FIREWALLS AND INTRUSION

COMP 232

LAB 05

KARAN TANK

Contents

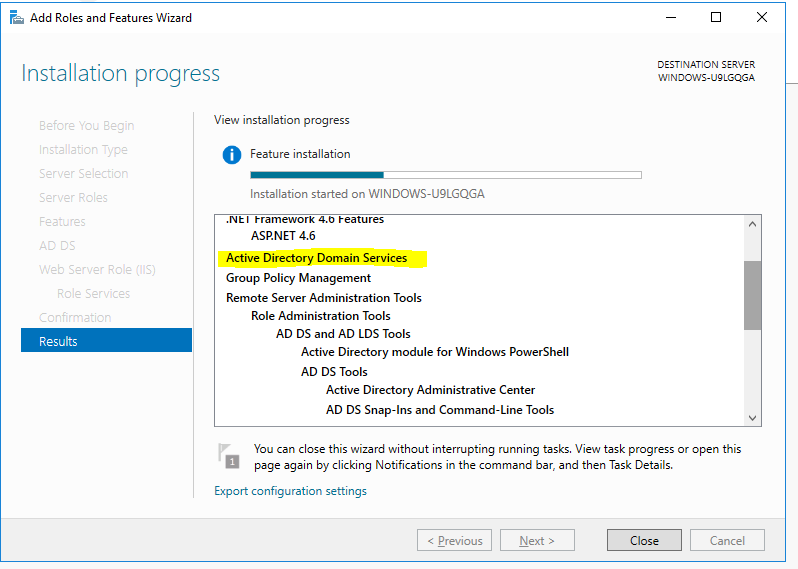
[Step 1 2](#_Toc23202059)

[Step 2 5](#_Toc23202060)

[Step 3 8](#_Toc23202061)

# Step 1

* For this, we will first setup 2 virtual machines windows server 2016 and windows 10
* On the server, we will open the server manager and install active directory domain services in the add roles and features.

Figure 1- setting up windows server 2016 as active directory

* We will then set up the new forest.
* For this, we will need to set up the root domain name.

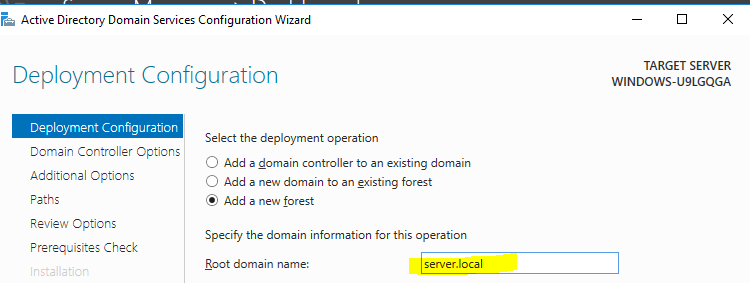


Figure 2- Setting up the root domain name / New forest

* Create the new forest

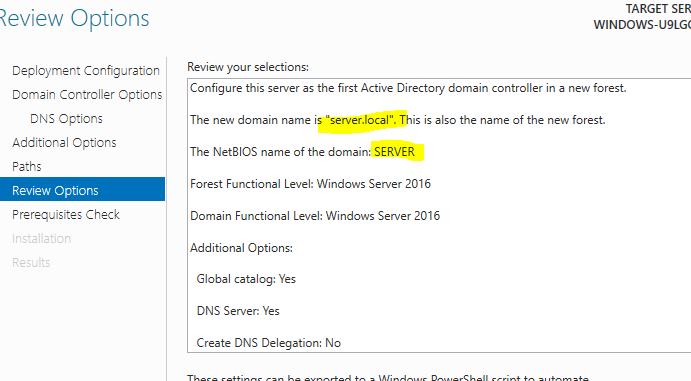


Figure 3

* Configure windows 10 with the DNS as the servers ip.
* You can do this, from the change adapter options

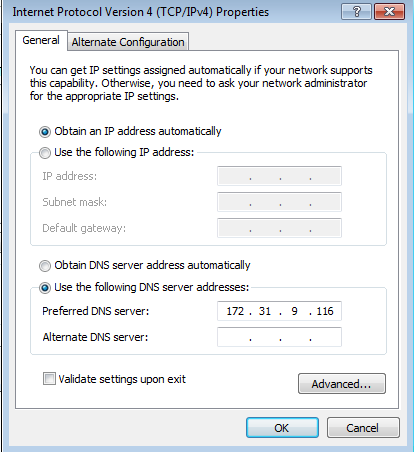


Figure 4- Configure windows 7/10 with AD's DNS

* Make windows 10 as the domain member. For this right click on this pc and go to computer name settings and add the member of name as the servers name.

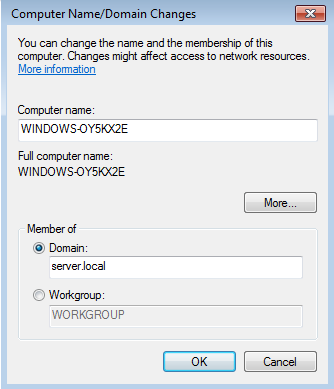


Figure 5- Windows 7/10 as a member of domain

* After you do this settings, the machine will restart as the member pc.

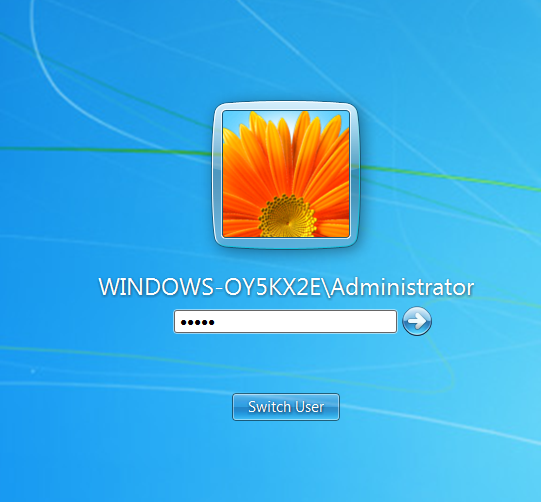


Figure 6-Logging after being domain member

* In the Active directory of the server, you should be able to see the you member pc in the computers tab.

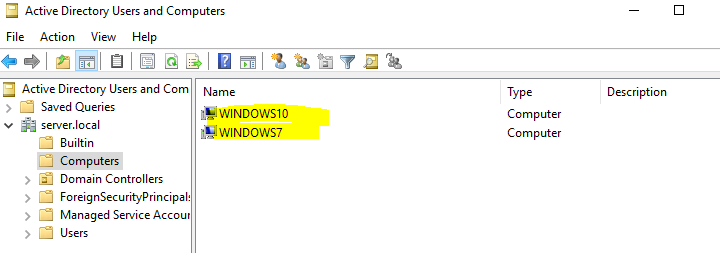


Figure 7

# Step 2

* We will be making windows 10 as the event collector and windows server 2016 as the event forwarding machine.
* For this, we will open the event viewer on the windows 10, and in the subscriptions tab, we will add a new subscription and select all windows log and add the server. Select the source initiated events.

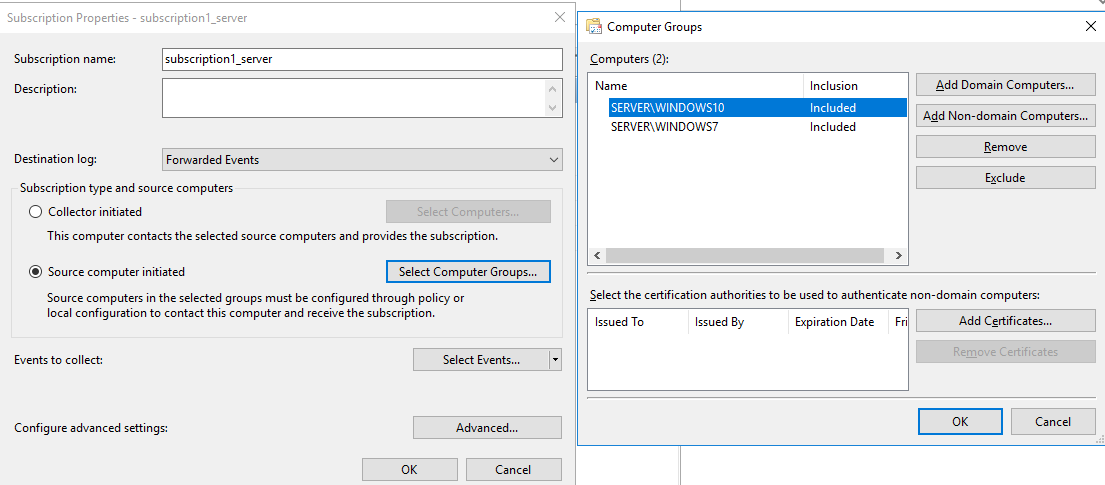


Figure 8

After setting up the subscription, you should see the logs in the forwarded events on the collector.

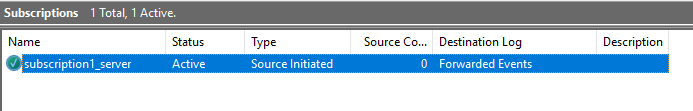


Figure 9

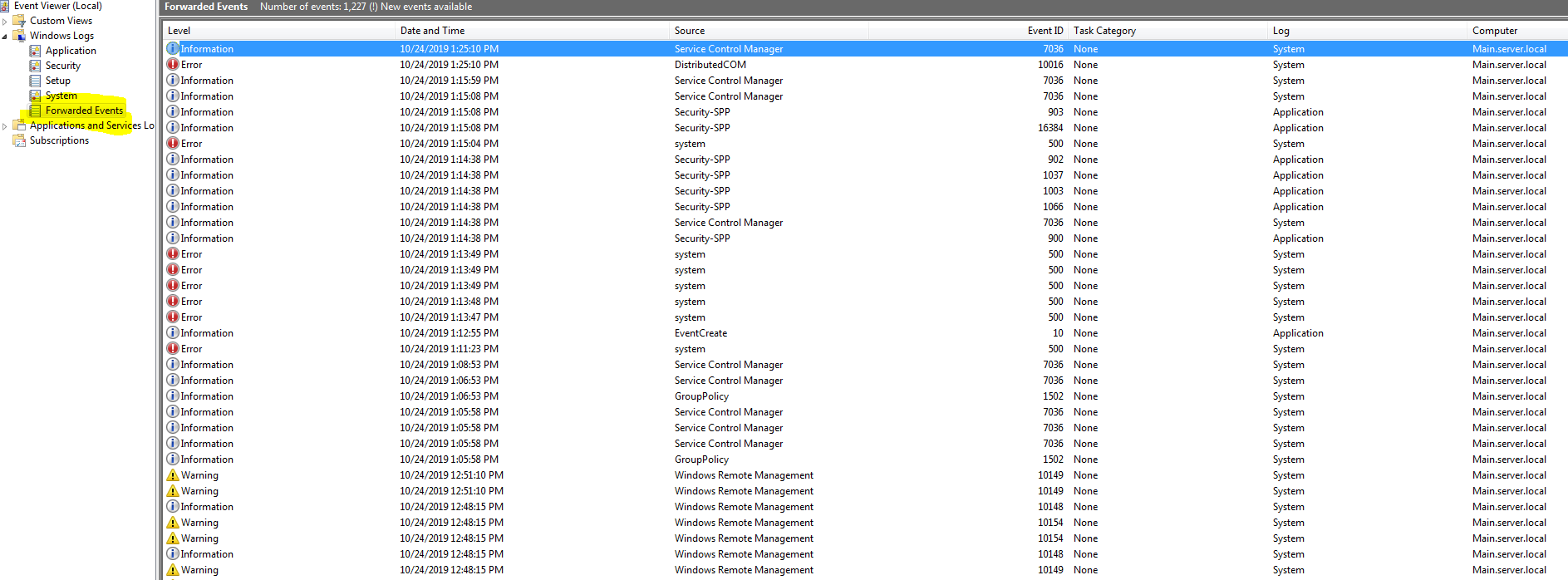


Figure 10

In the GPO settings, we will open the log access on the server and copy the channel access code there.

To get the channel access code, we will type the command wevutil gl security

We do this because, you can see the system and application logs, but the security logs does not get access easily.

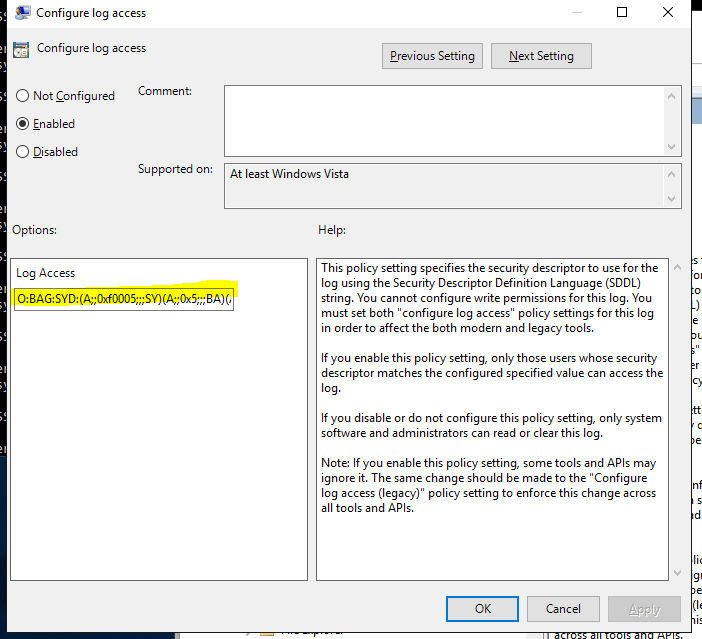


Figure 11

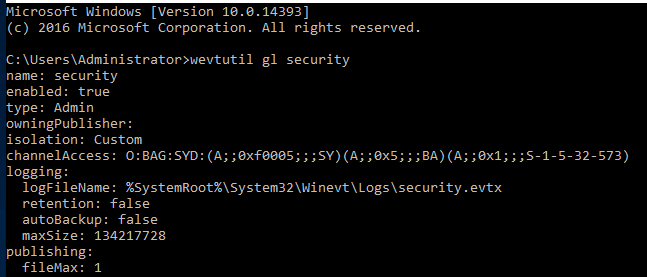


Figure 12

# Step 3

Now we will create a password,.txt file and we will go to its settings, security advanced settings, in the auditing we will add the access to everyone. And we will give it all type rights which means it will log if the file open is successful or opening file gave an error.

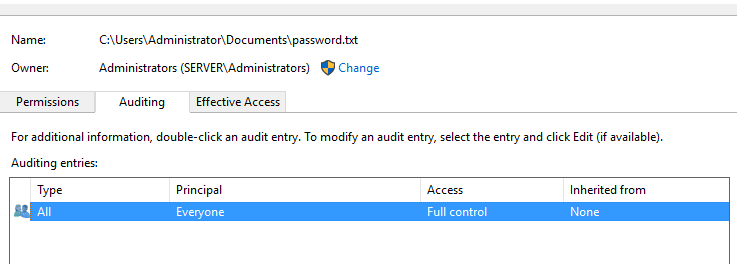


Figure 13

After that every time we open the file, we will see the logs into the security tab.

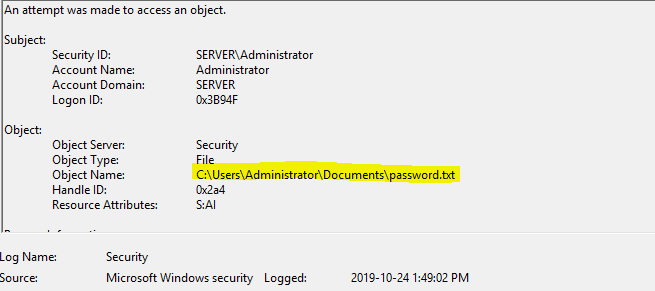


Figure 14

We will need to add the server and network services in the event log reader in the computer management.

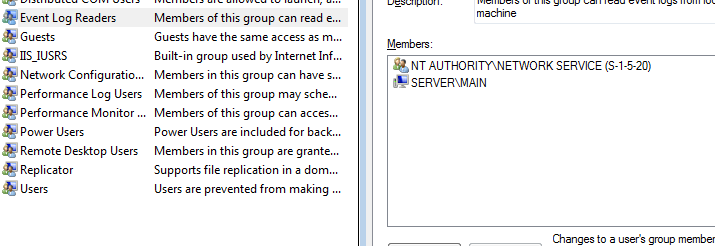


Figure 15

Now you should see the logs of the file opening on the event collector that is windows 10

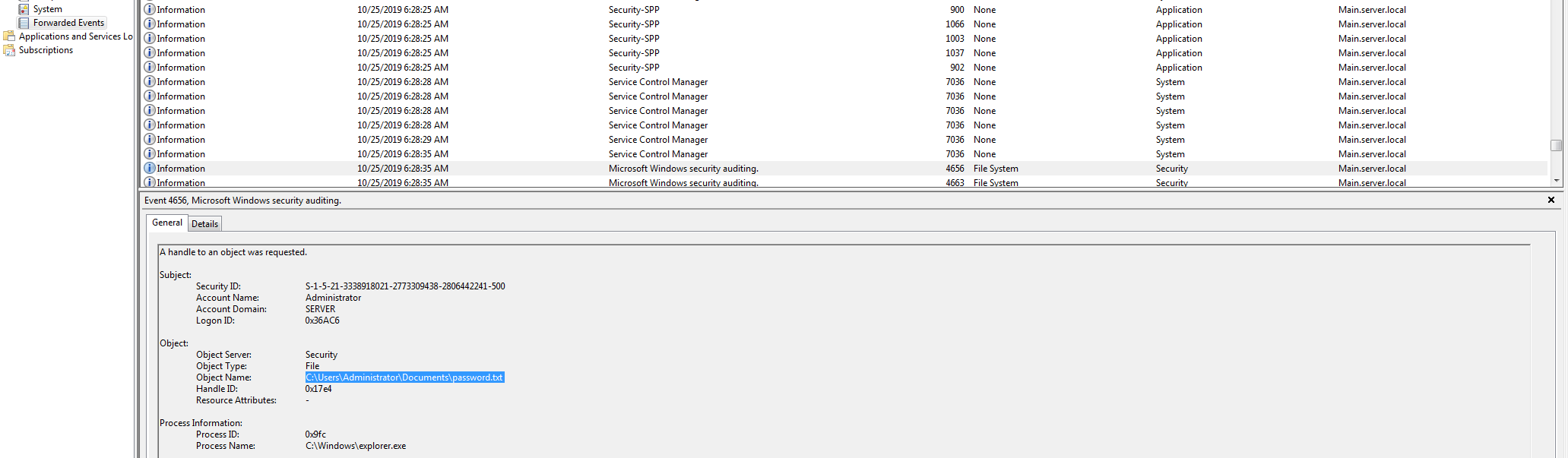


Figure 16