Systems Administration and Security

CIS3017-N-Fj1-2018

Word Count: 4999

Thomas Ruddock

Q5114161

Mohammad A. Razzaque

Teesside University

Table of Contents

Introduction

This report will have 4 questions with individual reports. In each question it will have sub-sections to keep it well-structured and on point, all references will be cited in the correct sections when used. After that is the reference section which will have the full Harvard style referencing from the cited references in the main body of the work.

Question 1: Selection of suitable cryptography for a company in expansion (959 words)

1. Security to the digital communications, symmetric-key or public-key cryptography

This report will talk about the difference between symmetric-key and public-key cryptography and which one is more suitable to a healthcare based company. Since the company is based in a healthcare service, I believe the company would want the fastest communication with its new office in the South. But also want the communication's to be secure because of sensitive data of the patients. I will be describing the both options with the advantages and disadvantages then finish off with a conclusion which will show the best option for the problem the company has.

1.1 Symmetric-key Encryption

Symmetric-key is a cryptography method which is using high level mathematical principles in storing and transmitting the data or message. Symmetric is one of the simplest kinds of encryption which include only one secret key or private key to cipher and decipher the information on this cryptography method. There are a number of different types of symmetric encryption like AES, Blowfish, RC4, DES, RC5 and RC6, the most commonly used symmetric algorithm is the AES-128, AES-192 and AES-256 In the two sections below it will show the advantages and disadvantages of using symmetric-key. The communication starts off with a plain text then gets encrypted by the secret key, which will then cipher the text (in a length of 128-bits and 256-bits) making it impossible to read it is then sent to the new office which will use the same secret key to decrypt the file which will then turn it back to plain text and able to read, edit, etc (SSL2BUY Wiki - Get Solution for SSL Certificate Queries, n.d.). Image shown below.

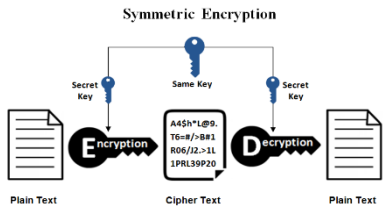


Figure 1

1.1.1 Advantages

- The main advantage of using symmetric over other encryption methods is the speed on which it encrypts and decrypts messages, making it suite well with the health care services.
- It is relatively inexpensive to create a very strong secret key for the ciphers compared to the public-key.
- Uses less computer resources compared to the public-key encryption method. Even though the company will have large number of storage space this point is not as important.
- Can keep different parts of the company secure by having multiple different secret-keys for different departments. IT keeps the company more secure in case of a compromised key.

1.1.2 Disadvantages

- It needs a secure channel for the secret key too be exchanged between the two offices. But since the company is still in the UK the key can be delivered in person to eliminate the other secure channel.
- It can become too many secret keys, since the company is about health care they will be multiple departments, with different keys and will need a system which can ensure the security of all the keys.
- One very big issue is the origin and authenticity of the message received cannot be guaranteed meaning the message could have been 3rd partied on its transit. This can lead to an issue since the company is about people lives.

1.2 Public-key Encryption

Public-key also known as asymmetric, this method is relatively new compared to symmetric-key. This method uses two keys the public key and secret or private key to encrypt and decrypt the message. The public-key method encrypts the message with the Public key which is freely available to anyone who would want to send the company a message, once it have been used to encrypt the message it becomes a cipher text (in a length of 1024-bits and 2048-bits) and the only way to see the contains of the file is to use the private and or secret key to decrypt the message. In the two sections below will be the advantages and disadvantages connecting to the company. The Public-key encryption is mainly used in every day communication, over the internet the main algorithms used is EIGamal, RSA, DSA, PKCS and Elliptic curve techniques (SSL2BUY Wiki - Get Solution for SSL Certificate Queries, n.d.).Image shown below.

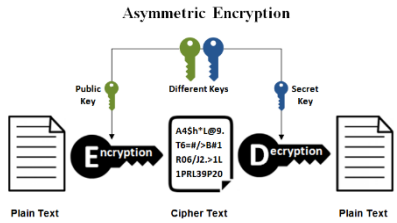


Figure 2

1.2.1 Advantages

- A benefit over the symmetric is convenience meaning that you won't have to distribute all the secret keys for each department, all they need to know is the public key and the private key is kept a secret.
- Another advantage over the symmetric method is that the message needs to be authenticated by the sender which means the message came from the person it says and not a 3rd party.
- It is more secure than passwords because a malicious user most have both keys to look like a real user on the company network.

1.2.2 Disadvantages

- It takes relatively more time than symmetric encryption which might slow down the work flow of the company, which will damage the speed and communication.
- If the private keys can't be protected, the security is not better than having a password.
- Since the company is expanding and big disadvantage is the method is not very good at scalability, it takes time to distribute the keys in large companies
- If the private key is lost for any department it means that all the messages won't be able to be decrypted.

1.3 Conclusion

To conclude this report the best encryption method for the company will be the symmetric-key encryption method. The few main reasons for picking this method. Firstly the company is opening a new office which mean expansion and Public-key is bad with scalability. Secondly the company is in the health care services meaning communication should be almost instant or close to it, since it is to do with people's lives and health. Thirdly it keeps the different departments more secure in case of a secret key leak, because each department will have a different key. Finally the securing of moving the secret keys to the new location in the South can be done in person, which prevents the keys getting sniffed while crossing the internet.

Question 2: Keccak (SHA-3) (661 words)

This short report will be talking about the SHA-3 also known as Keccak which will include its internal working and its strengths and weaknesses. SHA-3 also called secure hash algorithm 3. Keccak is based on a sponge construction and the results are squeezed out, instead of the older SHA which are Merkle-Damgard (M-D), because of this it will not be as vulnerable to the same types of attacks that the older algorithms had in earlier SHA algorithms. For example the length extension attacks which effect the older SHA algorithms like SHA-1 and SHA-2. This new algorithm was released by NIST (National Institutes of Standards and Technology) back in 2012. There are four different types of standards of SHA-3 called SHA3-224 which has r = 1152 (bitrate), c = 448 (capacity), it has 224 bits in output length and 112 bits in security level. Then one is SHA3-256 which has r = 1088 (bitrate), c = 512 (capacity), it has 256 bits in output length and 128 bits in security level. Next is SHA3-384 which has r = 832 (bitrate), c = 768 (capacity), it has 384 bits in output length and 192 bits in security level. The last one is called SHA3-512 which has r = 576 (bitrate), c = 1024 (capacity), it has 512 bites in output length and 256 bits in security level, (Keccak.team, n.d.) They have two extendable output functions SHAKE128 and SHAKE256.

The table below will show the strengths and weaknesses of the SHA-3 algorithm (Keccak) It will most likely have more strengths than weakness as it is a newer algorithm than SHA-1 and 2 and is less likely to show the weakness of new algorithm hitting the market which could affect it implementation.

Strengths	**Weaknesses**
New algorithm for cryptography coin mining and protection	Takes longer to compute the hashing when encrypting.
The older hacks from SHA-1 don't work on SHA-3.	A lot slower than SHA -1 in software only
When generating a message the hash values are much bigger that SHA-1 and SHA-2, in the area of hash value, password and cryptography.	Very little in common with SHA-2 it will make it a learning curve.
Extremely good in different environments	Almost none of the world's software or hardware supported it.
Susceptible to different analytical insights	The use would have to write their own code and firmware for every device they want the SHA-3 to be implemented on.

Has a high security margin with high quality analysis	SHA-3 was relativity a new-comer shortly after the SHA-2 migration from SHA-1.
Preforms extremely good on hardware, which gives it good overall performance	Most have mitigated to SHA-2 recently and less likely to move until as flaws are ironed out.
Has some design diversity from SHA-2	
More secure and harder to impossible to crack the encryption.	

In this table the author used some information from (Grimes, 2018) and (Kelsey, 2013).

2. Conclusion

In conclusion SHA-3 will be the next algorithm for better encryption security and once the flaws have been improved or ironed out we will see the move of people and companies turning to SHA-3 over SHA-2. But as of now I don't see that happening until and security threat has been detected in SHA-2, for example Google announced they did a successful real life SHA-1 collision attack (February 2017), which proves SHA-1 can be broken by this attack luckily there was a massive industry migration to SHA-2 before this attack was taken out. I believe this will happen again even through some crypto-professionals say it is almost impossible, if not impossible given the current understanding of math and physics, (Grimes, 2018).

The more people embrace the algorithm the more chance better hardware and software to accompany the algorithm will arise making the switch more appealing. With better encryption technology and algorithms will keep this system secure until even more powerful supercomputers are created in the future. Maybe in 10 years we will see SHA-4 be created and implemented.

Question 3: Prof. McMenteur's claim (377 words)

Professor Peter McMenteur's claim is not correct, when referencing Lamport's authentication scheme. The professor claimed to briefly study of the research paper he claimed that the scheme works even if the hash function is substituted by that is only easily to compute and harder to invert or decrypt for example a hash function without the property of the collision resistance. This claim is incorrect. After reading Lamport's paper.

One reason for this is the birthday paradox. Most people will not know this if they are not told about it. For example if 23 people in a room where asked what their birthday is, there is a chance of a least two people having the same birthday at 50%. It gets even higher is there is more people in a room for example if 75 people are present there is 99.9% chance there are two people with the same birthday, (Betterexplained.com, n.d.). The more people taking the experiment the higher the chance even though there is 365 days in a year and only 23 people it has a chance on 50% of two people have the same birthday. Image below will show the chances the number of people increases.

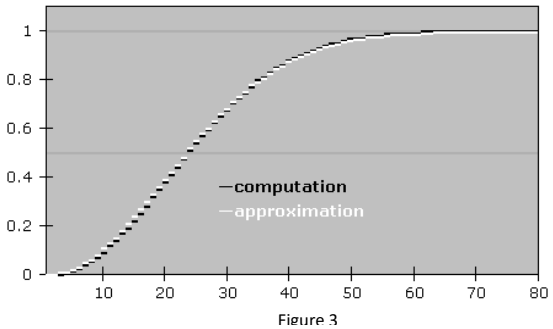


Figure 3

Because of the birthday paradox this compromises the one-way function, because if the password hash has been cracked you will be able to bypass the rest of the algorithm and will be able to get authenticated and access to the sensitive data. The birthday paradox proves that most people think the odds of someone guessing the password hash is higher than it really is, back in 1979. So Lamport's paper has given false results because of the bad maths and not including the birthday paradox formula. The function does not need to be collision resistant in order to be a one-way hash function. But the paper does not mentation ash functions at all, instead it talks about the construction of a encrypting a fixed plaintext which does not include any secure encryption algorithm, because of this it will use the input as a key and the cipher text will be the output, (Karonen, 2017).

So inclosing Professor Peter McMenteur's was incorrect on his claims after reading though Leslie Lamport's research paper called "Constructing Digital Signatures from One Way Function.

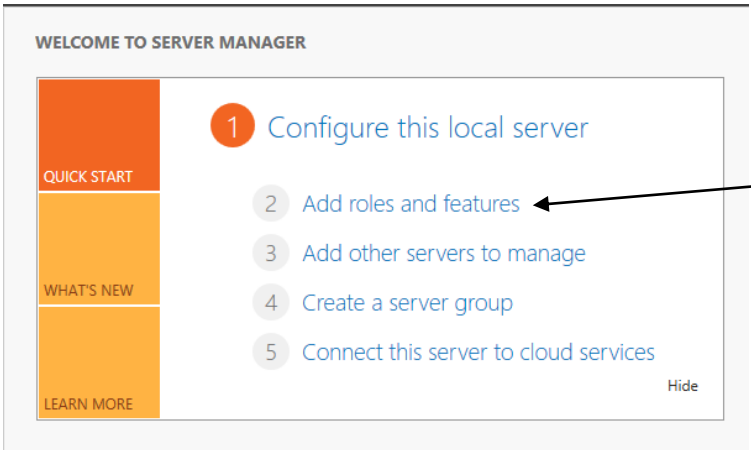
Question 4: Design and Implementation of a Secure Server Network (2882 words)

This report will have different subsections, the first section will show the configuration of the DNS server, DHCP server, Web server, Email server and FTP server. To show it has been completed there will be screenshots for evidence after that has been completed, they will be a simple network diagram of the network. The second section will show five different security attacks on the configured servers through Kali Linux and will have countermeasures on how to stop these attacks, these will also be captured through screenshots. The third section will show a detailed cost of implementing the solution in a table format there will be two options of products for the company to choose from a high end and middle range products.

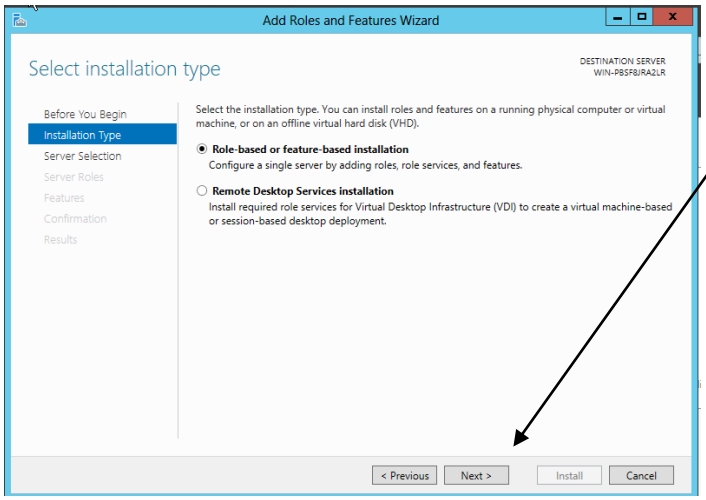
4.1 Server Configuration Windows 2012

4.1.1 DNS

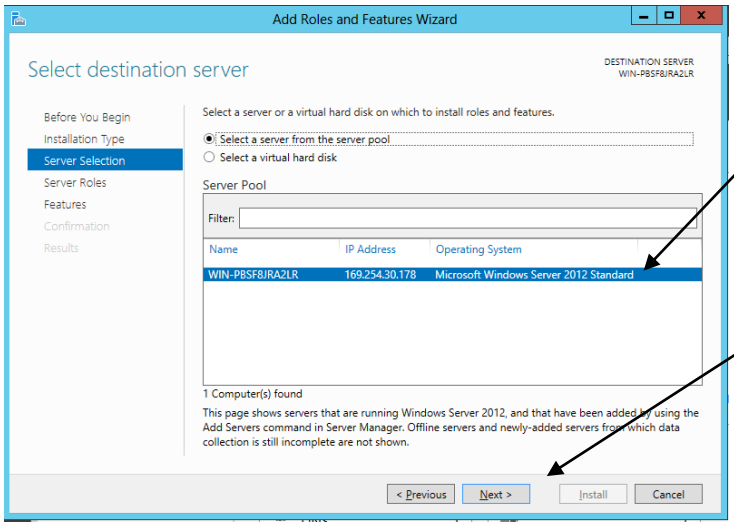
The DNS server will be the first one to be installed. DNS stands for domain name system and will be showing step by step install of this server.



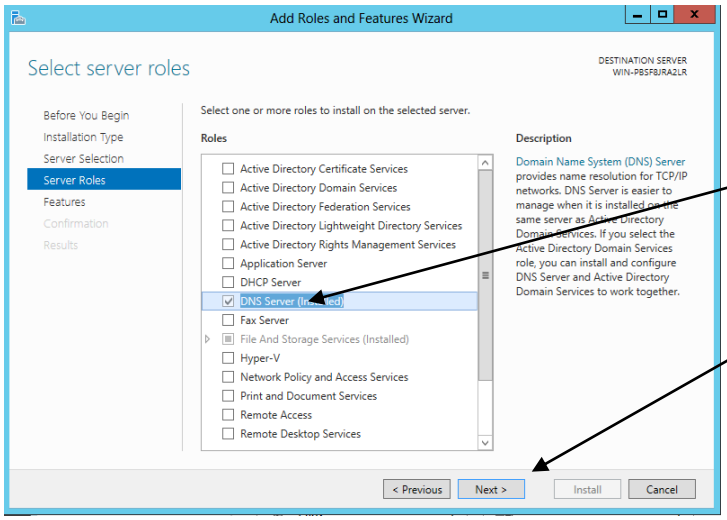
Once the Windows Server 2012 OS has opened the server manager will display then click on “2. Add roles and features”.



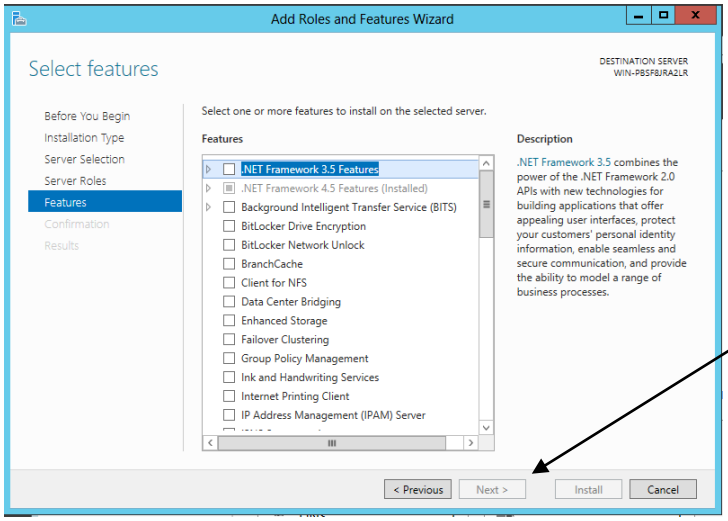
It will open the “add roles and features wizard, click next.



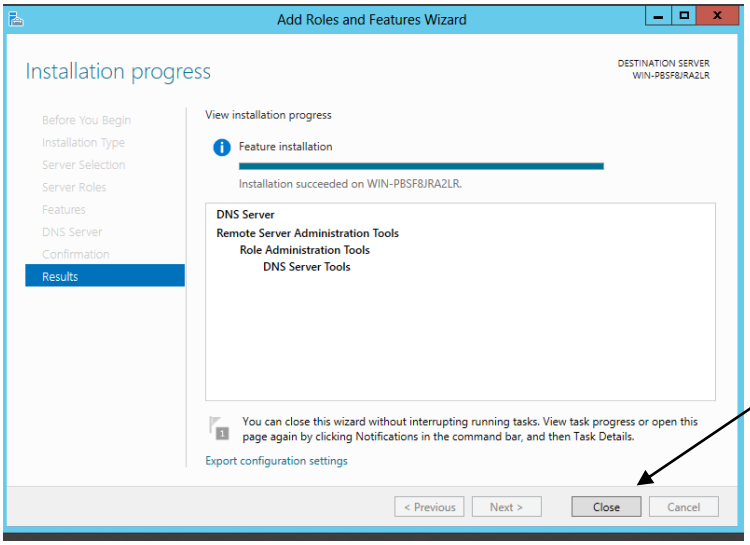
Make sure the server is selected, then click next.



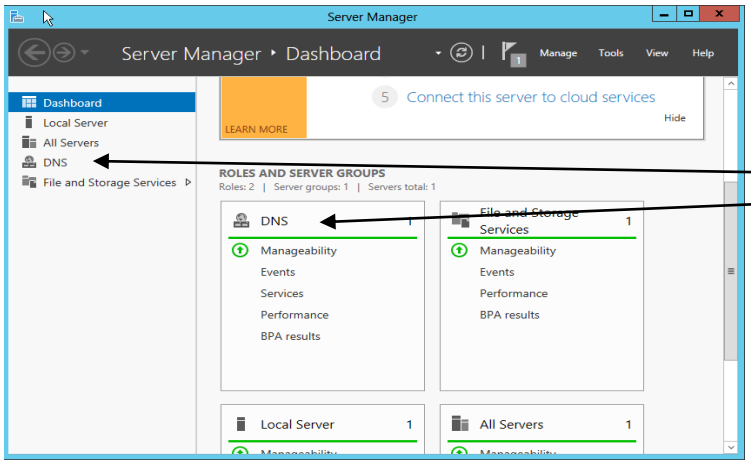
This page shows all the server roles make sure to click DNS server for this section, once chosen click next.



We will not be adding any feature so click next.

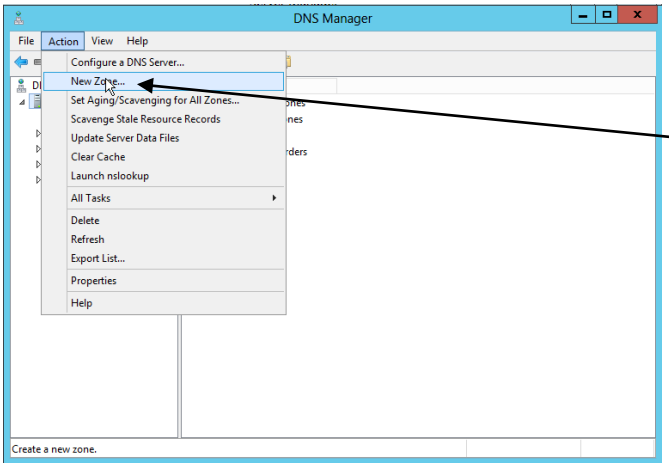


After confirmation which shows you what is going to be installed click install and wait a couple of minutes, after that click close.

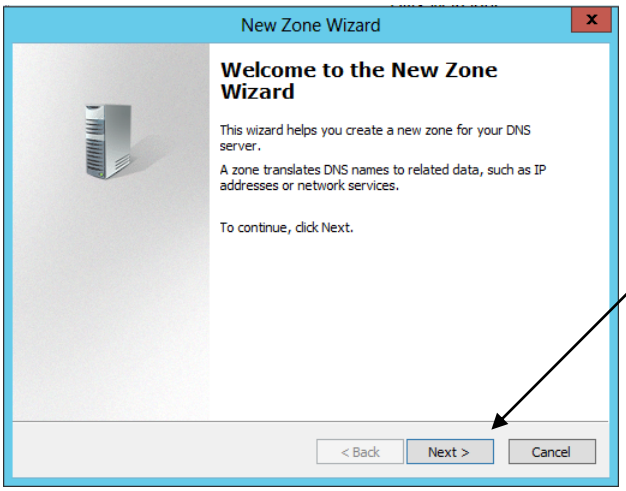


It will then take you to the server manager dashboard and show the DNS server up and running.

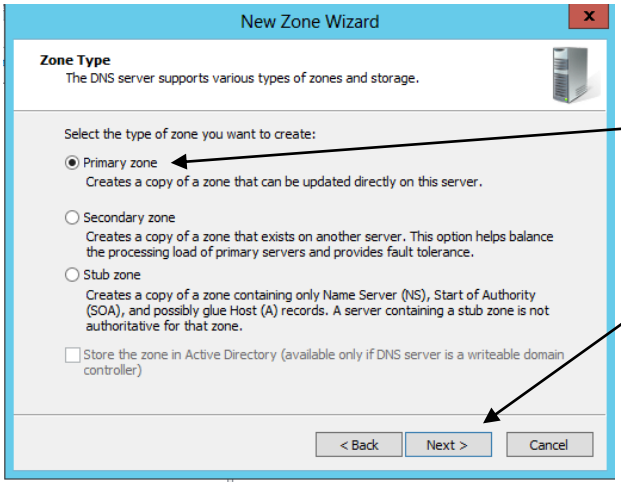
The next steps are to show how the zone was created for the company calling it “zana-enterprise.com” so a client (users) can join it.



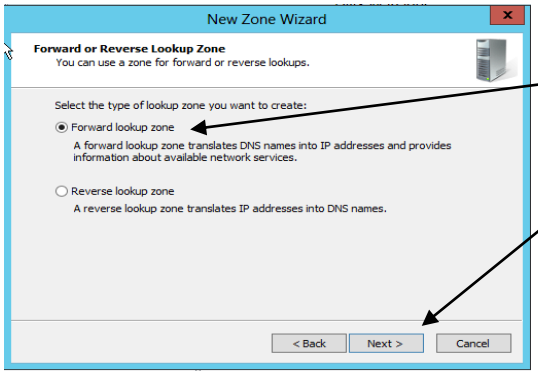
Open DNS manager, click the server and go to action then new zone.



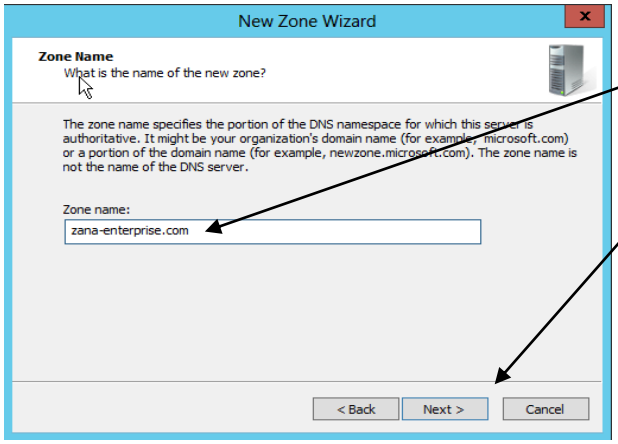
The New Zone wizard will pop up just click next.



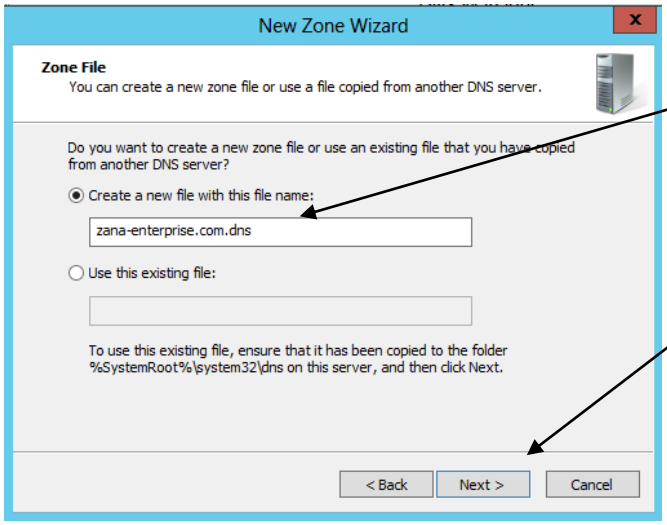
Make sure the Primary zone is selected then click next.



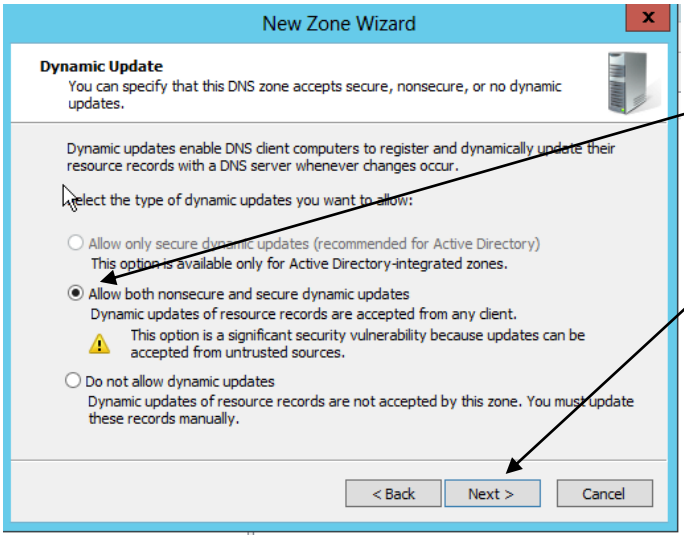
Make sure forward lookup zone has been selected, then click next.



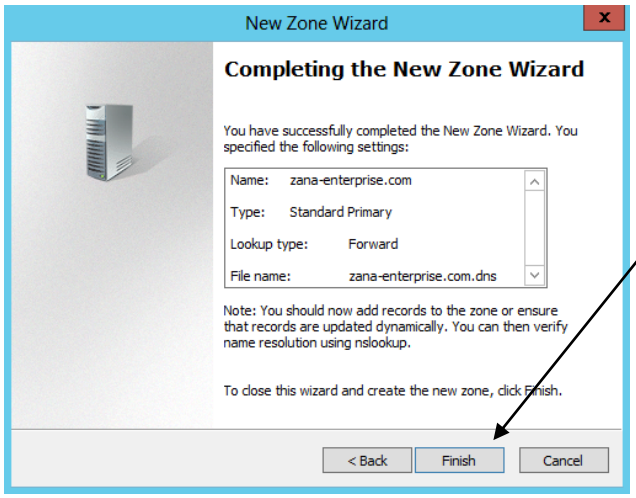
Then type in the zone name “zana-enterprise.com” then click next.



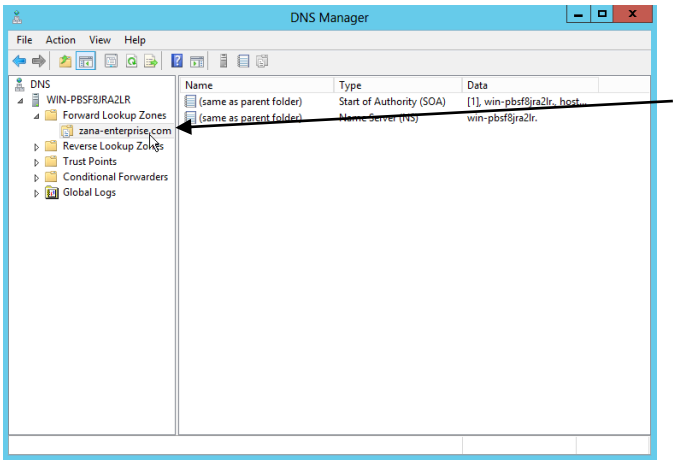
The zone file can be left default, then click next.



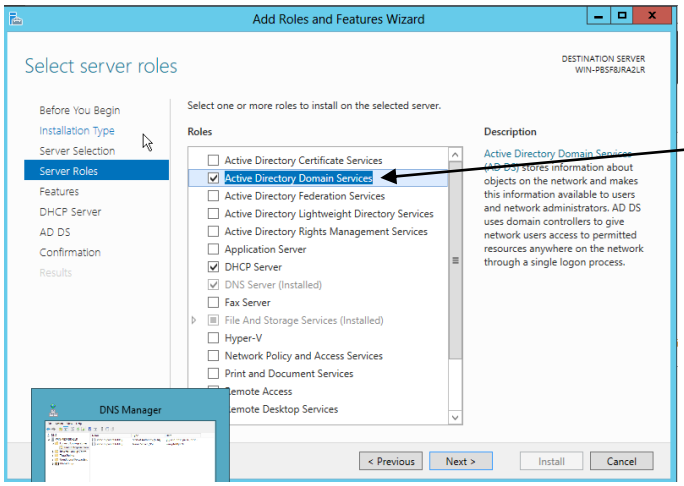
Choose “allow both non secure and secure dynamic updates, then click next.



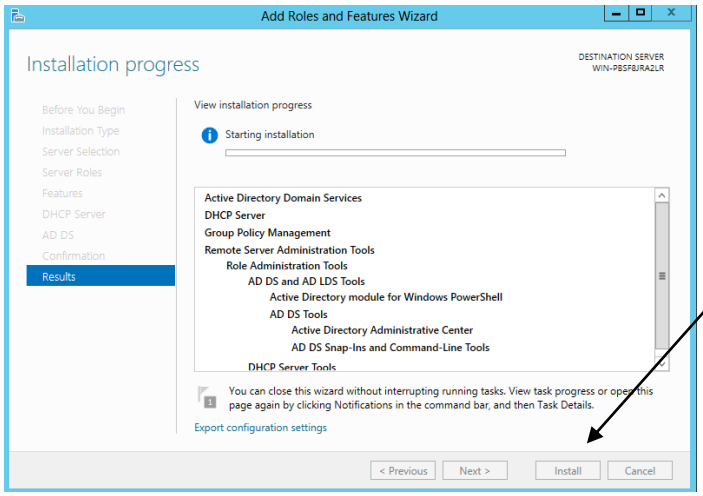
Then finally click finish to create the zone.



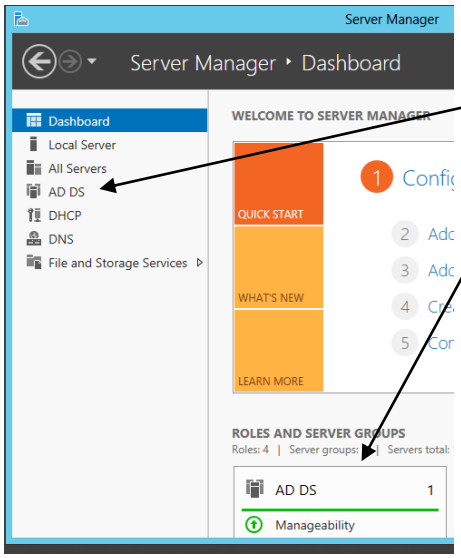
Back on DNS manager evidence it was completed



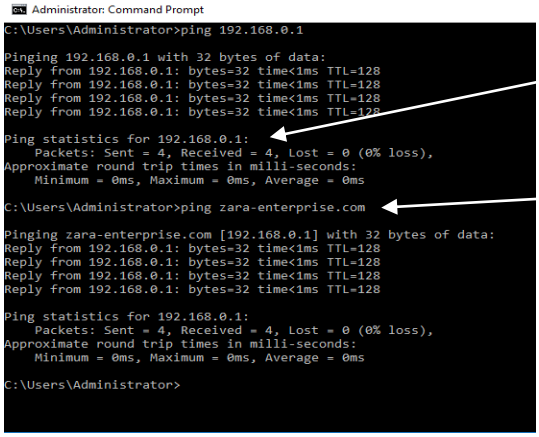
Go back to add roles and features and Add Active directory domain services, and finish the install like the DNS wizard.



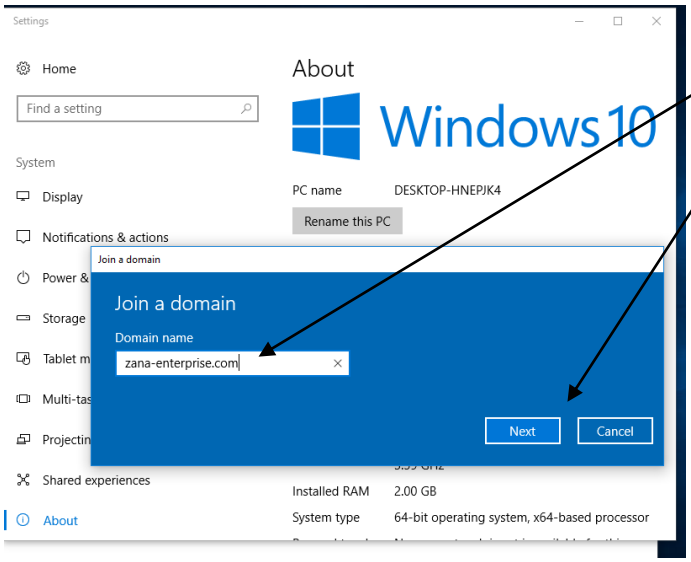
Click install, once finished click close.



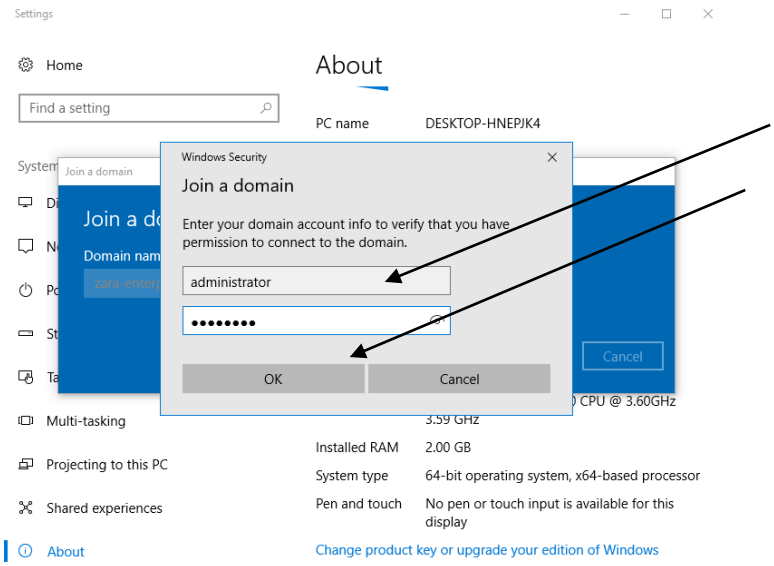
If done correctly it will display on the dash board.



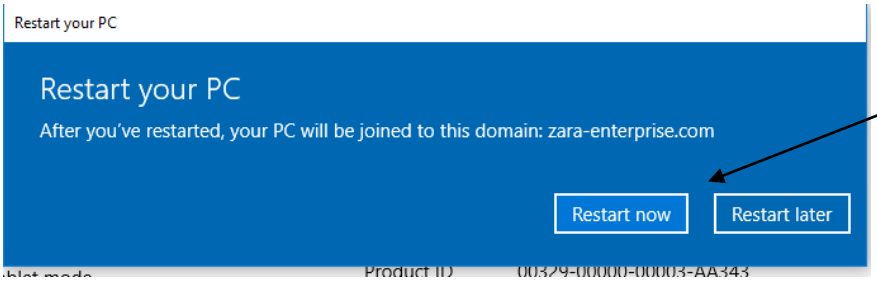
I then went on to the Windows 10 client open up cmd and pinged the IP address of the server and the domain name “zara-enterprise.com”.



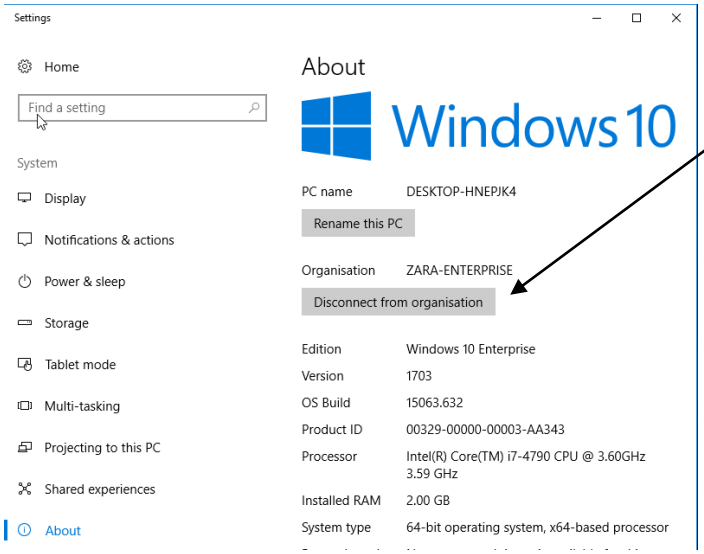
Go to about my PC and click on join domain and enter the domain “zara-enterprise.com”, then click next.



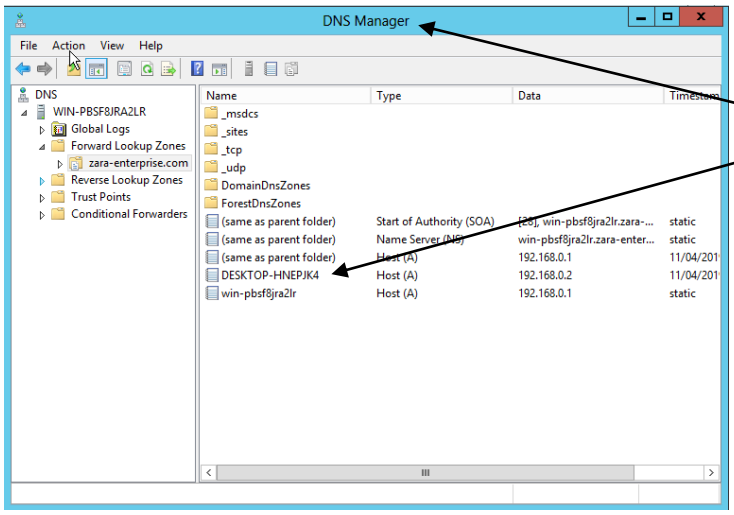
Log in on the domain account, enter user name and password then click ok.



Click restart, it will then be joined to domain.



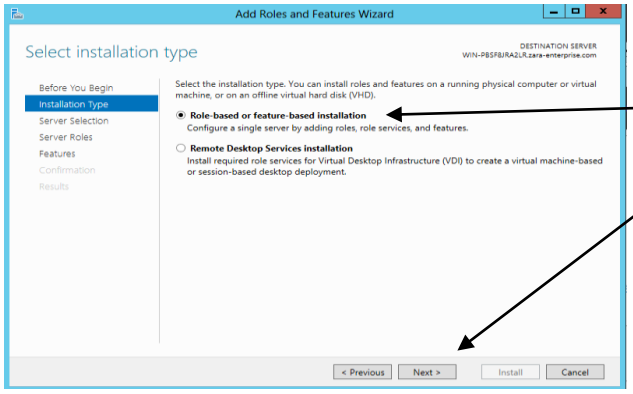
Go back to "about my PC" and it will display the domain.



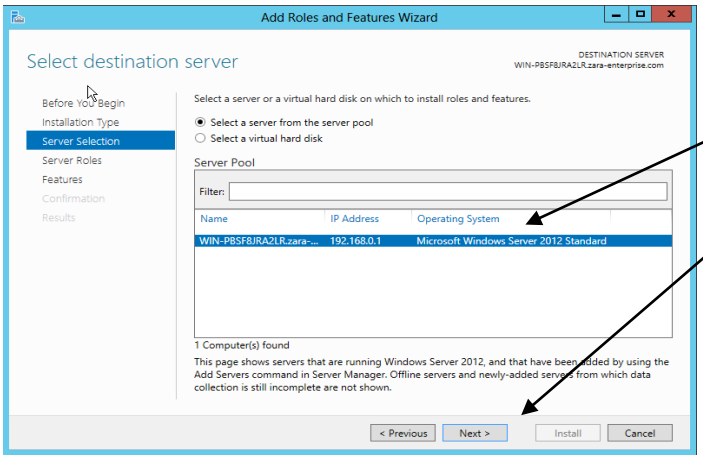
Then go back on the windows server 2012 and open the DNS Manager and see the new user connected to the host.

4.1.2 DHCP

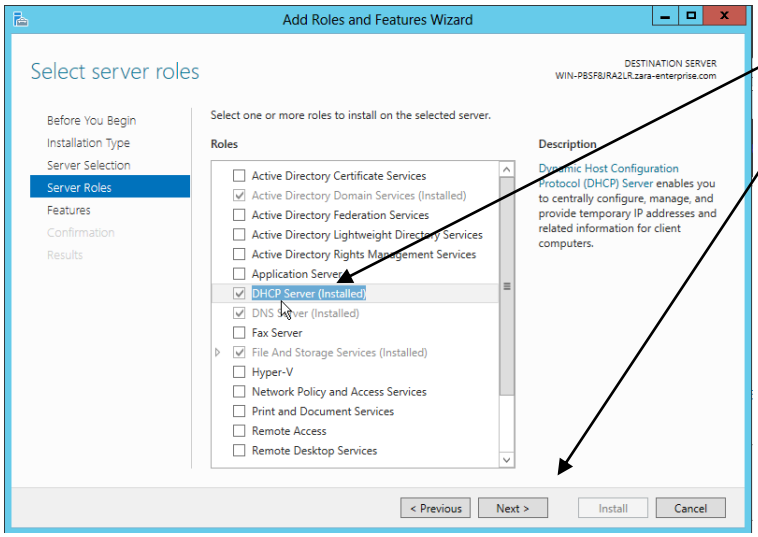
The DHCP server will be the second one to be installed. DHCP stands for Dynamic Host Configuration Protocol, it is used to assign dynamic IP addresses to any number of devices or nodes on the current network. The best reason to use DHCP is to have a different IP address for every time a device logs onto the network.



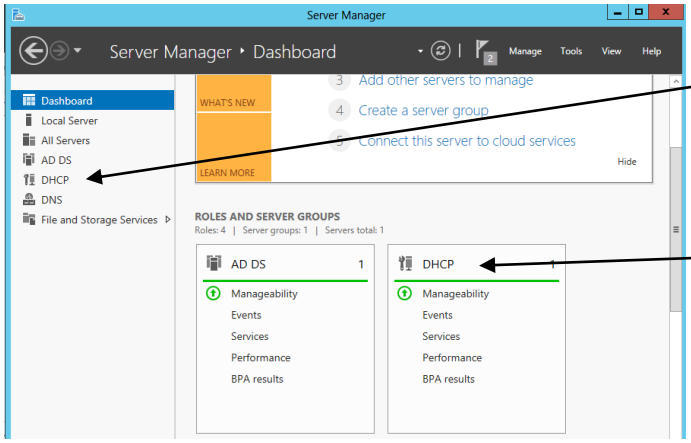
We go through the same process as the DNS server install, using the add roles and features wizard, click role based, then click next.



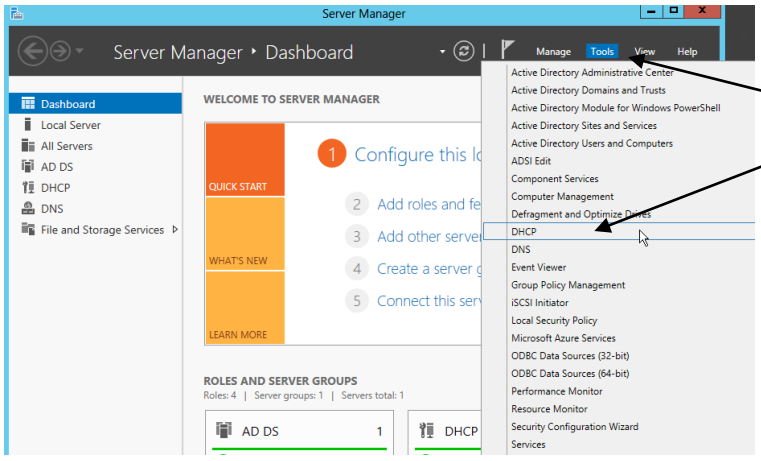
Carry on the same as DNS, click next.



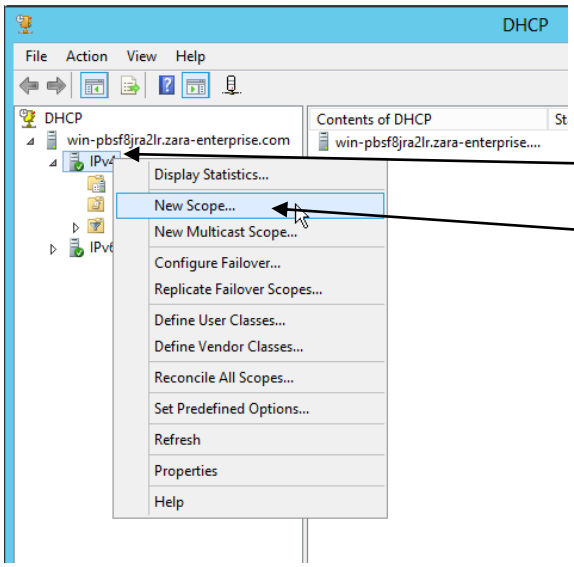
Now select the server “DHCP Server”, then click add features, then click next and continue through the pages and finish the install just like DNS server.



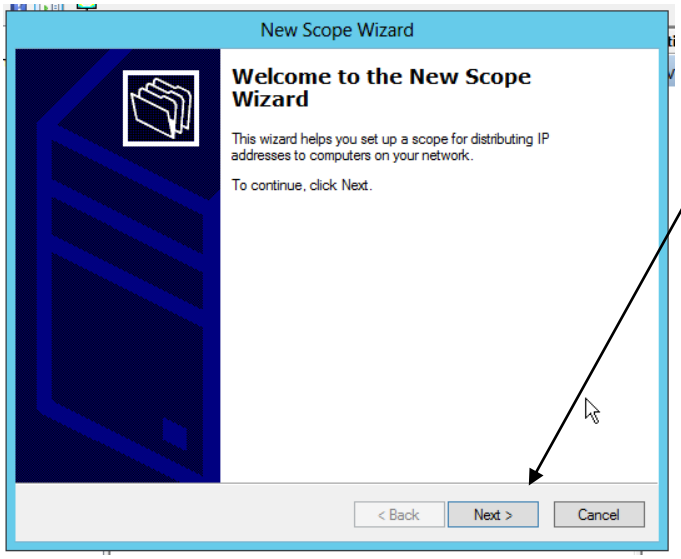
Once the install has finished go back to the server manger dashboard and will show it has been installed.



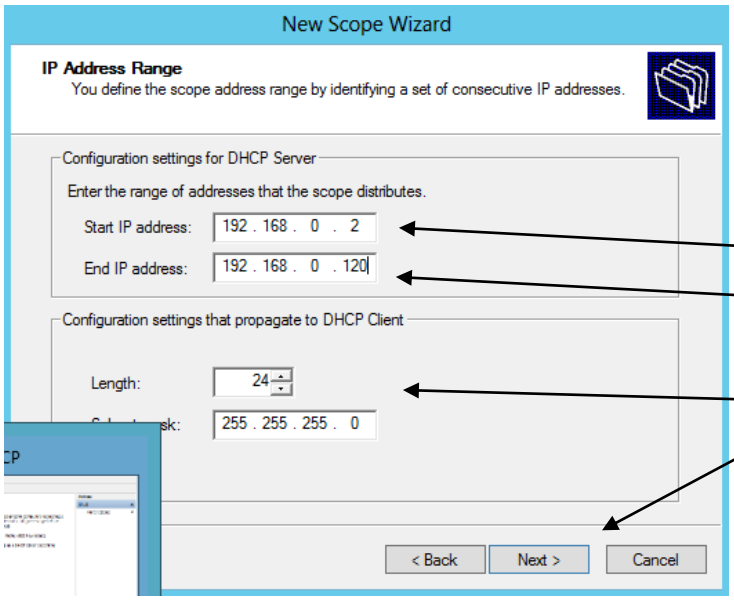
Next, we must configure the server, so click tools on the right, then click DHCP and will take us to the correct windows for installation.



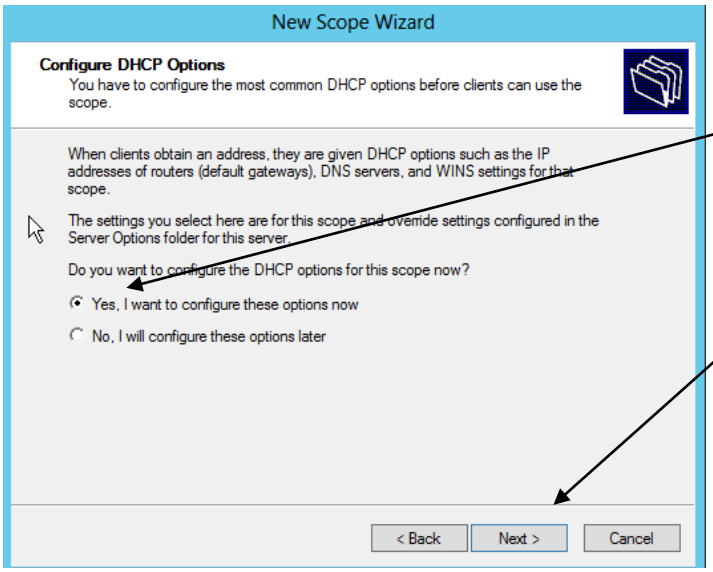
DHCP server has popped up, right click IPv4 and select new scope. This will allow us to set the subnet of the network.



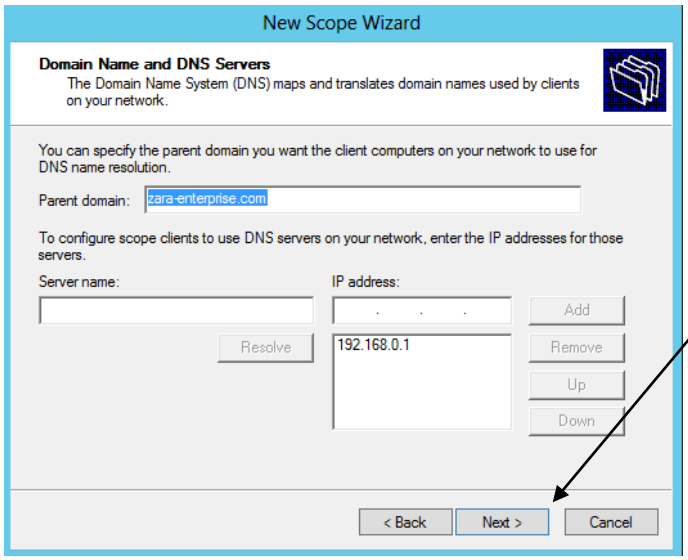
Once the wizard has opened it will get a brief explanation of what the “new scope” will do, click next.



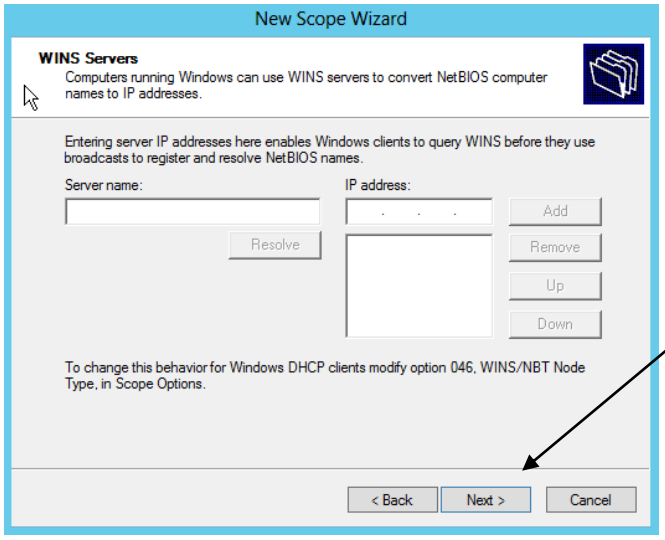
After clicking next we are on the IP address Range, this is the subnets that will be used for the network. We entered 192.168.0.2 for the start IP address, then 192.168.0.120 for the end of the subnet, then click next.



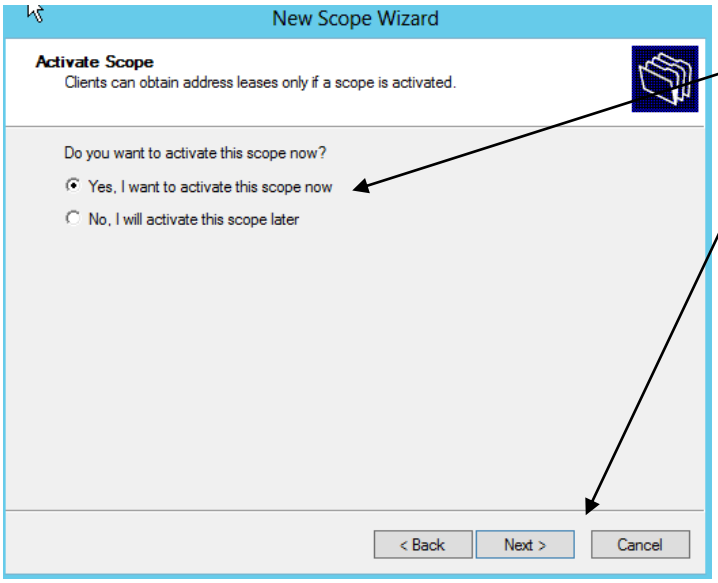
Check “yes, I want to configure these options now”, then click next.



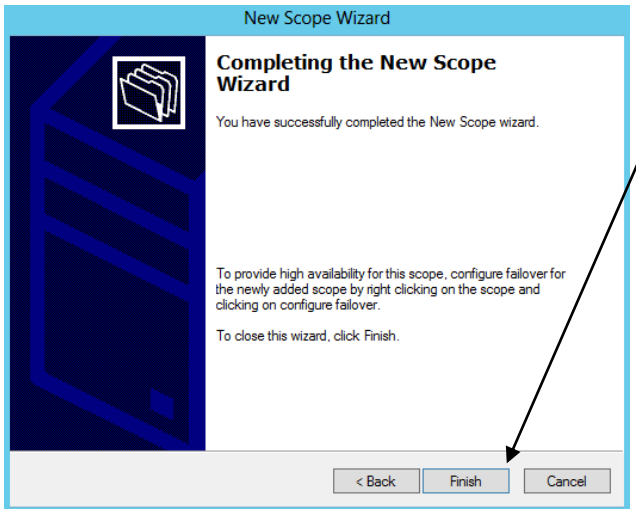
All information should be filled in, just click next.



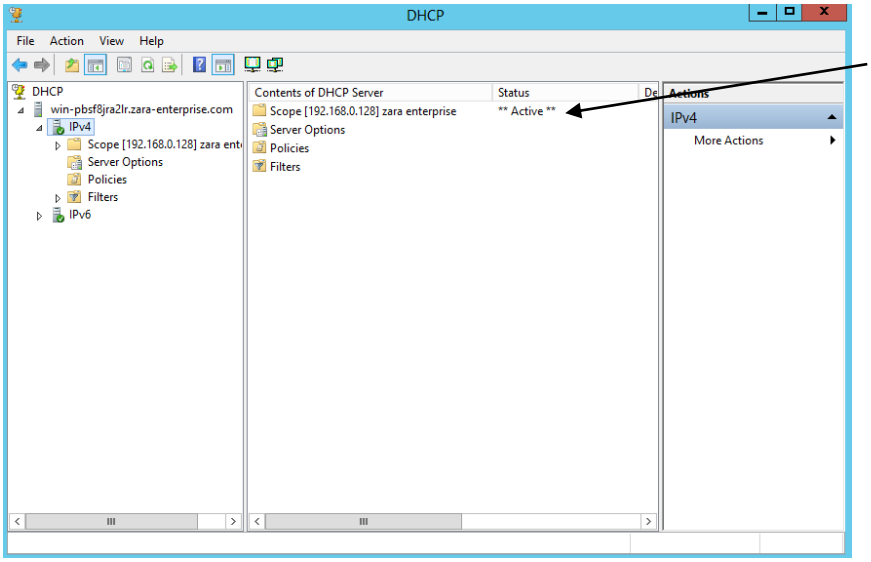
Skip this page as we don’t have a WINS Server. Click next.



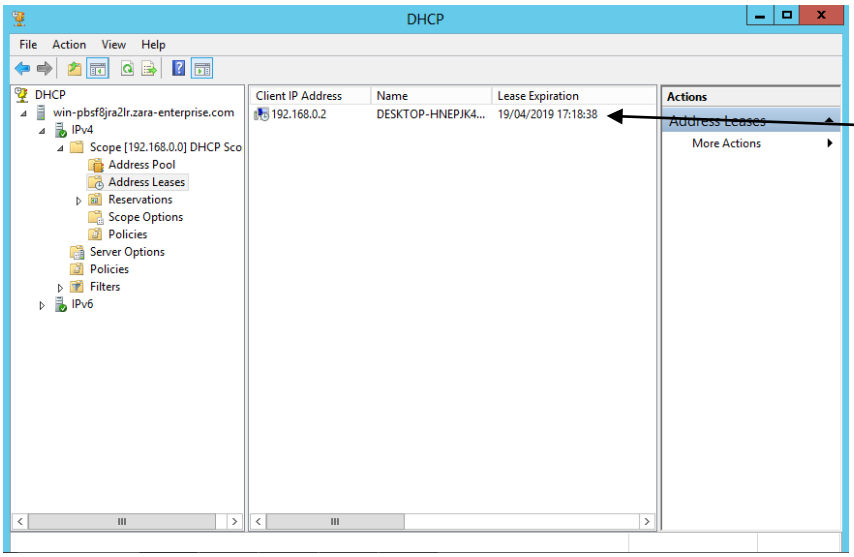
Click “yes. I want to activate the scope now”, Then click next.



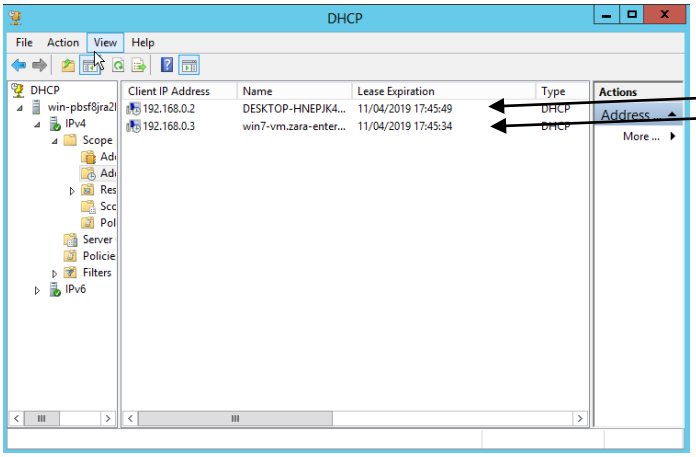
Click finish.



Once closed, you can see it has been completed.



Once we open the scope under IPv4 and click on address leases it shows on user has already been allocated, the first address, and shows when the lease will expire and then give out a new address.

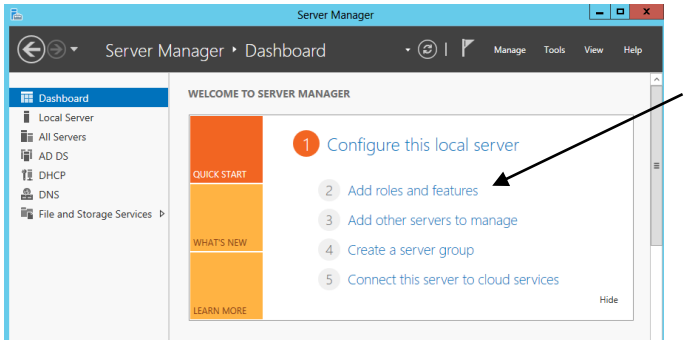


I then got another user to join they have both been given IP addresses and have lease expiration dates.

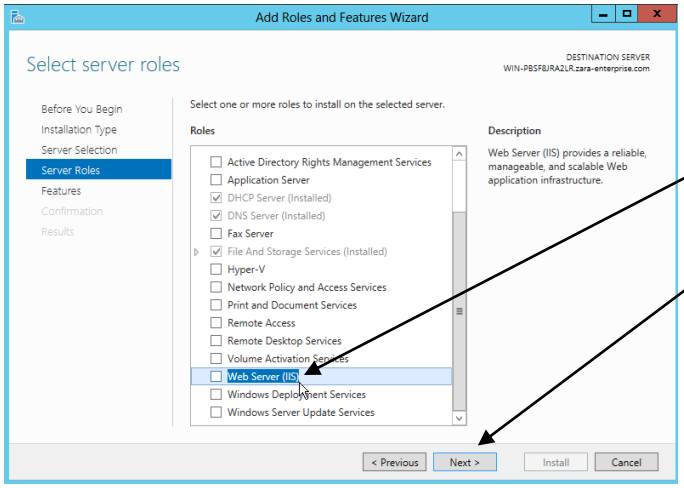
4.1.3 Web Server

This server will be the third one installed, it will also include configuration of the IIS and apache. This server will host and allow the users to access the website www.zana-enterprise.com.

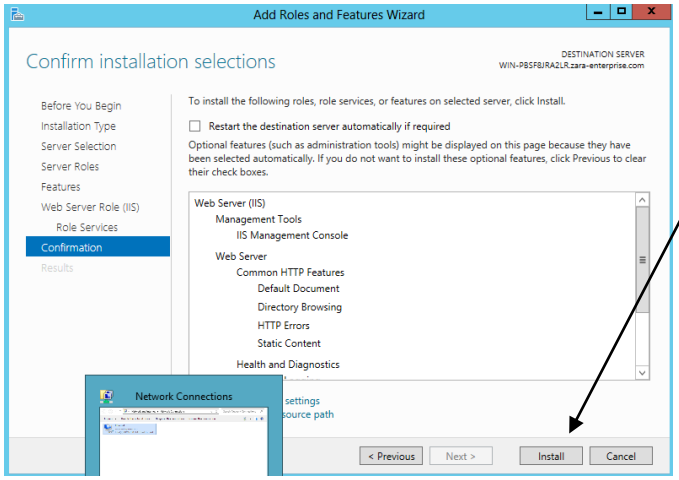
Let's first start off with the install of the server role.



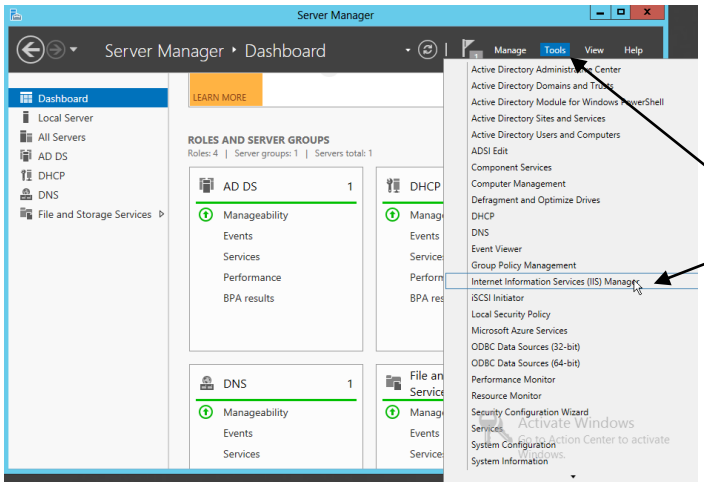
It starts off just like the other two servers by clicking "add roles and features".



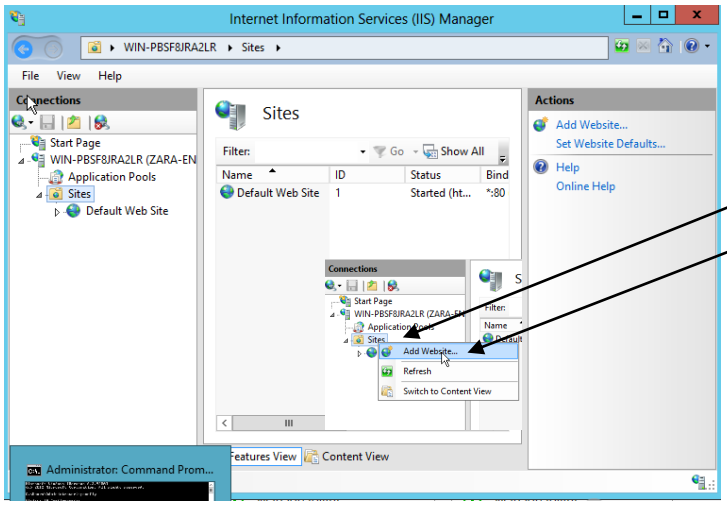
Keep clicking next until you reach the "select server roles" page and select "Web Server (IIS)", then click next.



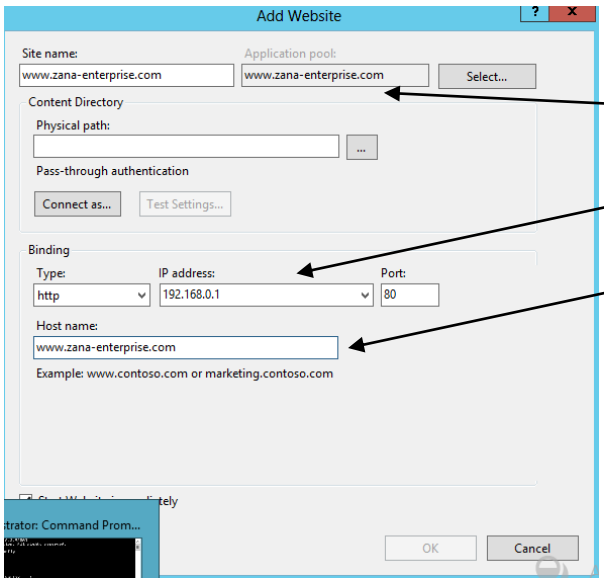
Again, keep clicking next, until you reach the "confirm installation selections", then click install.



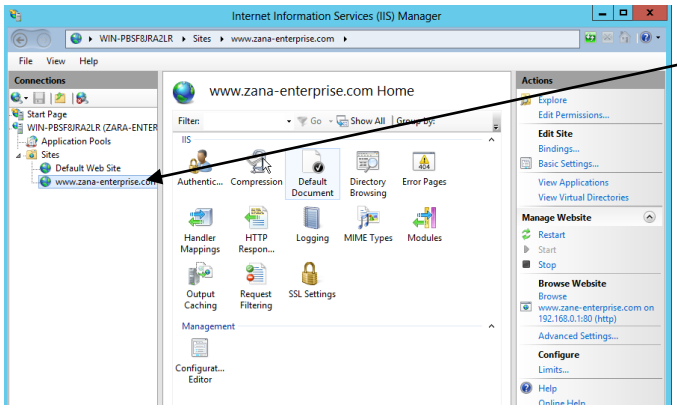
Go to server manager dashboard and click on tools on the top right of the window and select “Internet Information Services (IIS) Manager”.



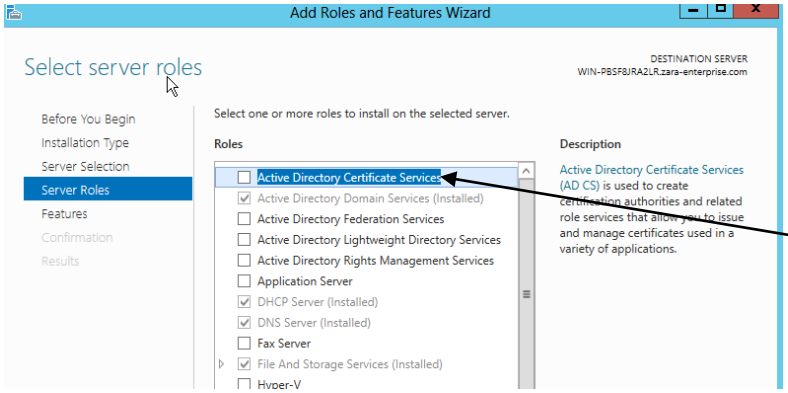
The Internet Information Services (IIS) Manager will then open, next thing to do is right click sites and select “add website”.



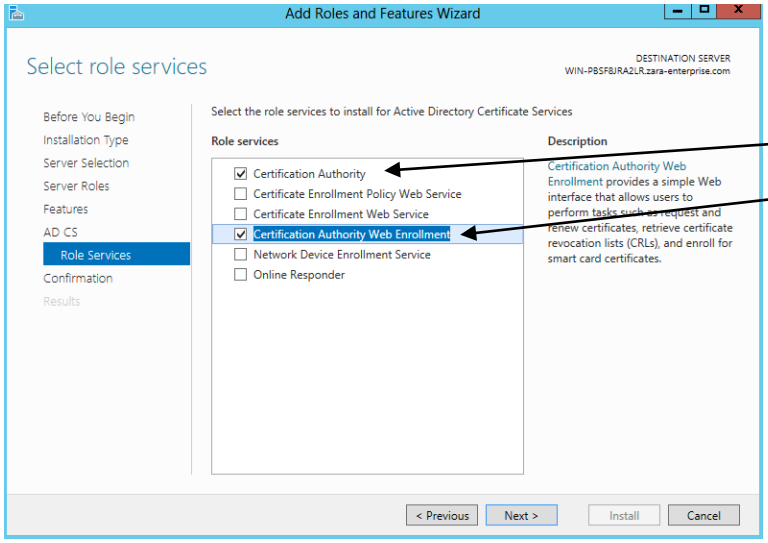
It will then give you a “add website” window, then fill out “site name”, “application pool”, the server IP address and final the “host name”.



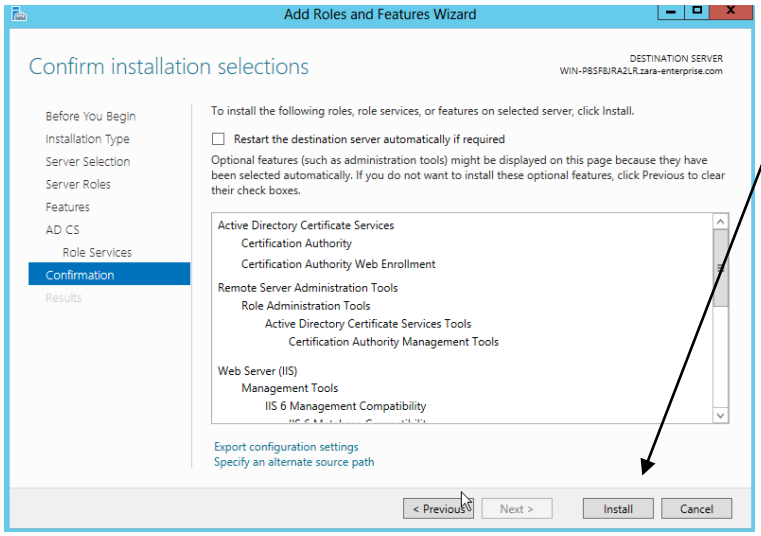
Can see website on the left.



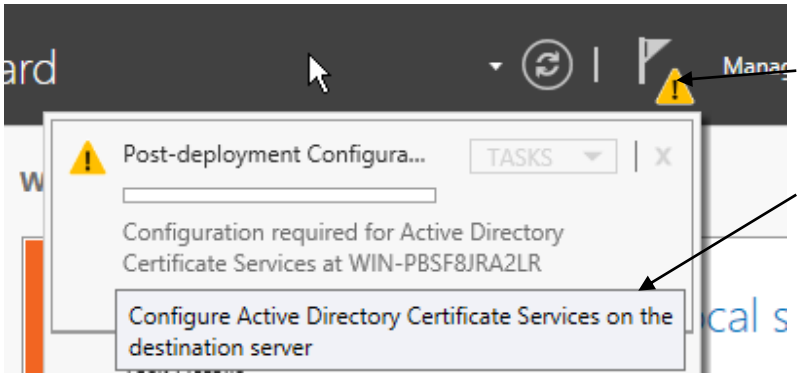
We will now install “active directory certificate services”, this will allow us to create the SSL, then click next.



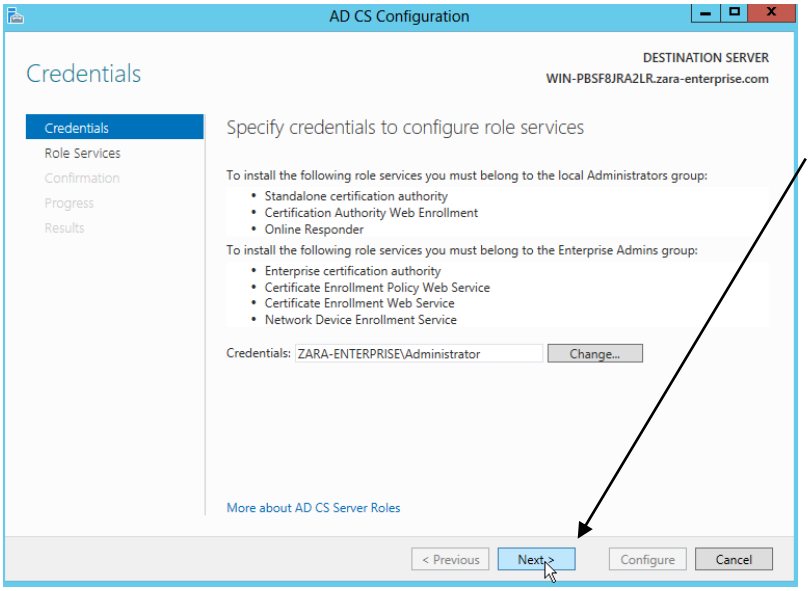
We then click next two more times until we reach “role services” and click “certification authority” and “certification authority web enrolment”, then click next.



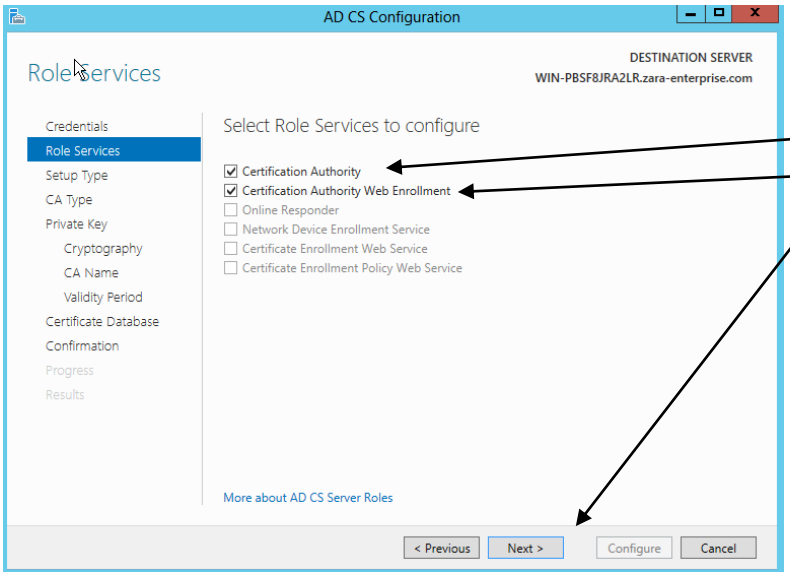
Once this is done click install and once it has been completed, close the wizard.



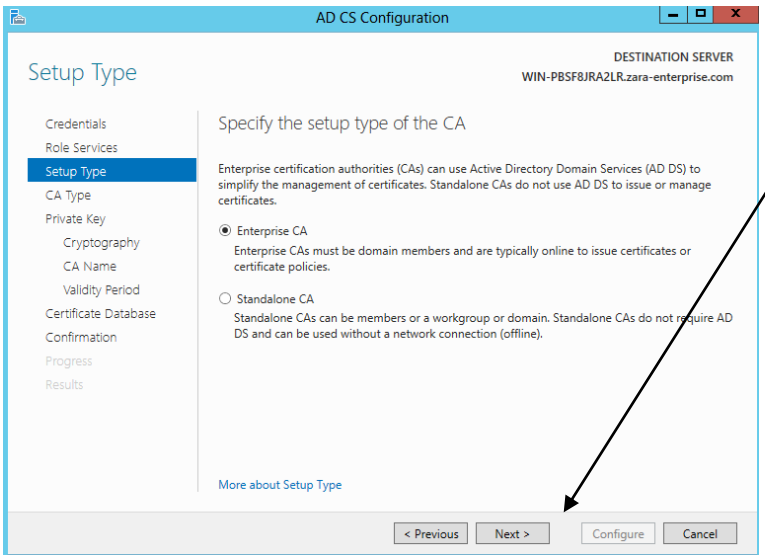
Once it is closed they will be a flag on the server manager dashboard click it and click configure “active directory certificate services on the destination server”



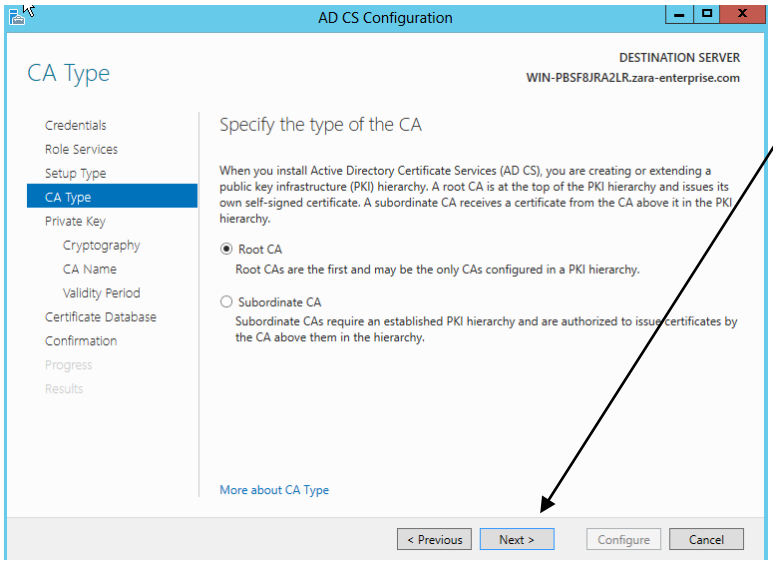
It will then come up with the AD CS Configuration, the credentials will fill itself in, then click next.



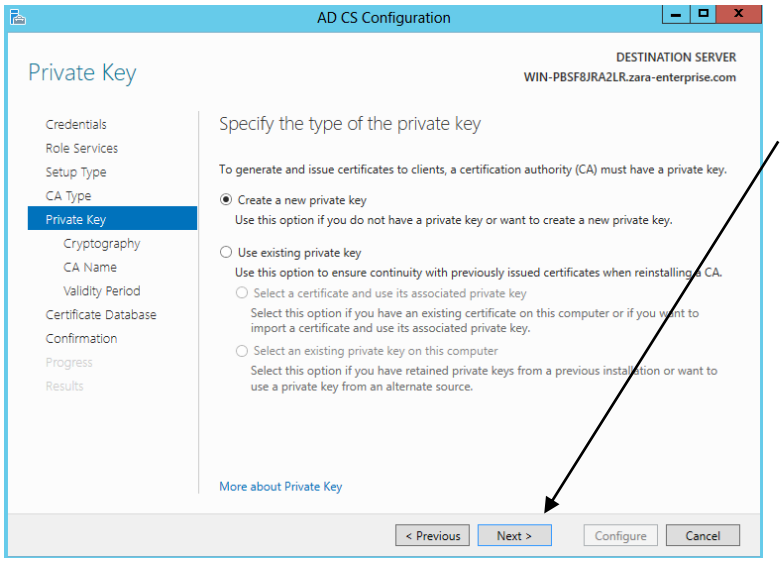
On “role Services”, click “certification authority” and “certification authority web enrolment”, then click next.



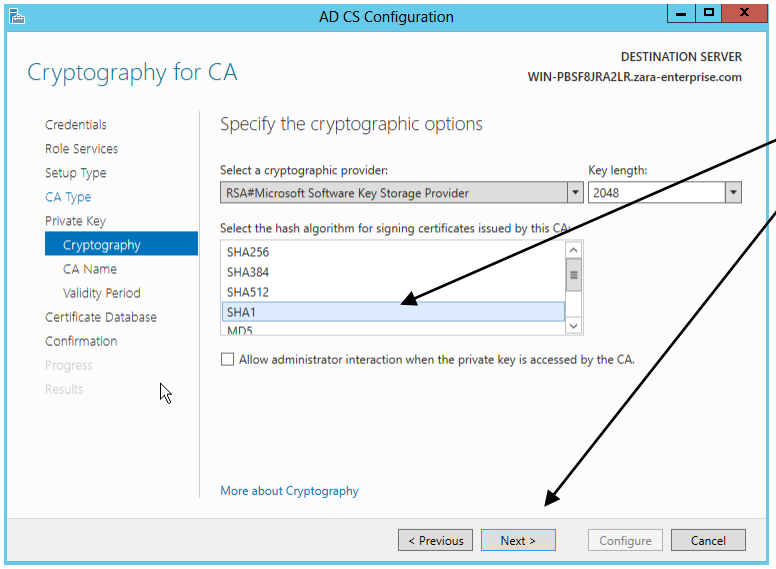
Click next.



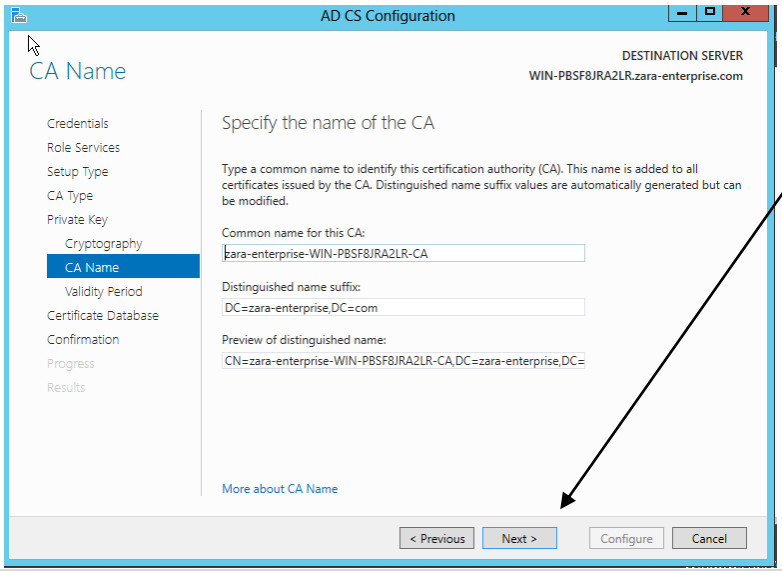
Click next again.



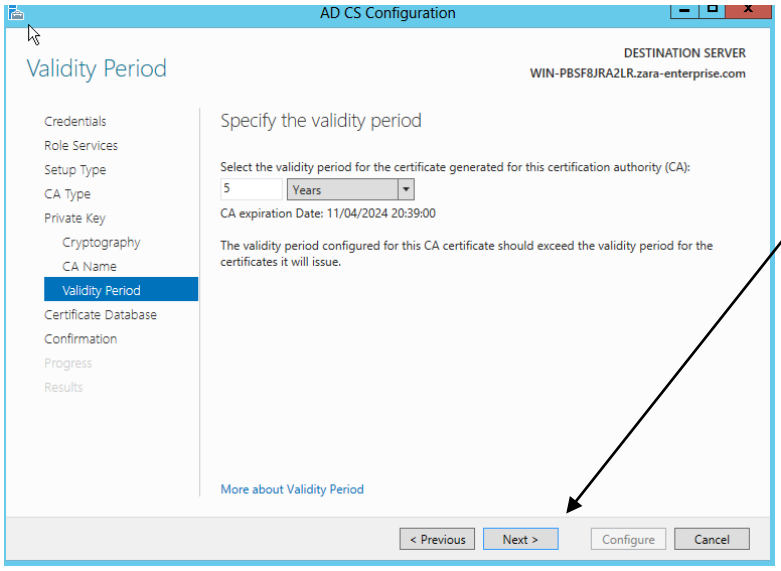
Choose create a new private key, then click next.



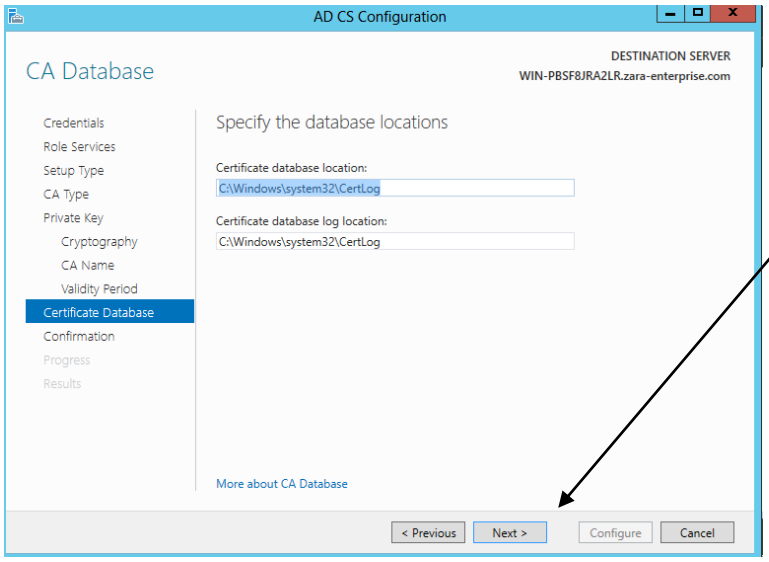
Leave “select a cryptographic provider” and “key length” default and choose SHA 1, the click next.



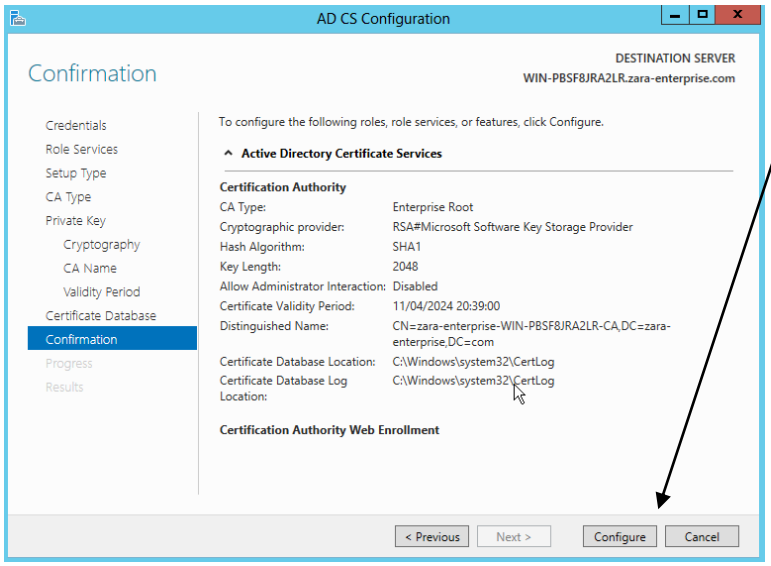
On the next page the text fields will automatically fill in, just click next.



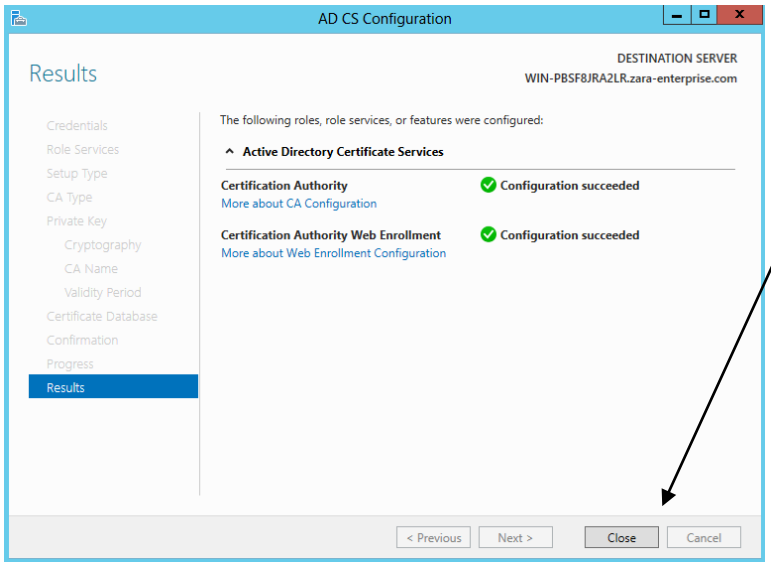
Leave it default, then click next.



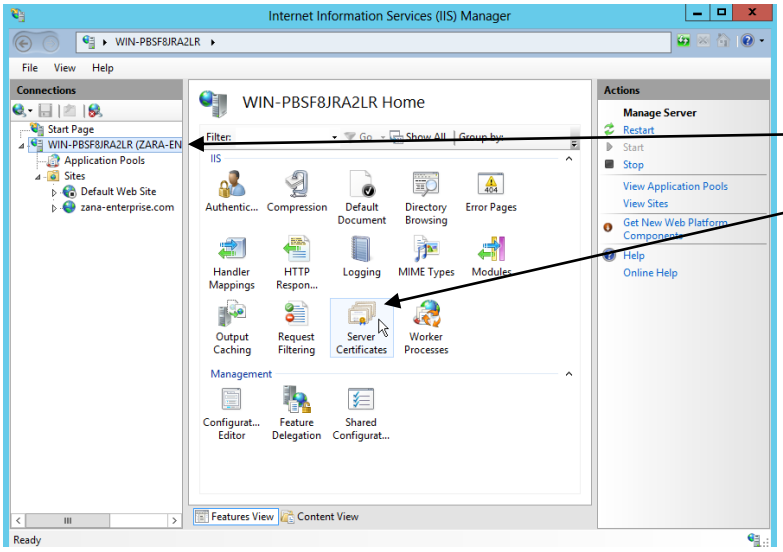
Again this page shows the location of the certificate data base, just click next.



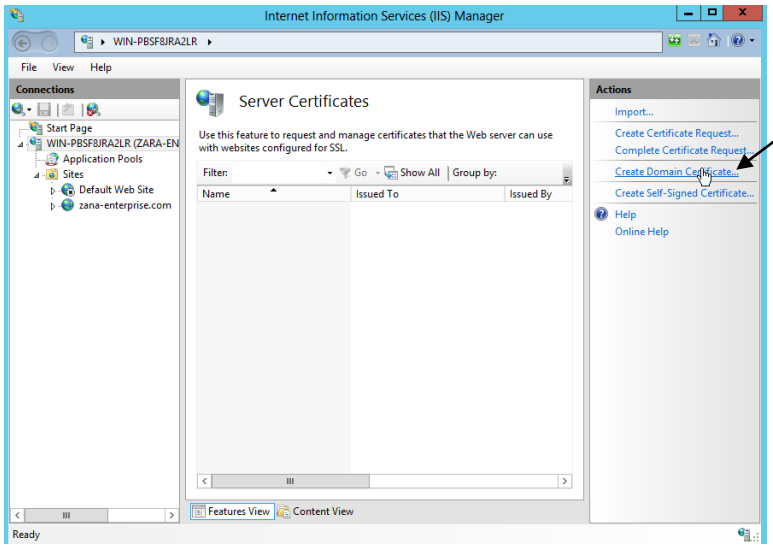
Finally we click configure to finish the configuration.



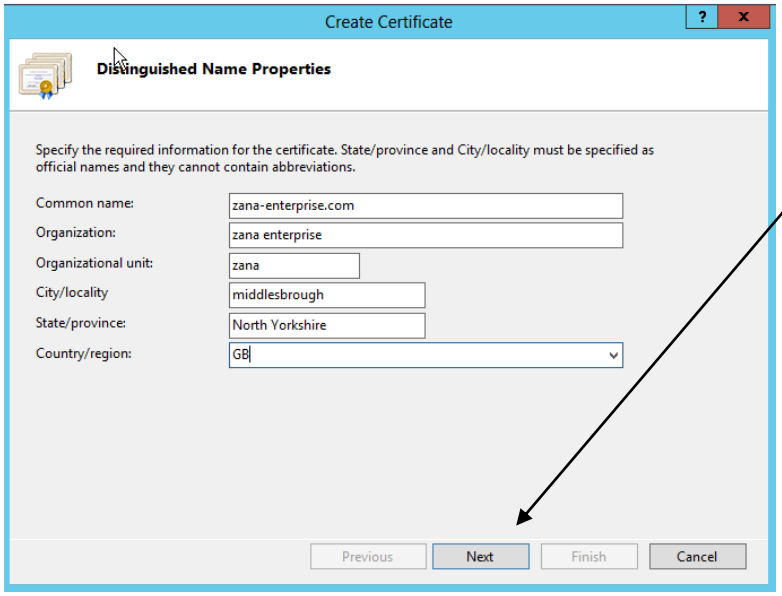
Once it has been configured, it will show if it has been configured correctly and successful. Then click close.



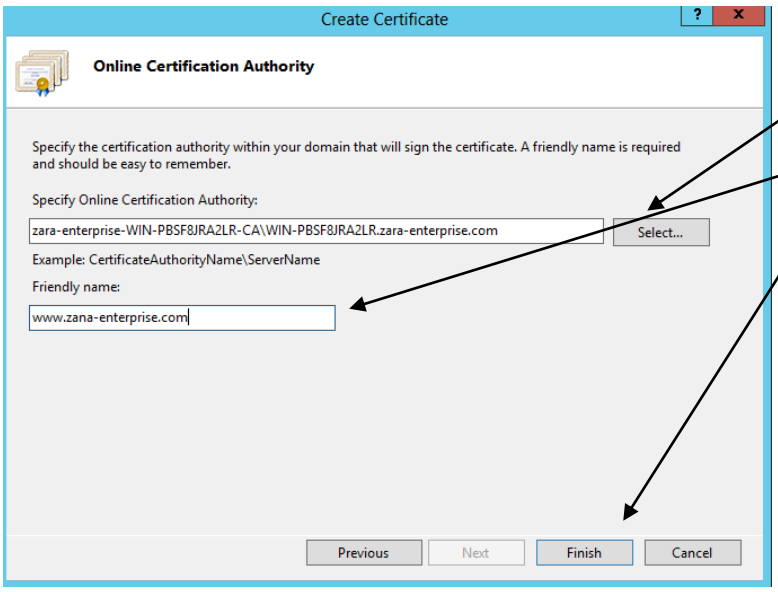
Next thing to do is create an SSL to the website, click on the server, then double click “server certificate”.



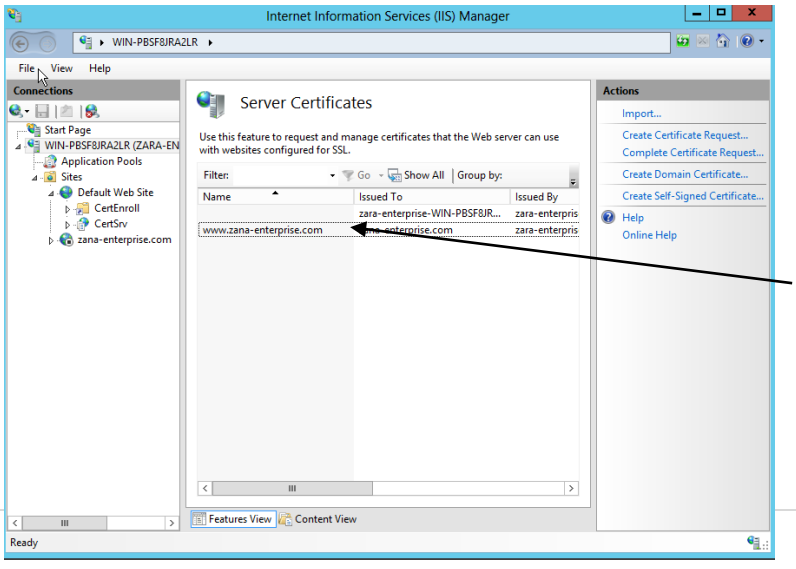
Then click “create domain certificate”, In the action tab.



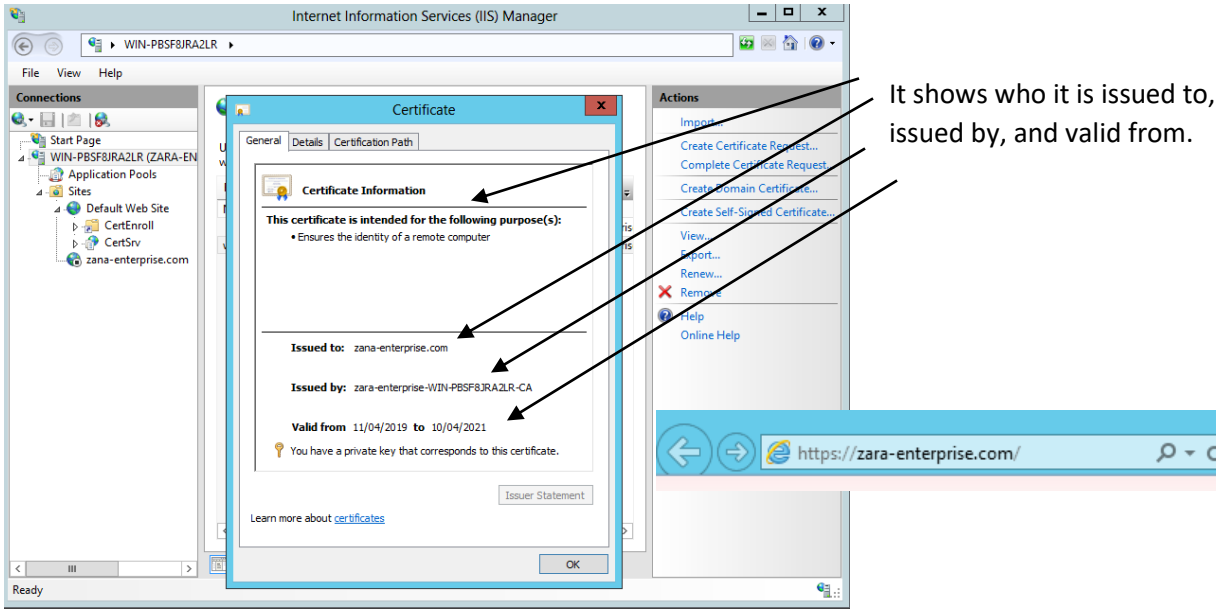
Then we fill out the relevant information for the certificate, then click next.



Then select the online certificate authority, and the friendly name. Then click finish.



You can see the SSL for the server certificates, displayed in the field, and if you double click "www.zana-enterprise.com" it will show the certificate.

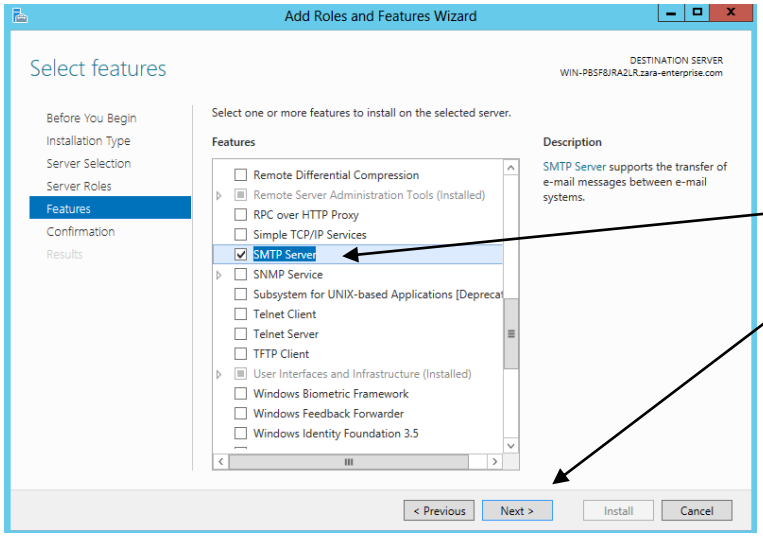


It shows who it is issued to, issued by, and valid from.

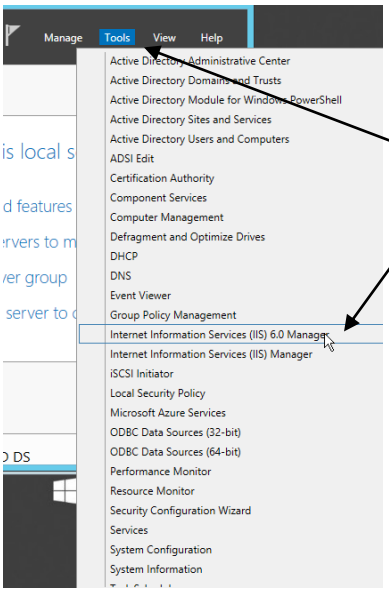
4.1.4 Email Server

The email web server will be the fourth server installed and configured. This server will allow users to send and receive emails through the SMTP server the email address used is user@zana-enterprise.com.

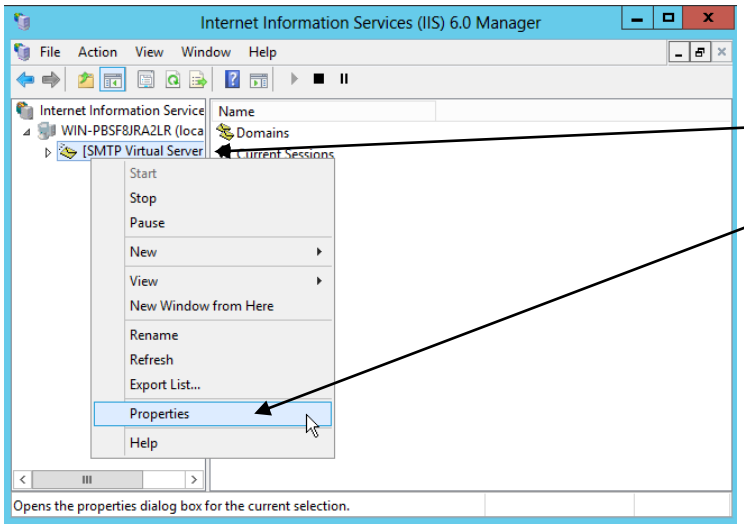
Let's start off with the server install.



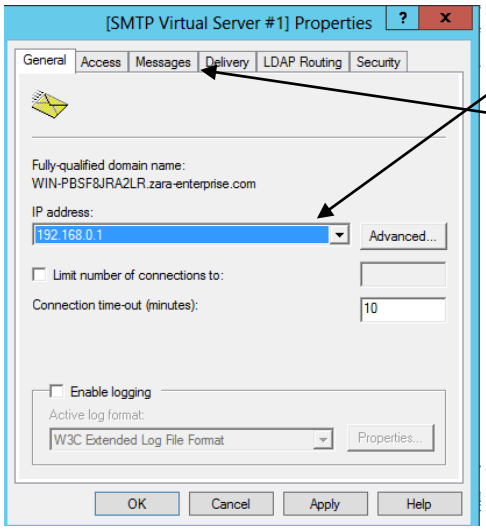
Go through the normal process as before and once you get to the features page and click SMTP server and then click next. Then click install.



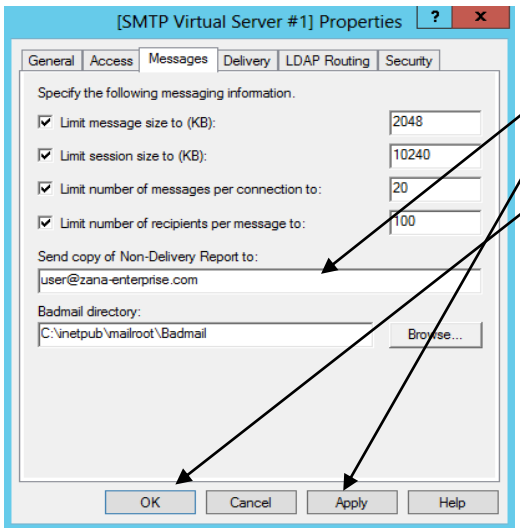
Once you go back to the dashboard, click and select Internet Information Service (IIS) Manager.



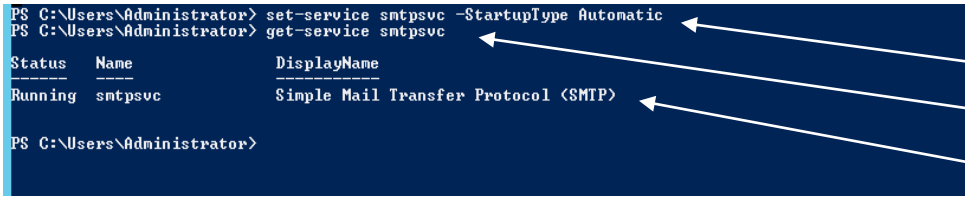
It will then open the IIS manager, then right click SMTP Virtual Server and click properties.



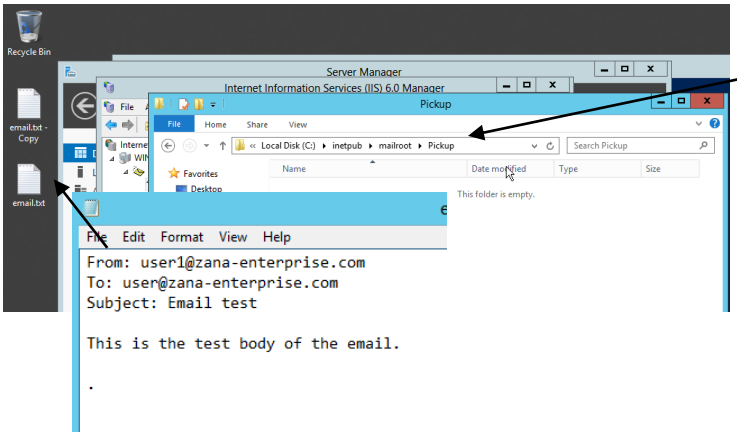
In IP address select the server IP where the messages go to and from. Then click “messages”.



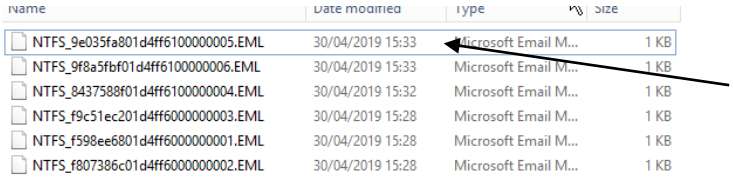
Then we add in the email address we would like it to go to. Then click apply and ok to close the window.



Open Powershell and type "set-service smtpsvc –StartupType Automatic", then type "get-service smtpsvc", it will then give you status of the SMTP server.



Next create a text file called "email.txt" and type out an email for testing, then copy the file from desktop to "c:\inetpub\mailroot\Pickup", once that happens the server will see it and send it off straight away.

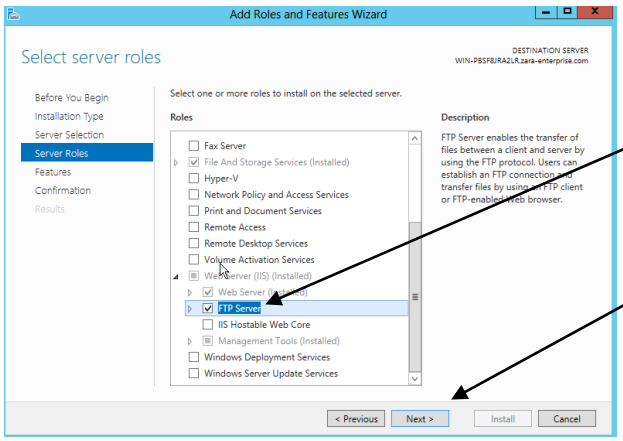


We then go to "c:\inetpub\mailroot\Drop", and see the mail, double click to open the message.

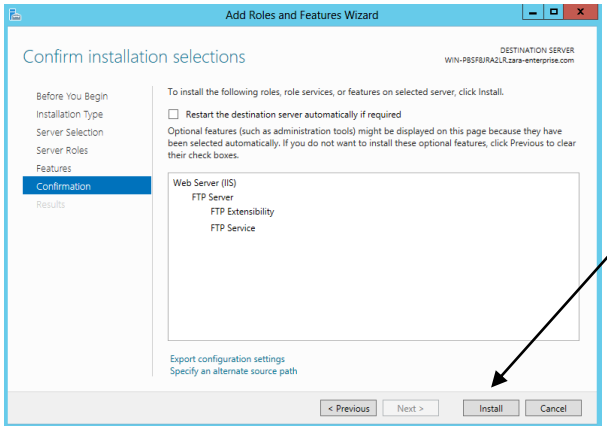
Once opened it will show the message sent.

4.1.5 FTP Server

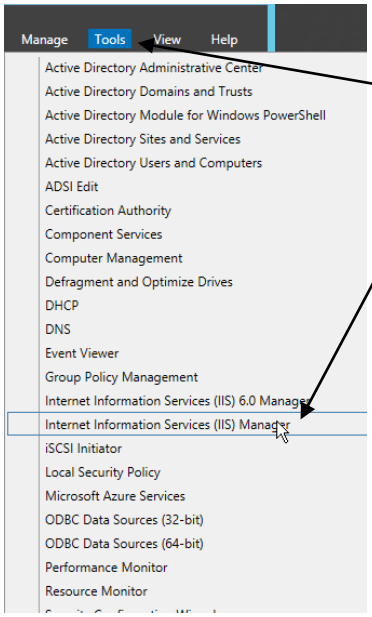
The next server and last server is the FTP Server this will allow user to access files and send files from other areas.



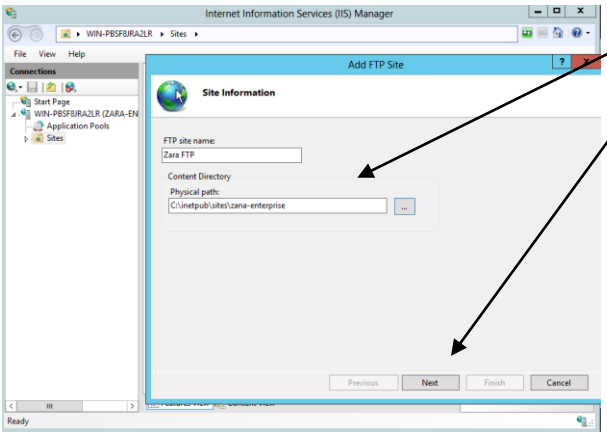
Firstly like the others we go through the add roles and features wizard, this page on “server roles” we click “FTP Server”, the click next.



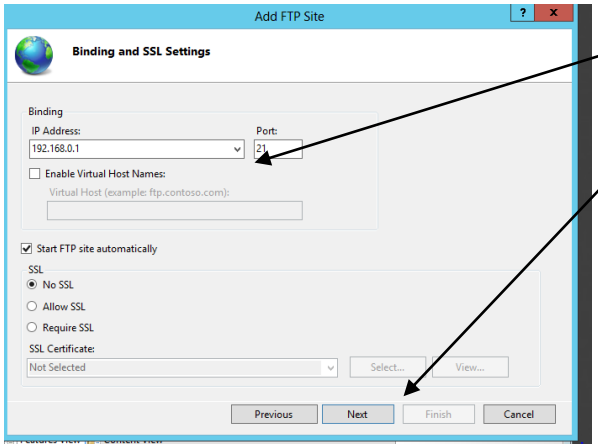
Then click install to finish the install.



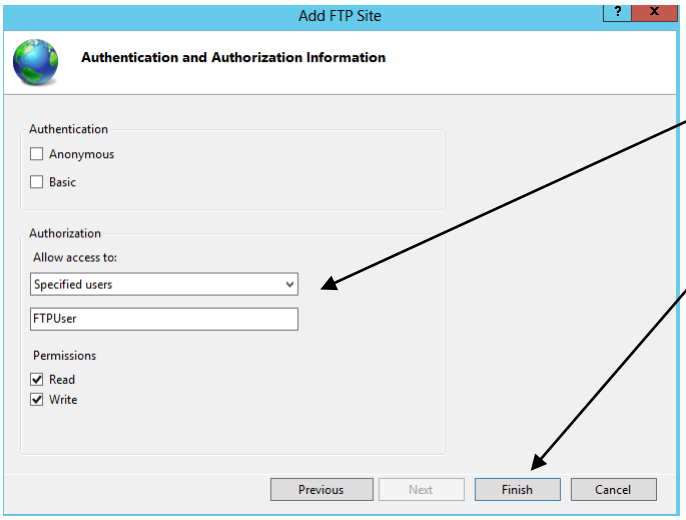
Go to tools then select “Internet Information Services (IIS) Manager”.



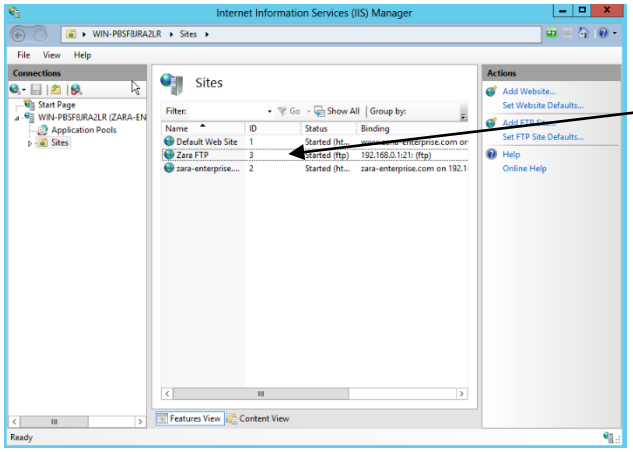
Fill out the fields and physical path. Then click next.



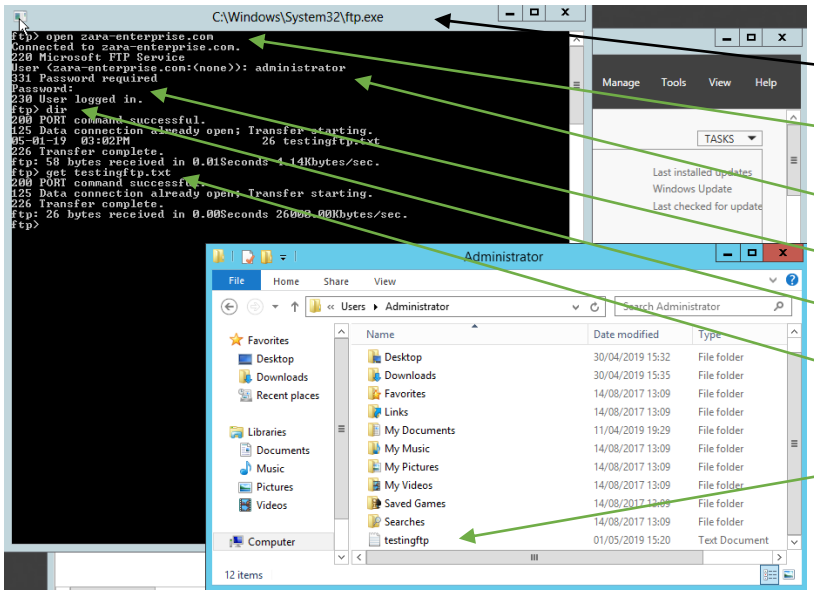
Then select the IP address for the domain, then select No SSL, then next.



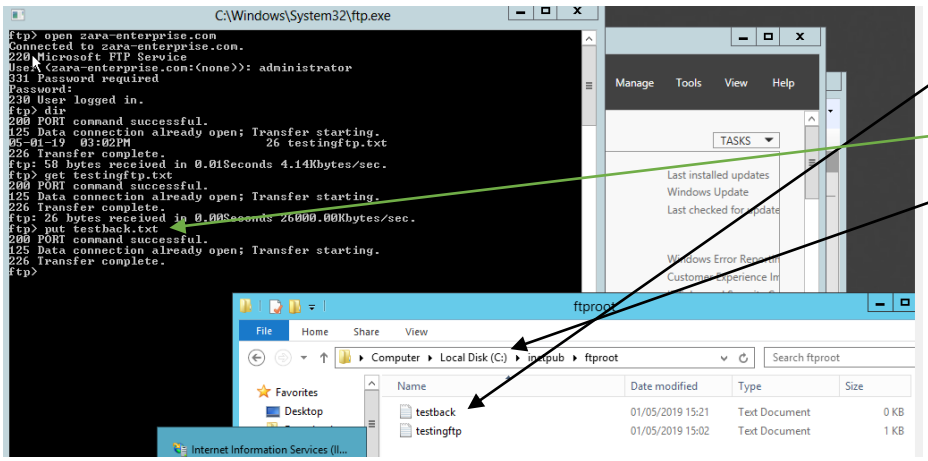
Select “specified users”, then select “read and write” permissions. Then click finish.



Proof FTP server was created.



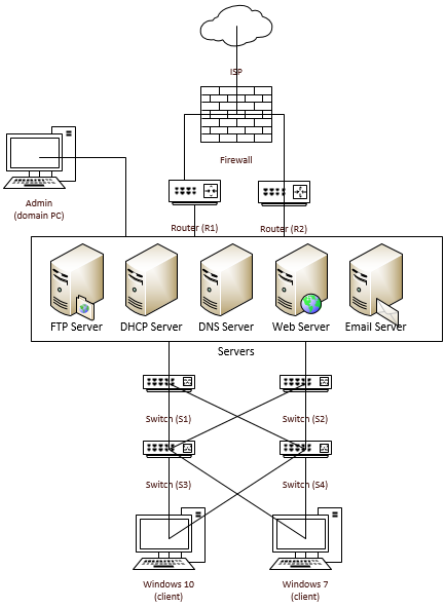
Click windows key then type “FTP” and open it, it will show the [FTP.exe](#) command controller, We type “open zara-enterprise.com”, it will then tell us to type user name we then type “administrator”, it will then ask for password type “Pa$$w0rd”, the type “dir” to check the files in current directory, then type “get testingftp.txt” it will then move the text fill to the admin user space.



We then create another file called “testback”, and type in the command prompt “put testback.txt”, it will then move the file to the “ftproot” folder in the local disk drive next to the “testingftp” file.

4.1.6 Network Diagram (COMPLETE DIAGRAM)

The diagram below shows what the servers and clients nodes look like in a network diagram.



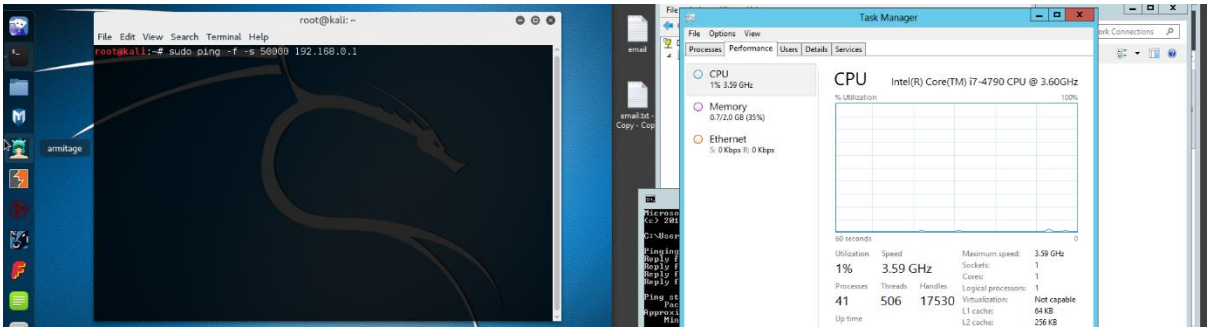
This network diagram is a very simple diagram which includes the internet connection, Firewall, routers, All Servers (FTP, DHCP, DNS, WEB, Email), switches with backups, then a Admin PC connecting to the servers, then the clients machines which was Windows 10 and Windows 7.

4.2 Five Security Attacks using Kali Linux

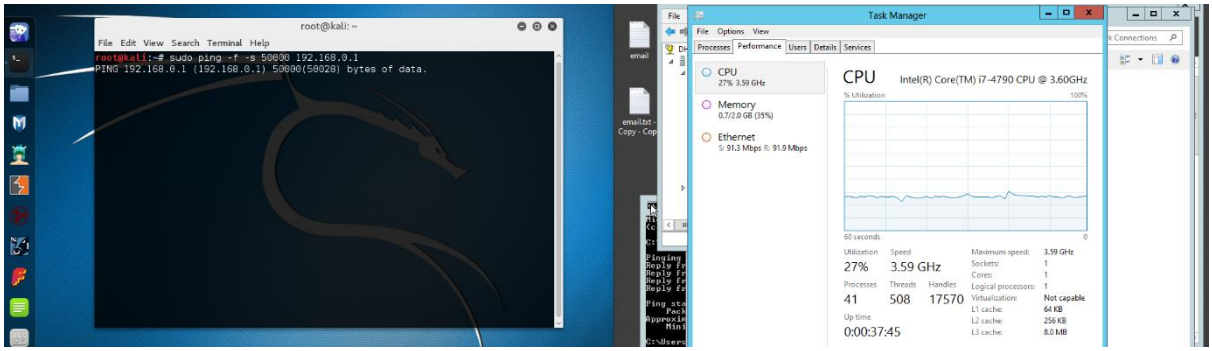
In this section it will show attacks on the servers we just created on Kali and give a solution on how to stop or mitigate the attacks.

4.2.1 Attack 1 (Ping Flood)

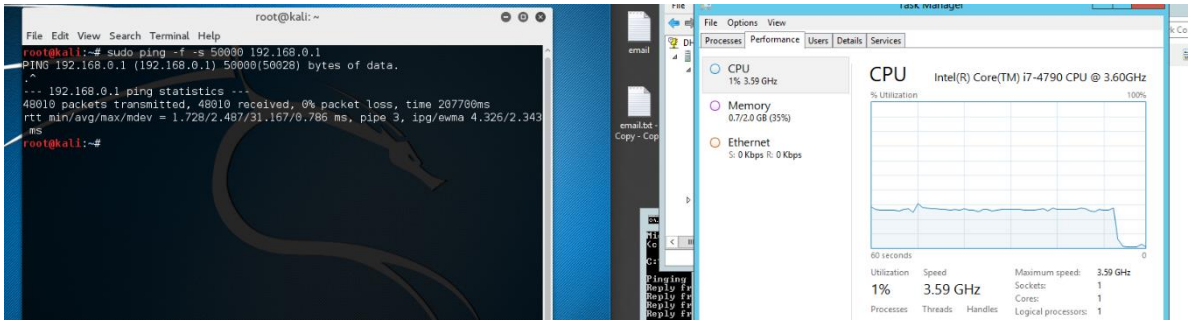
This attack will overload the DNS server and make it run slower depending on how my packets are sent at that time for this example I will be sending 50000 packets to the Windows Server 2012 IP address (192.168.0.1). This will be done on Kali the command used is “sudo ping –f –s 50000 192.168.0.1”. Images below will show evidence on making the Windows server 2012 machine working hard on CPU usage.



Kali on the left and Windows server 2012 on the right. You can see the CPU resting at 1% before the attack. You can also see the code used on the left in the Kali machine.



After the command has been executed on the left you can see the CPU usage jump to cope with the high traffic of the ping flood attack on the right.



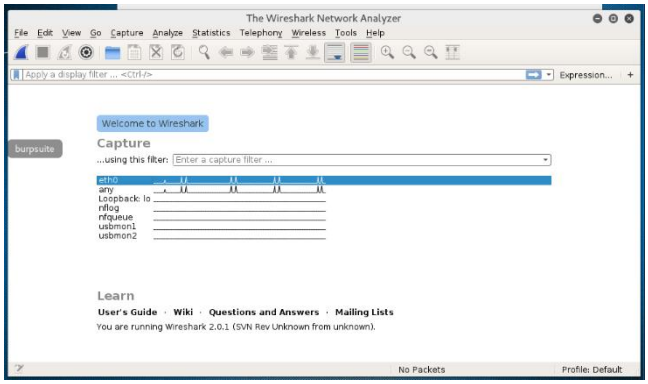
After the attack has stopped by pressing “Ctrl + c”, then you can see the CPU usage go back to 1% proving the attack was successful.

4.2.1.1 Solution

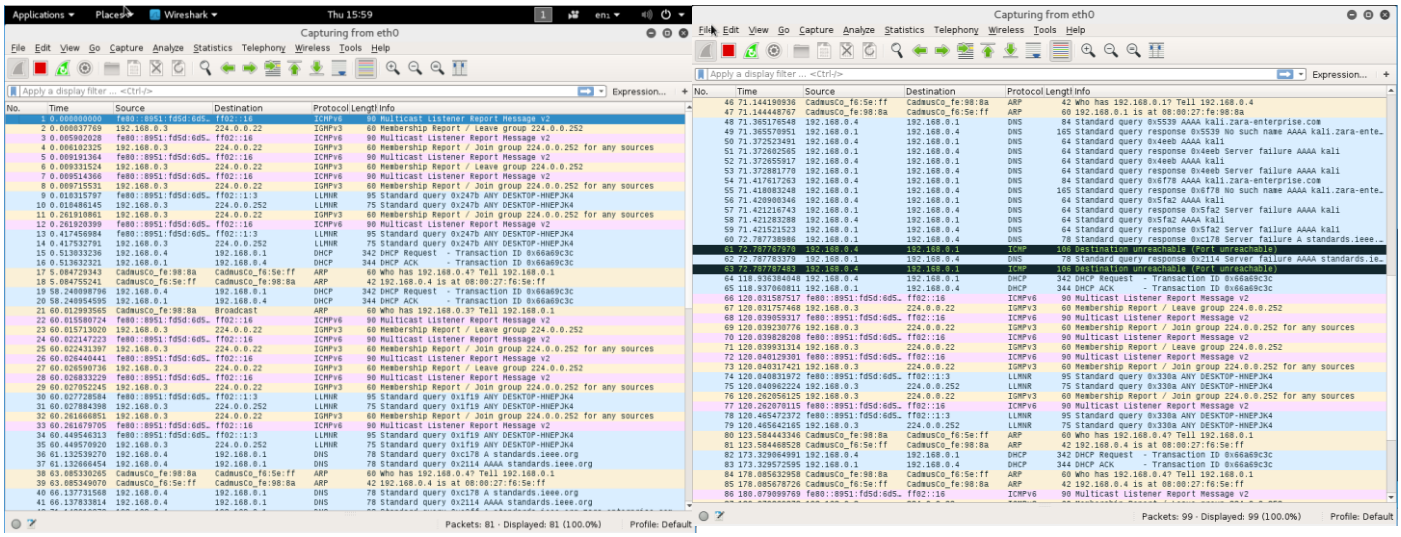
The solution to a Ping Flood or DDos is to get DDos Protection, this kind off protection mitigates the largest attacks immediately without having the server latency problems, it also restricts the amount of ping (packets) requests a PC or node can use.

4.2.2 Attack 2 (Packet Tracer)

This attack is to sniff the packets also known a packet tracer the software used is called Wireshark. We will be using Kali Linux again and sniffing a Windows server 2012, and Windows 10 machines which are connected to the Domain.



We select “eth0” to sniff, then click start it will then start to sniff the traffic of the servers used from DNS, DHCP and show the source of the traffic, the destination of the packet, the protocol it has been sent over, the length of the request and info of the packet.



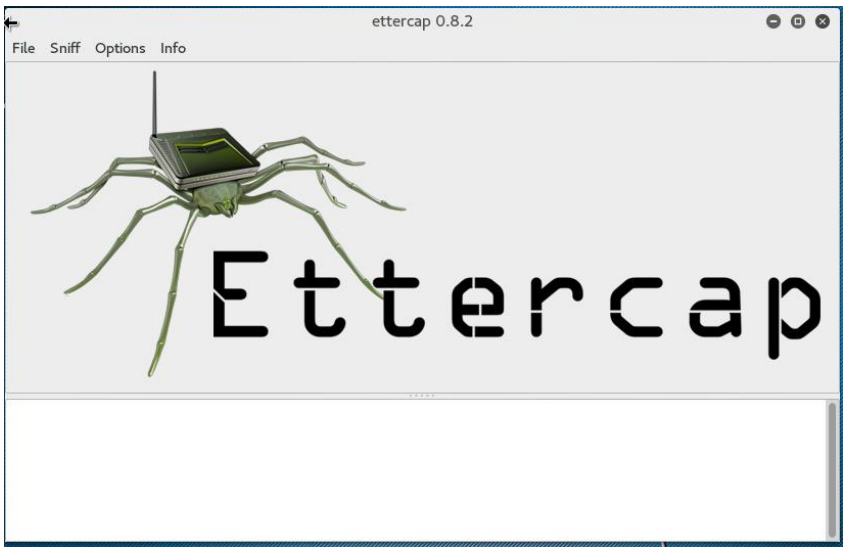
The two images above will show the traffic after the domain machines, pings of users PC, Request to access the website from selection 4.1.3. This evidence shows the IP address of the two machines talking and a hacker can use these information to attack IP and servers a number of hacks can come out of this from DDos, IP spoof, password sniff etc. This capture shows DNS, DHCP request so someone malicious can use this to do damage.

4.2.2.1 Solution

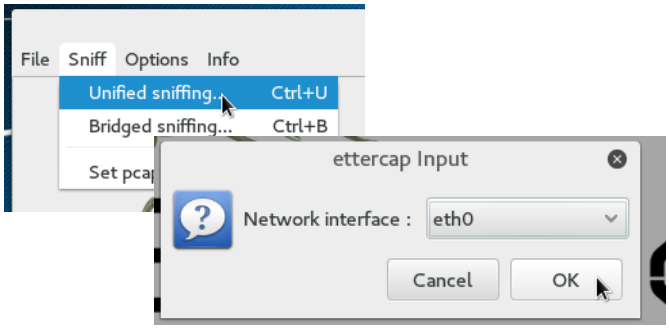
There are a number of solutions to prevent a packet sniffer, one simple method is to use HTTPS websites this will encrypt the information to and from the website. Another way is to have the network running on a VPN this will encrypt your traffic so the hackers doesn't know what it is. VPN are very cheap in the current year and still have good speeds, The VPN can be implemented on the Router of a network so no need for multiple VPNs for each PC on the network.

4.2.3 Attack 3 (Man in the Middle)

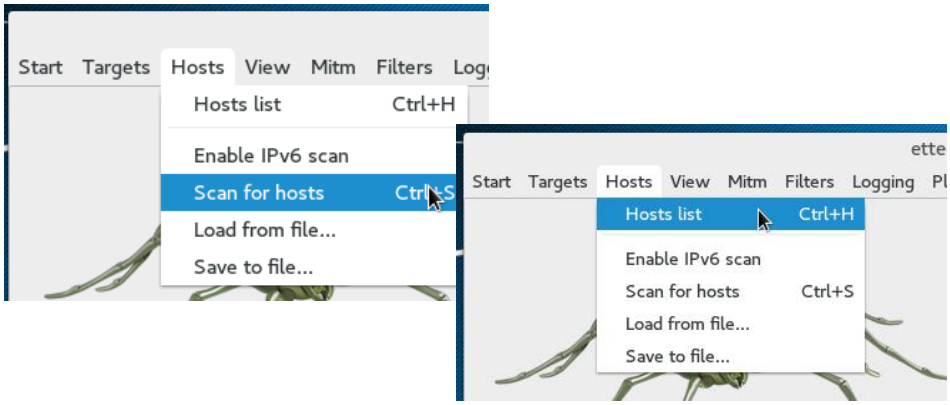
This attack is where a hacker gets in-between to PCs in this case the server and windows 7 PC. This allows the hackers to get the quests through a software to check what they are doing.



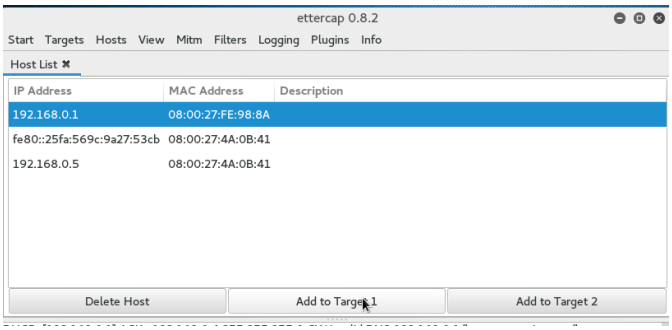
Open Ettercap in terminal (Ettercap –G).

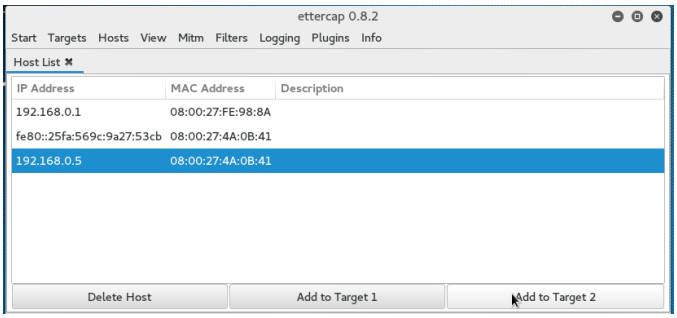


Once open, click sniff and select “Unified sniffing”, then select network interface “eth0”, then click ok.

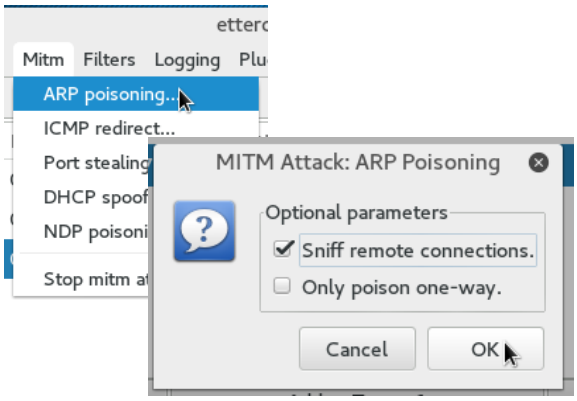


Then go to hosts and select “Scan for hosts”, then click “hosts list”.

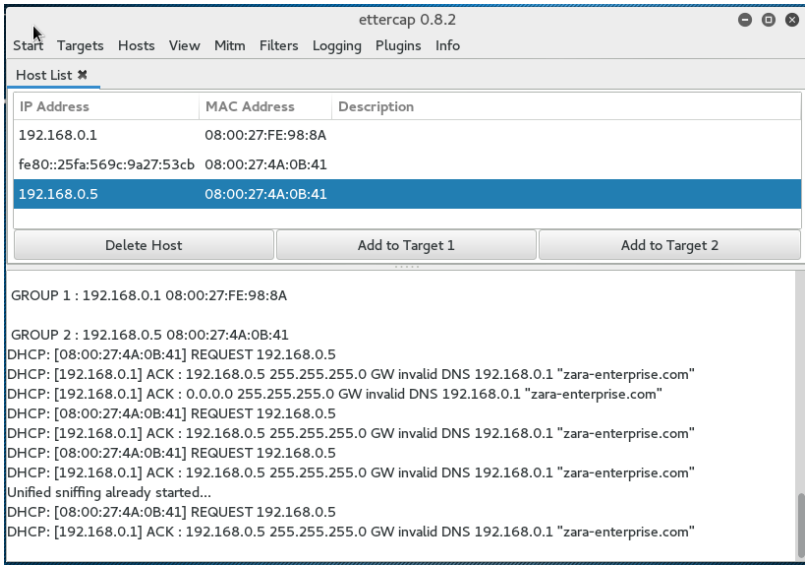




Then we select the server IP and click “add to target 1” and select the windows 7 IP and click “add to target 2”.

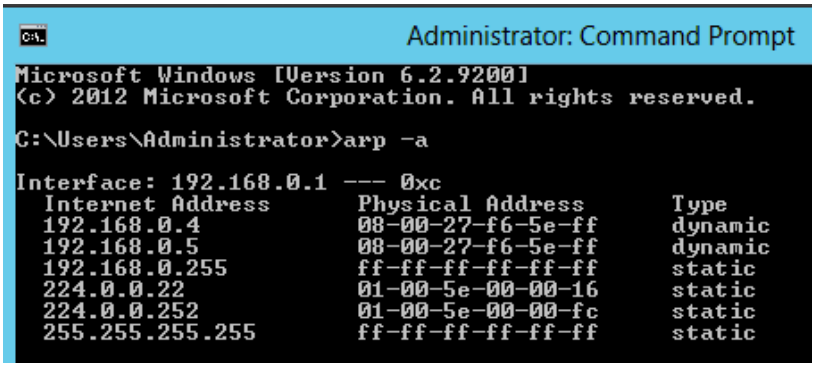


We then click Mitm and click “ARP poisoning”, then choose “sniff remote connections”, then click ok.



It will start to collect traffic from the attack.

After stopping the attack it will put the network back to normal where the Mitm is not there anymore.



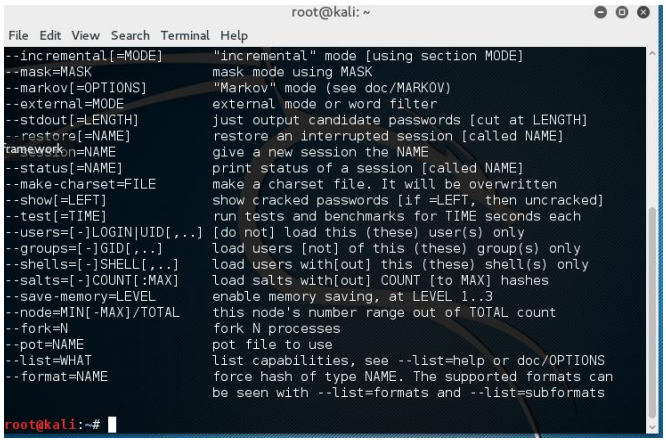
Then go back to the server and put command in cmd arp –a to see the interfaces and can see the hacker, because of the double addresses.

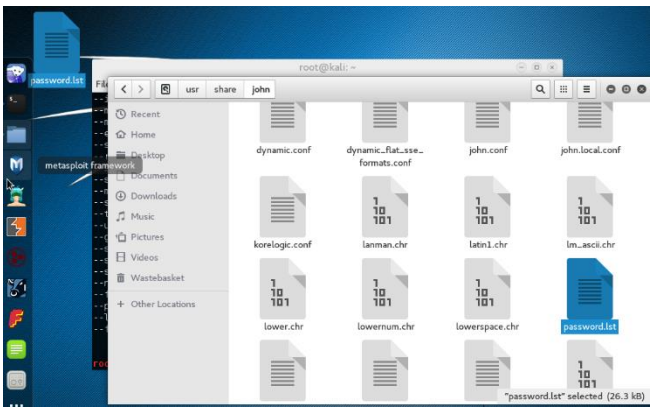
4.2.3.1 Solution

Again this is similar to attack 2 make sure the network has a VPN and browser with encryption.

4.2.4 Attack 4 (FTP server password crack)

This attack is using “John” password cracking software from Kali.





We open the John software and opens in terminal, then copy the password list from Jon to desktop.

```
root@kali:~# hydra -t 1 -l adminstrator -P /root/Desktop/password.lst -vV 192.168.0.1 ftp
```

```
root@kali:~# hydra -t 1 -l administrator -P /root/Desktop/password.lst -vV 192.168.0.1 ftp
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service orga
nizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-04 14:50:53
[DATA] max 1 task per 1 server, overall 64 tasks, 3548 login tries (l:1/p:3548), ~55 tries p
er task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "" - 1 of 3548 [child 0]
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "123456" - 2 of 3548 [child 0]
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "12345" - 3 of 3548 [child 0]
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "password" - 4 of 3548 [child 0]
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "password1" - 5 of 3548 [child 0
]
[ATTEMPT] target 192.168.0.1 - login "administrator" - pass "Pa$$w0rd" - 6 of 3548 [child 0]
[21][ftp] host: 192.168.0.1   login: administrator   password: Pa$$w0rd
[STATUS] attack finished for 192.168.0.1 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-04 14:50:53
```

After entering the line above it will search the vast selection of Passwords and found the password for the FTP server.

4.2.4.1 Solution

Best way to prevent this from happening is to have mandatory password changes.

4.3 Costing Table

This table will show a low and cost budget for the setup it will include the bare minimum to set up the network and additions will need to be add once the company get bigger.

Hardware	Low cost	High cost
Server	Smart Value Flexi | PowerEdge T430 | 8x3.5" | E5-2609v4 | 2x8GB | 1x1TB 7.2K SATA | H330 | 3Yr NBD (£1,102.50), (Dell.com, n.d.)	877623-031 HPE ProLiant ML350 Gen10 Tower Server (£7,074.00), (Serversandmore.co.uk, n.d.)
Ethernet cable	Nexans CAT 5E Ethernet Cable 100m Grey (£25.87), (Screwfix, n.d.)	100m Cat6 Heavy Duty External Solid Copper ED UTP Network Cable (£59.98), (Amazon.co.uk, n.d.)
Fibre Optic	LC-SC UPC Duplex Single Mode Fibre Patch Lead 2.0mm PVC (OFNR) 10m (40 pcs) (£183.36), (FS .com, n.d.)	NETGEAR AXC762020m Direct Attach SFP+ Cable (£299.46), (Broadband buyer.com, n.d.)
PC's	XPS 8920 (£769.00), (Dell.com, n.d.)	XPS Tower (£1,199.00), (Dell.com, n.d.)
Software (OS)	Windows server 2012 Foundation (£209.99), (Lizengo Great Britain, n.d.) / Windows 10 Pro (£32.99), (Lizengo Great Britain, n.d.)	Windows Server 2012 DataCenter (£1,899.99), (Lizengo Great Britain, n.d.) / Windows 10 Enterprise LTSB 2016 (£229.99), (Lizengo Great Britain, n.d.)
Switches	Cisco Catalyst 3560V2-48TS - switch - 48 ports - Managed - rack-mountable (£234.00), (Evaris.com, n.d.)	HP 2530-48G Switch - switch - 48 ports - Managed - desktop, rack-mountable, wall-mountable (£492.00), (Evaris.com, n.d.)
Router	Cisco RV320 (£191.46), (Comms-express.com, n.d.)	Cisco 1921 Integrated Services Router (£611.17), (Comms-express.com, n.d.)
Total	£2,749.17 Bare minimum that is without, multiple software, and PC for employees	£11,865.59 Bare minimum so the high cost setup, will cost more when number of PC rise with OS.

5 References

Figure 1 - SSL2BUY Wiki - Get Solution for SSL Certificate Queries. (n.d.). *Symmetric vs. Asymmetric Encryption – What are differences?*. [Online] Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences [Accessed 29 April 2019].

Figure 2 - SSL2BUY Wiki - Get Solution for SSL Certificate Queries. (n.d.). *Symmetric vs. Asymmetric Encryption – What are differences?*. [Online] Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences [Accessed 29 April 2019].

SSL2BUY Wiki - Get Solution for SSL Certificate Queries. (n.d.). *Symmetric vs. Asymmetric Encryption – What are differences?*. [Online] Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences [Accessed 29 April 2019].

Keccak.team. (n.d.). *Keccak Team*. [Online] Available at: https://keccak.team/keccak_specs_summary.html [Accessed 29 April 2019].

Grimes, R. (2018). *Why aren't we using SHA3?*. [online] CSO Online. Available at: https://www.csoonline.com/article/3256088/why-arent-we-using-sha3.html [Accessed 6 May 2019].

Kelsey, J. (2013). *SHA3 Past, Present, and Future*. [online] Csrc.nist.gov. Available at: https://csrc.nist.gov/CSRC/media/Projects/Hash-Functions/documents/kelsey_ches2013_presentation.pdf [Accessed 6 May 2019].

Betterexplained.com. (n.d.). *Understanding the Birthday Paradox – BetterExplained*. [online] Available at: https://betterexplained.com/articles/understanding-the-birthday-paradox/ [Accessed 6 May 2019].

Figure 3 - Bellows, A. (2006). *The Birthday Paradox*. [online] Damn Interesting. Available at: https://www.damninteresting.com/the-birthday-paradox/ [Accessed 6 May 2019].

Karonen, I. (2017). *Does Lamport's authentication scheme still work if the hash function is not collision-resistant?*. [online] Cryptography Stack Exchange. Available at: https://crypto.stackexchange.com/questions/39379/does-lamports-authentication-scheme-still-work-if-the-hash-function-is-not-coll [Accessed 6 May 2019].

Costing table References

Dell.com. (n.d.). *PowerEdge T430 Expandable 2-socket Tower Server | Dell UK*. [Online] Available at: https://www.dell.com/en-uk/work/shop/servers-storage-networking/smart-value-flexi-poweredge-t430-8x35-e5-2609v4-2x8gb-1x1tb-72k-sata-h330-3yr-nbd/spd/poweredge-t430/PET43001a [Accessed 4 May 2019].

Serversandmore.co.uk. (n.d.). *Buy 877623-031 HPE ProLiant ML350 Gen10 Tower Server here at Servers and More*. [Online] Available at: https://serversandmore.co.uk/proddetail.php?prod=877623-031+HPE+ProLiant+ML350+Gen10+Tower+Server&gclid=CjwKCAjw8LTmBRBCEiwAbhh-6HoYbfDwEZLivHcUyN986MTfPYkrFY4TJH2nF8cNfG3uV3-1OMjBfhoCPjEQAvD_BwE [Accessed 4 May 2019].

Screwfix. (n.d.). *Nexans cat 5e Ethernet cable 100m Grey*. [Online] Available at: https://www.screwfix.com/p/nexans-cat-5e-ethernet-cable-100m-grey/875fk [Accessed 4 May 2019].

Amazon.co.uk. (n.d.). *100m Cat6 Heavy Duty External SOLID COPPER Double Lined UTP Network Cable for Outdoor use BLACK Reel*. [Online] Available at: https://www.amazon.co.uk/External-COPPER-Double-Network-Outdoor/dp/B01GK898I0/ref=sr_1_3?adgrpid=54217853038&gclid=CjwKCAjw8LTmBRBCEiwAbhh-

6B3DayS2AZl8nSFyvh1aZzXqQzVjBy83jc738jhC5pGy1vcIwLcanRoCUHEQAvD_BwE&hvadid=259029093552&hvdev=c&hvlocphy=9046821&hvnetw=g&hvpos=1t1&hvqmt=e&hvrand=14447049507200743437&hvtargid=kwd-296601539403&hydadcr=28146_1724745&keywords=cat6+cable&qid=1556980248&s=gateway&sr=8-3 [Accessed 4 May 2019].

FS .com. (n.d.). *LC-SC Single Mode Fibre Patch Lead Duplex 10m (33ft) - Yellow*. [Online] Available at: https://www.fs.com/uk/products/40227.html [Accessed 4 May 2019].

Broadband buyer.com. (n.d.). *Netgear AXC762020m Direct Attach SFP+ Cable*. [Online] Available at: https://www.broadbandbuyer.com/products/32042-netgear-axc7620-10000s/?gclid=CjwKCAjw8LTmBRBCEiwAbhh-6Ooh2Z-biZ4q7p1uwS9qE2d81ObHOfLSW8YVCO-ILE6noz2qhwfeQxoC2eMQAvD_BwE [Accessed 4 May 2019].

Dell.com. (n.d.). *XPS 8930 VR Ready Desktop with 8th Gen Intel Processor | Dell UK*. [Online] Available at: https://www.dell.com/en-uk/work/shop/desktop-and-all-in-one-pcs/xps-tower/spd/xps-8930-desktop [Accessed 4 May 2019].

Dell.com. (n.d.). *XPS 8930 VR Ready Desktop with 8th Gen Intel Processor | Dell UK*. [Online] Available at: https://www.dell.com/en-uk/work/shop/desktop-and-all-in-one-pcs/xps-tower/spd/xps-8930-desktop/BDX89311 [Accessed 4 May 2019].

Lizengo Great Britain. (n.d.). *Windows Server 2012 Foundation*. [Online] Available at: https://www.lizengo.co.uk/microsoft/windows-server-2012-foundation [Accessed 4 May 2019].

Lizengo Great Britain. (n.d.). *Windows Server 2012 DataCenter*. [Online] Available at: https://www.lizengo.co.uk/microsoft/windows-server-2012-datacenter [Accessed 4 May 2019].

Lizengo Great Britain. (n.d.). *Windows 10 Pro*. [Online] Available at: https://www.lizengo.co.uk/microsoft/windows-10-pro [Accessed 4 May 2019].

Lizengo Great Britain. (n.d.). *Windows 10 Enterprise LTSB 2016*. [Online] Available at: https://www.lizengo.co.uk/microsoft/windows-10-enterprise-ltsb [Accessed 4 May 2019].

Evaris.com. (n.d.). *Cisco Catalyst 3560V2-48TS - switch - 48 ports - Managed - rack-mountable - Evaris*. [Online] Available at: https://www.evaris.com/shop/cisco-catalyst-3560v2-48ts-switch-48-ports-managed-rack-mountable?pid=5391&ppc_keyword=&gclid=CjwKCAjw8LTmBRBCEiwAbhh-6ItvMLtMctNXT3dCMzDRlSxSYTS4NmoY1SF02Rke2_7ALSqVHOYbmBoCXhAQAvD_BwE [Accessed 4 May 2019].

Evaris.com. (n.d.). *HP 2530-48G Switch - switch - 48 ports - Managed - desktop, rack-mountable, wall-mountable - Evaris*. [Online] Available at: https://www.evaris.com/shop/hp-2530-48g-switch-switch-48-ports-managed-desktop-rack-mountable-wall-mountable-3?pid=28253&ppc_keyword=&gclid=CjwKCAjw8LTmBRBCEiwAbhh-6DFJMd2LSWkKnAUfF8z0XXT38fAb7B33pbdlF5FcVhY0Iqp6gxu1YRoCe-cQAvD_BwE [Accessed 4 May 2019].

Comms-express.com. (n.d.). *CISCO RV320-K9-G5 RV320 - Dual Gigabit WAN VPN Router with Built-in....* [Online] Available at: https://www.comms-express.com/products/cisco-rv320/ [Accessed 4 May 2019].

Comms-express.com. (n.d.). *CISCO CISCO1921/K9 1921 Integrated Services Router | Comms Express*. [Online] Available at: https://www.comms-express.com/products/cisco-1921-integrated-services-router/ [Accessed 4 May 2019].