SMW Journal 2 Week 10

Done by: Lee Yi Terng (1904189)

Class: DISM/FT/2A/04 | Date: 27th June 2020

Submitted To: Ms Teo Seok Ling

# Topics Covered

* Policy Application Order
* Security Policies
* Internet Information Services (IIS) Web Server

# Internet Information Services (IIS) Web Server

This was from Exercise 3 of SMW Lab 4. It involved installing the IIS service into my SMW 2012 Server and hosting it. During installation of the web server, I encountered a problem during the Installation Progress. I was never able to finish the installation due to “Windows Remote Management was not started and attempts to start it had failed”. I tried restarting my VM, using various admin accounts, both local and domain to try and figure out what went wrong. I went to troubleshoot on Microsoft forums and finally realised that my Remote Management on SMW2012 was disabled for some reason. Hence, I went into the local admin account to activate it, and installation worked.

After installation, I set up a virtual directory called “C:\MyWebsite” as per practical requirements. I followed all the steps until I reached step 15, where there was the question of restricting the website only to clients from the smw.soc.com domain.

After installing the IP and Domain Restriction Server Role, I had this urge to go find out how to carry out this task. I googled and went to read documentation from Microsoft and found out how to access it through the IIS Manager.

After playing around with it for about an hour I discovered that the restrictions could be set at either the website level, or even at file level. I had to option to either restrict the whole website to only allow access from clients in the domain or restrict a certain folder like “userlist” or “webdoc” instead.

The restrictions also allow you to add either an Allow or Deny Entry based on your needs. By default, the restrictions you can set only include IP address ranges and a specific IP address. To include domains, you have to go to “Edit Feature Settings” on the right pane and tick “Enable Domain Name Restrictions”. In this window, you can also decide whether access should be allowed for unspecified clients. In my case, I put Deny. You can also change the “Deny Action Type” here, choosing from “Abort”, “Unauthorized”, “Not Found” or “Forbidden”. You can use this to decide what error message to send back when an unauthorized client try to access the website.

Finally, after all the settings are set up, I went to create an Allow entry for domain “smw.soc.com”. I then tested this with my Win10, SMW2016 and Host PC. My Host PC was unable to access the site while my Win10 and SMW2016 VMs could. This showed that it was working as intended.

As an added fun, I went to experiment with each of the Deny Action Types mentioned above to see the difference in both the returned page and the HTTP Response Headers.