

Assignment 2 Report

Group 12

Part 1	2
Linux	2
Window	2
Explanation	2
Part 2	3
For linux machines	3
Ftp server (https://www.howtoforge.com/tutorial/how-to-install-and-configure-vsftpd/):	3
Http server:	3
For Windows VM	4
Ftp server (https://vpsie.com/knowledge-base/how-to-setup-ftp-server-users-on-windows-2012-r2/):	4
1- Enable Web Server (IIS) role and FTP Server role service.	4
2- Create FTP users	5
3- Configuring FTP global IIS settings.	5
4- Creating FTP site.	6
5- IIS Firewall setup.	7
6- Windows Firewall setup.	7
7- Testing	8
Http server:	8
Install secure features	8
Set up http website	10
Set up system account for authentication	11
Restrict access to only one user	12
To achieve the ability to authenticate using user account:	14
Linux:	14
Windows	14
Part 3:	15
Contribution:	16

Part 1

1. Linux

a2user

VxSB8ykTA:bvLb)^~vLWAJ%jWXd35t2E

Root

DPkn\$qBZ_CUknsN\$yx=NsFMff2s2X^Q&

2. Window

a2user

SE&db&v`69p+<k`D=xLY2dNRVen!LjW\$

Administrator

v@ArN&&D2rcGa#nqLHyf4\$7Zcr4+HV_X

Explanation

Passwords are generated from <https://passwordsgenerator.net/> with length 32, include Symbol, Number, Lowercase, Uppercase, and leetspeak characters.

- These passwords are strong because since it is generated randomly, it is less vulnerable to dictionary attack, which usually is a combination of meaningful terms like a word, name, place.
- It is also long and uses a large alphabet, which helps prevent brute force attack to work in a reasonable time:
 - If someone were to know the length of the passwords, and that the alphabet is ASCII printable, it will take them 95^{32} guesses.
 - If someone were to know the 32 characters in the passwords (without knowing the order), it will still take them $32!$ guesses.
- The passwords are generated from the first letter of several words. There are no direction relation between these words and symbols. It is not a sentence or common words combinations, which make sure that it is strong to dictionary attacks. It is also long and uses a large alphabet, which helps prevent brute force attack to work in a reasonable time. Also, they are not rely on obvious substitutions. There is no guessing pattern for the passwords. The passwords for two machines are generated differently so that if one of the password leaks, the attacker won't break into the other machine too.

Part 2

1. For linux machines

- a. Ftp server (<https://www.howtoforge.com/tutorial/how-to-install-and-configure-vsftpd/>):

Install the following packages:

- vsftpd
- Install any missing dependencies

Edit /etc/vsftpd.conf to configure FTP server:

- anonymous_enable=YES # to enable anonymous access
- anon_root=/var/ftp/

b. Http server:

Install the following packages:

- [apache2](#)
- [apache2-bin](#)
- [apache2-data](#)
- [libapr1](#)
- [libaprutil1](#)
- [libaprutil1-dbd-sqlite3](#)
- [libaprutil1-ldap](#)
- [libc6](#)
- [libldap-2.4-2](#)
- [libpcre3](#)
- [libssl1.0.0](#)
- [libxml2](#)
- [zlib1g](#)
- [lsb-base](#)
- [mime-support](#)
- [procps](#)
- [libapache2-mod-authnz-external](#)
- [pwauth](#)
- Install any additional missing dependencies

Configure pwauth (for system account access):

- vim **/etc/apache2/apache2.conf**
- Add at end of file:

```
<IfModule mod_authnz_external.c>
    AddExternalAuth pwauth /usr/sbin/pwauth
    SetExternalAuthMethod pwauth pipe
```

`</IfModule>`

- vim **/etc/apache2/sites-enabled/000-default.conf**

- Edit the file to look like:

```
AddExternalAuth pwauth /usr/sbin/pwauth
SetExternalAuthMethod pwauth pipe
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
<Directory "/var/www/html">
    AuthType Basic
    AuthName "Login"
    AuthBasicProvider external
    AuthExternal pwauth
    Require user a2user # or any other account you want
</Directory>
```

- Restart apache2 by: `sudo service apache2 restart`

Configure default webpage for apache2:

- vim **/etc/apache2/sites-enabled/000-default.conf**
- Add this line inside `<Directory>` block:
`DirectoryIndex webcontent.html`
- Restart apache2 by: `sudo service apache2 restart`

2. For Windows VM

- a. Ftp server (<https://vpsie.com/knowledge-base/how-to-setup-ftp-server-users-on-windows-2012-r2/>):

1- Enable Web Server (IIS) role and FTP Server role service.

1. *Log in to the server by using an administrative account*
2. *Open Server Manager*
3. *Go to **Manage > Add Roles and Features***
4. *Click **Next***
5. *Select **Role-based or feature-based installation***
6. *Click **Next***
7. *Select **Select a server from the server pool**, and select your server*
8. *Click **Next**.*
9. *Scroll down and put a check mark in **Web Server (IIS)***
10. *An Add features window pops up. Put a check mark in the **Include management tools (if applicable)** option*
11. *Click **Add Features** button*
12. *Click **Next***

13. Click **Next**
14. Click **Next**
15. Scroll down and put a check mark in: **FTP server, FTP Service and FTP Extensibility.**
16. Click **Next**
17. Click **Install**
18. When installation is finished, click **Close**

2- Create FTP users

You need to create users in Windows in order to be able to use FTP services.

You can use either local or domain users.

In this case, I will create some local users.

The only thing that changes if you use domain users is, when you log in to FTP, you must use the domain/account format.

1. In Server Manager go to **Tools**
2. Click **Computer Management**
3. Click **Local Users and Groups**
4. Click **Users**
5. In the center pane, right-click a blank area and then select **New User...**
6. Enter the username information and click the **Create** button
7. Create as many usernames you need here.

*Optionally, you can create a group that contains all the FTP users in the **Groups** folder and add the users you created above.*

3- Configuring FTP global IIS settings.

You need to configure some global settings for your IIS server before creating your FTP site.

It is very easy, follow the steps below:

1. In Server Manager go to **Tools**
2. Click **Internet Information Services (IIS) manager.**
3. In the left pane, double-click the server icon (in the tree below the option **Start Page**)
4. If a window pops up asking about Microsoft Web Platform, select **Do not show this message**, and click the **No** button
5. In the center pane, double-click the **FTP Authentication** icon
6. If you want to allow anonymous users, right-click **Anonymous Authentication** and set it to **Enable**.
7. To allow access to the windows users you created in Part Two above, right-click **Basic Authentication** and set it to **Enable**.
8. In the left pane, double-click the server icon.
9. Double click the **FTP Authorization Rules** option

10. Delete all rules in the center pane.
11. After all rules have been deleted, right-click a blank area in the center pane and select the option **Add Allow Rule...**
12. Click the option **Specified users**.
13. In the text box type the usernames (separated by commas) you created in Part Two above.
14. Check either the boxes **Read** or **Write** depending the access you want to grant to the user or group of users you are adding.
15. Click the **OK** button
16. Repeat steps 8 to 15 if you want to add more users with different Read / Write permissions.

4- Creating FTP site.

1. Open Windows Explorer
2. Navigate to **C:\inetpub\ftproot**
3. This is the default local folder where the FTP directory tree will be saved
4. You can create your own folder in another directory or hard drive if you want.
5. Create your own folder at this point if it is desired.
6. Open **Server Manager**
7. Go to **Tools**
8. Click on **Internet Information Services (IIS) Manager**
9. In the left pane, right-click the server icon (in the tree below the option Start Page)
10. Click **Add FTP Site**
11. In FTP site name type a friendly name for your site. (**My FTP Site** for example)
12. In **Physical path** browse to the folder you created in steps 2 to 5
13. Click **Next**
14. In IP Address, click the drop down menu, and select the server's IP address you want to assign to the site
15. Port remains as **21** by default. You can change it if you want.
16. Ensure the option **Start FTP site automatically** is checked
17. Select the **No SSL** option if you are not required to use certificates. Otherwise, select one of the other options.
18. Click **Next**
19. In the Authentication section, put a check mark in **Anonymous** If you want to allow anonymous users.
20. Put a check mark also in **Basic** to allow access to users created in Part Two.
21. In the Allow access to: drop down menu, select: **Specified Users**
22. In the text box type the usernames of the users you created in Part Two.
23. Check the box **Read** to grant read access to users.
24. Check the box **Write** to grant write access to users.

25. Click **Finish**

5- IIS Firewall setup.

1. In Server Manager go to **Tools**
2. Click **Internet Information Services (IIS) manager**.
3. In the left pane, double-click the server icon (in the tree below the option **Start Page**)
4. In the center pane, double-click the **FTP Firewall Support** icon
5. In the **Data Channel Port Range** box, make sure the value is **0-0** to use the default port range.
6. Or, you can change it if you want by your own set of ports.
7. Click **Apply**
8. Close Internet Information Services (IIS) Manager

6- Windows Firewall setup.

By default, all exceptions needed for FTP are added to the Windows Firewall at the time you enable the FTP Server role.

Anyway, for troubleshooting purposes, I will show the configuration that needs to be in place in order to allow FTP traffic in your server.

1. Open Server Manager
2. In the left pane, click **Local Server**
3. In the right pane, click the hyperlink beside the **Windows Firewall** option. It should say **Public:On** (or Off).
4. The Windows firewall window opens. In the left pane click **Advanced Settings**
5. The Windows Firewall with Advanced Security window opens. In the left pane click **Inbound Rules**.
6. In the right pane, verify there's a rule called **FTP Server (FTP Traffic-In)**
7. Double click this rule.
8. In the **General** tab, verify the option **Enabled** is checked.
9. Go to the **Protocols and Ports** tab.
10. Verify the Protocol type is **TCP** and the **Local port** value is **21**.
11. Go to the **Advanced** tab
12. Make sure the profiles: **Domain**, **Private** and **Public** are checked.
13. Click **OK** button
14. Execute the same validation in steps 7-13 for the **FTP Server Passive (FTP Passive Traffic-In)** rule. Except that the local port value in this rule should be **1024-65535**
15. Execute the same validation in steps 7-13 for the **FTP Server Secure (FTP SSL Traffic-In)** rule. Except that the local port value in this rule should be **990**
16. In the left pane, click **Outbound Rules**

17. Execute the same validation in steps 7-13 for the **FTP Server (FTP Traffic-Out)** rule. Except that the local port value in this rule should be 20
18. Execute the same validation in steps 7-13 for the **FTP Server Secure (FTP SSL Traffic-Out)** rule. Except that the local port value in this rule should be 989
19. Close all windows.

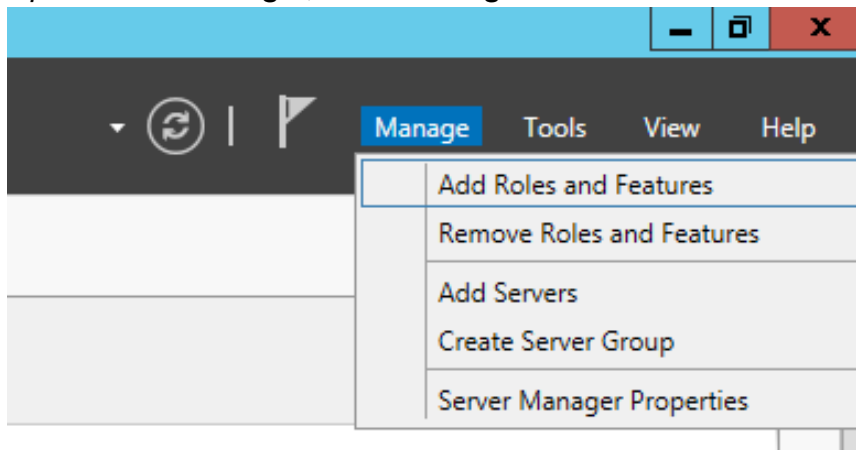
7- Testing

- The last part is to test your work.
- Make sure you can connect to the FTP service, first from the local machine and then from a remote computer.
- Try to log in, put files, get files, show folder contents, etc

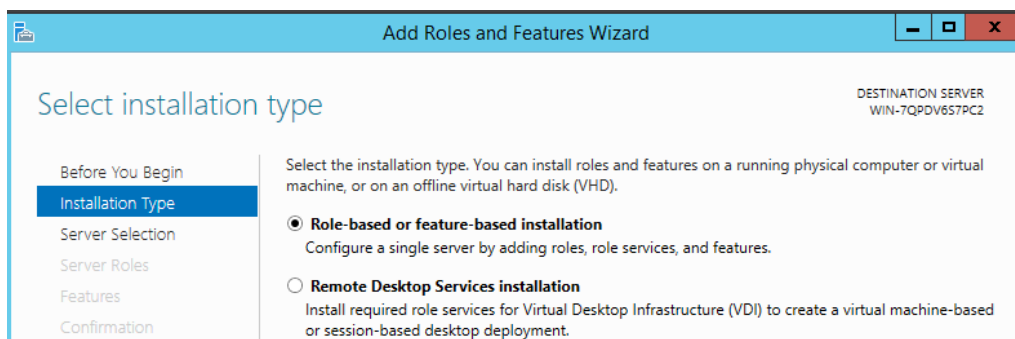
b. Http server:

Install secure features

- Open **Server Manager**, select **Manage > Add roles and Features**



- Click **Next**.
- Select **Role based or feature based installation**. Click **Next**.



- **Select your server. Click *Next*.**

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
WIN-7QPDV6S7PC2	10.229.12.5	Microsoft Windows Server 2012 R2 Standard

- **Select all under *Web Server (IIS)* > *Web Server* > *Security***

☒ Web Server (IIS) (18 of 43 installed)

☒ Web Server (15 of 34 installed)

☒ Common HTTP Features (4 of 6 installed)

☒ Health and Diagnostics (1 of 6 installed)

☒ Performance (1 of 2 installed)

☒ Security (Installed)

☒ Request Filtering (Installed)

☒ Basic Authentication (Installed)

☒ Centralized SSL Certificate Support (Installed)

☒ Client Certificate Mapping Authentication (Installed)

☒ Digest Authentication (Installed)

☒ IIS Client Certificate Mapping Authentication (Installed)

☒ IP and Domain Restrictions (Installed)

☒ URL Authorization (Installed)

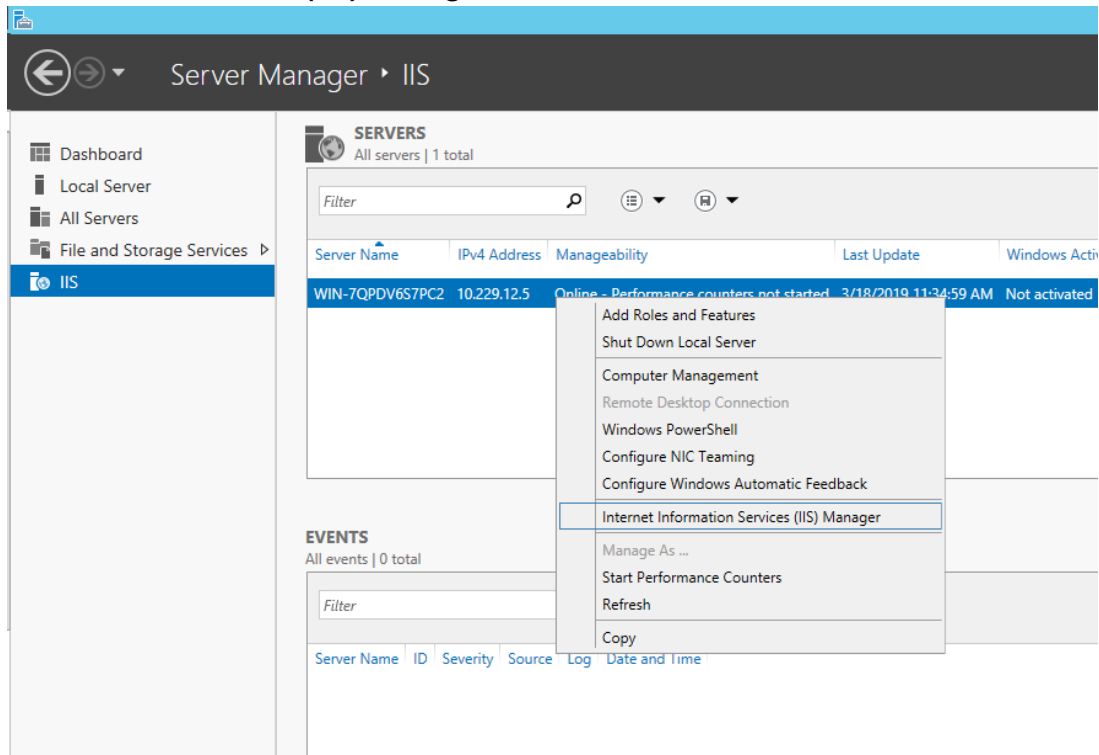
☒ Windows Authentication (Installed)

☐ Application Development

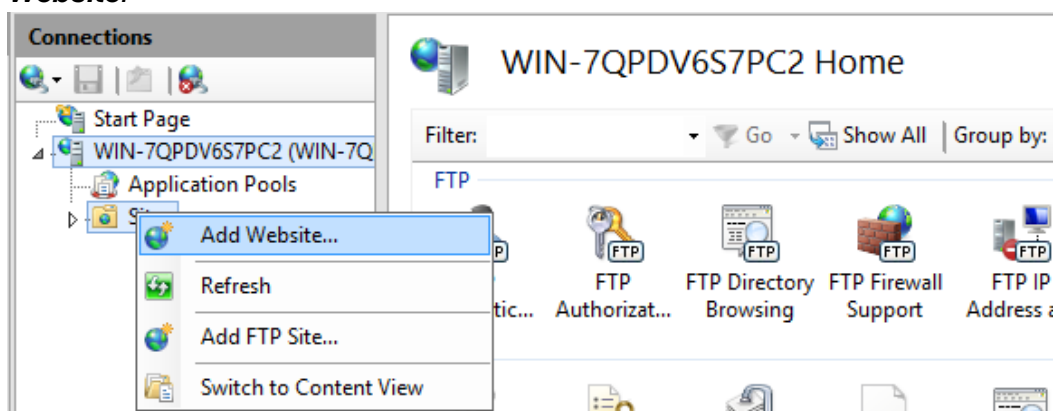
- ***Next Next and Install***

Set up http website

- Open **Server Manager**, and select **IIS**, right click your server and select **Internet Information Services (IIS) Manager**.

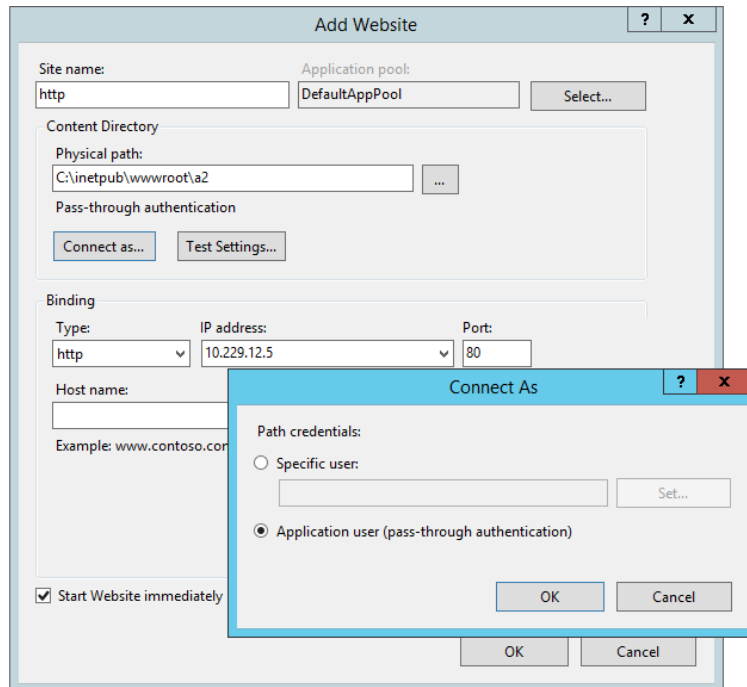


- In the **Connections** pane, right-click the **Sites** node in the tree, and then click **Add Website**.



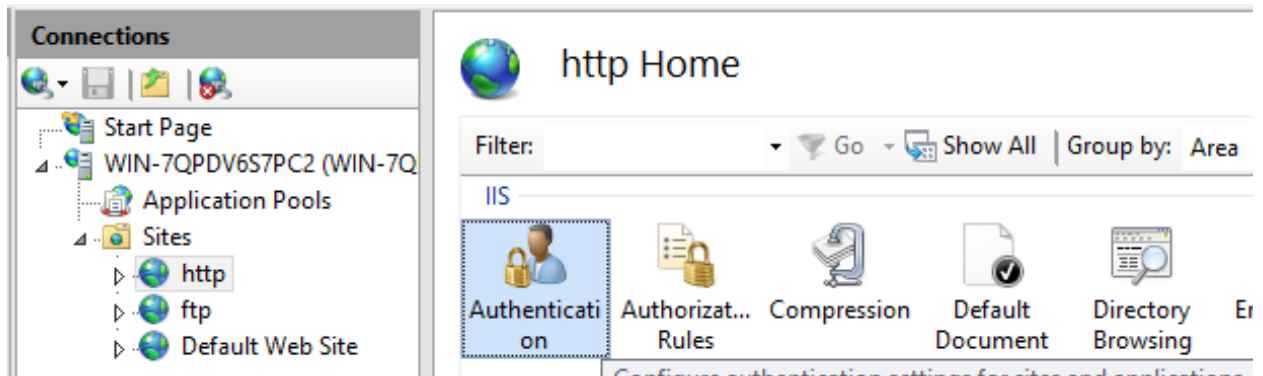
- In the **Add Website** dialog box, enter a friendly name for your website in the **Site name** box.
 - In the **Physical path** box, enter the physical path of the website's folder, or click the browse button (...) to navigate the file system to find the folder.
 - Select the **Application user (pass-through authentication)** option in the **Connect As** dialog box.
 - Select the protocol for the website from the **Type** list.

- Enter the IP address in the **IP address** box.
- Enter a port number in the **Port** text box.
- Select the **Start Website immediately** check box.
- Click **OK**

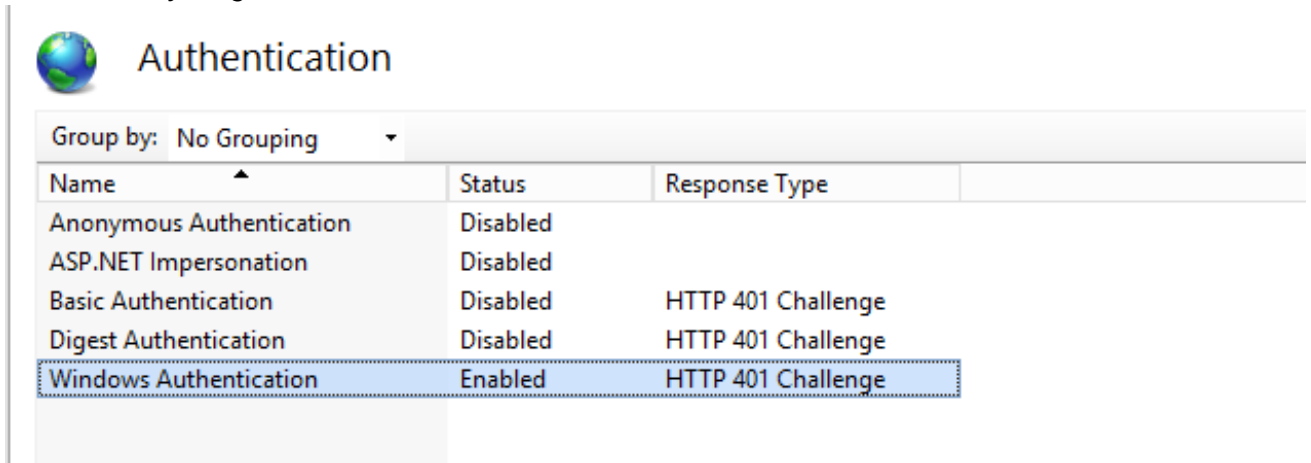


Set up system account for authentication

- In **Features View** of IIS Manager, double-click **Authentication**.



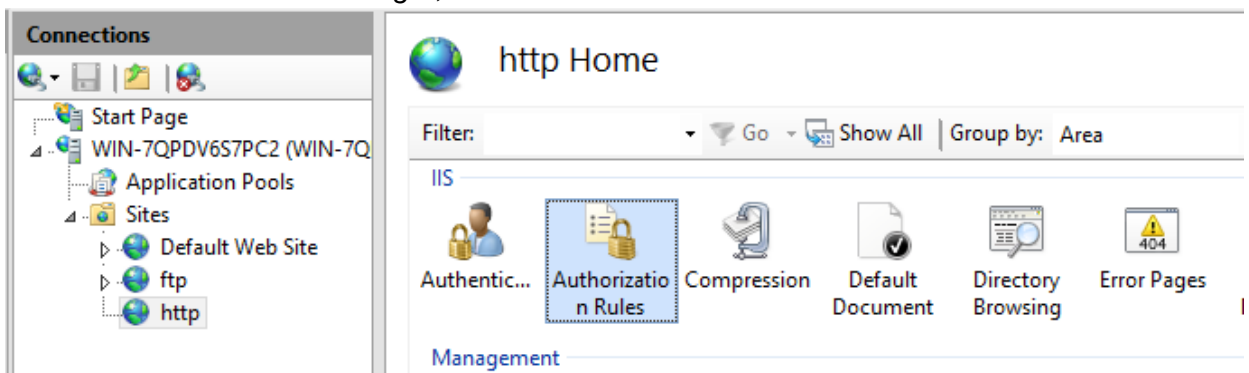
- Disable everything and enable **Windows Authentication**.



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Windows Authentication	Enabled	HTTP 401 Challenge

Restrict access to only one user

- In **Features View** of IIS Manager, double-click **Authorization Rules**.



Connections

- Start Page
- WIN-7QPDV6S7PC2 (WIN-7Q)
- Application Pools
- Sites
 - Default Web Site
 - ftp
 - http

http Home

Filter: [Go] Show All | Group by: Area

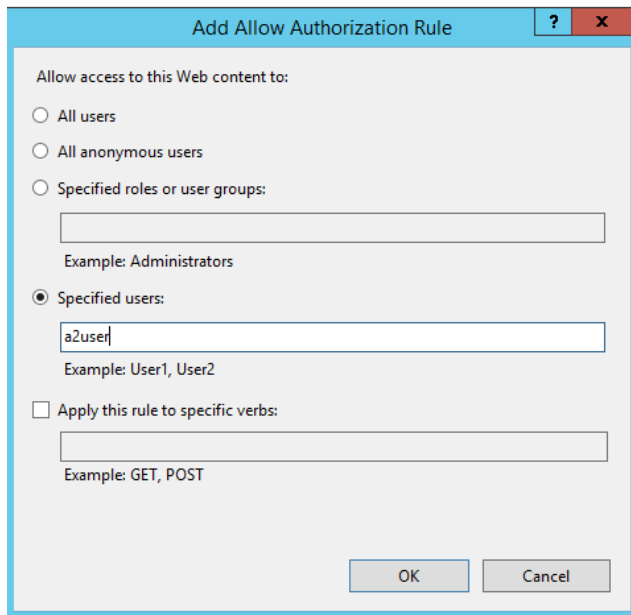
IIS

Authentic... Authorization Rules Compression Default Document Directory Browsing Error Pages

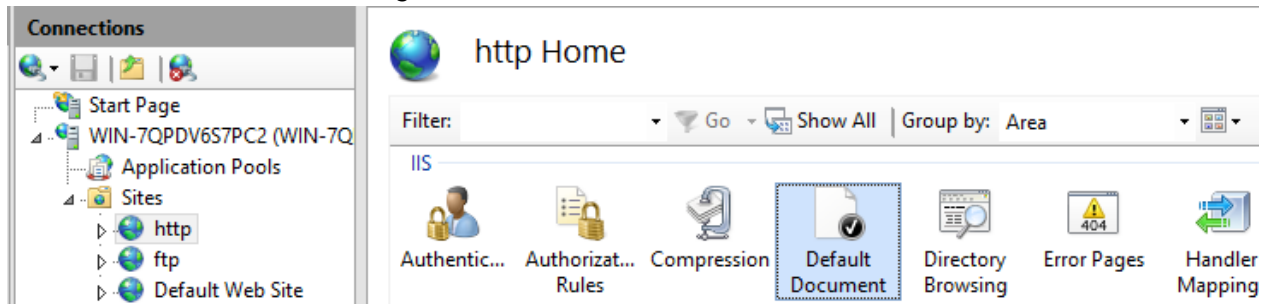
Management

- Delete all default rule. Select **Add Allow Rule...** on the right panel.

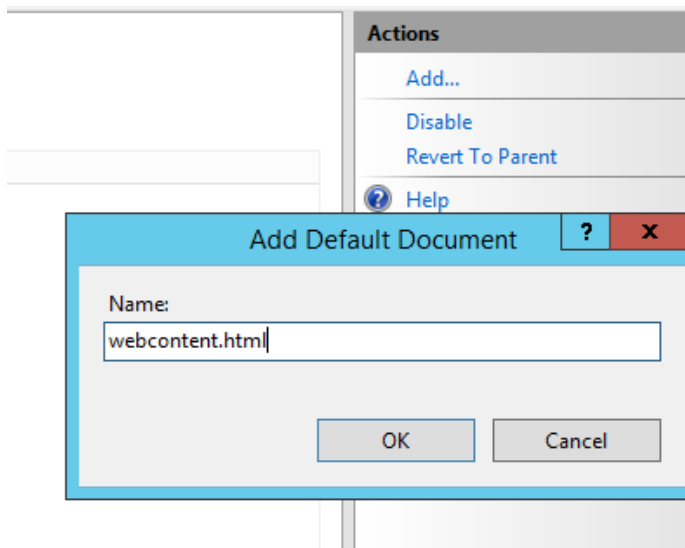
- Enter authorized user name created in part 1 (a2user)



- In **Features View** of IIS Manager, double-click **Default Document**.



- In the **Actions** pane, click **Add**.
- In the **Name** box, enter `webcontent.html` that you want to add to the list of default documents and then click **OK**. This is added to the top of the default document list.



To achieve the ability to authenticate using user account:

a. Linux:

- Install packages:
 - [libapache2-mod-authnz-external](#)
 - [pwauth](#)
- Configure **apache2.conf** and **000-default.conf** as shown above.

b. Windows

- Install **Security** features as shown above.
- Configure **Authentication** and **Authorization** as shown above.

If the user change their password, the new password will be used to authenticate http access. This is because the user database used by http service is the system user database and not a separate one.

There is not any similarity in the process, except for both requires system user account to be created.

Part 3:

- See attached html.
- Hover over each arguments to see its explanation.
- The purpose of each command is under “sudo iptables” section.

Contribution:

Minh Nguyen: Part2, Part 3

Jiaqi Liu: Part 1, Part 2

Xinyu Chen: