# Part 1

1. Access the virtual machine labeled SRV1
2. Log on with administrator and Password1
3. Set the built-in administrator account so it does not expire.
4. Set the name of the computer to be SRV1
5. The server is part of the 10.0.0.0/24. Set the following ip address information

IP v4 Address 10.0.0.10

Netmask Decimal form of /24

Gateway 10.0.0.254

Preferred DNS 1.1.1.1

1. Verify Internet Connectivity
2. Download Wireshark and install
3. Install the AD DS role
4. Make SRV1 a domain controller with domain name cyb394.com Be sure to allow DNS to be installed and configured during the promotion process.
5. After Domain install logon with Enterprise Domain Admin.
6. Create a new user with your name and set an appropriate logon name. Set the password to whatever you wish and set it to not expire. Add this user to the Enterprise Administrator and Domain Administrator security group
7. Update the default administrator password to be Security#1. Make sure the password is set to never expire.
8. Log off then logon with your personal administrative account
9. Open DNS using the DNS tool and set a forwarder to 1.1.1.1
10. Create a reverse lookup zone for your domain
11. Have your professor verify your settings.

# Part 2 (DON’T INSTALL AD-DS ON SRV2)

1. Access the virtual machine labeled SRV2
2. Set the name of the computer to be SRV2
3. Set the ip address settings so that you can join SRV2 to appropriate settings for the network.
4. Join SRV2 to the domain
5. Log on with your personal domain admin account
6. Verify internet connectivity
7. Install Wireshark.
8. Verify that SRV2 has a registered forward and reverse lookup address in DNS.

# Part 3 Part 2 (DON’T INSTALL AD-DS ON SRV3)

1. Repeat the same process for the virtual machine labeled SRV3. Make the appropriate name and address adjustments.

(Don’t JOIN SRV4 to the domain at this time)

# Part 4

1. Repeat the same process for the virtual machine labeled CLIENT1. Make the appropriate name and address adjustments.

# Part 5: Configure SRV1 to use an External Time Source

1. Issue the following command from and elevated command prompt on SRV1 on a single line.

w32tm /config /manualpeerlist:"tick.usno.navy.mil" /syncfromflags:manual /reliable:yes /update

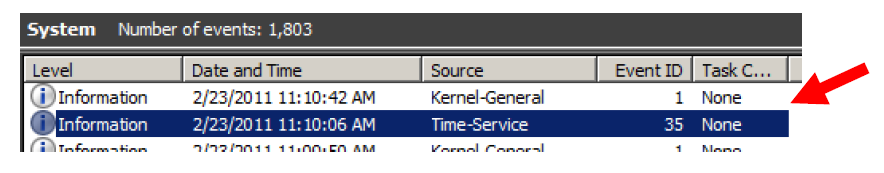
1. To check that these were set, use the following command.

w32tm /query /peers

1. To resync with time sources, issue this command

w32tm /resync

1. Check the Event Viewer and look in the Windows System log for Events 1 & 35.



# Part 6

1. Start your SRV1 image and log on with your personal administrative account. (Your other images should not be running yet.)
2. To make your lab work easier, you will set your system to stop showing the Shutdown Event Tracker when you shut down or restart. Create a new Group Policy Object called Disable Shutdown Event Tracker and link the policy to the Domain container. While you shouldn’t disable the Shutdown Event Tracker in a production environment, it helps to do this in a lab or testing situation.
3. The policy setting is in the Computer Configuration node in the Administrative Templates section in the System folder. Locate the policy setting.
4. Configure the policy so that the Shutdown Event Tracker will not be displayed.
5. Open an elevated command prompt and force the new policy to be applied to your computer.
6. Run GPRESULT /R to verify that the new policy is being applied.
7. Restart SRV1.
8. Did the Shutdown Event Tracker appear on shutdown? [ Y / N ]
9. (If it does display, troubleshoot the problem.)

# Part 7 Password Policies

1. Locate Account Policies under the Default Domain Policy
2. Adjust the Account Policies to accomplish the following objectives.

* Passwords to be at least 8 characters in length
* Users must change passwords at least once every two months (60 days).
* The system is to remember the last 5 passwords each user has used and don’t want any of those to be reused.
* A user must wait at least one day before changing a password once it has been changed.
* Pass phrases should be complex.
* Incorrect password attempts should force a lockout of 5 minutes.
* 10 bad password attempts are allowed before lockout.

# Part 8

1. Create an OU called CYB394 under the domain container.