cloudlogics

Scarborough's Cloud Specialists

CNET 327

Team Members:
Kris Starev – 300.480.279
Waqar Ahmed – 300.929.326
Gavin Forbes – 300.978.267
Tran Duc Tai – 300.923.196

School of Engineering Technology and Applied Science
SETAS
Centennial College – Progress Campus

Submitted to Professor Hussain Fatmi

December 1, 2020

DECLARATION OF AUTHORSHIP

I hereby certify that the report I am submitting is entirely my own original work except where otherwise indicated. I am aware of the Centennial College's rules and regulation concerning plagiarism, including those regulations concerning disciplinary actions that may result from plagiarism. Any use of the works of any other author, in any form, is properly acknowledged at their point of use.

Student Name: Gavin Forbes

Student Digital Signature: G Forbes

Student ID: 300.978.267

Student Name: Kristiyan Starev

Student Digital Signature: KBS

Student ID: 300.480.279

Student Name: Waqar Ahmed

Student Digital Signature: WA

Student ID:

Student Name: Duc Tai Tran

Student Digital Signature: DCT

Student ID: 300.923.196

ABSTRACT

Cloudlogics is a service-first oriented company that builds hardware and software architectures to meet a wide scale of technology needs. We offer industry-leading turn-key solutions in the software, infrastructure and platform as a service environment. As employees, we challenge each other to expand our knowledge and innovate. Our services are robust and flexible and scalable to meet the demands of any business.

Commented [HF1]: Very brief, summary of result not evident

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviations	Description
ACL	Access Control List
AD	Active Directory
AMI	Amazon Machine Image
API	Application Programming Interface
APTs	Advanced Persistent Threats
AWS	Amazon Web Services
AWS KMS	Amazon Web Services Key Management Service
CPU	Central Processing Unit
DHCP	Dynamic Host Control Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service
dot1Q	Networking Standard that supports VLANS
EC2	Elastic Cloud Computing
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GbE	Gigabit Ethernet
GPO	Group Policy Objects
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity Access Management
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MGT	Management Interface
ML	Machine Learning
NACL	Network Access Control List
NAT	Network Address Translation
NGFW	Next Generation Firewall
NTP	Network Type Protocol
OS	Operating System
OU	Organizational Unit
PA	Palo Alto
PBX	Private Branch Exchange
PHP	Hypertext Preprocessor
POP3	Post Office Protocol version 3
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User
RDP	Remote Desktop Program
RFC	Remote Function Call
RSAT	Remote Server Administration Tools
S3	Secure Storage Service

SAM	Security Access Management
SMTP	Simple Mail Transfer Protocol
SQL	Standardized Query Language
SRTP	Secure Real-Time Transport Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
STP	Spanning Tree Protocol
TLD	Top-level domain
TLS	Transport Layer Security
UNC	Universal Naming Convention
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPC	Virtual Private Cloud
VPG	Virtual Private Gateway
VPN	Virtual Private Network
VPS	Virtual Private Server
WAF	Web Application Firewall
WAMP Server	Windows Apache MySQL PHP Server
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLC	Wireless LAN Controller

INTRODUCTION

Project Description

In the light of recent global developments, many business entities have moved their operation to remote and virtual means. Center Addiction and Mental Health has requested from our team to upgrade their current aging network to meet the demands for computing and growth. In our recommendation we have provided a topology, services, server that we believe would meet the client's needs. We are also providing an alternative model in the event the client wishes to remain in control of their computing resources.

Commented [HF2]: Needs elaboration

Executive Summary

Cloudlogics is a growing network design company, helping clients plan and implement network installations. Our goal is to become Canada's industry leader in network consultation by creating innovative and valuable services to our expanding customer base. We are currently trying to expand into the growing health services sector and take advantage of recent government commitments to expand health care infrastructure from both the Federal and Provincial governments.

This report details our response to CAMH's (Centre for Addiction and Mental Health) request to redesign their aging network infrastructure. We have proposed an innovative cloud-based solution that will allow CAMH to provide quicker more efficient services to

their patients. We will also provide an alternative on-site model that would allow CAMH to keep their network resources under their complete control. Our report will analyze both options in respect to cost, benefits, limitations and network security strategy. We will detail network topologies and the process of installation for both options. We will conclude the report with a final recommendation of the topology model that we believe will best serve CAMH' needs

Business Case

SUMMARY OF BUSINESS CASE

Center for Addiction and Mental Health (CAMH) has approached Cloudlogics to upgrade their current outdated IT infrastructure. CAMH was established in 1998 by the Government of Canada, by the amalgamation of four separate institutions. They are the largest mental health teaching hospital in Canada and the only emergency mental health provider in Ontario. CAMH has developed its software tools and maintained its patient and research databases housed on-premises. The Director of IT has expressed their desire to move all current IT operations to a cloud-based solution to improve data processing and computing demands and to reduce the existing IT staff due to high expenditure.

BUSINESS OPPORTUNITY

Our partnership with CAMH provides us with a unique opportunity to enter the growing mental health services market. CAMH is an industry leader in mental health care and research with over 4000 physicians and ten satellite locations across Ontario. We believe

Cloudlogics will provide a template for future health services provider network upgrades and expansions with our plan to upgrade their existing legacy network to a cloud-based virtual private system. The current Ontario government's commitment to end' Hallway Medicine' has led to a doubling of health care spending from 2.2% in 2011-2017 to 4.4% from 2016-2019 .

This opportunity with CAMH will help Cloudlogics penetrate the health services sector and expand our own business significantly. Gaining significant market share in an industry that spends approx. Sixty-four billion annually will allow us to expand our business to a new level. Helping create fast, efficient, and reliable networks will not only help our business grow but support the government to succeed in ending Hallway Medicine.

Business Model and Alternatives

PROPOSED TOPOLOGY MODEL

Benefits

Our cloud-based implementation will provide maximum scalability for our client's network. Implementing the cloud infrastructure allows for data storage elasticity to expand or contract their capacity to meet evolving business needs. CAMH will be able to access powerful equipment to meet their demand in situations where there is a short term to drastically increase their processing ability. Our plan will also provide scalability in terms of network technology, as often the technologies implemented can quickly become obsolete. Cloud infrastructure will prevent CAMH from purchasing expensive new equipment, as would be the case with locally owned physical machines.

Time savings will be a significant benefit of setting up the network in the AWS environment. Monitoring and keeping on-premises equipment up and running can be very time-consuming. Our proposal will allow CAMH IT staff to avoid the need to troubleshoot their equipment continually. They will not need to upgrade/update operating systems, deploy security patches or other regular maintenance. Also, periodic back-ups will be performed automatically in the cloud environment.

CAMH will have significant overall cost savings from our cloud implementation strategy. On-premises equipment requires extensive energy costs to power the machines, provide adequate cooling and overall building power costs. If the business needs to expand its network equipment, there will be no overhead for purchasing machines or additional cooling infrastructure. As the business grows, there will not be a need to hire other on-site personnel to maintain the expanded infrastructure.

Business continuity will be a significant benefit of our cloud implementation plan. In a natural disaster, flood, local power outage or other crisis, CAMH data will be safely stored onto the AWS cloud. They will quickly recover and bring their networks back online in any situation, with minimum downtime

Costs

AWS allows its customer to utilize an efficient pay-per-use model which allows organizations to efficiently use the computing resources and services they only need. The standard deployment model of AWS Directory Services is priced at approximately $86/ month. The configuration meets the demand of our client for business-as-usual operations.

AWS Service	Cost Rate	Cost Price
Amazon EC	Per hour	
	Free-tier instance	$0.00
	On-demand	$0.051 to $6.00
	Windows (Free Tier)	$0.00
	Small Factor Instance	$0.032
	Medium Factor Instance	$0.0644
	Large Factor Instanced	$0.1208
EBS (Storage Drives)	Per GB used	
	GB/month (Free tier)	$0.00
	GB/month (General Use SSD)	$0.10
AWS Database per SQL instance	Per hour	$0.72 to $22
AWS Routing Services DNS	Per set of 1,000,000 queries	$0.40
AWS Hosted Route	Per zone	
	> 25 zones/month	$0.50
	< 25 zones/ month	$0.10
AWS Directory Service	Per month	$86
AWS VPC	Per	

	NAT Gateway/ hour	$0.045
	Elastic IP/ month	$0.005
	ENI/ hour	$0.015
	GB of utilized data/ month	$0.045

Table 1 - AWS Costs

Limitations

One of the limitations of the cloud-based model is a lack of redundancy in the overall network. To help give CAMH administrators peace of mind we will implement a small on-site data center for the purpose of backing up data.

A second limitation of the cloud-based model is its reliance on an internet connection. In the event of local internet outages, the hospital could potentially lose access to their network. For this reason, we are recommending acquiring the services of a second internet service provider to remedy this issue.

Risks

The biggest risk for CAMH with the cloud-based network will be putting its private confidential medical data in the hands of a third-party company. PHIPA violations could present a financial risk if this information was compromised. We do feel that AWS excellent reputation for data security greatly alleviates this risk. It is becoming more and more common for medical institutions to house their data storage in the cloud. Telus

EMR has become a popular cloud-based tool popular among doctors for storing medical files, in place of on-site patient files.

ALTERNATIVES

Physical servers and network equipment can be installed on-premises to minimize external service usage, entirely replacing the existing architecture. Health care providers are often apprehensive with privacy breaches, and considering the stigma of mental illness, we have a secondary upgrade plan prepared for CAMH. Building a local physical network, including a small, secure Data Centre, will address any privacy concerns. Although we feel AWS cloud security parameters and our network security configurations are strong enough to mitigate privacy concerns, Cloudlogics is prepared with a plan to help CAMH upgrade their network with a secure, physical architecture.

Costs

The costs for implementing the on-site network will be significant. CAMH's current network is old, uses outdated legacy equipment and will need to be built from the ground up. The costs for the equipment will be in excess of $325,000, with the need to upgrade routers, switches, servers, workstations and IP phones. In addition to the physical equipment there will also be increased utility costs in comparison to our cloud-based solution.

CAMH will also need to invest in training for the IT staff to familiarize themselves with the new equipment and protocols that they will use. In the cost analysis for the on-site

option, we have included $10,000 in funding to train IT staff to use the open-source Nagios network management platform. Nagios provides a one-week on-site training program at a cost of $2500 per individual, that will be necessary to ensure multiple IT staff members have the skills they will need to monitor the network.

Benefits

The main benefit of building the on-site option is the control and ownership of resources. In Ontario medical records fall under the regulation of the Personal Health Information Protection Act (PHIPA) of 2004. A violation of the act is punishable by fines reaching $500,000 for organizations. With on-site facilities and resources, hospital administration has these records under their control direct control, providing peace of mind. Third parties have any access to these files would constitute a breach of PHIP and put the hospital at risk of costly fines. However, we do feel the cloud option we have arranged does provide robust security features, to mitigate the clients concerns.

Another benefit of the on-site alternative is there is not reliance on an internet connection to access data. Localized power outages would leave the hospital unable to access patient records until the internet service is restored. Having an on-site network would allow the hospital to solve this issue.

Limitations

Scalability is an area of concern for the on-site design model. Adding hardware for data storage in the cloud is quick, seamless and with no installation required. Scaling up the

network will be both time consuming and costly for CAMH. New equipment will need to order, shipped, installed, tested and then configured. ordered, shipped, installed, tested and configured. This involves many departments such as finance, procurement and the IT department. In contrast this could be handled quickly within the IT department, with a pre-established budget for increasing resources.

Another limitation of the on-site alternative is its ability to effectively mitigate instances of flood or fire. Data backed up locally will be vulnerable to these instances and has the potential for complete loss. Damaged equipment from disaster events would need to be replaced, meaning longer downtime for CAMH's network. In a hospital environment this could cause harm to patients whose medical data is unable to be accessed.

Physical space is a real limitation for the on-site alternative. Currently the hospital does not have significant room to implement anything more than a small data room. As addiction and mental illness have been in the focus of the provincial health authorities, CAMH dedicates as much space as possible for patients in treatment. Implementing only local equipment will mean CAMH would have to use space that is currently being used for patient services. A smaller IT staff would be required for the cloud-based model and this could lead to freeing more space for patient treatment.

Risks

Theft and malicious inside actors present a significant risk to the CAMH on-site model. Networking equipment is very costly and could easily be resold for profit. On-site severs

and files can also be accessed by staff member with the intent of redistributing the material. In the case of politicians, prominent community members, athletes and celebrities this data could be sold to news outlets. This type of breach would put CAMH in risk of PHIPA fines and significant legal liability.

Equipment failure or damage during a catastrophic event are risks for the on-site alternative. Cloud based servers are far less prone to failure and do not have the maintenance requirements of local machines. This means IT staff that should be monitoring the network for potential issues like intrusion, will instead split their focus between the two. The local machines are also at risk of being damaged in catastrophic events like fire or flood. In a hospital setting loss of data from equipment damage or failure would present a real risk to patient health.

Time Schedules

TIMELINE FOR EXECUTIONS

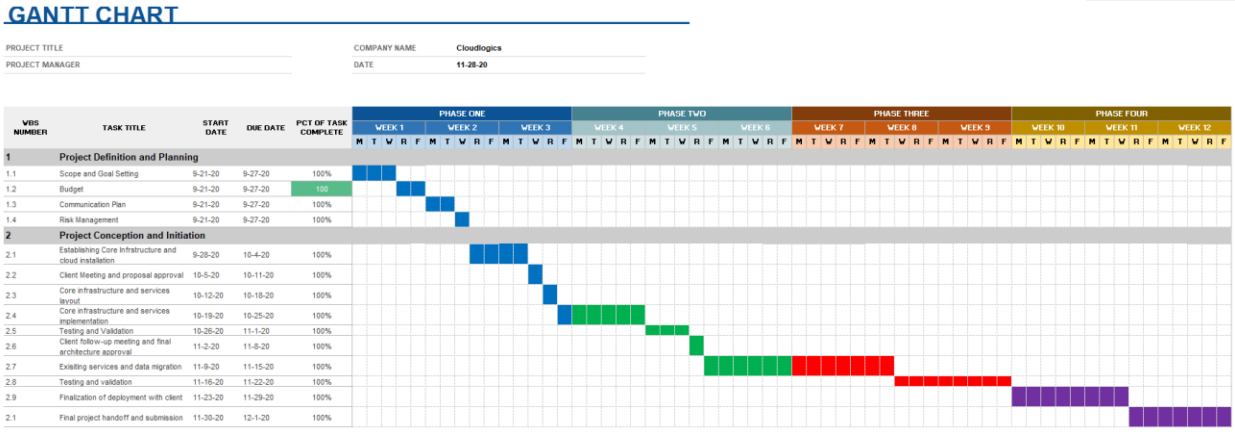
Cloudlogics and the client have agreed on the following execution timeline. However, we have advised the client of a 7-day possible extension in the event of unanticipated events impacting the original timeline.

Description	**Start Date**	**End Date**
Project Proposal	September 21, 2020	September 27, 2020
Establishing core Infrastructure and cloud initiation	September 28, 2020	October 4, 2020
Client meeting and proposal approval	October 5, 2020	October 11, 2020

Core Infrastructure and services layout	October 12, 2020	October 18, 2020
Core Infrastructure and services implementation	October 19, 2020	October 25, 2020
Testing and Validation	October 26, 2020	November 1, 2020
Client follow-up meeting and final architecture approval	November 2, 2020	November 8, 2020
Existing services and data migration	November 9, 2020	November 15, 2020
Testing and Validation	November 16, 2020	November 22, 2020
Finalization of deployment with client	November 23, 2020	November 29, 2020
Final Project submission and hand-off	November 30, 2020	December 6, 2020

GANTT CHART

Commented [HF3]: Where are the deliverables, risk analysis and budget



Solutions Infrastructure

AMAZON CANADA CLOUD SERVICES

Canadian Association for Mental Health is a mid-sized institution with several satellite office throughout Canada. As a health service and critical mental situations provider is essential for its operations both, on-site and off-site to have high availability for its employees and clients. By selecting AWS as an infrastructure provider, CAMH upgrades its legacy infrastructure and ensures that future expansions and computing needs can be met without sacrificing on-premises real estate. AWS provides its clients with 99.99% up-time guarantee of its services and infrastructure. Amazon has been a leader in the Infrastructure as a Service field for several years in a row now and has reached industry maturity and recognition. Thus, CAMH is being serviced by a well-established and sector approved service.

For CAMH to utilize the benefits of AWS, their main infrastructure and services have been fully located to the Cloud. CAMH has expressed their desire to access additional computing power for research purposes on special occasions on pay-per-use basis without any long terms commitment and AWS can delivered on that need. Adopting the cloud approach increases the institution's flexibility, agility and reduced over-head expenditures. Thus, allowing CAMH to re-channel funds towards important and critical services to help Canadians.

Services Utilized

- Amazon Virtual Private Cloud (VPC): Amazon Virtual Private Cloud provides logically isolated computing instances that can be scaled and configured to meet a wide range of computing demands and services.
- Amazon EC2: Amazon Elastic Cloud Computing provides a virtual environment to run a wide range of virtual instances with a variety of operating systems, load requirements, network resources and access levels. Utilizing EC2 allows CAMH to use pre-configured virtual templates, control security and connectivity, all from a web-based interface.
- IAM: The Identity Access Management is utilized by system administrators to restrict the access to the network resources and infrastructure based on position and authority level.
- VPC Internet Gateway: AWS based internet gateway, which is horizontally scaled, redundant, and highly available VPC component, permitting the communication among instances and the public internet.

Cloud Topology

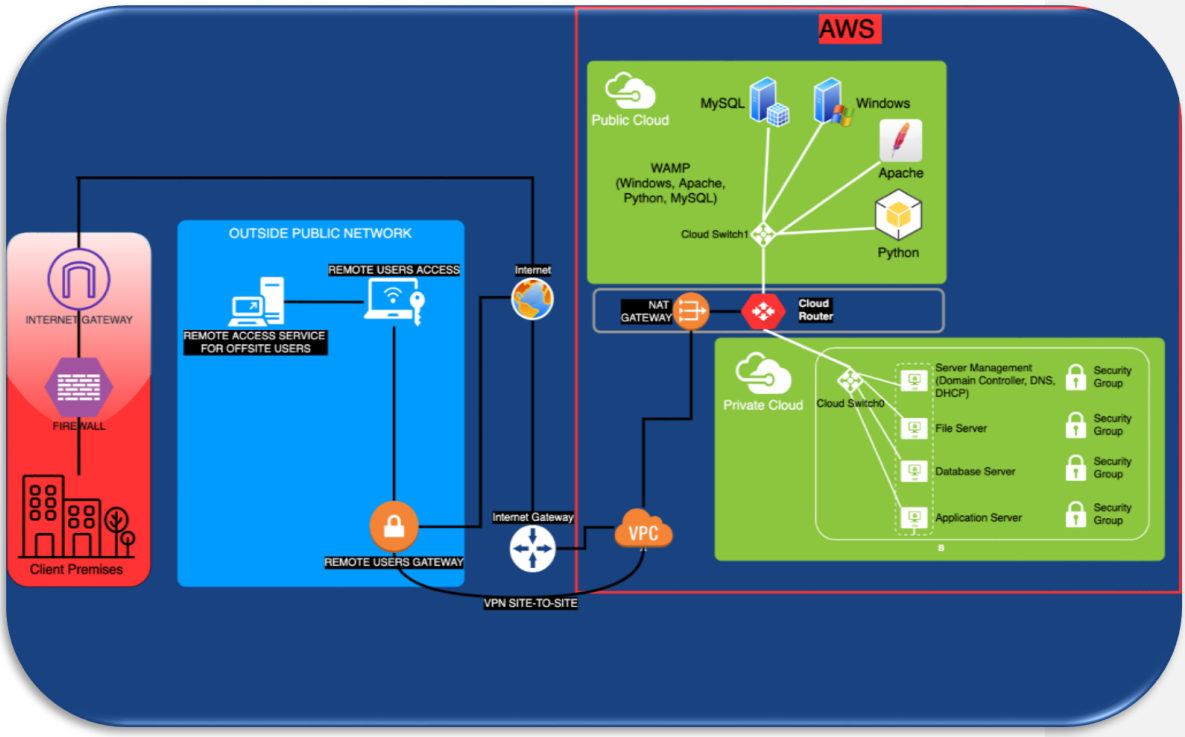


Figure 1 - AWS Topology

CLOUD SECURITY

Implementation & Approach

i. The cloud network is secured via multiple layers and best security practices.

ii. Monitoring tools are placed in the cloud to measure network utilization and provide information on issues and effectiveness

iii. To provide industry standard security measures, AWS Security services are utilized as they provide scalability, adaptability and high performance

Amazon Web Services

AWS was chosen amongst other competitors due to its security levels, flexibility, services, platforms interoperability, easy of implementation and deployment.

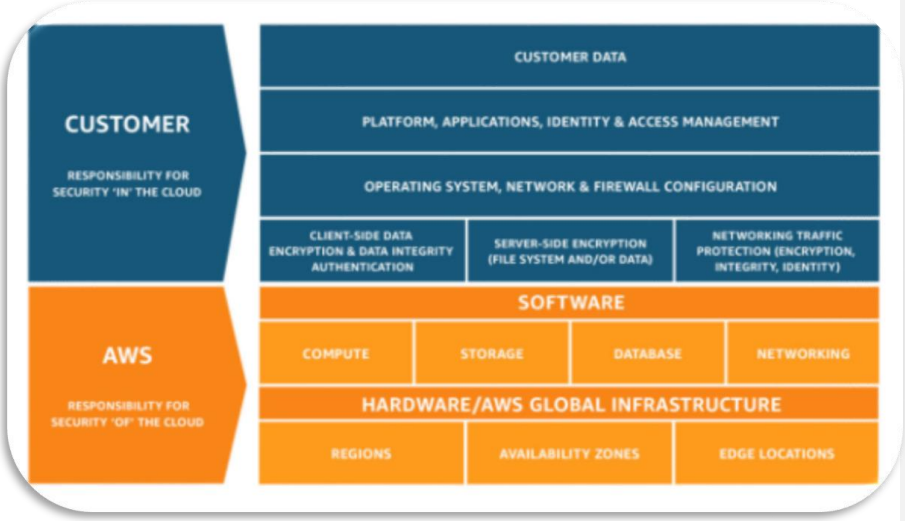


Figure 2 - AWS Client & Vendor Responsibilities

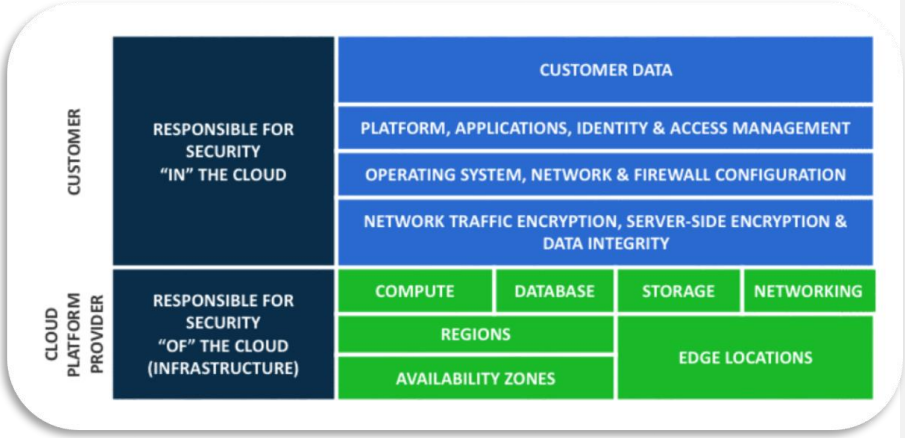


Figure 3 - Cloud provider vs. End-user – Responsibilities

Amazon Web Service Network Security Measures

i. Denial of Service Attack Mitigation, by utilizing multi-path high bandwidth connectivity, load balancing and web application firewall in the DNS

ii. AWS Identity and Access Management (IAM)

iii. AWS Access Control Lists controls and monitors traffic flows to ensure logical boundaries, traffic rules are implemented and enforced through the network for private and public access.

iv. Fault-Tolerant Infrastructure Design ensure up-time is unaffected during unexpected infrastructure faults (power, connectivity, threat actors). AWS has robust architecture that can withstand multiple simultaneous failures with limited or no down-time.

Virtual Private Cloud Security Measures

VPC establishes a logically isolated portion of the AWS Service Cloud and services as a platform to create Amazon EC2 virtual computing instances. It permits to create internal subnets, NATs, Internet Gateways similar to a real world instance. Most importantly, VPC comes pre-loaded with security features that can be enabled to secure and control access to a virtual environment.

i. Security Groups imitate a hardware firewall that control network traffic for all instances. However, multiple security groups can be involved with multiple virtual instances all permitting and functioning with different configurations.
ii. Server Security – all instances running on the AWS platform are protected by AWS Security Services. This is a must in order to protect from DDoS, port exploitation, and other cyber-attacks.

Cloud Security Measures

The below core security services are implemented to improve AWS security and compliance

i. AWS Identity and Access Management (IAM) – manages and controls access to the AWS Console. It allows system administrators in charge to provide lower level technicians access to the console without causing fatal errors due to lack of knowledge, experience, or mishap.
ii. User access monitoring – AWS logs all activity on to and from the console to provide timely alarming, alerting, and reporting.

iii. Incidence response – AWS provides tools to perform basic computer forensics to investigate any lost of data or service.

iv. Infrastructure security – provides multi-layer infrastructure security for AWS to reduce zero-day attacks, exploits and increase deployment efficiency.

CLOUD CONFIGURATIONS

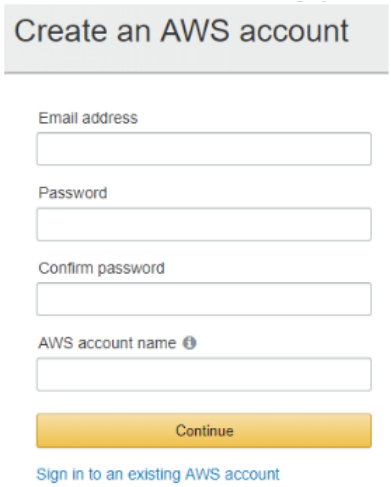
Part 1 – Begin AWS Configuration

Step 1 – Creating an AWS Account

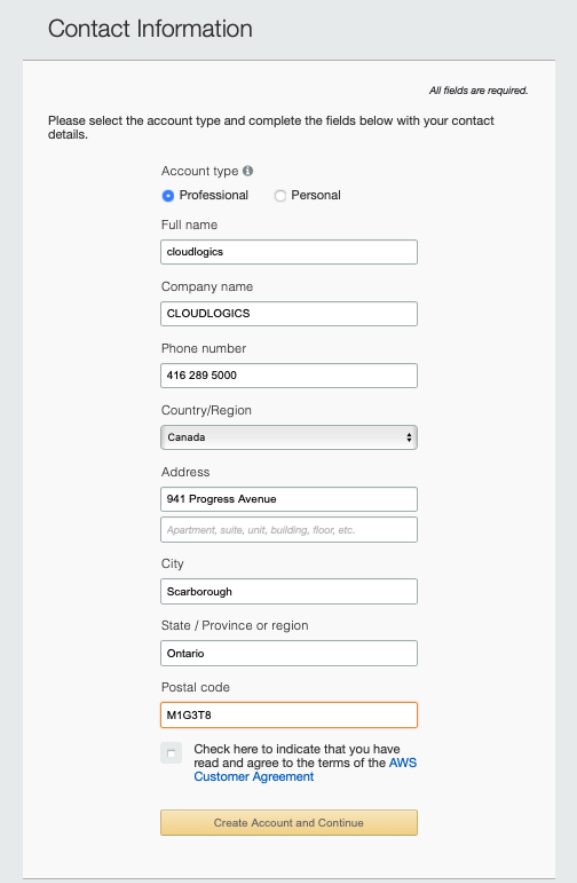
i. Using an internet browser, navigate to https://aws.amazon.com

ii. Click on the **Create an AWS Account** button at the top right corner.

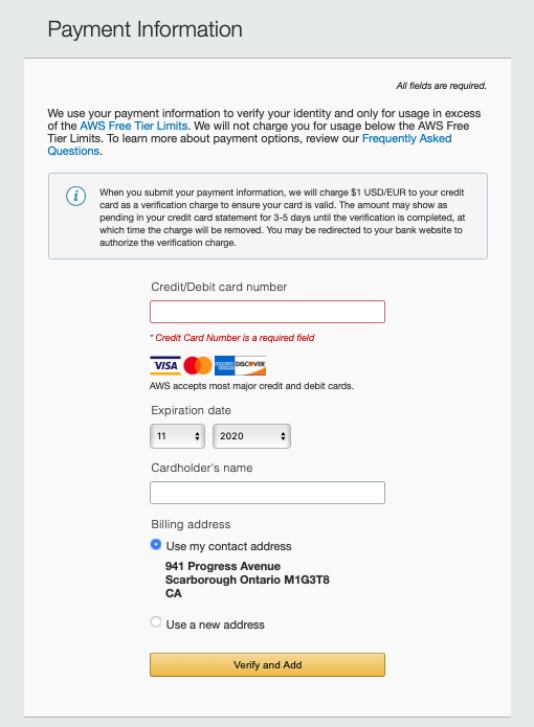
iii. On the "***Create an AWS Account***" page, fill out the required details and click on "***Continue***"



iv. On the "Contact Information" page, fil out the required information and click on "***Create account and Continue***"



v. On the payment information page, fill out the payment details and click "***Secure Submit***"



Step 2 – Follow the instructions to complete the required security procedures for the AWS setup

i. After completing the account, sign into the Management Console

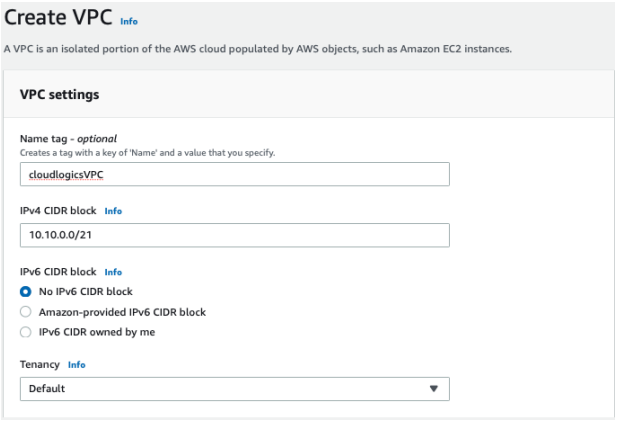
ii. Navigate to the "***Sign into the Console***" and enter the username and password details

iii. Once signed in, navigate to the AWS Console, which is the default account page

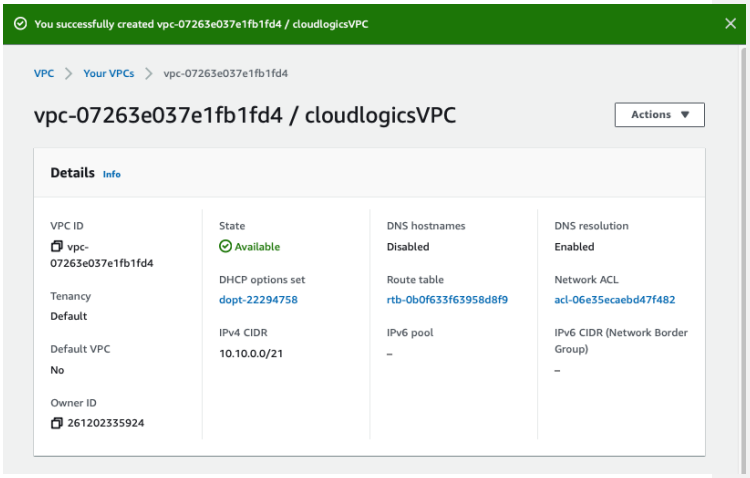
Part 2 – Configuring the Management Console

Step 1 – Virtual Private Cloud setup

- On the AWS Management Console page, click on "***Services***" drop-down tab on the left-top side
- From the drop-down menu, select the "***VPC***" option and then "Create VPC"



- Upon successful VPC creation, confirmation message appears



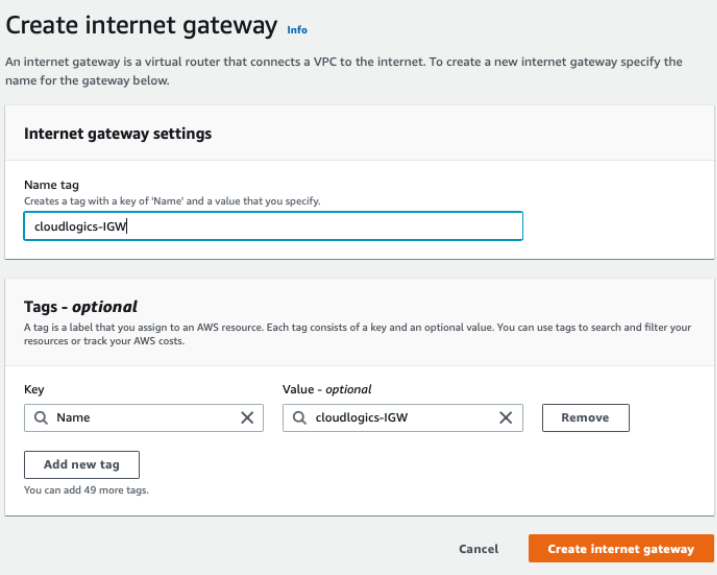
- Close the confirmation window to proceed

Step 2 – Internet Gateway configuration

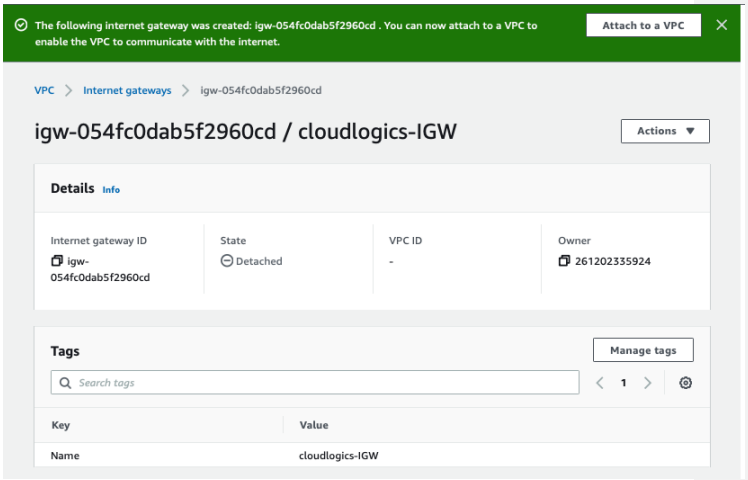
i. From the AWS Management Console, navigate to top left corner and click on "***Services***" to open the drop-down menu

ii. From the drop menu select "***VPC***" and click on "***Internet Gateways***"

iii. On the Internet Gateway home page click on "***Create Internet Gateway***", in the "***Name Tag***" field assign it a preferred name



iv. If the Internet Gateway is successfully created a confirmation message appears



v. Close the confirmation message to proceed

Step 3 – Connecting the VPC to the Internet Gateway

i. On the main Internet Gateway page, navigate to Internet Gateway, which was created in Step 2

ii. Click on "***Actions***" and selected "***Attach to VPC***" from the drop-down menu

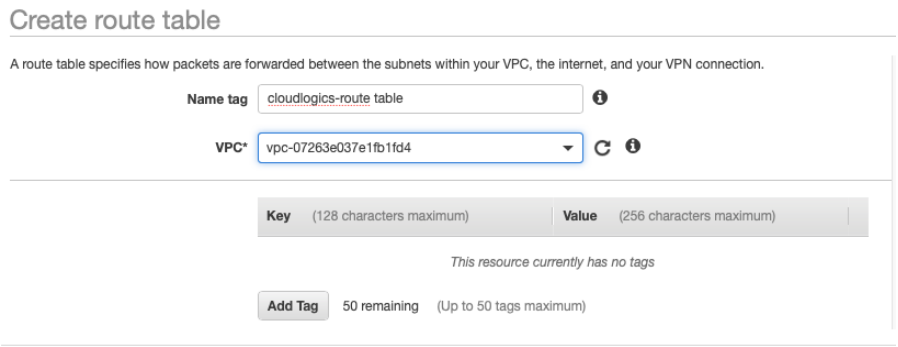
iii. Select the VPC created earlier and click on "***Attach***"

Step 4 – Creating a Routing Table

i. On the AWS Management Console page, click on "***Services***" at the top left and select "***VPC***" from the drop-down menu

ii. Navigate to the left ide of the page to VPC Dashboard, click on "***Route Tables***" and then "***Create route table***"

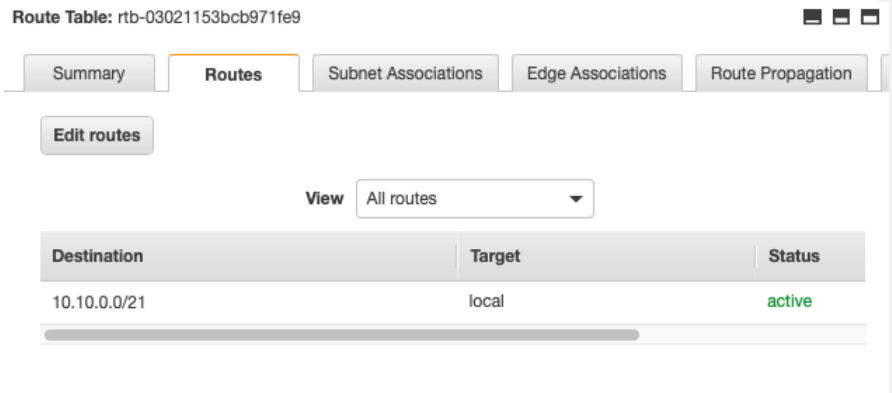
iii. Fill out the "***Name Tag***" and "***VPC***" fields with the necessary information



iv. To create the table, click on "***Create***"

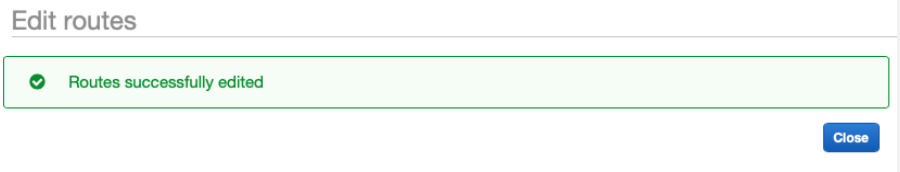
v. To create routes in the Routing Table, click on "***Routes***" and then "***Edit Routes***"

vi. One the "Edit Routes" page add the necessary routing information, including the target network



vii. When all routing information is entered, click on "***Save routes***" to compete the routing entry

viii. Confirmation message with appear confirming the successful or unsuccessful entry attempt



Part 3 – Configuration: Route Tables

The virtual instances created within AWS are stand-alone and require internal routing configuration to interconnect with other instances within the private network. A route table holds routing information which creates the interconnectivity among the privately connected instances.

Cloudlogics has created two route tables, public – serving as an Internet connection and Remote Desktop Sessions anchoring point and private – serving to interconnect all private instances to the public one. Thus, the private and most vulnerable instances are not exposed to the public internet.

Step 1 – Subnets

Public Subnet

Destination	Target	Status	Propagated
192.168.0.0/24	local	active	No
0.0.0.0/0	igw-03fa92c07aa18d040	active	No

i. Route one - "***Destination***" 192.168.0.0/24 with "***Target***" to "***local***" is configured. This entry acts as a Layer 3 switch and creates interconnectivity between the private and public subnet and virtual instances.

ii. Route two - "***Destination***" 0.0.0.0 with "***Target***" to "***igw-03fa92c07aa18d040***" is configured, which is the default route to the

Internet Gateway. Thus, all traffic originating and destined, to and from the internet uses this routes

Private Subnet

Destination	Target	Status	Propagated
192.168.0.0/24	local	active	No
0.0.0.0/0	nat-0b69b06655769dd54	active	No

i. Route one - "***Destination***" 192.168.0.0/24 with "***Target***" to "***local***" is configured. This entry acts as a Layer 3 switch and creates interconnectivity between the private and public subnet and virtual instances.

ii. Route two - "***Destination***" 0.0.0.0 with "***Target***" to "***nat-0b69b06655769dd54***" is configured, which is the default route to the NAT Gateway.

Step 2 – Network Topology Overview in VPC

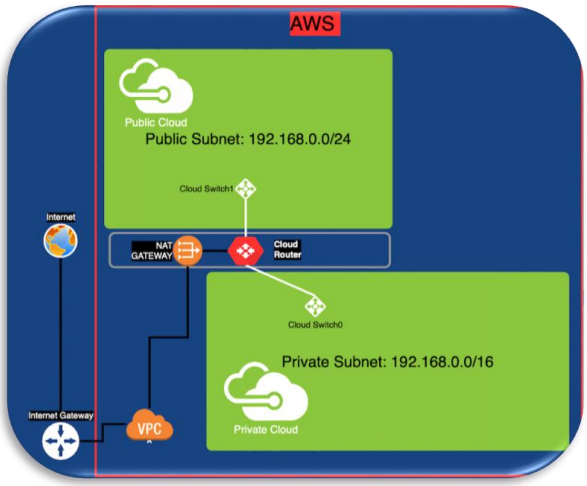


Figure 4 - Network Topology in VPC

Step 3 – AWS Subnets Configuration

Subnets are created to provide interconnectivity amongst private and public instances

i. Navigate to the VPC Dashboard and click on "***Subnets***"

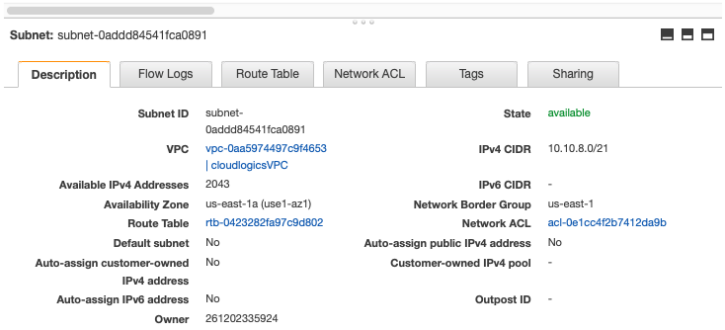
ii. Click on "***Create subnet***" to open the configuration window

iii. On the configuration window fill out the necessary information and click on "***Create***"

iv. Repeat the process for Public and Private subnets

Public Access Subnet

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IP
cl-subnet	subnet-0addd84541fca0891	available	vpc-0aa5974497c9f4653 |...	10.10.8.0/21	2043

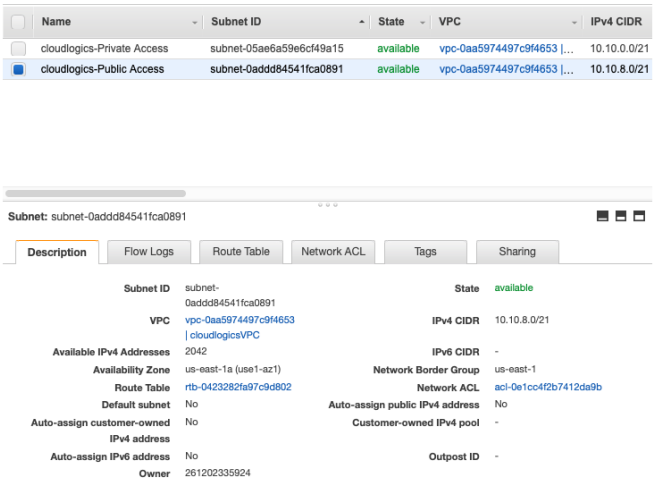


Subnet: subnet-0addd84541fca0891

Description | Flow Logs | Route Table | Network ACL | Tags | Sharing

Subnet ID	subnet-0addd84541fca0891	**State**	available
VPC	vpc-0aa5974497c9f4653 | cloudlogicsVPC	**IPv4 CIDR**	10.10.8.0/21
Available IPv4 Addresses	2043	**IPv6 CIDR**	-
Availability Zone	us-east-1a (use1-az1)	**Network Border Group**	us-east-1
Route Table	rtb-0423282fa97c9d802	**Network ACL**	acl-0e1cc4f2b7412da9b
Default subnet	No	**Auto-assign public IPv4 address**	No
Auto-assign customer-owned IPv4 address	No	**Customer-owned IPv4 pool**	-
Auto-assign IPv6 address	No	**Outpost ID**	-
Owner	261202335924		

Private Access Subnet



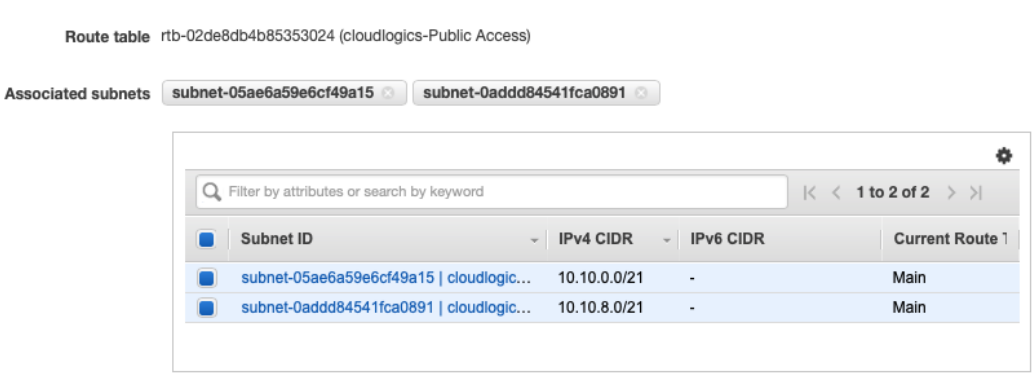
Step 4 – Subnet Association to the AWS Route Table

i. Navigate to the VPC Dashboard page and click on Route Table

ii. Click on "***Subnet Associations***" tab

iii. Click on "***Edit subnet associations***"

iv. Select the subnets created in Step 3 and associate them with the route table



v. Once done click on "***Save***" to save the changes

Part 3 – Security Groups and Security Rules

Step 1 – Security Groups Configuration

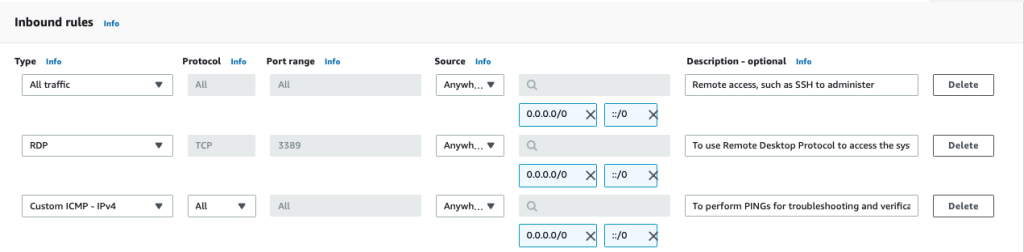
i. From the AWS Management Console home page, navigate to "***Services***" at the top left and open the drop-down menu

ii. From the drop-down menu select "***EC2***" to navigate to the EC2 Dashboard

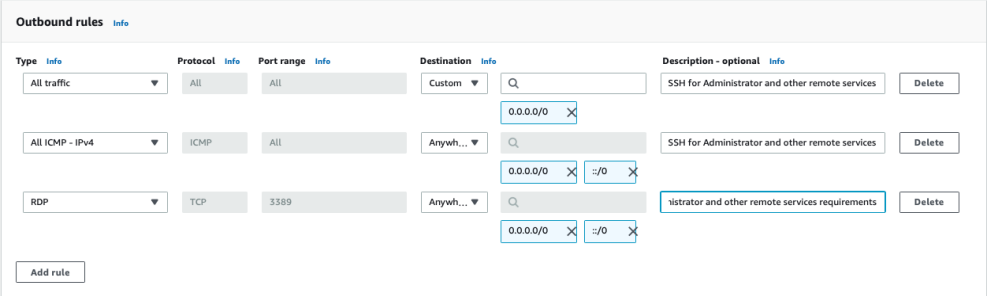
iii. Once on the EC2 Dashboard home page, navigate to "***Security Groups***", click on "***Create Security Group***" and fill out the necessary fields

iv. When the Security Group has been successfully created, the Inbound and Outbound rules are configured

v. Under the Security Group created in the previous step, click on the "***Inbound Rules***" tab and fill in the required information



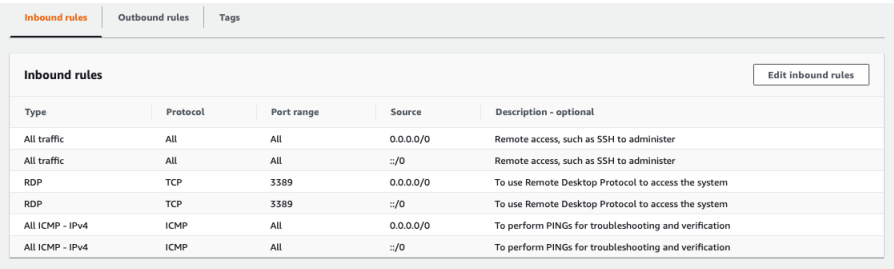
vi. Then click on the "***Outbound Rules***" tab and fill in the required information



vii. Click on the "***Create***" button to finalize the Security Group configuration

Security Group and Rules Configuration

Inbound Rules

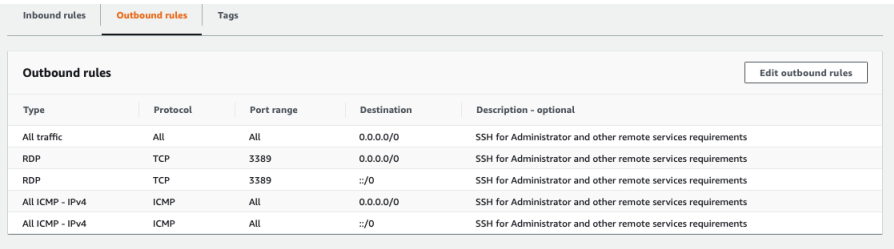


Inbound rules | Outbound rules | Tags

Inbound rules — Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
All traffic	All	All	0.0.0.0/0	Remote access, such as SSH to administer
All traffic	All	All	::/0	Remote access, such as SSH to administer
RDP	TCP	3389	0.0.0.0/0	To use Remote Desktop Protocol to access the system
RDP	TCP	3389	::/0	To use Remote Desktop Protocol to access the system
All ICMP - IPv4	ICMP	All	0.0.0.0/0	To perform PINGs for troubleshooting and verification
All ICMP - IPv4	ICMP	All	::/0	To perform PINGs for troubleshooting and verification

Outbound Rules



Inbound rules | Outbound rules | Tags

Outbound rules — Edit outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	0.0.0.0/0	SSH for Administrator and other remote services requirements
RDP	TCP	3389	0.0.0.0/0	SSH for Administrator and other remote services requirements
RDP	TCP	3389	::/0	SSH for Administrator and other remote services requirements
All ICMP - IPv4	ICMP	All	0.0.0.0/0	SSH for Administrator and other remote services requirements
All ICMP - IPv4	ICMP	All	::/0	SSH for Administrator and other remote services requirements

Step 2 – Security Pair Configuration

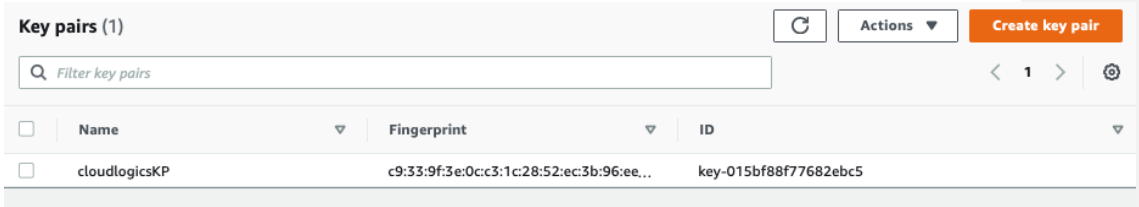
AWS utilizes a security pair key with uniquely associated with each virtual instance and it is used to decrypt and retrieve the Administrator's password to access the instance

i. From the AWS Management Console home page, click on the "***Services***" drop-down menu at the top left corner of the page

ii. From the drop-down menu, select "***EC2***" and then click on "***Key Pairs***"

iii. Click on "***Create Key Pair***" button to start the process

iv. In the "***Key pair name***" fill in the necessary information and click "***Create***" button to finish the process



v. The key pair has been created and can be downloaded from the AWS website

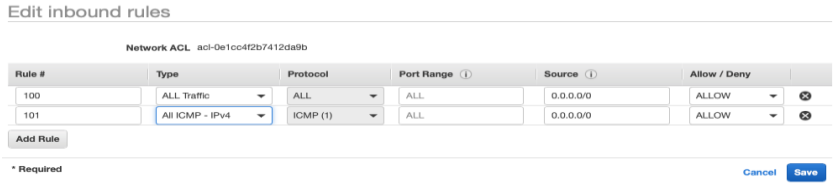
Configuring Network ACLs

i. From the AWS Management Console home page, navigate to "***Services***" at the top left corner and open the drop-down menu

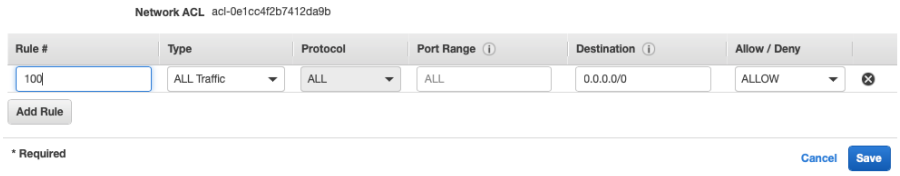
ii. From the drop-down menu select "***VPC***" to navigate to the VPC Dashboard page

iii. Navigate to "***Network ACLs***" and select the ACL to edit

iv. Click on "***Inbound Rules***" tab to make changes



v. When completed with "***Inbound Rules***" click on "***Outbound Rules***" tab right next



vi. When all configurations changes have been made, click on "***Save***" to finish

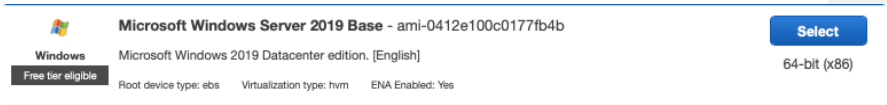
Part 4 – EC2 Instances Configuration

i. From the AWS Management Console home page, navigate to "***Services***" at the top left corner of the page and open the drop-down menu

ii. From the drop-down menu select "***EC2***" and then navigate to "***Instances***"

iii. On the Instances page, click on "***Launch Instance***" to begin the creation process

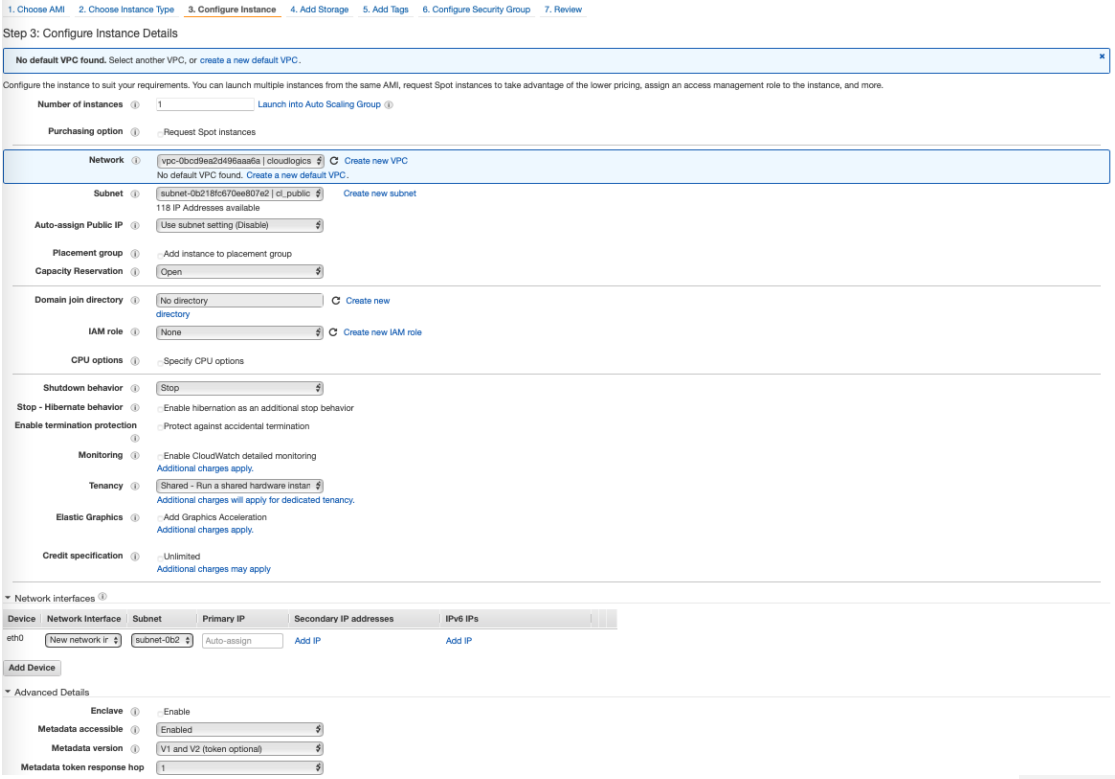
iv. On "***Step 1: Choose an Amazon Machine Image (AMI)"*** page, select the "***Microsoft Windows Server 2019 Base***" and click on the "***Select***" button to create an instance under the selected OS



v. On "***Step 2: Choose an Instance Type***" select the desired instance type in regards to the computing power required

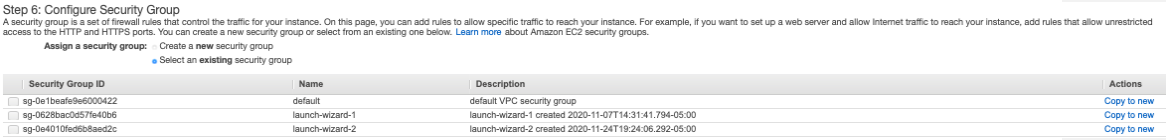
vi. Click "***Next: Configure Instance Details***"

vii. On " ***Configure Instance Details***" page, make the desired selections and fill in the necessary information about the instance



viii. Click on "***Next: Add Storage***", no settings need to be changed here, leave default and click on "***Next: Add Tags***", then "***Next Configure Security Group***"

ix. On the Security Group page, selected the desired security group from the ones created earlier to match the security requirements for the instance



x. Once the Security Group is selected, click on "***Review and Launch***" to review the settings for the instance and launch it

xi. Upon successful instance launch, a notification window appears requesting a security key pair to be associate with the instance.

xii. Select the existing key option and choose the key pair created earlier.

xiii. The instance has been launched, security key pair selected, and the machine instance is preparing for operation

Step 2 – Configuration: Instances

Instance Tag	IP Address Assigned	Subnet Type	Details
File Server	192.168.0.199	Private	Server for hosting company's files
Cloudlogics_Public	Private:192.168.0.12 Public: 3.239.65.53	Public/ Private	Connection server to access the private subnet
Domain Controller	192.168.0.160	Private	DHCP, DNS, and Domain Controller services
WAMP Server	Private: 192.168.0.87 Public: 34.200.250.205	Public/ Private	Server to host the company's website

Application Server	192.168.0.63	Private	Server for hosting in-house developed application and third-party applications that require hosting
Database Server	192.168.0.122	Private	Server to host various databases the company maintains
Ubuntu Server	Private: 192.168.0.39 Public: 3.237.173.30	Public/ Private	Server to host VPN

Table 2 - Instance Configurations

Connecting to Virtual Instances via RDP

Connecting to the instances is possible only if they are connected to a public internet network with a Global Unique IP address. The server instances located on the private subnets do not have access to the public domain. Thus, a RDP connection is established with the "***cloudlogics_Public***" server first and a second RDP connection from the publicly visible server to the desired server on the private subnet.

- From the AWS Management Console navigate "***Services***" and click on the drop-down menu
- From the drop-down menu, under "**EC2**", selected "***Instance***s"
- Place a check mark by the instance to be launched and click on "Connect"

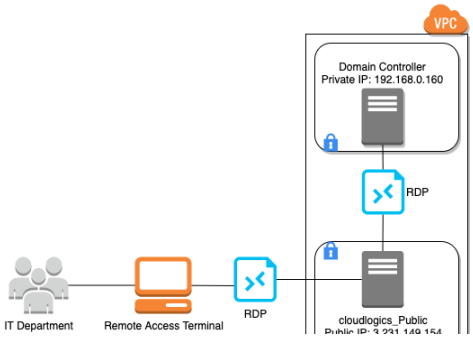
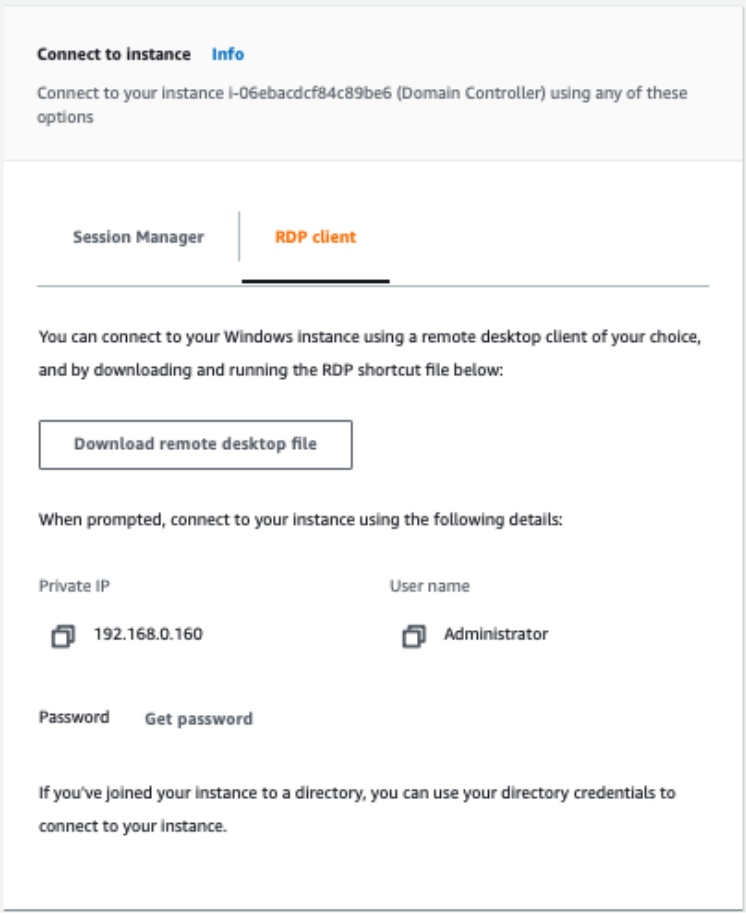


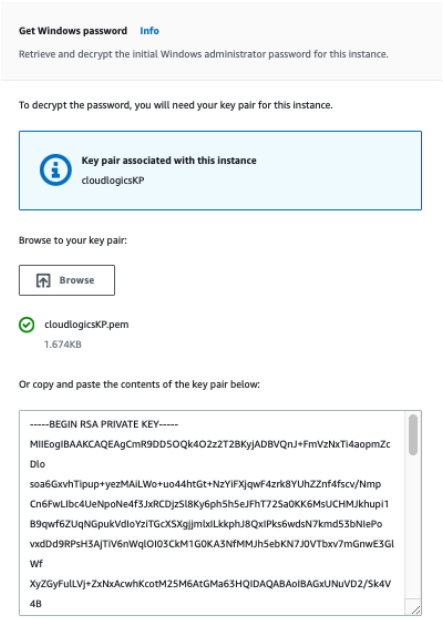
Figure 5- RDP Connection

☐	WAMP Server	i-0fe6f9f837af3f2a1		t2.micro	–	No alarms +	us-east-1a	–
☑	Application Server	i-027b0563f39d657a2		t2.micro	–	No alarms +	us-east-1a	–
☐	Database Server	i-01bd6355df41717d7		t2.micro	–	No alarms +	us-east-1a	–
☐	Ubuntu Server - ...	i-087dd576ec1d50860		t2.micro	–	No alarms +	us-east-1a	–

- The "Connect to instance" page appears providing two options to remotely connect to the instance

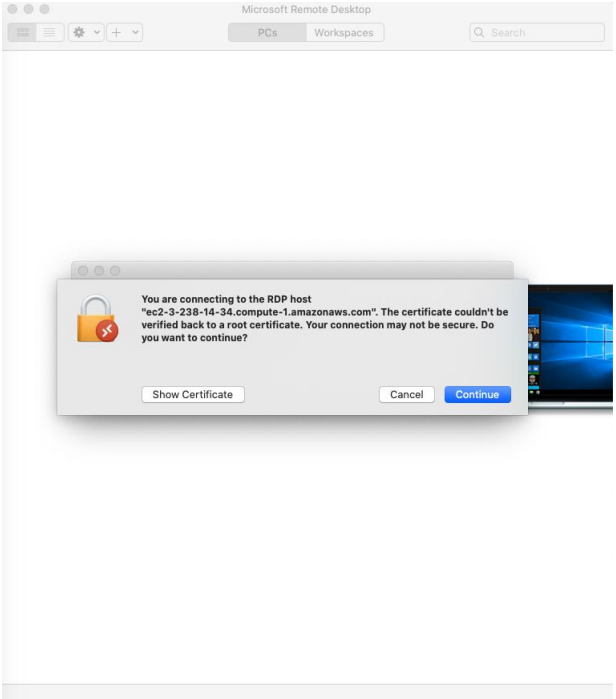


- Select "***RDP client***", username is provided. To retrieve the password, click "Get Password", navigate to the folder that contains the .PEM key created earlier and open it

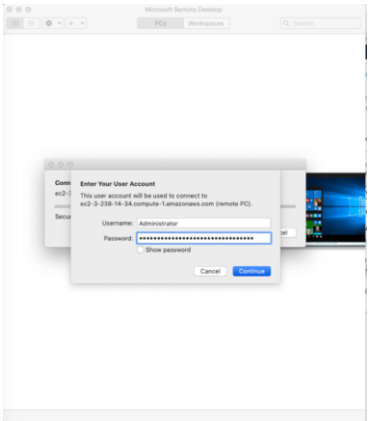


- To reveal the password, click on “Decrypt Password”

- The password is decrypted and connection to the instance can be made
- Navigate to “***Download Remote Desktop File***” and open it



- RDP window appears requesting for a remote desktop connection to be established
- Populate the username and password field with instance's credentials



- If correct settings are applied the connection is established and the virtual instance's desktop appears

Step 3 – Elastic IP

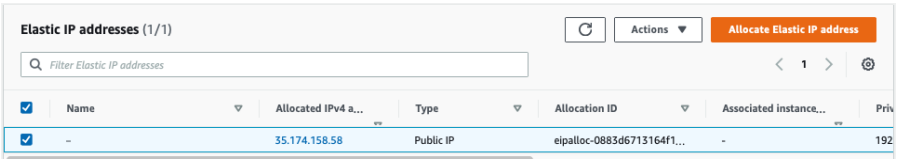
Elastic IP is utilized for creating and configuring NAT Gateways and provides a statis public IP to virtual instances. AWS provides Elastic IPs for a fee.

i. From the AWS Management Console navigate to "***Services***" and click to open the drop-down menu

ii. Navigate and click on "***VPC***" to open the VPC Dashboard and click on "***Elastic IP***""

iii. Click on "***Allocate new address***" to obtain the elastic IP;

iv. In the "***Allocate new address***" window, select "***Amazon Pool for IPv4 address pool***" and click allocate. Elastic IP is now reserved



v. Click on “Finish” to complete the process

Step 4 – Assigning Elastic IP

i. Navigate to the Elastic IP we created earlier
ii. Click on “***Actions***” and open the drop-down menu and click on “***Associate Address***”
iii. On the “***Associate Address***” page, fill in all necessary information and click on “***Associate***”
iv. The Elastic IP addresses now associated with the corresponding instance

Step 5 – Creating a NAT Gateway

NAT Gateway provides internet access to machines located on the Private Subnet and are only associated with a private IP

- From the AWS Management Console home page navigate to the top left corner and click on “***Services***” to open the drop-down menu
- From the drop-down menu select “***VPC***” and navigate to “***NAT Gateways***”
- Click on “***Create NAT Gateway***” to open the configuration page
- Select the subnet that is required to be associated with the NAT Gateway, select the Elastic IP created earlier and click on “Create a NAT Gateway” to complete the configuration

Step 6 – IAM Account

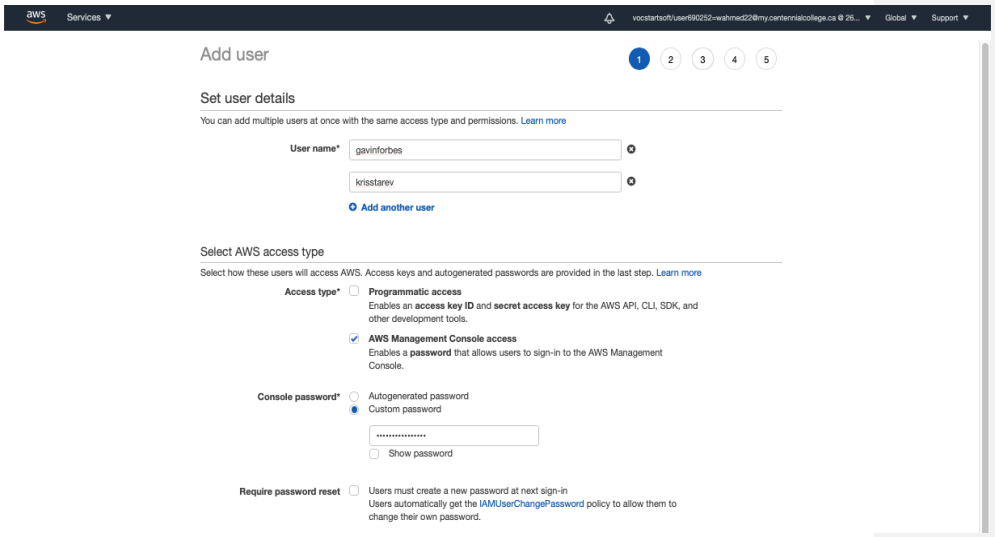
IAM account provides restricted access to other authorized personnel to access and configure the AWS infrastructure. It’s excellent way to allow continued AWS

management and maintenance without the danger of unexperienced and unskilled personal making detrimental configuration errors.

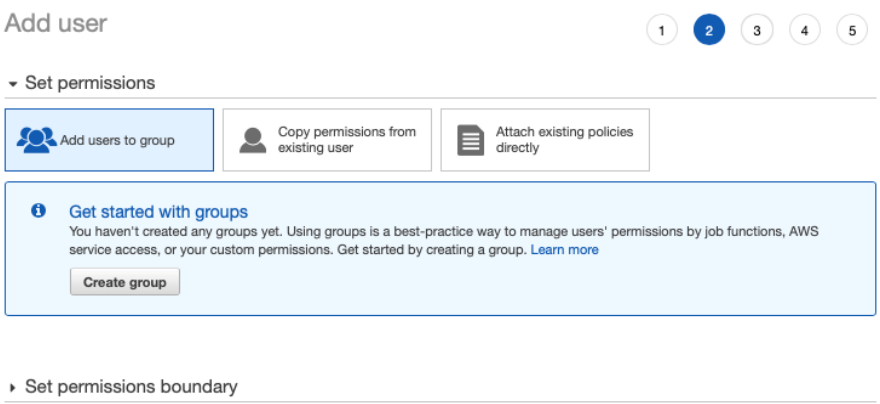
i. From the AWS Management Console home page navigate to the top right corner and click on "***Services***" to open the drop-down menu

ii. From the drop-down menu select "***IAM***" and click on "***Add User***", the "***Add User***" page appears

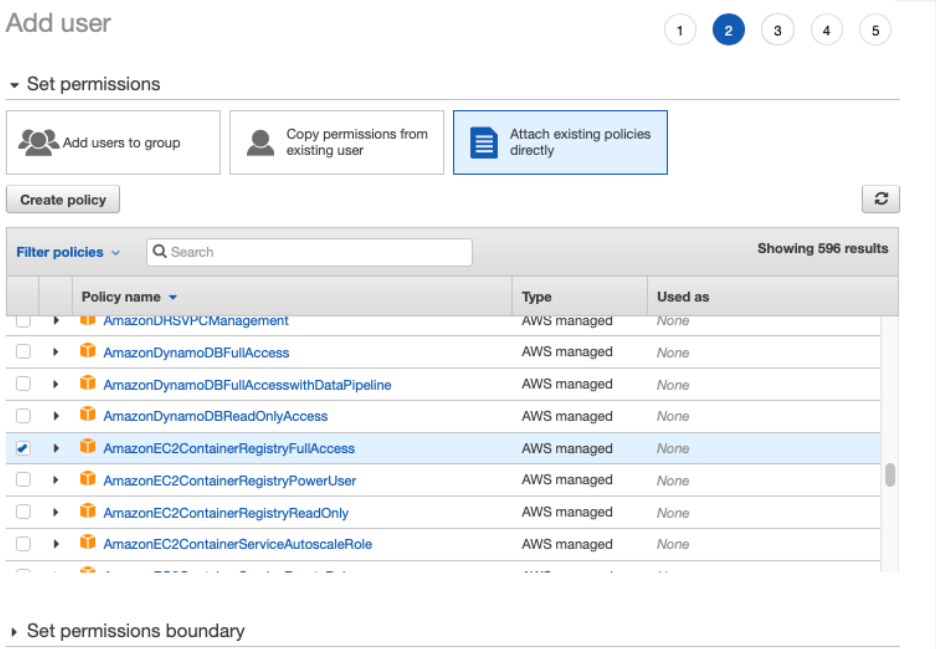
iii. Fill in the required information, such as username, AWS access level and select "***Next: Permissions***"



iv. On the "***Set Permissions***" page the user being created can be assigned to a new or existing permissions group, copy an existing user's permission level or attach the IAM user to an existing policy.

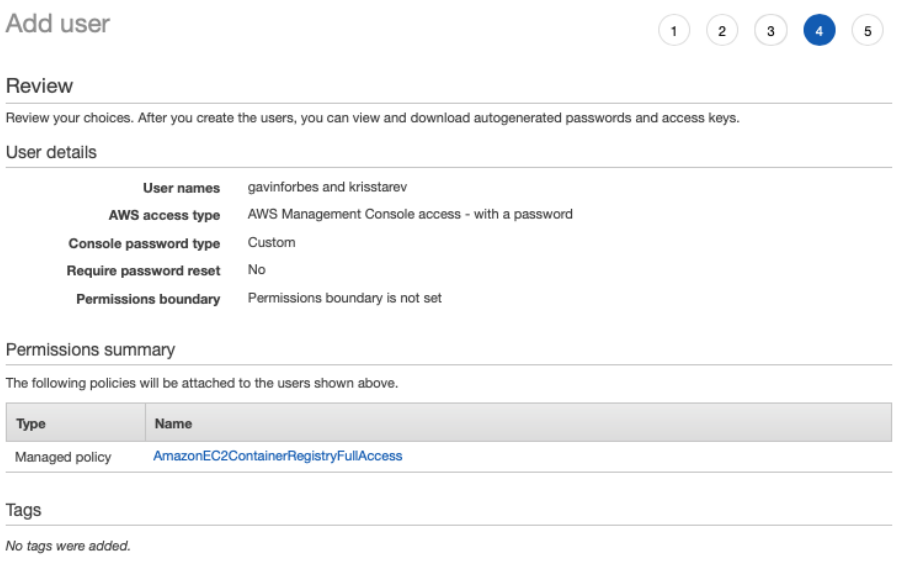


v. To ensure high level of security, select "***Attach existing policies directly***", select the policy that best matches the new user's level of access and click on "***Next: Tags***"



vi. On the "***Tags***" page leave everything as is and click on "***Next: Review***"

vii. On the "***Review***" review all data is correct



viii. If all is correct on the "***Review***" page, click on "***Create user***" to finalize the process. The newly created IAM account appear in the IAM users page

ix. The username and password can now be used to login into the AWS Management Console with the limitation set out by the policy

NETWORK INFRASTRUCTURE

Topology

IP Addressing Scheme

VLAN	Network Address	Subnet	Available Addresses
10	192.168.0.0	255.255.252.0	1022
20	192.168.4.0	255.255.255.128	126
30	192.168.4.128	255.255.255.192	62
40	192.168.4.192	255.255.255.192	62
50	192.168.11.0	255.255.255.0	256
60	192.168.5.32	255.255.255.224	30
70	192.168.5.64	255.255.255.224	30
80	192.168.5.96	255.255.255.224	30
90	192.168.5.128	255.255.255.248	6

Table 3 - IP Addressing Scheme

Network Management Tools

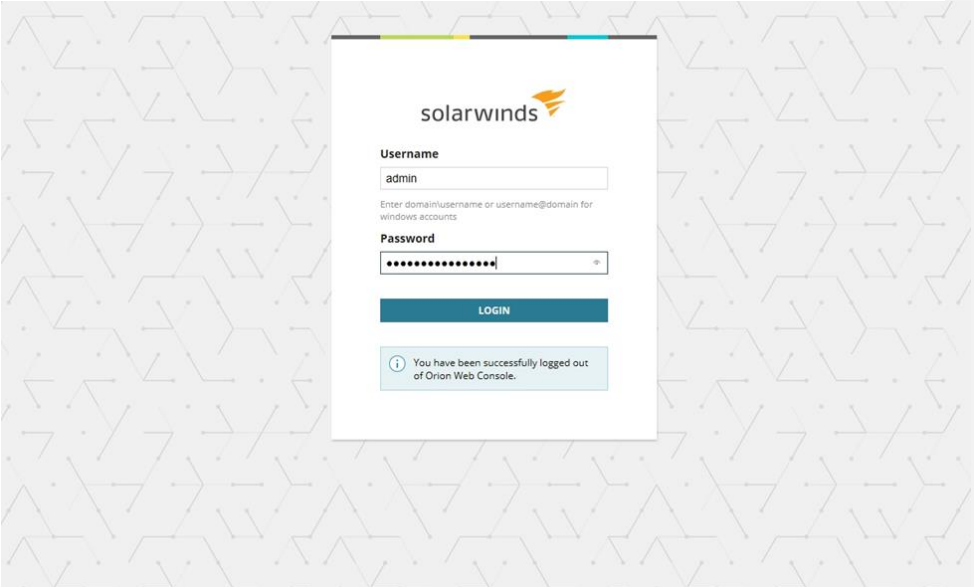
SOLARWINDS NETWORK MANAGEMENT

Our network security strategy includes the deployment of the SolarWinds Network Management Platform. SolarWinds is an industry leader in the management platforms with powerful tools to monitor network performance and security metric. The SolarWinds Network Performance Monitor will use the Simple Network Management Protocol (SNMP) to poll all the devices on the CAMH network including workstations. We believe implementing this system, while expensive, will provide significant value to the clients heightened security needs. SolarWinds is priced according the number of nodes on the network, all devices from servers to laptops. As the CAMH network will have less than 2000 nodes, the per year cost of the software license is $19,345, which

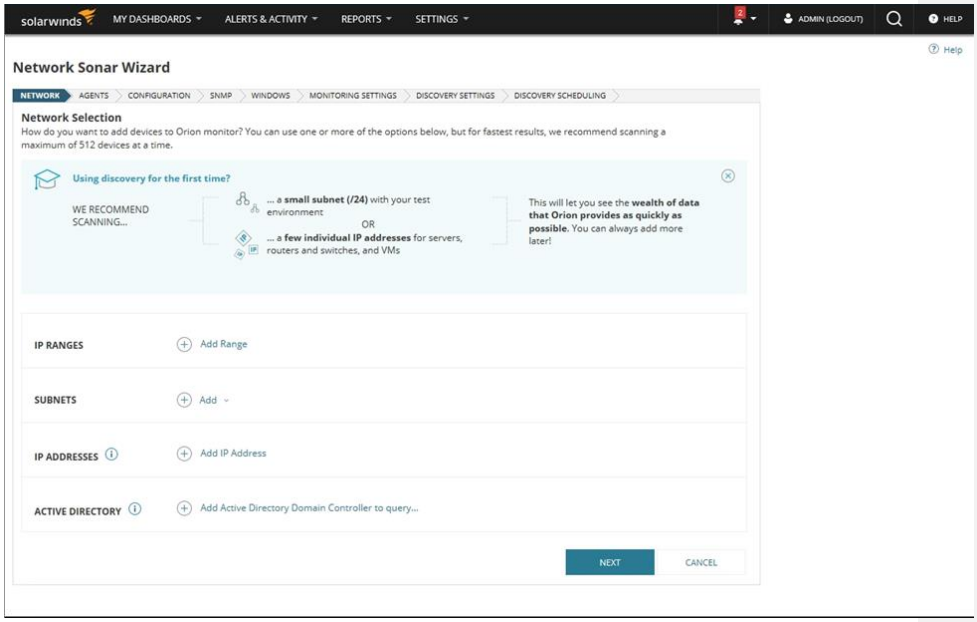
also includes support services available 24/7. SolarWinds should free up resources for the IT department to respond quickly to network problems, as they will have a powerful tool to help monitor the network.

SolarWinds Installation

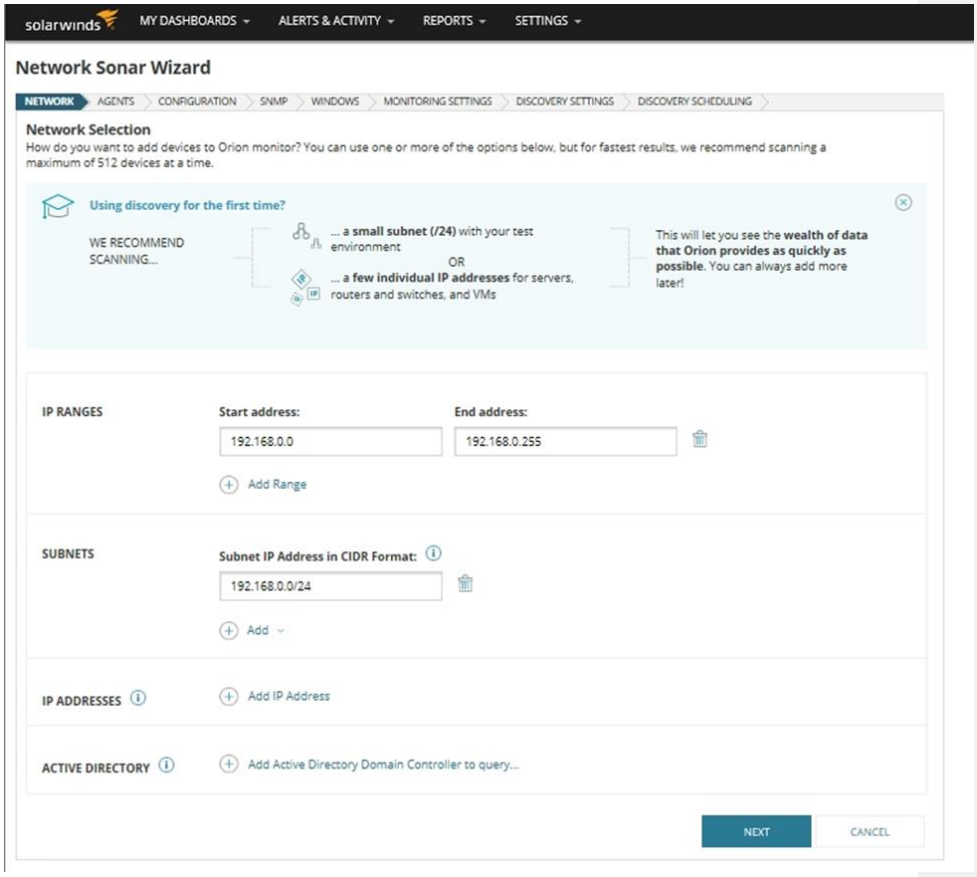
i. Download the software from the SolarWinds site. After installing on a dedicated CAMH server, you are prompted to choose an administrator username and password.



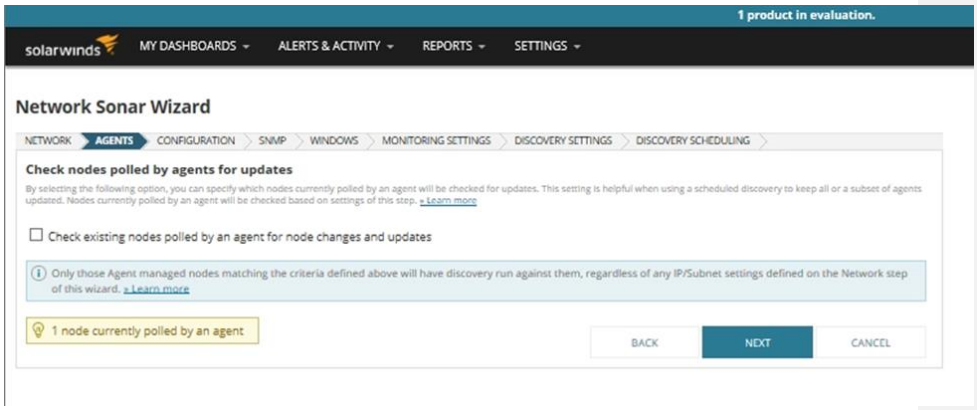
ii. Next, we use the set-up wizard to choose the subnets will be monitored by the SolarWinds



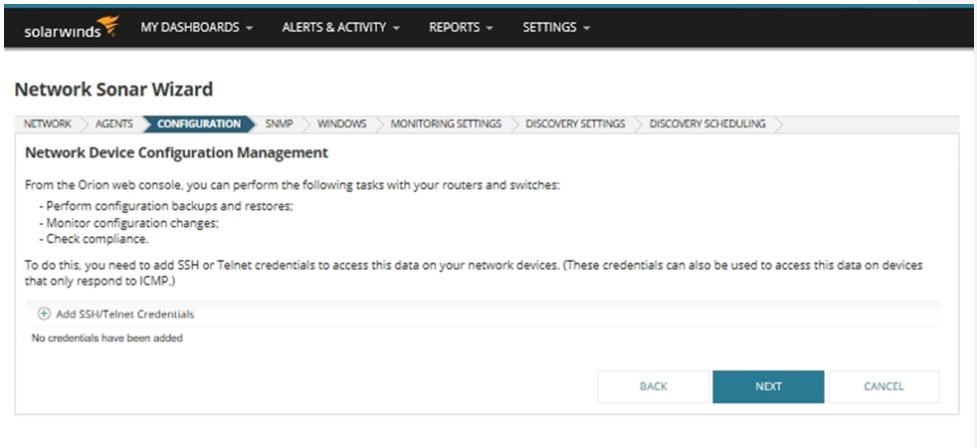
iii. For the purposes of this report, we will include a smaller IP range as there are limitations on the number of nodes that can monitored on the free trial version. We have selected the IP range 192.168.0.0 - 192.168.0.255, with a 192.168.0.0/24 subnet.



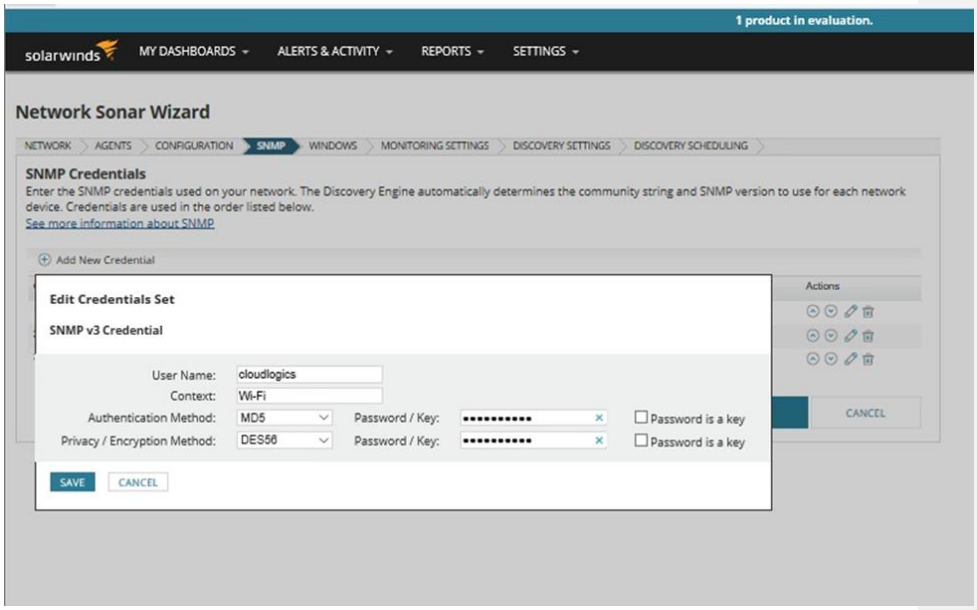
iv. The setup wizard then checks for nodes to be polled by the agents for updates



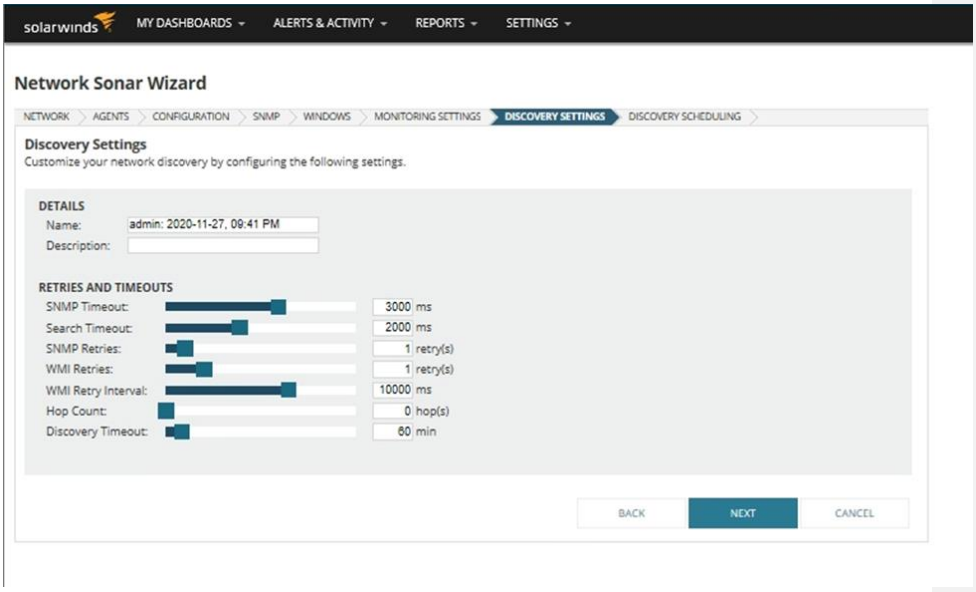
v. Next enter SSH/Telnet credentials to allow you to remotely configure devices from the Dashboard.



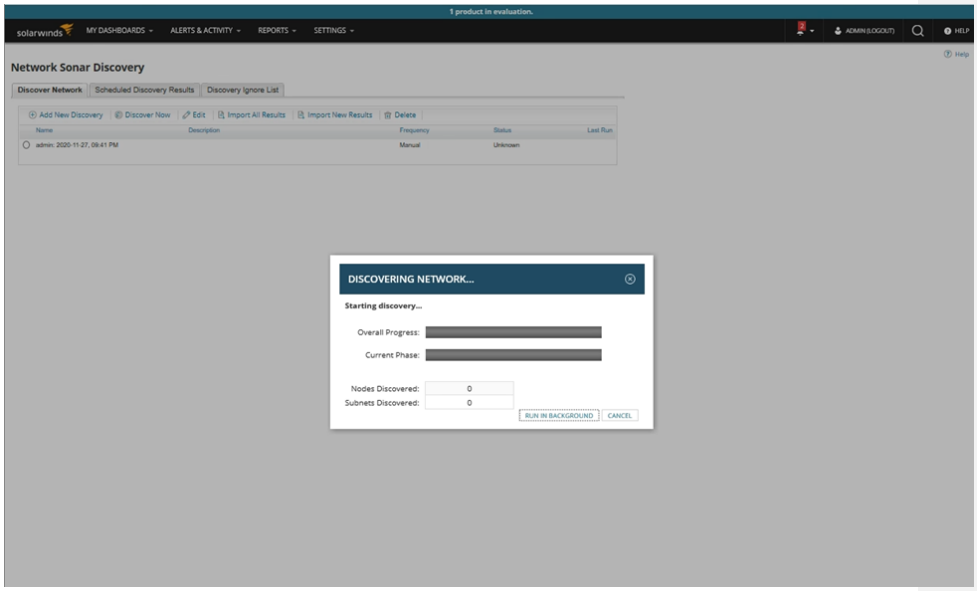
vi. Now the wizard checks SNMP credentials used on the CAMH network



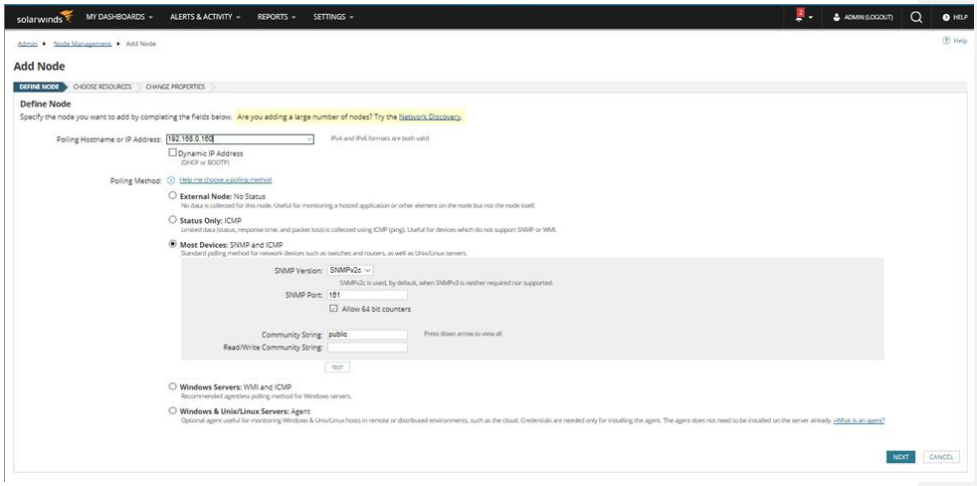
vii. The network discovery can be customized and fine-tune the process according to our requirements



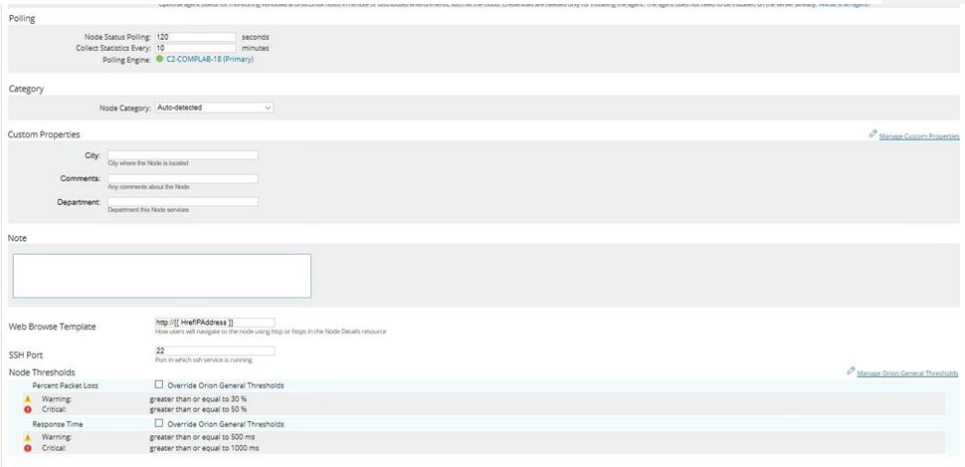
viii. After this step SolarWinds begins the network discovery process



ix. We can now add nodes and select the polling method of our choice. For CAMH we select ‘Most Devices’



x. In the final setup step, we configure the polling times for our network nodes. We have chosen to poll nodes status every 120 seconds and to collect every node statistic every 10 minutes



Network Configuration

ON-SITE WIRELESS

Wireless Security Analysis

Client Wireless Security Needs

- Enhanced security measures to protect health records
- Privacy of patients with stigmatizing metal health and addiction issues.
- No unsecured, unauthenticated guest network, creating network security holes.
- Prevention of patients gaining access to wireless networks

As CAMH treats medical patients primarily for mental health and addiction issues, security was a point of emphasis when designing their network strategy. These health issues carry significant stigma for those suffering from them and as such there is a heightened need for privacy for these patients. Another security concern for CAMH was the physical security of the patients and the need to protect them, in some cases from themselves. This hospital is a secure facility that does not permit patients to use cellphone or their own personal electronic devices. This led to the decision to not implement a Guest Wi-Fi service for their on-site network. Guest Wi-Fi requiring giving passwords to a large pool of individuals, which could easily be learned by patients. This would encourage some patients to sneak devices into the facility and to be able to contact individuals who do not act in their best interests. In order to provide data security, we have designed a wireless network using a Cisco 2504. Wireless Controller and a RADIUS server for authentication. The Wireless Controller will add increased security

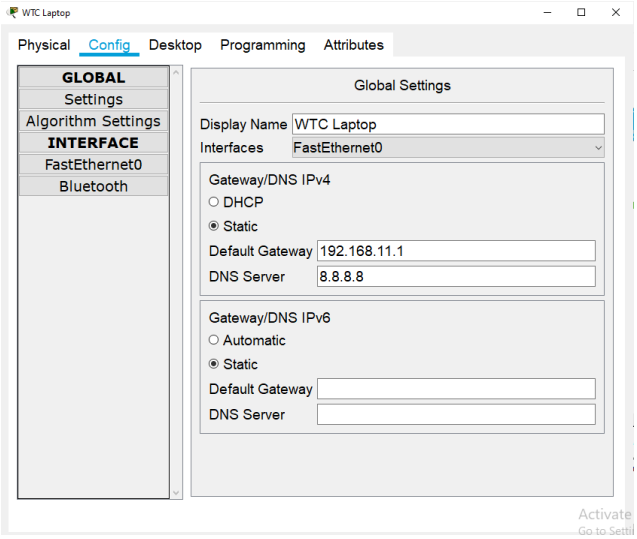
and improve performance of the wireless network by providing a platform to monitor the wireless access points. The Cisco 2504 controller has the ability to search the wireless network for Rouge AP's and identify them before they gain access to the network. This controller uses CAPWAP (Control and Provisioning Wireless Access Points) protocol to be able to manage an array or lightweight wireless access points. The wireless access points send out discovery messages to search for a controller. The two devices are then connected by a securely using the Datagram Transport Layer Security (DTLS) protocol (fieldengineer.com). The information passed between the devices will allow CAMH's IT department view information being sent across the wireless network and identify who which users are connected.

To further enhance the wireless network, we have decided to implement a RADIUS server to authenticate users on the network. In a production environment a RADIUS server can pull users authentication details from the Active Directory services of the domain controller. This means passwords don't need to be sent or given to users on the wireless network. The user would sign in with their previously configured domain passwords. The RADIUS server matches the credentials being used to access the wireless network to the ones stored in Active Directory. The result is we will be able to better protect the network from hackers by not exposing the SSID and passwords used in open Wi-Fi networks. Credentials will be able to control and managed via group policies to ensure adherence domain password rules. For example, a group policy could force users to change their password every six weeks, which would be pass through to the wireless users. RADIUS servers in real time environments can use per-user VLAN tagging, to

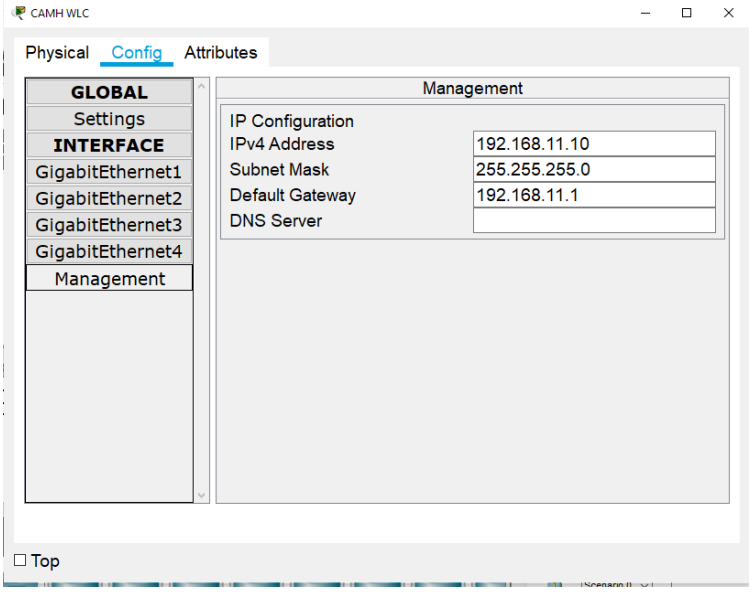
further segregate access to sensitive information from other departments that don't require access (Keller, August 2020).

ON-SITE WIRELESS SETUP

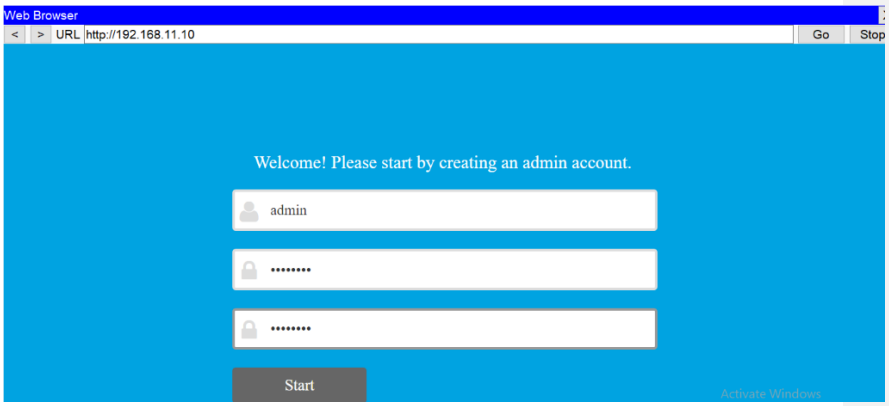
Wireless Controller Configuration



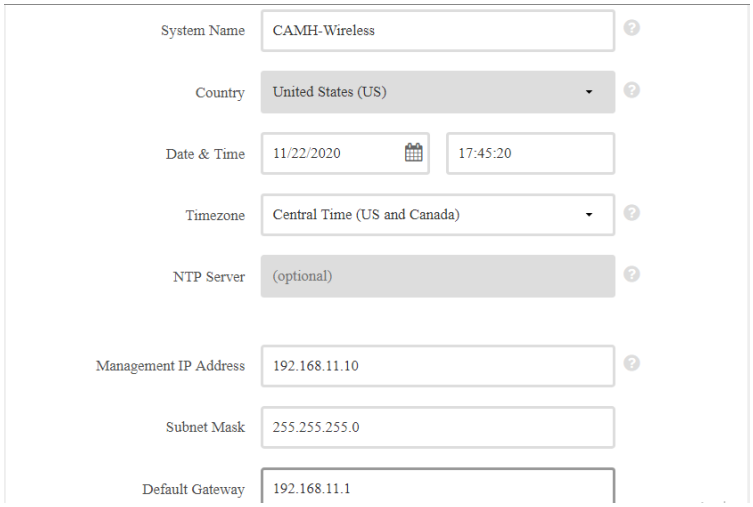
i. Attach a PC to the WLC via an Ethernet cable and configure both devices with IP addresses on the same network/subnet.



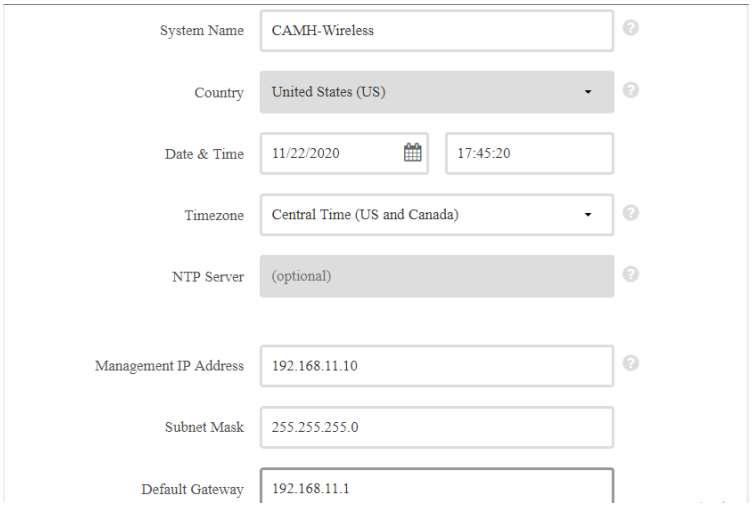
ii. Log into the WLC via a web browser and create an administration ID and password



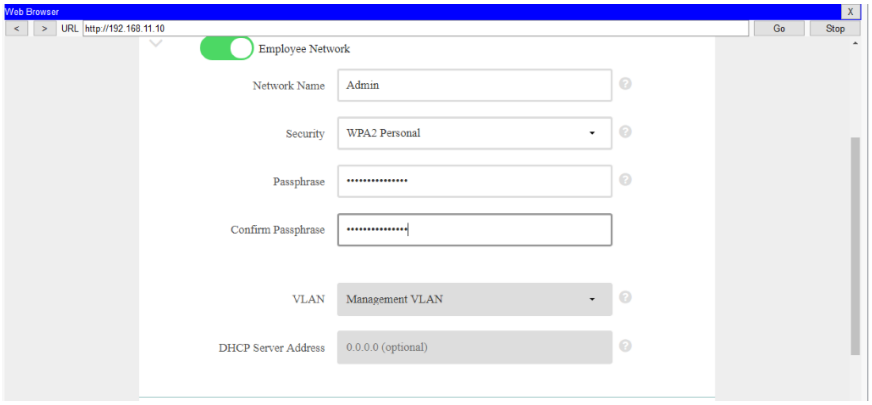
iii. Setup WLC Management IP address configurations with the correct network mask, then select Next



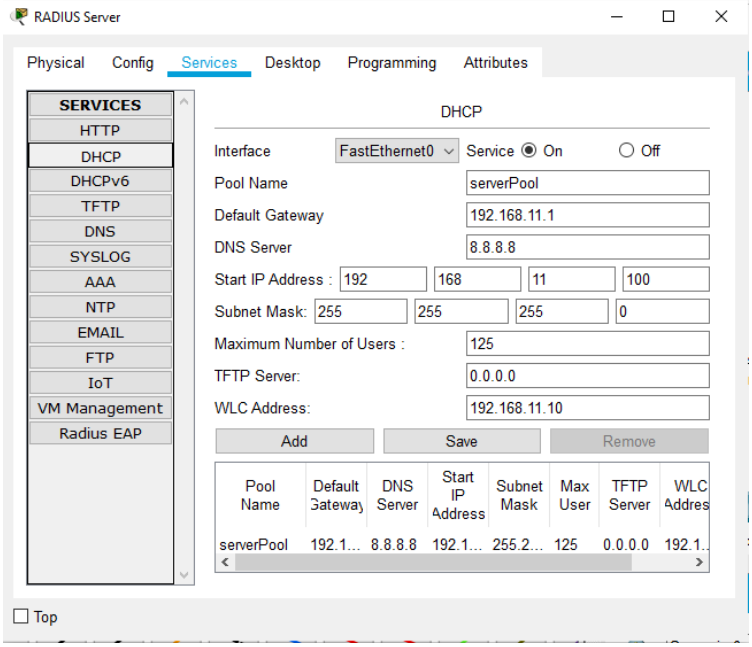
iv. Setup WLC Management IP address configurations with the correct network mask, then select Next



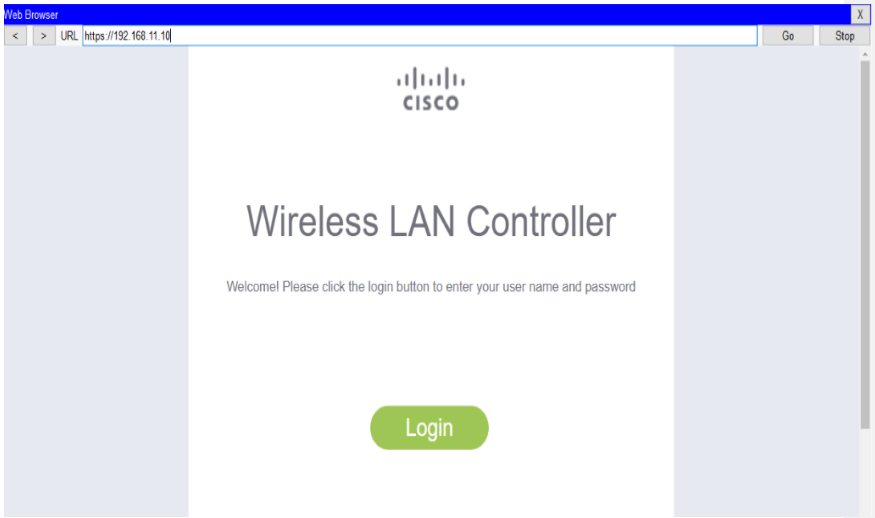
v. Setup wireless network SSID, WPA2 password. Then click ‘Next’, then ‘Next’ again and then select ‘Apply’ to save the configurations.



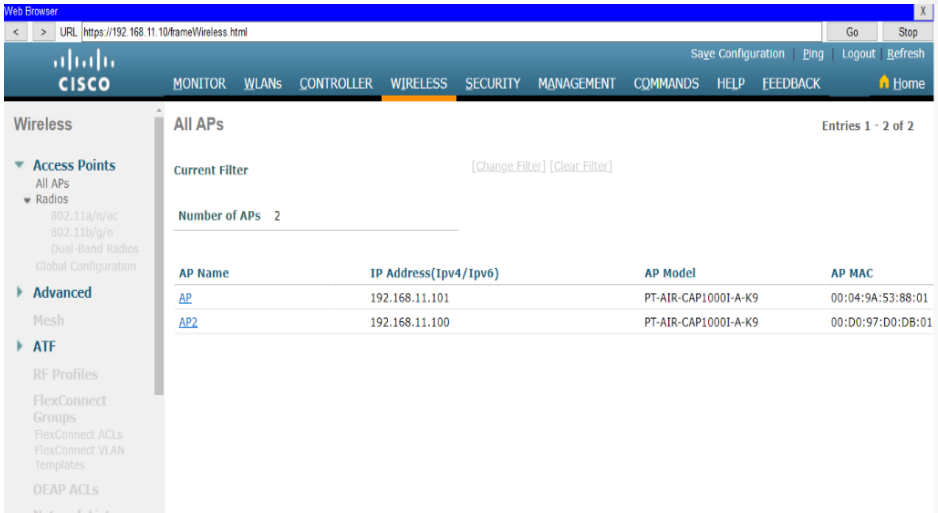
We then need to configure DHCP settings for the network on the RADIUS server. Here we select the maximum numbers of wireless users that can access the network at one time. Once we save the settings our lightweight access points will have receive DHCP addresses to gain connectivity with the network.



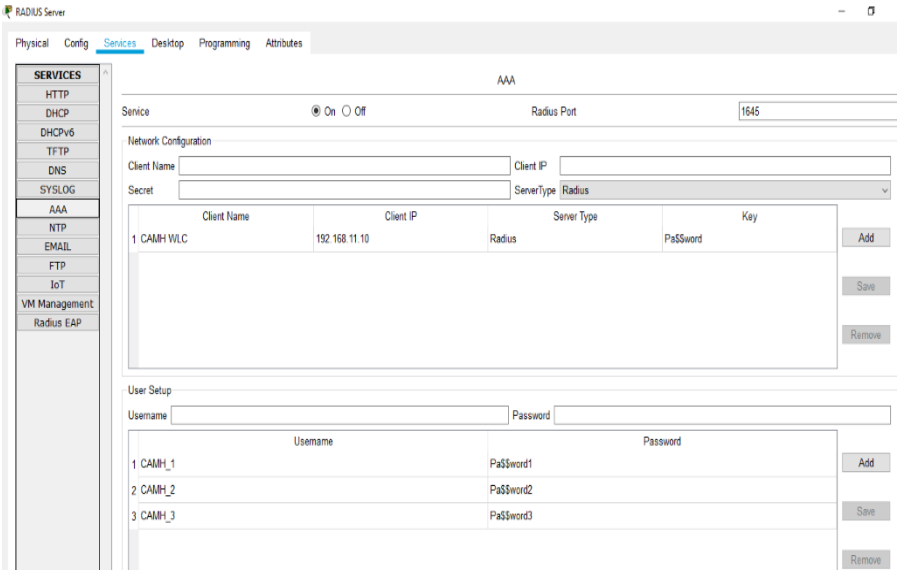
Now that the Cisco 2504 WLC has been configured with an administration ID, we need log back in HTTPS, instead of the unsecure HTTP connection we initially used to configure the device.



Now the on-site network administrator can select the ‘Wireless’ tab in the main dashboard and see wireless access points under management of the WLC. From this screen the administrator can also see the MAC address, the uptime, the status and the throughput for access point



Now we need to configure AAA authentication on the RADIUS server. To do you select ‘Services’ and ‘AAA’ on the server configuration module. RADIUS requires the WLC IP address, the SSID and password configured on the WLC earlier. You can now add usernames and passwords to give mobile devices access to the network. However, in a normal production environment the RADIUS server would be programmed to pull user credentials from the domain controllers Active Directory records. Unfortunately, due to the limitations of the Packet Tracer software this can only be stated in theory and not practically configured.



Now the configuration of the Cisco 2405 Wireless Controller and the RADIUS server have been completely configured. We can test connectivity of the network by entering the user credentials that we saved on the RADIUS server in the previous step. Go to the interface setting for each of the mobile devices and choose the Wireless interface. The SSID ‘Admin’ needs to be entered and WPA2 selected from the Authentication field. Finally, enter the username (CAMH_1) and password that saved on the RADIUS server.

After completing this step, the mobile devices are able to securely access the CAMH wireless network.

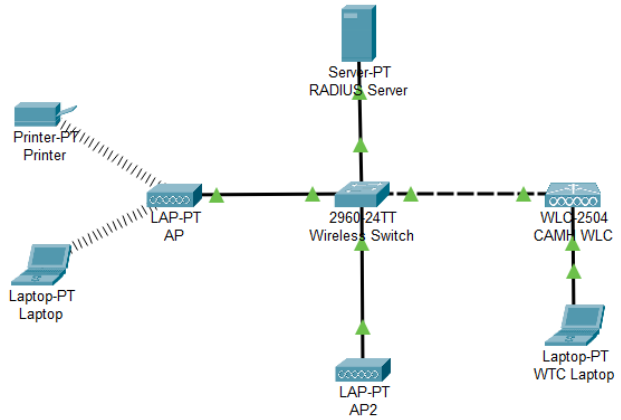
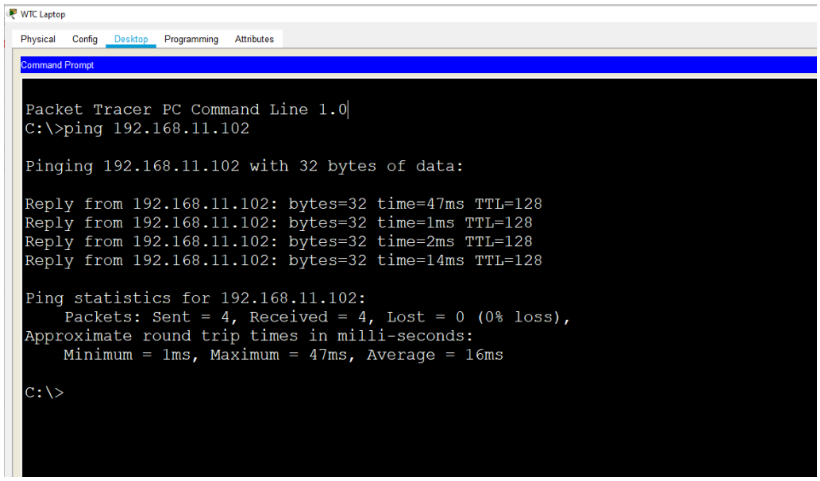


Figure 6 - On-premises Topology

We can now prove end to end connectivity of the secure wireless network by a ping test from the WTC laptop to the wireless laptop



ON-SITE LAN ANALYSIS

Security

Our strategy to secure the CAMH on-site LAN network is a combination of layers of security measures aimed at protecting confidential patient records. For the purpose of this report there are limitations with options to demonstrate network security from the Cisco Packet Tracer platform. In an ideal scenario we would be able to implement a network management software platform as well as enterprise level anti-virus applications to our design.

The first layer of our LAN network security design is the deployment of a Cisco 5505 Adaptive Security Appliance (ASA) firewall.

The Cisco 5505 ASA technical specifications

- Throughput 150 Mb/sec
- Offers IPsec VPN for secure connection
- 8 Ethernet ports, including 2 PoE
- 3 VLANS with no trunking configured, 20 possible with trunking.
- Triple Data Encryption Standard/Advanced Encryption standard (3DES/AES)

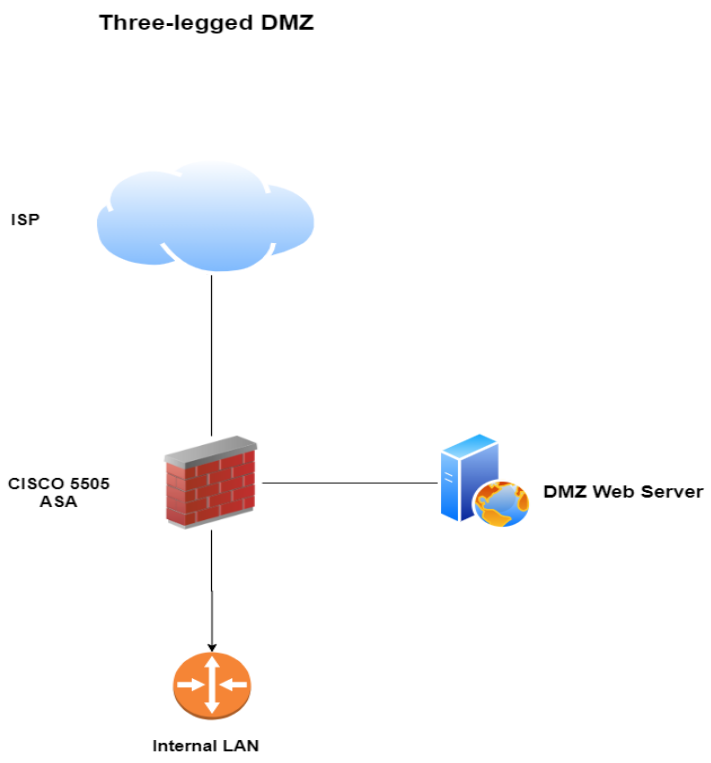


Figure 7 - Three-Legged DMZ

Deploying the ASA will give us the ability to set up a Demilitarized Zone (DMZ) to our LAN design. The DMZ is a zone connected to ASA that allows users to access a CAMH Web Server that is separated from the interior LAN. The purpose of implementing a DMZ in our network design is to secure the private data on the network from unknown hosts looking to access information from the CAMH web services. These hosts that originate from outside the network don't use domain authentication protocols and would pose significant threat to network security if not segregated. We will be implementing a three-legged DMZ model, meaning there will be one firewall with three interfaces. Interface Ethernet 0/0 Ethernet faces into the network, interface Ethernet 0/1 faces outside the network acting as gateway to/from the LAN and interface Ethernet 0/2 faces the DMZ allowing outside access to a CAMH web server. The following diagram illustrates the three-legged DMZ topology.

One limitation of configuring the ASA via Packet Tracer is the inability to manage the device with a Cisco Adaptive Security Device (ASDM). The ASDM provides a user-friendly graphical user interface that provides many easy to configure security features. For our purposes we will completing basic configuration through the command line interface on the ASA.

Cisco 5505 ASA Configuration

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.6.2 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.16.0.2 255.255.0.0
!
interface Vlan3
 no nameif
 security-level 50
 ip address 192.168.10.2 255.255.255.0
!
```

The first step in configuring the ASA is set up three VLANS, one for the inside network, one for the outside network and one for the DMZ. Each VLAN is configured with a 'nameif' command that indicates which part of the network it attaches to. In a three-legged model these are nameif Inside, nameif Outside and nameif DMZ. The ASA sets default 'security-levels' for each zone, 100 indicates a trusted source, while 0 indicates no trust and restricts access. We also configure IP address for each interface.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.6.2 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.16.0.2 255.255.0.0
!
interface Vlan3
 no nameif
 security-level 50
 ip address 192.168.10.2 255.255.255.0
!
```

```
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
```

i. Next, we need to configure Ethernet 0/1 (Outside) and Ethernet (DMZ 0/2 interfaces as a switchport for the appropriate VLAN.

```
!
interface Ethernet0/0
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
```

ii. NAT is now configured on the ASA

```
!
class-map kris
 match default-inspection-traffic
!
policy-map kris2
 class kris
  inspect icmp
!
```

iii. To allow ping tests to validate connectivity a change is needed to allow the ASA to inspect ICMP packets. The Cisco 5505 ASA contains a global policy-map that defines which protocols the ASA it can process. By default, the ASA does not have ICMP traffic in its global policy-map so we need to create a policy-map that will allow it.

```
!
class-map kris
 match default-inspection-traffic
!
policy-map kris2
 class kris
  inspect icmp
!
```

Cisco 2960 Switch configuration

iv. The first step after renaming the hostname for the switch is configuring switchports/trunk for each attached Fast Ethernet port. This will allow us to establish inter-vlan routing after we configure our router.

```
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
CAMH_Switch(config-if)#
CAMH_Switch(config-if)#int fa0/2
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
CAMH_Switch(config-if)#int fa0/3
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
CAMH_Switch(config-if)#int fa0/4
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
CAMH_Switch(config-if)#int fa0/5
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
CAMH_Switch(config-if)#int fa0/6
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
CAMH_Switch(config-if)#int fa0/7
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 70
% Access VLAN does not exist. Creating vlan 70
CAMH_Switch(config-if)#int fa0/8
CAMH_Switch(config-if)#switchport mode access
CAMH_Switch(config-if)#switchport access vlan 80
% Access VLAN does not exist. Creating vlan 80
CAMH_Switch(config-if)#int gi0/1
CAMH_Switch(config-if)#switchport mode trunk
```

v. Port-security will then be added to each switch interface. This is done to allow the switch to match mac addresses with known mac addresses on the VLAN. If correct number of mac addresses are already in the mac address table for the VLAN it will cause the switch to drop the packet.

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode trunk
 switchport port-security maximum 2
 switchport port-security mac-address sticky
!
interface FastEthernet0/6
 switchport access vlan 60
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
```

Cisco 2911 Router Configuration

i. Our router configuration is based on our router on a stick topology implemented for our on-site premises. This topology allows us to separate different types of traffic on different VLANS such as voice and data. In a real-world scenario with a large network this configuration could cause congestion and degrade network performance. This is since all traffic would enter and exit through the same interface port. For our purposes this will not be an issue. The first step in the router configuration is establishing sub-interfaces for each VLAN using dot1q encapsulation and issue the no shut command to the parent interface.

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.252.0
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.4.1 255.255.255.128
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.4.129 255.255.255.192
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.4.193 255.255.255.192
!
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 192.168.11.1 255.255.255.0
!
interface GigabitEthernet0/1.60
 encapsulation dot1Q 60
 ip address 192.168.5.33 255.255.255.224
!
interface GigabitEthernet0/1.70
 encapsulation dot1Q 70
 ip address 192.168.5.65 255.255.255.224
!
interface GigabitEthernet0/1.80
 encapsulation dot1Q 80
 ip address 192.168.5.97 255.255.255.224
!
interface GigabitEthernet0/1.90
 encapsulation dot1Q 90
 ip address 192.168.5.161 255.255.255.224
```

ii. Next, we will configure DHCP services on the router interface directly connected to the switch. This will allow our hosts to gain IP addresses according to their default gateway and group them in their correct segment. Here we established DHCP pools for each of our VLANs except for wireless. Our wireless VLAN will be gaining their DHCP service from the previously configured RADIUS server.

```
!
ip dhcp pool DOCTORS-POOL
 network 192.168.0.0 255.255.252.0
 default-router 192.168.0.1
ip dhcp pool HR-POOL
 network 192.168.4.192 255.255.255.192
 default-router 192.168.4.193
ip dhcp pool IT-POOL
 network 192.168.4.128 255.255.255.192
 default-router 192.168.4.129
ip dhcp pool ADMINISTRATION-POOL
 network 192.168.4.0 255.255.255.128
 default-router 192.168.4.1
ip dhcp pool PRINTERS-POOL
 network 192.168.5.32 255.255.255.224
 default-router 192.168.5.33
ip dhcp pool CUSTOMERSERVICE-POOL
 network 192.168.5.64 255.255.255.224
 default-router 192.168.5.65
ip dhcp pool SECURITY-POOL
 network 192.168.5.96 255.255.255.224
 default-router 192.168.5.97
!
!
```

iii. Once we finish setting up the DHCP service, we will exclude the network address for each VLAN subnet.

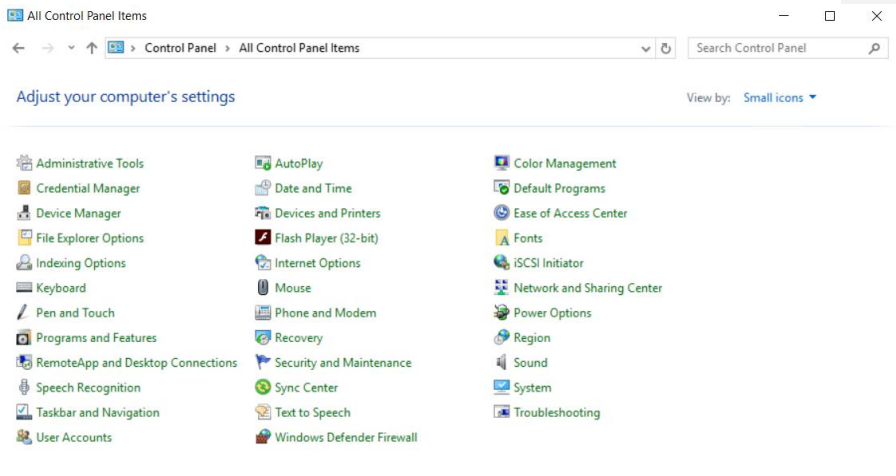
```
!
ip dhcp excluded-address 192.168.0.0
ip dhcp excluded-address 192.168.4.0
ip dhcp excluded-address 192.168.4.128
ip dhcp excluded-address 192.168.4.192
ip dhcp excluded-address 192.168.5.0
ip dhcp excluded-address 192.168.5.32
ip dhcp excluded-address 192.168.5.64
ip dhcp excluded-address 192.168.5.96
!
```

SERVER IMPLEMENTATION

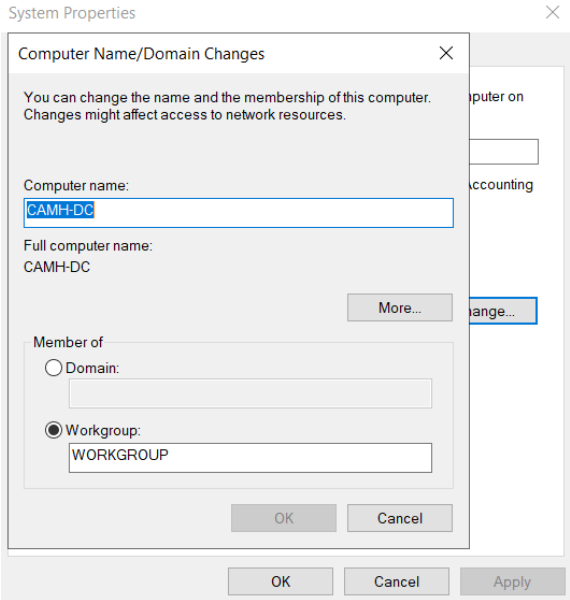
Part 1 – Active Directory Setup

Step 1 – Rename the instance

i. Navigate to the "***Control Panel***" and then "***System***"



ii. Click on "***Computer Name/Domain Changes***", select the "Domain" radio button and enter the desired domain name

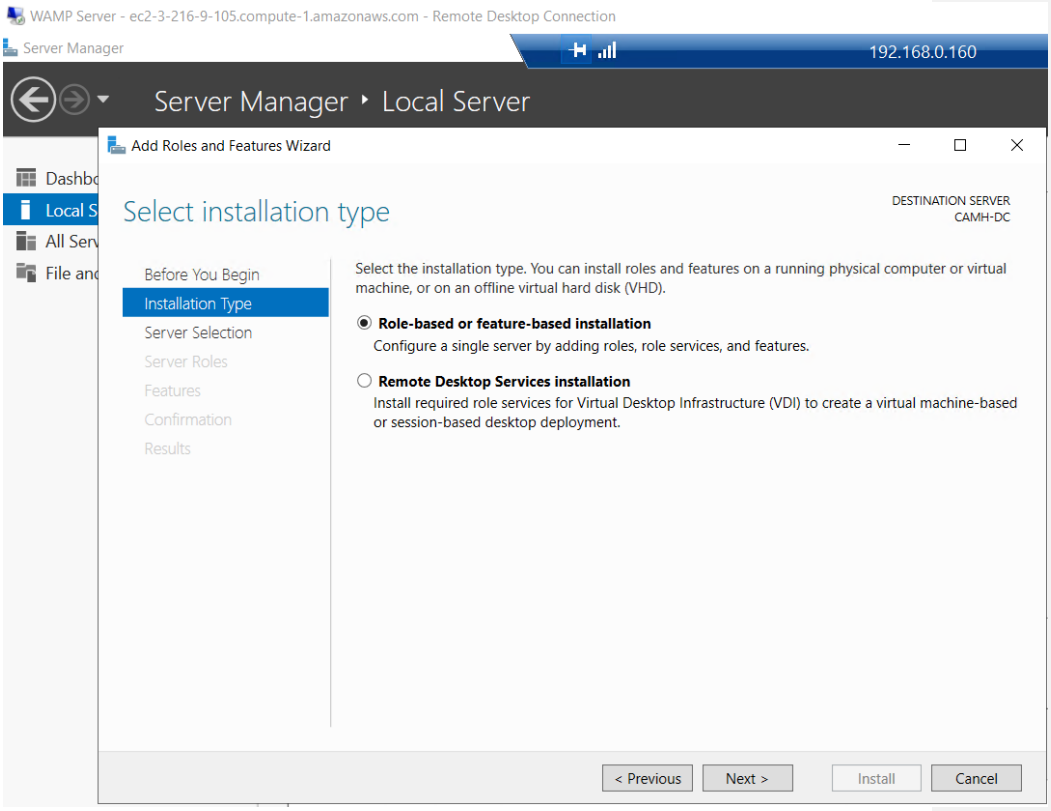


iii. If the domain name is correct and available, a window appears requesting credentials to join the domain

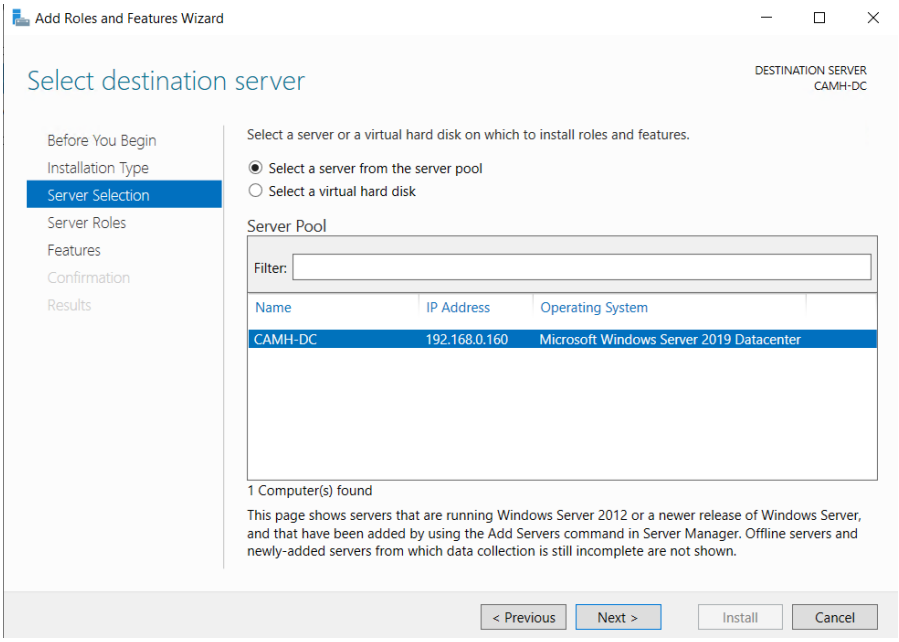
Step 2 – Add Active Directory Domain Service Role

i. From the top right corner of the "***Service Manager***" window click on "***Manage***" and then select "***Add Roles and Features***"

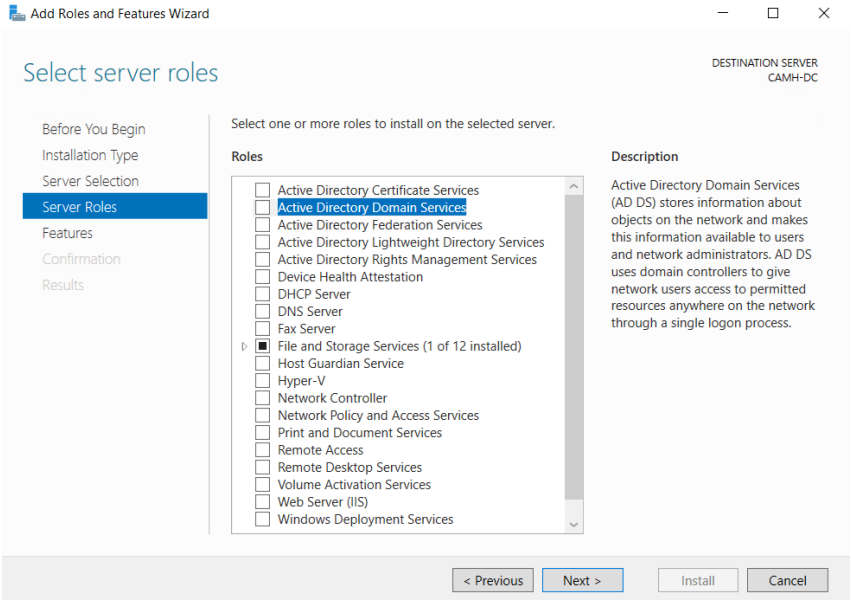
ii. "Add Roles and Features" wizard appears, click next and choose "***Role-Based or Feature-Based installation***" and click next



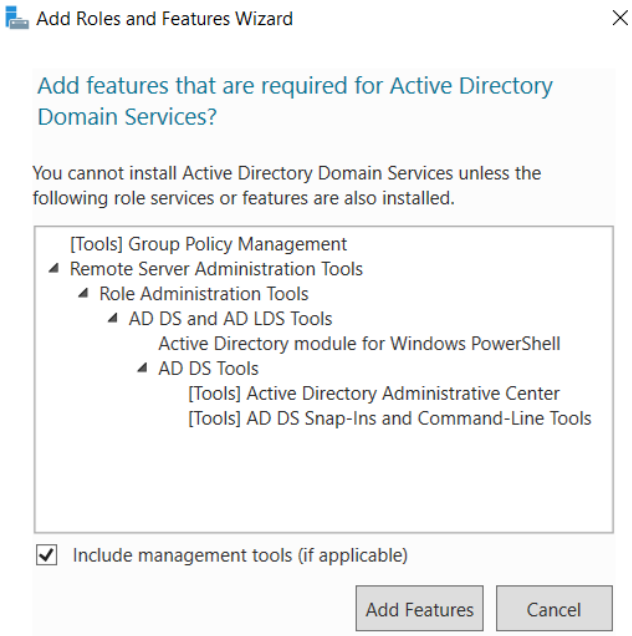
iii. Choose "***CAMH-DC***" and click next



iv. Place a checkmark on "***Active Directory Domain Services***"

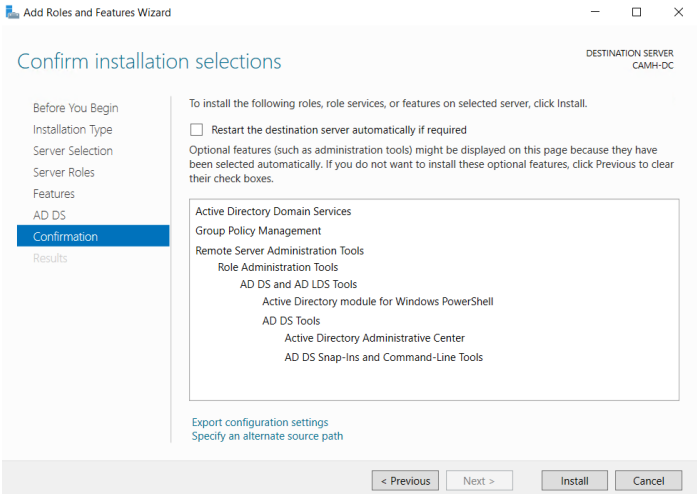


i. Click on "Add Features" in the windows that appears



ii. Click next on the following three pages

iii. At the "Confirm installation ***selections***" window click on "Install" to start the installation process and click on "***Close***" to let the process complete in the background

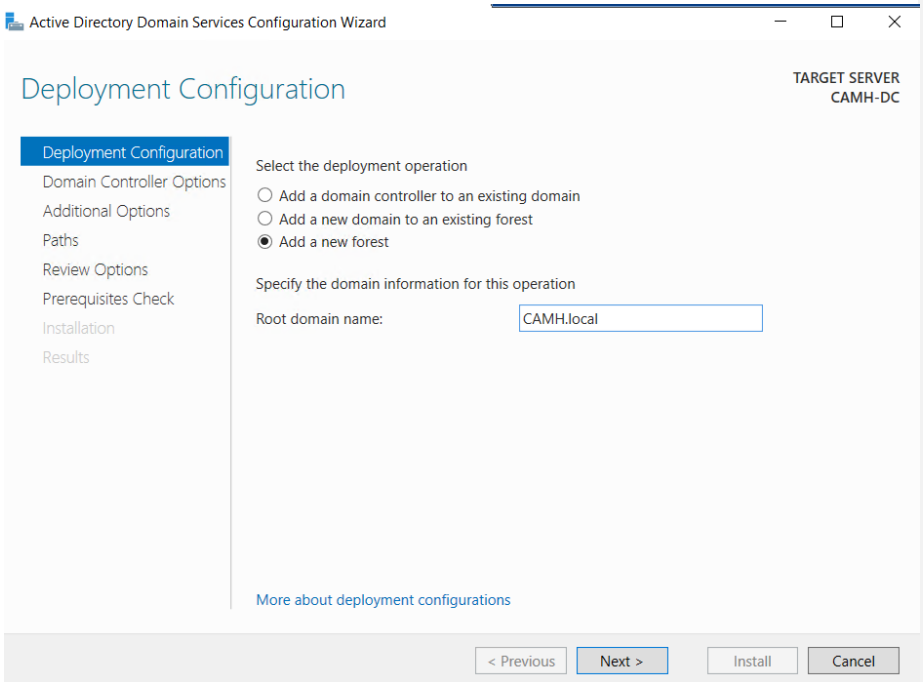


Step 3 – Promote server to a domain controller

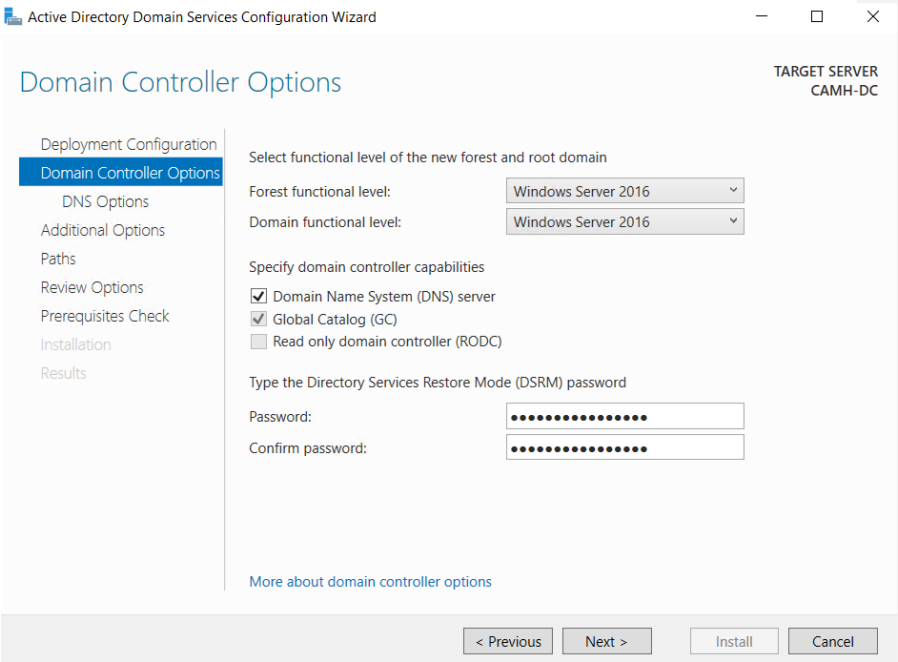
i. On the main "Server Manager" window, a notification appears when the previous Step 2 is completed, to promote the server to a domain controller

ii. Click on "Promote server to a domain controller"

iii. The promoting process involves creating a forest for the new domain, select "***Add a new forest***" and fill in the "***Root domain name***" with desired domain name

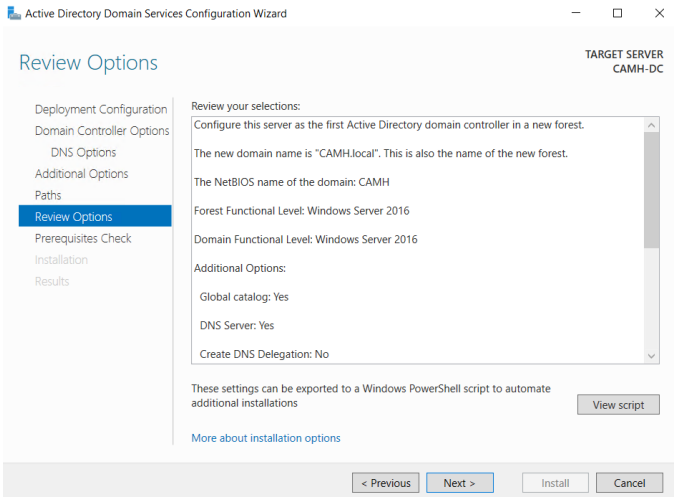


iv. On the "***Domain Controller Options***" window type in the DSRM password

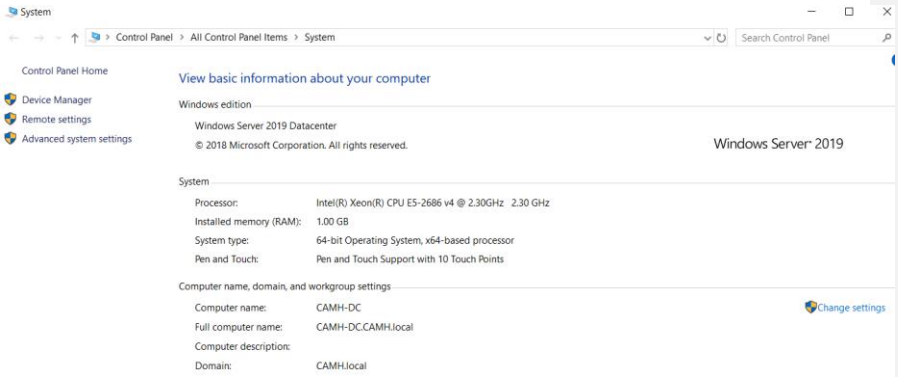


v. Leave the next three configuration screens with their default values

vi. On the "Review Options" page wait for the prerequisites to finish and click on "***Install***"



vii. Once the installation is complete the server will restart the complete the process. To confirm the domain name is successfully created, navigate to the "***System Information***" and make note of the "***Domain:***"

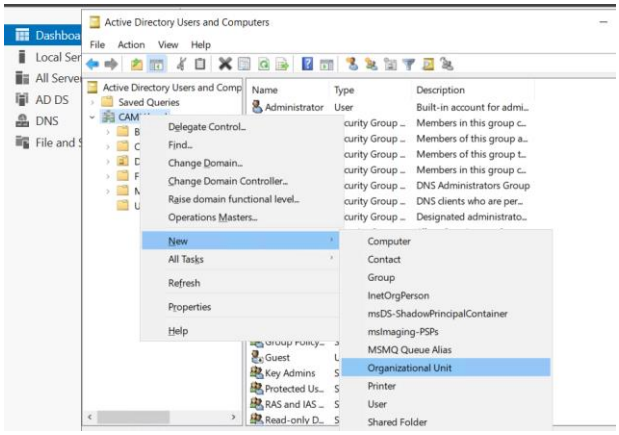


Step 4 – Create a new user account

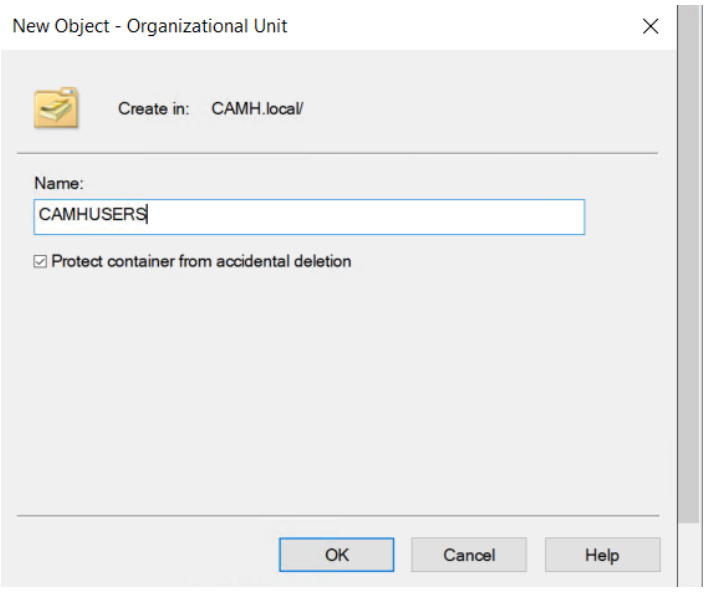
i. From the "***Server Manager***" window, navigate to Tools and then "***Active Directory User and Computers***"

ii. Navigate to the "***CAMH.local"*** domain and right-click the domain name to open the menu

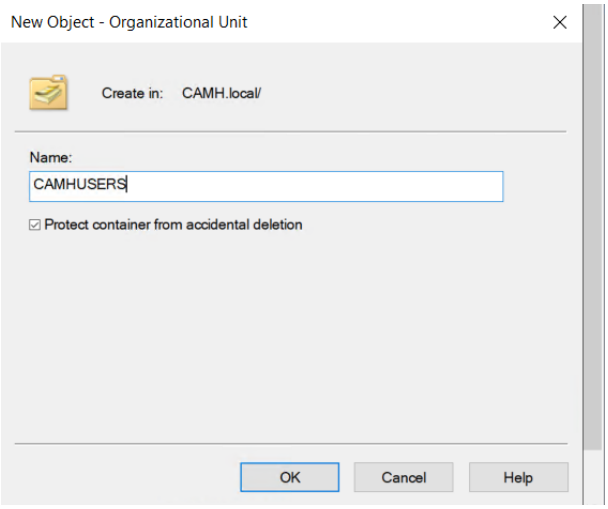
iii. Navigate and hover the mouse cursor over "***New***" to open the secondary menu and click on "***Organizational Unit***"



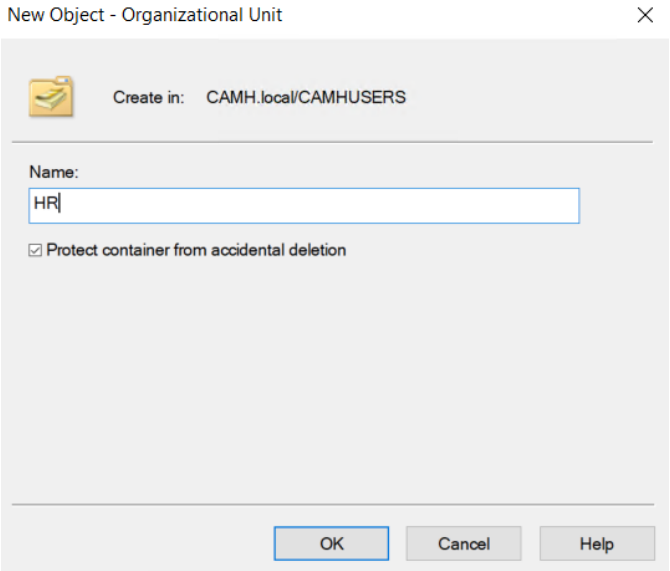
iv. In the "***New Object – Organizational Unit***" window that appears name the OU as desired



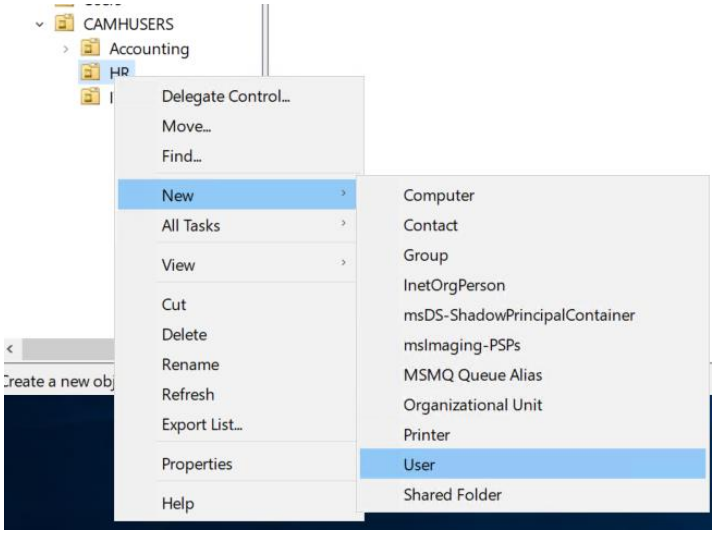
v. Once the new OU is created right-click it and hover the mouse cursor over "***New***" and then "***Organizational Unit***" to create an OU inside the first OU. This is for the user of the domain



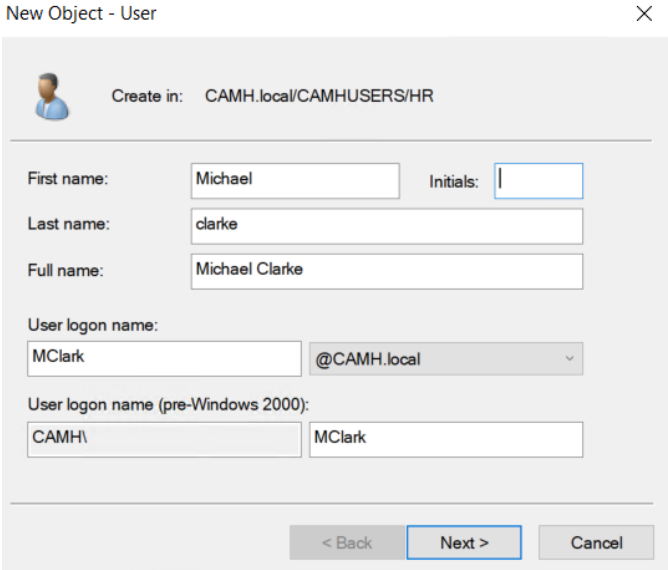
vi. Once the new "***CAMHUSERS***" OU is created, right click it and create a new OU within it, this is to be used for the users of a department



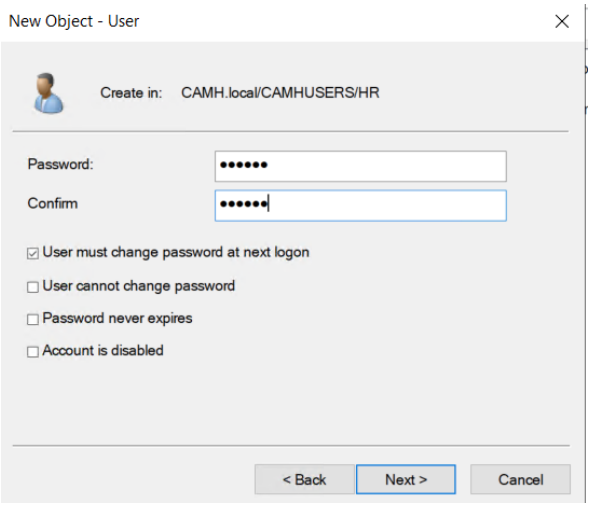
vii. To create a user account within an OU, right click the department name and select "***New***", then "***User***"



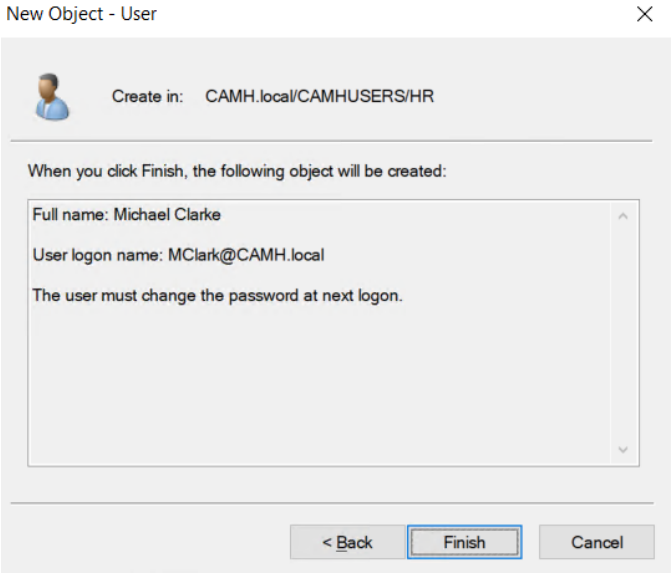
viii. Fill in the required user information to create the user account and click "***Next***" on the "***New Object – User***" window



ix. Populate the password field with the desired user password and place a check mark on the "***User must change password at next logon***" and then click "***Next***"

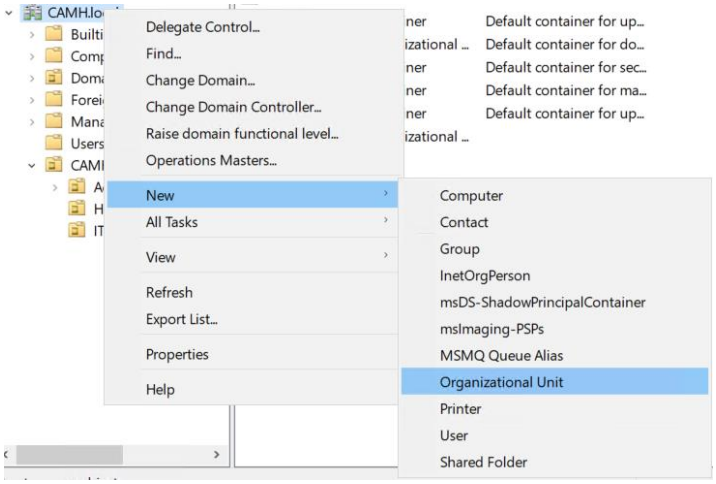


x. At the confirmation screen, verify all information is correct and click on "***Finish***" to complete the user creation

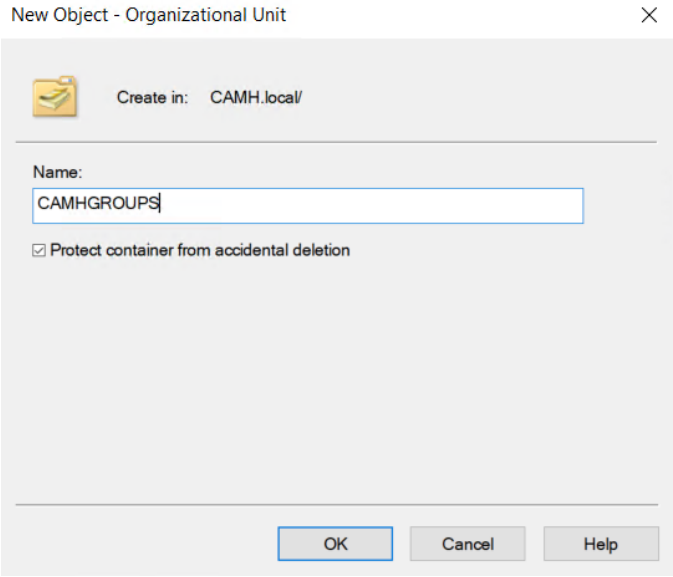


Step 5 – Create Security Group

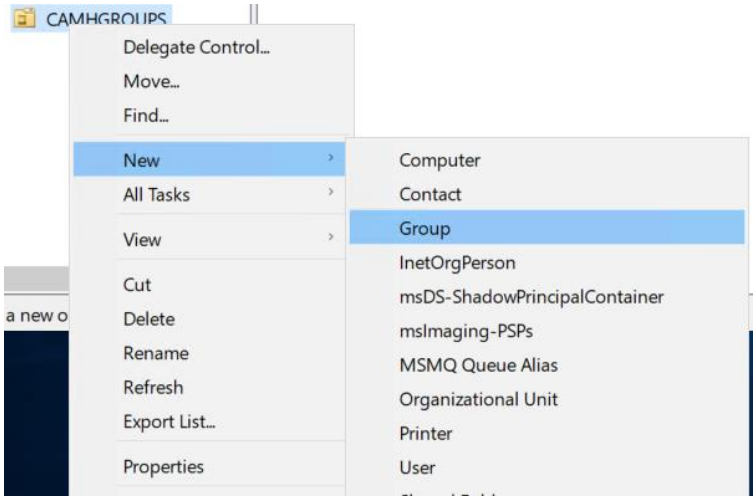
i. Navigate to the "CAMH.local" and right click the domain name, then select "***New***" and "***Organizational Unit***"



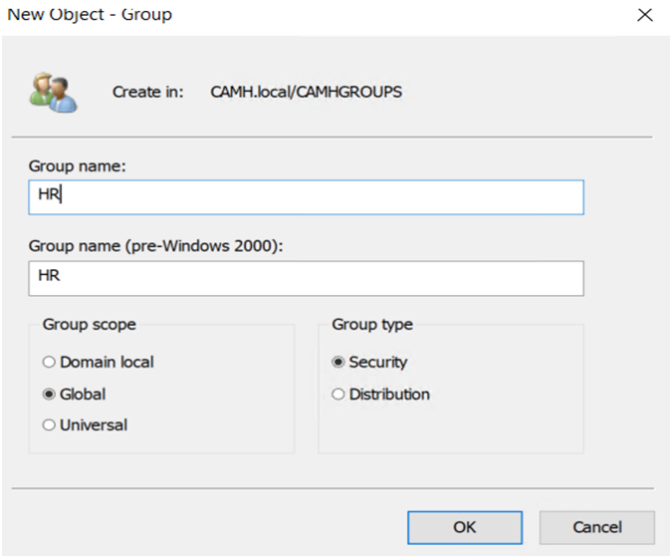
ii. In the new "***New Object – Organizational Unit***" window type in the OU name "CAMHGROUPS" name and click "***OK***"



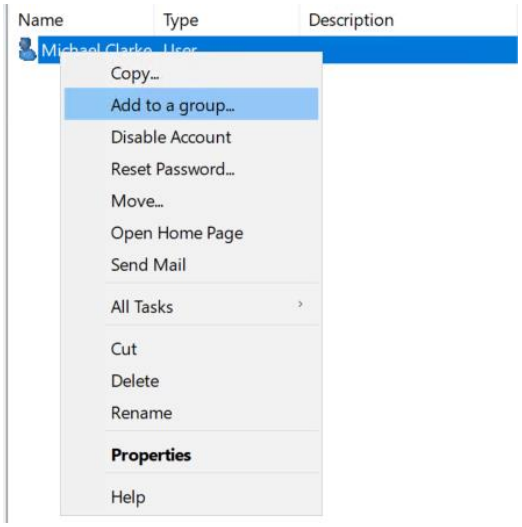
iii. With the new OU created, right click it and select "***New***", then "***Group***"



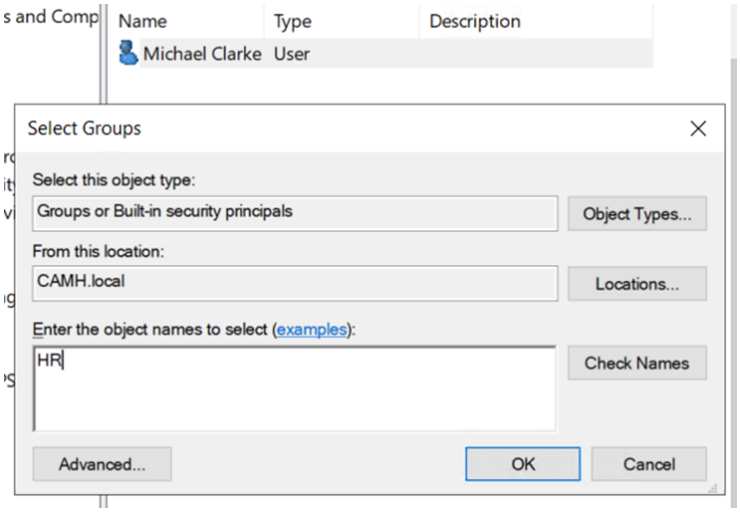
iv. For the new group name type in "***HR***", "***Group Scope***" should be "***Global***" and "***Group Type***" should be "***Security***", ensure those radio button are selected, click "***OK***" to create the group



v. Add the user previously created to the security group named "***HR***", right click on the user's name, then "***Properties***" or choose "***Add to a group***"

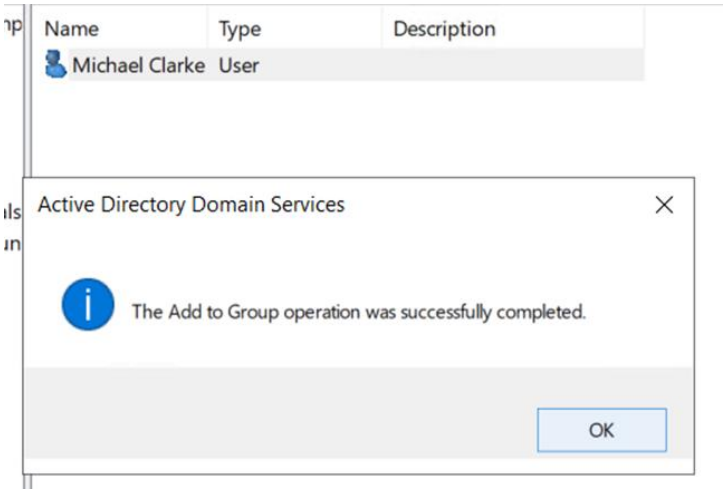


vi. In the "***Select Group***" window that appears, type in the desired group name, and click "***Check Names***"



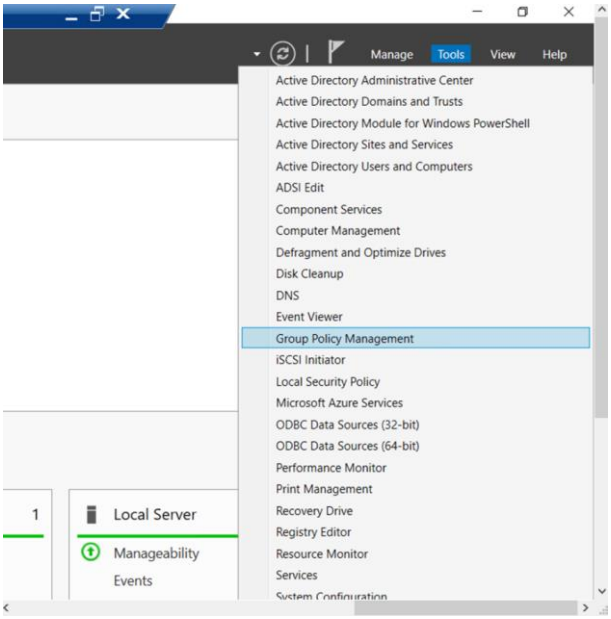
vii. Once "***HR***" is verified as a valid group, click on "***OK***" to complete the process. Confirmation window appears confirming the successful

addition. Click “OK”

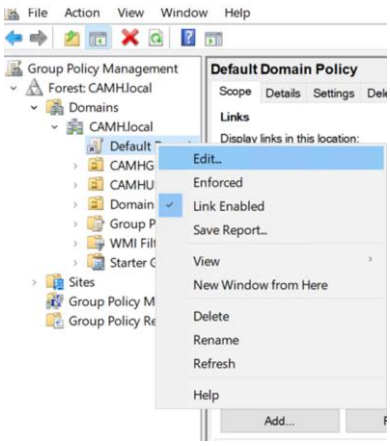


Step 6 – Password Group Policy

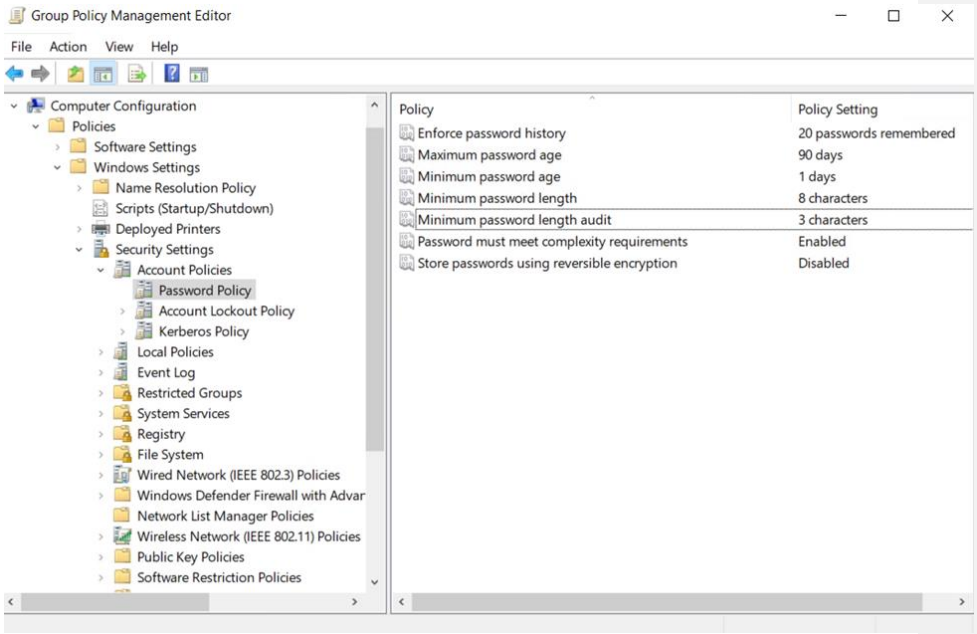
i. Open the “***Group Policy Management***” from the “***Server Manager***” dashboard window



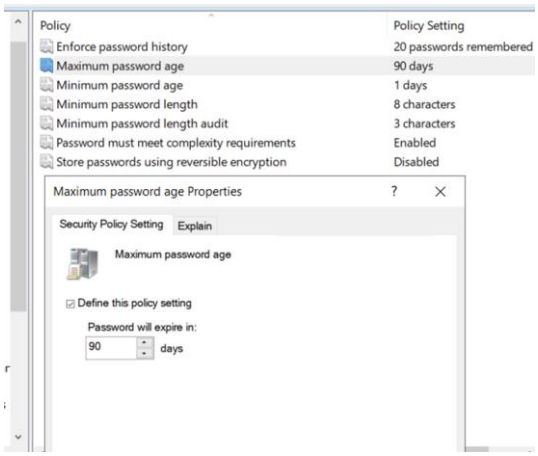
ii. Right click on the "***Default Domain Policy***", and then click on "***Edit***"



iii. The "Group Policy Management Editor" window appears, navigate to "Computer Configuration" > "Policies" > "Windows Settings" > "Security Settings" > "Account Policies" and click on "Password Policy"



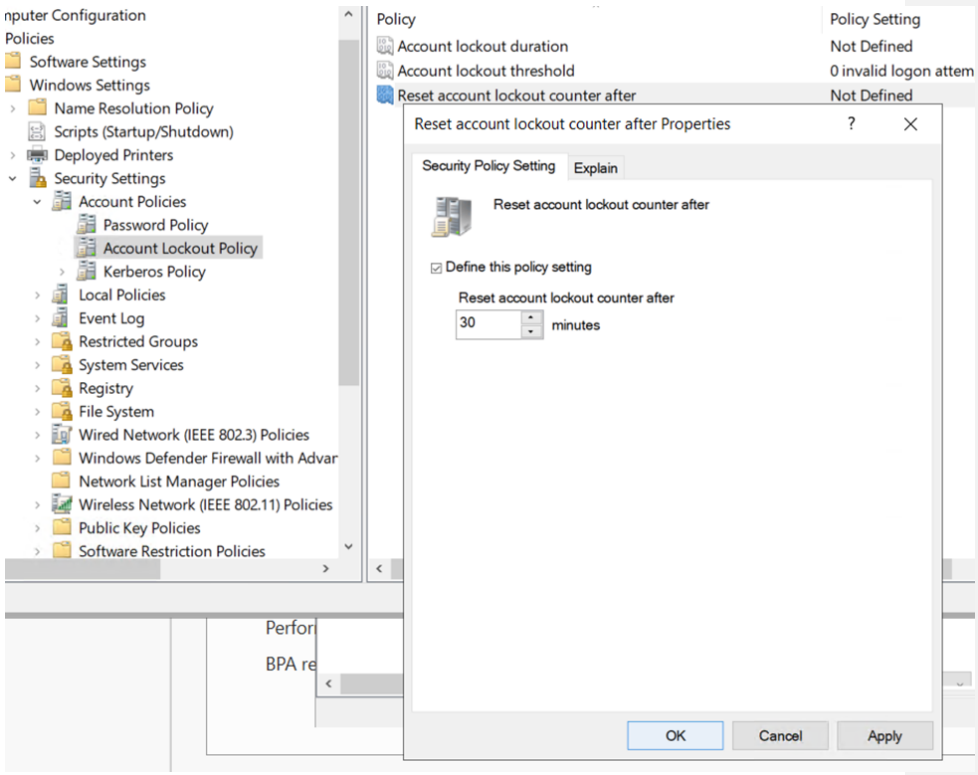
iv. Double click on each policy to change its default values to meet the desired configuration



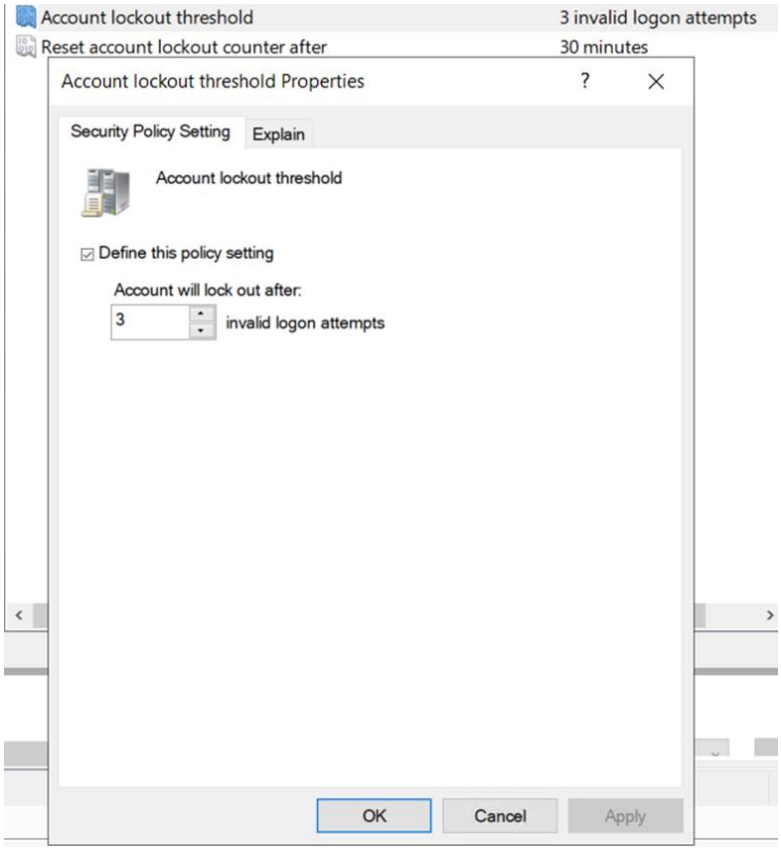
Group Policy for Account Lockout Threshold

In the “Account Lockout Policy”, the account lockout threshold is defined and can be changed to meet the policies of the company

i. Double click on "***Reset account lockout counter after***" and change the value to 30 minutes

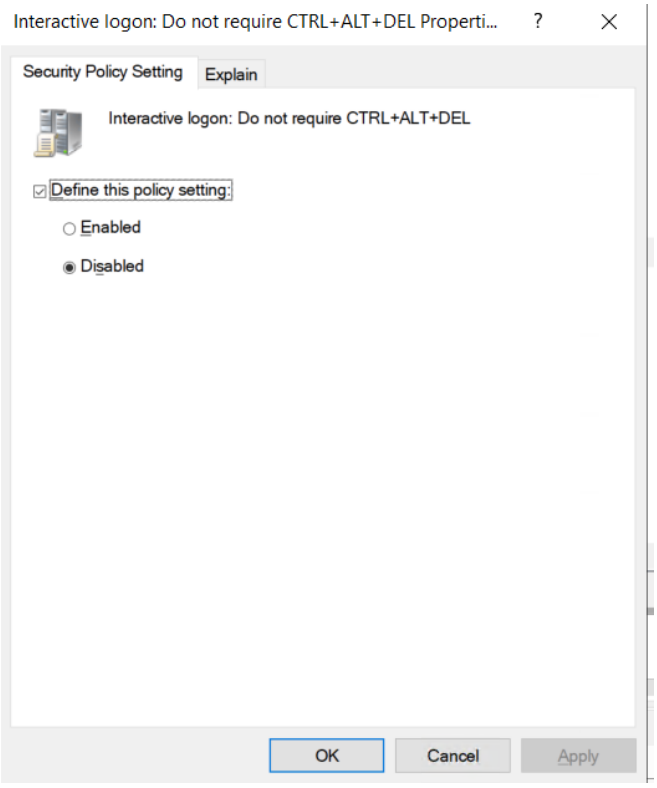


ii. To protect the domain and the company from unauthorized access and brute force attacks, change the "***Account lockout threshold***" to 3 attempts



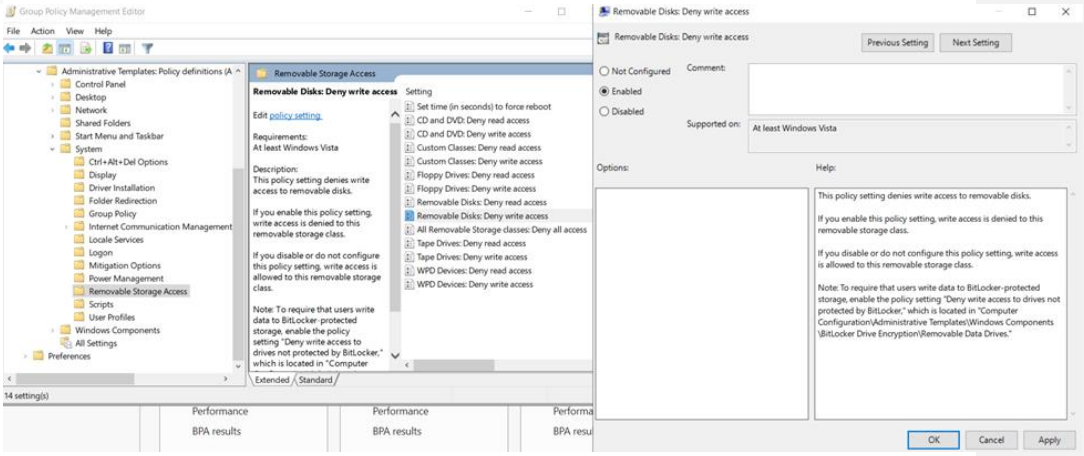
Group Policies for Interactive logon

i. Under Local Policies -> Security Options, double click on Interactive logon: Do not require CTRL+ALT+DEL, select Disabled and click OK

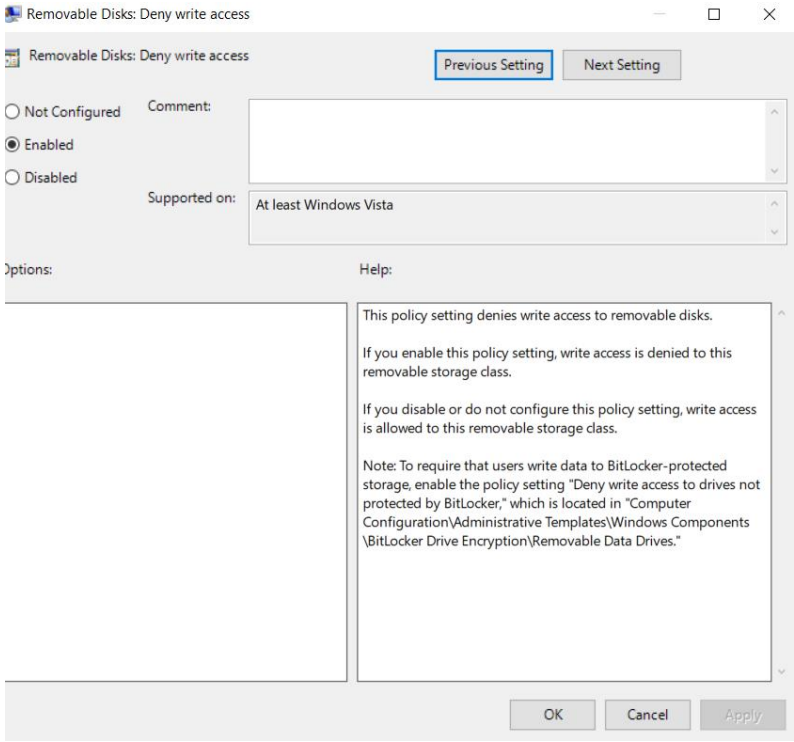


Group Policy for Deny write access on Removable Disks

Go to User Configuration -> Policies -> Administrative Templates -> System -> Removable Storage Access to configure the Removable Disks: Deny write access

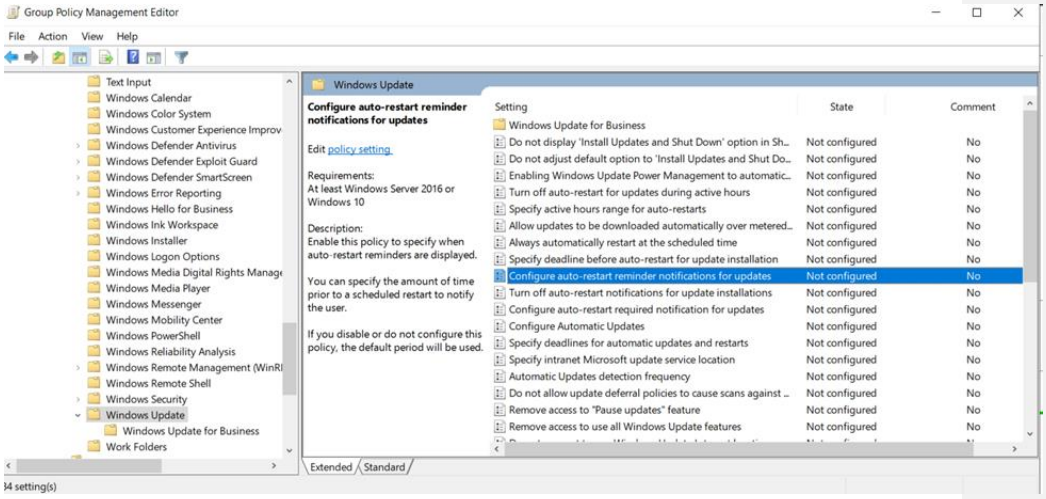


i. Double click on Removable Disks: Deny write access, select Enable and click OK

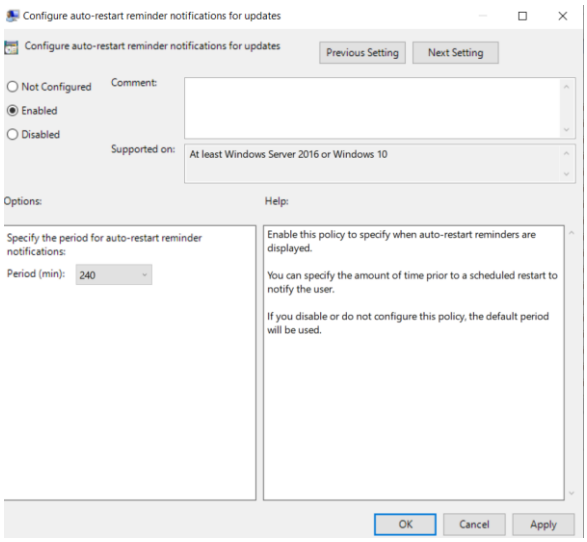


Group policy for enable auto-restart reminder notifications for updates

i. Go to Computer Configuration -> Policies -> Administrative Templates -> Windows Components, click on Windows Update. Double click on Configure auto-restart reminder notifications for updates.

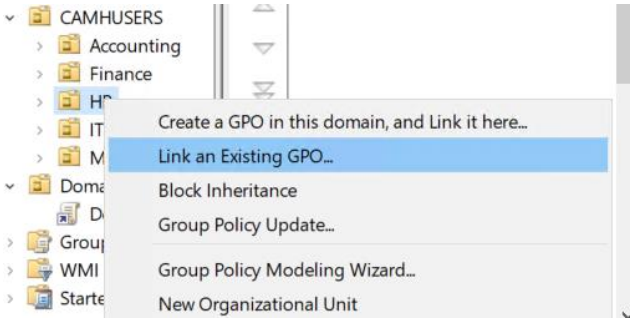


ii. Select Enable, choose appropriate options based on the company's procedure and click OK.

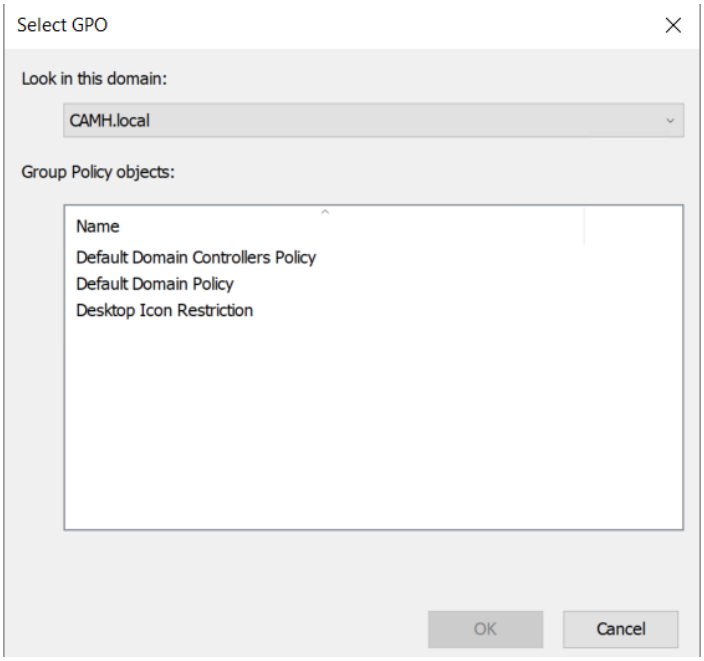


Step 7 – Link Group Policy to User Group

i. Right click on a user group and choose Link an Existing GPO



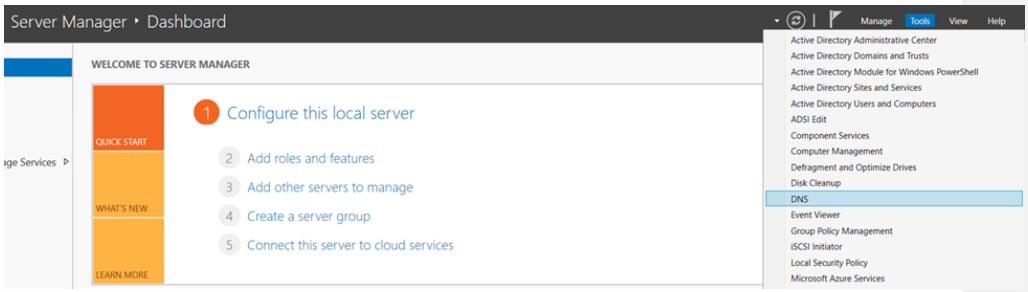
ii. Choose the suitable group policy and click OK



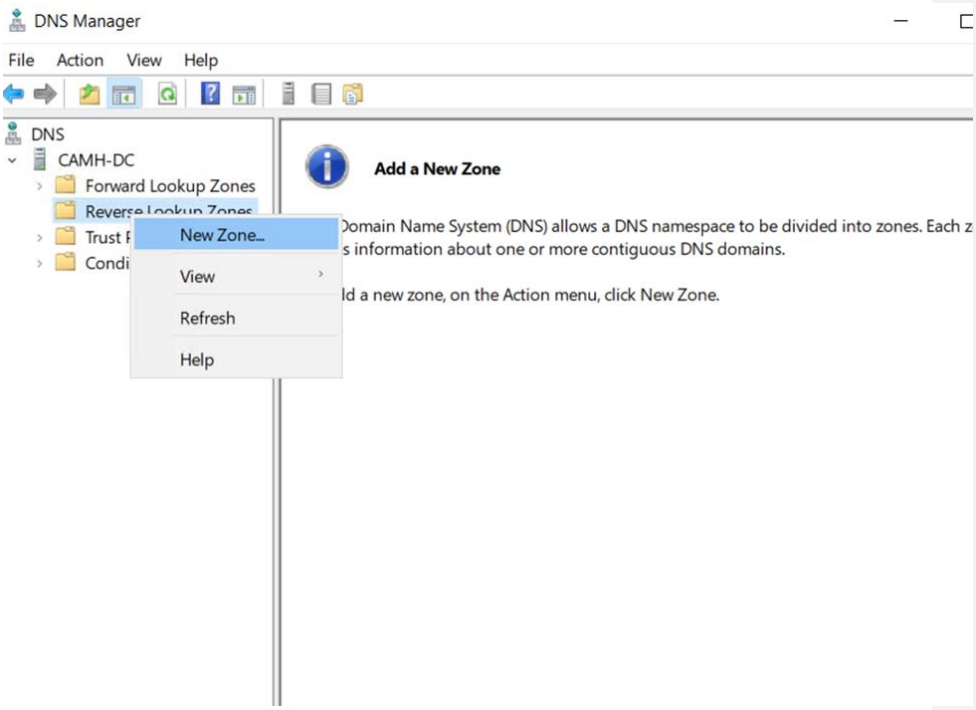
Part 2 – Setting up DNS Server

Step 1 – Install DNS feature

i. Click Tools -> DNS to open the DNS Manager

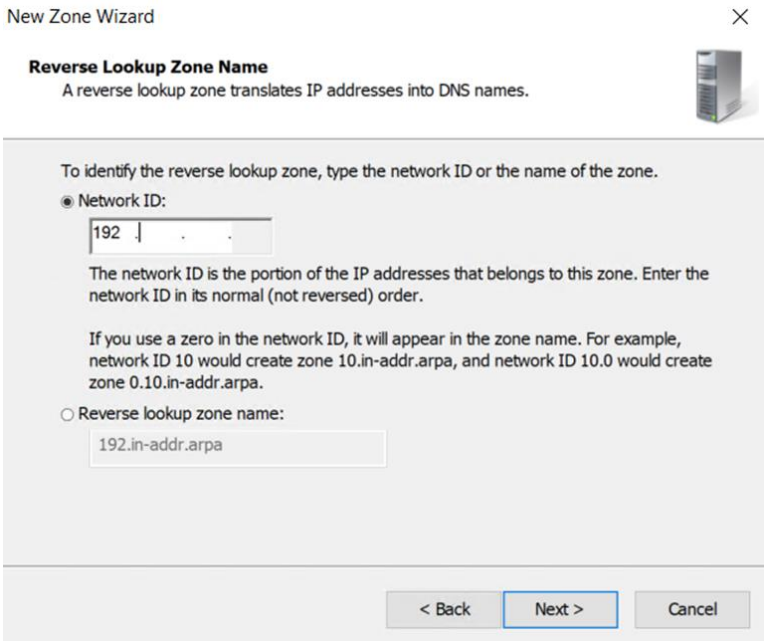


ii. In DNS Manager, expand CAMH-DC and right click on Reverse Lookup Zones

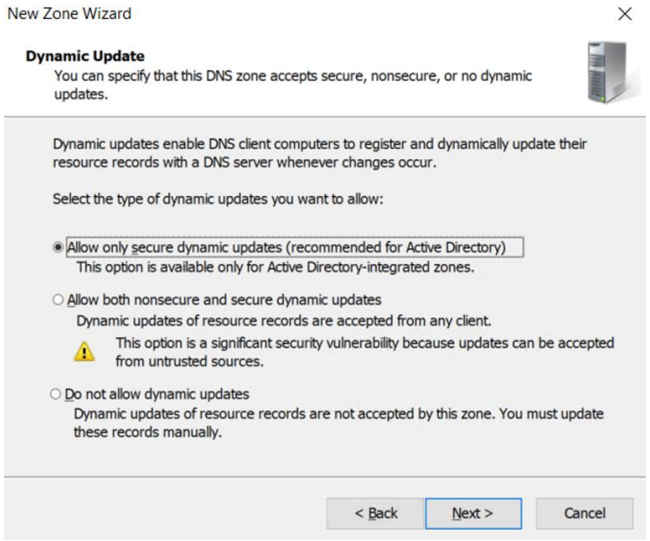


iii. Create a Revers Lookup Zone

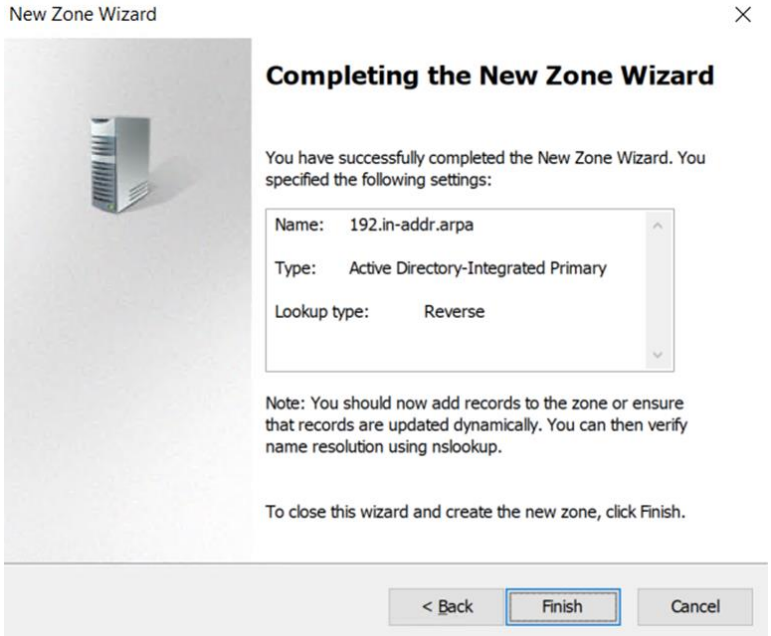
iv. The New Zone Wizard will pop up, click Next. Keep the next three pages as their default values. Enter the Network ID: 192 and click Next



v. Choose Allow only secure dynamic updates and click Next.



vi. Once verify the information is correct, click Finish.



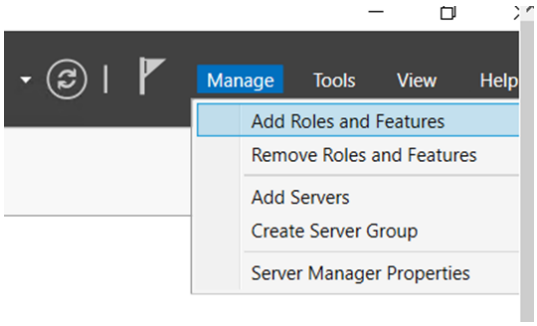
vii. A test ping from the Domain Controller to the test server "cloudlogics_Public"

```
C:\Windows\system32>ping 192.168.0.12

Pinging 192.168.0.12 with 32 bytes of data:
Reply from 192.168.0.12: bytes=32 time=30ms TTL=127
Reply from 192.168.0.12: bytes=32 time=28ms TTL=127
Reply from 192.168.0.12: bytes=32 time=32ms TTL=127
Reply from 192.168.0.12: bytes=32 time=29ms TTL=127

Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 32ms, Average = 29ms

C:\Windows\system32>
```

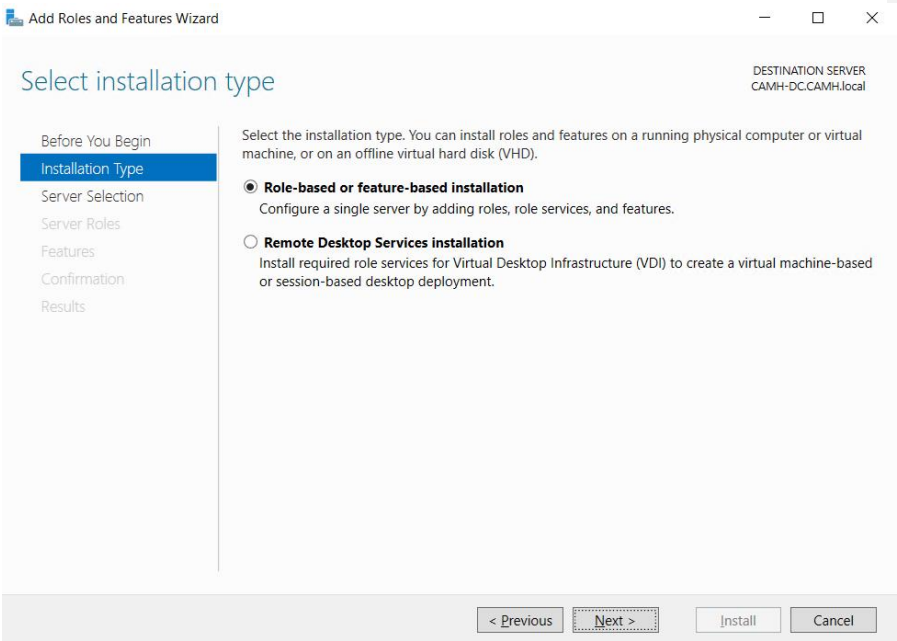
Part 3 – Setting up DHCP Server

Step 1 – Add DHCP feature role

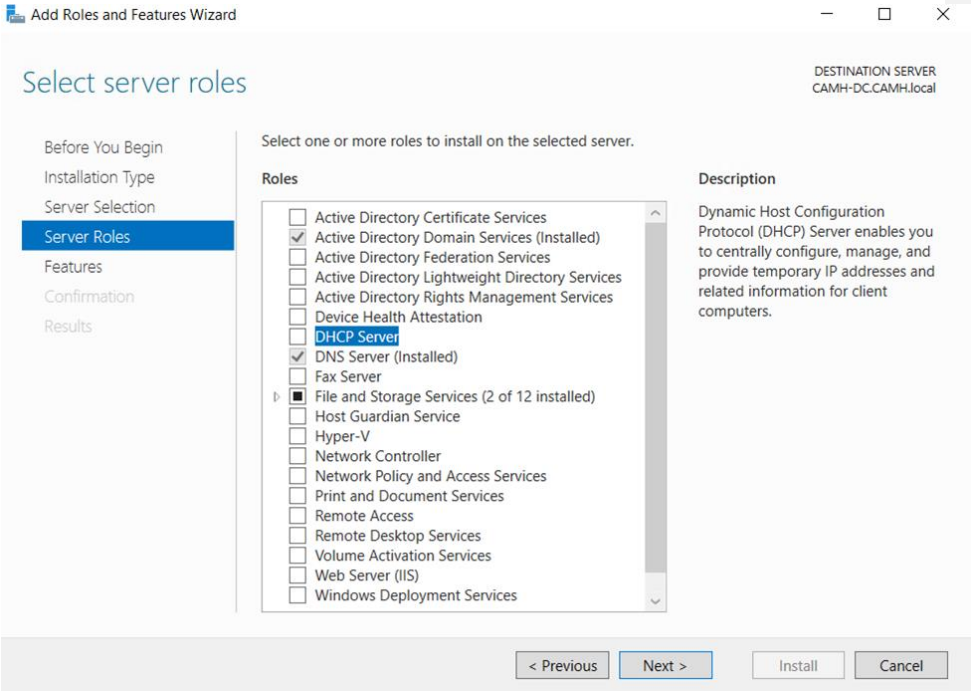
i. In Server Manager, click Manage -> Add Roles and Features



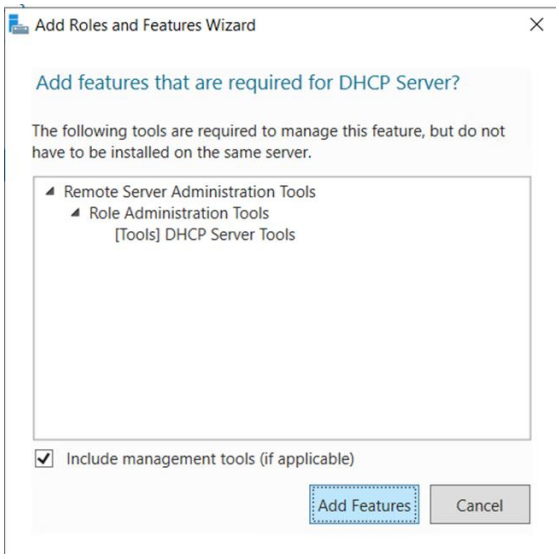
ii. The Add Roles and Features Wizard window pops up, click Next and keep the next two pages as default.



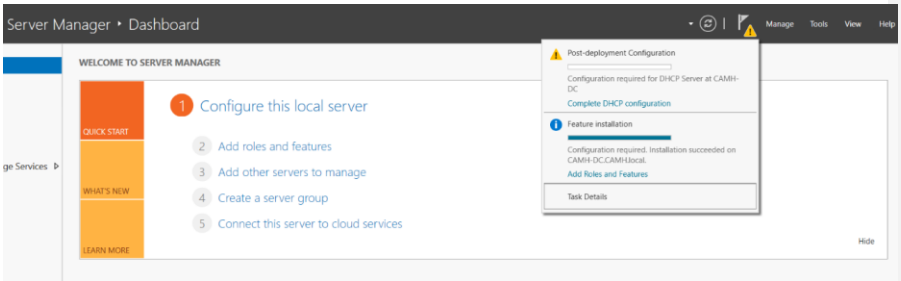
iii. Select DHCP Server Role



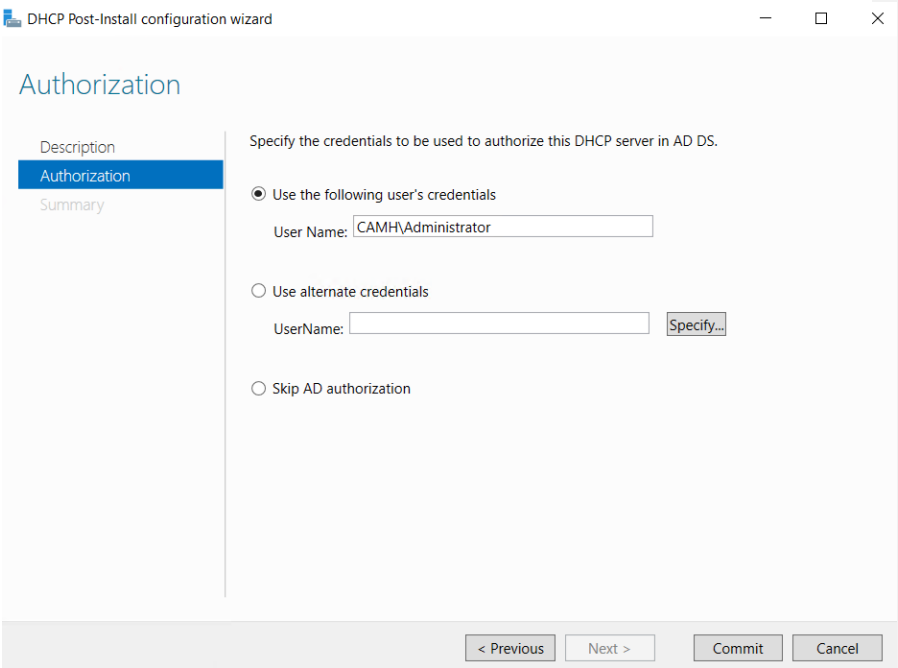
iv. Click Add Features in the pop-up window



v. After the installation is done, click on Complete DHCP configuration.

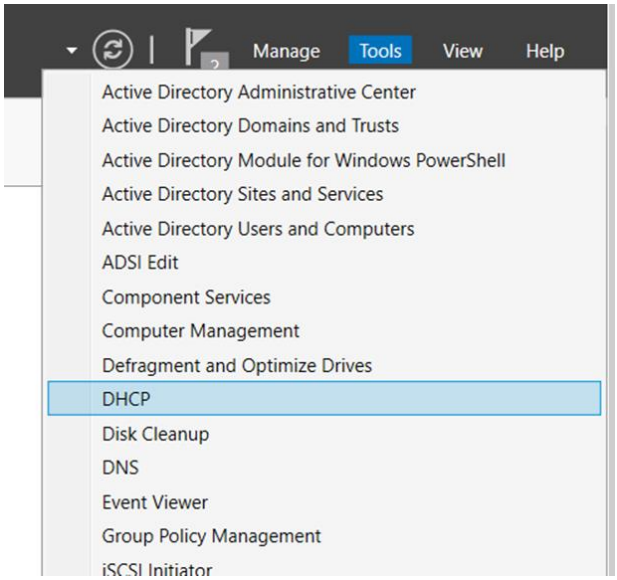


vi. Click on Next as the wizard window pops up. Use Administrator account as the default credentials and click Commit.

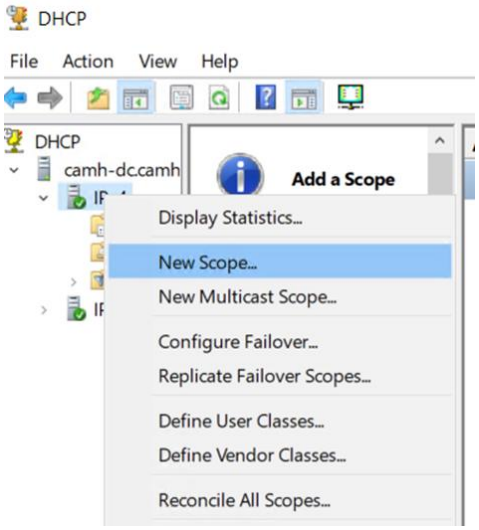


Step 2 – Add New Scope

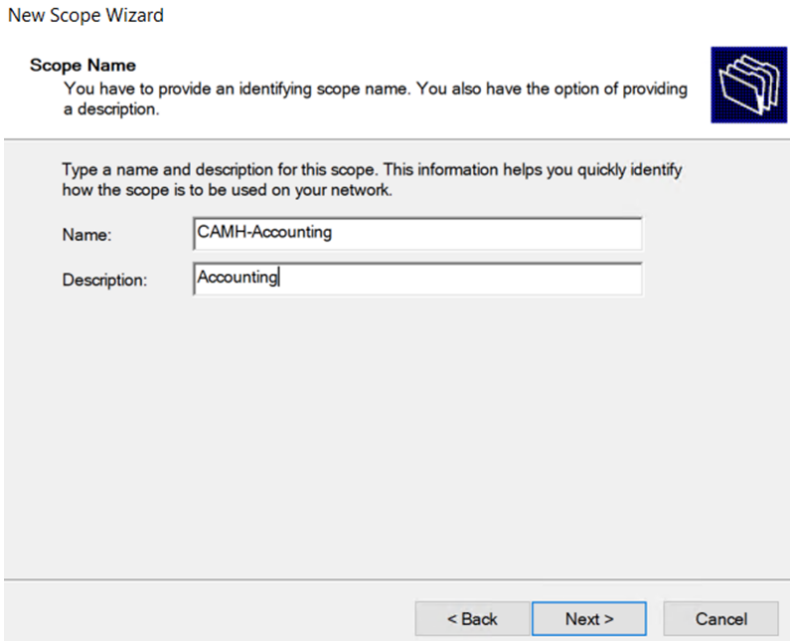
i. In Server Manager, click Tools -> DHCP.



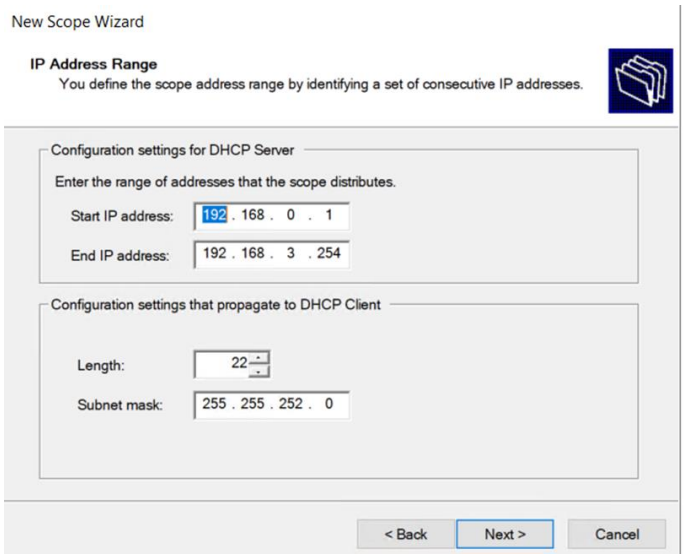
ii. Click on IPv4 and choose New Scope.



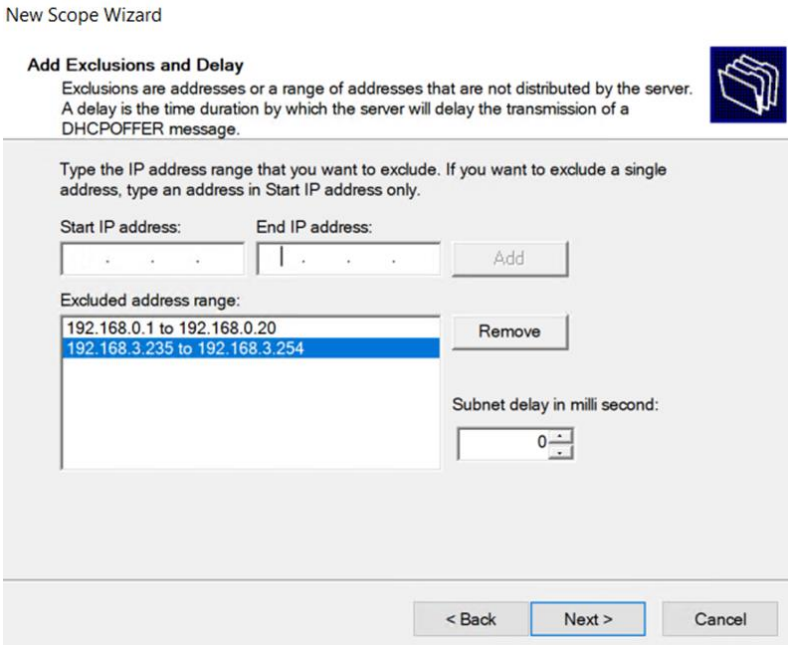
iii. Click Next when the New Scope Wizard pops up, enter name and description for the new scope.



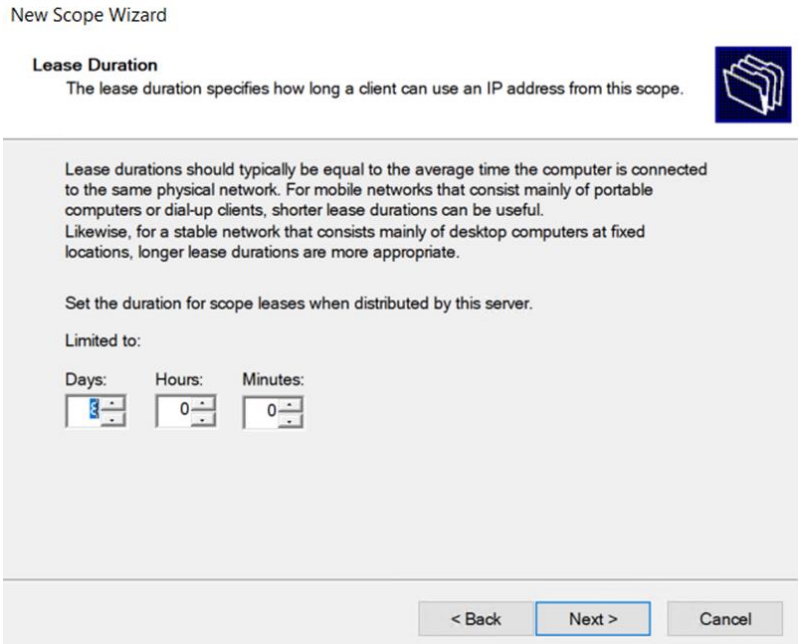
iv. Enter IP address range for the new scope.



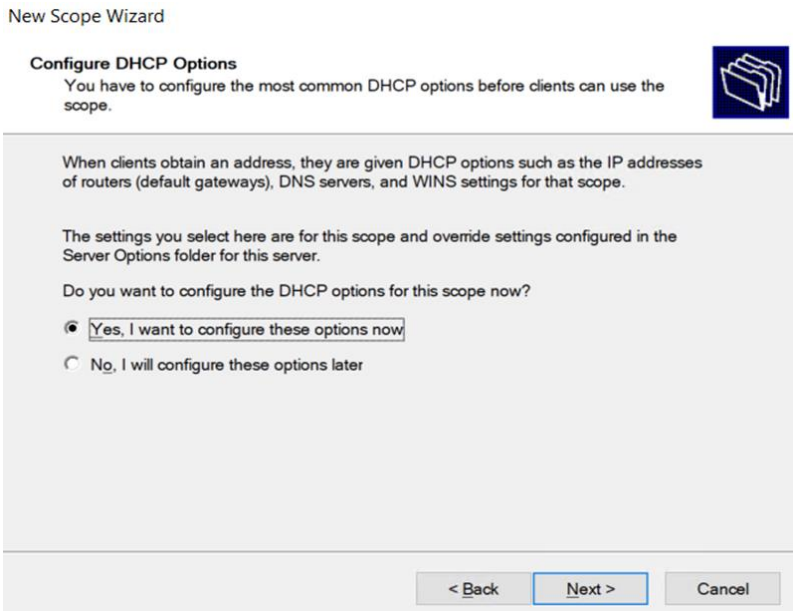
v. Add exclusions if there is any



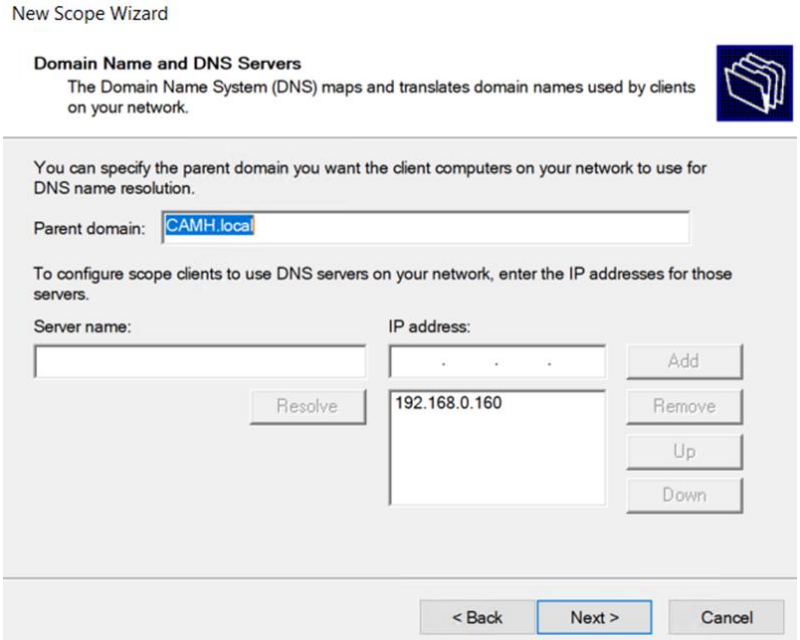
vi. Set the duration for 8 days.



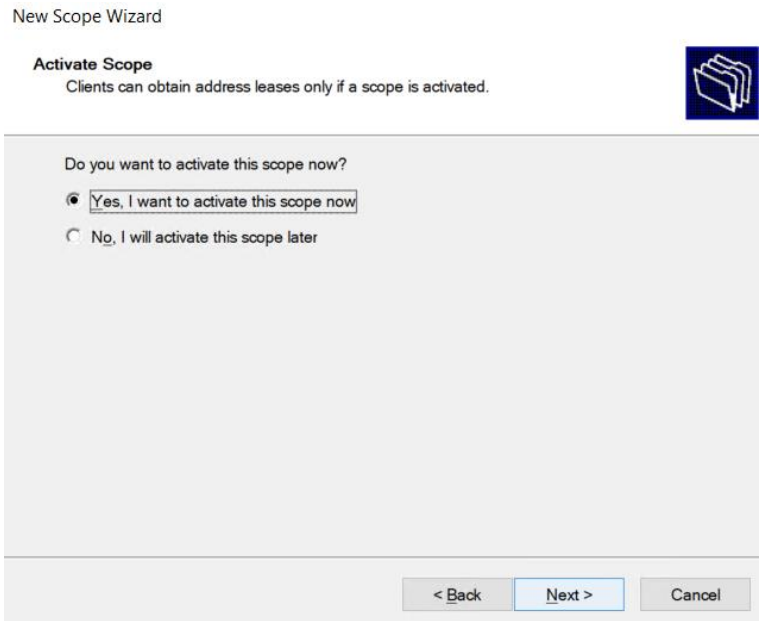
vii. Select Yes and click Next for the next page.

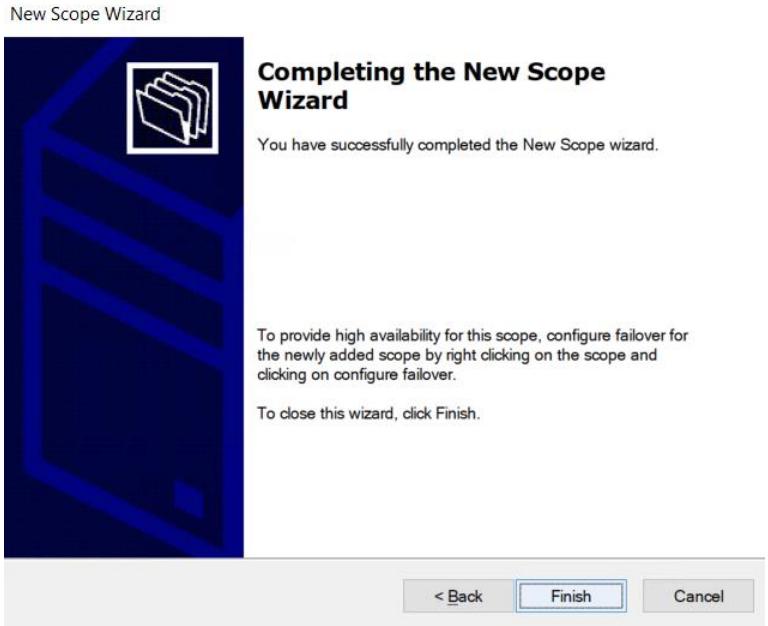


viii. Add DNS server IP address.



ix. Select Active the scope now. Click Next and Finish.

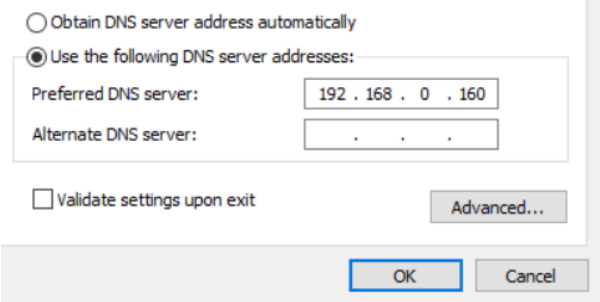

New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< Back
Next >
Cancel


New Scope Wizard
Completing the New Scope Wizard
You have successfully completed the New Scope wizard.
To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.
To close this wizard, click Finish.
< Back
Finish
Cancel

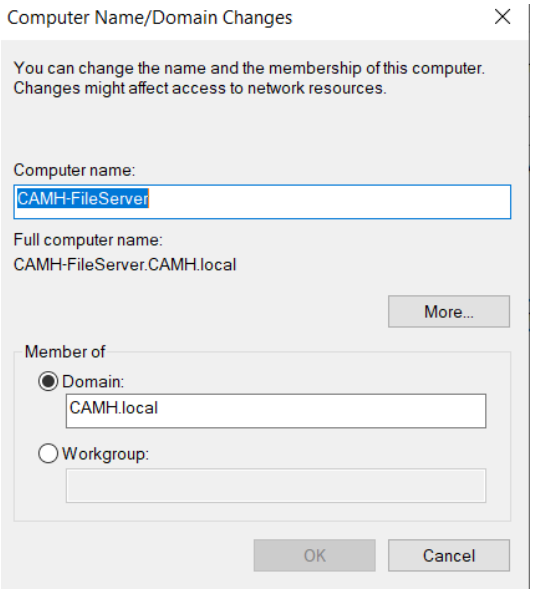
Part 4 – Setting up File Server

Step 1 – Join the server to the domain

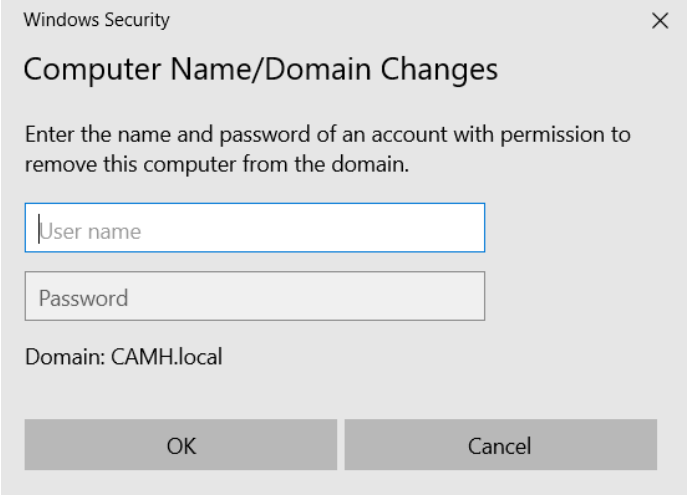
i. Go to Control Panel -> Network and Sharing Center -> Change Adapter setting -> IPv4 to change the DNS server address.



ii. Go to System in Control Panel, under Computer name, domain and workgroup settings, click on Change settings. Change Computer name and type the domain name

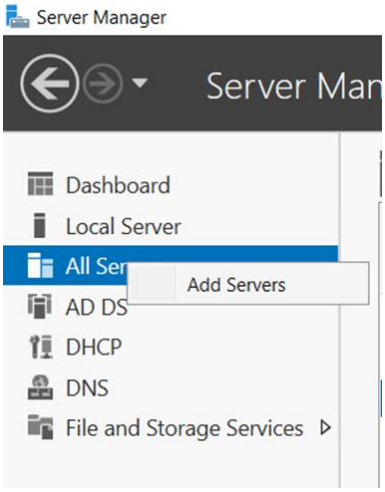


iii. Type the credentials and restart the server.

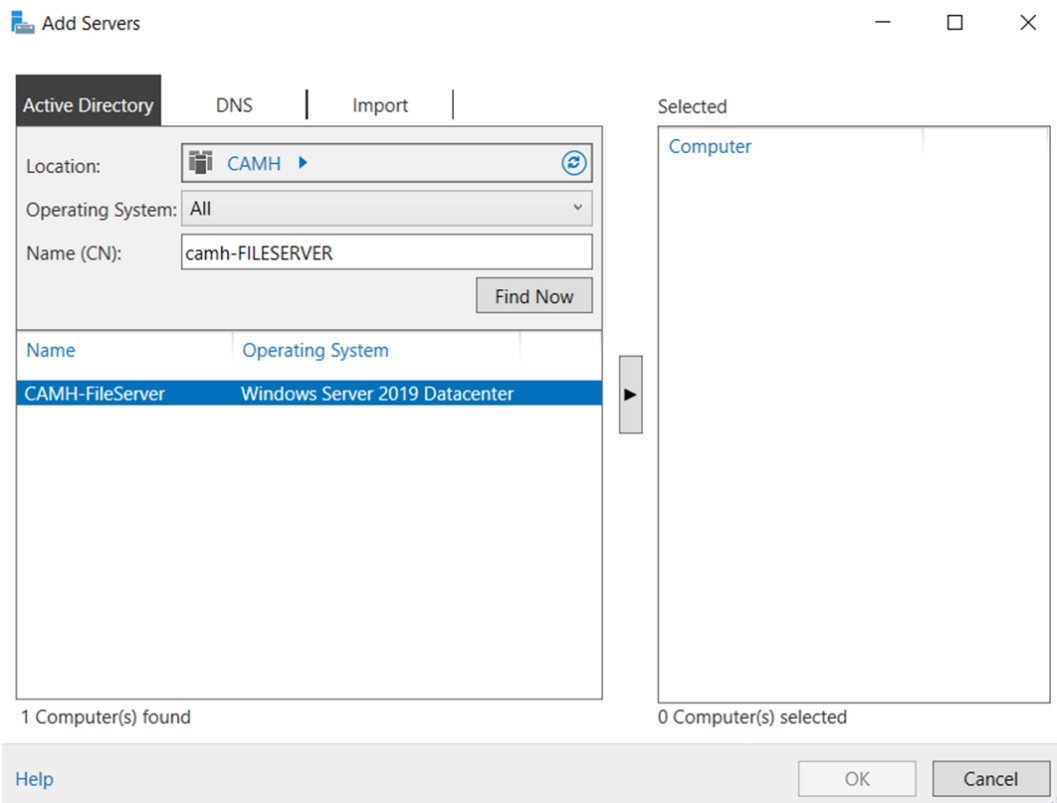


Step 2 – Add file server role

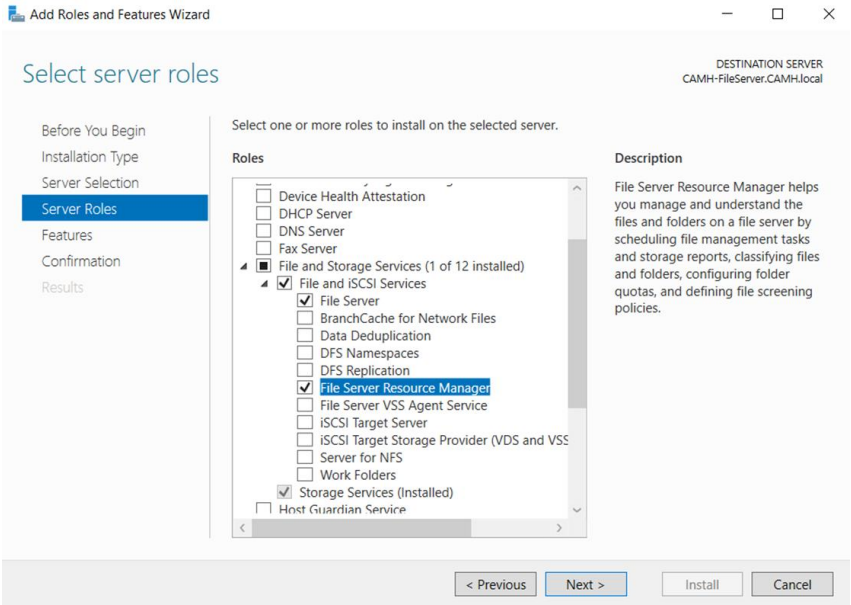
i. From domain controller open server manager and then add servers so we can manage all servers from one server.



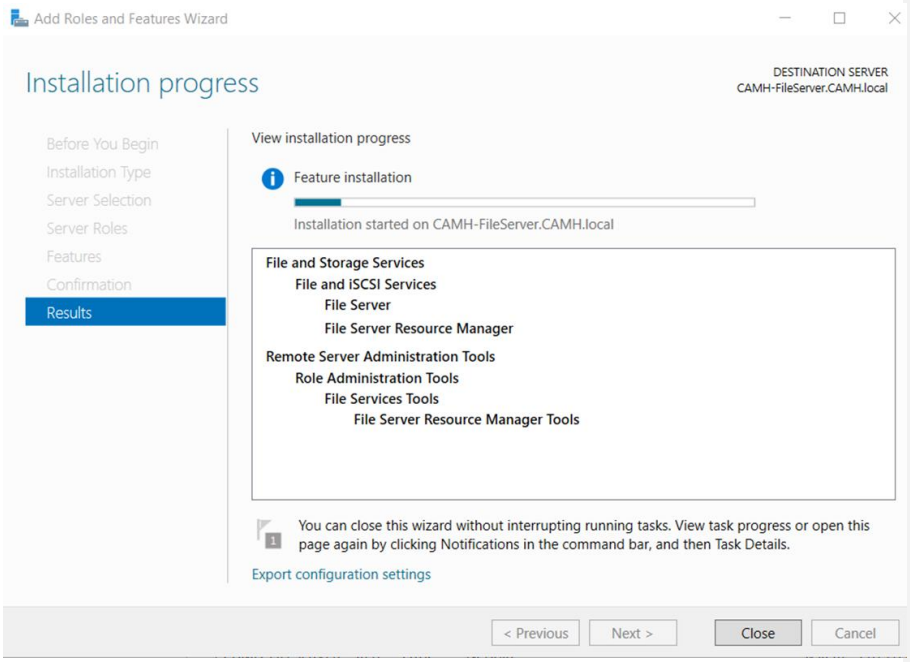
ii. Add server window will open, Enter the name of the server CAMH-FileServer, and click ok



iii. The Add Roles and Features Wizard window pops up, click Next and keep the next two pages as default. Click on File and Storage Services and check File Server, File Server Resource Manager and Storage Services

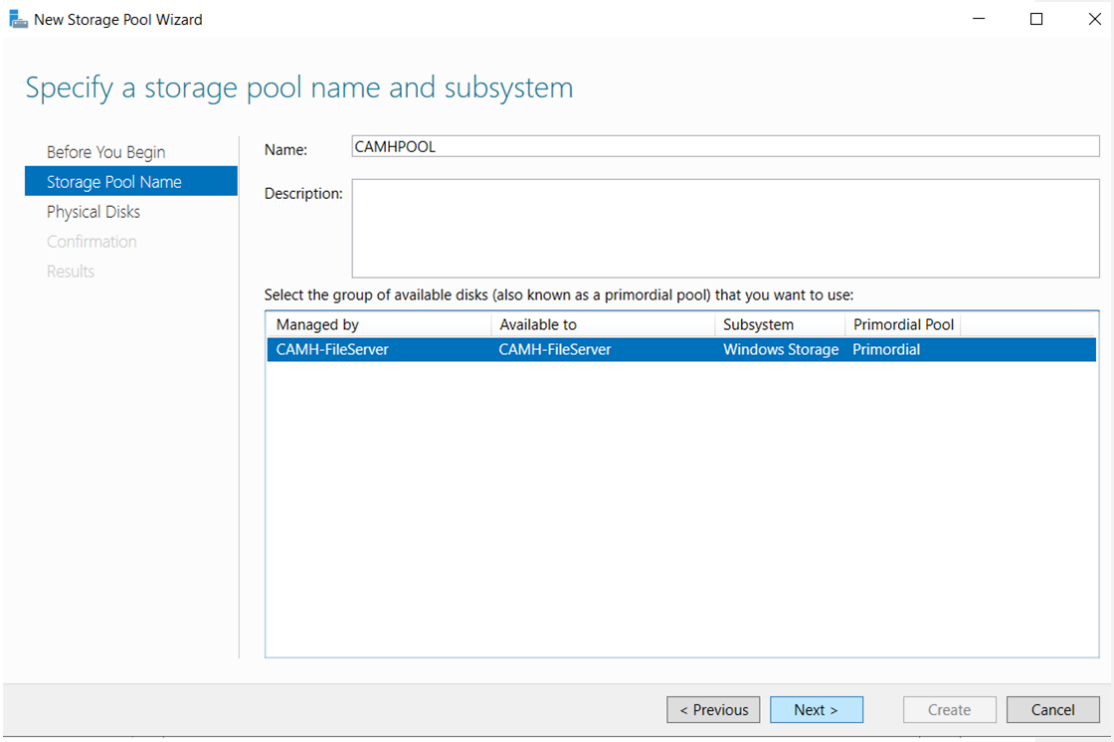


iv. Keep the next pages default and click install. Installation process will continue

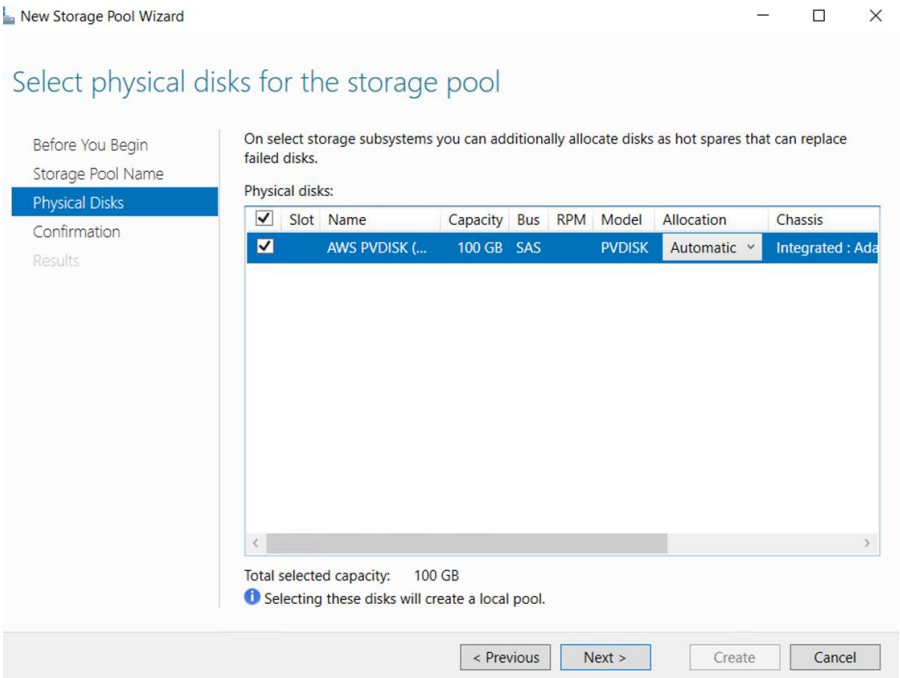


Creating a File Pool

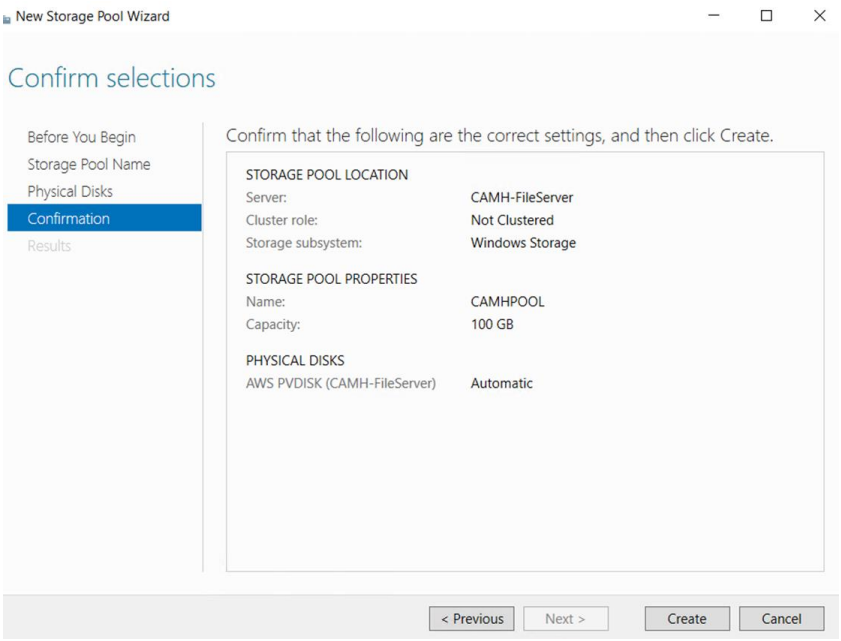
i. In Server Manager, click on File and Storage Services. Click on Storage Pools, right click on Primordial and select New Storage Pool. Click on Next and type the Storage Pool Name



ii. Check physical disks that will be used for the pool and click Next.



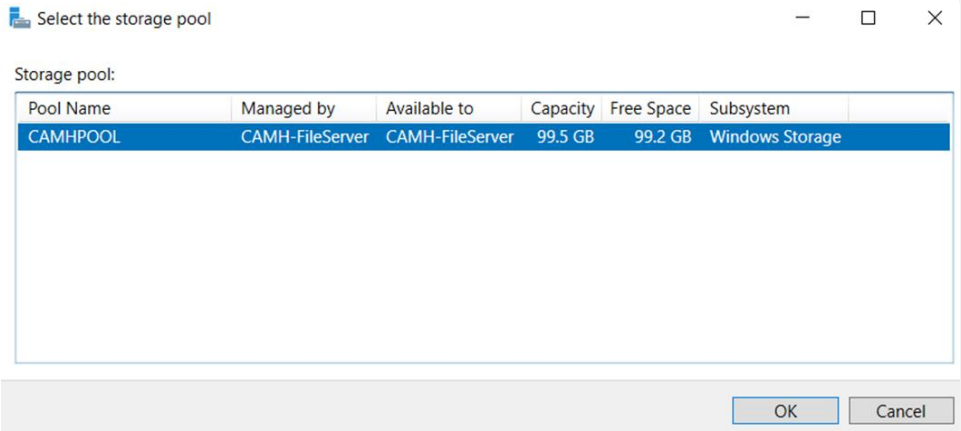
iii. When confirmed, click on Create



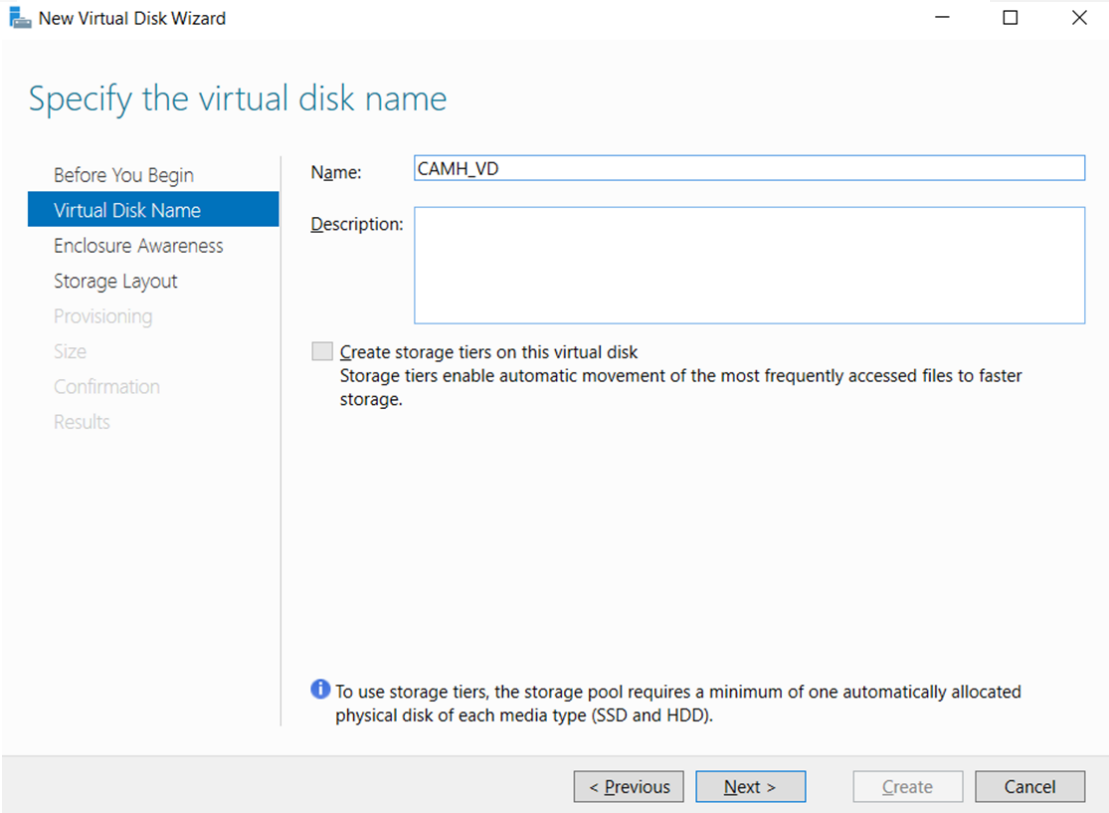
Step 3 – Creating a virtual disk

i. Click the link in Virtual Disks section to create virtual disk.

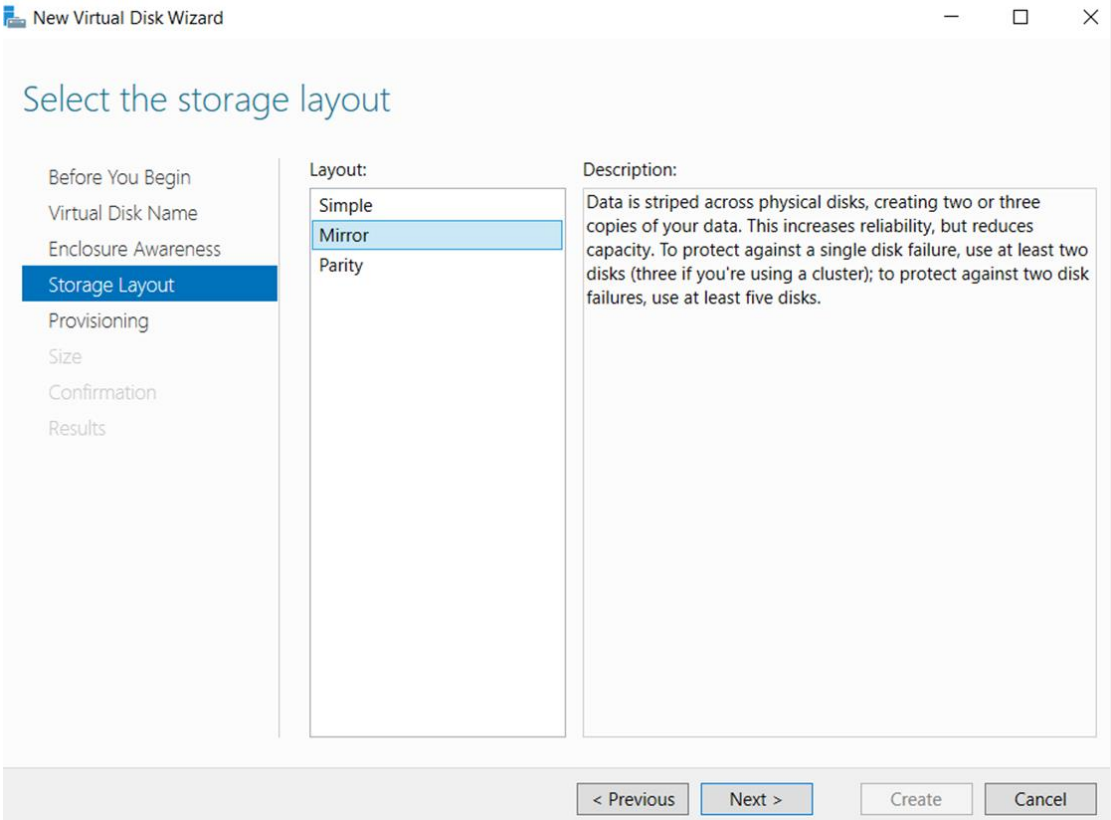
ii. Select the desired storage pool manager



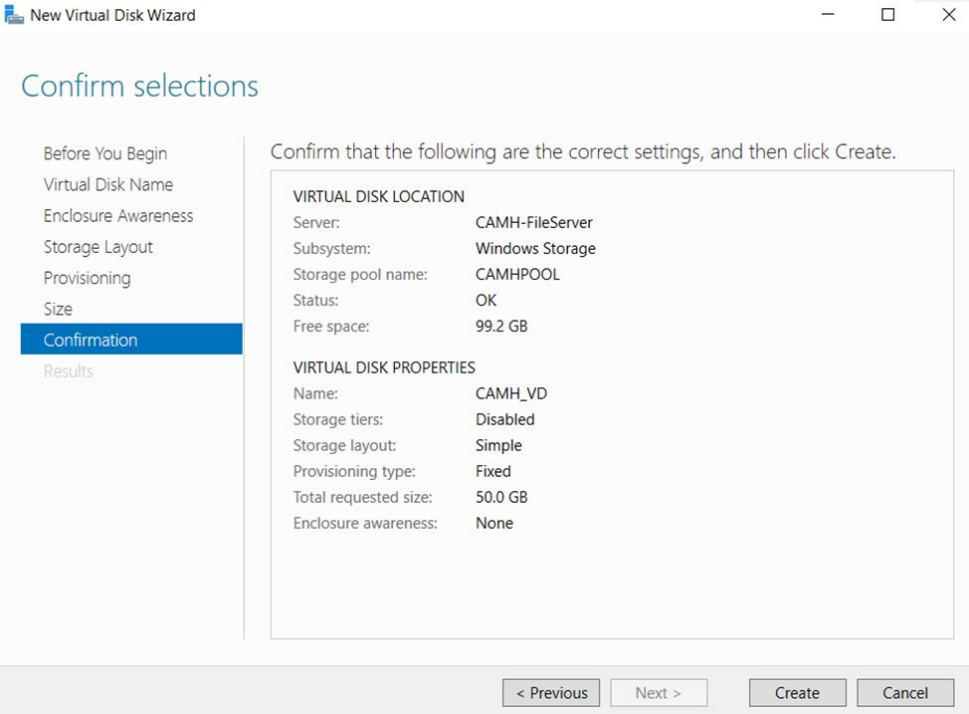
iii. Enter the name CAMH_VD in New Virtual Disk wizard and click next



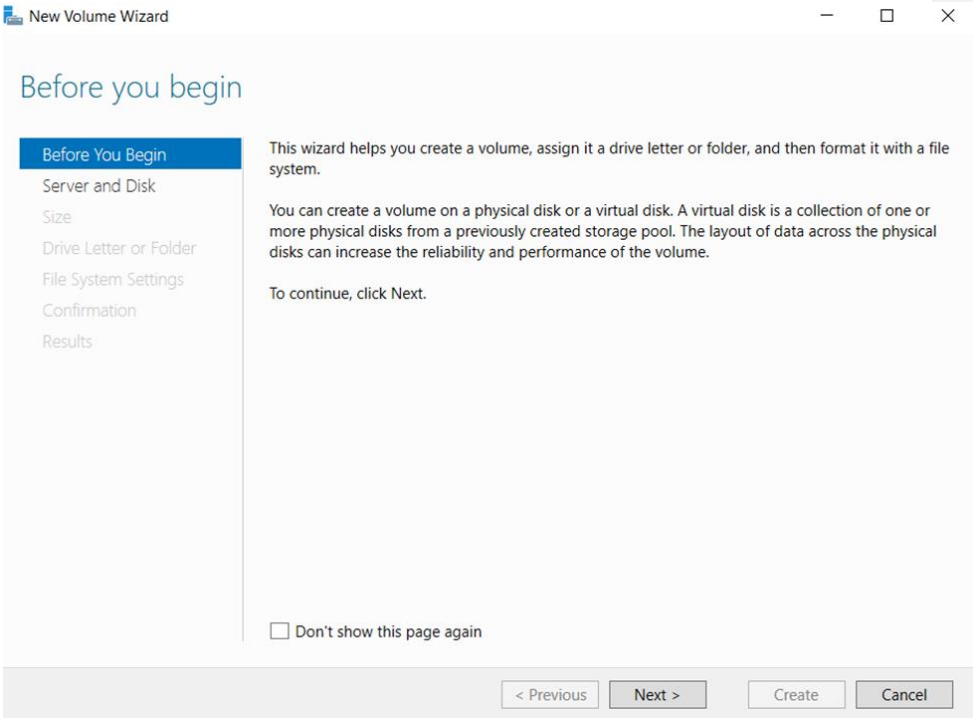
iv. Select Mirror and click next.



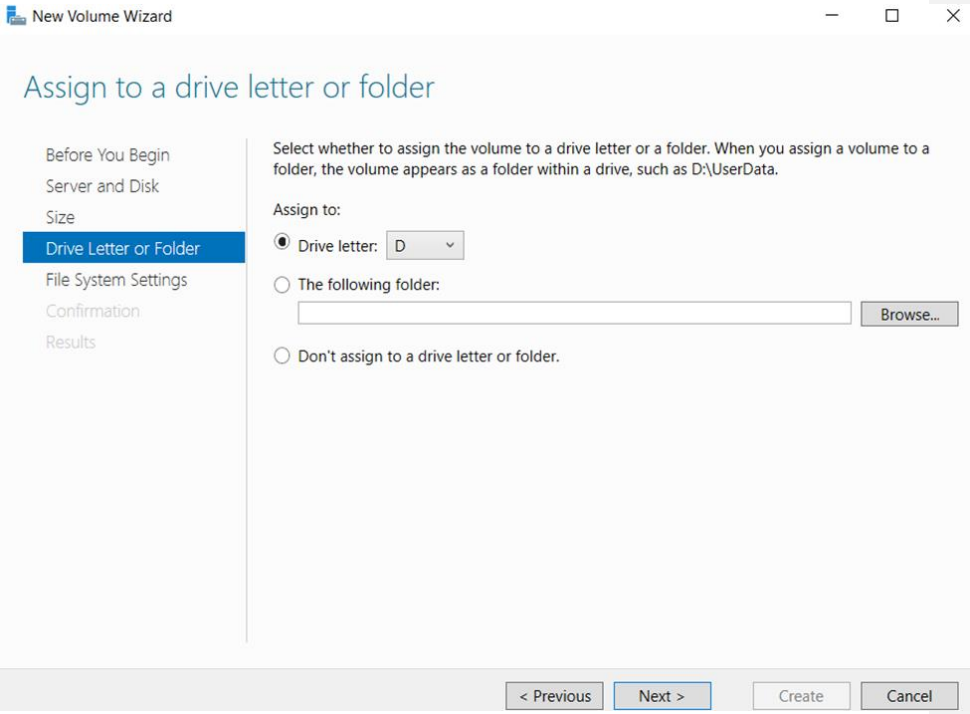
v. Review the confirmation page and select create



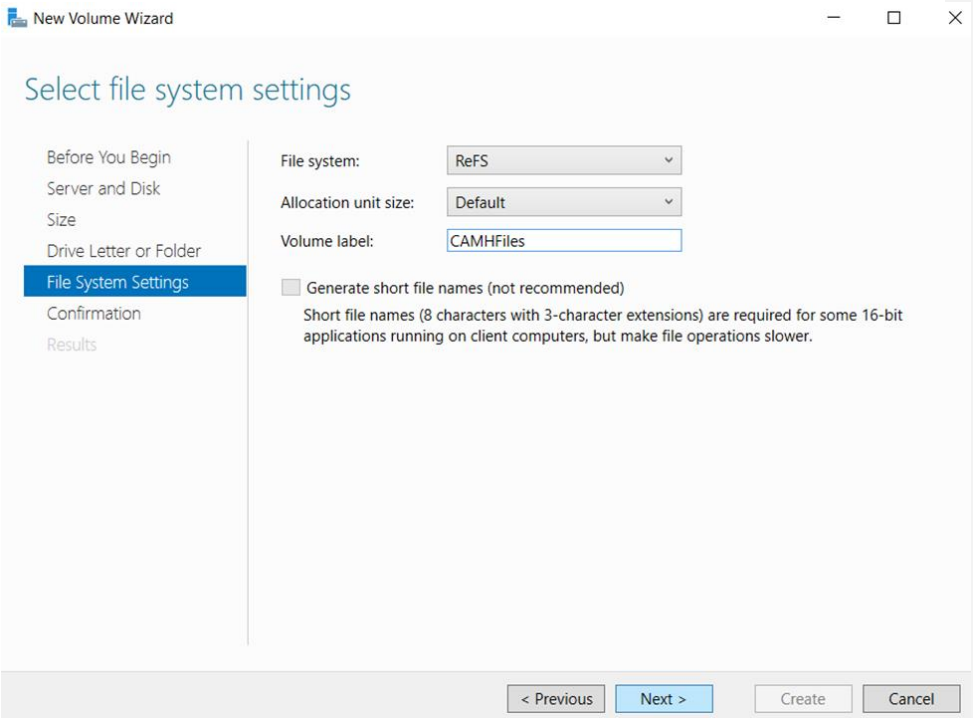
vi. Once the creation process completed the New Volume Wizard window will appear.



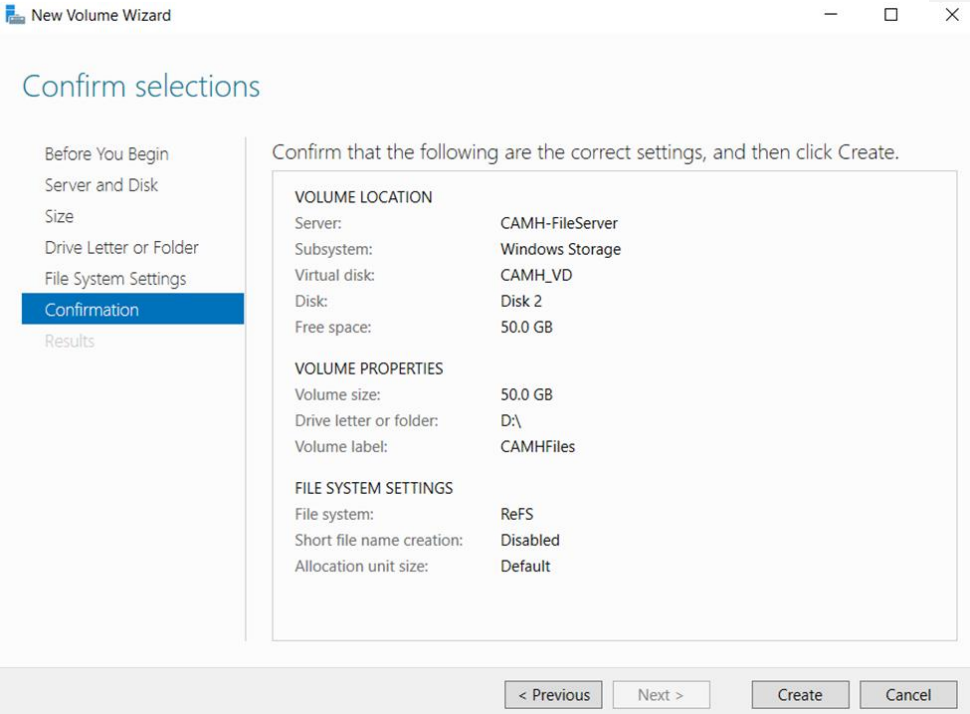
vii. Click Next in the New Volume Wizard. Select the virtual disk and click on Next. Set the volume size to its capacity, assign a Drive letter to the volume, and click Next.



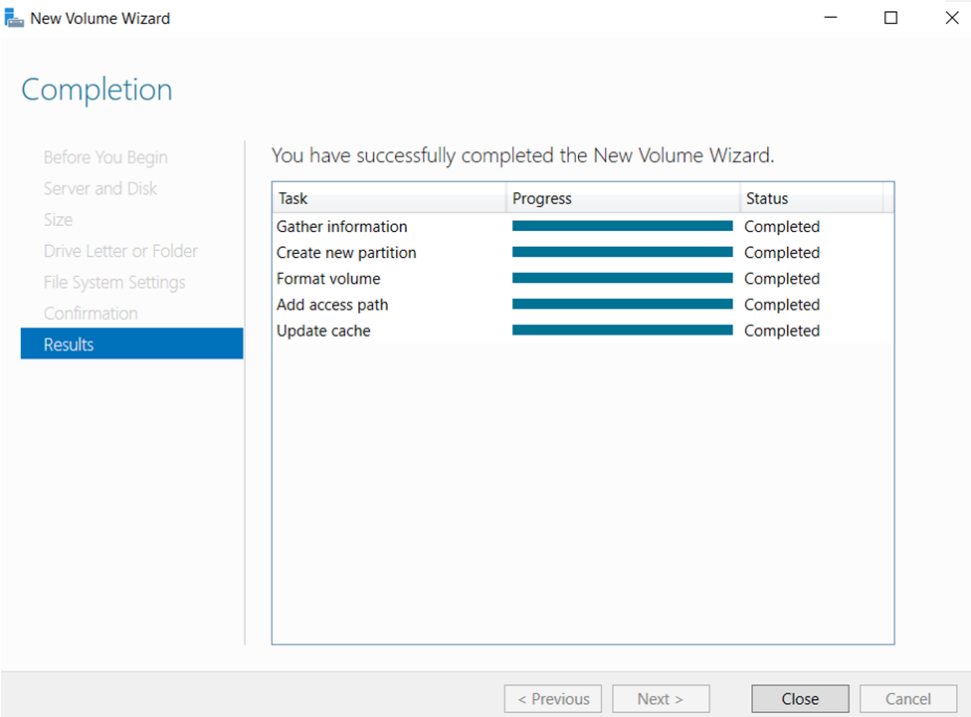
viii. Change the File system to ReFS and name the volume label as CAMHFiles.



ix. Confirmed the final settings and click create.



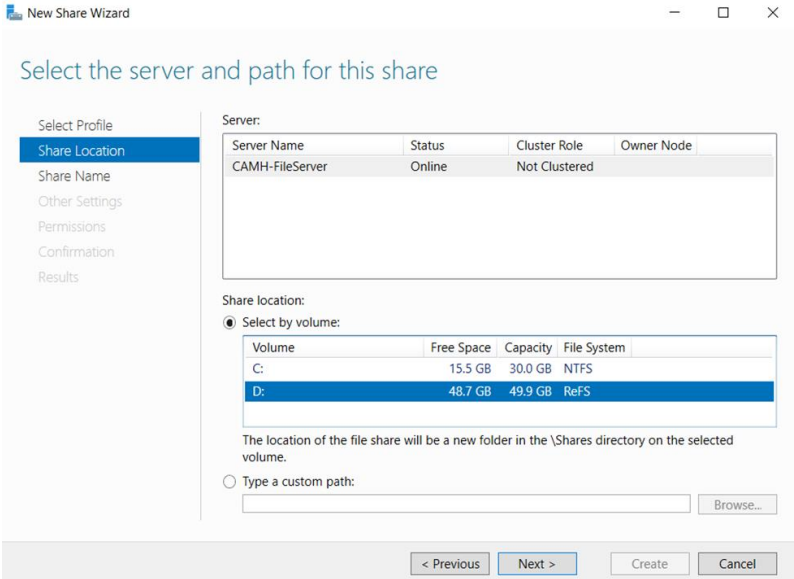
x. The successful completion window will appear.



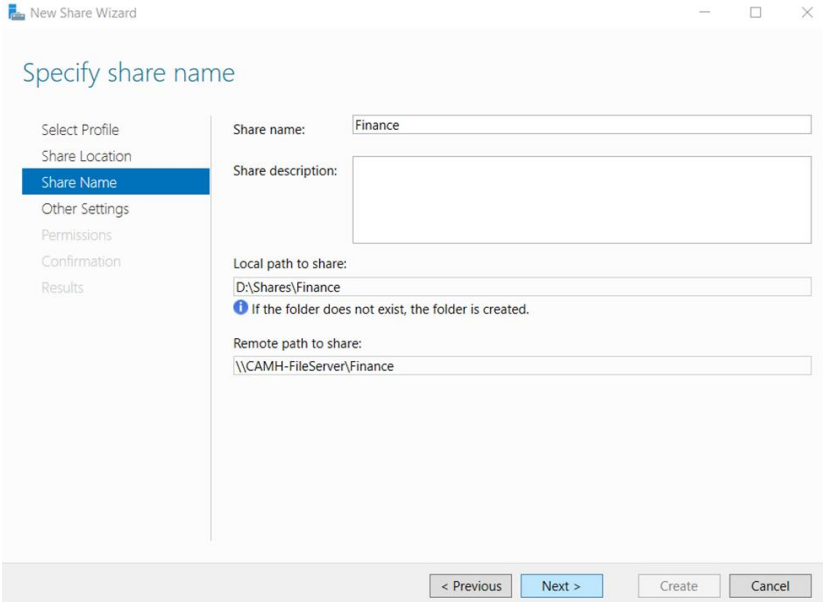
Step 4 – Creating a file share

i. In Server Manager, click on File and Storage Services -> Shares. Click on to create a file share, start the New Share Wizard

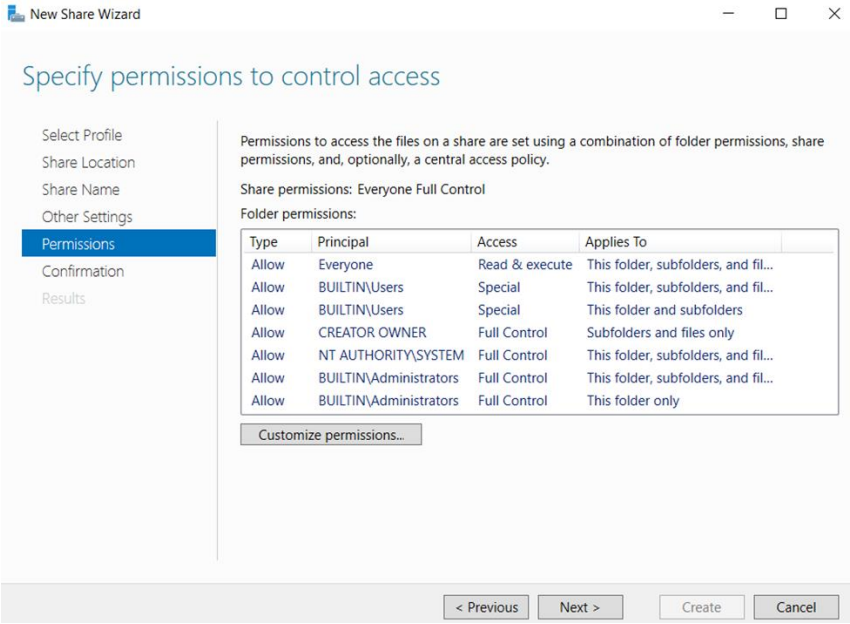
ii. Select the desired volume and click next.



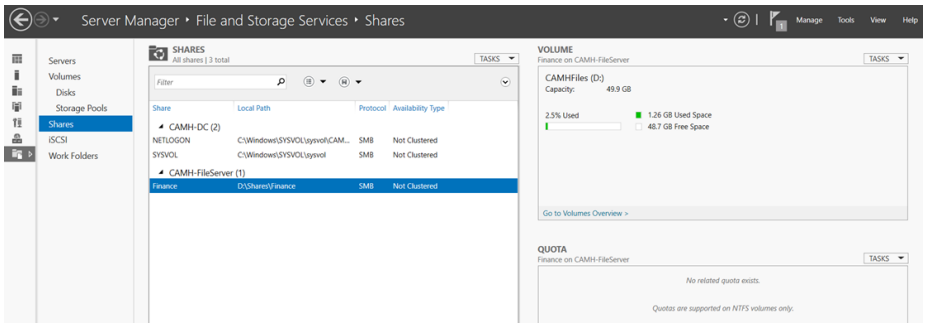
iii. Label the share folder as Finance for finance department.



iv. Permission can be edited on permission window while creating the shared folder



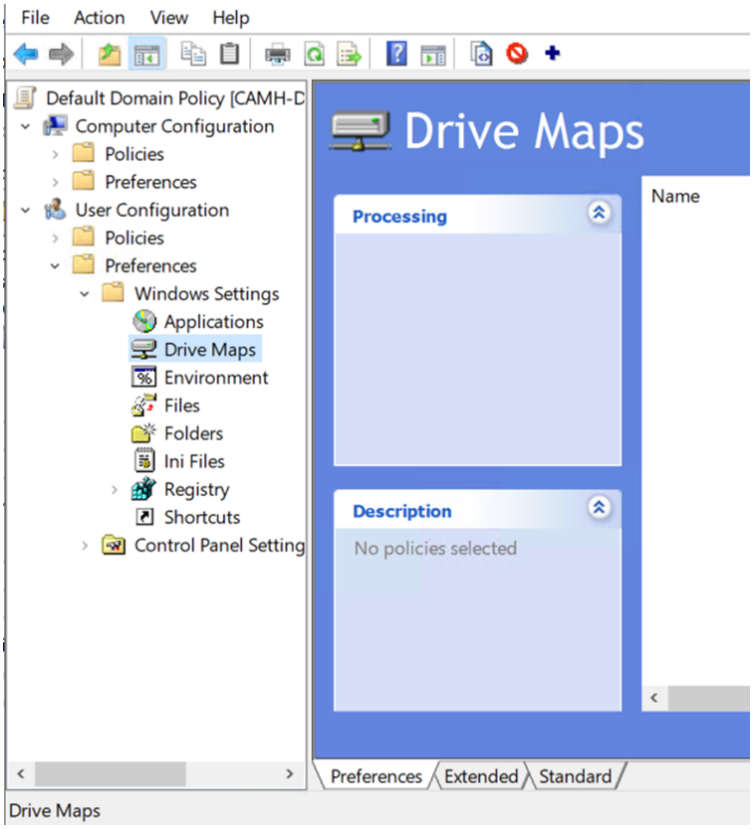
v. Click create on next window. It will appear under share option on server manager



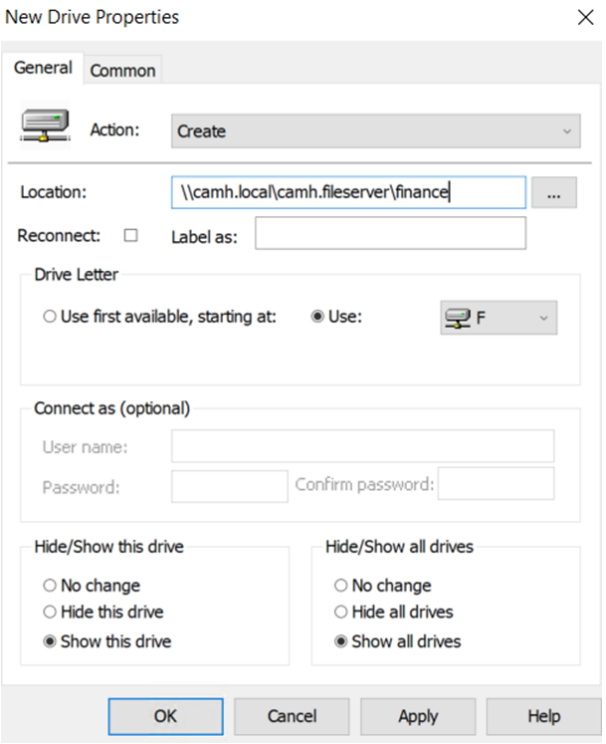
Step 5 – Mapping the network drive via Group Policy

i. Open Group Policy Management from the start menu. Right click on Default Domain Policy and click on Edit. In the Group Policy Management Editor, click on User Configuration -> Preferences ->

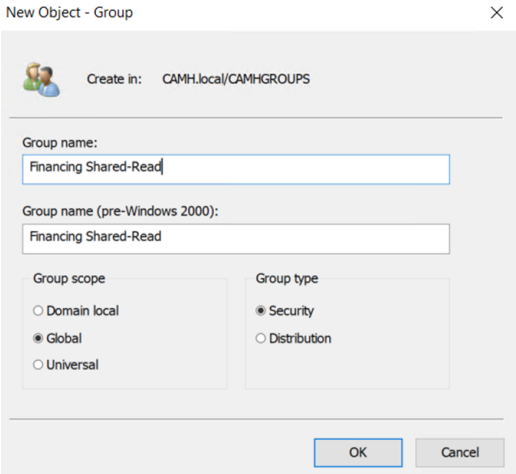
Windows Settings. Right click on Drive Maps and choose New -> Mapped Drive



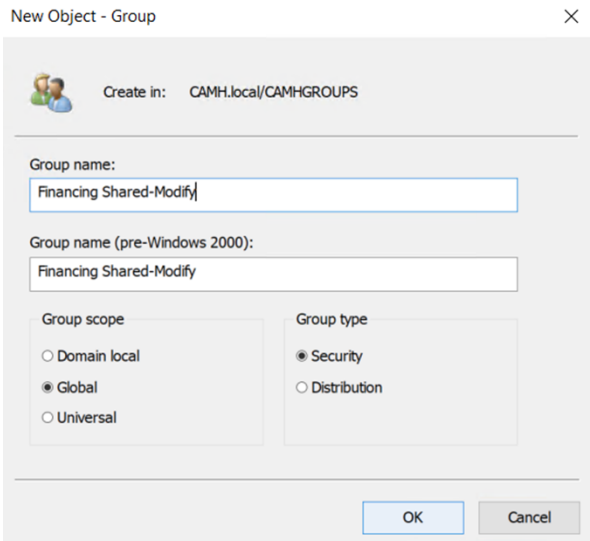
ii. In Action drop down manual, select Create. Use the full UNC path for the drive location. Set a drive letter as well. Select Show this drive and Show all drive in the bottom two sections. Click OK.



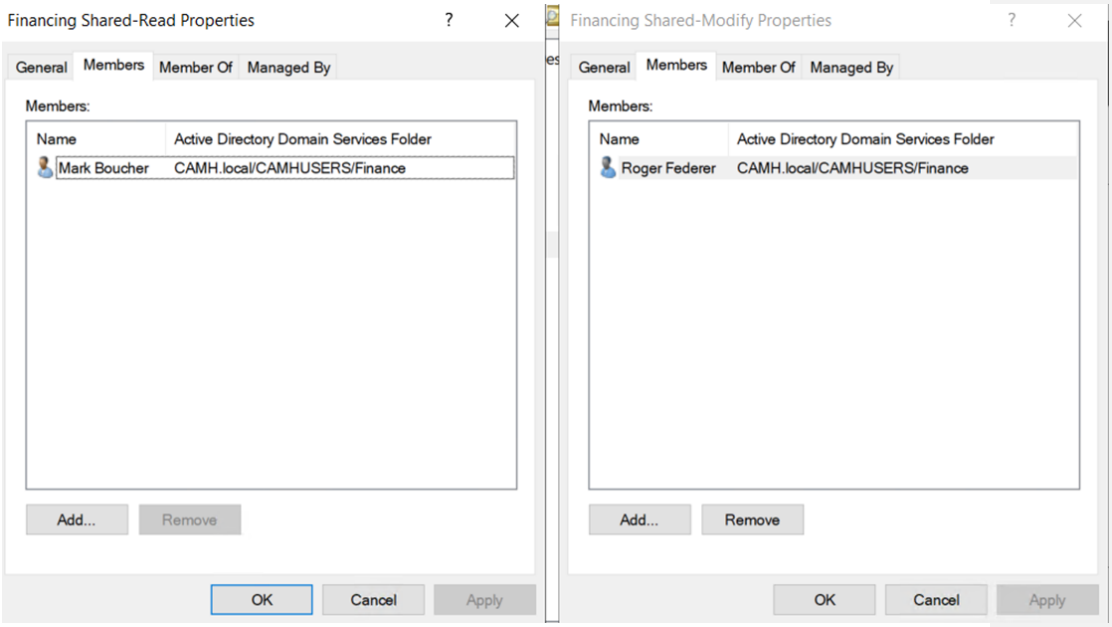
iii. Set the permission for shared folder.



iv. Create security group for Financing Shared-read and Financing Shared - modify.

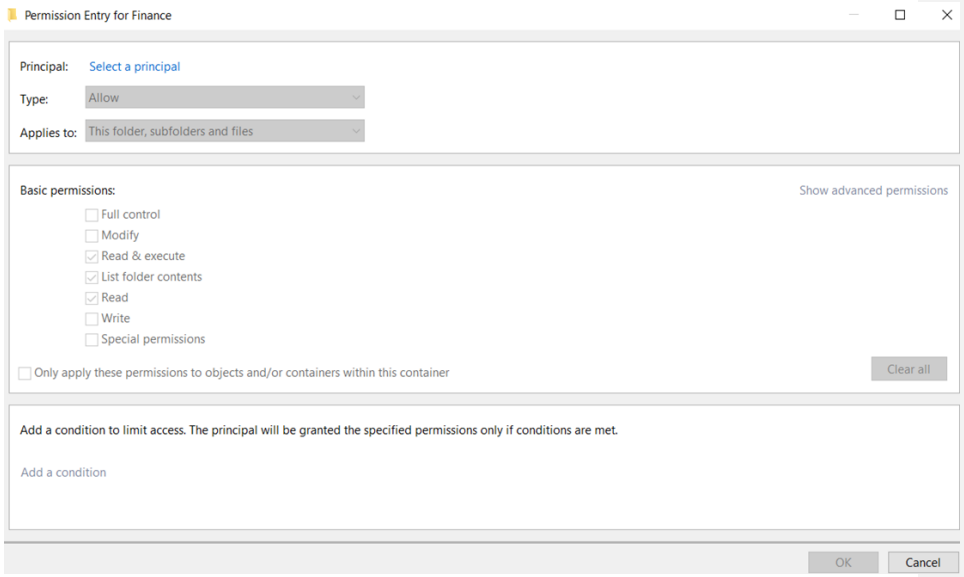


v. Add members two different groups

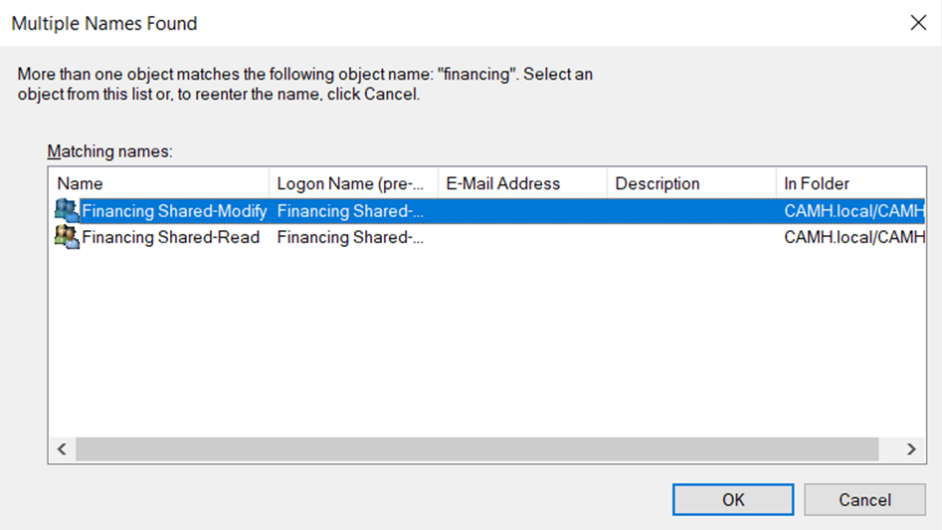


vi. In File Server, go to the network folder and right click on Financing -> Properties -> Security -> Advanced. In the pop-up window, click on

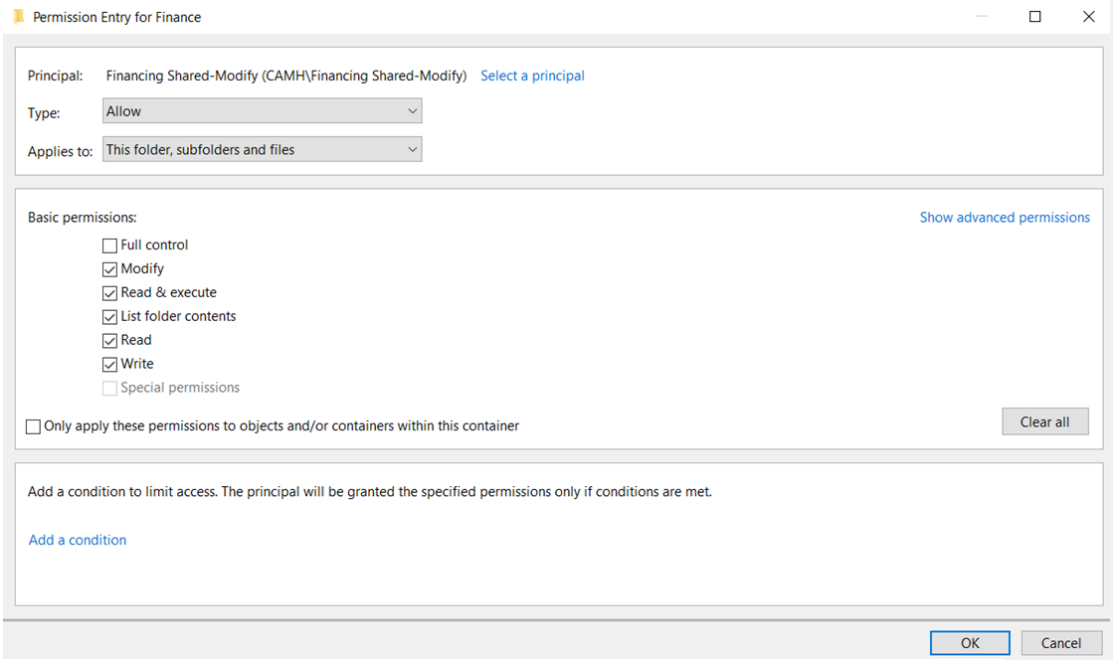
Add. In the Permission Entry for Accounting window, click on Select a principal.



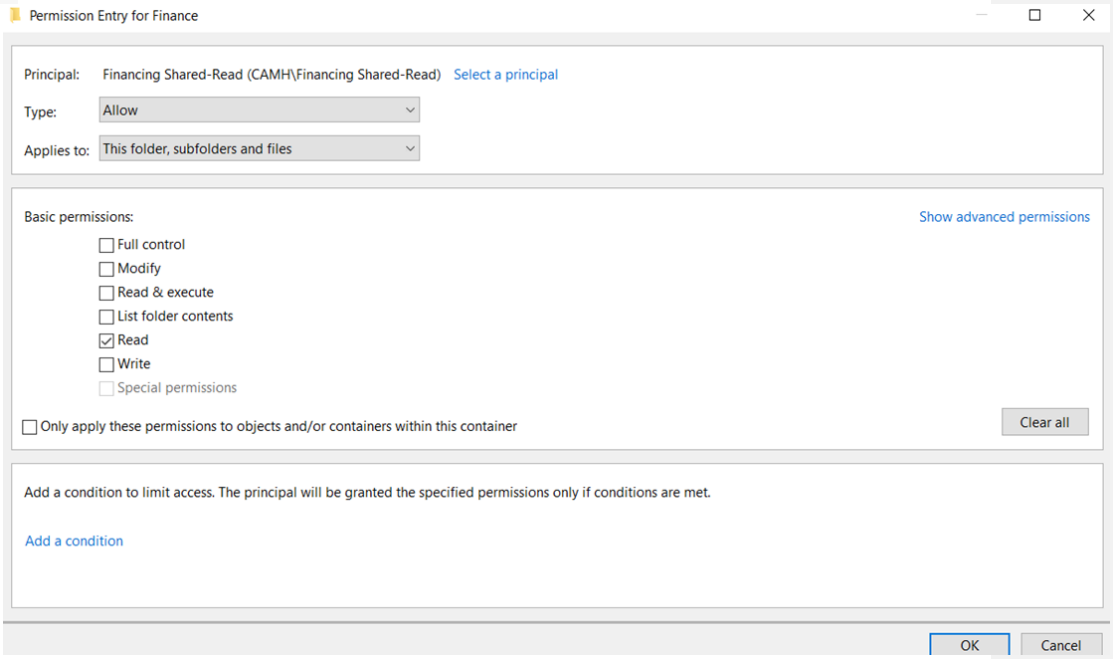
vii. Enter Financing in the pop-up window and Financing Shared-Modify and click OK twice.



viii. In the Basic permissions section, check the Modify checkbox and click OK.

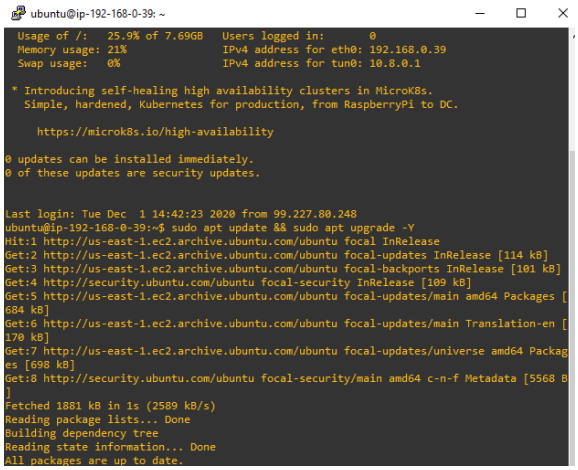


ix. Add read group for Financing shared folder and select only Read permission.



Part 5 – Ubuntu Server PiVPN configuration

i. Run "sudo apt update && sudo apt upgrade -Y" to ensure the latest Ubuntu repositories have been installed on the instance

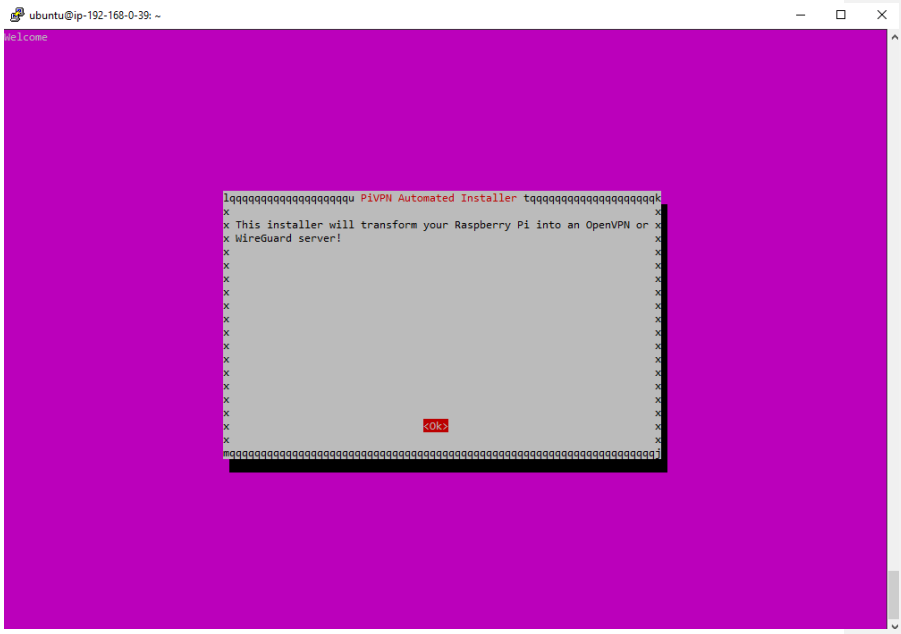


ii. Once the update and upgrades have completed, install the PiVPN with command

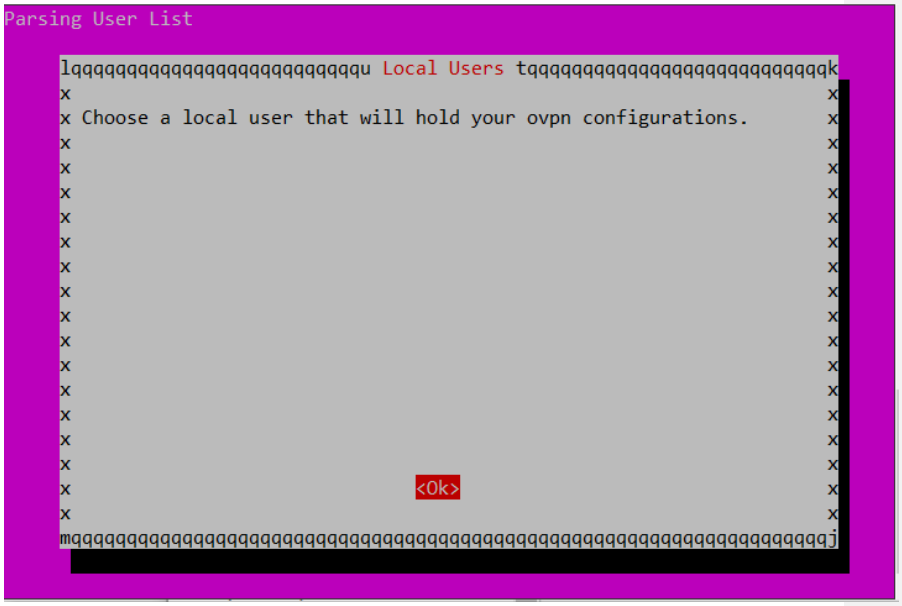
“sudo curl -L https://install.vpn.pivpn.io | bash”

```
ubuntu@ip-192-168-0-39:~$ sudo curl -L https://install.pivpn.io | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   162  100   162    0     0    465      0 --:--:-- --:--:-- --:--:--   465
100 83088  100 83088    0     0   142k      0 --:--:-- --:--:-- --:--:-- 1071k
```

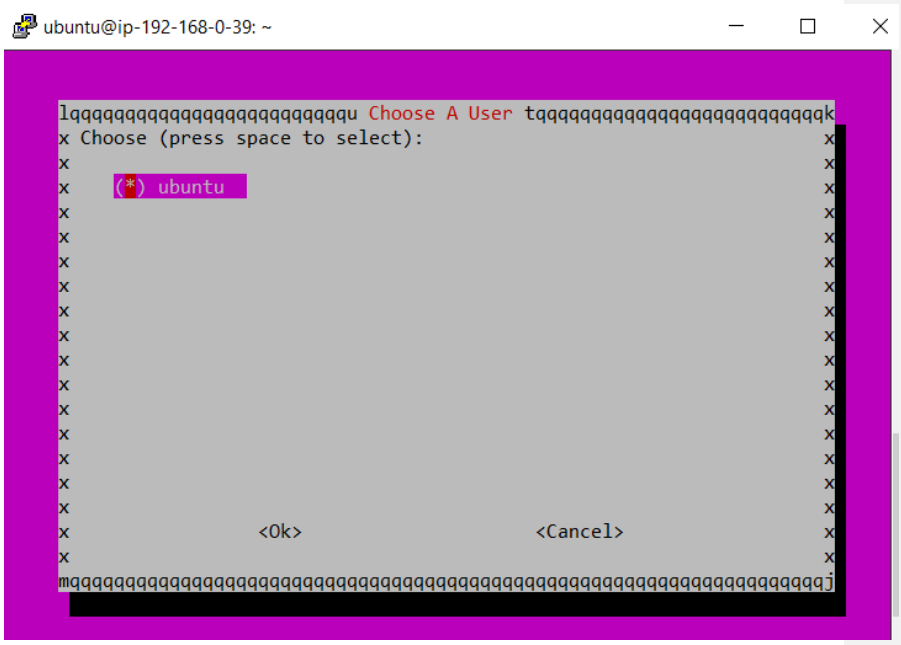
iii. The installation starts with PiVPN automatic installer



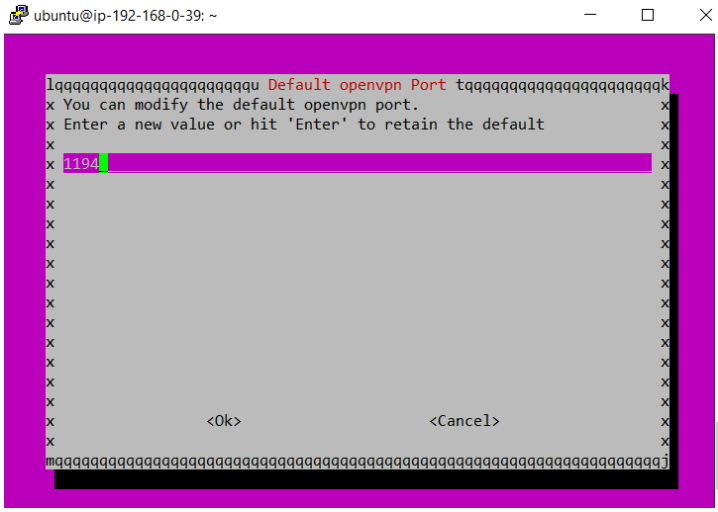
iv. The installer asks for the location for the OVPN files to be saved to later retrieval, once the destination is selected select “Ok” to continue



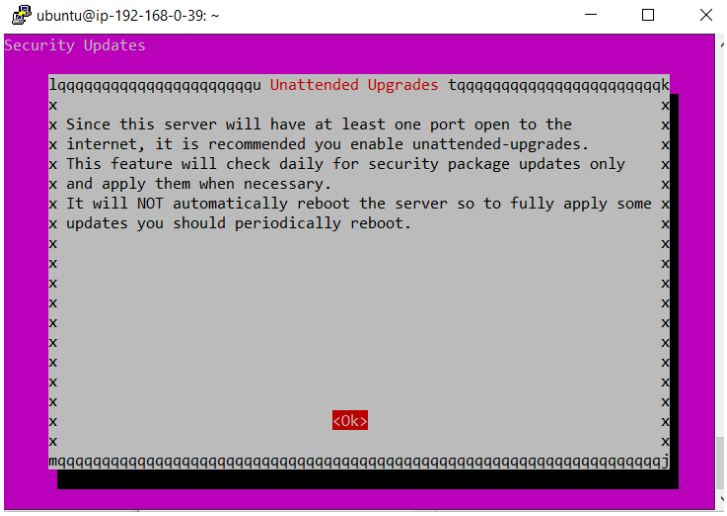
v. The installer asks for a server instance to install PiVPN onto, select the Ubuntu instance and select “Ok”



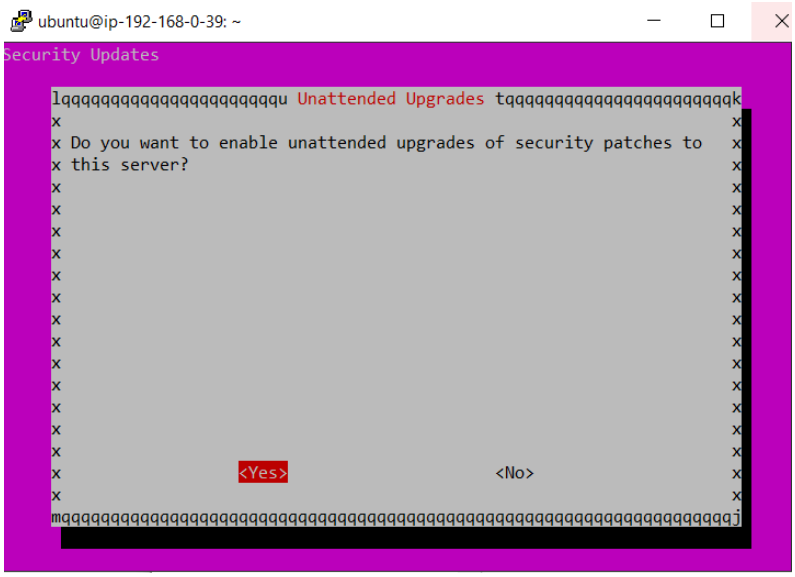
vi. The installer asks for the port to be used for PiVPN service, leave the default port "1194" and select "Ok". Ensure the port is permitted in the security group settings to allowed connections.



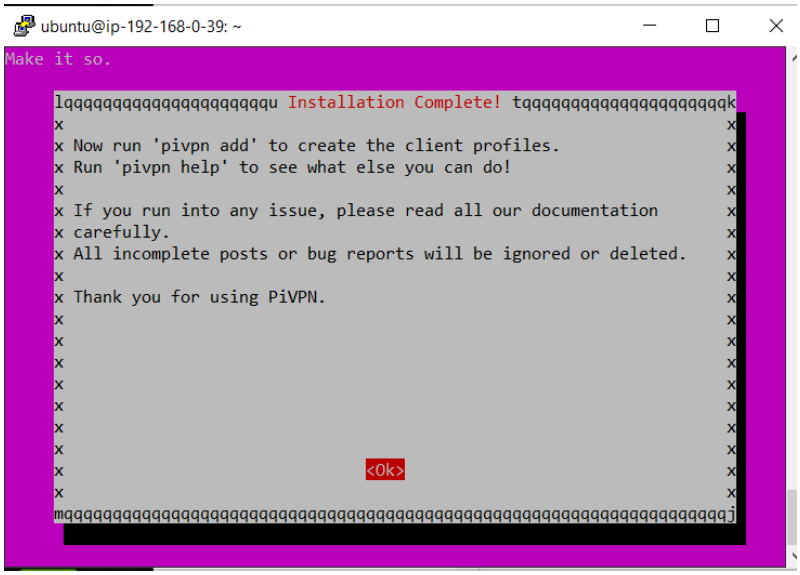
vii. The installer advises to enable "Unattended Upgrade" to ensure the install is up to date



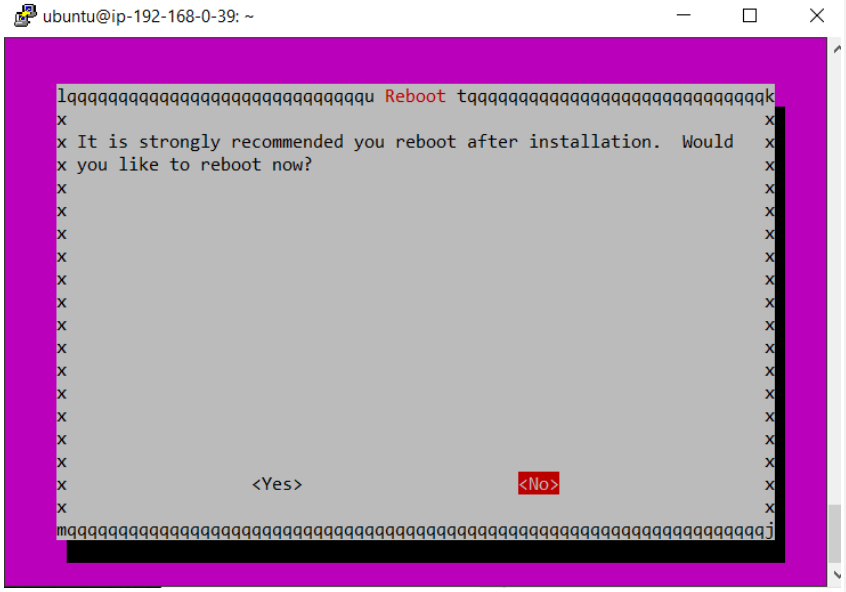
viii. Select "Yes" to enable the "Unattended Upgrades"



ix. The installation is complete and the OVPN profiles need to be created for user to connect to the VPN server remotely



x. Once the process is complete reboot the system to finalize the install



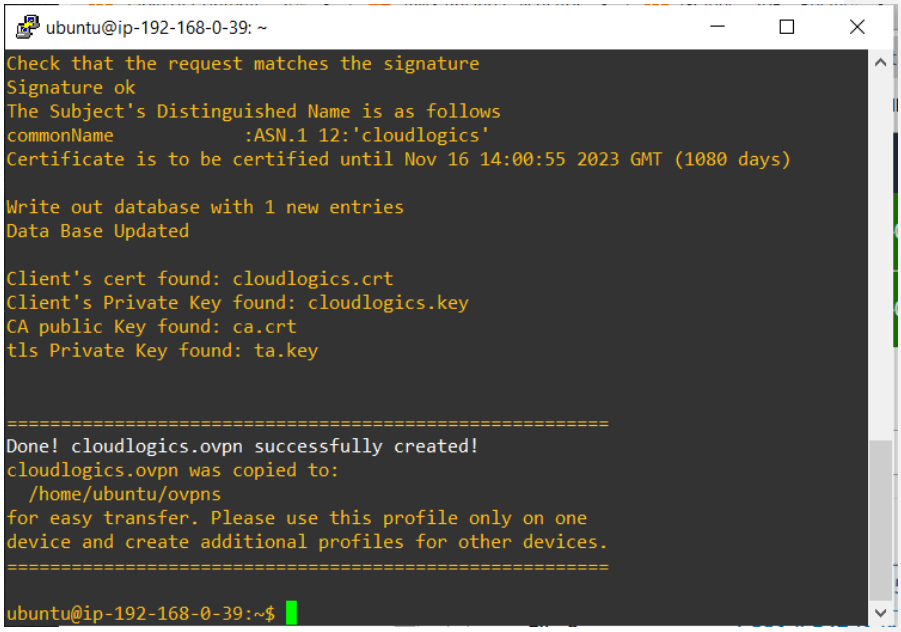
xi. The system starts the reboot sequence

```
PuTTY (inactive)
Xn

An updated CRL has been created.
CRL file: /etc/openvpn/easy-rsa/pki/crl.pem

./easyrsa: 341: set: Illegal option -o echo
Adding system user `openvpn' (UID 113) ...
Adding new group `openvpn' (GID 119) ...
Adding new user `openvpn' (UID 113) with group `openvpn' ...
Creating home directory `/var/lib/openvpn/' ...
::: Install Complete...
::: Restarting services...
:::    Checking for unattended-upgrades... already installed!
/usr/bin/debconf-apt-progress: can't open /tmp/tmp.SOzw7lCTOw: Permission denied
 at /usr/bin/debconf-apt-progress line 249, <STDIN> line 3.
::: Setupfiles copied to /etc/pivpn/openvpn/setupVars.conf
::: Installing scripts to /opt/pivpn...
 done.
::: Flushing writes to disk...
::: done.

Rebooting system...
:::
ubuntu@ip-192-168-0-39:~$
```

xii. When the system reboots, client OVPN need to be created to remote connections, in the CLI enter command “pivpn add” to start the process, when prompted enter the client name, password twice, and hit “Enter” to finish the process

```
ubuntu@ip-192-168-0-39: ~
0 updates can be installed immediately.
0 of these updates are security updates.


Last login: Tue Dec  1 13:51:37 2020 from 99.227.80.248
ubuntu@ip-192-168-0-39:~$ pivpn add
::: Create a client ovpn profile, optional nopass
:::
::: Usage: pivpn <-a|add> [-n|--name <arg>] [-p|--password <arg>]|[nopass] [-d|-
-days <number>] [-b|--bitwarden] [-i|--iOS] [-o|--ovpn] [-h|--help]
:::
::: Commands:
:::  [none]               Interactive mode
:::  nopass               Create a client without a password
:::  -n,--name            Name for the Client (default: 'ip-192-168-0-39')
:::  -p,--password        Password for the Client (no default)
:::  -d,--days            Expire the certificate after specified number of days
(default: 1080)
:::  -b,--bitwarden       Create and save a client through Bitwarden
:::  -i,--iOS             Generate a certificate that leverages iOS keychain
:::  -o,--ovpn            Regenerate a .ovpn config file for an existing client
:::  -h,--help            Show this help dialog

Enter a Name for the Client:
```

xiii. The process is complete and the OVPN file has been created and ready for use



TROUBLESHOOTING

AWS Cloud

REMOTE CONNECTION TO AWS INSTANCE ISSUES

External Access

Connecting to any instance does not work because the instances are on private subnet and do not have globally routable IP address to be accessed externally. Thus, "cloudlogics_PUBLIC" is created with a globally routable IP address that is accessed externally. The public server is then connected to the internal network, allowing access to all instances via RDP connection.

Connection Time Out Issues

If connection to the instances is timing out, Security settings need to be verified for potential blocks. Navigate to the Security tab at the bottom of the Management Console page and click on ***Inbound rules.*** Verify the following permissions are in place:

- For Windows instances: check that port 3389 (RDP) is permitted
- For Linux/Unix instances: check that port 22(SSH) is permitted

If the security group does not have the above rules assigned, navigate to the Security Group page. On the ***Inbound rules***, click on ***Edit rules***, then ***Add rule*** and for ***Type*** choose SSH. For source select ***Custom*** and enter the IP address of the desired machine in CIDR notation. When complete, select ***Save rules*** to complete the process.

Server Connection Unexpectedly Terminated

When connected to an instance via PuTTY is possible the connection to be terminated with a warning message "***Server unexpectedly closed network connection***". The cause could be the keepalives in PuTTY configuration settings is not enabled. Some servers disconnect remote clients when they have not received any communication for a specified period. Ensure the PuTTY configuration settings is set to 59 seconds between keepalives to maintain the connection.

Windows Administrator Forgotten Password

If the Windows Administrator password has been lost, a recovery of the instance could be performed to regain administrative access. The below procedure only work if the original private key that was used for the instance's launch is available.

To the reset the password please follow these steps:

1. Verify that the EC2Launch v2 is running
    a. Open the AWS EC2 Management Console and navigate to Instances
    b. Select the instance that requires a password reset
    c. Then choose ***Action, Monitor and troubleshoot, Get sys log***
    d. Locate the EC2 launch record, (e.g. Launch: EC2Launch v2 service v1.0.421). If the launch record is present, the service is running, and password reset could be performed
2. Disconnect the Root volume from the instance
    a. Open the AWS EC2 Management Console and navigate to ***Instances***

b. Select the instance that requires the password reset and choose ***Actions, Instance state, Stop instance***. Wait for the instance's state to change to ***Stopped*** before proceeding to the next step

3. New key pair must be created for the instance to allow access, but the original key must be deleted first
    a. Delete the original key first
    b. Create a new key using the AWS EC2 Management Console
    c. Select the affected instance, note the instance type, subnet, security group assigned, IAM role, and VPC, which is needed later in process
    d. Select ***Actions, Image and templates, Create image***
    e. Create a new instances and apply the previously used cloud security key.

Network Management

One of the more common problems reported about the SolarWinds Orion software is services 'flapping', meaning they cannot start. This can be cause by many different issues, so there several steps to troubleshooting this problem.

Step 1. - Check SolarWinds Log Files

- C:\ProgramData\SolarWinds\Logs\Orion - (OrionWeb.log- Web Console Related Logs)
- C:\ProgramData\SolarWinds\InformationService\v3.0\ Solarwinds.InformationService.log)
- C:\ProgramData\SolarWinds\JobEngine.v2\Logs (Polling-Related Logs)

Step 2 – Check Windows Events/Errors for SolarWinds related Services

In in Windows navigate to Windows Events, then expand the Windows Logs, open Application and Service Logs and choose Solarwinds,net. We can then filter this file for error messages to help isolate the error causing the problem. As SolarWinds comes with a highly available support team, IT members can contact support for their expertise. This is an important point to emphasize with the Network Manager for CAMH, that his/her staff have high level SolarWinds analysts at their disposal 24 hours a day, 7 days a week.

Step 3 – Check MSQM is set to 0 on all Polled clients

- Go to Computer Management tab, and open Services and Application. Then open Message Queuing, Private Queues and make sure all values are set to 0. Ensure none are set to Q

Step 4 – Check Server Statistics and Settings

- Check disk space available on the SolarWinds server/database server.
- Ensure SQL Express Edition (10GB limit) isnt being used
- Check for Windows updates or pending updates. Complete them and restart the server.

Step 5 – Use the SolarWinds Service Configuration Wizard

- Log into the SolarWinds server with administrator credentials.
- Navigate to the Control Panel and select Programs and Features
- Right-Click SolarWinds Orion Core Services and select repair.

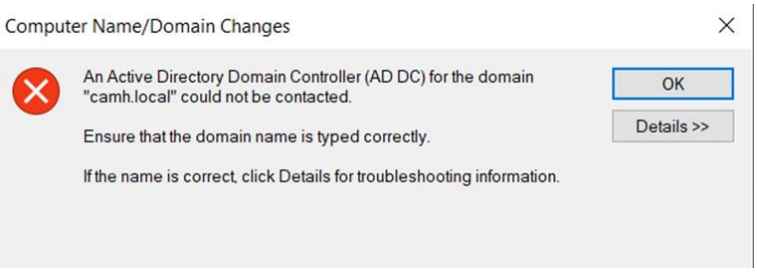
It is important to resolve the services 'flapping' problem in the correct order. Skipping right to the repair Wizard will not help indicate whether there is sufficient disk space available, or if the MSQM values are correctly set. As with most troubleshooting issues, methodically following the steps in correct order will produce the best results.

SolarWinds has the benefit of being very user friendly and options to help easily identify problem nodes. The SolarWinds dashboard has a NPM Summary tab to view an overall summary. There is also a Top Ten tab that will show existing health problems with network nodes. From this tab there are a series of Top Ten issues including Top 10 Interfaces by Utilization and Top 10 Nodes by Percent Packet Loss. This information can help the CAMH IT staff identify and resolve problem nodes.

Server Management

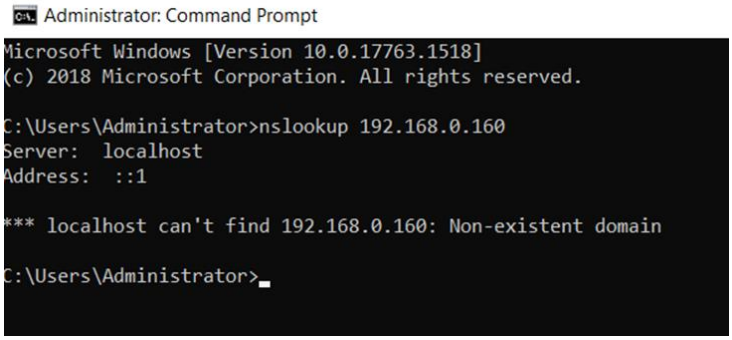
TROUBLESHOOTING DNS SERVER

When we try to connect first server to domain. It prompts following window even though DNS IP address was updated on the server.

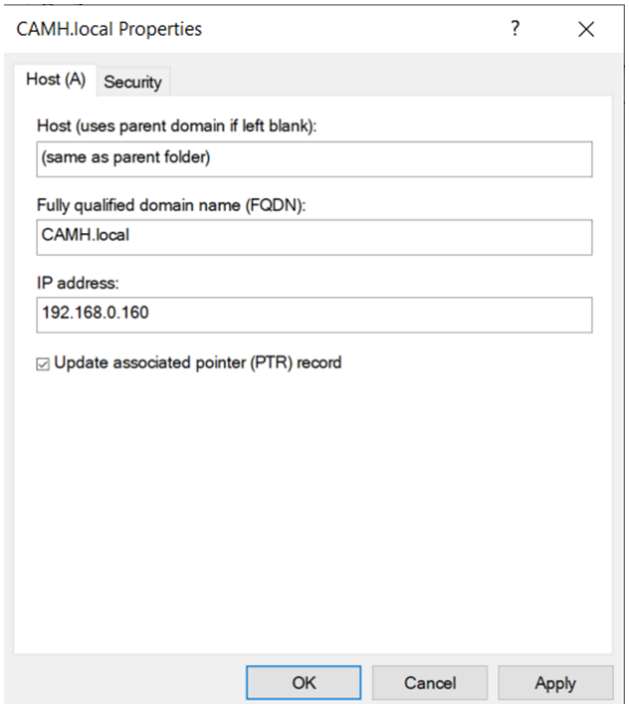


On further research we find out that DNS server is not resolving IP address to its name.

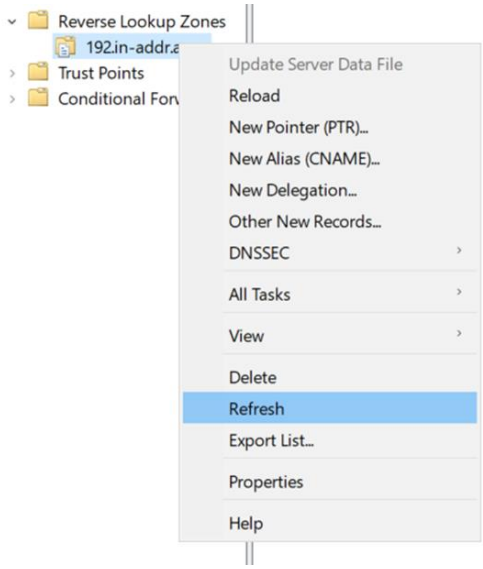
We ran nslookup command. See the result



i. Navigate to DNS services and expand “CAMH.local” and then click “Forward lookup zones”
ii. Open the properties of server and then check the box “Update the associated pointer (PTR) record”



iii. Expand “Reverse Lookup Zones” and right click on “192.in-addr.arpa” and refresh it.



iv. Verify the nslookup command and see it resolve the IP address to name and vice versa

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup 192.168.0.160
Server:  localhost
Address:  ::1

Name:    camh.local
Address:  192.168.0.160


C:\Users\Administrator>
```

Command Prompt

```
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\k.star>nslookup 192.168.0.160
Server:  camh.local
Address:  192.168.0.160

Name:    camh.local
Address:  192.168.0.160


C:\Users\k.star>
```

Network Security

Troubleshooting network security for the on-site model starts with the Cisco 5505 ASA and its configurations. An often-used tool in network troubleshooting is the 'ping' command. After configuring the ASA we tried a series of ping test to show connectivity to the outside network. Initially these ping tests were unsuccessful.

```
CAMH-InternalRouter#ping 172.16.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

After researching online resources, it became apparent that the unsuccessful pings were due to the default settings of the ASA. For security purposes the global-policy map does not support the inspection of several protocols, one of those being ICMP packets. Fortunately, there is an easy fix. All we need to do is create a separate policy-map that enables ICMP traffic.

```
!
class-map kris
 match default-inspection-traffic
!
policy-map kris2
 class kris
  inspect icmp
!
service-policy kris2 global
!
```

After completing this step, we again attempt a ping to the Outside network and get a successful result. The first ping result does show some packet loss but this is only to the

delay in updating the ARP table. A second ping test shows connectivity with no packet loss.

```
CAMH-InternalRouter#ping 172.16.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms

CAMH-InternalRouter#ping 172.16.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Commented [HF4]: Analysis of result, conclusion and recommendation are not done

REFERENCES:

Table #. Cloud provider vs. End-user – Responsibilities

What is shared responsibility in the cloud? (2020, June 05). Retrieved November 14, 2020, from https://cloudcheckr.com/cloud-security/shared-responsibility-model/?gclid=CjwKCAiA-_L9BRBQEiwA-bm5fnIHcjFxEnf6jNqWdtA5XMWFbeZh24AQbBAxbOj1lWLRqSgeyhsDyBoC61QQAvD_BwE

What is Wireless LAN Controller, Job Description and Salary? (n.d.). Retrieved November 20, 2020, from https://www.fieldengineer.com/skills/wireless-lan-controller

JumpCloud. 2020. How Does RADIUS Improve Wifi Security? - Jumpcloud. [online] Available at: <https://jumpcloud.com/blog/radius-improve-wifi-security> [Accessed 9 November 2020].

AWS. (n.d.). *Cloud Security Resources - Amazon Web Services (AWS)*. Retrieved from https://aws.amazon.com/security/security-resources/

Alert Logic. (n.d.). *AWS Security – Amazon Web Services Security Monitoring*. Retrieved from https://www.alertlogic.com/solutions/platform/aws-security/

SolarWinds (n.d.). *Network Performance Monitor - Network monitoring software designed to reduce network outages and improve performance*. Retrieved from https://www.solarwinds.com/network-performance-monitor