hard Disk for the Controller: SATA

- a. Select Choose existing disk.
 - b. Browse to the image of the MS Windows Server 2012 R2 Datacenter and select it.
8. Save and close the settings.

Virtual Machine Installation

Note: Any steps not mentioned here are left at the default values.

1. Select the default settings for language, keyboard, and USB.

2. Enter the product key (in this project, the key was obtained from DreamSpark).
3. Select the GUI option.
4. Select Custom Install.
5. Select only Drive 0, and click Next.
6. Wait while the system installs...
7. Send the Ctrl+Alt+Del signal to the VM to begin (only Ctrl+Del), login, and start.

Server Configuration

At this stage, the Server Manager Dashboard screen should appear, along with the network screen. All of the steps below can be executed in PowerShell, but for timeliness and simplicity, many of the configurations detailed below are presented as GUI-based operations, except in instances where it was simpler or perhaps necessary to use PowerShell.

NTP Configuration

Network Time Protocol (NTP) is used to sync clocks between different computers over the network. It is helpful to set up a NTP server inside your network to allow you to synchronize all your logs in one place.

Note: Backups should be made prior to any changes that are made to the registry.

1. Open PowerShell and type in the following lines:

```
PS C:\Users\Administrator>Stop-Service w32time  
PS C:\Users\Administrator>w32tm /config  
/manualpeerlist:"0.us.pool.ntp.org 1.us.pool.ntp.org  
2.us.pool.ntp.org" /syncfromflags:MANUAL /reliable:yes /update
```

The expected output should be “The command completed successfully.”

2. To further verify, type `regedit` into the PowerShell to access the Registry Editor.

3. Navigate to

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\TimeProvide  
rs\NtpServer
```

4. In PowerShell, type in the following line:

```
PS C:\Users\Administrator>Start-Service w32time
```

It is strongly recommend this configuration be applied to all domain controllers and possibly made into a Group Policy object as a startup script for the Domain Controllers organization unit within Active Directory. This is accessed through Server Manager > Tools > Group Policy Management > Forest > Domains > Domain Name > Group Policy Objects > Default Domain Controllers Policy > Right click to edit.

5. Setting the Time on Windows Server by right clicking on the clock (located on the bottom right-hand corner) and select Adjust date/time.
6. Check if the Internet Time tab is available. If yes, skip to step 5. If no, continue to step 3.
7. Open PowerShell and type in the following line:

```
PS C:\Users\Administrator> net stop w32time
```

The following output should be shown to the screen:

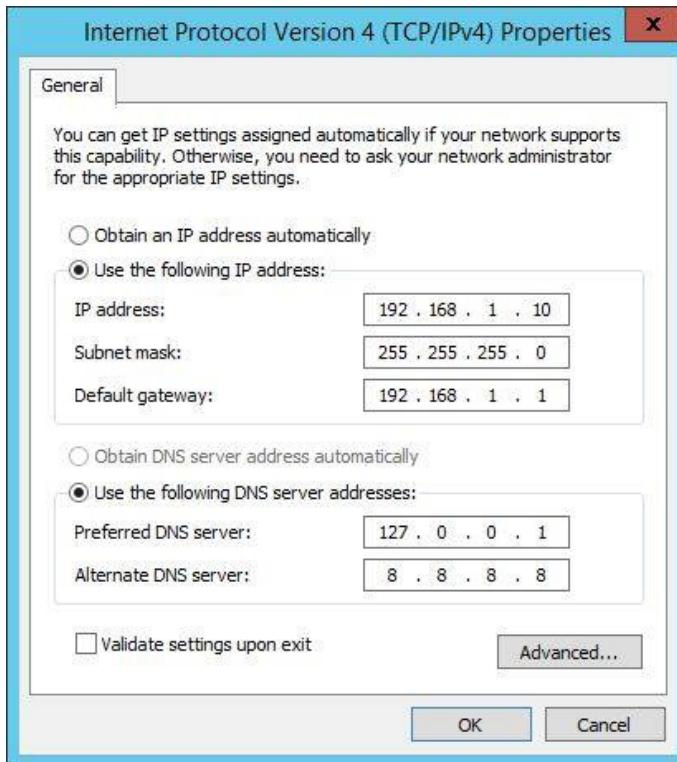
```
The Windows Time service is stopping.  
The Windows Time service was stopped successfully.
```

8. Again, right click on the clock (located on the bottom right-hand corner) and select Adjust date/time.
9. Select the Internet Time tab. The message “This computer is not set to automatically synchronize with an Internet time server” should appear.
10. Click Change settings and enter `time-c.nist.gov`
11. Select the Date and Time tab.
12. Change time zone to the desired time zone (In this case, (UTC-05:00) Eastern Time (US & Canada) was used).

Set Static Server IP

1. Change Computer Name [WinKOI-2012]
2. Public On setting (default), Windows Firewall Error reporting of this.
 - a. Select Yes send auto reports, notify of possible solutions.
3. Disable Remote Management.

4. For Ethernet, change the default DHCP value to Static to set up the DNS server role by going to Control Panel > Network & Internet > Network Connections.
5. Change IE Enhanced Security Config to OFF (ON by default).
6. Go to Control Panel > Network and Sharing Center > Ethernet > Properties, uncheck IPv6 and update IPv4 Properties as shown below.



Network settings for the Windows Server VM

Add Roles & Features: Active Directory, DNS and NFS

Active Directory

Active Directory (AD) authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory Domain Services (AD DS) stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches. AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that provides flexible support for directory-enabled applications,

without the dependencies that are required for Active Directory Domain Services (AD DS). AD requires a Domain Name Server (DNS) to be configured, so that all the computers in AD can talk to each other within the network.

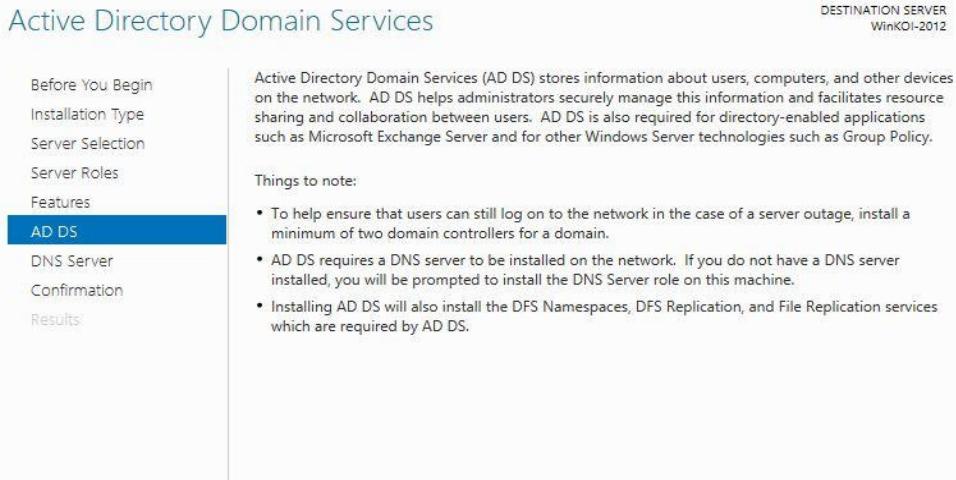
For more information, see <https://technet.microsoft.com/en-us/>

Active Directory Installation

1. From the Dashboard, click Add roles and features
2. Choose Role-based or feature-based installation
3. Select the default server pool (only one).
4. Go to AD: Domain services > Following Role Services required to install domain services.
5. Go to Remote server administrator tools > role administrator tools > AD DS and AD LDS tools > AD DS tools > AD Administrative Center > AD DS Snap-ins and command line tools.
6. Check Install management tools (if available).

Active Directory Configuration

1. Navigate to the notifications or to the AD DS in Server Management.
 - a. Promote this server to a domain controller.



Screenshot of the AD DS installation

2. Start the Deployment Configuration wizard.

3. Select Deployment operation: add new forest.
4. Specify the root domain name (in this case, fantom.koi was used).
5. Set the DRSM password.
6. Ignore pop-ups that relate to setting up DNS.
7. Verify NetBIOS domain name assigned to domain, which auto-fills in with fantom.
8. Use the default paths for:
 - a. Database folder & log files: C:\Windows\NTDS
 - b. SYSVOL folder: C:\Windows\SYSVOL
9. Make a backup copy of the PowerShell script auto-generated by the wizard.
10. Save and close.

NFS Installation

1. Select DNS Server, remote server administrator tools > role administrator tools> DNS Server Tools (check include management tools (if applicable) option).
2. Keep the default features.

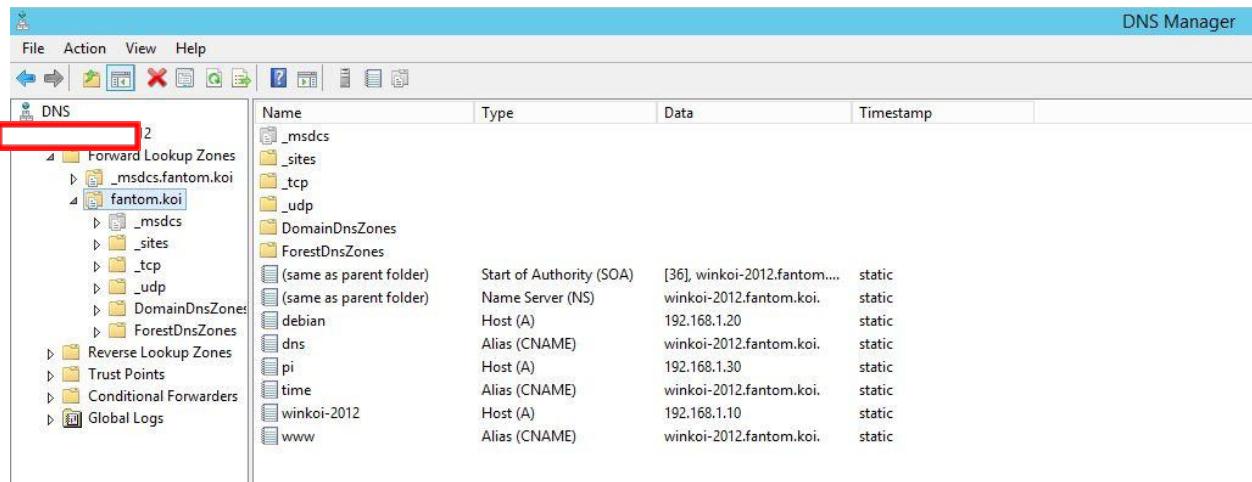
NFS Configuration

1. For File & Storage Services from the drop down sub-menu:
 - a. Select Server for NFS.
 - b. Select the defaults for services for network file system management.
 - c. Click install.
- 7.

DNS Configuration

- 1 . Access the Server Manager > Tools > DNS.
- 2 . Enter `winkoi-2012.fantom.koi` for the Forward Lookup Zone.
- 3 . Navigate to the Tools > DNS > Forward Lookup Zone > right-click on the domain name.
- 4 . Select properties to get to the dynamic updates and change to NONE.
- 5 . Select Reverse Lookup Zone from the left panel.

- 6 . Click on the Action tab in the menu bar and select Open Wizard for New Zone.
- 7 . For all DNS servers running on a domain controllers in this domain (fantom.koi), use the default values.
- 8 . Reverse lookup for IPv4.
- 9 . Enter **192.168.1** for the reverse lookup zone name (auto-completes reverse look up name: 1.168.192.in-addr.arpa).
- 10 . Ensure all machines are static at this stage.
- 11 . In this example, the Windows Server VM's IP address is **192.168.1.10** and the Debian Server VM's IP address is **192.168.1.20**
- 12 . Do not allow dynamic updates as before.
- 13 . On the left panel, right click the server name (WINKOI-2012 in this case) and select properties.



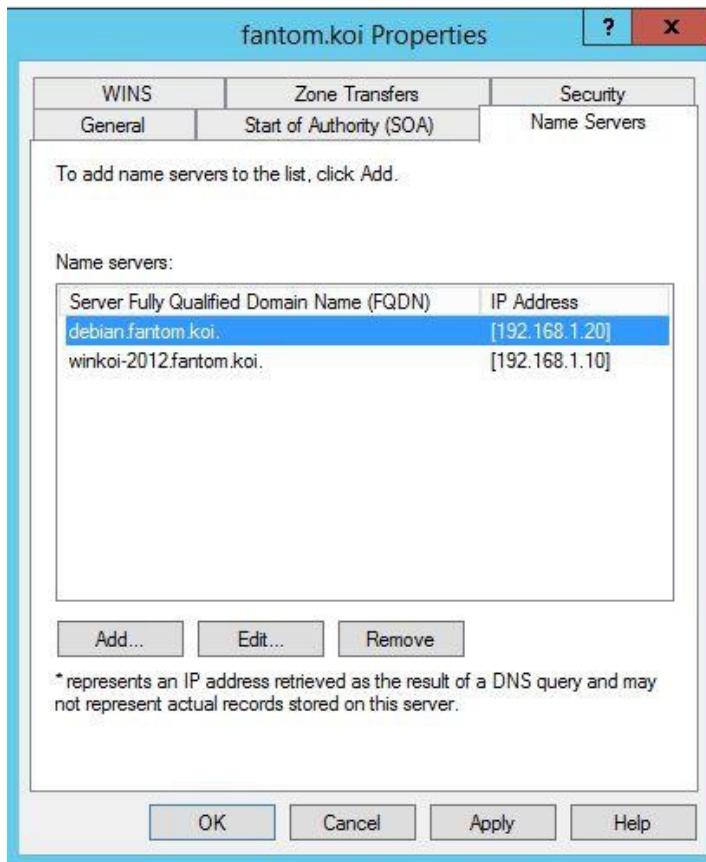
Screenshot of the DNS Manager

- 14 . Select the Forwarders tab and add **8.8.8.8** and **8.8.4.4**
- 15 . Select the Monitoring tab and check the following boxes:
 - a. Simple and Recursive query to DNS server.
 - b. Test now: passed for both.
 - c. Perform auto.testing at the following intervals and choose 10 minutes.

16 . Right click fantom.koi from the left panel (located underneath WINKOI-2012) and click properties.

17 . Select the Name Servers tab.

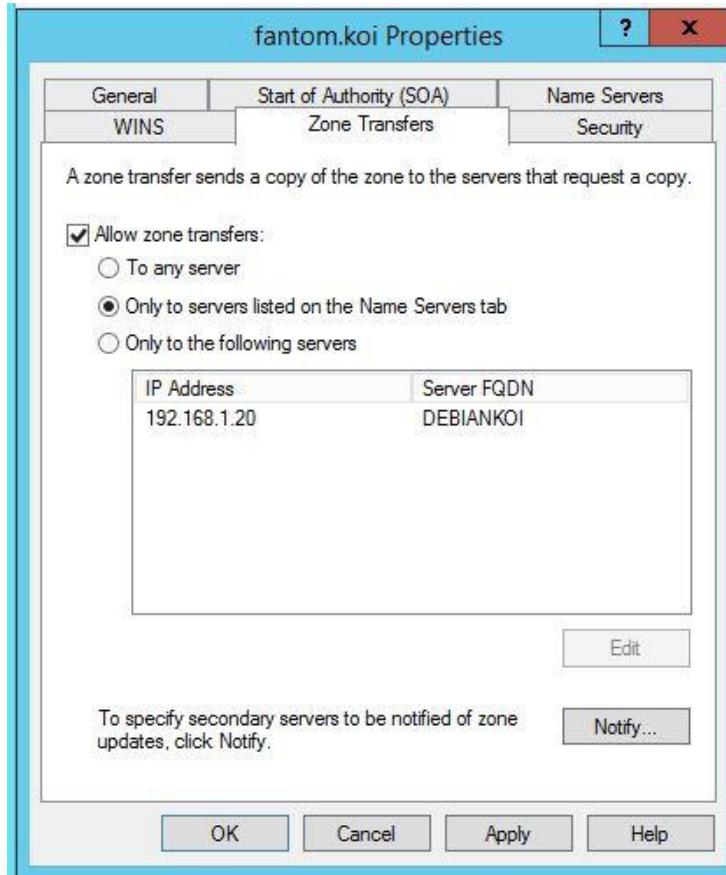
18 . Add the following information according to the figure below using the Add button:



Screenshot of the FQDN and IP addresses to be added

19 . Select the Zone Transfers tab in the same fantom.koi Properties window.

- a. Check Allow zone transfers.
- b. Check Only to servers listed on the Name Servers tab.
- c. Click the Notify button in the bottom right-hand corner and select Automatically notify: servers listed on the name servers tab.



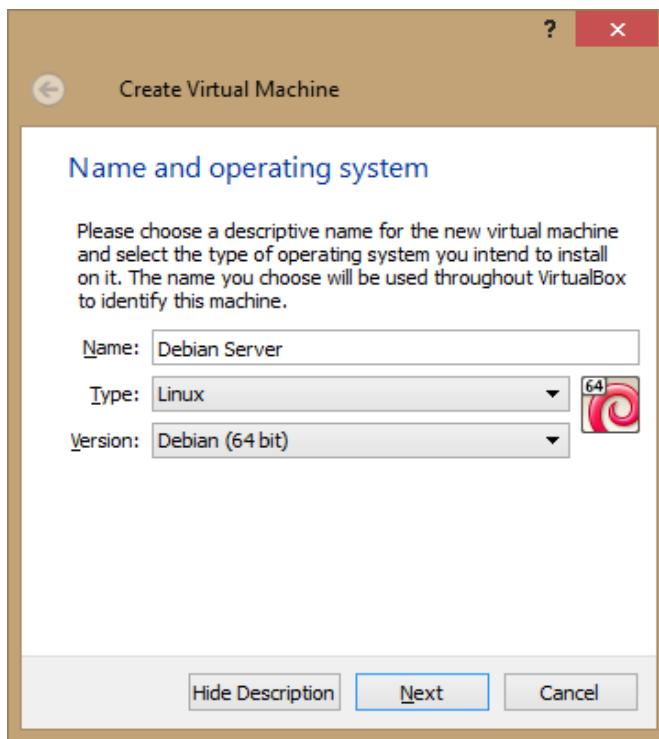
Screenshot of step 19 above

Debian Server

Virtual Machine Setup

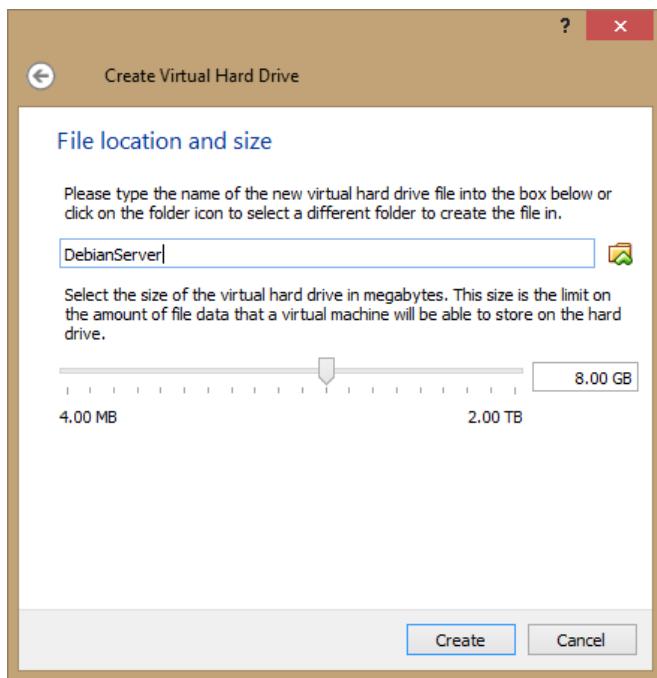
In this part, the Debian Server VM will be set up with the exact settings that will be specified below using Oracle VM VirtualBox software, using Debian GNU/Linux version 7.8.9 “Wheezy” is downloaded and used.

1. Open Oracle VM VirtualBox and select New.
2. Enter the information below. While the name isn't important, the type and version must be set to Linux and Debian (64 bit).



Entering the name, type and version of the Debian VM

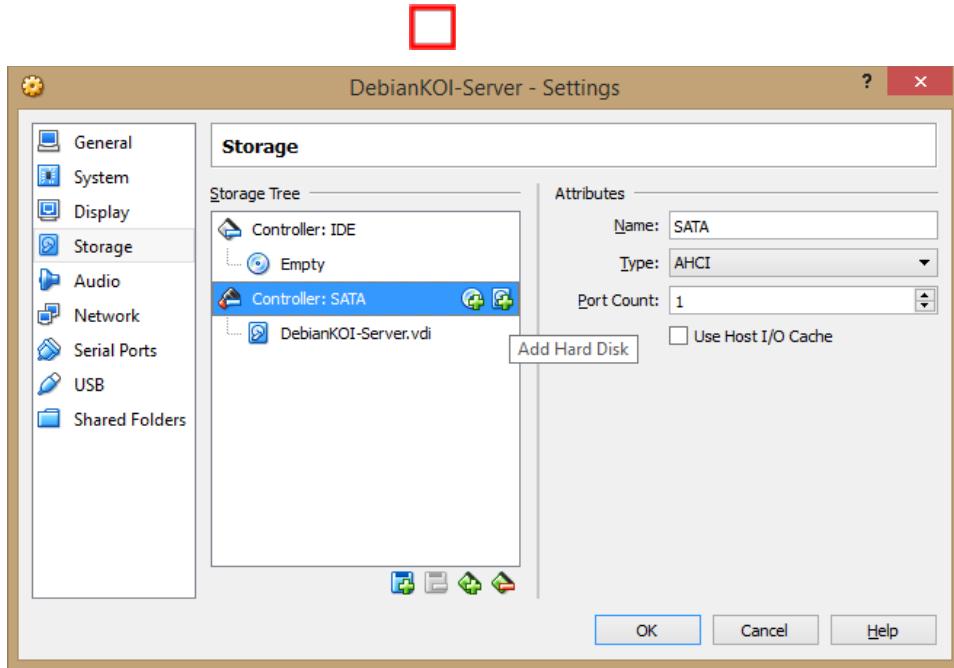
3. Set the Memory Size to at least 2048 MB.
4. Select Create a virtual hard drive now.
5. Select VDI (VirtualBox Disk Image).
6. Select Dynamically allocated.
7. Enter a name of the new virtual machine of your choosing, then set the size of the VM to 8 GB as seen below.



Selecting the location and size for the Debian VM

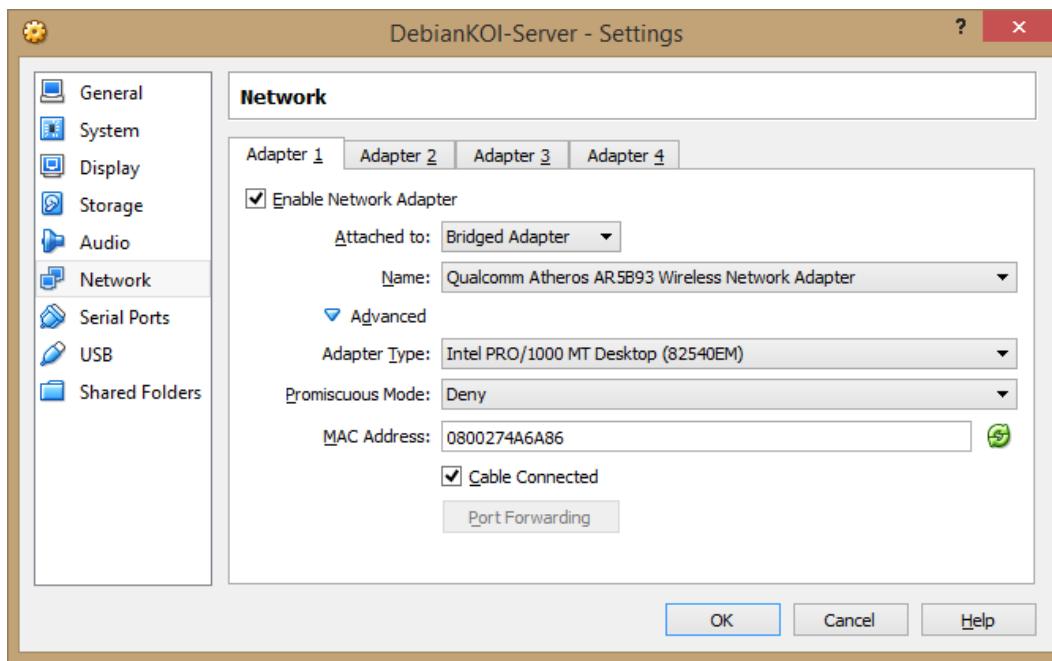
8. Click Create.
9. Select the newly created Debian Server VM and select Settings from up top.
10. Select Storage from the left panel.

11. Next, highlight Controller: IDE and select the AddDisk icon.



Adding an installation ISO to the Controller: IDE

12. Select Choose existing disk.
13. Browse to the image of the Debian GNU/Linux version 7.8.9 "Wheezy" and select it.
14. Again, access the Settings of the Debian Server VM. This time, navigate to System, click on the Processor tab and make sure that Processor(s) is 1.
15. Select Network from the left panel.
 - a. Check Enable Network Adapter
 - b. Select Attached to: Bridged Adapter



VirtualBox Network Settings for the Debian VM

16. Select Shared Folders from the left panel.
 - a. Click on the folder with the green plus icon.
 - b. Browse to a desired folder.
 - c. Select Auto-mount.
17. Save and close Settings.

NTP Configuration

1. Install NTP on the Debian Server VM by typing `apt-get install ntp ntpdate -y`
2. To ensure that NTP works with the Windows Server, type `ntpdate -q` `WINDOWS SERVER_IP` (In this project, the IP address is 172.16.1.10). Below is the output when NTP works with the Windows Server.

```
server 192.168.1.10, stratum 1, offset -0.163219, delay 0.04243
11 Apr 17:39:25 ntpdate[3757]: adjust time server 192.168.1.10
offset -0.163219 sec
```

- 3 . Open the /etc/bind/named.conf.options file
 - a. Set the DNS forwarder to “dns.fantom.koi”
 - b. Save and close the file.
- 4 . Sync the Debian Server’s time with the Windows Server
 - a. Open the /etc/ntp.conf file
 - b. Add “server time.fantom.koi” to that file.
 - c. Save and close the file.

Virtual Machine Installation

Note: Any steps not mentioned here are left at the default values.

1. Select the Debian Server VM from the list and click Start.
2. Select Advanced Install > Expert Install.

Note: It is recommended to go with advanced install since it allows for more customizations, which helps when tracing back the steps during troubleshoot.
3. Select default settings for Language, Keyboard, and USB.
4. Select and load the following installer components
 - a. fuse-modules-3.2.0.4-amd64-di
 - b. ntfs-modules-3.2.0.4-and64-di
 - c. openssh-clients-udeb
5. For the DHCP option, select autoconfig. This option was selected so the updates and packages could be retrieved. It was switched to static later on.
6. Enable Root login.
7. Next, set up the new user. Create a username and password of your choice. In this project, username: koi, password: koipw.
8. Set NTP to 0.debian.pool.ntp.org
9. Keep the default disc partition options.
10. Wait while the system installs...
11. Select the default kernel and package manager.

12. Select a mirror

13. Choose the following software selection:

- a. Debian Desktop Environment
- b. Web Server
- c. DNS Server
- d. File Server
- e. SSH
- f. Standard System Utilities

14. Install Grub with its default settings.

15. Finish installation.

DNS Configuration

In this part, puTTY will be used to SSH into the Debian Server from the Windows Server.

Note: It's assumed here that on the Debian Server, Bind9 is already installed, and the network interface file is set to static.

1. Edit the file /etc/bind/named.conf.local and add the following lines:

```
zone "fantom.koi" {
    type slave;
    masters { 198.168.1.10; };
    file "/var/lib/bind/db.fantom.koi";
};
```

The purpose of the line “type slave” above is to set the type of the DNS server to slave, which specifies that the zone data is obtained from another nameserver.

Testing the Infrastructure

Creating User Groups

We modified two scripts, addgeese and addsantas, that are very similar. Each script takes in a .csv file of users and adds those users to a particular group in our AD environment.

1. To create groups:

- a. Go to Server Manager > Tools > Active Directory Users and Computers > Select Users Folder > Action > New > Groups
- b. Select Group Scope: Domain Local, Global, Universal
- c. Select Group type: Security or Distribution
- d. Title your group and click OK.

2. To add users to the groups, run the scripts in the Windows Server VM:

1. Copy the scripts and .csv files onto the server.
2. Open PowerShell Integrated Scripting Environment (ISE) as an Administrator.
3. Open each script.
4. Change the path in each script for the .csv files to to the location that contain the .csv files.
5. Click run in PowerShell for each script to add all the users were to the appropriate groups, Geese and Santas.

3. To change the permissions for the Santas Administrator group:

1. Go to the Server Manager > AD Users & Groups > Users > Santas > Properties.
2. Right click on Santas > add to a group... > advanced > starts with: admin.
3. Find now and click OK.



Screenshot of creating a new group.

Windows 7 Client

Virtual Machine Setup and Installation

Covering this portion of the project was omitted because it was not essential to the overall goals of the project. Anyone interested in creating a similar VM can use the detailed notes for the creation of the servers described earlier. The infrastructure was designed intentionally so that other client VMs could also be utilized without issue.

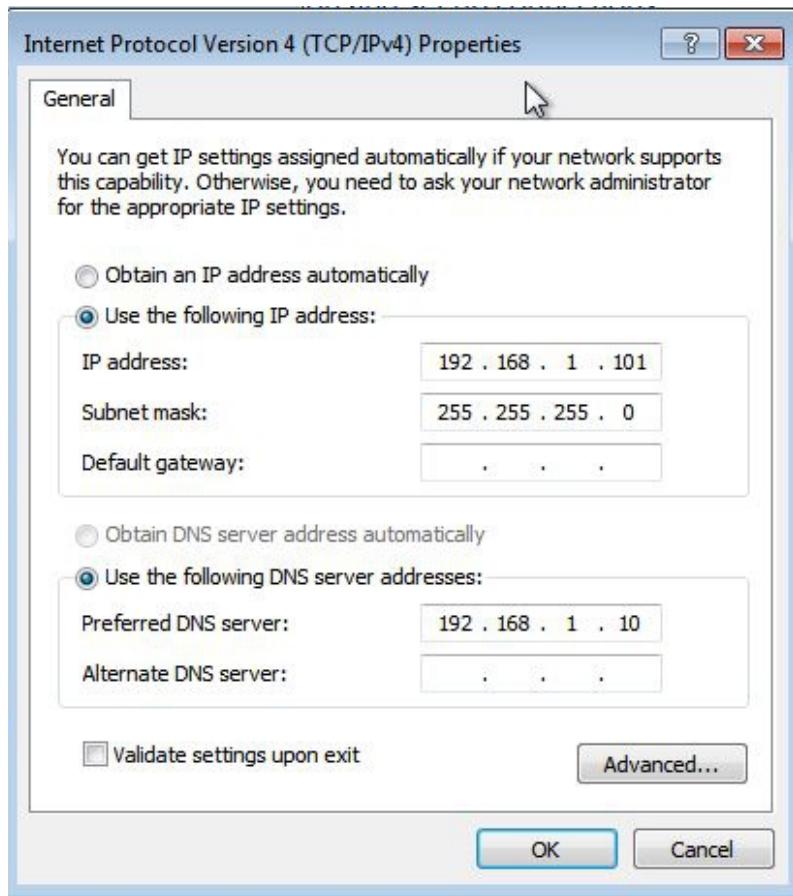
Client Configuration

Set Windows 7 to Static IP

Because this project does not have a DHCP server to dynamically give out IP addresses, the client server is set statically. In a real world environment, DHCP addressing would usually be the most desirable option.

1. Navigate to Control Panel > Network and Sharing Center > Local Area Connection > Properties > IP version 4 > Properties > Use the Following IP Address

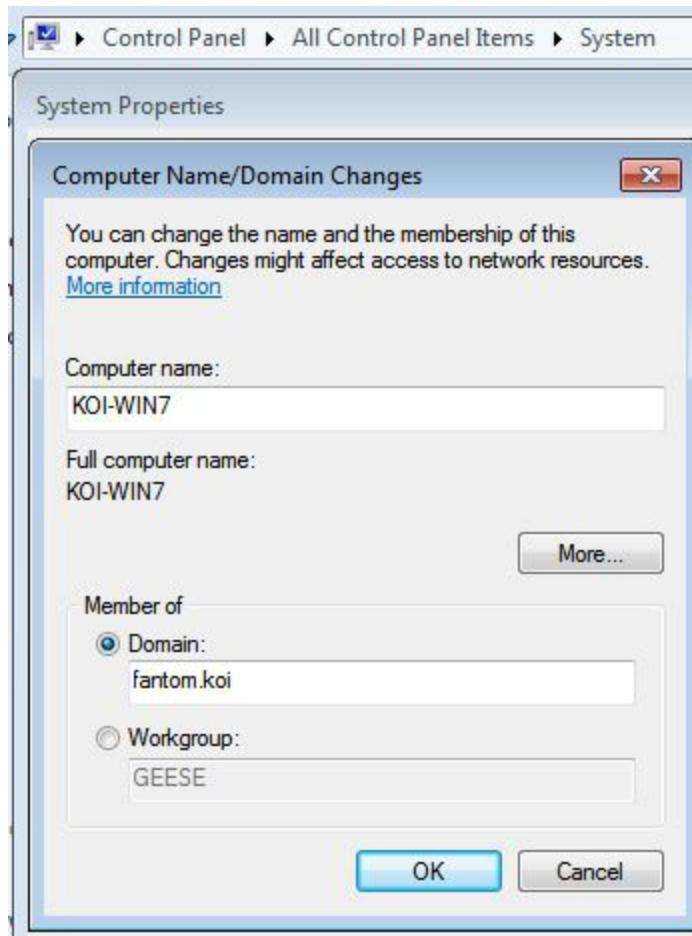
IP Address: 192.168.1.101
Subnet: 255.255.255.0
Use the following DNS server addresses:
Preferred DNS server: 192.168.1.10
Alternate DNS server: 192.16.1.20



Network settings for the Windows 7 VM

Add Windows 7 Client to the Domain

1. Navigate to Control Panel > System > Change Settings > Change Member of Domain
2. Click the radio button and type in the desired domain [fantom.koi]



Adding the Windows 7 VM to the Domain

The Windows Security window pops up for Computer Name/Domain Changes and you are prompted to enter a user name and password of an account that already has permission to join the domain. Sign in with the Administrator account from the Windows Server. At first login, the administrator will be prompted to create a new password. This is stored in the Santa group on the Windows Server.

Mounting the NFS Share

To Mount the network drive:

1. File Explorer > "Alt" > Tools > Map A Network Drive

2. Pick the drive letter that you wish to mount the share as, then enter `\winkoi-2012.fantom.koi\Koi-NFS` as the folder.
3. Check the box to reconnect at login if you wan the share to be available every time you use the computer and click Finish.

If prompted at this point to turn on network discovery to mount the NFS directory.

1. Navigate to Network and Sharing Center > Advanced Sharing Settings
2. Turn on file and print sharing option and save changes

At this point in the mounting of the NFS share, the Windows 7 VM required updating. Lacking time to download and install the 153 updates required for this VM, this step was unable to be completed. It is a simple step, however, and the NFS was tested between servers and found to be working correctly.

Run the Infrastructure

Once the infrastructure has been set up properly and tested. Since the project is essentially a back end for businesses, it just passively runs in the background. To use the infrastructure you have to monitor log files and ensure that the system is maintained and updated.

Maintain the Infrastructure

To maintain the infrastructure, specific steps must be followed to minimize possible difficulties that one might encounter. First, if any changes are made to a configuration file or the registry, always make a backup file or backup of the registry prior to altering any data. This will prevent system malfunctions that would otherwise be too difficult to diagnose as the original file can be restored. Second, ensure that the Ethernet cables or Wi-Fi connections are secured. Loose connections are often overlooked as the culprits of many problems. Third, ensure that root access is granted for the Debian Server VM, while the administrator privilege is granted for the Windows Server VM. Root or administrative access is required to prevent unauthorized

changes, which is essential in keeping the infrastructure from being tampered with. Lastly, the connections between the Debian Server and Windows Server VMs must be flowing freely. If any difficulties arise during any of the steps above, disabling the firewall or antivirus can possibly solve the issues.

Update the Infrastructure

Like all infrastructures, this infrastructure must be kept up-to-date to keep it running smoothly. The following tasks are to be completed regularly in order to achieve said purpose. The tasks listed below do not need to be completed in any particular order.

2. Update the Windows Server VM by installing the important updates suggested by Windows Update located in the Control Panel.
3. Update the Debian Server VM by using the command `apt-get update; apt-get upgrade` or similar versions.
4. Users can be added or removed from the active directory to keep the directory up-to-date.
5. Groups can be added as needed according to the guidelines above.

Note: For more information on the differences between the scope of each group, see Appendix A.

Significant Features of the Infrastructure

In this infrastructure, the abilities to access shared documents, remote management, and maintain consistent logins across workstations are the most notable features. These features are necessary for many academia and business settings, where being able to access shared documents from any workstation is a must to have the utmost productivity. Management is also able to track and manage users, which can eliminate any unauthorized users from disrupting the work-flow. Due to its complexity, the downside is that it requires many

operations to get the whole infrastructure set up. However, the upside is that once the infrastructure is up and running, it can greatly streamline the productivity of an organization, such as this university.

Summary

This project successfully demonstrated that implementing internal networked services for a commercial enterprise is feasible using the labs and outside information. In this project, the group encountered many difficulties initially when setting up and configuring both servers. Despite the obstacles, the group as a whole learned how to incorporate both platforms together after the problems have been solved. Collectively, the group learned to replicate many aspects that would appear in a business infrastructure, such as maintaining consistent logins across workstations. However, the knowledge gained from this project is not confined to just this particular setup. Similar infrastructures in the real world, such as accessing shared documents and allowing remote management between multiple platforms, will benefit from this project as well.

Appendix A

Adding Guests Additions

Note: Guest Additions are designed to be installed inside a virtual machine after the guest operating system has been installed. They consist of device drivers and system applications that optimize the guest operating system for better performance and usability.

Navigate to the Devices tab on the Windows Server VM.

Select Insert guest adds (last option).

Open Windows Explorer.

Under devices and drives, open D:\VirtualBox Guest Additions.

Select VBoxWindowsAdditions application to go into the setup wizard (4.3.16).

Continue clicking next for all the prompts to set up & install.

Finish & Reboot now.

Once the VM is back up, disable the VirtualBox time sync because adding guests auto-installs it.

Start Command Line Prompt.

Type in the following command:

```
C:\Program Files\Oracle\VirtualBox>VBoxManage  
setextradata "VM name"  
"VBoxInternal/Devices/VMMDev/0/Config/GetHostTimeDisabled"  
1
```

Appendix B

Add Admins to Santas Group

```
# Create Active Directory Accounts and add users to multi groups
# By CHSA 9/03/2014
# Edited by Team K.O.I. 04/18/2015

Import-Module ActiveDirectory -ErrorAction SilentlyContinue
$LogFile = "AddUser.log"
# Get domain DNS suffix
$dnsroot = '@' + (Get-ADDomain).dnsroot

# Import the file with the users. You can change the filename to reflect your file
$users = Import-Csv F:\SantasToAdd.csv
foreach ($user in $users) {
    try {
        $login = $user.SamAccountName
        $defpassword = (ConvertTo-SecureString $user.Password -AsPlainText -force)
        New-ADUser -SamAccountName $login -Name $login -DisplayName
        ($user.FirstName + " " + $user.LastName) -Surname $user.LastName -UserPrincipalName
        ($login + $dnsroot) -Description $user.title -Enabled $true -ChangePasswordAtLogon $true
        -PasswordNeverExpires $false -AccountPassword $defpassword -PassThru

        "Create user $login ==> Ok" | Add-Content $LogFile
    }
    catch
        [Microsoft.ActiveDirectory.Management.ADIdentityAlreadyExistsException] {
            "/!\ ERROR creating user: $login $_" | Add-Content $LogFile
        }
    #####
    # Add Santas to Group
    #####
    try {
        add-adgroupmember Santas $login
        "*** Adduser to group Santas OK for user ==> $login " | Add-Content $LogFile
    }
    catch [Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException] {
        "/!\ Group Santas doesn't exist" | Add-Content $LogFile
    }
}
```

Appendix B

The following table describes the differences between the scopes of each group.

Group Scope	Group can include as members...	Group can be assigned permissions in...	Group scope can be converted to...
Universal	<ul style="list-style-type: none"> -Accounts from any domain within the forest in which this Universal Group resides -Global groups from any domain within the forest in which this Universal Group resides -Universal groups from any domain within the forest in which this Universal Group resides 	Any domain or forest	<ul style="list-style-type: none"> -Domain local -Global(as long as no other universal groups exist as members)
Group	<ul style="list-style-type: none"> -Accounts from the same domain as the parent global group -Global groups from the same domain as the parent global group 	Member permissions can be assigned in any domain	Universal (As long as it is not a member of any other global groups)
Domain Local	<ul style="list-style-type: none"> -Accounts from any domain -Global groups from any domain -Universal groups from any domain -Domain local groups but only from the same domain as the parent domain local group 	Member permissions can be assigned only within the same domain as the parent domain local group	Universal (as long as no other domain local groups exist as members)

Source: [https://technet.microsoft.com/en-us/library/cc755692\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx)