Introducing Active Directory Domain Services (AD DS)

Lab 4: Install an AD DS Domain Controller to Create a Single Domain Forest

CSCI 4417-001
Spring 2016
Jack Ramsey, Lecturer

Install a New Windows Server 2012 Forest with the Windows Interface

Required Materials

This lab will require the use of the two AWS Windows Server 2012R2 instances *lastname*WindowsDC01 and *lastname*WindowsMS01 that we've already created

Launch Windows Server 2012 R2 instances

1. Launch your soon-to-be domain controller (DC) instance, *lastname*WindowsDC01 and its soon-to-be first member server, *lastname*WindowsMS01 (to complete this lab, I launched a second member server, since I'd already done it with the MS01 server. So some of the included screen shots may show -02 instead of 01

2. When it's ready, RDP to your Domain Controller

3. You may be prompted to install updates. Do so. While the updates are installing, proceed with the remaining steps in this section

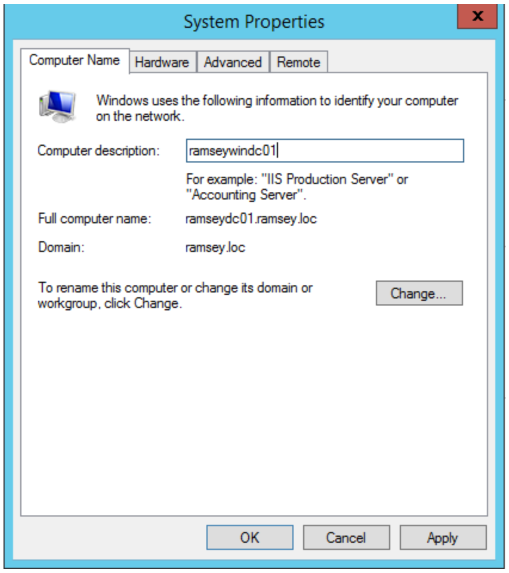
4. The first thing we want to do is change the server's name.

5. You can access the appropriate dialog by right-clicking on the Metro button in the lower left corner of the display and selecting System. In the window that then displays, click on the 'Change settings' link on the right.

6. Name the machine ***lastname*windc01** (the length field is limited, so if you have a long last name, you may need to abbreviate it). If you get an error message about truncating the name, then you've gone past the character limit and will have to abbreviate your name. Case probably doesn't matter here – I used 'RamseyWinDC01' last semester and the last lab worked fine for me. But this might be a good time to get in the habit of Linux limitations

7. Click on the 'Change' button.

8. Again, modify the server's domain name as you did in Step 7.



Windows uses the following information to identify your computer on the network.

Computer description: ramseywindc01

For example: "IIS Production Server" or "Accounting Server".

Full computer name: ramseydc01.ramsey.loc

Domain: ramsey.loc

To rename this computer or change its domain or workgroup, click Change.

Figure 1: Changing the server's domain name, Step 9

9. You'll have to restart the computer for the changes to take effect. To do this (the best way), right-click on the Metro button, hover over 'Shut down or sign out', and click on Shutdown. Give it a reason – Other (planned). Then return to the EC2 console and again shut it down from there. That's the only way you'll know for sure when to start it back up, as the dashboard won't tell you on reboots

10. While the server is restarting, RDP in to your member server

11. Rename this machine as you did the domain controller to ***lastname*****winms01**, with the same length restrictions

12. Shut down, and then restart the member server following the steps outlined in #9

Install Active Directory Domain Services

1. Now restart your DC and RDP to it. Launch the Server Manager by clicking on the 'Server Manager' button (to the right of the Metro button). It'll take a moment to populate all of the installed roles (none, at this point)

2. At the top of the display, click on '2 Add roles and features'

3. Click 'Next' and proceed through the Wizard. Since the operation is wizard based and fairly straightforward, I'm not going to burden you with a bunch of detailed instructions. However,

    1. The Role is 'Active Directory Domain Services.' You'll be prompted to add features – do so

   2. After that, accept defaults and click through to ‘Finish’

4. After AD DS is installed, you’ll notice an exclamation mark hovering by a flag icon in the upper left of the display. Click on this. There’ll be a link to ‘Promote this server to domain controller.’ Click on that. Oddly enough, I think I mentioned this in class, Windows Server 2012 won’t let you run the application, dcpromo.exe, from the command line (it used to)

5. This will require setting up the Domain Name Server (DNS) role. Again, it is wizard based, but you’ll need some info:

   1. You’ll be creating a new forest

   2. Name your root domain *lastname*.loc

   3. Leave the functional levels as they are (‘Windows Server 2012 R2’).

   4. Again, the DSRM password should be ‘Passw0rd!’.

   5. On the next screen, you’ll see an error message: “A delegation for this DNS server cannot be created…” Before (safely) ignoring it, consider why the alert is displayed. Hint: you’re creating a Forest level DNS server

   6. You can click through to the end and ‘Install’

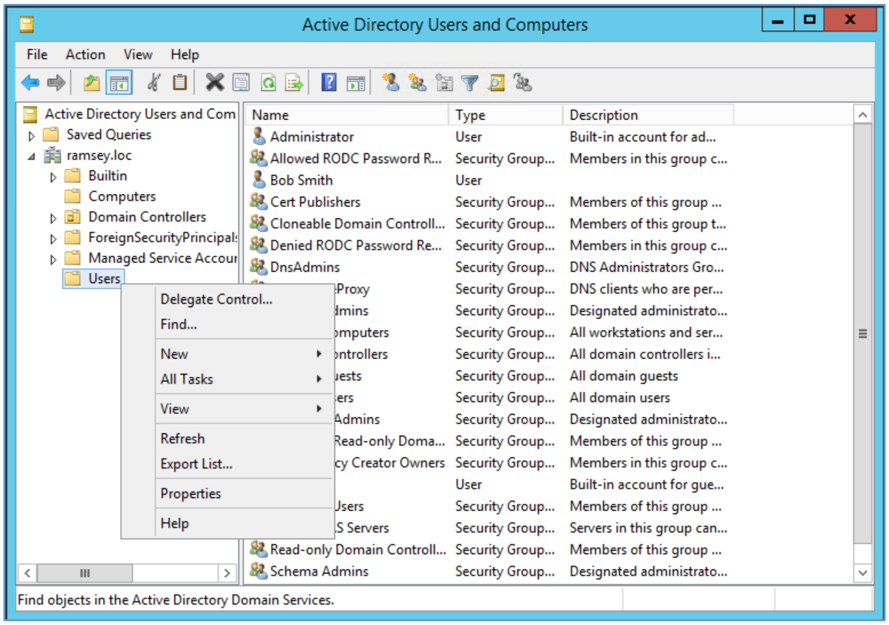
6. Once AD DS is installed, let’s add a user and make him a Domain Administrator

   1. In the upper right corner of the Server Manager, click on ‘Tools’

   2. Select ‘Active Directory Users and Computers’

   3. You may have to drill down a bit by expanding the tree on the left pane of the display, starting with your domain name

   4. Right-click on the ‘Users’ folder and select New->User



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password R...	Security Group...	Members in this group c...
Bob Smith	User	
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controll...	Security Group...	Members of this group t...
Denied RODC Password Re...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
:Proxy	Security Group...	DNS clients who are per...
dmins	Security Group...	Designated administrato...
omputers	Security Group...	All workstations and ser...
ontrollers	Security Group...	All domain controllers i...
uests	Security Group...	All domain guests
ers	Security Group...	All domain users
Admins	Security Group...	Designated administrato...
Read-only Doma...	Security Group...	Members of this group ...
cy Creator Owners	Security Group...	Members in this group c...
	User	Built-in account for gue...
Jsers	Security Group...	Members of this group ...
S Servers	Security Group...	Servers in this group can...
Read-only Domain Controll...	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...

Find objects in the Active Directory Domain Services.

Figure 2: Adding a user

5. Enter ‘Bob Smith’ for the first and last names and ‘bsmith’ in the email field, then ‘Next’

6. Enter ‘Passw0rd!’ for the password and uncheck ‘User must change password at next logon’ --

   Warning! Not best practice in the RW, but ok for lab purposes

7. Click through to ‘Finish’

8. Click on the ‘Users’ folder and select Bob

9. Right-click on Bob

10. Select Bob’s Properties

11. Click on the ‘Member Of’ tab

12. Click the ‘Add’ button

13. Enter ‘Domain’ in the search box and then click the ‘Check Names’ button

14. Select ‘Domain Admins’ group and click ‘OK’

15. Select the ‘Domain Admins’ group in the properties window and click the ‘Set Primary Group’ button

16. Then click ‘OK’ to leave Bob

17. Exit out of the AD DS Users and Computers MMC (Microsoft Management Console).

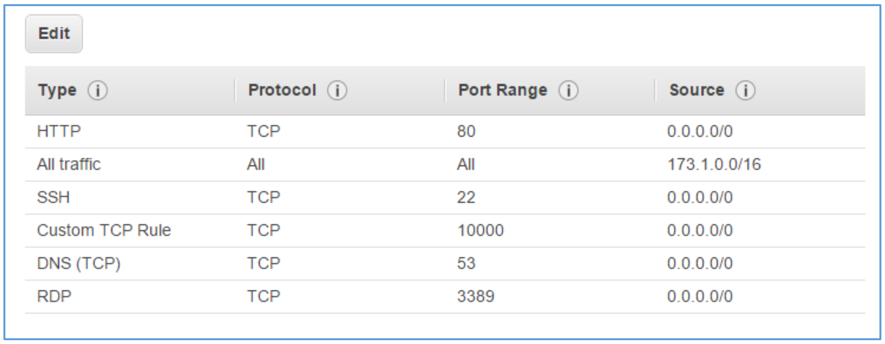
Join your Member Server to the Domain

1. In order to ensure that all of the machines on your private network can communicate with one another, we need to add another rule to the inbound rules in our security group

2. Navigate to the security group, select the Inbound tab, and Edit

3. The type will be ‘All traffic;’ Protocol, ‘All;’ Port Range, ‘All;’ and Source, ‘173.1.0.0/16’

4. Save your changes



Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
All traffic	All	All	173.1.0.0/16
SSH	TCP	22	0.0.0.0/0
Custom TCP Rule	TCP	10000	0.0.0.0/0
DNS (TCP)	TCP	53	0.0.0.0/0
RDP	TCP	3389	0.0.0.0/0

Figure 3: New rule for private network

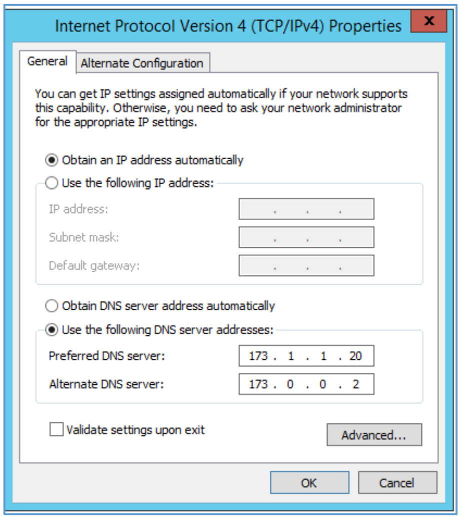
5. RDP in to your member server instance ***from*** your DC01 instance, using the private IP address assigned to the MS01 instance (it should be 173.1.1.30)

6. Log in using Administrator and your admin password (should be Passw0rd!)

7. Navigate to the Network Adapter settings as you did with the domain controller (Right-click on the Metro button and select ‘Network connections.’ You’ll only have one adapter. Right-click on it and click on ‘Internet Protocol version 4 (TCP/IPv4)’ and select ‘Properties.’)

8. You can leave the IP address assignment to DHCP

9. Enter the private IP address of your domain controller in the Preferred DNS server field (173.1.1.20). You may want to add 8.8.8.8 as a secondary DNS (anyone know what this is?)



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 173 . 1 . 1 . 20

Alternate DNS server: 173 . 0 . 0 . 2

□ Validate settings upon exit

Figure 41: Changing the DNS server

10. Launch PowerShell (the icon in the taskbar) of the MS01 instance

11. It should be running in Administrator mode. If it doesn't say 'Administrator' in the title bar, exit out, right-click on the above pictured icon, and select 'Run as Administrator' from the menu

12. Type in the following command:

```
nslookup lastname.loc
```

    This should confirm that your member server is hitting the domain controller (it might take a minute or two)

13. Type in the following command:

```
add-computer -domainname lastname.loc -restart
```

    Before you hit Enter, backspace the line out of existence, then type

```
add-com
```

    and hit Tab. See, Tab completion also works for PowerShell! When you've typed

```
-domainn
```

    ** Note: two "n's"

    hit Tab again

    Joining the domain *may* fail the first couple of times – It may take a minute or two for the member server to recognize your domain/forest. You can re-access the command by tapping the up arrow. It shouldn't though, if the `nslookup` command worked

14. You will be prompted to enter your Administrator credentials

15. Let's confirm that Bob is indeed a Domain Administrator

16. Use Bob's credentials: bsmith/Passw0rd!

17. If all works out, you'll be disconnected from the member server as it reboots

18.

    a. RDP will try to reconnect whenever a connection is severed. Just wait patiently (for me, it was around Retry #5)

    b. In lab, everyone was simply disconnected after Step 17. If this happens, wait four minutes and attempt to reconnect

19. When the MS01 instance prompts you for login in credentials, again use Bob's

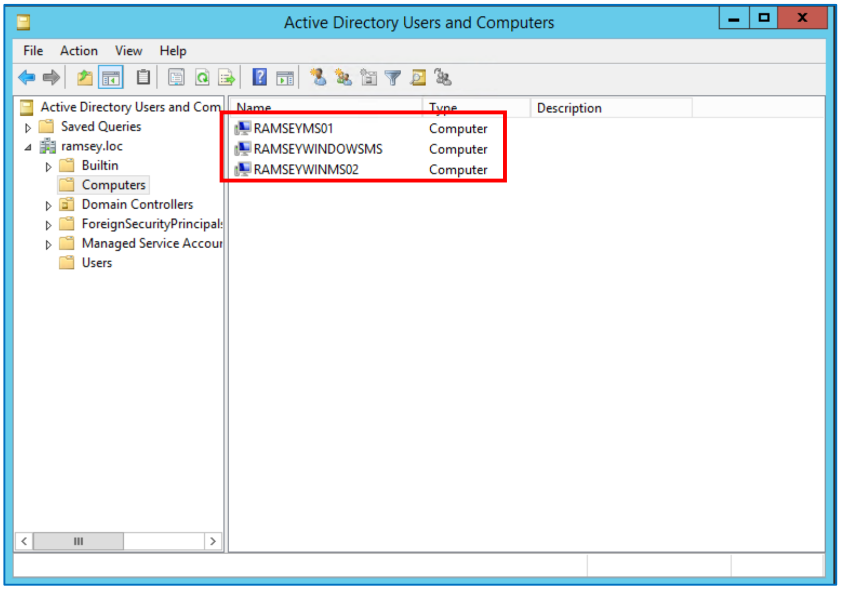
20. Once you're successfully logged in, confirm that Bob is a Domain Admin by launching the Server Manger (if he doesn't have permission, it won't launch – a domain user can now log in to MS01 as well, but not with administrative privileges)

21. Sign out of the MS01 instance by right-clicking on the Metro button, hovering over 'Shut down or sign out,' and selecting 'Sign out.' This will sign you out and close Remote Desktop

22. As a final confirmation of your success in creating and populating a domain, return to the Active Directory Users and Computers MMC

23. This time, click on Computers, on the right, instead of Users

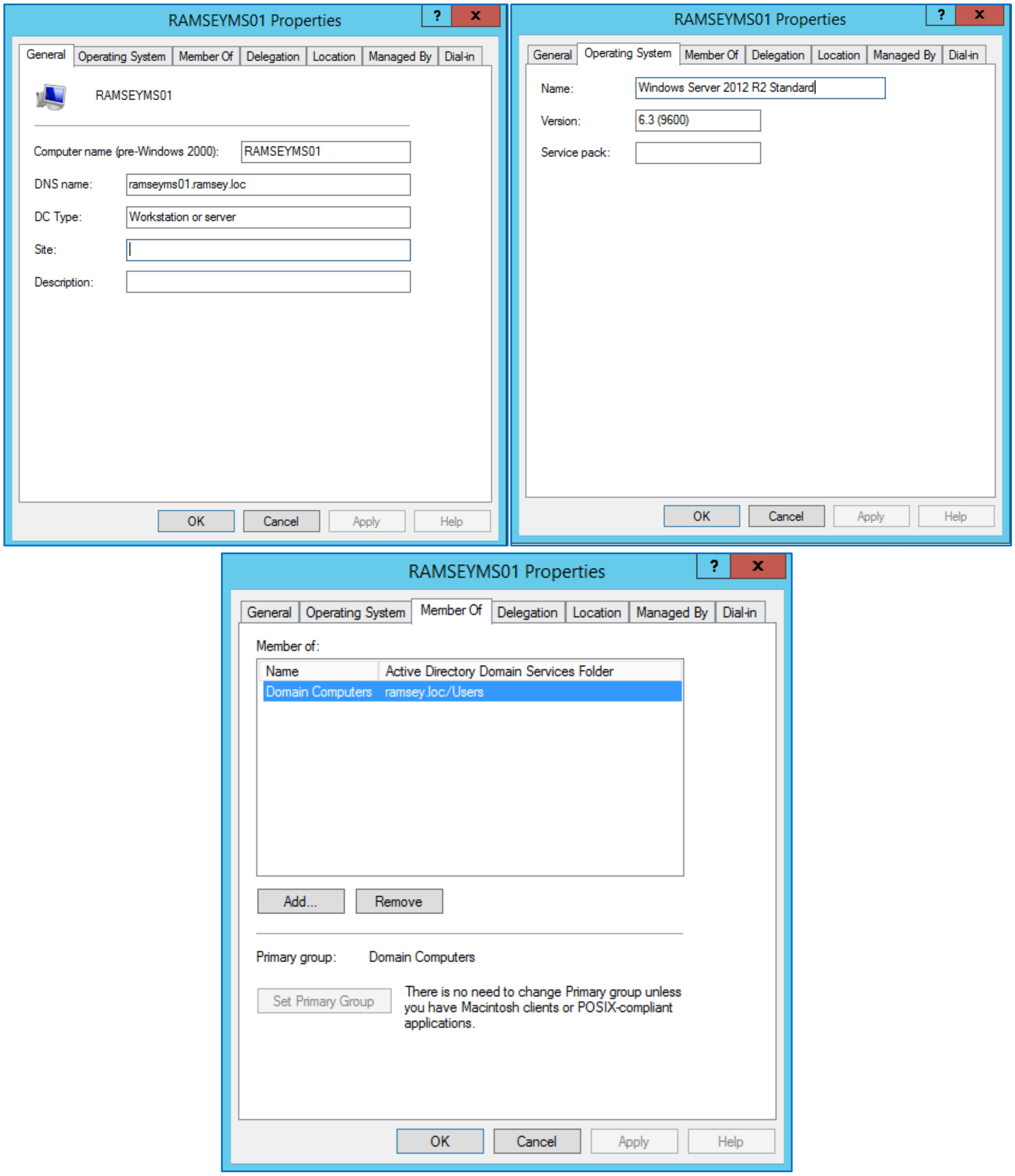
24. You should see your MS01 instance listed



Name	Type	Description
RAMSEYMS01	Computer	
RAMSEYWINDOWSMS	Computer	
RAMSEYWINMS02	Computer	

Figure 5: Confirming addition of instance

25. You can examine the properties of the server by right-clicking on its name in the right pane and selecting ‘Properties’



RAMSEYMS01

Computer name (pre-Windows 2000): RAMSEYMS01

DNS name: ramseyms01.ramsey.loc

DC Type: Workstation or server

Site:

Description:

Name: Windows Server 2012 R2 Standard

Version: 6.3 (9600)

Service pack:

Member of:

Name	Active Directory Domain Services Folder
Domain Computers	ramsey.loc/Users

Primary group: Domain Computers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Figure 6: Member server properties

26. Neat, huh?

Ubuntu

1. Let’s do a quick exercise with Ubuntu to wrap up today’s activities
2. Launch your Ubuntu instance and SSH in to it
3. Once you are logged in, enter the following commands:

```
sudo wget wget http://www.webmin.com/download/deb/webmin-current.deb
```

(wget is a utility for downloading files directly from websites. This will download an installation package for an application called Webmin)

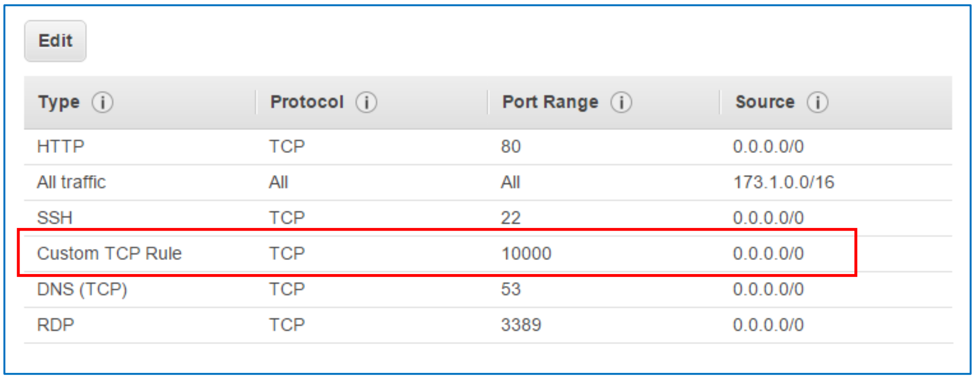
```
sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl
libpam-runtime libio-pty-perl apt-show-versions python
```

(This will install necessary packages to support Webmin)

```
dpkg --install webmin_1.760_all.deb
```

(dpkg is the Debian package management tool. apt-get is a higher level Ubuntu tool that secretly uses dpkg to manage software. This will install the Webmin package. It takes a few minutes. You can use the -i switch instead of --install. I just used --install because it tells you at a glance what you're doing with this command.)

4. While Webmin is installing, navigate to your security groups. Add a new rule, Custom TCP Rule, TCP, 10000, 0.0.0.0/0. Webmin uses port 10000 over a secure https:// connection to connect to the instance via the web



Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
All traffic	All	All	173.1.0.0/16
SSH	TCP	22	0.0.0.0/0
Custom TCP Rule	TCP	10000	0.0.0.0/0
DNS (TCP)	TCP	53	0.0.0.0/0
RDP	TCP	3389	0.0.0.0/0

Figure 7: Opening port 10000 for Webmin

5. Return to your Ubuntu instance
6. Since we're using key encryption to log in to our AWS instances, we can't use root to log in to Webmin – and in real life, wouldn't want to
7. So, in anticipation of next week's lab, we're going to create a new user named 'webmin'

```
sudo adduser webmin
```

(You'll be prompted to enter a password – Passw0rd! – and confirm it. For the remaining prompts, you can simply hit Enter)

Now that we have our new 'user,' we have to elevate its privileges, so enter:

```
sudo usermod -a -G sudo webmin
```

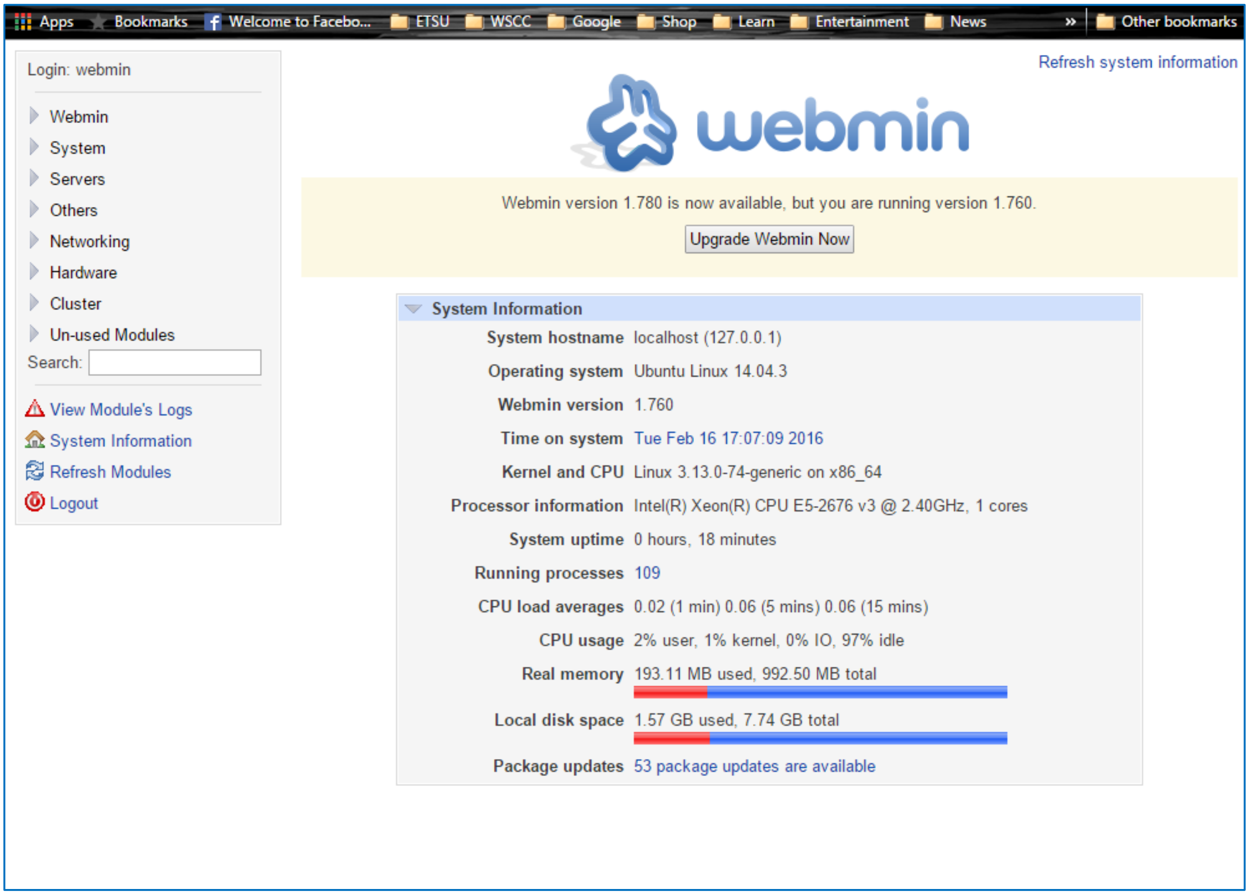
(What this does is modify user webmin by adding it to the sudo group, granting administrative priveleges)

8. Now, copy the public IP address of the Ubuntu instance and launch a web browser
9. Before pasting the address into the address bar, enter https://
10. Paste the public IP address in after https://
11. Add ':10000' after the IP address

12. Press Enter

You'll receive a dire security warning. Reassure your browser that you do indeed know what you're doing and will accept the consequences of ignoring its sage advice

13. After washing its hands of you and your tomfoolery, you should see a log in screen for Webmin
14. Enter webmin/Passw0rd!
15. And…..viola! A web-based administrative console. I know I stress CLI skills to exhaustion, and they are important, may many administrators swear by Webmin for quick fixes. You can use it to install services, administer users, monitor resources, edit and manage files, etc. Take a minute or two to look at the various options
16. When you're done, log out of Webmin



Login: webmin

Webmin version 1.780 is now available, but you are running version 1.760.

System hostname	localhost (127.0.0.1)
Operating system	Ubuntu Linux 14.04.3
Webmin version	1.760
Time on system	Tue Feb 16 17:07:09 2016
Kernel and CPU	Linux 3.13.0-74-generic on x86_64
Processor information	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz, 1 cores
System uptime	0 hours, 18 minutes
Running processes	109
CPU load averages	0.02 (1 min) 0.06 (5 mins) 0.06 (15 mins)
CPU usage	2% user, 1% kernel, 0% IO, 97% idle
Real memory	193.11 MB used, 992.50 MB total
Local disk space	1.57 GB used, 7.74 GB total
Package updates	53 package updates are available

Figure 8: Webmin web-based management console

Be sure to shut down all of your instances

Your lab report is due by the beginning of class next Tuesday. It should be completed following the guidelines presented in D2L.