AT1 Template

This template is created based on the marking criteria of AT1 along with the assessment requirements. You are required to follow the instructions to attach the lab results as required below each Heading and remove all the red text instructions when you complete the portfolio.

For the first attempt, please name your portfolio after the format of *Firstname_Lastname*_AT1_Attempt_1 and submit it to Connect.
For the second attempt, please name your portfolio after the format of *Firstname_Lastname*_AT1_Attempt_2 and submit it to Connect

Lab 1 Results

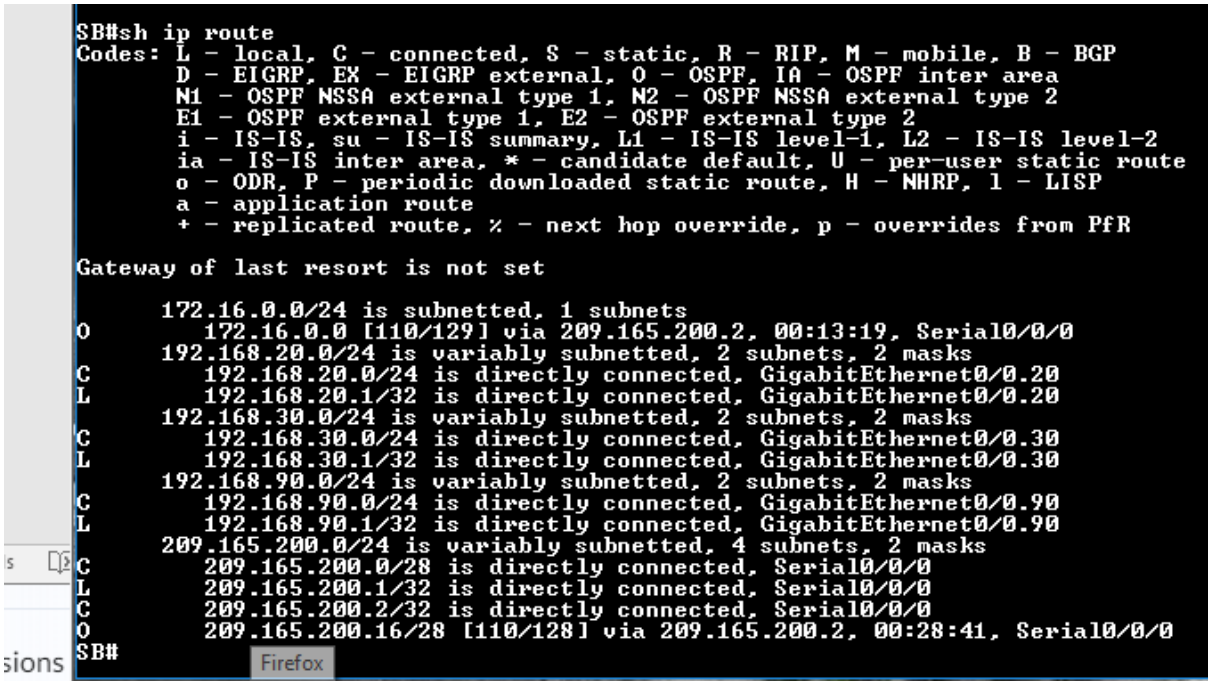
a. Show interface s0/0/0 on the SB Router to verify the ppp encapsulation and take a screenshot and paste it below.

```
SB#sh interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 209.165.200.1/28
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:08, output hang never
  Last clearing of "show interface" counters 01:26:19
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2767 packets input, 99248 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     108 runts, 0 giants, 0 throttles
     125 input errors, 17 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     2935 packets output, 108166 bytes, 0 underruns
     0 output errors, 0 collisions, 355 interface resets
     29 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

b. Show run on the SB Router and take a screenshot of the commands that configure interface s0/0/0 as ppp encapsulation and ppp authentication.

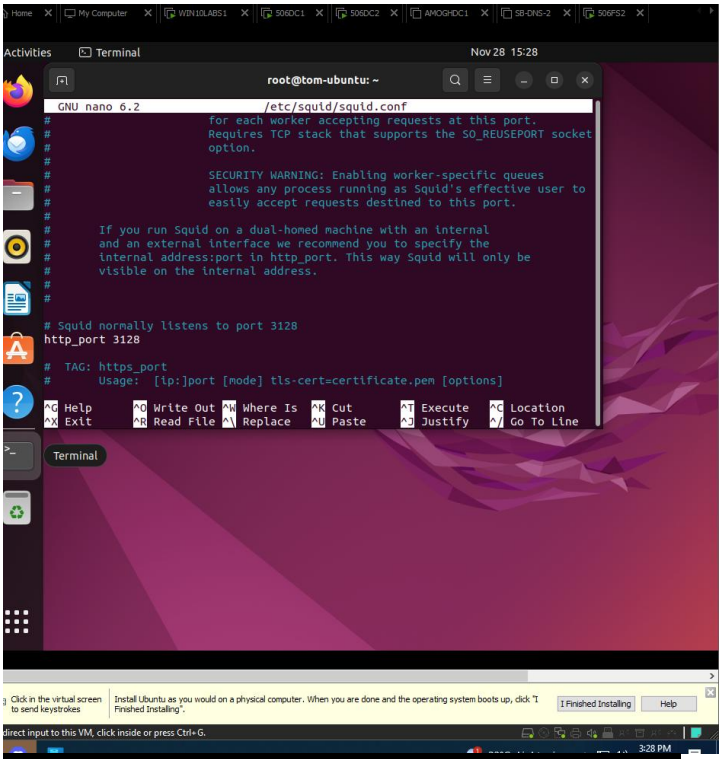
```
SB#sh run int s0/0/0
Building configuration...

Current configuration : 115 bytes
!
interface Serial0/0/0
 ip address 209.165.200.1 255.255.255.240
 encapsulation ppp
 ppp authentication chap
end
```

c. Show ip route on the SB Router to verify the OSPF routing information and take a screenshot and paste it below.

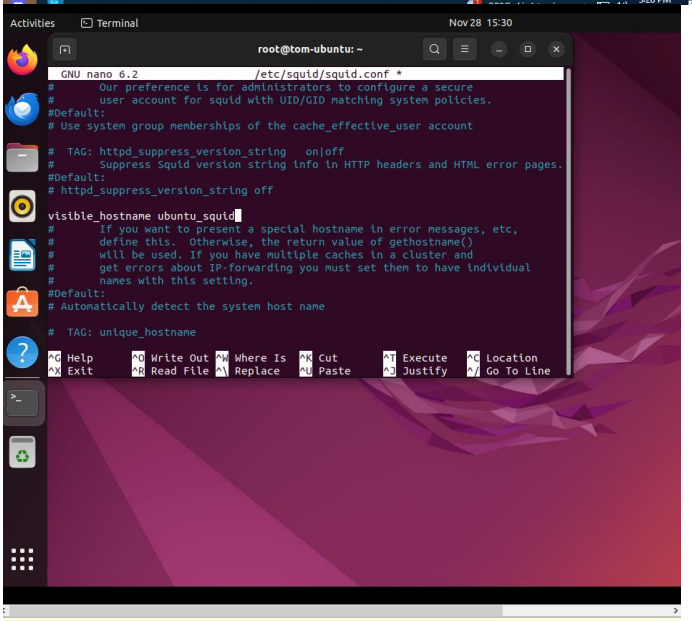


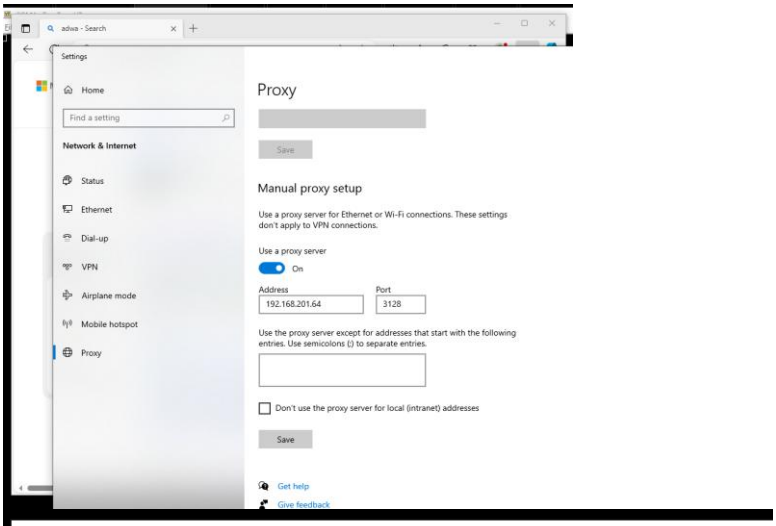
Lab 2 Results

a. Display the NAT table by issuing the show ip nat translations command on the SB Router. Take a screenshot and paste it below.
b. Install a simple proxy server and configure proxy client settings on a Windows PC. Demonstrate the proxy services running with screenshots. Briefly describe what is proxy.
c. A proxy server is a critical intermediary component in network infrastructure. It plays a pivotal role in managing and controlling client-server communication. When a client requests access to a resource, the proxy server acts as a go-between, forwarding the request to the destination server on behalf of the client. One of its essential functions is caching, where frequently accessed content is stored locally. This cache improves network performance by serving this cached content to clients, reducing the load on the destination server and saving bandwidth. Moreover, proxies can provide a layer of anonymity for clients by masking their IP addresses, which is often used for privacy and security reasons. Additionally, they serve as a security barrier, inspecting incoming and outgoing traffic, detecting and blocking malicious activity based on predefined rules.


Activities
Terminal
Nov 28 15:28
root@tom-ubuntu: ~
GNU nano 6.2 /etc/squid/squid.conf
for each worker accepting requests at this port.
Requires TCP stack that supports the SO_REUSEPORT socket
option.
SECURITY WARNING: Enabling worker-specific queues
allows any process running as Squid's effective user to
easily accept requests destined to this port.
If you run Squid on a dual-homed machine with an internal
and an external interface we recommend you to specify the
internal address:port in http_port. This way Squid will only be
visible on the internal address.
Squid normally listens to port 3128
http_port 3128
TAG: https_port
Usage: [ip:]port [mode] tls-cert=certificate.pem [options]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line
Terminal

Click in the virtual screen to send keystrokes
Install Ubuntu as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
direct input to this VM, click inside or press Ctrl+G.
3:28 PM


Activities
Terminal
Nov 28 15:30
root@tom-ubuntu: ~
GNU nano 6.2 /etc/squid/squid.conf *
Our preference is for administrators to configure a secure
user account for squid with UID/GID matching system policies.
#Default:
Use system group memberships of the cache_effective_user account
TAG: httpd_suppress_version_string on|off
Suppress Squid version string info in HTTP headers and HTML error pages.
#Default:
httpd_suppress_version_string off
visible_hostname ubuntu_squid
If you want to present a special hostname in error messages, etc,
define this. Otherwise, the return value of gethostname()
will be used. If you have multiple caches in a cluster and
get errors about IP-forwarding you must set them to have individual
names with this setting.
#Default:
Automatically detect the system host name
TAG: unique_hostname
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

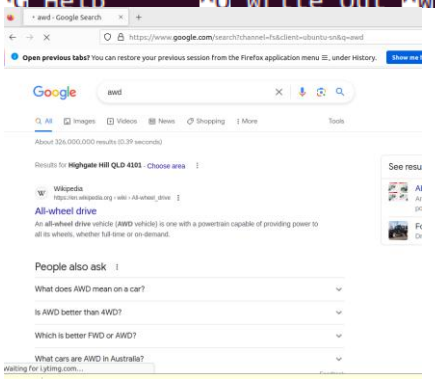


Select Command Prompt

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tom>ping 192.168.201.64

Pinging 192.168.201.64 with 32 bytes of data:
Reply from 192.168.201.64: bytes=32 time<1ms TTL=64
Reply from 192.168.201.64: bytes=32 time<1ms TTL=64
Reply from 192.168.201.64: bytes=32 time<1ms TTL=64
Reply from 192.168.201.64: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.201.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\tom>
```

```
root@tom-ubuntu:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:dd:6f:6a brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.201.64/22 brd 192.168.203.255 scope global dynamic noprefixrout
e ens33
       valid_lft 85813sec preferred_lft 85813sec
    inet6 fe80::5d20:be5e:f60f:e80f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@tom-ubuntu:~#
```

```
 GNU nano 6.2                    /etc/squid/squid.conf
#       Our preference is for administrators to configure a secure
#       user account for squid with UID/GID matching system policies.
#Default:
# Use system group memberships of the cache_effective_user account

#  TAG: httpd_suppress_version_string   on|off
#       Suppress Squid version string info in HTTP headers and HTML error page
#Default:
# httpd_suppress_version_string off

visible_hostname ubuntu_squid
acl localnet src 192.168.200.0/22
#       If you want to present a special hostname in error messages, etc,
#       define this.  Otherwise, the return value of gethostname()
#       will be used. If you have multiple caches in a cluster and
#       get errors about IP-forwarding you must set them to have individual
#       names with this setting.
#Default:
# Automatically detect the system host name


^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
```



Lab 3 Results

a. Briefly describe the following:

- what are the steps to configure this firewall?

The configuration you've described is for setting up a Zone-Based Firewall (ZBF) on Cisco routers. The Zone-Based Firewall is a more flexible and robust solution compared to classic firewall filtering methods. It operates by defining security zones and applying policies between these zones. Here's a step-by-step guide for configuring the Zone-Based Firewall:

Steps to Configure Zone-Based Firewall (ZBF)
Initial Configuration and Licensing

Enable securityk9 package to allow ZBF configuration.
Reload the router to enable the license.
Creating Security Zones

Define security zones, typically as "Inside" and "Internet".

Use the zone security command to create these zones.
Creating Security Policies

Define class-maps (e.g., cmap-inside) to classify traffic.
Match protocols like TCP, UDP, and ICMP in the class-map.
Creating Policy-Maps

Create policy-maps (e.g., Inside-to-Internet) to specify the actions for the traffic.
Use the policy-map type inspect command.
Creating Zone Pairs

Define zone pairs to establish policies between zones.
For example, create a zone pair from Inside to Internet.
Applying Security Policies to Zone Pairs

Apply the policy-maps to the relevant zone-pairs.
Use the zone-pair security command to associate policy-maps with zone pairs.
Assigning Interfaces to Security Zones

Assign physical and logical interfaces to the defined security zones.
Use the zone-member security command on the interfaces.
Verification and Troubleshooting

Use various show commands to verify the configuration, like show zone-pair security and show policy-map type inspect zone-pair.
To troubleshoot, you can temporarily remove interfaces from security zones.

ALL THE CONFIGURATIONS USED ARE BELOW FOR ZBF, DOCUMENTED

C. INITIAL CONFIGURATION TO RUN ZBF AND ZONE COMMANDS - NEED TO RUN THE LICENCES

```
SB
MG
!### Enabling securityk9 package###!
!### This allows ZBF to be configured properly :)###!
en
conf t
license boot module c1900 technology-package securityk9
yes

!### Need to reload switch to enable the licence properly###!
do write memory
do copy running-config startup-config

!###Press enter manually after this so it reloads###!
do reload


!### Enabling securityk9 package###!
!### This allows ZBF to be configured properly :)###!
en
conf t
license boot module c1900 technology-package securityk9
yes

!### Need to reload switch to enable the licence properly###!
do write memory
do copy running-config startup-config

!###Press enter manually after this so it reloads###!
do reload
```

Security zones are created in global configuration mode, and the command allows for zone name definition. Create two zones named Inside and Internet on both router SB and MG:

```
SB
MG
en
sh lic feat
!### creating security zones###!

conf t
zone security Inside
zone security Internet
end
show run | section zone
!##


en
sh lic feat
!### creating security zones###!
en
```

```
conf t
zone security Inside
zone security Internet
end
show run | section zone
!##
```

Step 2. Create Security Policies.
Create an inspect class-map to match traffic to be allowed from the Inside zone to the Internet zone. Because we trust the Inside zone, we allow all the main protocols, including tcp, udp, and icmp.

```
SB
MG
conf t
class-map type inspect match-any cmap-inside
match protocol tcp
match protocol udp
match protocol icmp

end
```

```
conf t
class-map type inspect match-any cmap-inside
match protocol tcp
match protocol udp
match protocol icmp

end
```

The class-map name is up to your choice. In this lab, please name the class-map from Inside zone to Internet zone as "cmap-inside". Created the class-map named "cmap-inside" on both router SB and MG.

Create an inspect policy-map named Inside-to-Internet on both router SB and MG. The policy map is to decide the fate of the selected traffic captured by a class-map.

```
SB
MG
conf t
policy-map type inspect Inside-to-Internet
class cmap-inside
inspect
end
```

```
conf t
policy-map type inspect Inside-to-Internet
class cmap-inside
inspect
end
```

Step 3. Create the Zone Pairs.
A zone pair allows you to specify a unidirectional firewall policy between two security zones. In this lab, there is only one zone pair is required, Inside to Internet. This zone-pair defines unidirectional traffic flowing from Inside to Internet and allowing the returning traffic in response to the traffic originating from the Inside to flow through, in the direction of Internet to Inside. If Internet-initiated traffic needs to flow in the Internet-to-Inside direction, another zone-pair must be created.
Create the zone-pair named Inside-to-Internet on both router SB and MG with the source is Inside and destination is Internet.
Note: the source and the destination must be consistent with the security zones name (case sensitive).

```
SB
MG
!###Defining a zone-pair for traffic flowing from Inside to Internet###!
conf t
zone-pair security Inside-to-Internet source Inside destination Internet
end
```

```
!###Defining a zone-pair for traffic flowing from Inside to Internet###!
conf t
zone-pair security Inside-to-Internet source Inside destination Internet
end
```

Verify the zone-pairs were correctly created by issuing the show zone-pair security command. Notice that no policies are associated with the zone-pairs yet. The security policies will be applied to zone-pairs in the next step.

```
SB
MG
show zone-pair security
show zone-pair security
```

Step 4. Applying Security Policies.
Associate the policy-maps to the zone-pairs on both the SB router and MG router:
Note: the inspected policy name must be consistent with the policy map defined before (case sensitive).

```
SB
MG
conf t
zone-pair security Inside-to-Internet source Inside destination Internet
 service-policy type inspect Inside-to-Internet
end
```

```
conf t
zone-pair security Inside-to-Internet source Inside destination Internet
 service-policy type inspect Inside-to-Internet
end
```

Verify the zone-pairs again by issuing the show zone-pair security command. Notice that the policies associated with the zone-pairs are now displayed.

```
SB
MG
show zone-pair security
show zone-pair security
```

To obtain more information about the zone-pairs, their policy-maps, the class-maps and match counters, use the show policy-map type inspect zone-pair command.

```
SB
MG
show policy-map type inspect zone-pair

!###Aforementioned command will not work as the zone-pair is not specified as its a one to many attribute###!
!###Using this instead...###!
show policy-map type inspect zone-pair Inside-to-Internet
!###doesnt work still so i just show the generic sessions###!
show policy-map type inspect zone-pair sessions
show policy-map type inspect zone-pair

!###Aforementioned command will not work as the zone-pair is not specified as its a one to many attribute###!
!###Using this instead...###!
show policy-map type inspect zone-pair Inside-to-Internet
!###doesnt work still so i just show the generic sessions###!
show policy-map type inspect zone-pair sessions
```

Step 5. Assign Interfaces to the Proper Security Zones.
Interfaces (physical and logical) are assigned to security zones with the zone-member security interface command.
Assign the LAN interfaces to the Inside zone on both router SB and MG. On SB router, make sure the zone-member security should be configured on each subinterface, not the physical interface:
Note: the security zone name must be consistent with the security zones defined before (case sensitive).
Note: If you need to troubleshoot with the network connectivity and not sure whether it is caused by the ZBF or the other network configuration problems, you can simply unassign the interfaces to the security zones to deactivate the ZBF and exclude the ZBF caused factors.

```
MG
SB
conf t
interface GigabitEthernet0/0.20
zone-member security Inside

interface GigabitEthernet0/0.30
zone-member security Inside

interface GigabitEthernet0/0.90
zone-member security Inside
end
```

```
conf t
interface GigabitEthernet0/0
 zone-member security Inside
end
```

Assign the WAN interfaces to the Internet zone on both router SB and MG:

SB
MG
conf t
interface s0/0/0
zone-member security Internet
end

conf t
interface s0/0/0
zone-member security Internet
end

- what are firewall applications?

Firewalls, including Zone-Based Firewalls, are used in various applications:

Network Security

Protect internal networks from unauthorized external access.
Control traffic based on policies and rules.
Virtual Private Network (VPN)

Secure VPN connections for remote access or site-to-site VPNs.
Intrusion Prevention and Detection

Some advanced firewalls have IDS/IPS capabilities to detect and prevent attacks.
Application Filtering and Control

Control access to specific applications or services.
Traffic Management

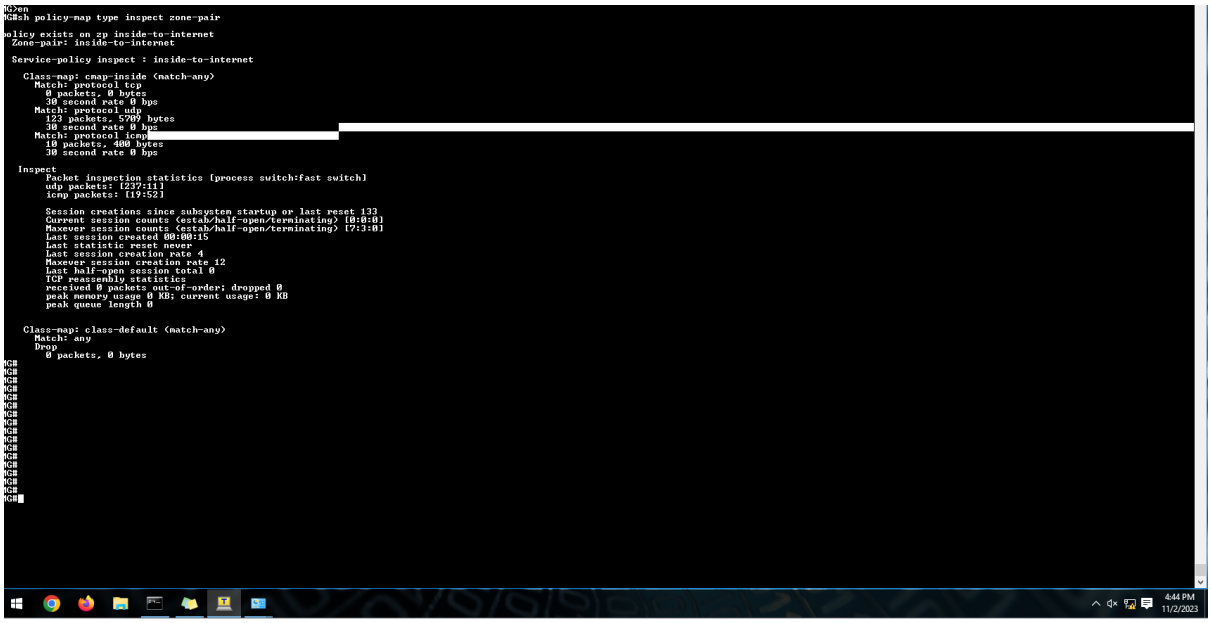
Prioritize or limit bandwidth for certain types of traffic.
Monitoring and Reporting

Generate logs and reports for network traffic and security events.
Firewalls are fundamental components in network security, providing a barrier between trusted and untrusted networks and controlling access based on defined security policies.

b. Issue the **show zone security** command on both router SB and MG to demonstrate the zones are properly created, and the interfaces were correctly assigned. Take the screenshots from SB and MG then paste them below:

```
policy exists on zp inside-to-internet
  Zone-pair: inside-to-internet

  Service-policy inspect : inside-to-internet

    Class-map: cmap-inside (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        64 packets, 3194 bytes
        30 second rate 0 bps
      Match: protocol icmp
        7 packets, 312 bytes
        30 second rate 0 bps

   Inspect
        Packet inspection statistics [process switch:fast switch]
        udp packets: [136:6]
        icmp packets: [7:50]

        Session creations since subsystem startup or last reset 71
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [4:2:0]
        Last session created 00:02:29
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 10
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes

policy exists on zp internet-dmz
  Zone-pair: internet-dmz

  Service-policy inspect : internet-dmz

    Class-map: internet-dmz (match-any)
      Match: protocol http
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0
        TCP reassembly statistics
        received 0 packets out-of-order; dropped 0
        peak memory usage 0 KB; current usage: 0 KB
        peak queue length 0


    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

c. Issue the **show policy-map type inspect zone-pair** command to demonstrate the zone-pairs, their policy-maps, the class-maps and match counters. Take the screenshot of the output from SB and paste it below:



Lab 4 Results

a. Display the routing table by issuing the **show ip route** command on router SB and the router MG. Take the screenshots from SB and MG then paste them below:

```
MG(config)#do sh ip route 172.16.12.1
Routing entry for 172.16.12.0/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Tunnel0
      Route metric is 0, traffic share count is 1
MG(config)#
```

-

```
!
router ospf 1
 router-id 3.3.3.3
 network 172.16.0.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 209.165.200.16 0.0.0.15 area 0
!
```

-

```
MG(config)#do sh ip route 172.16.12.1
Routing entry for 172.16.12.0/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Tunnel0
      Route metric is 0, traffic share count is 1
MG(config)#
```

-
-

```
:B(config)#sh ip route
                ^
% Invalid input detected at '^' marker.

:B(config)#do sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.2
                is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        172.16.0.0/24 is directly connected, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/27 is directly connected, GigabitEthernet0/0.20
L        192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/27 is directly connected, GigabitEthernet0/0.30
L        192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
      192.168.90.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.90.0/29 is directly connected, GigabitEthernet0/0.90
L        192.168.90.1/32 is directly connected, GigabitEthernet0/0.90
      209.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C        209.165.200.0/28 is directly connected, Serial0/0/0
L        209.165.200.1/32 is directly connected, Serial0/0/0
C        209.165.200.2/32 is directly connected, Serial0/0/0
L        209.165.200.10/32 is directly connected, Serial0/0/0
:B(config)#
:B(config)#
:B(config)#
:B(config)#

MG(config)#sh ip route
                ^
% Invalid input detected at '^' marker.

MG(config)#do sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.17 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected
                is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.0.0/24 is directly connected, GigabitEthernet0/0
L        172.16.0.1/32 is directly connected, GigabitEthernet0/0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.2/32 is directly connected, Tunnel0
S     192.168.20.0/24 is directly connected, Tunnel0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.16/28 is directly connected, Serial0/0/0
L        209.165.200.18/32 is directly connected, Serial0/0/0
MG(config)#
```

Lab 5 Results

a. Use the command **show crypto isakmp sa** to verify the peers between 209.165.200.1 and 209.165.200.18. Take a screenshot and pasted it to AT4 Part 2 template.

SB	MG
	

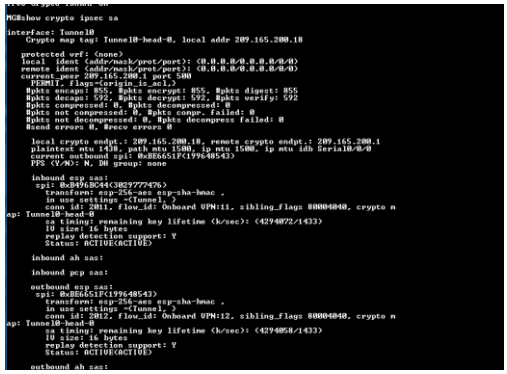
```
SB>en
SB#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state
209.165.200.18  209.165.200.1   QM_IDLE

IPv6 Crypto ISAKMP SA

SB#
```

```
MG#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
209.165.200.1   209.165.200.18  QM_IDLE           1001 ACTIVE
```

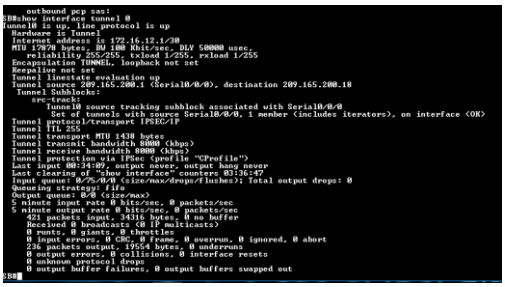
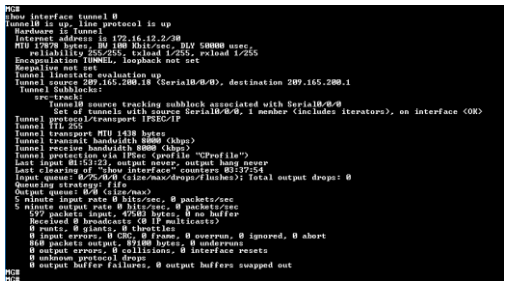
b. Use the command **show crypto ipsec sa** to verify the number of packets encrypted by IPSec when traversing through the GRE tunnel. Take a screenshot and pasted it to AT4 Part 2 template.

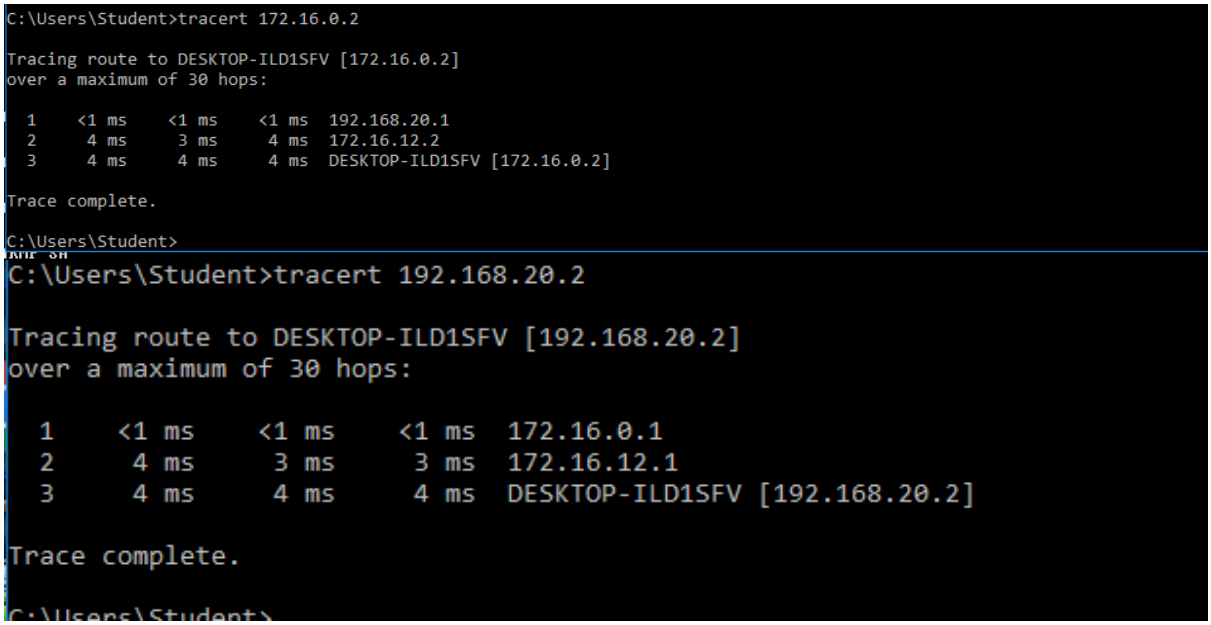
SB	MG
	

```
SB#
SB#
SB#
SB#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 209.165.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 209.165.200.18 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 224, #pkts encrypt: 224, #pkts digest: 224
    #pkts decaps: 497, #pkts decrypt: 497, #pkts verify: 497
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 209.165.200.1, remote crypto endpt.: 209.165.200.18
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xB8E4DBCA(3135552458)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x71B23093(1907546579)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: Onboard VPN:9, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4168577/407)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8E4DBCA(3135552458)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2010, flow_id: Onboard VPN:10, sibling_flags 80004040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4168682/407)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
SB#
```

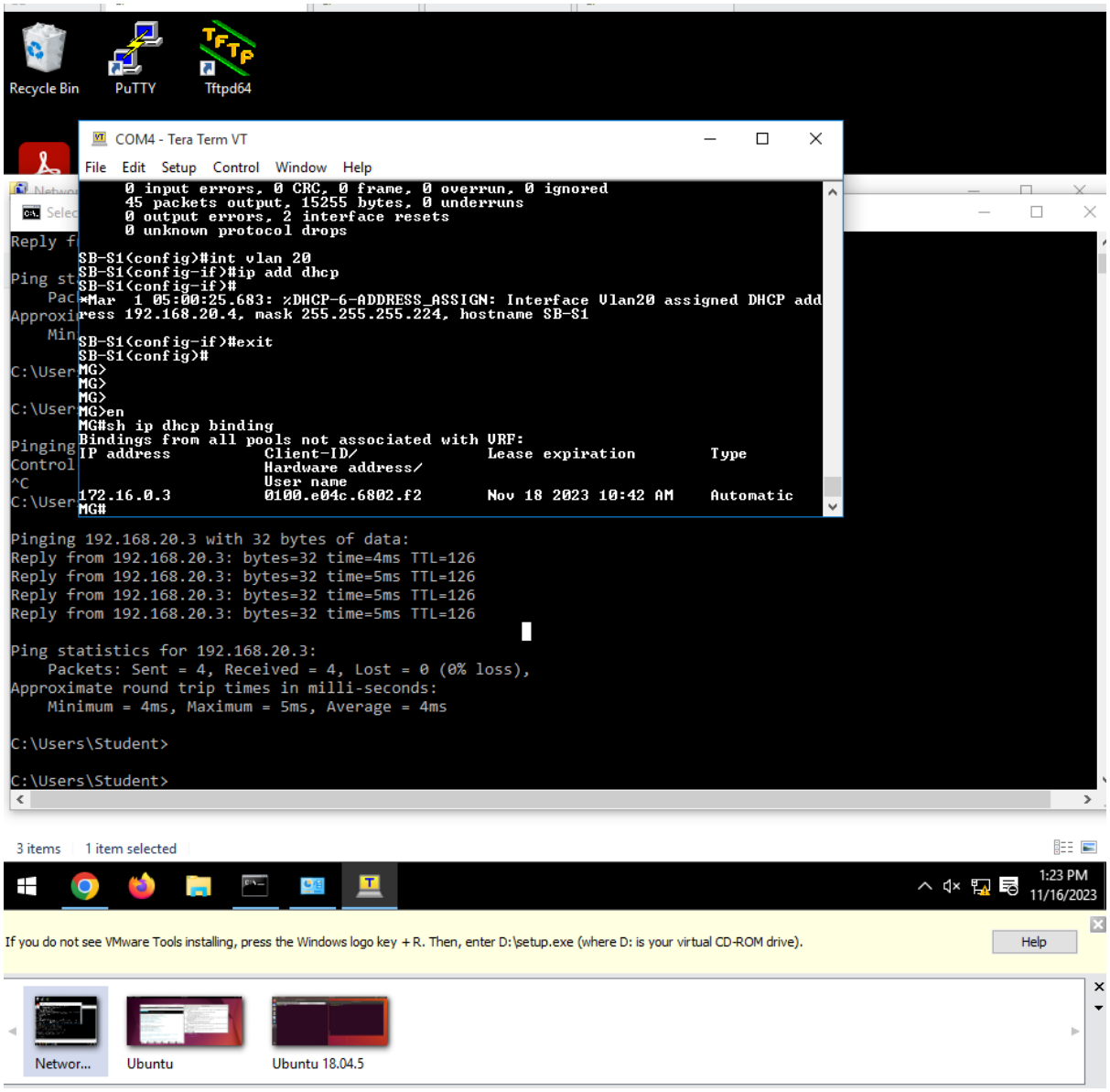
c. Use the command **show interface tunnel 0** to verify the tunnel protocol is using IPSEC/IP instead of GRE. . Take a screenshot and pasted it to AT4 Part 2 template.

SB	MG
	



Lab 6 Results

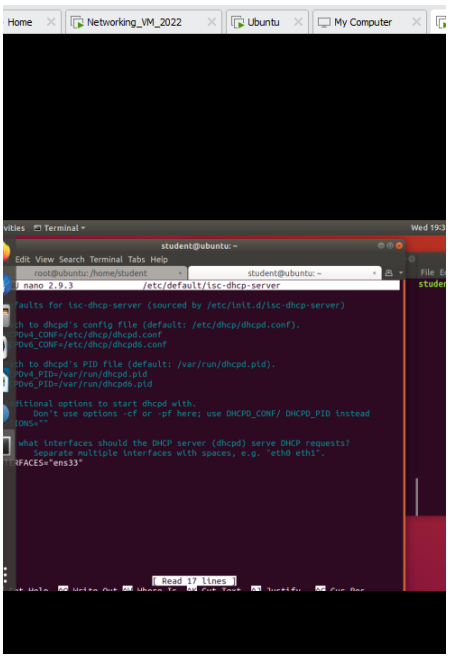
a. Use the command “show ip dhcp binding” on the router MG to demonstrate the IPs released to the MG PC. Take the screenshot and paste it below.



b. Take a screenshot of the contents of ***/etc/dhcp/dhcpd.conf*** file on the SB Ubuntu DHCP server and paste it below.

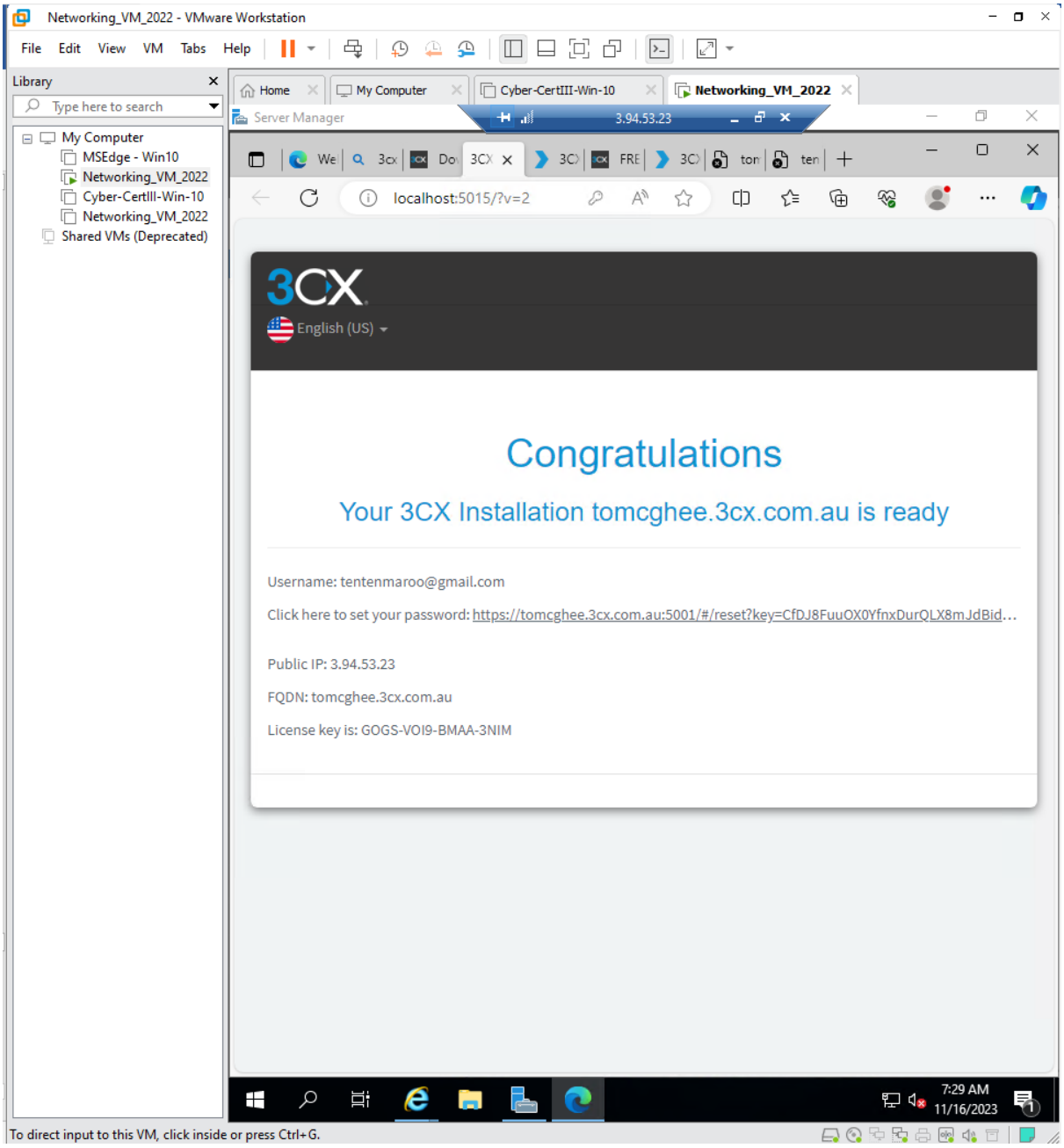
```
5                        /etc/dhcp/dhcpd.conf

0.3 192.168.20.30;
nask 255.255.255.192;
st-address 192.168.1.63;
y of VLAN 20
192.168.20.1;
name-servers 192.168.90.130;

ting
80.0 netmask 255.255.255.224 {
0.3 192.168.30.30;
nask 255.255.255.192;
st-address 192.168.30.127;
192.168.30.1;
name-servers 192.168.90.130;

90.0 netmask 255.255.255.248 {

end dhcp log messages to a different log file (you also
```

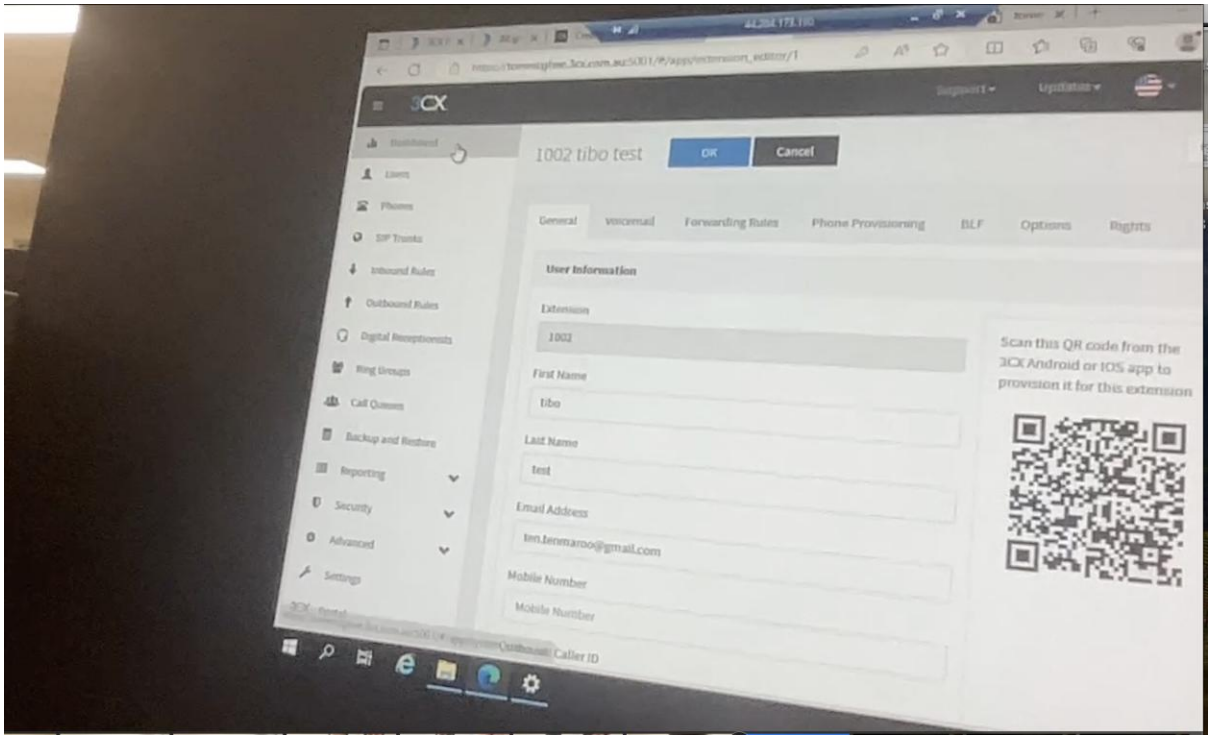
c. Take a screenshot of the contents of ***/etc/default/isc-dhcp-server*** file on the SB Ubuntu DHCP server and paste it below

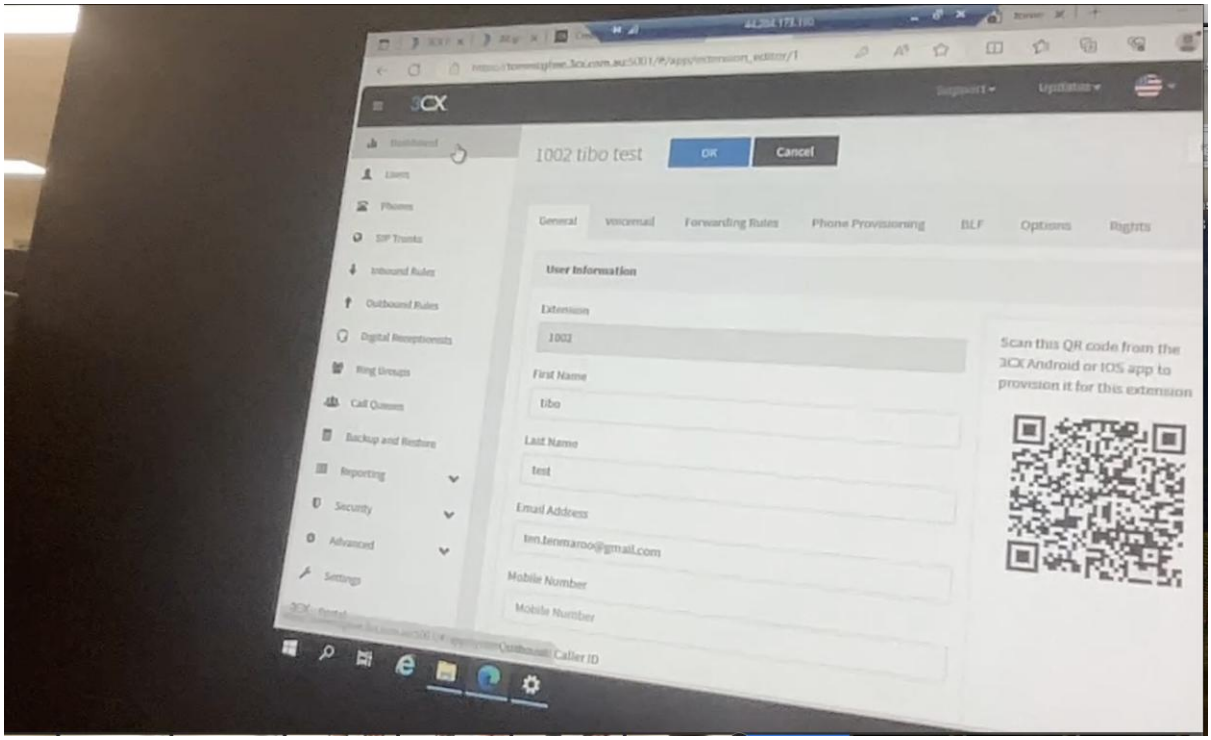


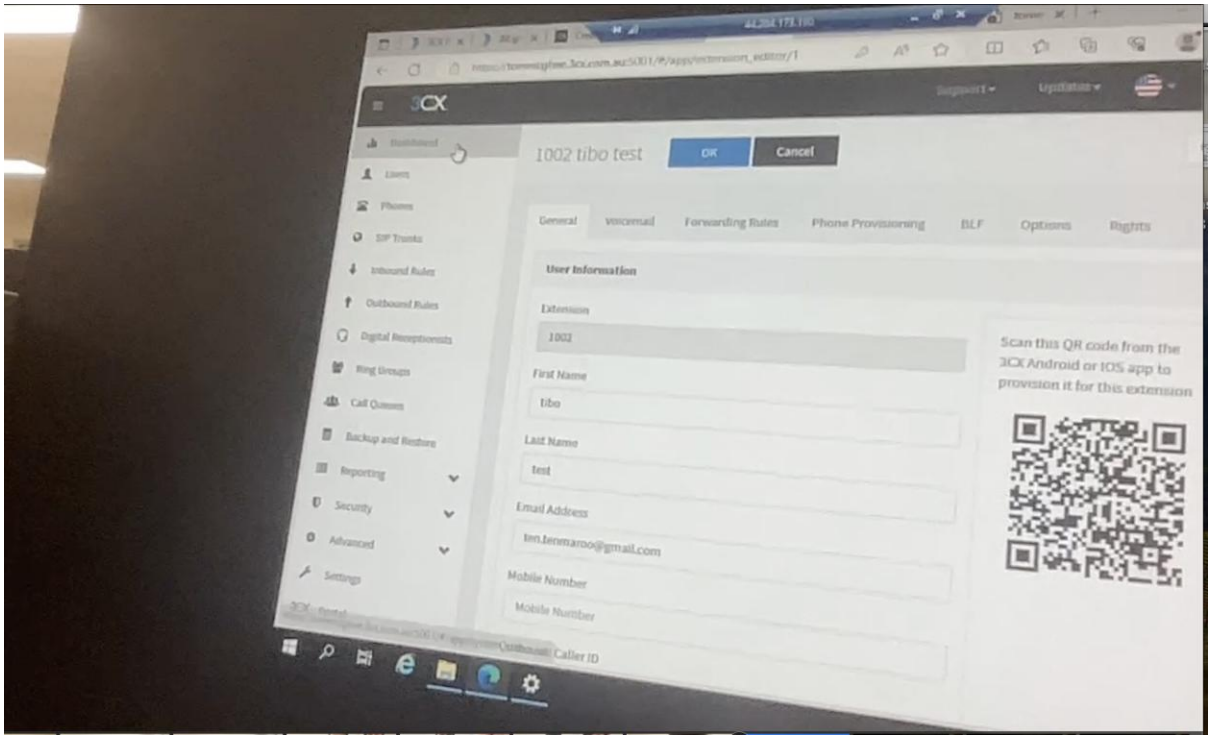
Lab 7 Results

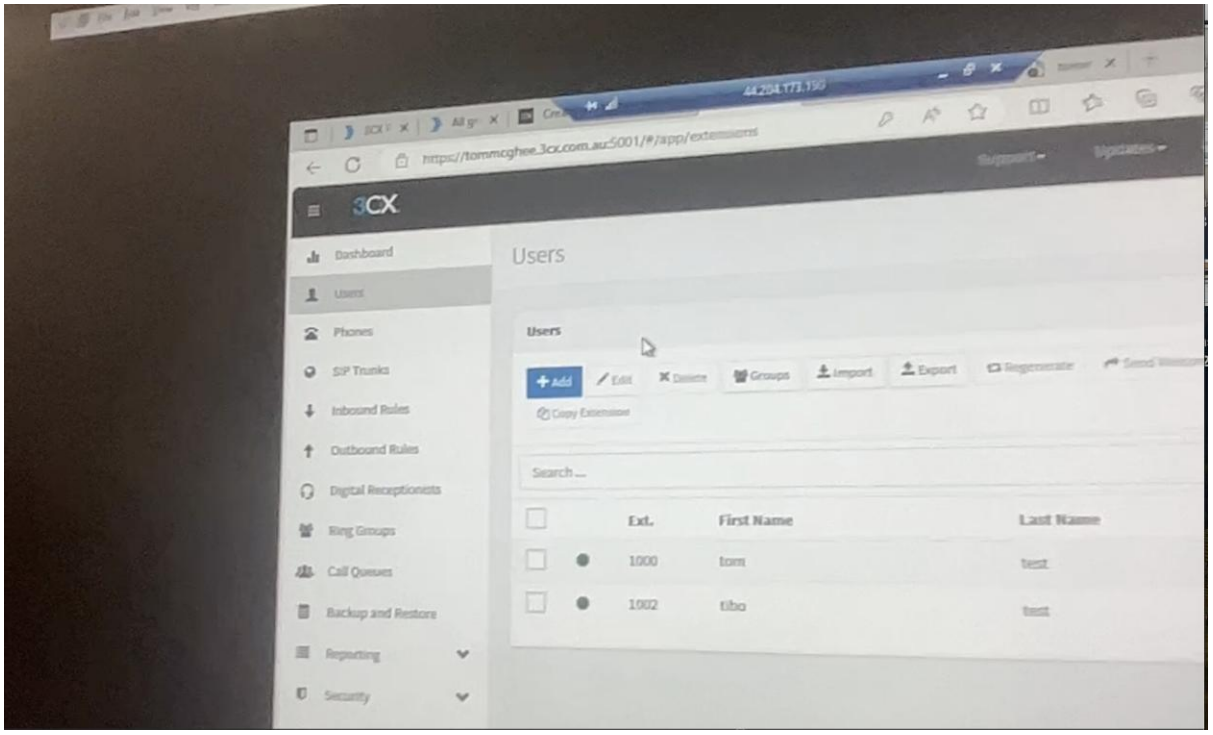
a. Screen shots of successful ip phone registration on the CMEs.

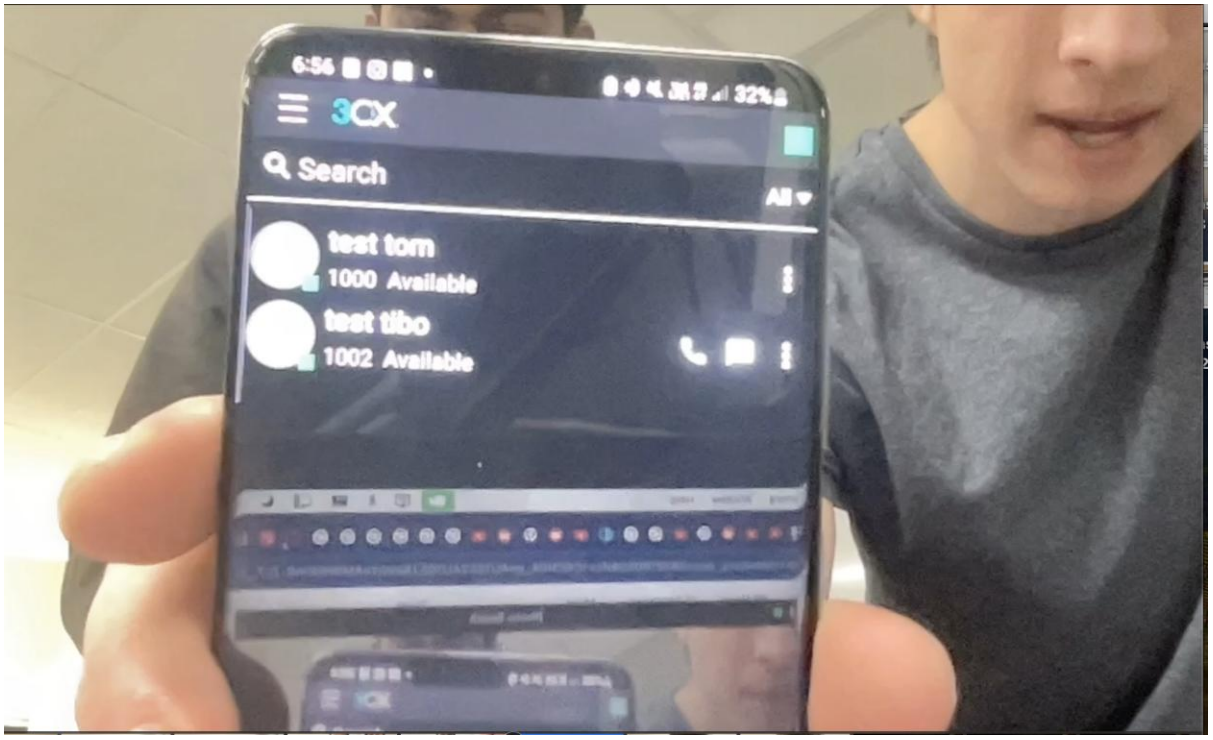

Networking_VM_2022 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
MSEdge - Win10
Networking_VM_2022
Cyber-CertIII-Win-10
Networking_VM_2022
Shared VMs (Deprecated)
Home
My Computer
Cyber-CertIII-Win-10
Networking_VM_2022
Server Manager
3.94.53.23
localhost:5015/?v=2
3CX
English (US)
Congratulations
Your 3CX Installation tomcghee.3cx.com.au is ready
Username: tentenmaroo@gmail.com
Click here to set your password: https://tomcghee.3cx.com.au:5001/#/reset?key=CfDJ8FuuOX0YfnxDurQLX8mJdBid...
Public IP: 3.94.53.23
FQDN: tomcghee.3cx.com.au
License key is: GOGS-VOI9-BMAA-3NIM
7:29 AM
11/16/2023
To direct input to this VM, click inside or press Ctrl+G.

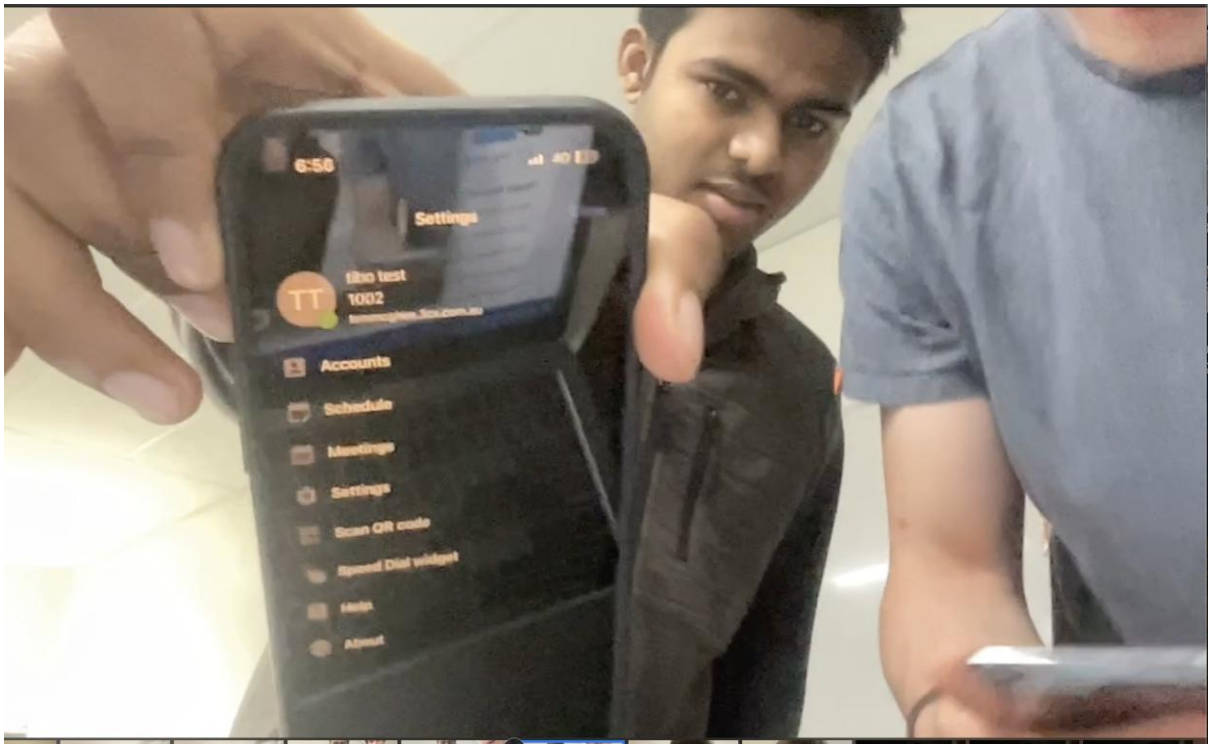

3CX
1002 tibo test
OK
Cancel
General
Voicemail
Forwarding Rules
Phone Provisioning
BLF
Options
Rights
User Information
Extension
1002
First Name
tibo
Last Name
test
Email Address
tim.lemmens@gmail.com
Mobile Number
Scan this QR code from the 3CX Android or iOS app to provision it for this extension

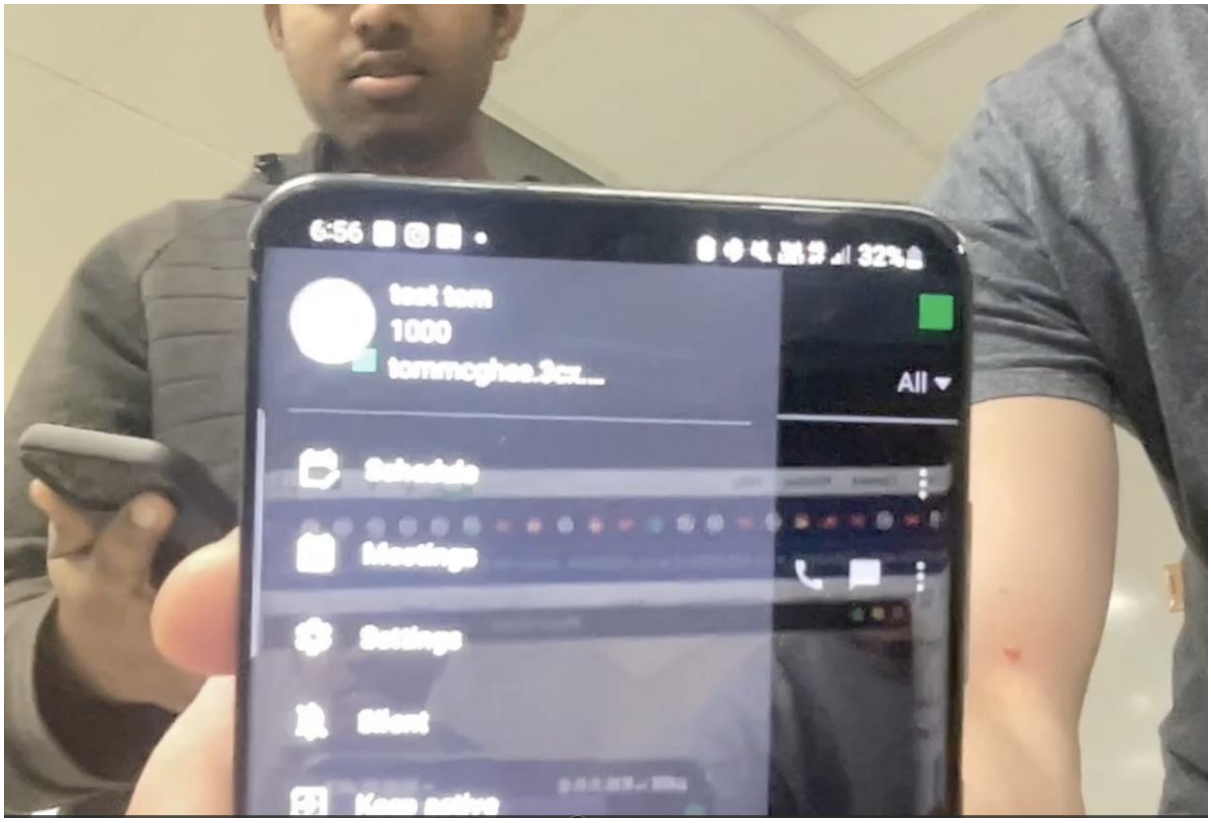

3CX
1002 tibo test
OK
Cancel
General
Voicemail
Forwarding Rules
Phone Provisioning
BLF
Options
Rights
User Information
Extension
1002
First Name
tibo
Last Name
test
Email Address
tim.lemmens@gmail.com
Mobile Number
Scan this QR code from the 3CX Android or iOS app to provision it for this extension

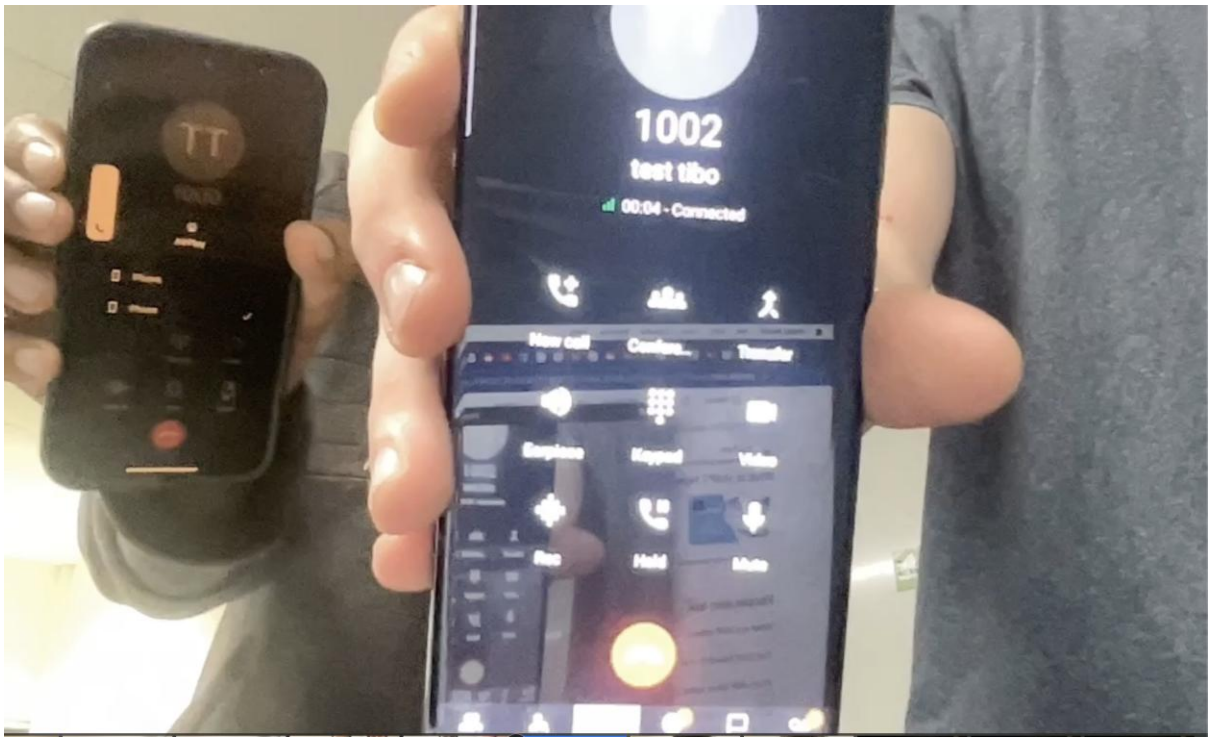

3CX
1002 tibo test
OK
Cancel
General
Voicemail
Forwarding Rules
Phone Provisioning
BLF
Options
Rights
User Information
Extension
1002
First Name
tibo
Last Name
test
Email Address
tim.tennaroo@gmail.com
Mobile Number
Scan this QR code from the 3CX Android or iOS app to provision it for this extension

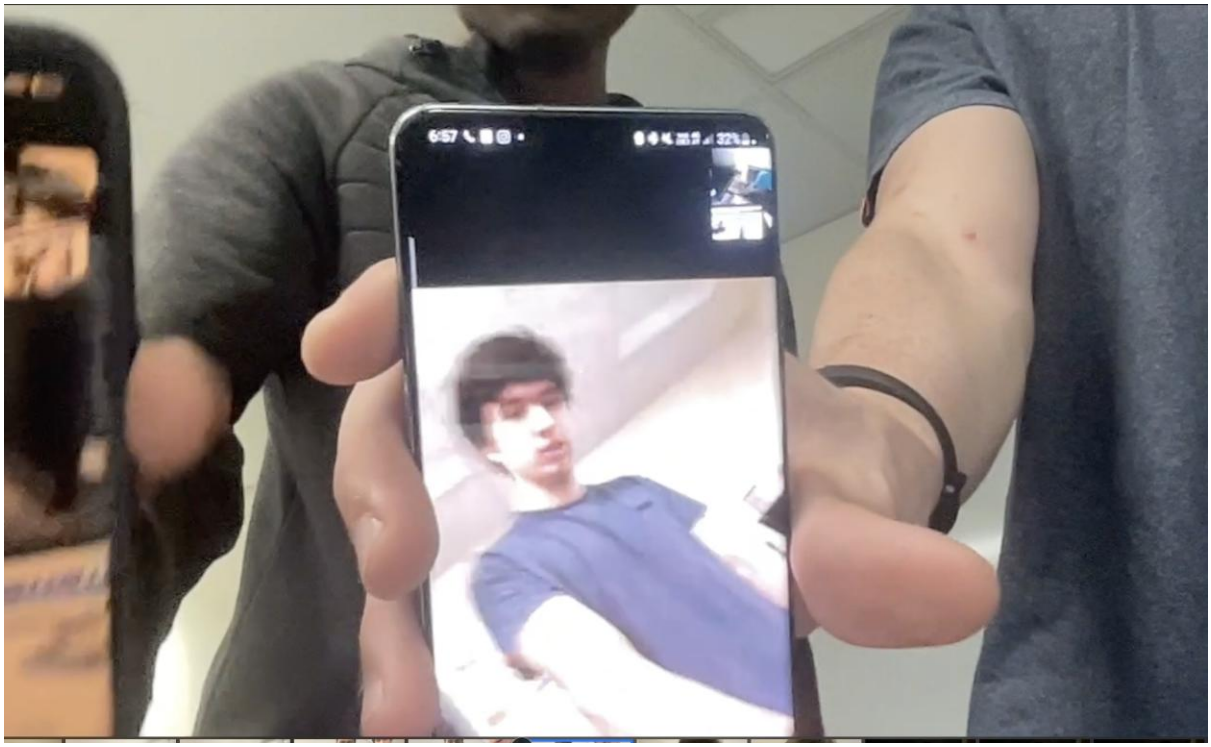

3CX
Users
Dashboard
Users
Phones
SIP Trunks
Inbound Rules
Outbound Rules
Digital Receptionists
Ring Groups
Call Queues
Backup and Restore
Reporting
Security
Add
Edit
Delete
Groups
Import
Export
Search ...
Ext.
First Name
Last Name
1000
tom
test
1002
tibo
test


6:56
3CX
Search
All
test tom
1000 Available
test tibo
1002 Available


6:58
Settings
tibo test
1002
Accounts
Schedule
Meetings
Settings
Scan QR code
Speed Dial widget
Help
About


6:56
test tom
1000
All
Meetings
Settings
Silent


1002
test tibo
00:04 - Connected
Keypad
Video
Hold
Mute



\

Lab 8 Results

Lab 8.1 Paste screenshots of the two load sharing domain controllers. You should name the controllers after the format as depicted below which should vary from person to person based on the student's name:

- dc1.student1*firstname.student2firstname*
- dc2. student1*firstname.student2firstname*

Please briefly describe what is NTP?

NTP, or Network Time Protocol, is a fundamental protocol for ensuring accurate time synchronization across networked devices. It operates in a hierarchical manner, with time servers synchronizing their clocks with higher-stratum servers. This cascade ensures that devices within a network share a consistent and precise time reference. Accurate time is vital for numerous network operations, including log synchronization, security protocols, and coordination between distributed systems. Without synchronized time, network-related tasks and security measures

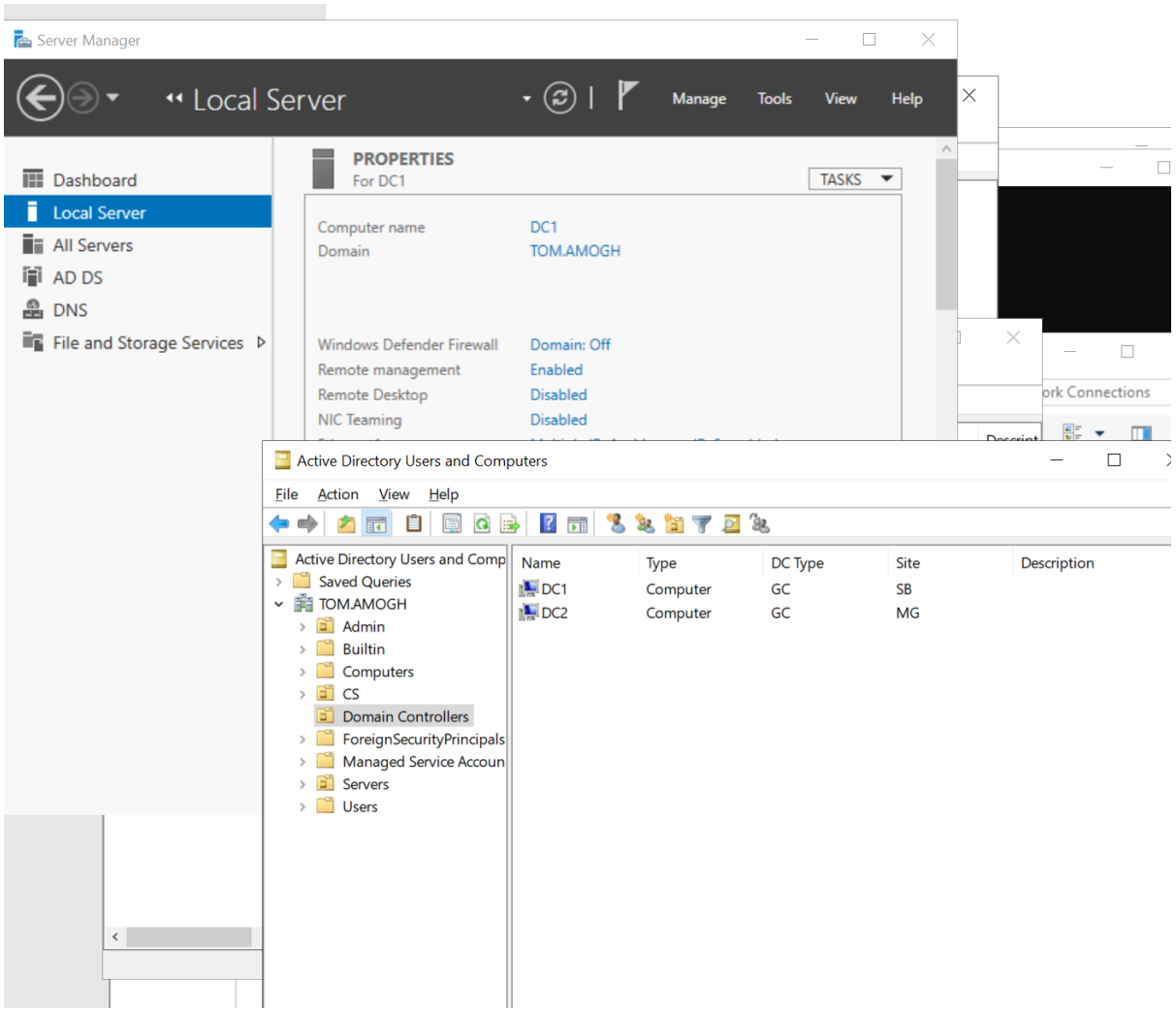
Please briefly describe what is user authentication?

User authentication is the cornerstone of network security. It involves verifying the identity of users before granting access to resources. Common methods include the traditional username and password combination, biometric authentication using physical traits like fingerprints, hardware tokens that generate one-time passcodes, and Two-Factor Authentication (2FA), combining multiple authentication factors for enhanced security. User authentication ensures that only authorized individuals can access sensitive data and systems, contributing significantly to overall network security.

Please briefly describe what are Active Directory services?

Active Directory (AD) is a robust directory service offered by Microsoft. It provides a wide range of network services, including user and resource management, authentication and authorization, group policy management, and Single Sign-On (SSO) capabilities. With AD, administrators can efficiently organize and manage users, computers, and network resources within a hierarchical structure. AD's role in authentication and authorization ensures that users have appropriate permissions to access network resources. Group policies enable administrators to enforce security settings and configurations across the network. Additionally, SSO simplifies user access by allowing them to log in once and access multiple resources without repeated authentication.

The screenshot should be similar to the one attached below. Please remove the demonstrated screenshot when you submit this template.



Lab 8.2 Follow the tutorial video 8.2-Create Sites and Subnets to do sublab 8.2 and take a screenshot at the end and paste it here. The screenshot should be similar to the one attached below. Please remove the demonstrated screenshot when you submit this template.

Please briefly describe how ADDS Sites implement load balancing across DCs to share with the client AD requests.

Active Directory Domain Services (ADDS) Sites do not implement load balancing across Domain Controllers (DCs) in the traditional sense. Instead, they prioritize site-local affinity and fault tolerance over load balancing for client AD requests. However, there are certain technical aspects to consider: Site Topology:

In ADDS, organizations define multiple AD Sites based on their network topology. These sites typically represent physical or logical network segments.
Subnet Mapping:

Subnets are associated with specific AD Sites. When a client machine logs in, it detects its IP subnet and identifies the corresponding AD Site. This subnet mapping helps clients determine their site membership.
Site Cost:

Within the AD Sites configuration, administrators can assign costs to site links. These costs influence the replication schedule and path selection for AD replication traffic, not client AD requests.
Site-Local Affinity:

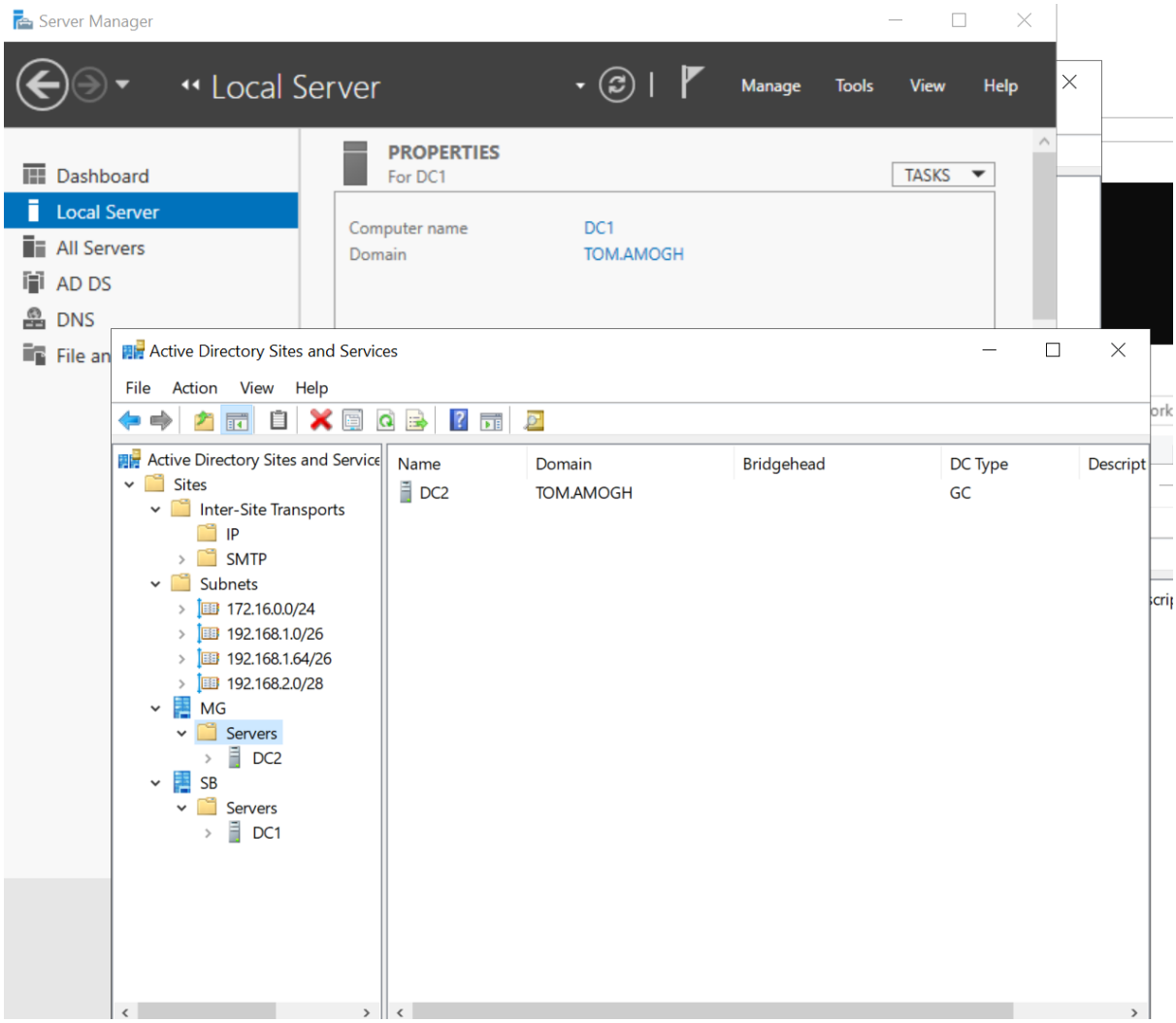
Active Directory clients, including workstations and servers, have built-in site awareness. They prioritize DCs within their own site when making AD requests. This ensures that clients preferentially target DCs within their proximity, reducing latency and conserving bandwidth.
DNS SRV Records:

DNS service (SRV) records are used by clients to locate DCs for various AD services. Clients will query DNS for DCs within their own AD Site before considering DCs in other sites. This prioritizes site-local DCs for client AD requests.
Replication:

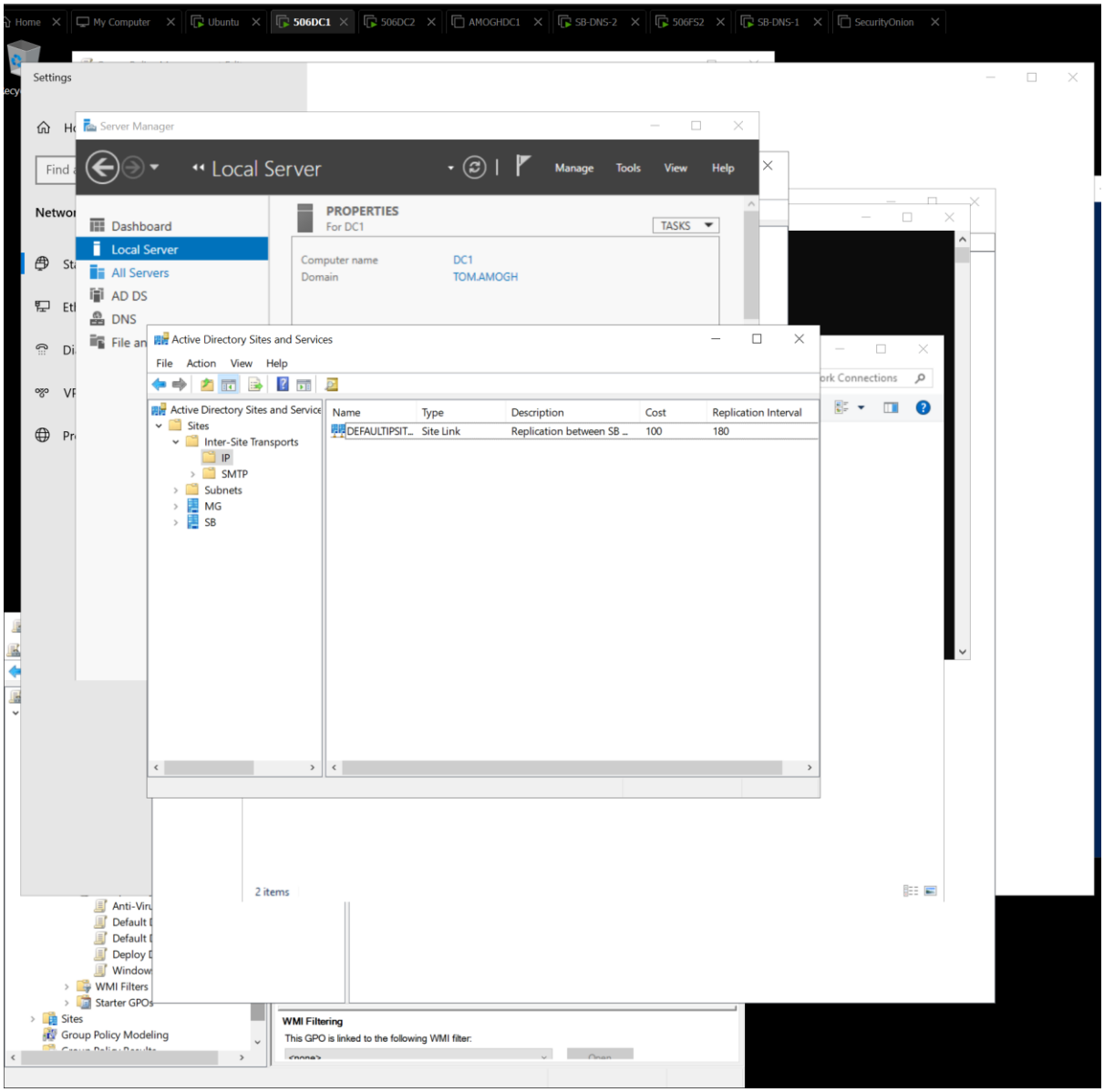
While not directly related to client AD requests, ADDS Sites are critical for controlling AD replication. AD replication ensures that changes made in one site are efficiently replicated to other sites to maintain data consistency. This process includes optimizing replication topology for efficient data transfer.
Redundancy and Failover:

To enhance fault tolerance, organizations often deploy multiple DCs within each site. In case of a DC failure, clients can automatically failover to another DC within the same site. This redundancy minimizes disruptions to AD services.
LDAP Site Coverage:

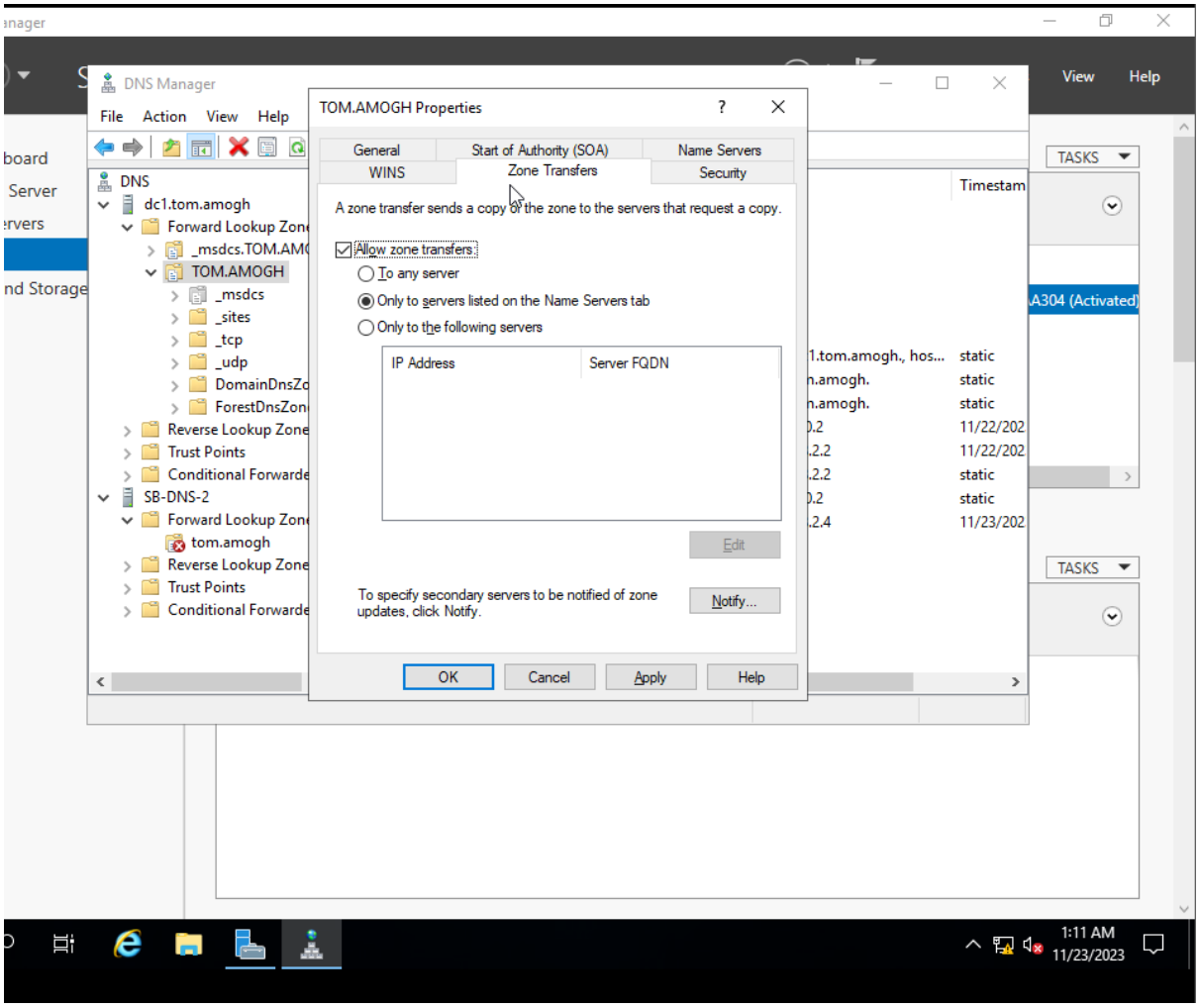
LDAP queries made by clients are site-aware and typically directed to DCs within the client's own site. This minimizes the need for cross-site queries.

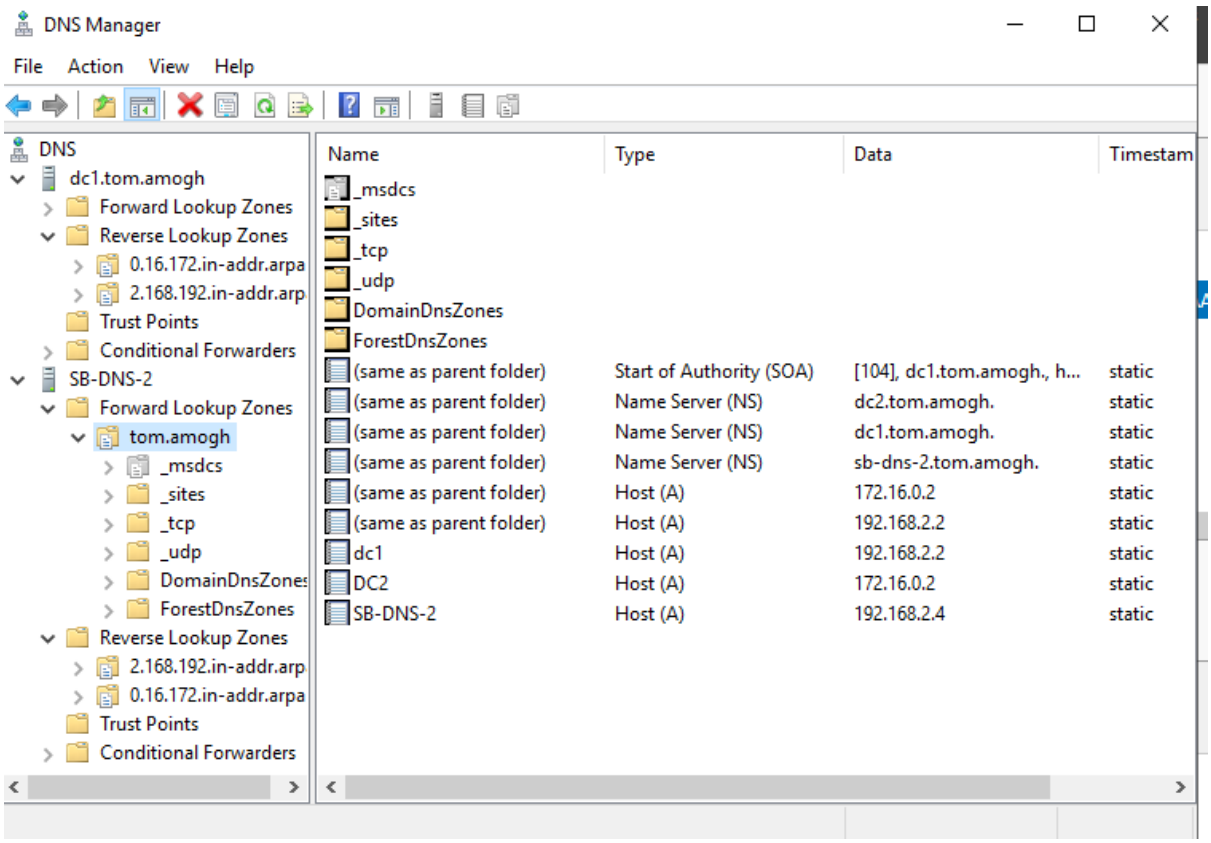


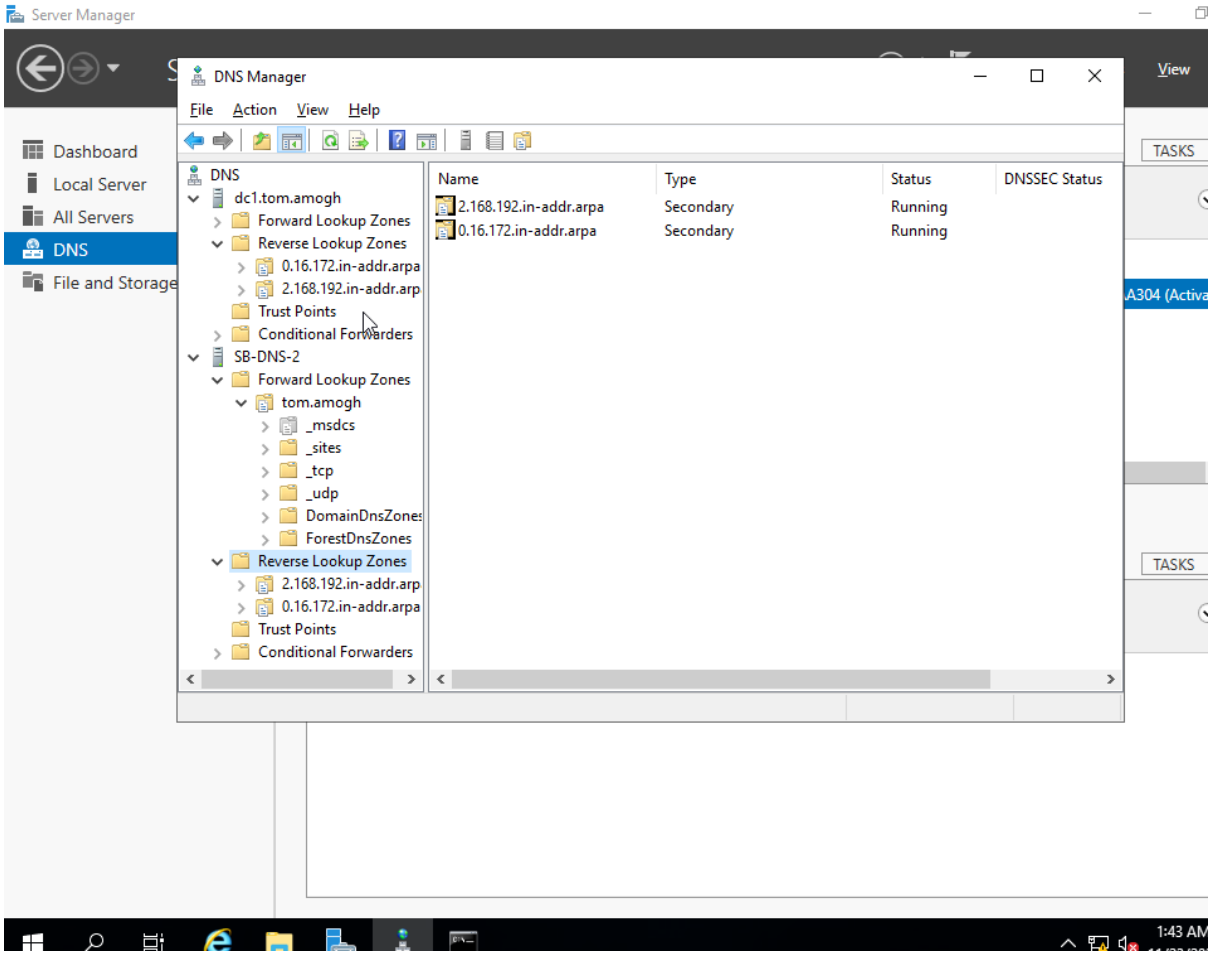
Lab 8.3 Follow the tutorial video 8.3-Configure Domain Controller Replication between sites to do sublab 8.3. Take a screenshot similar to the following which demonstrates the subnets, sites, DCs, replication between SB & MG, and the domain name on the background. Remove the demonstrated example when you submit this template.

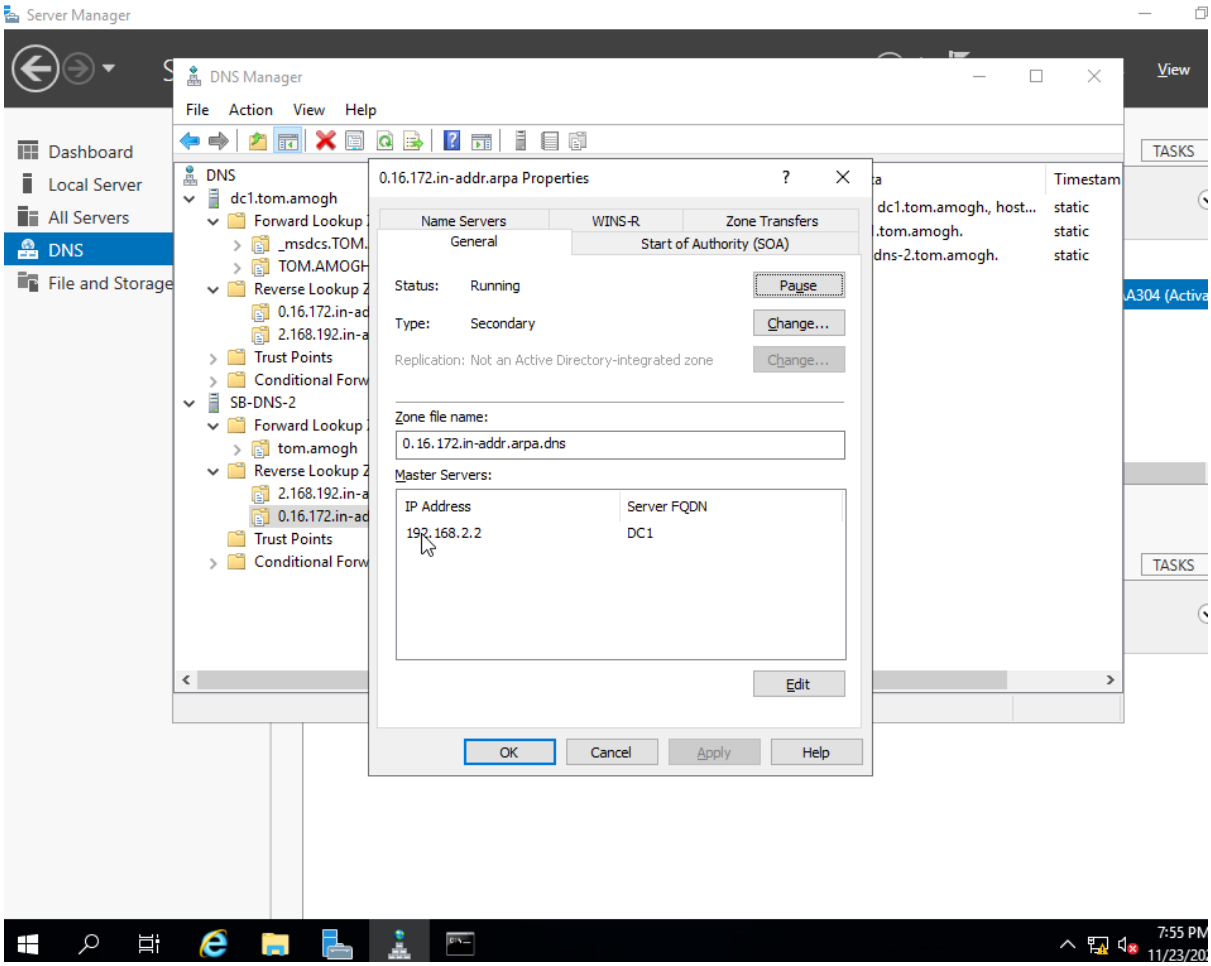


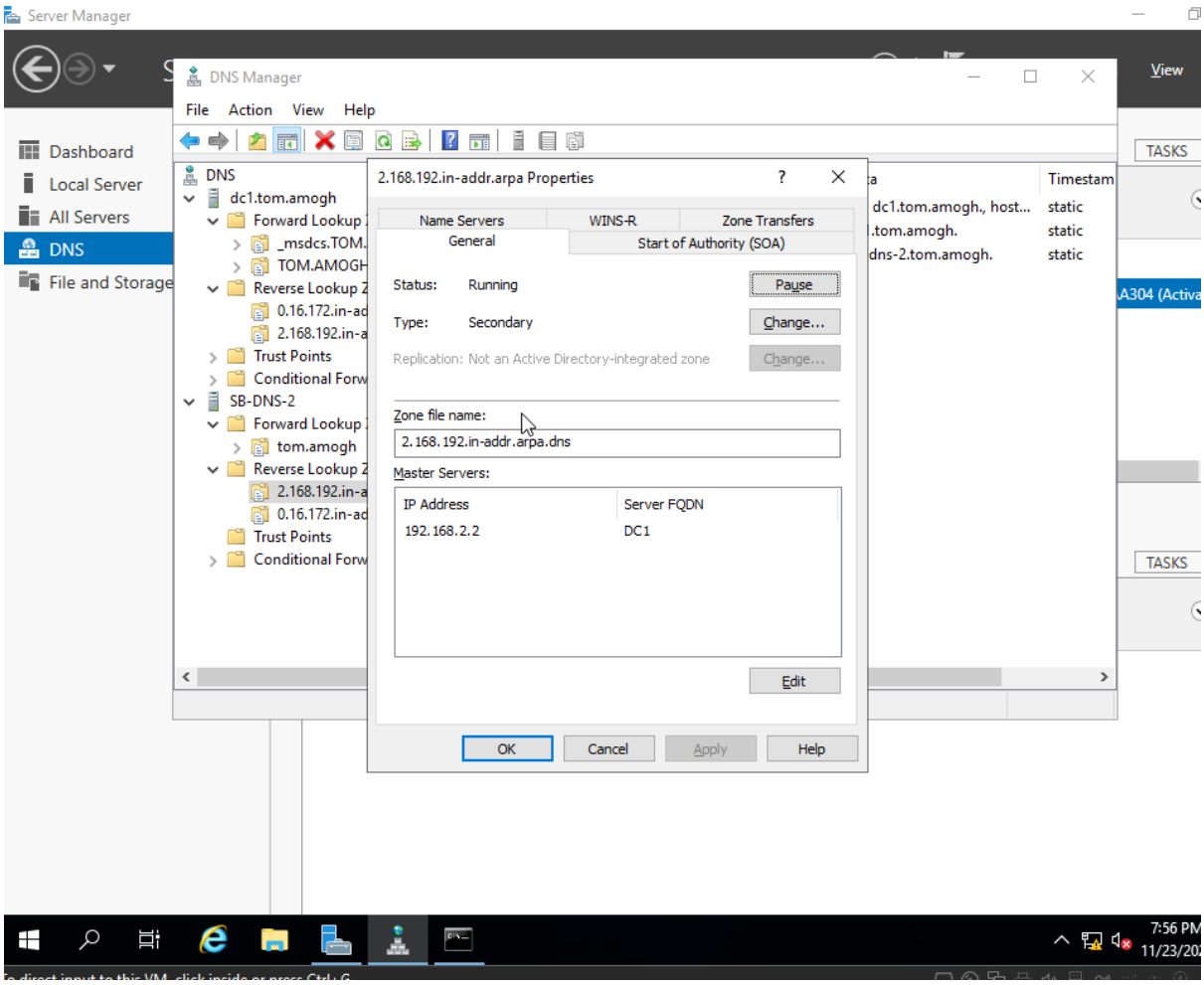
Lab 8.4 Follow the tutorial video 8.4- Configure DNS Replication with Active Directory integrated Zone Replication to do sublab 8.4. Take screenshots similar to the following which displays the domain name on the background. Please remove the demonstrated screenshots at the end.


DNS Manager
File Action View Help
DNS
dc1.tom.amogh
Forward Lookup Zone
_msdcs.TOM.AMO
TOM.AMOGH
_msdcs
_sites
_tcp
_udp
DomainDnsZo
ForestDnsZon
Reverse Lookup Zone
Trust Points
Conditional Forwarde
SB-DNS-2
Forward Lookup Zone
tom.amogh
Reverse Lookup Zone
Trust Points
Conditional Forwarde
TOM.AMOGH Properties
General
Start of Authority (SOA)
Name Servers
WINS
Zone Transfers
Security
A zone transfer sends a copy of the zone to the servers that request a copy.
Allow zone transfers
To any server
Only to servers listed on the Name Servers tab
Only to the following servers
IP Address
Server FQDN
Edit
To specify secondary servers to be notified of zone updates, click Notify.
Notify...
OK
Cancel
Apply
Help
Timestam
1.tom.amogh., hos... static
n.amogh. static
n.amogh. static
0.2 11/22/202
.2.2 11/22/202
.2.2 static
0.2 static
.2.4 11/23/202
TASKS
TASKS
A304 (Activated)
View
Help
1:11 AM
11/23/2023

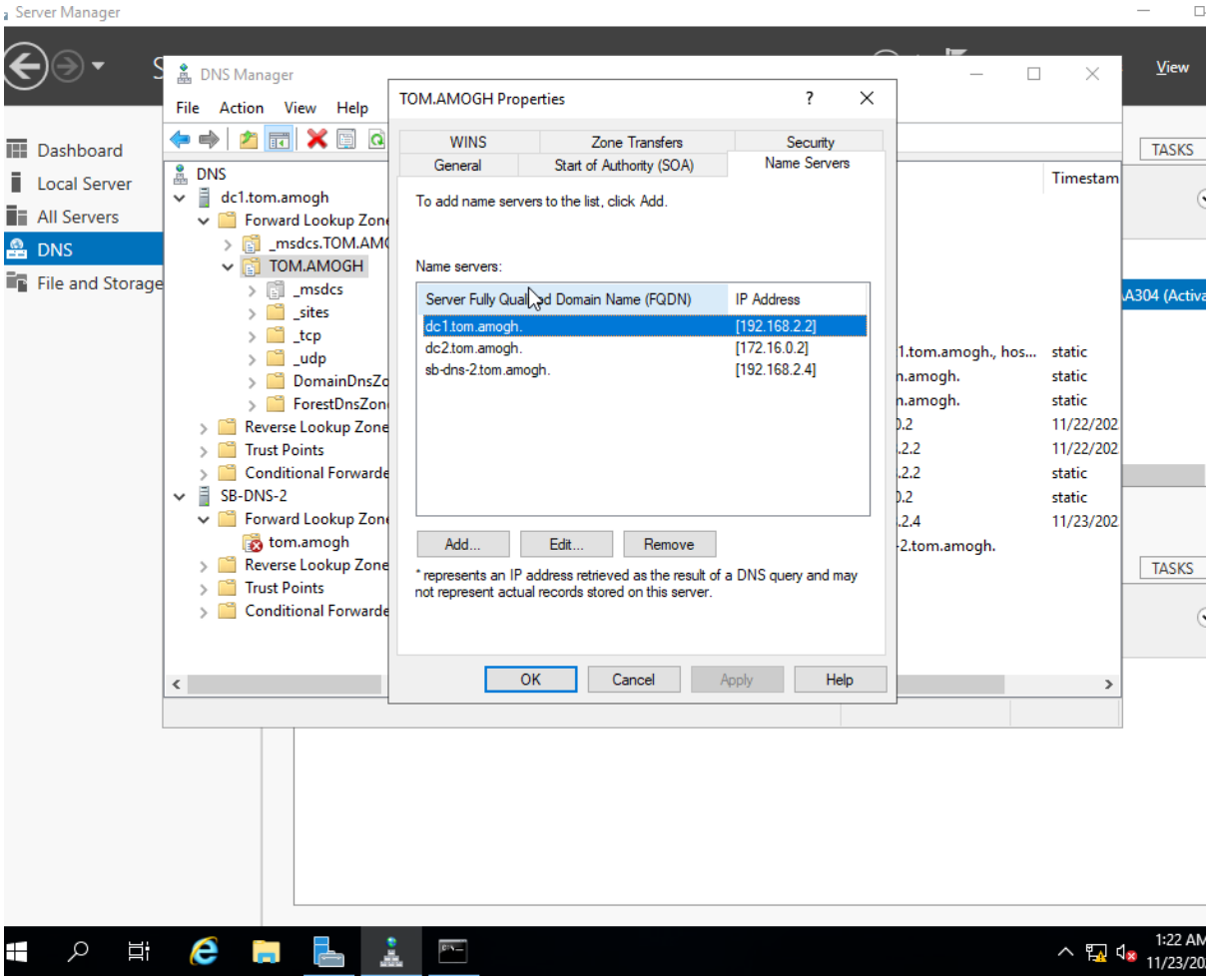

DNS Manager
File Action View Help
DNS
dc1.tom.amogh
Forward Lookup Zones
Reverse Lookup Zones
0.16.172.in-addr.arpa
2.168.192.in-addr.arp
Trust Points
Conditional Forwarders
SB-DNS-2
Forward Lookup Zones
tom.amogh
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
2.168.192.in-addr.arp
0.16.172.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Data
Timestam
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
(same as parent folder) Start of Authority (SOA) [104], dc1.tom.amogh., h... static
(same as parent folder) Name Server (NS) dc2.tom.amogh. static
(same as parent folder) Name Server (NS) dc1.tom.amogh. static
(same as parent folder) Name Server (NS) sb-dns-2.tom.amogh. static
(same as parent folder) Host (A) 172.16.0.2 static
(same as parent folder) Host (A) 192.168.2.2 static
dc1 Host (A) 192.168.2.2 static
DC2 Host (A) 172.16.0.2 static
SB-DNS-2 Host (A) 192.168.2.4 static

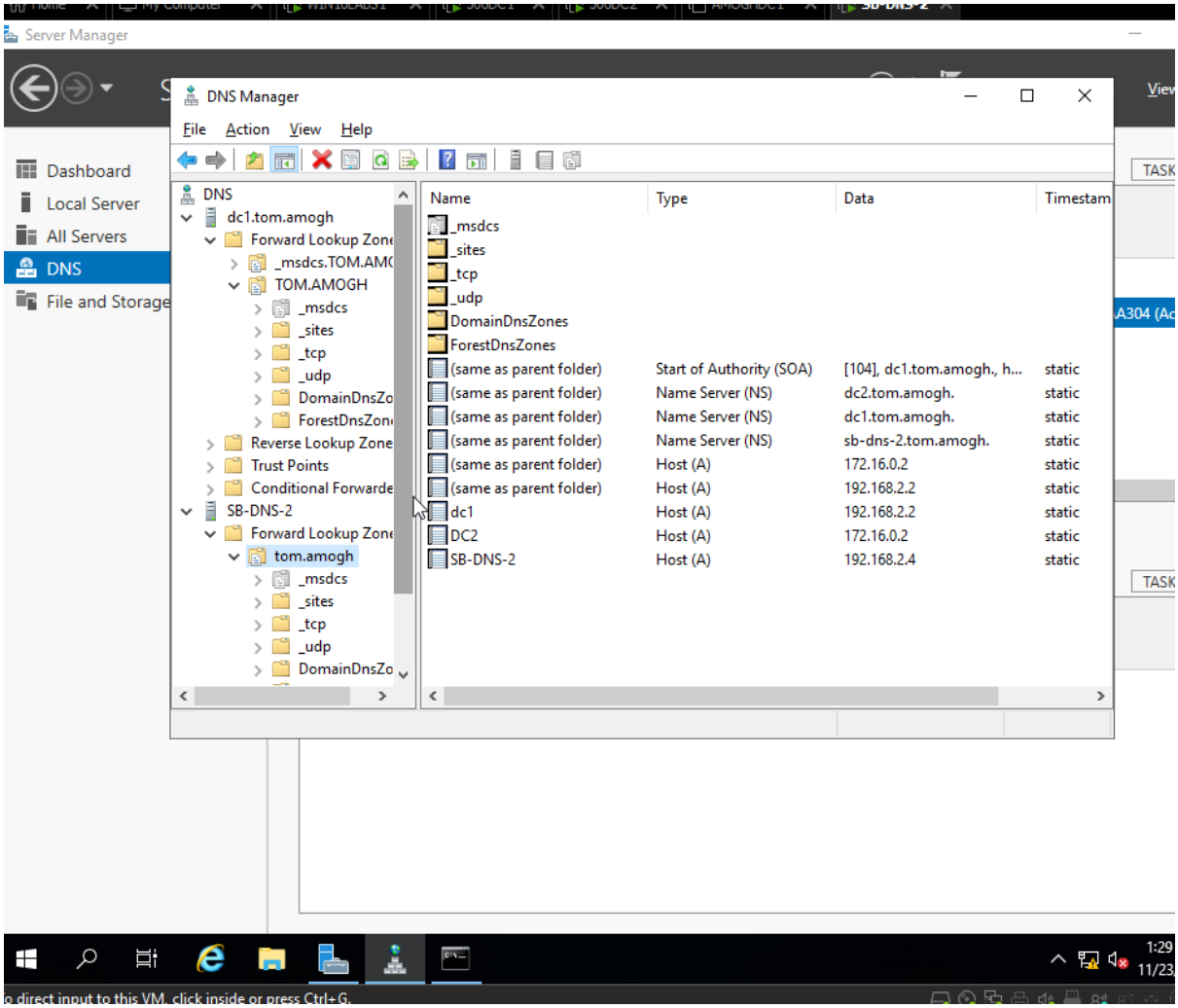

Server Manager
Dashboard
Local Server
All Servers
DNS
File and Storage
DNS Manager
File Action View Help
DNS
dc1.tom.amogh
Forward Lookup Zones
Reverse Lookup Zones
0.16.172.in-addr.arpa
2.168.192.in-addr.arp
Trust Points
Conditional Forwarders
SB-DNS-2
Forward Lookup Zones
tom.amogh
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
2.168.192.in-addr.arp
0.16.172.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Status
DNSSEC Status
2.168.192.in-addr.arpa Secondary Running
0.16.172.in-addr.arpa Secondary Running
TASKS
TASKS
1:43 AM


Server Manager
DNS Manager
File Action View Help
Dashboard
Local Server
All Servers
DNS
File and Storage
DNS
dc1.tom.amogh
Forward Lookup
_msdcs.TOM.
TOM.AMOGH
Reverse Lookup
0.16.172.in-ad
2.168.192.in-a
Trust Points
Conditional Forw
SB-DNS-2
Forward Lookup
tom.amogh
Reverse Lookup
2.168.192.in-a
0.16.172.in-ad
Trust Points
Conditional Forw
0.16.172.in-addr.arpa Properties
Name Servers
WINS-R
Zone Transfers
General
Start of Authority (SOA)
Status: Running
Pause
Type: Secondary
Change...
Replication: Not an Active Directory-integrated zone
Change...
Zone file name:
0.16.172.in-addr.arpa.dns
Master Servers:
IP Address
Server FQDN
192.168.2.2
DC1
Edit
OK
Cancel
Apply
Help
dc1.tom.amogh., host...
.tom.amogh.
dns-2.tom.amogh.
Timestam
static
static
static
TASKS
TASKS
View
7:55 PM

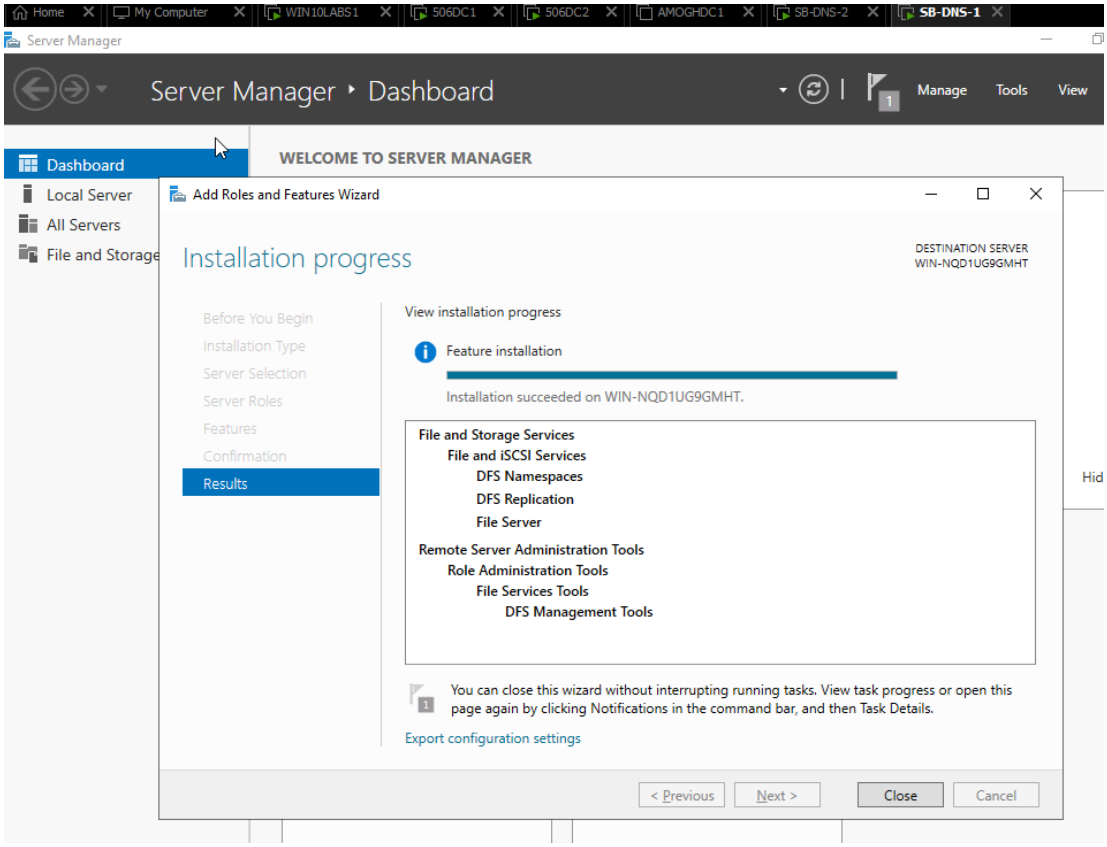


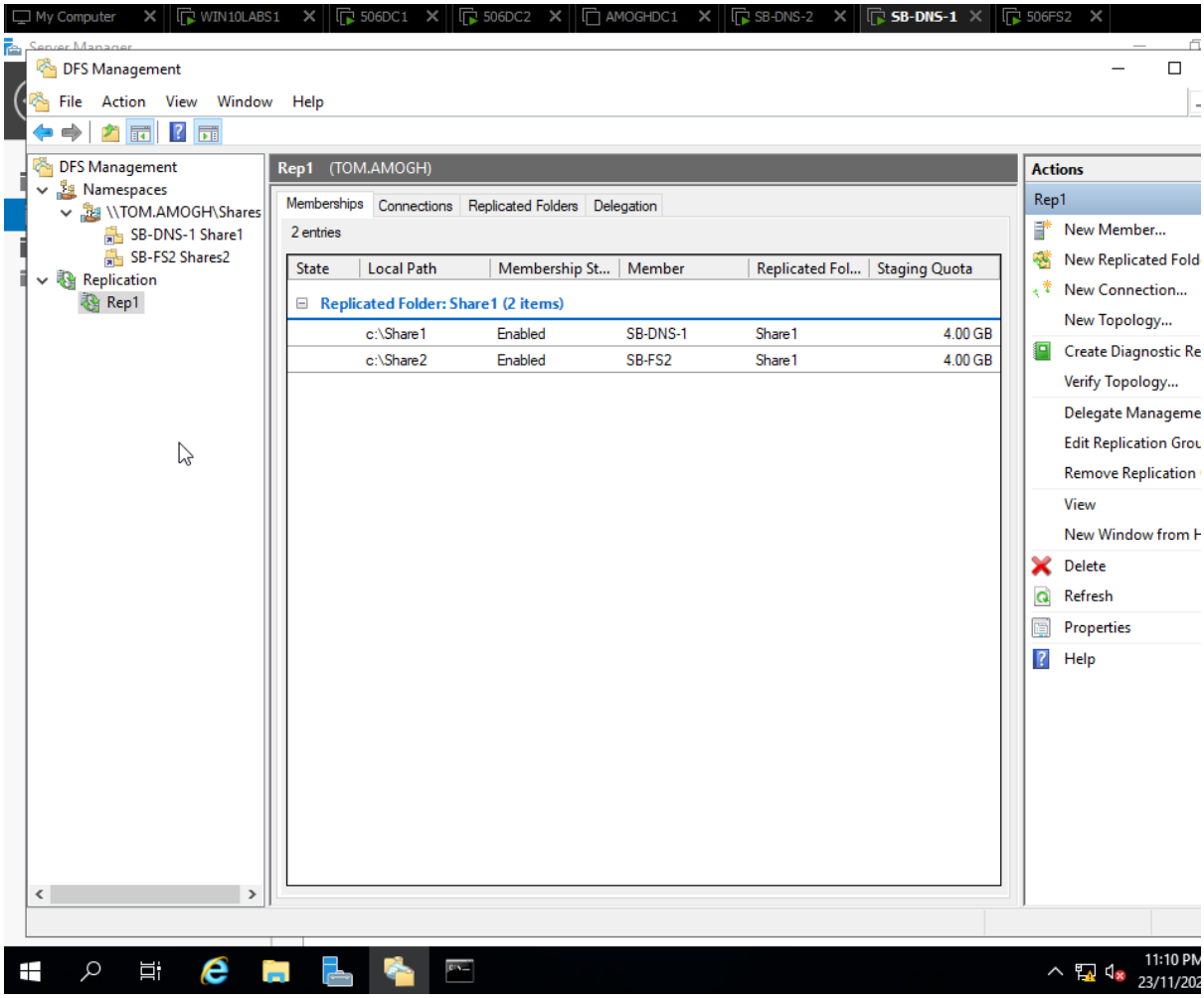
SCREENSHOT FOR 4.1


Server Manager
DNS Manager
File Action View Help
TOM.AMOGH Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
To add name servers to the list, click Add.
Name servers:
Server Fully Qualified Domain Name (FQDN)
IP Address
dc1.tom.amogh.
[192.168.2.2]
dc2.tom.amogh.
[172.16.0.2]
sb-dns-2.tom.amogh.
[192.168.2.4]
Add...
Edit...
Remove
* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.
OK
Cancel
Apply
Help
Dashboard
Local Server
All Servers
DNS
File and Storage
TASKS
DNS
dc1.tom.amogh
Forward Lookup Zone
_msdcs.TOM.AMO
TOM.AMOGH
_msdcs
_sites
_tcp
_udp
DomainDnsZo
ForestDnsZon
Reverse Lookup Zone
Trust Points
Conditional Forwarde
SB-DNS-2
Forward Lookup Zone
tom.amogh
Reverse Lookup Zone
Trust Points
Conditional Forwarde
Timestam
1.tom.amogh., hos... static
n.amogh. static
n.amogh. static
0.2 11/22/202
.2.2 11/22/202
.2.2 static
0.2 static
.2.4 11/23/202
-2.tom.amogh.
1:22 AM

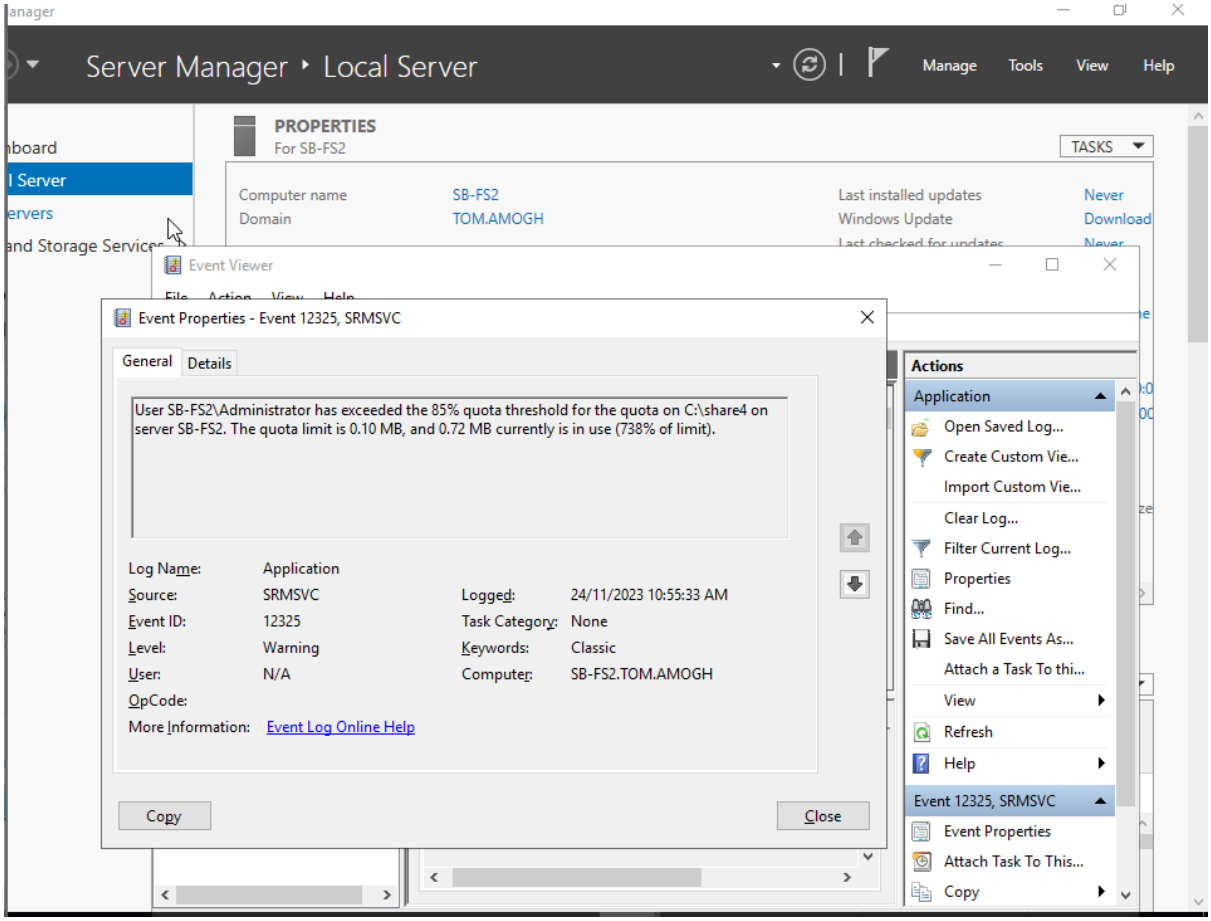


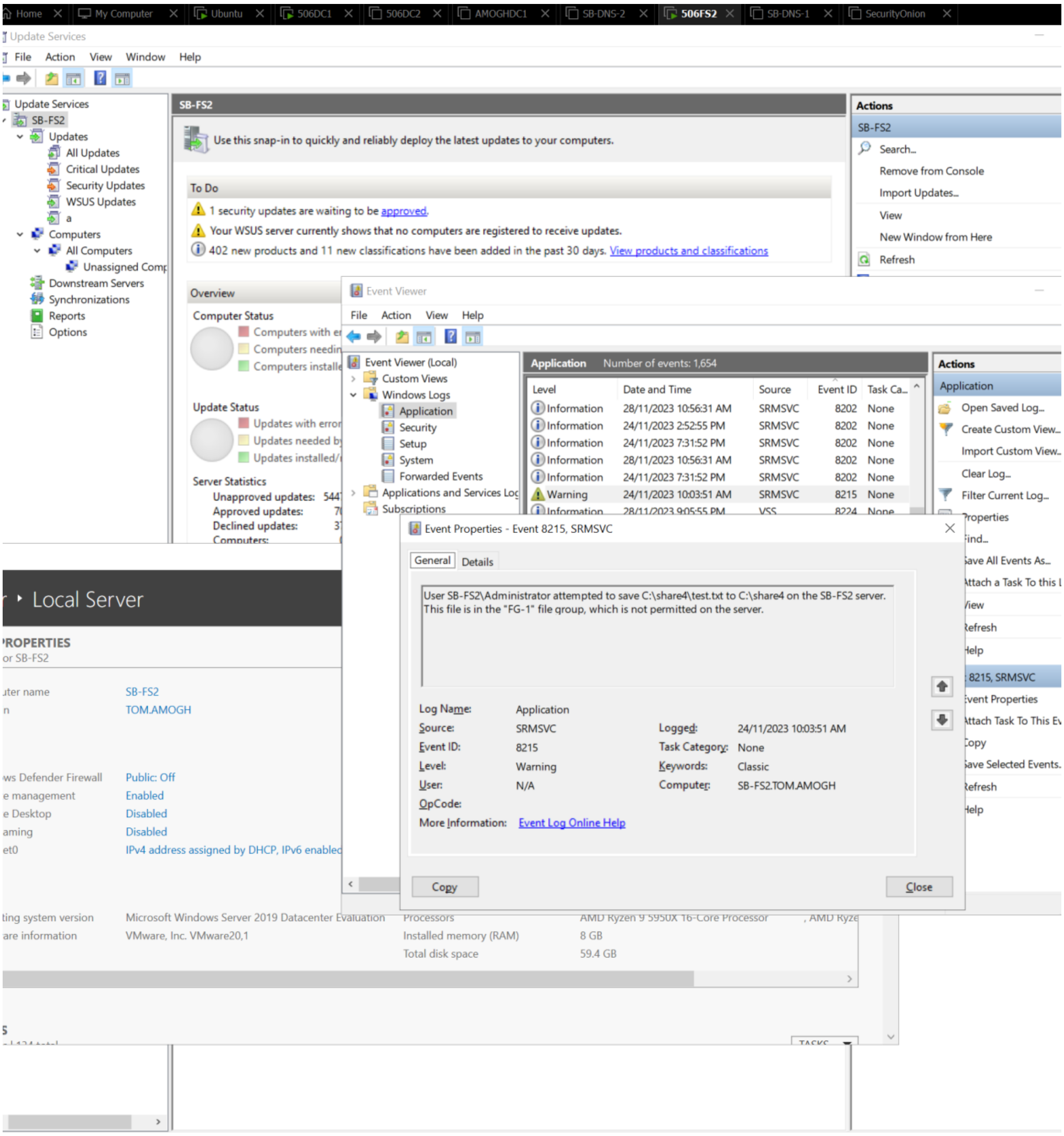
Lab 8.5 Follow the tutorial video 8.5 Install and configure DFS to do sublab 8.5. Take screenshots similar to the following which displays the domain name on the background. Please remove the demonstrated screenshots at the end.

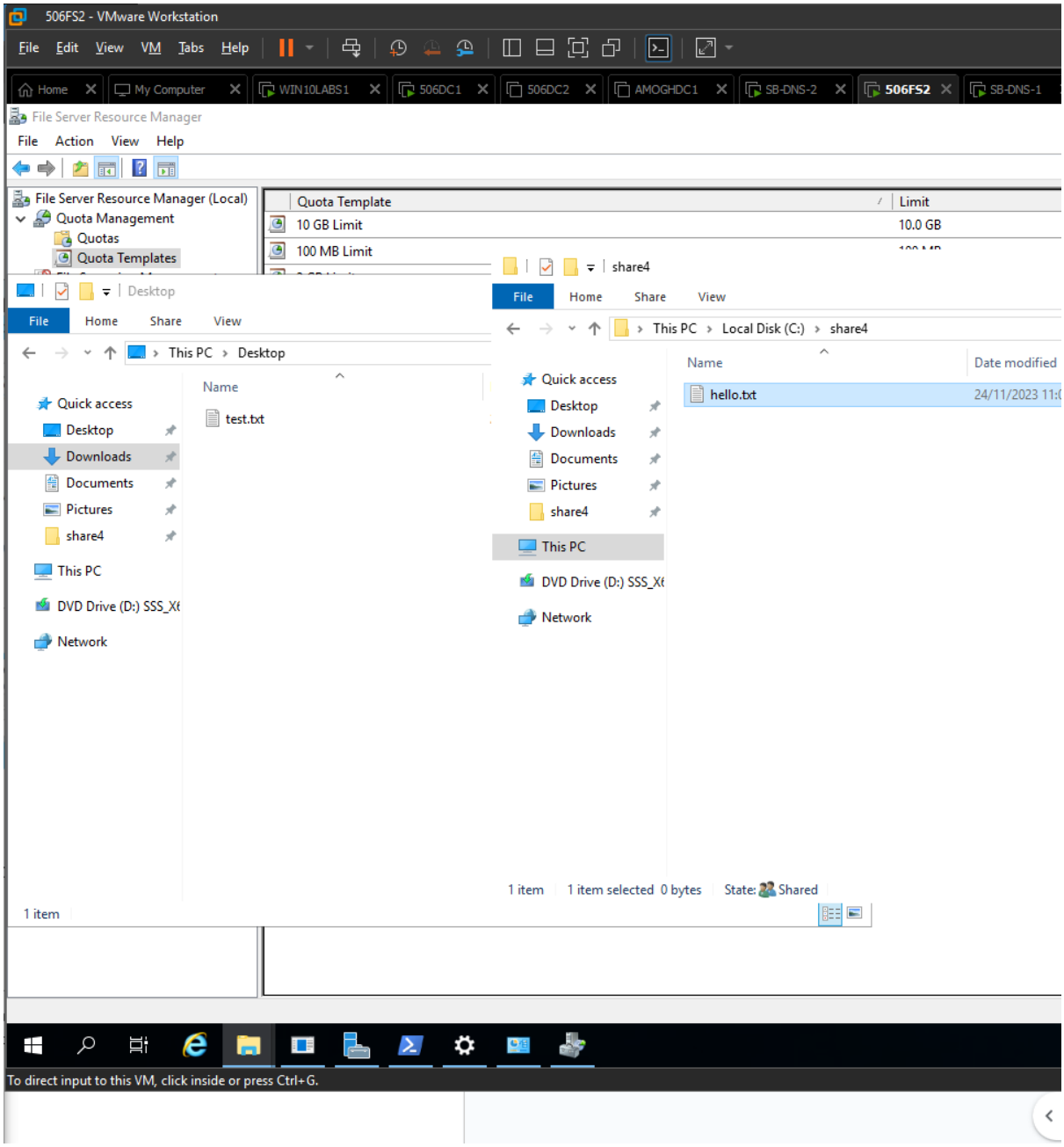

Home
My Computer
WIN10LABS1
506DC1
506DC2
AMOGHDC1
SB-DNS-2
SB-DNS-1
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Dashboard
Local Server
All Servers
File and Storage
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-NQD1UG9GMHT
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on WIN-NQD1UG9GMHT.
File and Storage Services
File and iSCSI Services
DFS Namespaces
DFS Replication
File Server
Remote Server Administration Tools
Role Administration Tools
File Services Tools
DFS Management Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

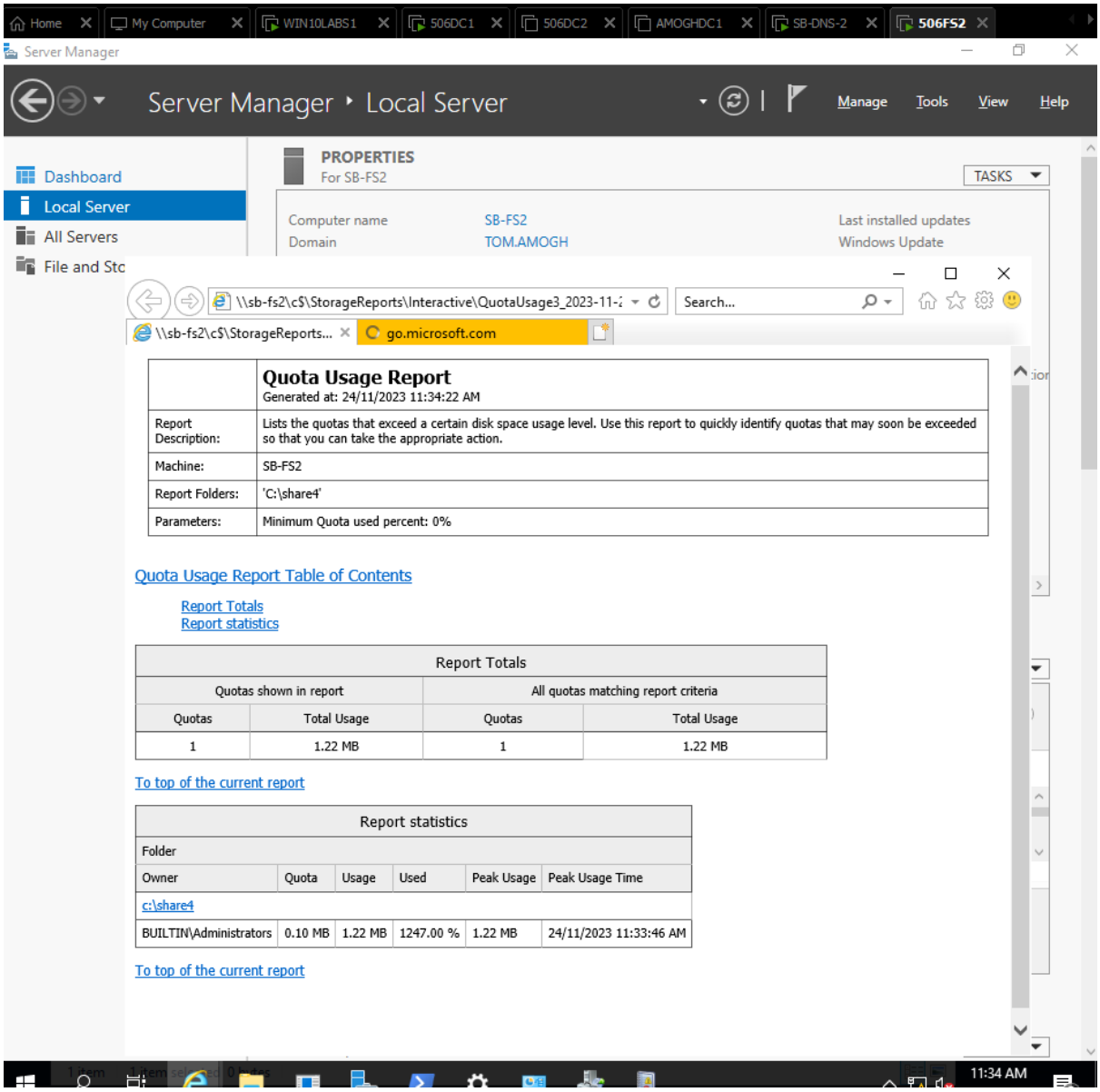

My Computer
WIN10LABS1
506DC1
506DC2
AMOGHDC1
SB-DNS-2
SB-DNS-1
506FS2
DFS Management
File
Action
View
Window
Help
DFS Management
Namespaces
\\TOM.AMOGH\Shares
SB-DNS-1 Share1
SB-FS2 Shares2
Replication
Rep1
Rep1 (TOM.AMOGH)
Memberships
Connections
Replicated Folders
Delegation
2 entries
State
Local Path
Membership St...
Member
Replicated Fol...
Staging Quota
Replicated Folder: Share1 (2 items)
c:\Share1
Enabled
SB-DNS-1
Share1
4.00 GB
c:\Share2
Enabled
SB-FS2
Share1
4.00 GB
Actions
Rep1
New Member...
New Replicated Fold
New Connection...
New Topology...
Create Diagnostic Re
Verify Topology...
Delegate Manageme
Edit Replication Grou
Remove Replication
View
New Window from H
Delete
Refresh
Properties
Help
11:10 PM

Lab 8.6 Follow the tutorial video 8.6_Install and configure FSRM. Take screenshots similar to the following which displays the domain name on the background. Please remove the demonstrated screenshots at the end.

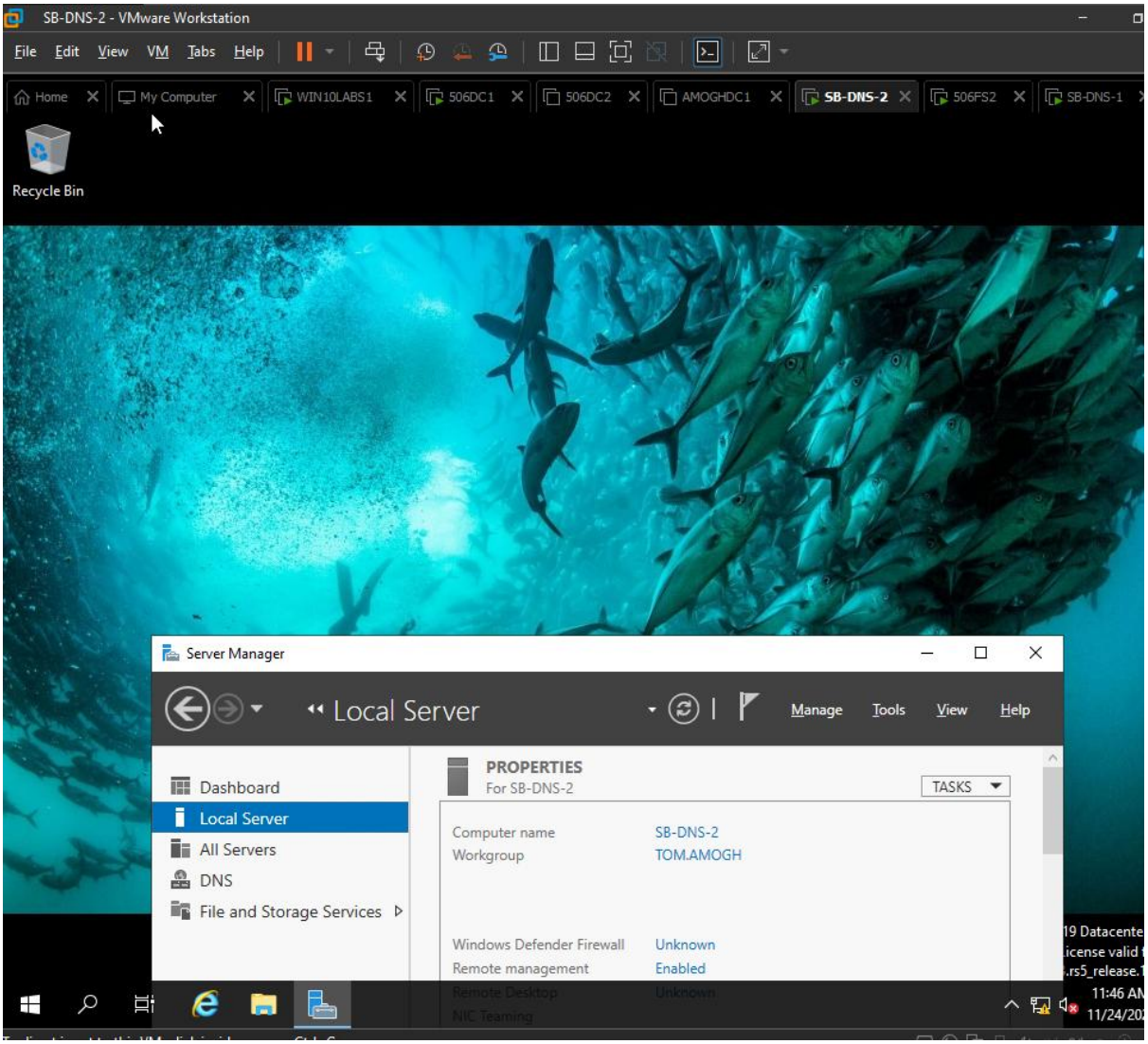


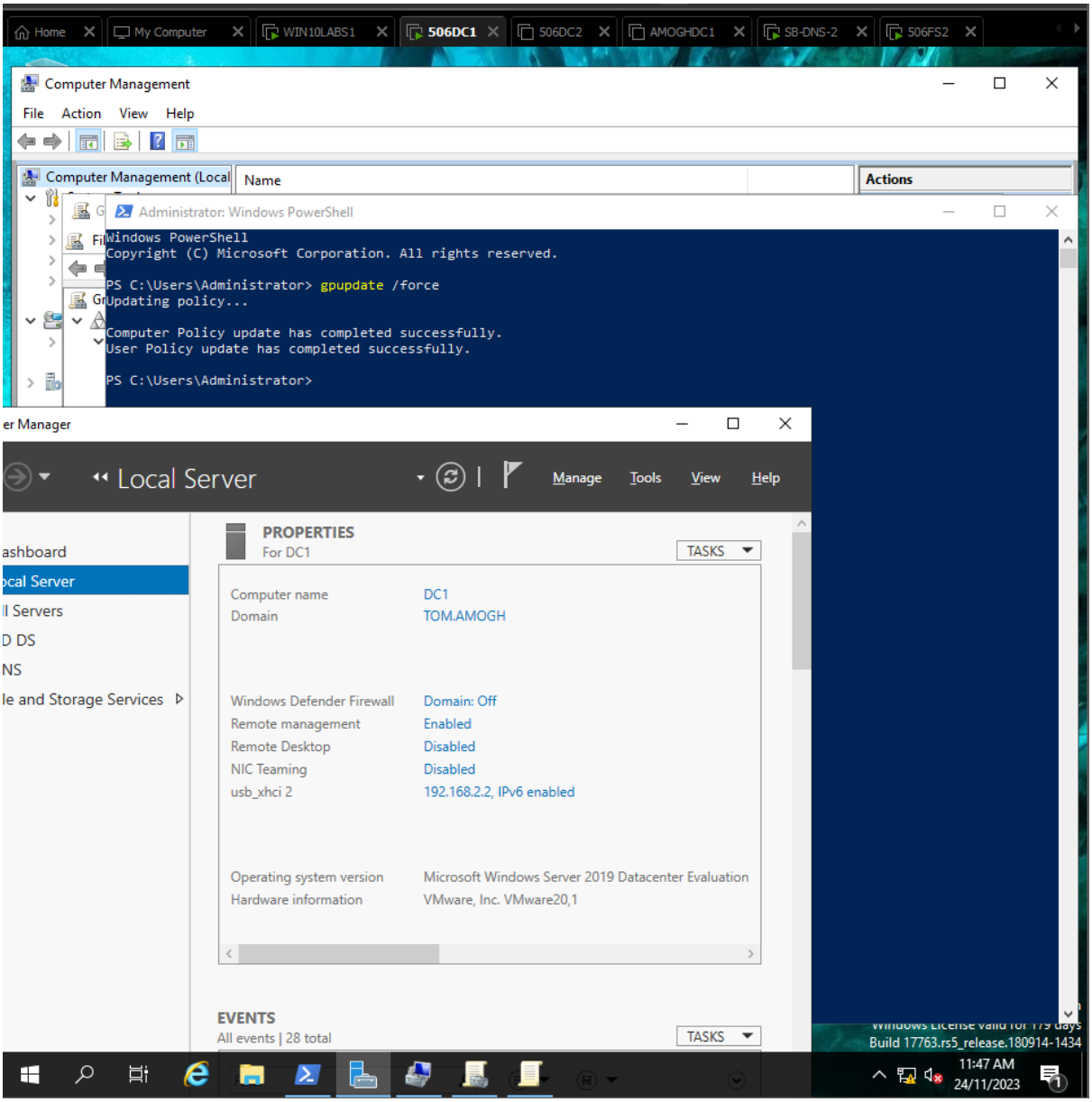

Update Services
File Action View Window Help
Update Services
SB-FS2
Updates
All Updates
Critical Updates
Security Updates
WSUS Updates
Computers
All Computers
Downstream Servers
Synchronizations
Reports
Options
SB-FS2
Use this snap-in to quickly and reliably deploy the latest updates to your computers.
To Do
1 security updates are waiting to be approved.
Your WSUS server currently shows that no computers are registered to receive updates.
402 new products and 11 new classifications have been added in the past 30 days. View products and classifications
Overview
Computer Status
Update Status
Server Statistics
Actions
SB-FS2
Search...
Remove from Console
Import Updates...
View
New Window from Here
Refresh
Event Viewer
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Application Number of events: 1,654
Level Date and Time Source Event ID Task Ca...
Information 28/11/2023 10:56:31 AM SRMSVC 8202 None
Information 24/11/2023 2:52:55 PM SRMSVC 8202 None
Information 24/11/2023 7:31:52 PM SRMSVC 8202 None
Information 28/11/2023 10:56:31 AM SRMSVC 8202 None
Information 24/11/2023 7:31:52 PM SRMSVC 8202 None
Warning 24/11/2023 10:03:51 AM SRMSVC 8215 None
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Event Properties - Event 8215, SRMSVC
General Details
User SB-FS2\Administrator attempted to save C:\share4\test.txt to C:\share4 on the SB-FS2 server. This file is in the "FG-1" file group, which is not permitted on the server.
Log Name: Application
Source: SRMSVC
Logged: 24/11/2023 10:03:51 AM
Event ID: 8215
Task Category: None
Level: Warning
Keywords: Classic
User: N/A
Computer: SB-FS2.TOM.AMOGH
OpCode:
More Information: Event Log Online Help
Copy
Close
Local Server
SB-FS2
TOM.AMOGH
Public: Off
Enabled
Disabled
IPv4 address assigned by DHCP, IPv6 enabled
Microsoft Windows Server 2019 Datacenter Evaluation
VMware, Inc. VMware20,1
Installed memory (RAM) 8 GB
Total disk space 59.4 GB


506FS2 - VMware Workstation
File Edit View VM Tabs Help
Home
My Computer
WIN10LABS1
506DC1
506DC2
AMOGHDC1
SB-DNS-2
506FS2
SB-DNS-1
File Server Resource Manager
File Action View Help
File Server Resource Manager (Local)
Quota Management
Quotas
Quota Templates
Quota Template
Limit
10 GB Limit
10.0 GB
100 MB Limit
Desktop
File Home Share View
This PC › Desktop
Quick access
Desktop
Downloads
Documents
Pictures
share4
This PC
DVD Drive (D:) SSS_X
Network
Name
test.txt
1 item
share4
File Home Share View
This PC › Local Disk (C:) › share4
Name
Date modified
hello.txt
1 item
1 item selected 0 bytes
State: Shared
To direct input to this VM, click inside or press Ctrl+G.

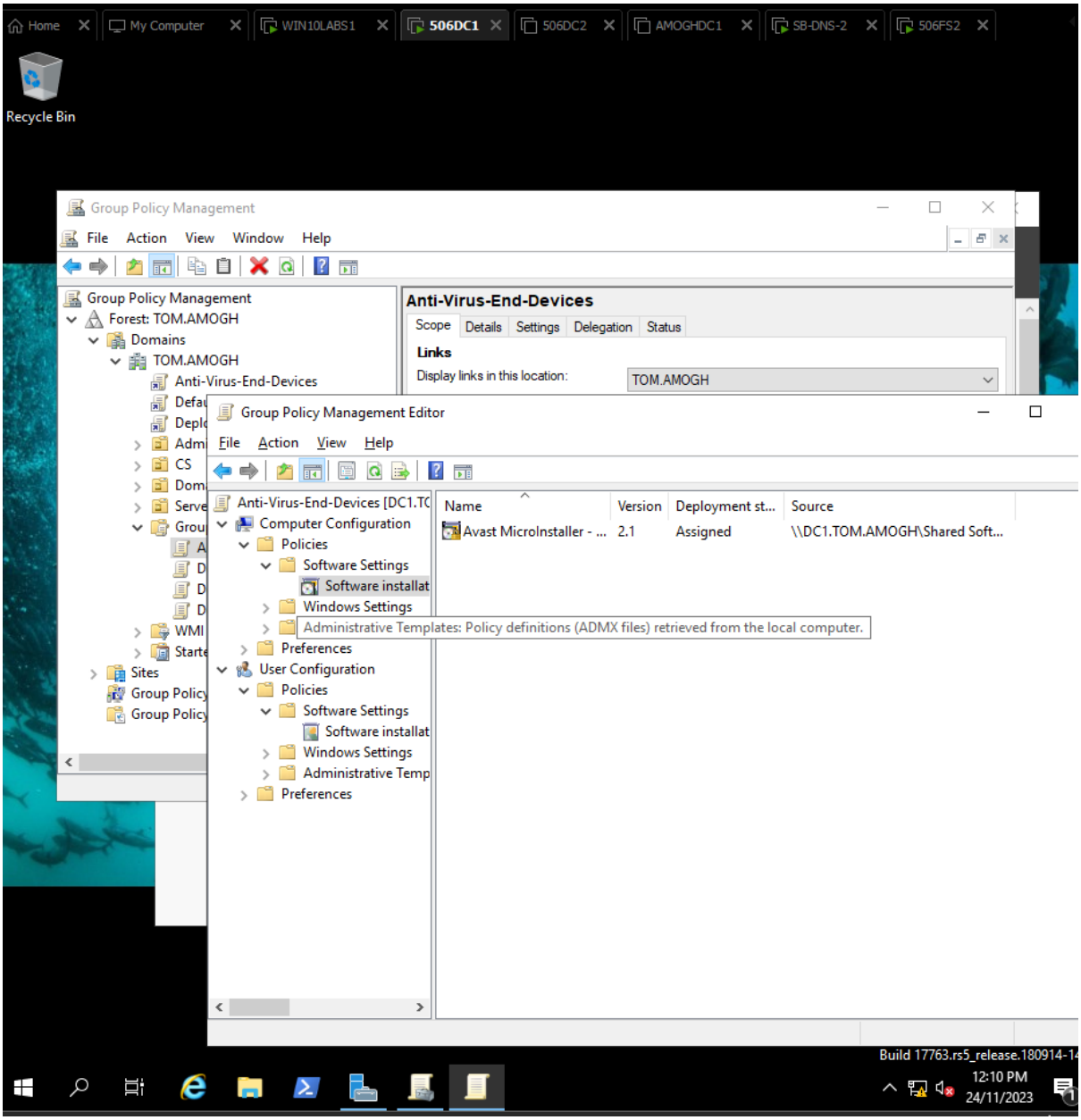


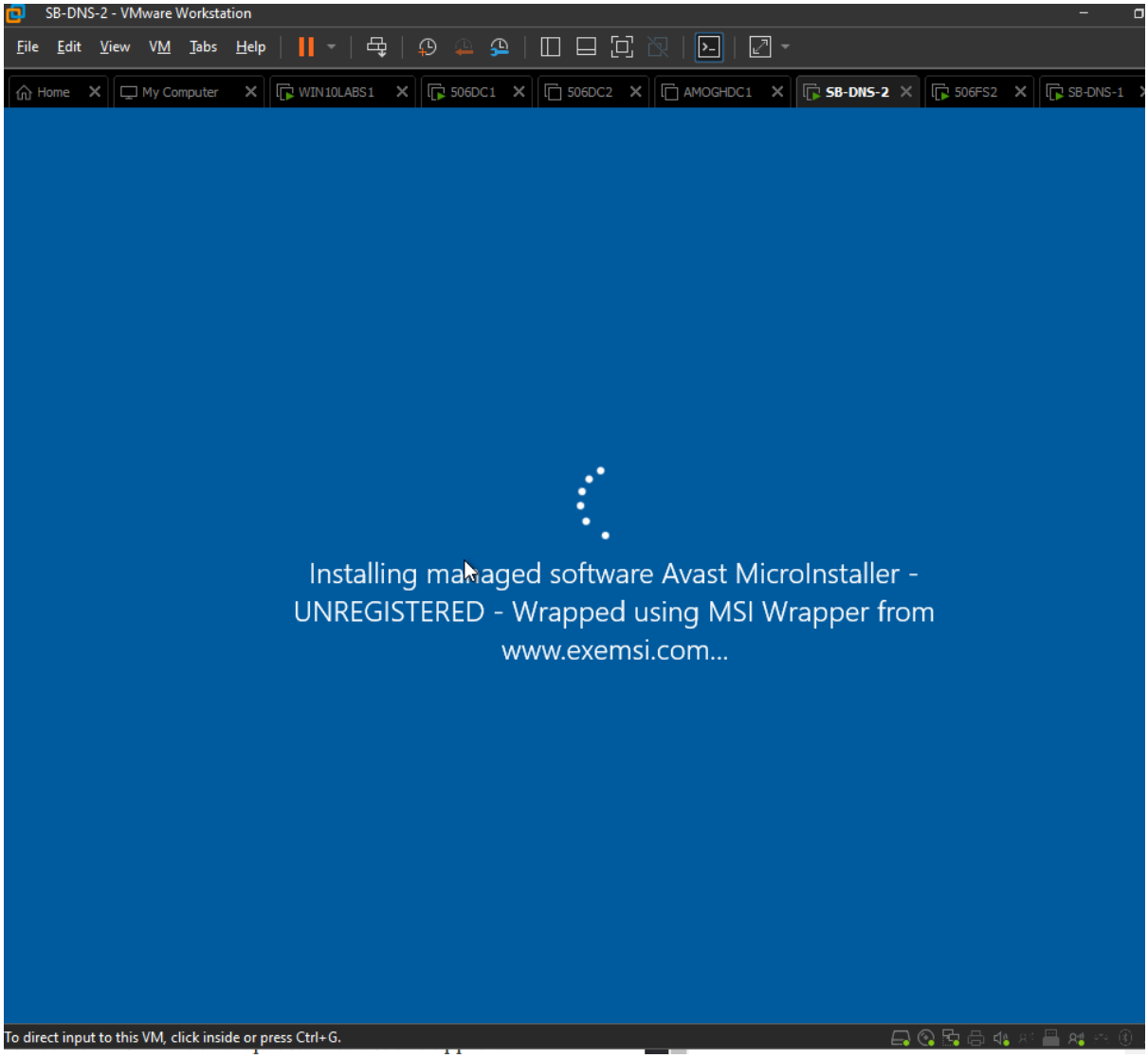
Lab 8.7 Follow the tutorial video 8.7 - Deploy Desktop Management via GPO to finish this subtask. Take screenshot at the end of the lab which displays the domain name on the background.


SB-DNS-2 - VMware Workstation
File Edit View VM Tabs Help
Home
My Computer
WIN10LABS1
506DC1
506DC2
AMOGHDC1
SB-DNS-2
506FS2
SB-DNS-1
Recycle Bin
Server Manager
Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
DNS
File and Storage Services
PROPERTIES
For SB-DNS-2
TASKS
Computer name SB-DNS-2
Workgroup TOM.AMOGH
Windows Defender Firewall Unknown
Remote management Enabled
Remote Desktop Unknown
NIC Teaming



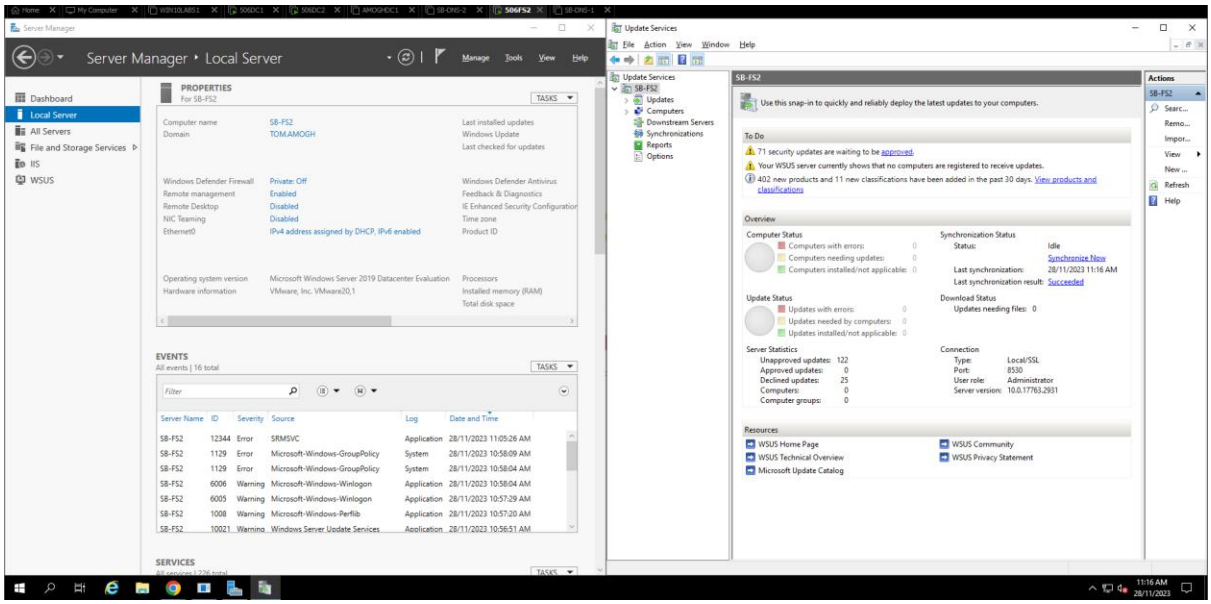
Lab 8.8 Follow the tutorial video 8.8 - Configure Anti-Virus Software Deployment via GPO to finish this subtask. Take screenshots similar to the following **which displays the domain name on the background**. Please remove the demonstrated screenshots at the end.

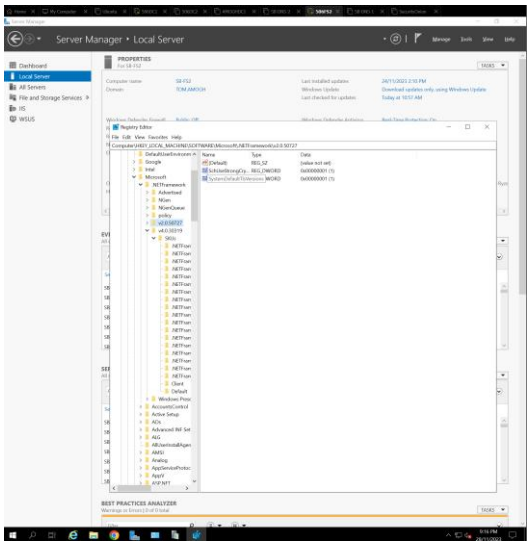

Home
My Computer
WIN10LABS1
506DC1
506DC2
AMOGHDC1
SB-DNS-2
506FS2
Recycle Bin
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: TOM.AMOGH
Domains
TOM.AMOGH
Anti-Virus-End-Devices
Anti-Virus-End-Devices
Scope Details Settings Delegation Status
Links
Display links in this location:
TOM.AMOGH
Group Policy Management Editor
File Action View Help
Anti-Virus-End-Devices [DC1.TO
Computer Configuration
Policies
Software Settings
Software installat
Windows Settings
Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.
Preferences
User Configuration
Policies
Software Settings
Software installat
Windows Settings
Administrative Temp
Preferences
Name
Version
Deployment st...
Source
Avast MicroInstaller - ...
2.1
Assigned
\\DC1.TOM.AMOGH\Shared Soft...
Build 17763.rs5_release.180914-14
12:10 PM
24/11/2023

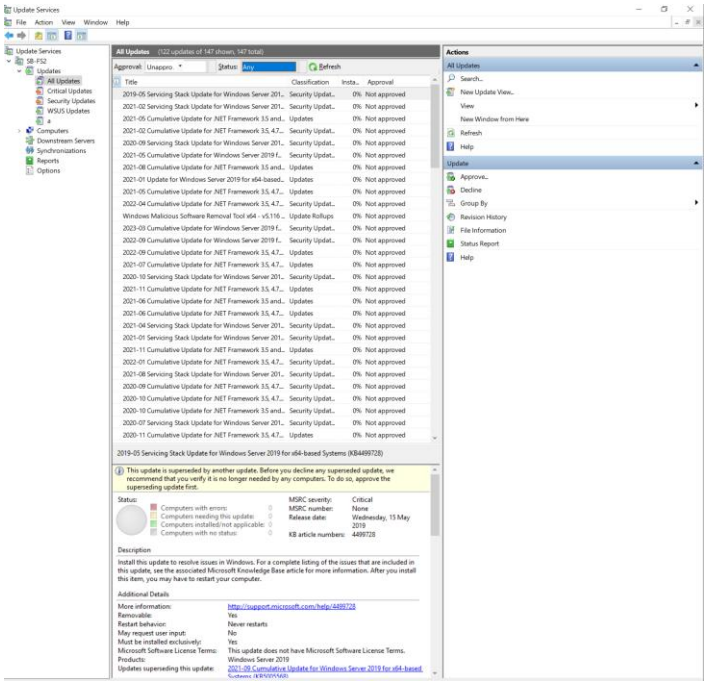


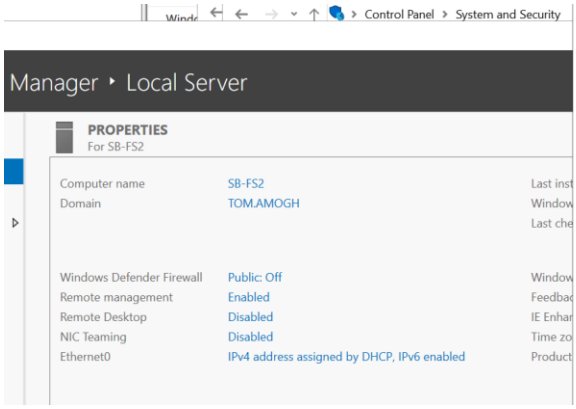
Lab 8.9 Follow the tutorial video 8.9_Install and configure WSUS. Take screenshots similar to the following which displays the domain name on the background. Please remove the demonstrated screenshots at the end. Take screenshots to demonstrate that the IIS server role has been installed on the WSUS server. Briefly describe what is web application.

Web applications are software programs accessible through web browsers over a network connection. They come in various forms, including static websites that display fixed content, dynamic applications that generate content based on user interactions or database data, and interactive applications that enable user actions like online shopping or social networking. These applications utilize web technologies such as HTML, CSS, JavaScript for front-end presentation, and backend server scripting languages like PHP, Python, or Ruby to process and manage data. Web applications are ubiquitous, serving a wide range of purposes, from e-commerce to content management.


Server Manager
Server Manager • Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
WSUS
PROPERTIES
For SB-FS2
TASKS
Computer name SB-FS2
Domain TOM.AMOGH
Last installed updates
Windows Update
Last checked for updates
Windows Defender Firewall Private: Off
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 IPv4 address assigned by DHCP, IPv6 enabled
Windows Defender Antivirus
Feedback & Diagnostics
IE Enhanced Security Configuration
Time zone
Product ID
Operating system version Microsoft Windows Server 2019 Datacenter Evaluation
Hardware information VMware, Inc. VMware20,1
Processors
Installed memory (RAM)
Total disk space
EVENTS
All events | 16 total
Server Name ID Severity Source Log Date and Time
SB-FS2 12344 Error SRMSVC Application 28/11/2023 11:05:26 AM
SB-FS2 1129 Error Microsoft-Windows-GroupPolicy System 28/11/2023 10:58:09 AM
SB-FS2 1129 Error Microsoft-Windows-GroupPolicy System 28/11/2023 10:58:04 AM
SB-FS2 6006 Warning Microsoft-Windows-Winlogon Application 28/11/2023 10:58:04 AM
SB-FS2 6005 Warning Microsoft-Windows-Winlogon Application 28/11/2023 10:57:29 AM
SB-FS2 1008 Warning Microsoft-Windows-Perflib Application 28/11/2023 10:57:20 AM
SB-FS2 10021 Warning Windows Server Update Services Application 28/11/2023 10:56:51 AM
SERVICES
Update Services
File Action View Window Help
SB-FS2
Updates
Computers
Downstream Servers
Synchronizations
Reports
Options
Use this snap-in to quickly and reliably deploy the latest updates to your computers.
To Do
71 security updates are waiting to be approved.
Your WSUS server currently shows that no computers are registered to receive updates.
402 new products and 11 new classifications have been added in the past 30 days. View products and classifications
Overview
Computer Status
Computers with errors: 0
Computers needing updates: 0
Computers installed/not applicable: 0
Synchronization Status
Status: Idle
Synchronize Now
Last synchronization: 28/11/2023 11:16 AM
Last synchronization result: Succeeded
Update Status
Updates with errors: 0
Updates needed by computers: 0
Updates installed/not applicable: 0
Download Status
Updates needing files: 0
Server Statistics
Unapproved updates: 122
Approved updates: 0
Declined updates: 25
Computers: 0
Computer groups: 0
Connection
Type: Local/SSL
Port: 8530
User role: Administrator
Server version: 10.0.17763.2931
Resources
WSUS Home Page
WSUS Technical Overview
Microsoft Update Catalog
WSUS Community
WSUS Privacy Statement
Actions
SB-FS2
Refresh
Help
11:16 AM
28/11/2023


Server Manager • Local Server
PROPERTIES
BEST PRACTICES ANALYZER





2021-01 Update for Windows Server 2019 for x64-based Systems (KB4589208)

Successfully installed on 24/11/2023

2023-11 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB503

Successfully installed on 24/11/2023

Driver Updates (1)

VMware, Inc. - System - 9.8.18.0

Successfully installed on 23/11/2023

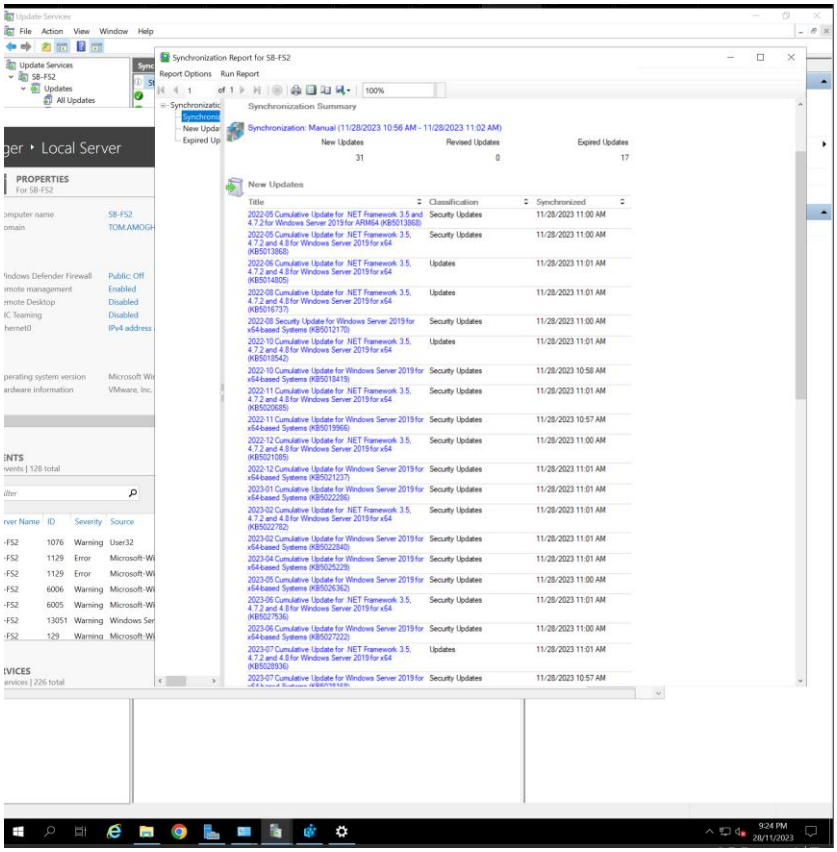
Definition Updates (2)

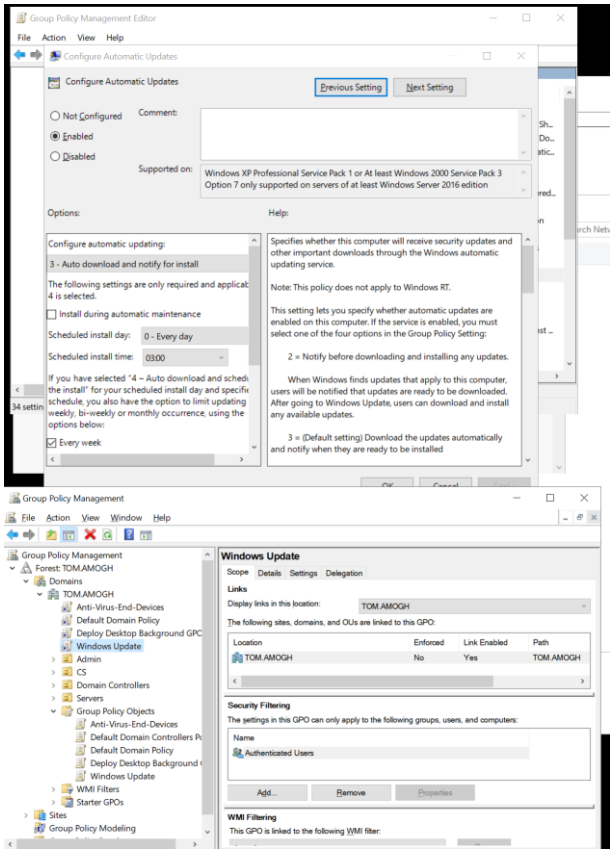
Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2

Successfully installed on 24/11/2023

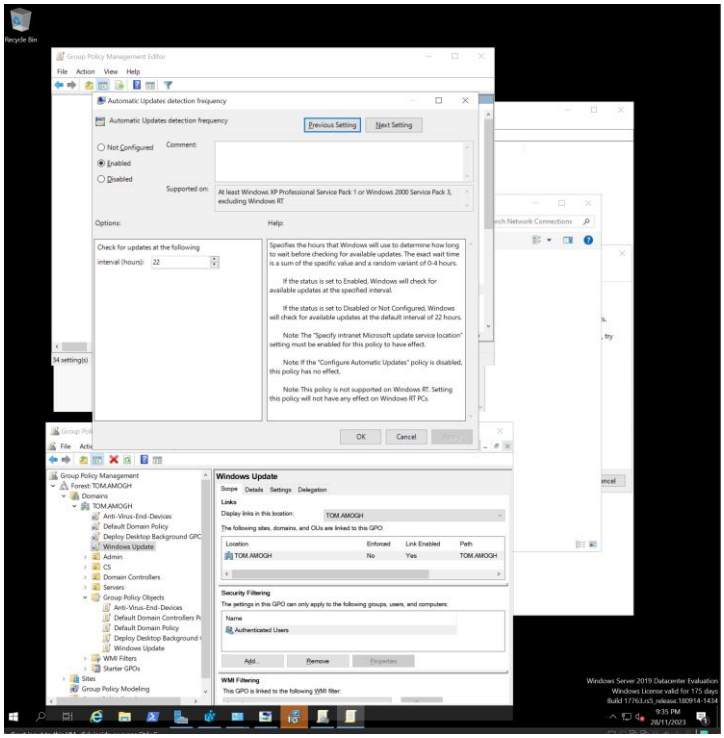
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.401.10

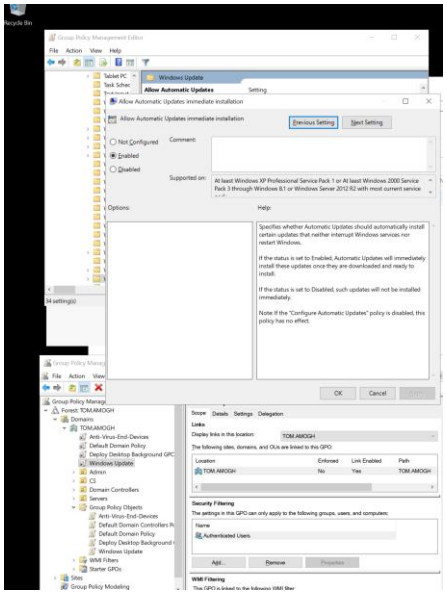
Successfully installed on 24/11/2023

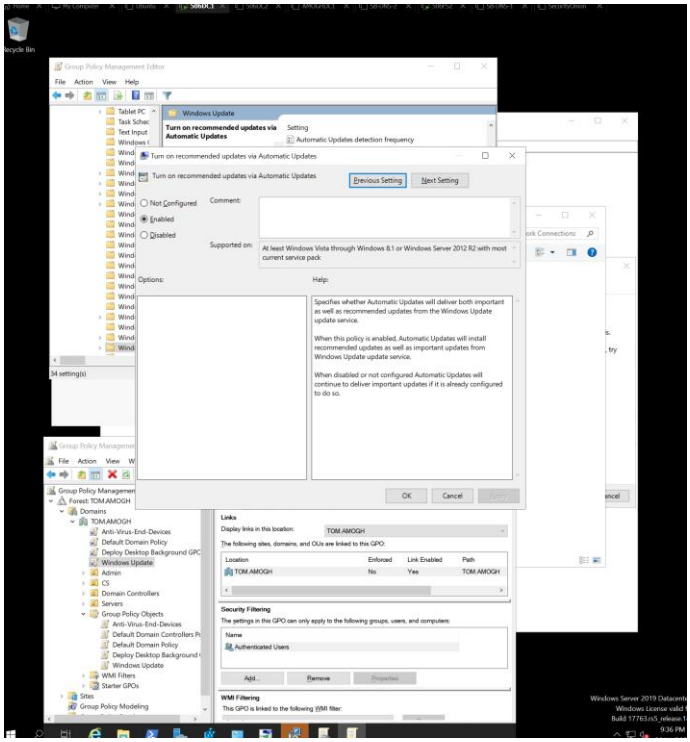

Update Services
File Action View Window Help
Synchronization Report for SB-FS2
Report Options Run Report
Synchronization Summary
Synchronization: Manual (11/28/2023 10:56 AM - 11/28/2023 11:02 AM)
New Updates
Revised Updates
Expired Updates
31
0
17
New Updates
Title
Classification
Synchronized
Local Server
PROPERTIES
For SB-FS2
9:24 PM
28/11/2023


Group Policy Management Editor
File Action View Help
Configure Automatic Updates
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Option 7 only supported on servers of at least Windows Server 2016 edition
Options:
Help:
Configure automatic updating:
3 - Auto download and notify for install
Install during automatic maintenance
Scheduled install day:
0 - Every day
Scheduled install time:
03:00
Every week
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.
Note: This policy does not apply to Windows RT.
This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:
2 = Notify before downloading and installing any updates.
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

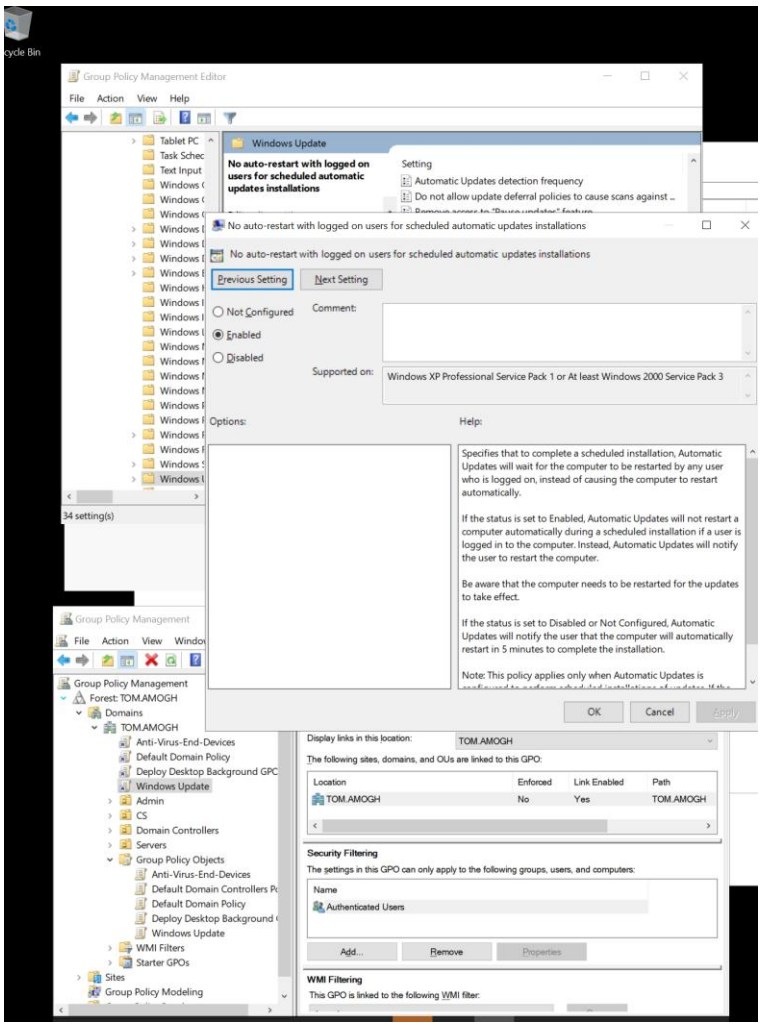
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: TOM.AMOGH
Domains
TOM.AMOGH
Anti-Virus-End-Devices
Default Domain Policy
Deploy Desktop Background GPO
Windows Update
Admin
CS
Domain Controllers
Servers
Group Policy Objects
Anti-Virus-End-Devices
Default Domain Policy
Windows Update
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Windows Update
Scope Details Settings Delegation
Links
Display links in this location: TOM.AMOGH
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
TOM.AMOGH
No
Yes
TOM.AMOGH
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:

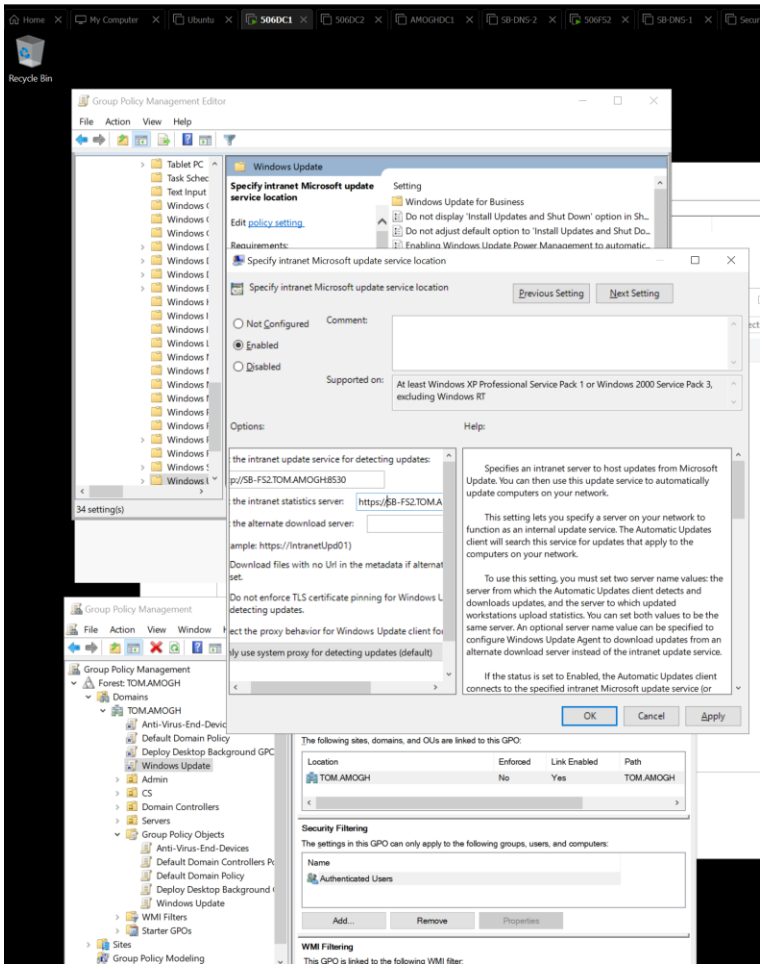

Recycle Bin
Group Policy Management Editor
File Action View Help
Automatic Updates detection frequency
Automatic Updates detection frequency
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT
Options:
Help:
Check for updates at the following interval (hours): 22
Specifies the hours that Windows will use to determine how long to wait before checking for available updates. The exact wait time is a sum of the specific value and a random variant of 0-4 hours.
If the status is set to Enabled, Windows will check for available updates at the specified interval.
If the status is set to Disabled or Not Configured, Windows will check for available updates at the default interval of 22 hours.
Note: The "Specify intranet Microsoft update service location" setting must be enabled for this policy to have effect.
Note: If the "Configure Automatic Updates" policy is disabled, this policy has no effect.
Note: This policy is not supported on Windows RT. Setting this policy will not have any effect on Windows RT PCs.
OK
Cancel
Apply
34 setting(s)
Group Policy Management
Forest: TOM.AMOGH
Domains
TOM.AMOGH
Anti-Virus-End-Devices
Default Domain Policy
Deploy Desktop Background GPO
Windows Update
Admin
CS
Domain Controllers
Servers
Group Policy Objects
Anti-Virus-End-Devices
Default Domain Controllers Policy
Default Domain Policy
Deploy Desktop Background GPO
Windows Update
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Windows Update
Scope
Details
Settings
Delegation
Links
Display links in this location:
TOM.AMOGH
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
TOM.AMOGH
No
Yes
TOM.AMOGH
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:
Windows Server 2019 Datacenter Evaluation
Windows License valid for 175 days
Build 17763.rs5_release.180914-1434
9:35 PM
28/11/2023

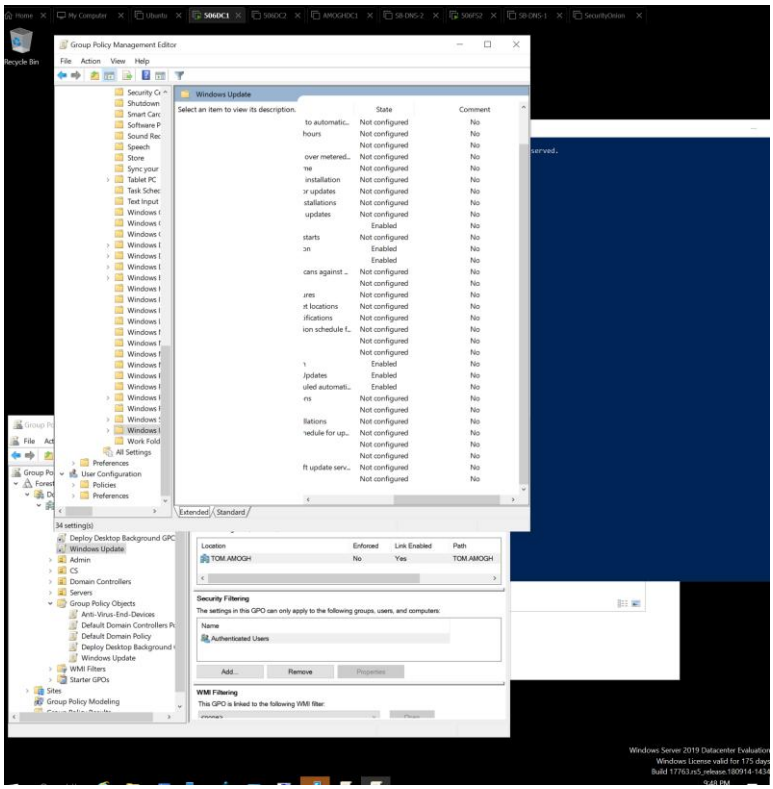

Recycle Bin
Group Policy Management Editor
File Action View Help
Windows Update
Allow Automatic Updates
Setting
Allow Automatic Updates immediate installation
Allow Automatic Updates immediate installation
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 through Windows 8.1 or Windows Server 2012 R2 with most current service
Options:
Help:
Specifies whether Automatic Updates should automatically install certain updates that neither interrupt Windows services nor restart Windows.
If the status is set to Enabled, Automatic Updates will immediately install these updates once they are downloaded and ready to install.
If the status is set to Disabled, such updates will not be installed immediately.
Note: If the "Configure Automatic Updates" policy is disabled, this policy has no effect.
OK
Cancel
Apply
34 setting(s)
Group Policy Management
Forest: TOM.AMOGH
Domains
TOM.AMOGH
Anti-Virus-End-Devices
Default Domain Policy
Deploy Desktop Background GPO
Windows Update
Admin
CS
Domain Controllers
Servers
Group Policy Objects
Anti-Virus-End-Devices
Default Domain Controllers Policy
Default Domain Policy
Deploy Desktop Background GPO
Windows Update
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Scope
Details
Settings
Delegation
Links
Display links in this location:
TOM.AMOGH
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
TOM.AMOGH
No
Yes
TOM.AMOGH
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering

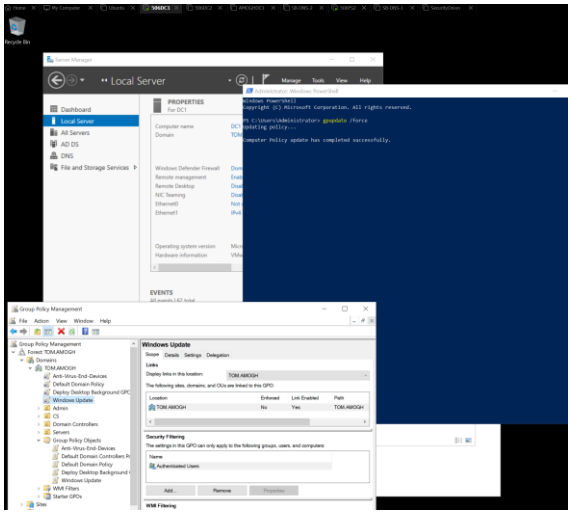


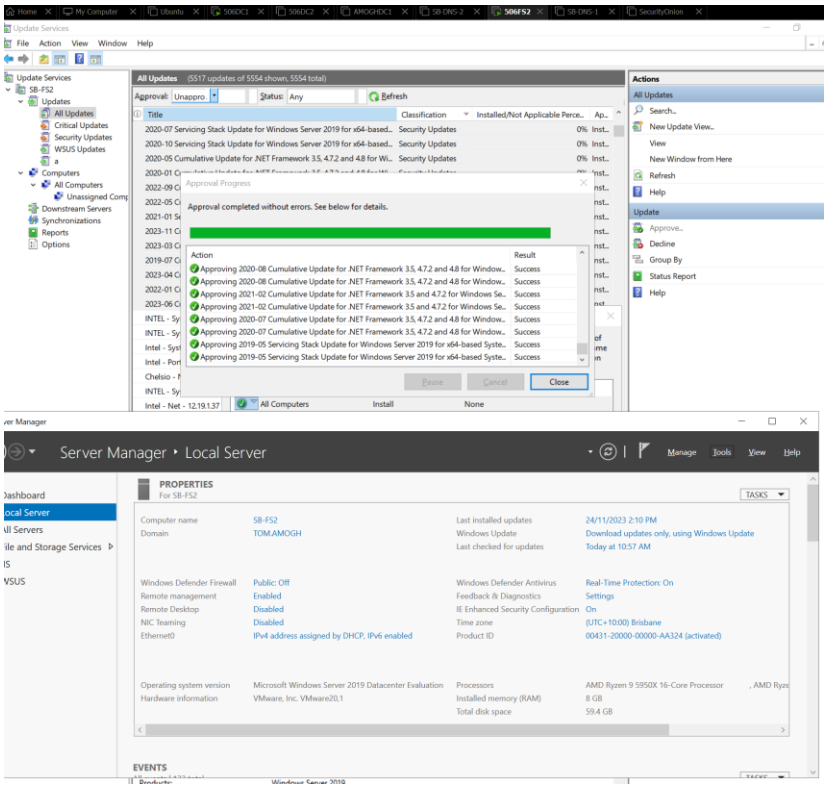
(ignore orange installer vmware tools reinstalling had network driver issues)




Group Policy Management Editor
Windows Update
Specify intranet Microsoft update service location
Edit policy setting
Requirements:
Setting
Windows Update for Business
Specify intranet Microsoft update service location
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT
Options:
Help:
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.
This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.
To use this setting, you must set two server name values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server. An optional server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.
If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service (or
OK
Cancel
Apply
Group Policy Management
Forest: TOM.AMOGH
Domains
TOM.AMOGH
Default Domain Policy
Windows Update
Admin
CS
Domain Controllers
Servers
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
TOM.AMOGH
No
Yes
TOM.AMOGH
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add...
Remove
Properties
WMI Filtering
This GPO is linked to the following WMI filter:


Group Policy Management Editor
Windows Update
Select an item to view its description.
State
Comment
Extended
Standard
Windows Server 2019 Datacenter Evaluation

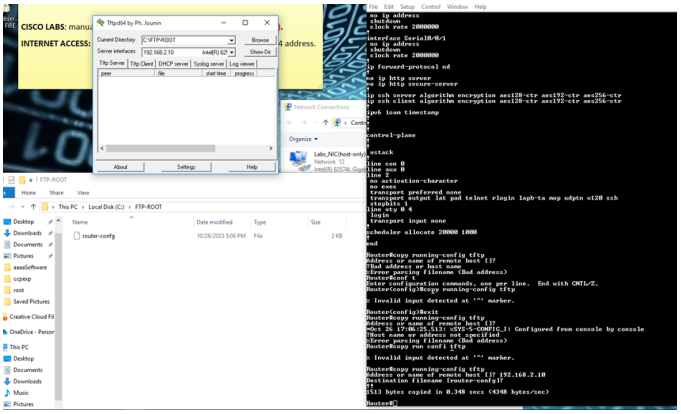




Lab 8.10 Install a simple FTP server and demonstrate the FTP services running with screenshots. Briefly describe what is FTP protocol.

FTP is a standard protocol and is layer 7 in the OSI model. ftp client can be used to establish connections usign the prefix ftp://. FTP can either be in Active, which is a much simpler way of setting it up where the client initiates the command and opens a connection from port 20. Passive mode is a lot more difficult to understand where it opens a random port and informs the client of the port through the control connection(port 21).

however what we are doing here is TFTP (Trivial File Transfer protocol), TFTP uses port 69 (UDP) for connection and has no authentication methods like FTP. TFTP specializes in PXE and Router configurations like what we are doing due to the simplicity and lightweight implementation of it.

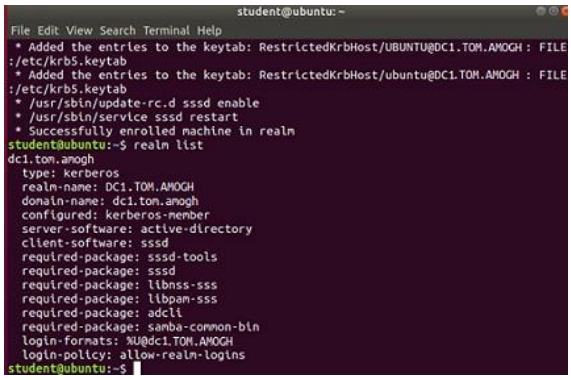


(PRACTICAL DEMONSTRATED IN CLASS, DID THIS ALONGSIDE COPYING RUNNING-CONFIGS TO THE REGISTRY OF NVRAM SO CONFIGS WOULD STAY, HERE IS MY EXTENDED CONFIGURATION:

```
config-register 0x2142
do wr
copy run start
!!turn off router power
!!turn on
do copy start run
reload
```

FThis specific command was able to not run the starting configuration files and just run into ROMMON mode which enabled the config files to later be copied (which were still saved) and then run the router without tftp which made it much easier to transfer between labs and configuration sets that we've previously done.

Lab 8.11 Follow the tutorial video 8.10_ Joining a Ubunutu to AD Domain. Take screenshots similar to the following which displays the domain name on the terminal. Please remove the demonstrated screenshots at the end.

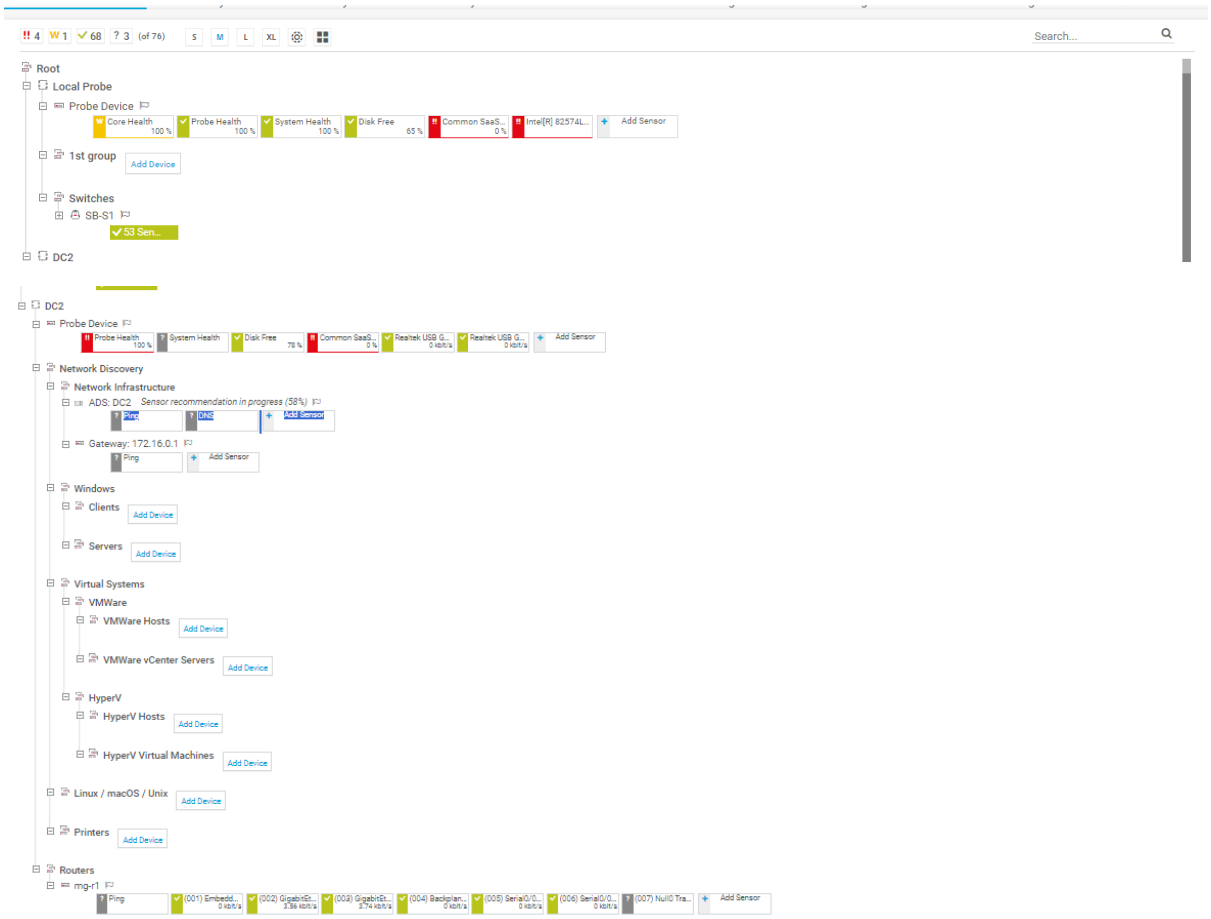


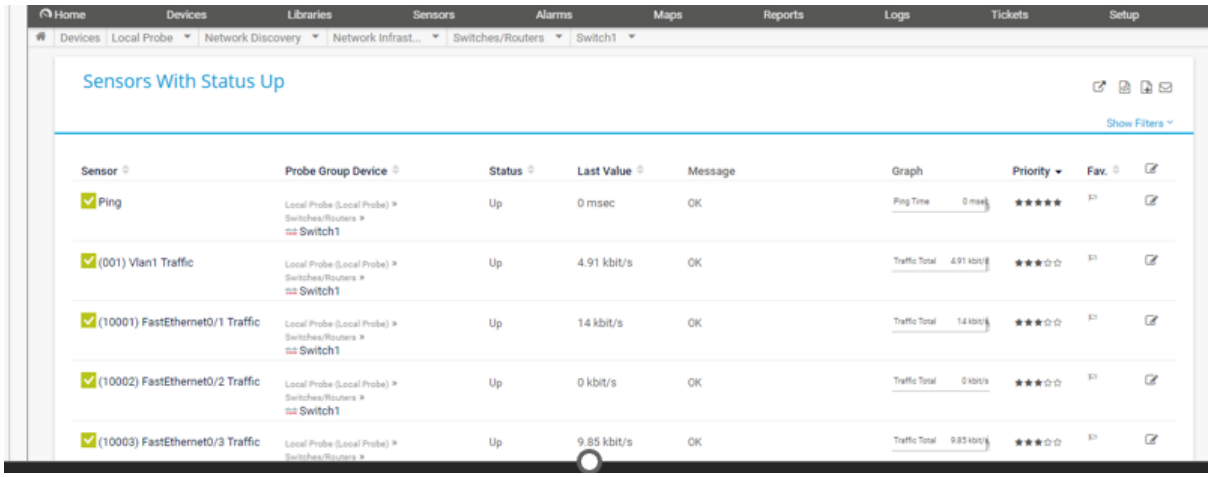
Lab 9 Results

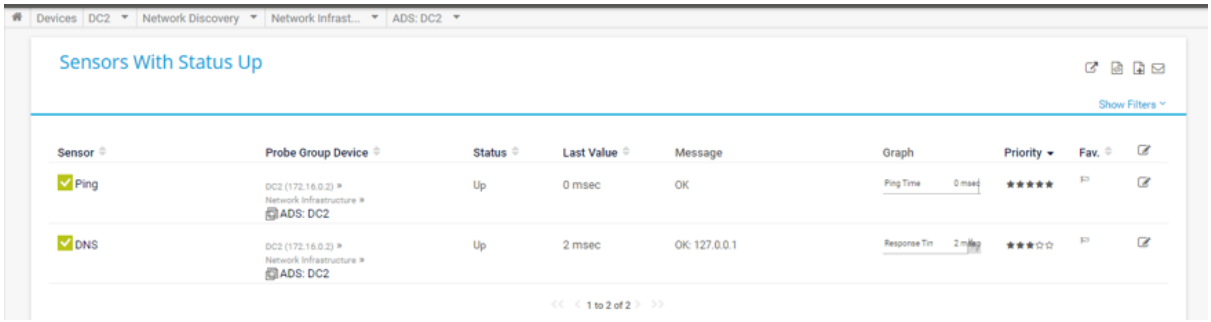
Follow the PRTG tutorial video and refer to the teaching lab manual on Connect to finish the lab. Obtain sign-off from the teacher and attach the lab screenshots below.

See the details that are highlighted with the red tangle. They should demonstrate your domain name on the background, devices under local probe should have the sensors of both snmp traffic and syslog, and devices under remote probe should have both snmp traffic sensor and syslog sensor.

PRTG SETUP IN CLASS SUCCESSFULLY.

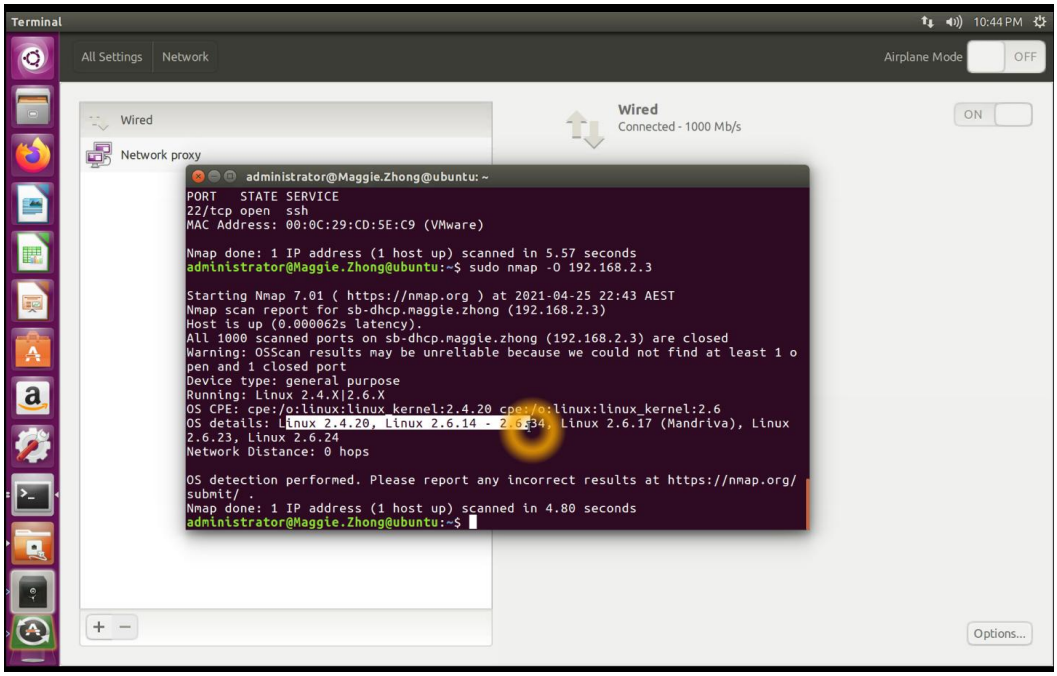


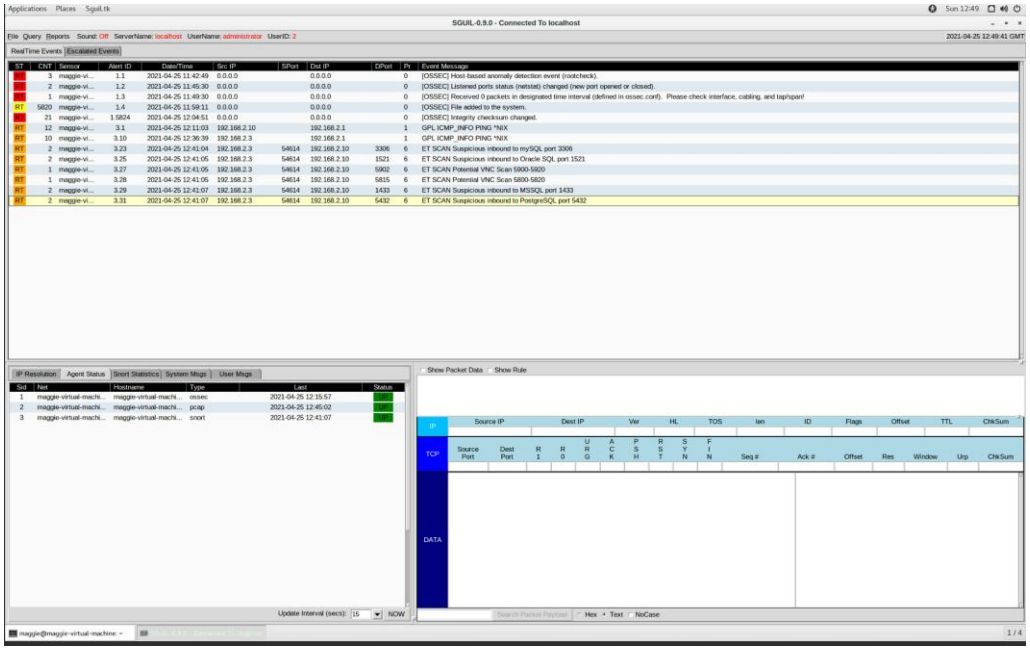




Lab 10 Results

Follow the tutorial video for Security Onion to do the lab. Take screenshots similar to the following and replace the demonstrated ones when you get marked off from the teacher.





Part 10.1. Write a troubleshooting report about the following aspects:

- Describe network symptoms that came across to you.

  Users were experiencing intermittent network connectivity issues.

  DNS queries were occasionally failing, preventing access to websites.

  Email delivery was delayed, with some messages not arriving for hours.

  There were reports of slow user authentication and login processes.

  Access to network file shares was sporadic, impacting workflow.

- Describe what troubleshooting tools and techniques, including any network diagnostic utilities you use to find out what is the cause to the network issues.

  Ping and Traceroute: Used to check for connectivity problems and visualize the path network traffic takes.

  NSLookup/Dig: To test DNS resolution functionality and ensure proper DNS operation between different servers.

  Wireshark: To capture and analyze network traffic, particularly examining DNS, SMB, and authentication protocols.

  Event Viewer/Server Logs: To check for any system errors or service failures that correlate with reported issues.

  Active Directory Replication Status Tool: This was used to verify that the domain controllers were properly replicating data.

- Describe how you resolve the issues

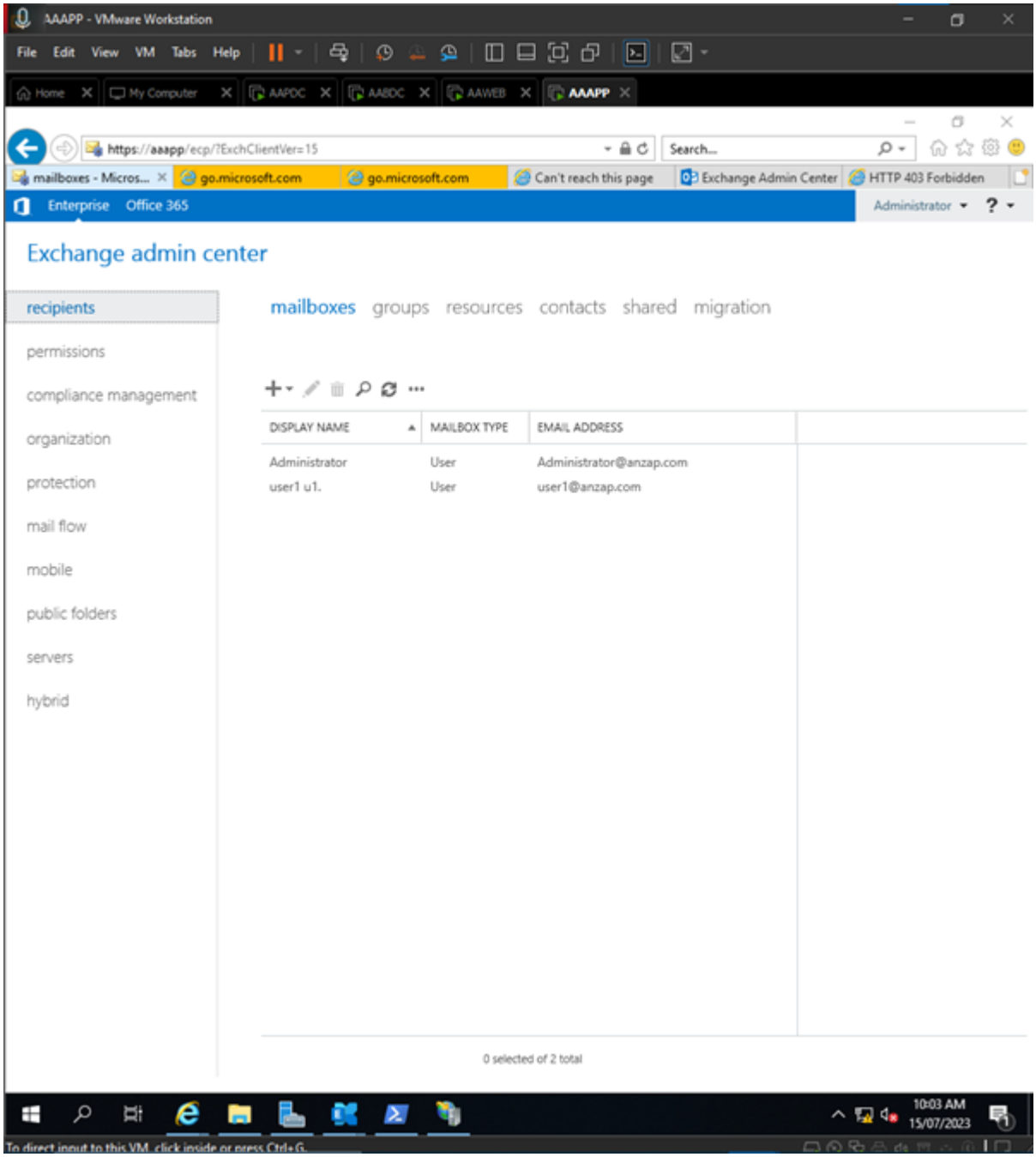
  DNS Issues: Configured DNS zone transfers and executed a forced sync between the domain controllers to ensure consistent DNS resolution across the network.

Email Delays: Troubleshot the mail server's queue processing settings and incremented server resources to manage high volume of email traffic.

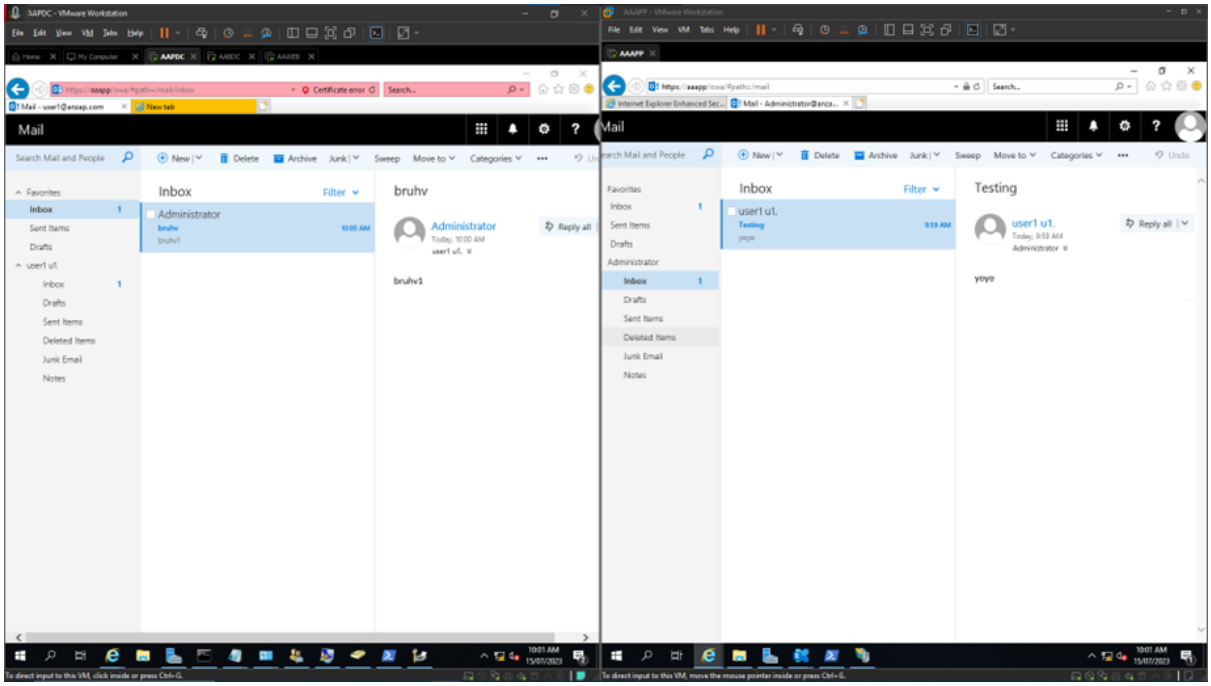
Authentication Delays: Deployed additional domain controllers and configured load balancing to handle peak login periods.

File Share Access: Identified and replaced a faulty network switch and updated the infrastructure to include network redundancy, preventing future access interruptions.

Import other domain users to the email list



Test send and receive emails with different user accounts


Mail
Inbox
Filter
Administrator
bruhv
bruhv1
Testing
user1 u1.
yoyo
Reply all