

Linux Machines & Windows Active Directory

Configured Devices

- 1 Windows 7 machine (testing)
- 1 Windows 2008 Server
- 1 file server on (Red Hat Linux)
- 1 file server on (Ubuntu Linux)
- 1 web server (Ubuntu Linux)
- 1 proxy server (Ubuntu Linux)

Step 1:

Set up Windows Domain Controller

Windows Domain Controller

- Process:
- Install Windows Server OS
- Activate license and install updates
- Install DHCP role
 - Configure DHCP
- Install Active Directory and DNS role
 - Domain controller (dcpromo.exe)
 - Configure DNS (forward and reverse zones)
 - Configure Active Directory
- Test configuration on devices

Challenges

Active Directory

(Error) Message 1

```
C:\Users\Administrator>nslookup valembrun.local
(root) nameserver = i.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = a.root-servers.net
(root) nameserver = m.root-servers.net
(root) nameserver = l.root-servers.net
(root) nameserver = k.root-servers.net
(root) nameserver = j.root-servers.net
i.root-servers.net      internet address = 192.36.148.17
h.root-servers.net      internet address = 128.63.2.53
g.root-servers.net      internet address = 192.112.36.4
f.root-servers.net      internet address = 192.5.5.241
e.root-servers.net      internet address = 192.203.230.10
d.root-servers.net      internet address = 128.8.10.90
c.root-servers.net      internet address = 192.33.4.12
b.root-servers.net      internet address = 128.9.0.107
a.root-servers.net      internet address = 198.41.0.4
m.root-servers.net      internet address = 202.12.27.33
l.root-servers.net      internet address = 198.32.64.12
k.root-servers.net      internet address = 193.0.14.129
j.root-servers.net      internet address = 192.58.128.30
Server: UnKnown
Address: ::1

Name:   valembrun.local
Address: 192.168.16.100
```

- Issue: nslookup displaying list of root servers
- Solution: resolved FQDN in Active Directory install/configuration

Active Directory

(Error) Message 2

```
C:\Users\Administrator>nslookup valembrun.local
Server: UnKnown
Address: ::1

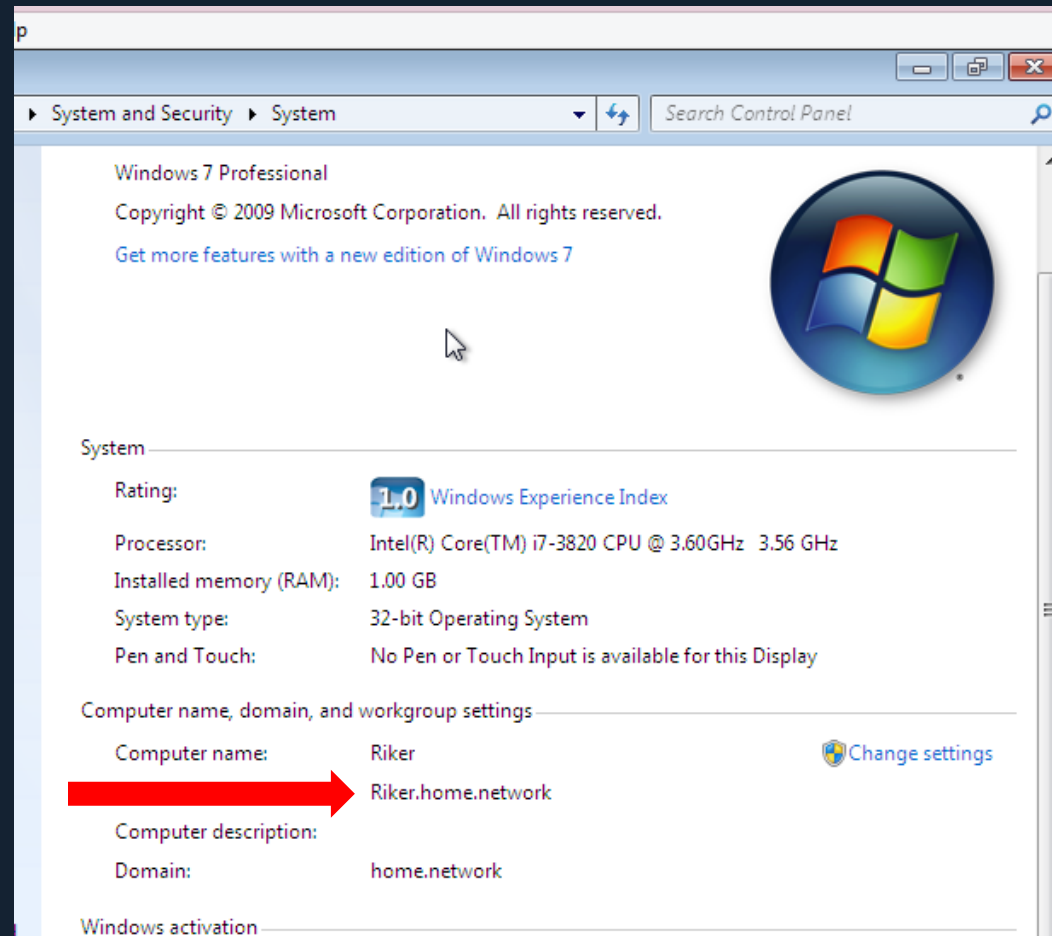
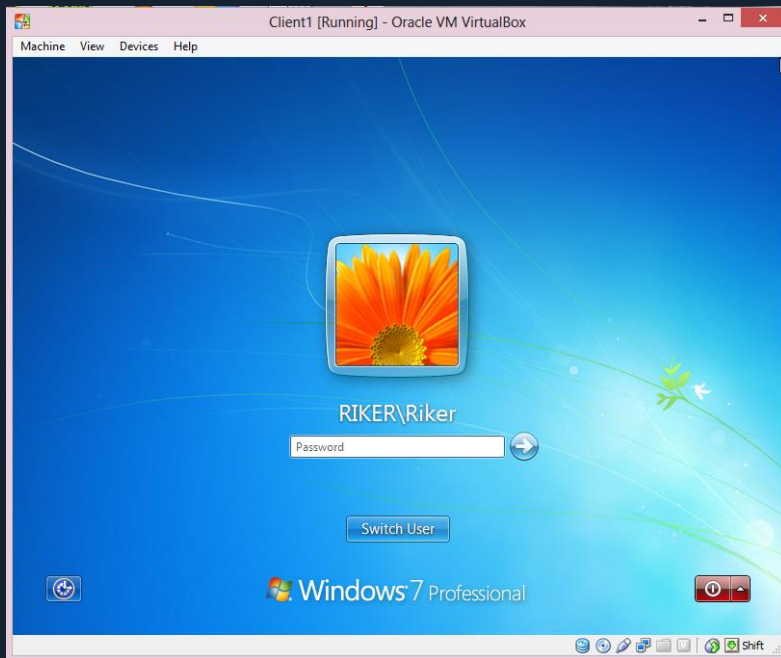
Name:   valembrun.local
Address: 192.168.16.100
```

- Issue: nslookup
- Solution: Used dcdiag in command line to resolve failed test issues, also edited reverse lookup zone

Step 2:

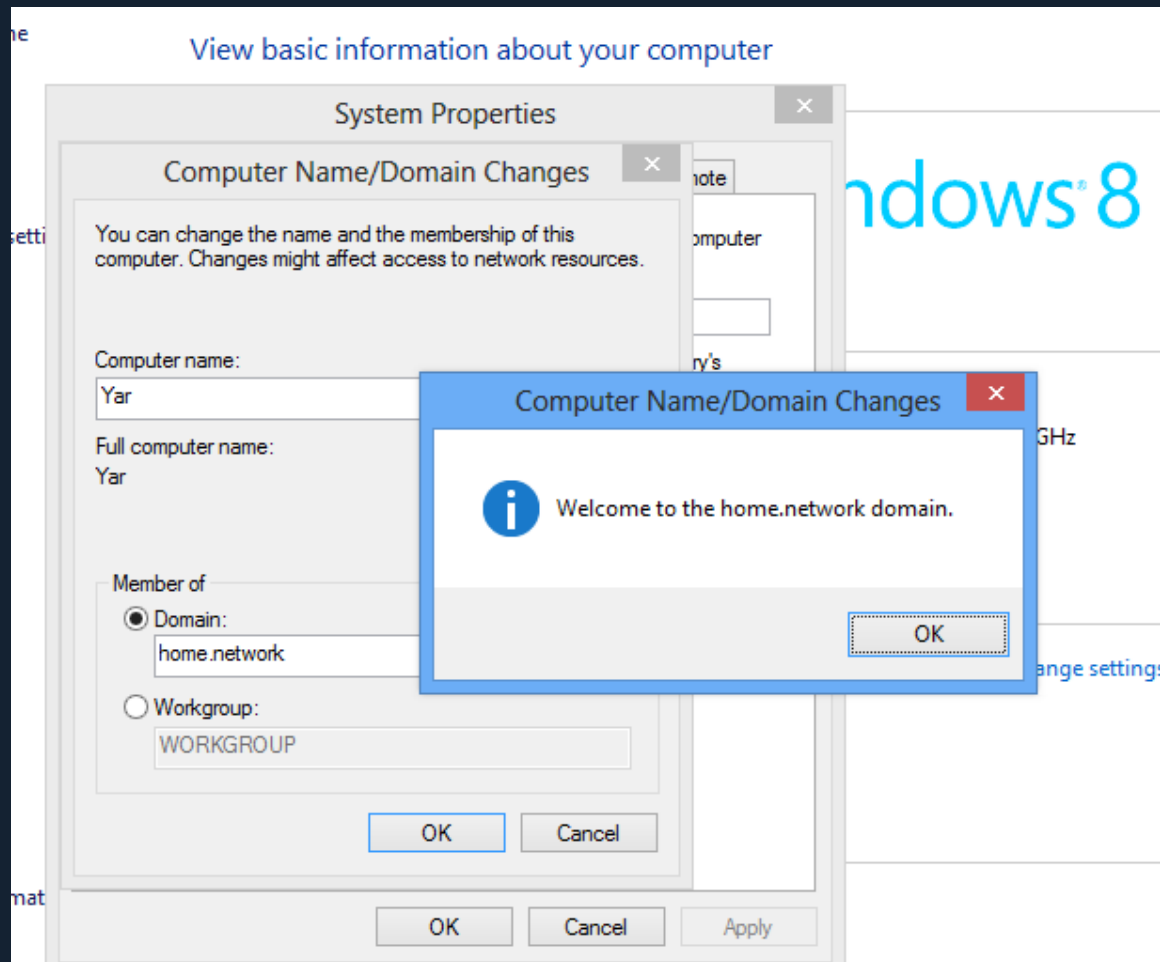
**Setup & Testing
(Windows)**

Windows 7



Successfully added to domain!

Windows 8



Successfully added to domain!


Step 3:


**Setup & Testing
(Linux)**

Linux Device Recognizes Windows Server

from address pool

(192.168.16.16 – 192.168.16.36)

```
[root@valemburn projectfiles]# ifup eth0
Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/5
state: activated
Connection activated
[root@valemburn projectfiles]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:9F:22:73
           192.168.16.18  Bcast:192.168.16.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9f:2273/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41482 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20383 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59545048 (56.7 MiB)  TX bytes:1370199 (1.3 MiB)

[root@valemburn projectfiles]# nslookup home.network  nslookup successful
Server:      192.168.16.100
Address:     192.168.16.100#53

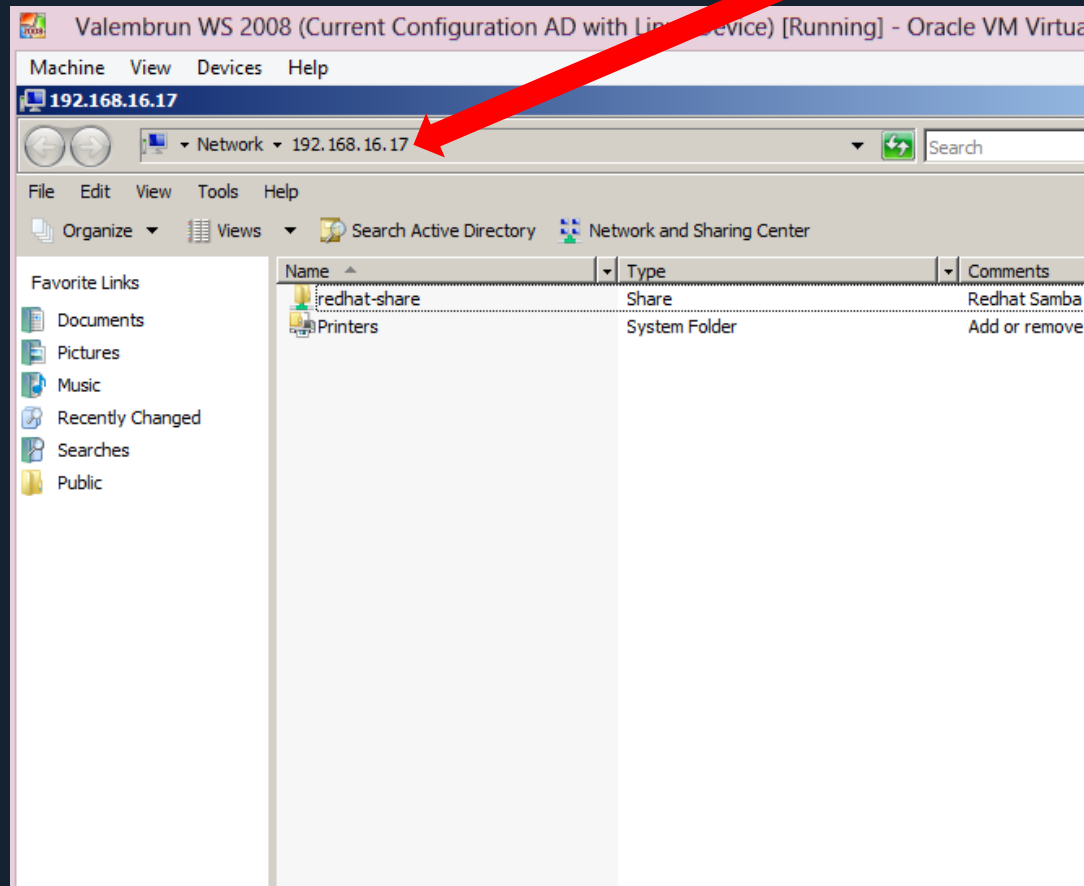
Name:   home.network
Address: 192.168.16.100
```

Joining Red Hat Linux Machine to Windows Domain

- Step 1: Install:
 - Samba
 - Winbind
 - Kerberos
- Step 2: Configure:
 - NTP (time synchronization)
 - /etc/krb5.conf
 - /etc/samba/smb.conf
 - /etc/nsswitch.conf

Challenges

IP address
of Red Hat VM



Through Samba I am able to share files using the IP address of my device,
but I'm unable to add the device to Active Directory

Machine View Devices Help

redhat-share (\\192.168.16.17)

Network 192.168.16.17 redhat-share Search

redhat-share (\\192.168.16.17) Properties

General Network Security Previous Versions Customize

Object name: \\192.168.16.17\redhat-share

Group or user names:

Everyone
root (Unix User\root)
root (Unix Group\root)

To change permissions, click Edit.

Edit...

Permissions for Everyone

Allow

Deny

Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions

For special permissions or advanced settings,
click Advanced.

Advanced

[Learn about access control and permissions](#)

OK

Cancel

Apply

Folders

```
[root@valemburn ~]# net ads join -U Administrator
Enter Administrator's password:
kinit succeeded but ads_sasl_spnego_krb5_bind failed: Ticket expired
Failed to join domain: failed to connect to AD: Ticket expired
```

```
[root@valemburn ~]# net ads join -U Administrator
Enter Administrator's password:
Failed to join domain: failed to lookup DC info for domain 'HOME.NETWORK' over r
pc: Logon failure
```

```
[root@home samba]# kinit administrator@home.network
kinit: Cannot find KDC for requested realm while getting initial credentials
[root@home samba]# nano /etc/krb5.conf
```

```
[root@home ~]# kinit administrator@home.network
Password for administrator@home.network:
kinit: Clock skew too great while getting initial credentials
```

Reviewed and re-
edited all configured
files

Researched error and
applied "fixes"

Unable to resolve the
issue after a day of
(re)editing, I reverted
VM to a previous state
and started all over
again

Resolved time synchronization
by using Windows server time


```
[root@home ~]# kinit administrator@home.network
Password for administrator@home.network:
kinit: KDC reply did not match expectations while getting initial credentials
```

```
root@home:~
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /etc/krb5.conf

#[logging]
# default = FILE:/var/log/krb5libs.log
# kdc = FILE:/var/log/krb5kdc.log
3 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
default_realm = home.network
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
forwardable = yes

[realms]
home.network = {
    kdc = home.network:88
    admin_server = home.network:749
    default_domain = home.network
}

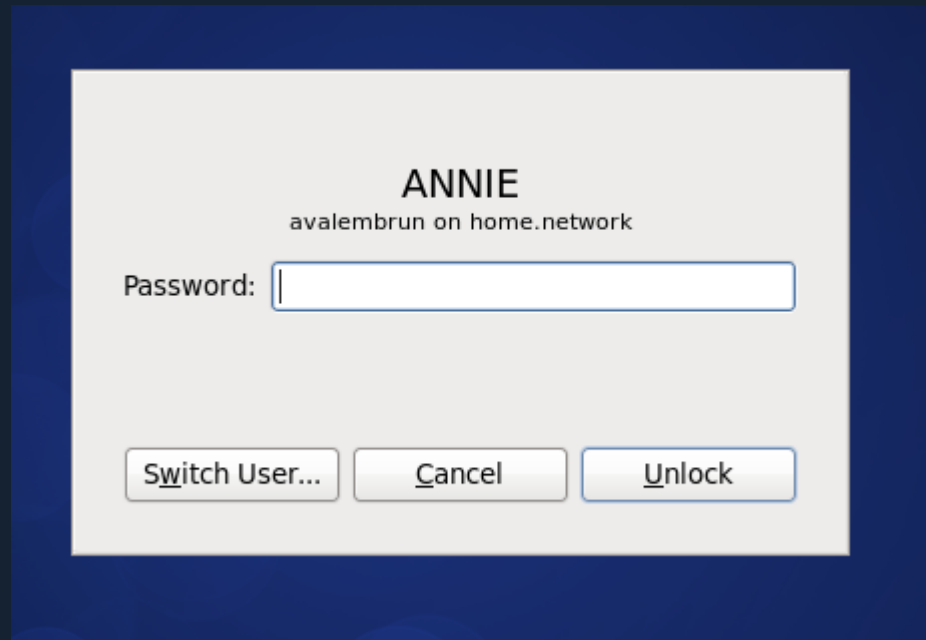
[domain_realm]
.home.network = HOME.NETWORK
home.network = HOME.NETWORK
```

Error caused by lack of
CAPITALIZATION

CORRECT

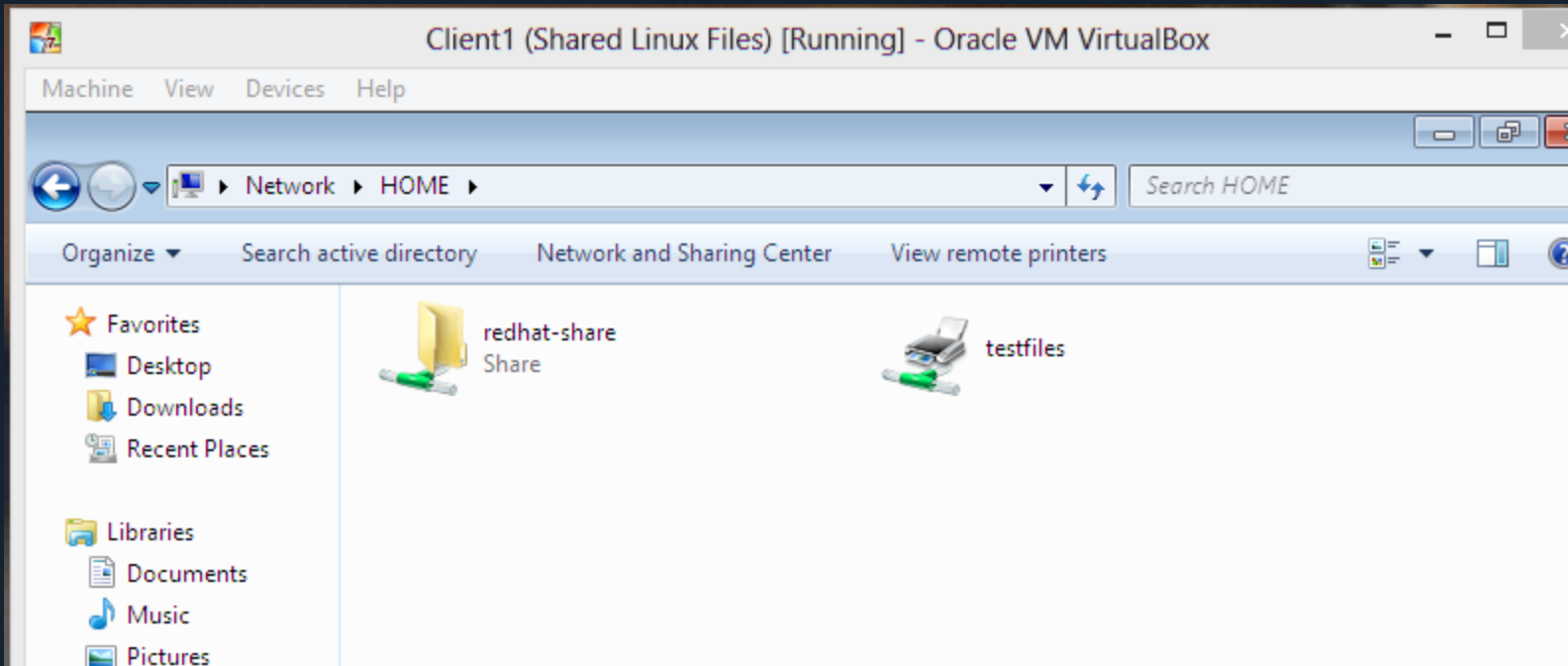
```
[libdefaults]
default_realm = HOME.NETWORK
dns_lookup_realm = false
```

Red Hat



Many errors later Success!

Windows 7 Computer

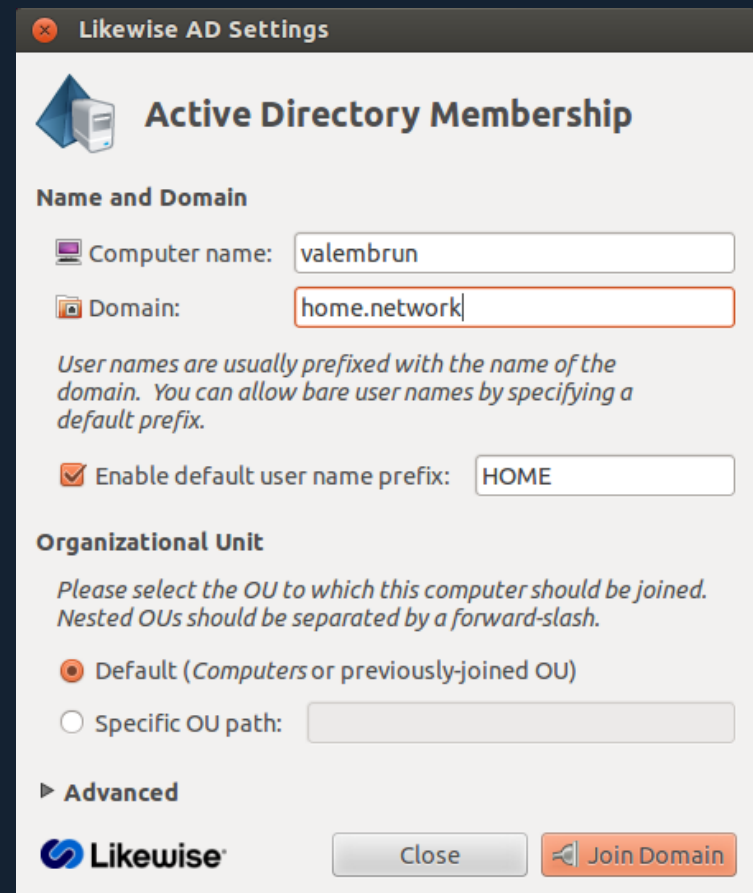


Red Hat Computer

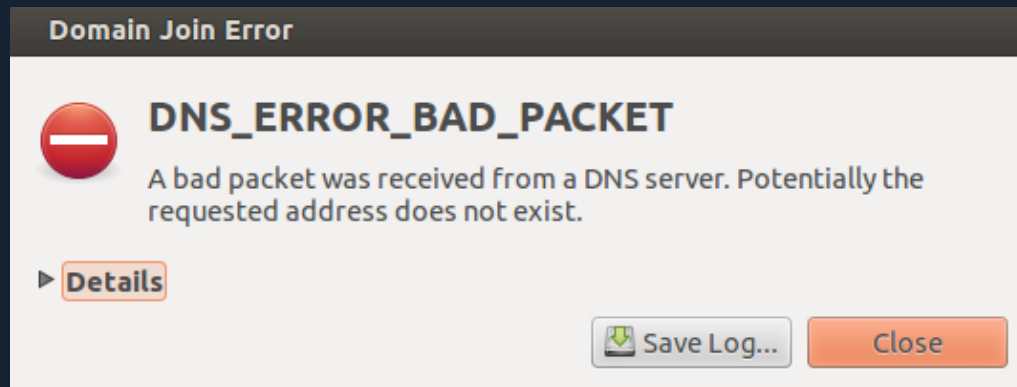
```
[root@home etc]# cd /network
[root@home network]# ls
rhat
[root@home network]# ll rhat
total 8
drwxrwxr-x. 2 root root 4096 Dec 10 00:56 share
drwxr-xr-x. 2 root root 4096 Dec 10 00:57 testfiles
```

Joining Ubuntu Linux Machine to Windows Domain

- Ubuntu:
- Step 1: Install:
 - Likewise-open
- Step 2: Configure files:
 - /etc/nsswitch.conf
 - /etc/lightdm/lightdm.conf
- Step 2:
- Configure Active Directory Membership (Likewise AD Settings)



The screenshot shows the 'Likewise AD Settings' window. The title bar says 'Likewise AD Settings'. The main heading is 'Active Directory Membership' with a blue diamond icon. Under 'Name and Domain', there are two text boxes: 'Computer name:' with 'valembrun' and 'Domain:' with 'home.network'. Below these is a note: 'User names are usually prefixed with the name of the domain. You can allow bare user names by specifying a default prefix.' There is a checked checkbox 'Enable default user name prefix:' and a text box 'HOME'. Under 'Organizational Unit', there is a note: 'Please select the OU to which this computer should be joined. Nested OUs should be separated by a forward-slash.' There are two radio buttons: 'Default (Computers or previously-joined OU)' which is selected, and 'Specific OU path:' with an empty text box. At the bottom, there is a '► Advanced' link, the 'Likewise' logo, and two buttons: 'Close' and 'Join Domain'.



Resolving the Error:

- 1) Edited `/etc/resolv.conf` file (different format then for Red Hat)
- 2) Turned off Windows Firewall (not good practice but necessary)
- 3) Restarted machine
- 4) Reattempted joining domain
- 5) Turned Windows Firewall back on



The trust relationship between this workstation and the primary domain failed.

OK

 Windows 7 Professional

In the middle of trying to configure Red Hat VM for Active Directory, I was set back by two sudden errors which caused me to lose my Windows and Linux users.



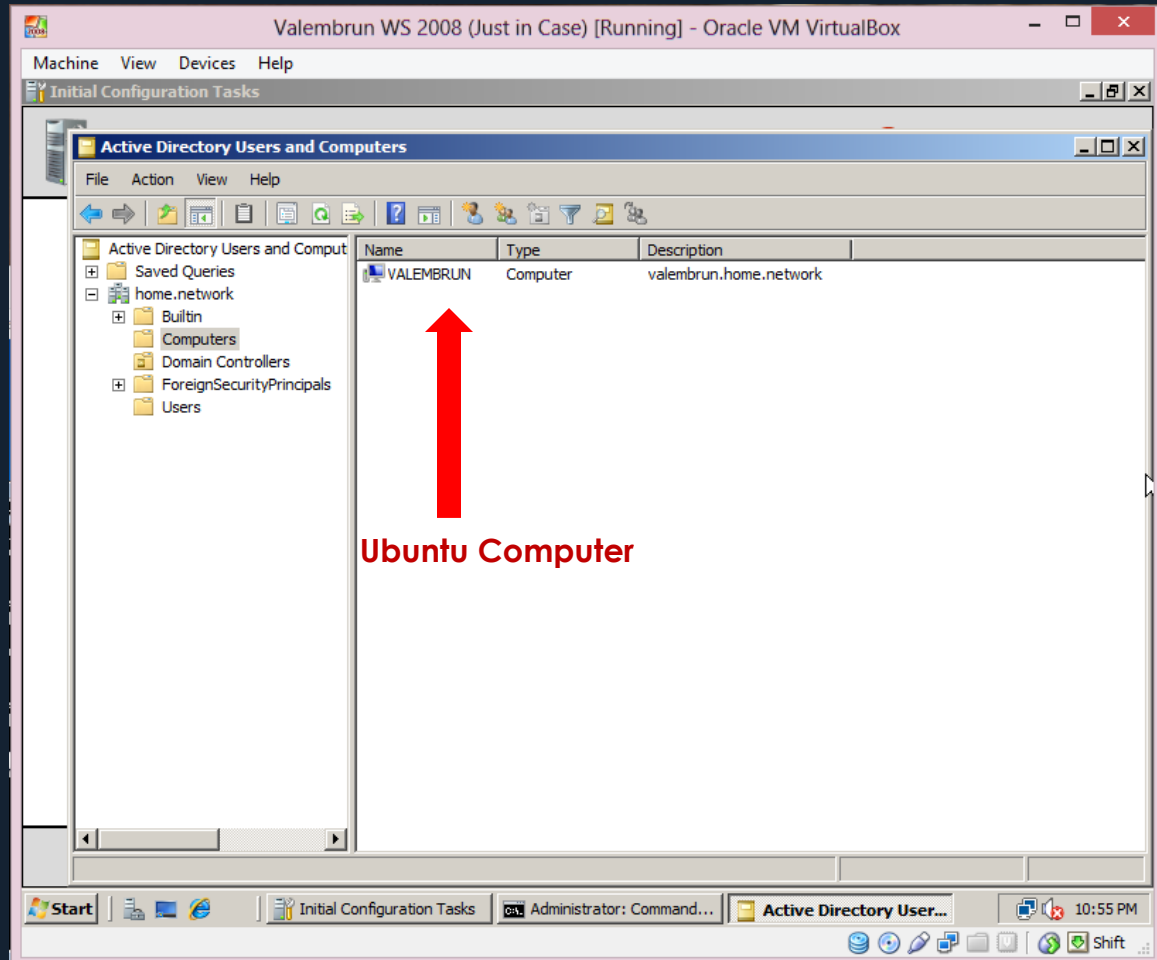
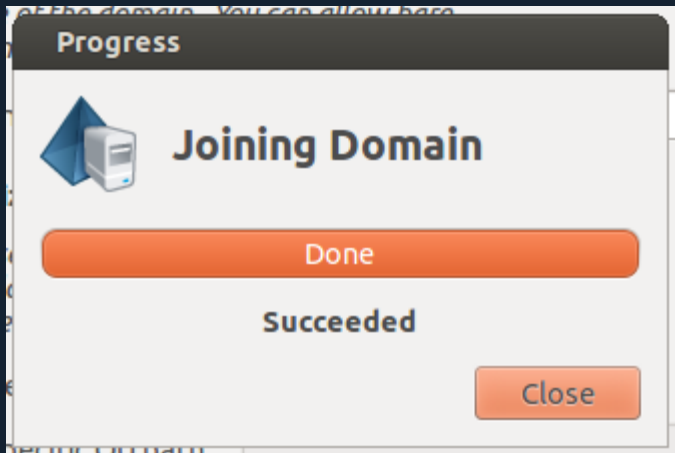
The security database on the server does not have a computer account for this workstation trust relationship.

OK

 Windows 7 Professional

I had to add both the users and computers back to Active Directory

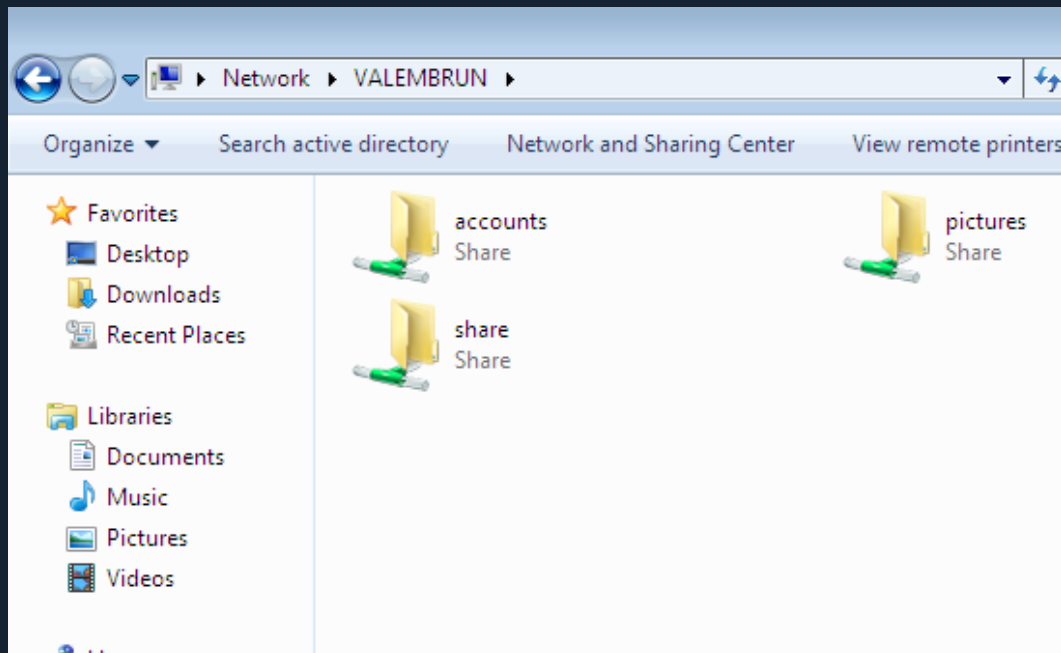
Ubuntu



A few errors later Success!

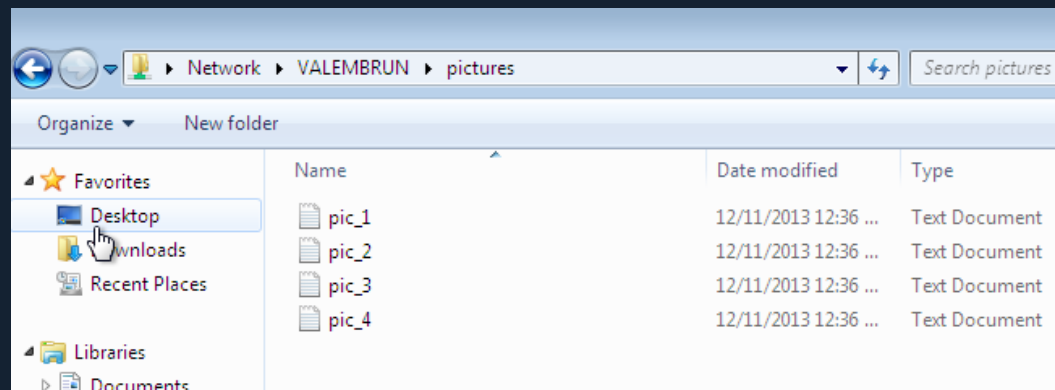
Ubuntu File Server

Windows 7 Computer



Ubuntu Computer

```
root@valemburun:/docs/samba/pictures# ll
total 8
drwxr-xr-x 2 root root 4096 Dec 11 00:36 ./
drwxr-xr-x 6 root root 4096 Dec 11 00:33 ../
-rw-r--r-- 1 root root    0 Dec 11 00:36 pic_1.txt
-rw-r--r-- 1 root root    0 Dec 11 00:36 pic_2.txt
-rw-r--r-- 1 root root    0 Dec 11 00:36 pic_3.txt
-rw-r--r-- 1 root root    0 Dec 11 00:36 pic_4.txt
```



[share]

```
comment = Linux Files  
path = /docs/samba/share  
browsable = yes  
guest ok = yes  
read only = yes  
create mask = 0755
```

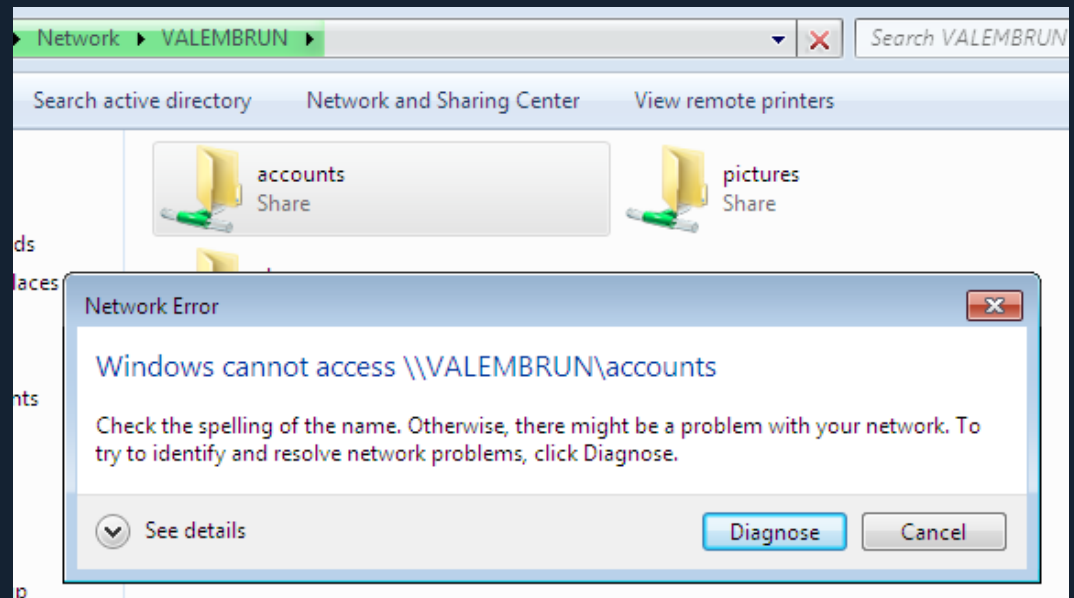
[pictures]

```
comment = A Bunch of Pictures  
path = /docs/samba/pictures  
browsable = yes  
guest ok = yes  
read only = no  
create mask = 0700
```

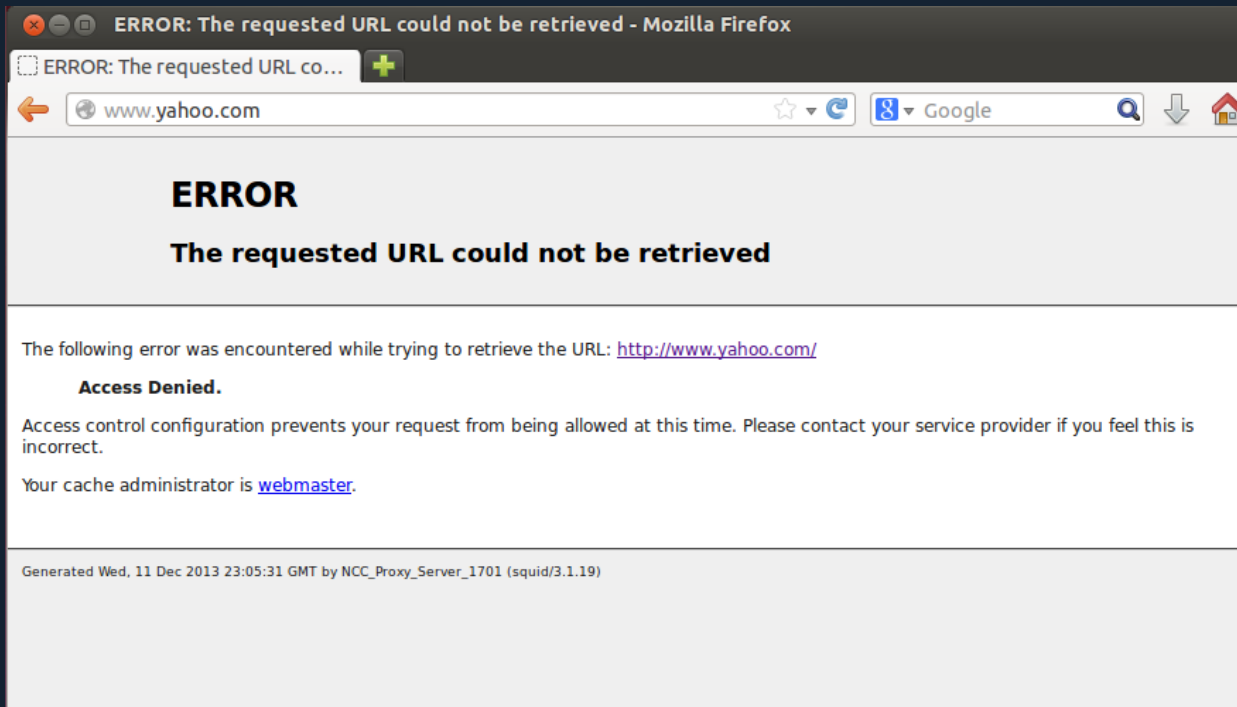
[accounts]

```
comment = Accounts data directory  
path = /data/accounts  
valid users = picard  
public = no  
writable = yes
```

Permissions prevent access



Proxy Server



Configured to prevent access to specific websites and any website outside of https

Also relays the proxy server preventing access

```
3751 #Default:
3752 # httpd_suppress_version_string off
3753
3754 # TAG: visible_hostname
3755 visible_hostname NCC_Proxy_Server_1701
3756
3757 # If you want to present a special hostname in error messages, etc,
3758 # define this. Otherwise, the return value of gethostname()
3759 # will be used. If you have multiple caches in a cluster and
3760 # get errors about IP-forwarding you must set them to have individual
3761 # names with this setting.
```

Apache Web Server

← 192.168.16.19

Linux Web Server!

Web server located in Active Directory.

This web server is in development.

root@valembun: /var/www

GNU nano 2.2.6 File: index.html

```
<html><body><h1>Linux Web Server!</h1>
<p>Web server located in Active Directory.</p>
<p>This web server is in development.</p>
</body></html>
```

User overview

	User	Host	Password	Global privileges	Grant
<input type="checkbox"/>	administrator	192.168.16.100	Yes	USAGE	No
<input type="checkbox"/>	Any	%	--	USAGE	No
<input type="checkbox"/>	Any	localhost	No	USAGE	No
<input type="checkbox"/>	Any	valembun	No	USAGE	No
<input type="checkbox"/>	debian-sys-maint	localhost	Yes	ALL PRIVILEGES	Yes
<input type="checkbox"/>	phpmyadmin	localhost	Yes	USAGE	No
<input type="checkbox"/>	root	127.0.0.1	Yes	ALL PRIVILEGES	Yes

Challenges

Configuring Linux machines so that they can join the Windows domain was very discouraging at times – whatever could go wrong, did go wrong. Even with the Ubuntu GUI, configurations still took a better part of a day, which made me very appreciative of the Windows GUI.

Red Hat configurations were another story. I had to reset the virtual machine to a previous snapshot many times because a configuration that worked the previous day, no longer worked with the configurations of a different file – reediting that file and restarting the program (i.e. SMB) would do nothing. Working entirely from the command line, it was hard to know what was affecting what (even after reviewing log files).

Many of the configurations I did for these machines, would not pass on a larger network with 1000s of computers. However, with a home or smaller network, there is more leeway for mistakes and reconfigurations.

What I Learned

- Linux distributions may have the same foundation, but the process of doing things is different (i.e. Red Hat vs. Ubuntu)
- Ubuntu may be more user-friendly than Red Hat, but it's not easy
- Some of the measures I took are not good practice because by dealing with the symptoms, I created more problems for myself later
- Linux and Windows can work together . . . But that doesn't mean it's painless
- Linux terminal is case sensitive
- User-friendly Linux distributions have a larger (more helpful) community