PROJECT IMPLEMENTATION

Optimus Consultant

MAN KIT KWAN / 16442974

Table of Contents

1.0 Configuration on Routers 5

1.1 Configuring Basic Router Setting 5

Step 1: Cable the network as shown in the topology. 5

Step 2: Configuring Basic Setting on All Routers. 5

Step 3 Display Router Information 6

1.2 Configuring HSRP 7

Step 1 Configuring First Hop Redundancy Using HSRP on Hamilton Routers 7

Step 2 Verifying HSRP on Master and Backup Router 7

1.3 Configuring IPv4 Default Route 8

Step 1 Configuring a Default Route on All Routers 8

Step 2 Verifying the Routes 8

1.4 Configuring AAA Security 9

Step 1 Setting Up the Local AAA Security on All Routes 9

Step 2 Verifying AAA Security 9

1.5 Configuring Basic DHCP 10

Step 1 Setting Up Basic DHCPv4 on Edge-Hamilton-Router and Branches Routers 10

Step 2 Verifying DHCP Address Pool 10

1.6 Configuring Port Address Translation (PAT) 11

Step 1 Setting Up Access-list / PAT / Inside and Outside interface on Edge Router 11

Step 2 Verifying Access Control Lists and PAT 11

1.7 Configuring Dynamic Multipoint VPN over IPsec on Edge Router and Branches Routers 12

Step 1 Setting Up GRE Tunnel 12

Step 2 Setting Up ISAKMP Policy 13

1.8 Configuring EIGRP Routing Protocol on GRE Tunnel 14

Step 1 Setting Up EIGRP Routing Protocol on All Routers 14

Step 2 Verifying EIGRP Routing Protocol 14

1.9 Configuring Syslog 15

Step 1 Setting Up syslog 15

Step 2 Verifying Default Logging Setting 15

1.10 Configuring an Intrusion Prevention System (IPS) 16

Step 1 Verify or create the IPS directory in router flash on Router 16

Step 2 Configuring the IPS Crypto Key 16

Step 3 Configuring IOS IPS 17

Step 3 Verifying IPS 17

2.0 Configuration on Switches 18
2.1 Configuring Basic Switches Setting 18
Step 1 Configuring Basic Setting on All Switches 18
Step 2 Setting Up Basic Security features, Banner and SSH 18
2.2 Configuring AAA Security feature 19
Step 1 Setting Up the Local AAA Security feature on All Switches 19
Step 2 Verifying AAA Security 19
2.3 Configuring EtherChannel and PVST+ 20
Step 1 Setting Up LACP between Switches and PVST+ 20
Step 2 Verifying LACP Protocol and EtherChannel Connection 20
2.4 Configuring Switch Security Features 21
Step 1 Setting Up Switch Port Security on LAN Switch 21
Step 2 Verifying Port Security on the interface 21
3.0 Configuration on ASA 22
3.1 Configuring Basic ASA Setting 22
Step 1 Configuring Basic Setting on All ASAs 22
Step 2 Verify the Status of Interfaces 22
3.2 Configuring ASA Failover for Active/Standby mode 23
Step 1 Setting Up Failover on Master and Backup ASA 23
Step 2 Verify ASA Failover Status on Both ASA 23
3.3 Configuring Basic ASA Setting with Security Feature 24
Step 1 Setting Up Basic Features on Main ASA 24
Step 2 Verifying Configuration 24
3.4 Configuring EIGRP Routing Protocol 25
Step 1 Setting Up EIGRP Routing Protocol on Main ASA 25
Step 2 Verifying EIGRP Routing Protocol Status 25
3.5 Configuring Access Control List and Policy Map 26
Step 1 Setting Up Policy Map on Main ASA to Permit ICMP Traffic 26
Step 2 Setting Up Access Control List to Permit Essential Services 26
Step 3 Verify Access Control List and interface 27
4.0 Basic Configuration on Windows Server 28
4.1 Installing Windows Server 2019 28
Step 1 Booting Up with the Installation C/D and install the system with guide 28
Step 2 Installing Active Directory Role and ISCSI File Share feature 28
Step 3 Configuring Active Directory Domain Services 30
Step 4 Configuring ISCSI Target Services 31
Step 5 Verify the ISCSI Disk and Target 32

5.0 Basic Configuration on Linux and Active Directory 33
5.1 Installing Linux 33
Step 1 Booting Up the Installation C/D 33
Step 2 installing the system follow with the Graphic Guide 33
Step 3 Updating the system and Adding Extra Add-ons 35
Step 4 Updating the system and Adding Extra Add-ons 35
5.2 Creating High-Availability Cluster with Pacemaker 36
Step 1 Installing essential Software and dependencies 36
Step 2 Disabling the Firewall 36
Step 3 Configure corosync file 36
Step 4 Auth Key Creation and file Synchronize 38
Step 5 Hosts File Configuration 38
Step 6 High-Availability Cluster Creation 38
Step 6 Verifying the Status of Cluster Server 39
Step 7 Adding Virutal-IP and Apache Web Service for Cluster Resources 39
5.3 Creating Split Brain Detection as Quorum 40
Step 1 Connecting Quorum Drive via ISCSI from Admin Server 40
Step 2 Enabling the Software Watchdog Device 40
Step 3 Creating SBD Device 41
Step 4 Testing SBD Device Functionality 42
Step 5 Adding Fencing Agent to Cluster Server 42
5.4 Creating Samba Share with Active Directory Authentication 43
Step 1 Editing the Samba Configuration File for Authentication features on File Share 43
Step 2 Editing the Kerberos File for connecting the Domain 44
Step 3 Joining the Windows Domain on Linux Servers 45
Step 4 Verifying the Domain Computers on the Windows Server 45
5.5 Creating Active Directory Users and OUs (Organization Unite) 46
Step 1 Adding the Organization Unite in Active Directory 46
Step 2 Importing the users by PowerShell Scripting 47
Step 3 Creating CSV file 48
Step 4 Executing the Script in PowerShell 48
Step 5 Verifying the Active Directory Users 49
5.6 Synchronization the folder between Master and Backup Node via Resilio-Sync 50
Step 1 Download and unzip the Resilio-Sync from the official website 50
Step 2 Access the resilio-sync via Browser 51
Step 3 Activating the Licences of Resilio-Sync 52
Step 4 Link two nodes for synchronization 53

Step 5 Configuring frequency of sync time 54
Step 6 Configuring Synchronization folder 54
6.0 Configuration on Samba Share and its permissions 56
6.1 Configuring Active Directory Group for Users 56
Step 1 Grouping the Users to appropriate Group 56
Step 2 Verifying the Groups and Users on Linux Server 57
6.2 Configuring the Permission on Samba Share 58
Step 1 Paste the Setting on Both nodes 58
Step 2 Reboot the SMB Services 60
Step 3 Verifying the Permission 60
7.0 Configuration on Proxy Server 62
7.1 Creating AnyConnect VPN on ASA Device 62
Step 1 Enabling HTTP on ASA 62
Step 2 Installing ASDM and Accessing to the ASA 62
Step 3 Configuring the Basic Setting on ASA 63
Step 4 Configuring AnyConnect VPN 63
Step 5 Configuring Split Tunnel mode 66
Step 6 Connecting the Proxy Server via remote users 68
8.0 Configuration on WDS and DHCP Service 70
8.1 Configuring WDS and DHCP Service 70
Step 1 Install the WDS and DHCP Service 70
Step 2 Configuring DHCP Service 70
Step 3 Configuring WDS Service 74
Step 4 Verifying the WDS Services 77

1.0 Configuration on Routers

1.1 Configuring Basic Router Setting

Step 1: Cable the network as shown in the topology.

i. Attach the devices as shown in the topology diagram, and cable as necessary

ii. Power on all the devices in the topology.

Step 2: Configuring Basic Setting on All Routers.

1. Enable the privileged EXEC Mode.

Router> enable

Router> config terminal

2. Set Up the hostname.

Router> Hostname Hamilton-Edge-Router ***#Depend on the Devices***

3. Disable DNS lookup.

Router> no ip domain-lookup

4. Configure IP Address on interfaces followed by the IP Table.

#Depend on the Devices.

Router>interface g0/0 ***#Depend on the interface***

Router> ip address 202.14.63.131 255.255.255.0 ***#Depend on the interface***

Router>no shutdown

5. Set Up SSH, Banner and Extra Security on All Routers.

Router>enable password cisco12345

Router>username admin privilege 15 algorithm-type sha256 secret cisco12345

Router>ip domain-name optimus.com

Router>crypto key generate rsa general-keys modulus 2048

Router>ip ssh version 2

Router>ip ssh time-out 120

Router>ip ssh authentication-retries 5

Router>line vty 0 4

Router>privilege level 15

Router>exec-timeout 15 0

Router>transport input ssh

Router>service password-encryption

Router>Banner MOTD #UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED!#

Step 3 Display Router Information

1. Verify the status of interfaces.

Router#show ip int bri

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	202.14.63.131	YES	NVRAM	up	up
GigabitEthernet0/1	10.1.1.1	YES	NVRAM	up	up
GigabitEthernet0/2	10.1.2.1	YES	NVRAM	up	up
GigabitEthernet0/3	unassigned	YES	NVRAM	administratively down	down
NVI0	202.14.63.131	YES	unset	up	up

1.2 Configuring HSRP

Step 1 Configuring First Hop Redundancy Using HSRP on Hamilton Routers

1. **Configure HSRP on Router-Hamilton-Master.**

Router>int g0/1

Router>standby version 2

Router>standby 1 ip 172.16.0.19

Router>standby 1 priority 150

Router>standby 1 preempt

2. **Configure HSRP on Router-Hamilton-Backup.**

Router>int g0/1

Router>standby version 2

Router>standby 1 ip 172.16.0.19

Step 2 Verifying HSRP on Master and Backup Router

1. **Verify the HSRP Status.**

Router#show standby

GigabitEthernet0/1 - Group 1 (version 2)
  State is Active
    2 state changes, last state change 02:17:44
  Virtual IP address is 172.16.0.19
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.160 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)

1.3 Configuring IPv4 Default Route

Step 1 Configuring a Default Route on All Routers

#Outside Address based on the G0/0 interface.

Router> ip route 0.0.0.0 0.0.0.0 g0/0 202.14.63.3

Step 2 Verifying the Routes

1. Display the route.

Router#show 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 202.14.63.3 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 202.14.63.3, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/24 is directly connected, GigabitEthernet0/1
L        10.1.1.1/32 is directly connected, GigabitEthernet0/1
C        10.1.2.0/24 is directly connected, GigabitEthernet0/2
L        10.1.2.1/32 is directly connected, GigabitEthernet0/2
C        202.14.63.0/24 is directly connected, GigabitEthernet0/0
L        202.14.63.131/32 is directly connected, GigabitEthernet0/0
```

1.4 Configuring AAA Security

Step 1 Setting Up the Local AAA Security on All Routes

1. Create local Users for AAA Authentication.

Router> username admin privilege 15 algorithm-type sha256 secret cisco12345

2. Configure AAA features.

Router>aaa new-model

Router>aaa authentication login default local-case enable

Router>aaa authorization exec default local

Step 2 Verifying AAA Security

1. Display the AAA Users.

Router #show aaa sessions

Total sessions since last reload: 2

Session Id: 1

Unique Id: 11

User Name: *not available*

IP Address: 0.0.0.0

Idle Time: 0

CT Call Handle: 0

Session Id: 2

Unique Id: 12

User Name: admin

IP Address: 0.0.0.0

Idle Time: 0

CT Call Handle: 0

#Re-login the Device, the authentication is required.

User Access Verification

Username: admin

Password:

1.5 Configuring Basic DHCP

Step 1 Setting Up Basic DHCPv4 on Edge-Hamilton-Router and Branches Routers

1. Configure DHCP Pool on Master and Backup Router.

Router>ip dhcp excluded-address 172.16.0.1 172.16.0.19

Router>ip dhcp pool Hamilton-DHCP-1

Router>network 172.16.0.0 255.255.255.0

Router>default-router 172.16.0.19

Router>dns-server 1.1.1.1

2. Configure ip-helper on Master and Backup Router.

Router>int g0/1

Router>ip helper-address 10.1.1.1

Step 2 Verifying DHCP Address Pool

1. Verify DHCP Pool on all Routers.

Router#show ip dhcp pool Hamilton-DHCP-1

Pool Hamilton-DHCP-1 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 0

Pending event : none

1 subnet is currently in the pool :

Current index	IP address range	Leased addresses
172.16.0.1	172.16.0.1 - 172.16.0.254	0

1.6 Configuring Port Address Translation (PAT)

Step 1 Setting Up Access-list / PAT / Inside and Outside interface on Edge Router

1. Configure Port Address Translation.

Router>access-list 10 permit 172.16.0.0 0.0.255.255

Router>access-list 10 permit 10.10.0.0 0.0.255.255

Router>ip nat inside source list 1 interface g0/0 overload

Router>interface g0/0

Router>ip nat outside

Router>interface g0/1

Step 2 Verifying Access Control Lists and PAT

1. Verify the Access Control Lists.

Router#show access-lists 10

Standard IP access list 10

10 permit 172.16.0.0, wildcard bits 0.0.255.255

20 permit 10.10.0.0, wildcard bits 0.0.255.255

2. Verify NAT Statistics.

Router#show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)

Peak translations: 0

Outside interfaces:

GigabitEthernet0/0

Inside interfaces:

GigabitEthernet0/1, GigabitEthernet0/2

Hits: 0 Misses: 0

CEF Translated packets: 0, CEF Punted packets: 0

Expired translations: 0

1.7 Configuring Dynamic Multipoint VPN over IPsec on Edge Router and Branches Routers

Step 1 Setting Up GRE Tunnel

1. Set Up on Edge-Hamilton-Router.

Router>interface Tunnel 10

Router>bandwidth 100000

Router>no ip split-horizon eigrp 10

Router>no ip next-hop-self eigrp 10

Router>ip address 10.100.1.1 255.255.255.0

Router>ip nhrp authentication DMVPN

Router>ip nhrp map multicast dynamic

Router>ip nhrp network-id 10

Router>tunnel source g0/0

Router>tunnel mode gre multipoint

2. Set Up on Branches Routers.

Router>interface Tunnel 10

Router>ip address 10.100.1.2 255.255.255.0

Router>ip nhrp authentication DMVPN

Router>ip nhrp map 10.100.1.1 202.14.63.131

Router>ip nhrp map multicast 202.14.63.131

Router>ip nhrp network-id 10

Router>ip nhrp nhs 10.100.1.1

Router>tunnel source g0/0

Router>tunnel mode gre multipoint

Step 2 Setting Up ISAKMP Policy

1. Configure IPsec Policies for Security.

Router>crypto isakmp policy 10

Router>authentication pre-share

Router>encryption aes 256

Router>group 24

Router>hash sha512

Router>crypto isakmp key cisco address 0.0.0.0

Router>crypto ipsec transform-set DMVPN esp-aes 256 esp-sha512-hmac

Router>crypto ipsec profile DMVPN

Router>set transform-set DMVPN

Router>int tunnel 10

1.8 Configuring EIGRP Routing Protocol on GRE Tunnel

Step 1 Setting Up EIGRP Routing Protocol on All Routers

1. Enable EIGRP Routing Protocol.

Router>router eigrp 10

Router>network 10.0.0.0

Router>network 172.16.0.0

Router>redistribute static

Router>no auto-summary

Step 2 Verifying EIGRP Routing Protocol

1. Verify EIGRP Protocol at the end of the Router configuration.

Router#show ip eigrp neighbors

Router#show ip route eigrp

Router#show ip eigrp topology

Router#show ip protocols

1.9 Configuring Syslog

Step 1 Setting Up syslog

1. Install tftpd64 Software on the syslog Server and Strat the Program.

Router>logging host 10.11.2.2

Step 2 Verifying Default Logging Setting

1. Veirfy the System Logging Setting

Router#show logging

```
Trap logging: level informational, 37 message lines logged
    Logging to 10.10.0.110  (udp port 514, audit disabled,
          link up),
          2 message lines logged,
          0 message lines rate-limited,
          0 message lines dropped-by-MD,
          xml disabled, sequence number disabled
          filtering disabled
    Logging Source-Interface:       VRF Name:
```

1.10 Configuring an Intrusion Prevention System (IPS)

Step 1 Verify or create the IPS directory in router flash on Router

1. Display the contents of flash memory.

Router#show flash

2. If the ipsdir directory is not listed, create it in privilege mode.

Router >mkdir ipsdir

Create directory filename [ipsdir]?

Created dir disk0:/ipsdir

Step 2 Configuring the IPS Crypto Key

1. Copy and paste the crypto key file into edge router.

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
  exit
  exit
```

2. Create an IPS Rule.

Router>ip ips name IPS

3. Configure the IPS Signature storage location in router flash memory.

Router> ip ips config location flash:ipsdir

4. Enable IPS SDEE event notification and syslog support.

Router>ip http server

Router>ip ips notify sdee

Router> ip ips notify log

Router> service timestamps log datetime msec

Step 3 Configuring IOS IPS

1. Set up the pre-defined signature categories.

Router> ip ips signature-category

Router> category all

Router> retired true

Router> category ios_ips basic

Router> retired false

2. Apply on the interface.

Router> interface g0/0

Router> ip ips IPS in

3. Copy the Signature package into the router and compile.

Router> copy scp://admin@202.14.63.3/IOS-S983-CLI.pkg flash:

Router>copy flash:IOS-S983-CLI.pkg idconf

Step 3 Verifying IPS

Router# show ip ips signature count

Router# show ip ips all

2.0 Configuration on Switches

2.1 Configuring Basic Switches Setting

Step 1 Configuring Basic Setting on All Switches

1. Set Up the Hostname.

Switch>hostname Switch-Hamilton-Master

Step 2 Setting Up Basic Security features, Banner and SSH

1. Configure Basic Features and Securities.

Switch>enable password cisco12345

Switch>username admin privilege 15 algorithm-type sha256 secret cisco12345

Switch>ip domain-name optimus.com

Switch>crypto key generate rsa general-keys modulus 2048

Switch>ip ssh version 2

Switch>ip ssh time-out 120

Switch>ip ssh authentication-retries 5

Switch>line vty 0 4

Switch>privilege level 15

Switch>exec-timeout 15 0

Switch>transport input ssh

Switch>service password-encryption

2.2 Configuring AAA Security feature

Step 1 Setting Up the Local AAA Security feature on All Switches

1. **Create local Users for AAA Authentication. (user is created on 2.1.2)**

Switch>username admin privilege 15 algorithm-type sha256 secret cisco12345

2. **Configure AAA features.**

Switch>aaa new-model

Switch>aaa authentication login default local-case enable

Switch>aaa authorization exec default local

Step 2 Verifying AAA Security

#The Step is the same as the Router Section under 1.4.2.

2.3 Configuring EtherChannel and PVST+

Step 1 Setting Up LACP between Switches and PVST+

1. Enable LACP on all Interfaces that connected with Switches.

Switch>int range g0/1 - 2

Switch>channel-group 10 mode active

Switch>int range g1/0 - 1

Switch>channel-group 20 mode active

#Enable the PVST+ Spanning Tree Protocol.

Switch>spanning-tree mode rapid-pvst

Step 2 Verifying LACP Protocol and EtherChannel Connection

1. Veirfy the etherchnnel connection.

Switchr#show etherchannel summary

Number of channel-groups in use: 2

Number of aggregators: 2

Group Port-channel Protocol Ports

------+-------------+-----------+---

10 Po10(SU) LACP Gi0/1(P) Gi0/2(P)

20 Po20(SU) LACP Gi1/0(P) Gi1/1(P)

2.4 Configuring Switch Security Features

Step 1 Setting Up Switch Port Security on LAN Switch

1. Set Up Port Security on the port that connected to the PCs

Switch>int range g3/2-3

Switch>switchport port-security mac-address sticky

Switch>switchport port-security aging type inactivity

Step 2 Verifying Port Security on the interface

1. Verify the port security of a specific interface.

Switch#show port-security interface g3/2

Port Security : Disabled

Port Status : Secure-down

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

3.0 Configuration on ASA

3.1 Configuring Basic ASA Setting

Step 1 Configuring Basic Setting on All ASAs

1. Set Up the IP Address on Interfaces with Name

ASA>int g0/0

ASA>nameif OUTSIDE

ASA>ip addr 172.16.0.3 255.255.255.0

ASA>no shut

ASA>int g0/3

ASA>nameif INSIDE

ASA>ip addr 10.10.0.1 255.255.255.0

ASA>no shut

ASA>int g0/1

ASA>no shut

ASA>int g0/2

Step 2 Verify the Status of Interfaces

1. Display the Status of Interfaces.

ASA# show int ip bri

Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0/0	172.16.0.3	YES CONFIG up	up
GigabitEthernet0/1	192.168.1.1	YES unset up	up
GigabitEthernet0/2	192.168.2.1	YES unset up	up
GigabitEthernet0/3	10.10.0.1	YES CONFIG up	up
GigabitEthernet0/4	unassigned	YES unset administratively down	down
GigabitEthernet0/5	unassigned	YES unset administratively down	down
GigabitEthernet0/6	unassigned	YES unset administratively down	down
Management0/0	unassigned	YES unset administratively down	down

3.2 Configuring ASA Failover for Active/Standby mode

Step 1 Setting Up Failover on Master and Backup ASA

1. Configure Failover features

ASA>failover

ASA>failover lan unit primary

ASA>failover lan interface FAILOVER g0/1

ASA>failover link STATEFULL g0/2

ASA>failover interface ip FAILOVER 192.168.1.1 255.255.255.252 standby 192.168.1.2

ASA>failover interface ip STATEFULL 192.168.2.1 255.255.255.252 standby 192.168.2.2

Step 2 Verify ASA Failover Status on Both ASA

1. Verify Failover Status.

ASA # show failover

Failover On

Failover unit Primary

Failover LAN Interface: FAILOVER GigabitEthernet0/1 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 2 of 61 maximum

MAC Address Move Notification Interval not set

Version: Ours 9.12(2)4, Mate 9.12(2)4

Serial Number: Ours 9ANC38WGJVH, Mate 9ASXMKX3DS2

Last Failover at: 11:56:57 UTC Apr 17 2020

```
This host: Primary - Active
 Active time: 3178 (sec)
 slot 0: ASAv hw/sw rev (/9.12(2)4) status (Up Sys)
   Interface OUTSIDE (172.16.0.3): Normal (Waiting)
   Interface INSIDE (10.10.0.1): Normal (Waiting)
Other host: Secondary - Standby Ready
 Active time: 0 (sec)
   Interface OUTSIDE (0.0.0.0): Normal (Waiting)
   Interface INSIDE (0.0.0.0): Normal (Waiting)
```

3.3 Configuring Basic ASA Setting with Security Feature

Step 1 Setting Up Basic Features on Main ASA

1. Configure Basic features and Securities

ASA>hostname ASA-Hamilton-Master

ASA>enable password cisco12345

ASA>username admin password cisco12345 privilege 15

ASA>aaa authentication enable console LOCAL

ASA>password encryption aes

ASA>aaa authentication ssh console LOCAL

ASA>crypto key generate rsa general-keys modulus 2048

ASA>ssh 10.10.0.0 255.255.0.0 INSIDE

ASA>ssh version 2

ASA>route OUTSIDE 0.0.0.0 0.0.0.0 172.16.0.19

Step 2 Verifying Configuration

ASA#show aaa local user

ASA#show ssh sessions detail

ASA#show route

3.4 Configuring EIGRP Routing Protocol

Step 1 Setting Up EIGRP Routing Protocol on Main ASA

1. Configure *EIGRP Routing Protocol*

ASA>router eigrp 10

ASA>network 172.16.0.0

ASA>network 10.10.0.0

ASA>no auto-summary

Step 2 Verifying EIGRP Routing Protocol Status

1. Verify EIGRP Status.

ASA # show eigrp topology

EIGRP-IPv4 Topology Table for AS(10)/ID(172.16.0.3)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - reply Status, s - sia Status

P 10.10.0.0 255.255.255.0, 1 successors, FD is 2816

via Connected, INSIDE

P 172.16.0.0 255.255.255.0, 1 successors, FD is 2816

via Connected, OUTSIDEno auto-summary

ASA # show eigrp neighbors

EIGRP-IPv4 Neighbors for AS(10)

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	172.16.0.2	OUTSIDE	10	00:00:45	174	1044	0	8
0	172.16.0.1	OUTSIDE	11	00:00:48	236	4779	0	8

3.5 Configuring Access Control List and Policy Map

Step 1 Setting Up Policy Map on Main ASA to Permit ICMP Traffic

1. Configure Policy Map to Permit ICMP Traffic

ASA>policy-map global_policy

ASA>class inspection_default

ASA>inspect icmp

Step 2 Setting Up Access Control List to Permit Essential Services

1. Import the Access Control Lists to Master ASA

ASA>policy access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq http

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq https

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 445

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 88

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 53

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 135

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 123

ASA>access-list GENERAL extended permit tcp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 139

ASA>access-list GENERAL extended permit udp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 137

ASA>access-list GENERAL extended permit udp 172.16.0.0 255.252.0.0 host 10.10.0.0 eq 138

ASA>access-list GENERAL extended permit tcp any host 10.10.0.110 eq 514

ASA>access-list GENERAL extended permit tcp any any eq 63430

ASA>access-list GENERAL extended permit tcp any any eq 5000

ASA>access-list GENERAL extended permit udp any any eq 63430

ASA>access-list GENERAL extended permit udp any any eq 1900

ASA>access-group GENERAL in interface outside

Step 3 Verify Access Control List and interface

1. **Display the Access Control Lists.**

ASA>show access-list GENERAL

4.0 Basic Configuration on Windows Server

4.1 Installing Windows Server 2019

Step 1 Booting Up with the Installation C/D and install the system with guide

1. **Insert the Installation C/D into PC or Load it on VMware**
2. **Install the Windows Server 2019 followed by the guide**
3. **Set the Computer Name to SERVER-AD**

Step 2 Installing Active Directory Role and ISCSI File Share feature

1. Navigate to the Server Manager and Open the Add roles and features:

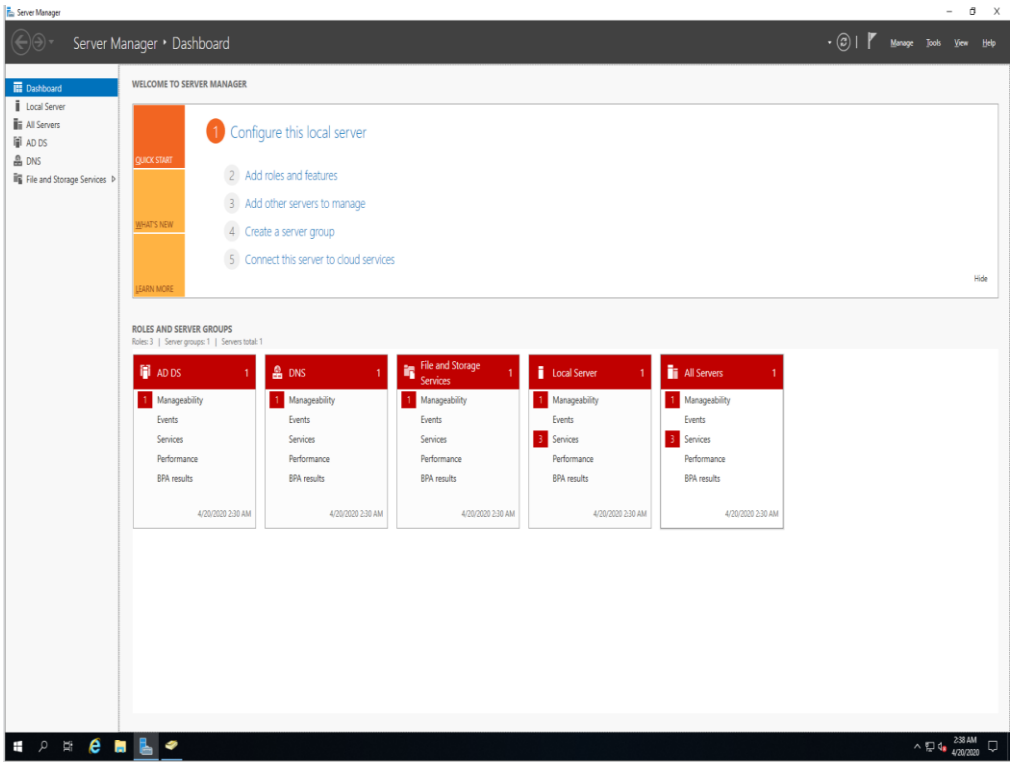


Figure 1 Server Manager

2. Select the Active Directory Domain Services and ISCSI Target Server under the Fire and Storage Services:

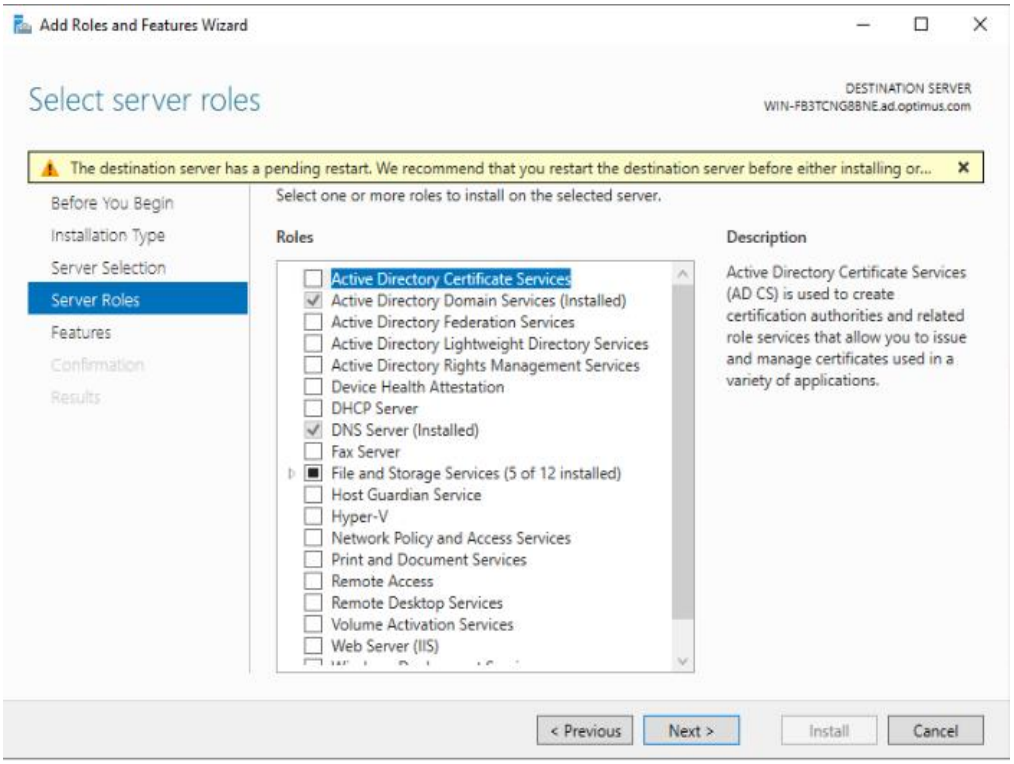


Figure 2 Add roles and features

3. Click Next to finish the installation.

Step 3 Configuring Active Directory Domain Services

1. The Notifications Pane opens and displays a Post-deployment Configuration notification:

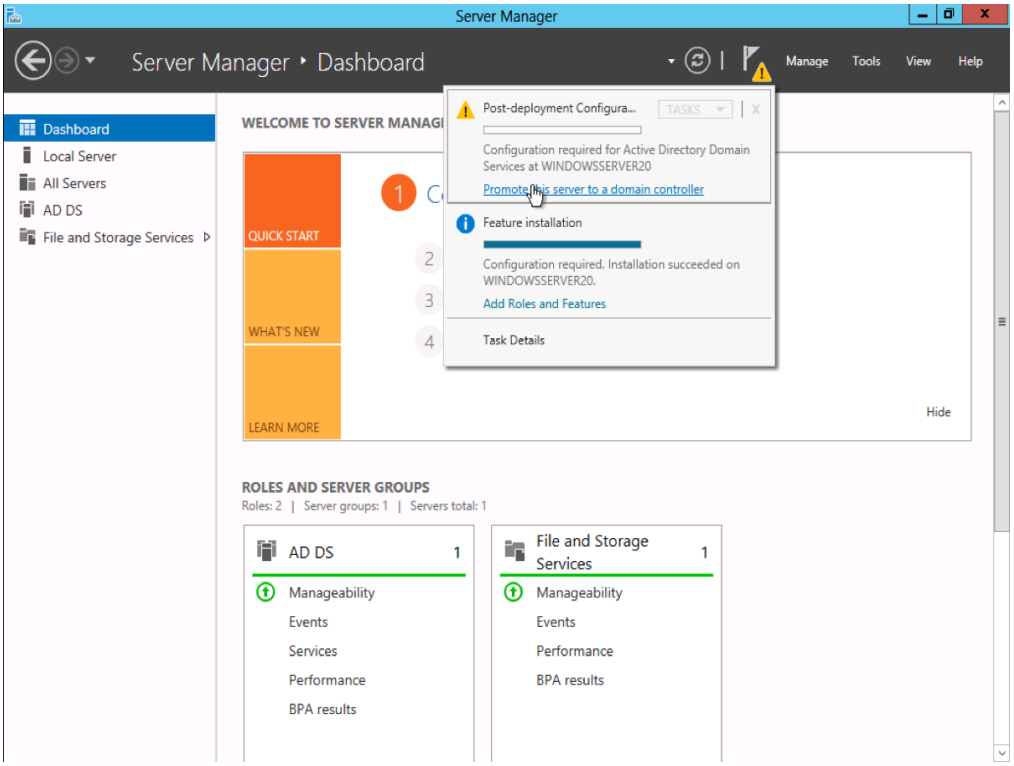


Figure 3 Configuring Active Directory

2. Follow the wizard to complete the Active Directory Setting:

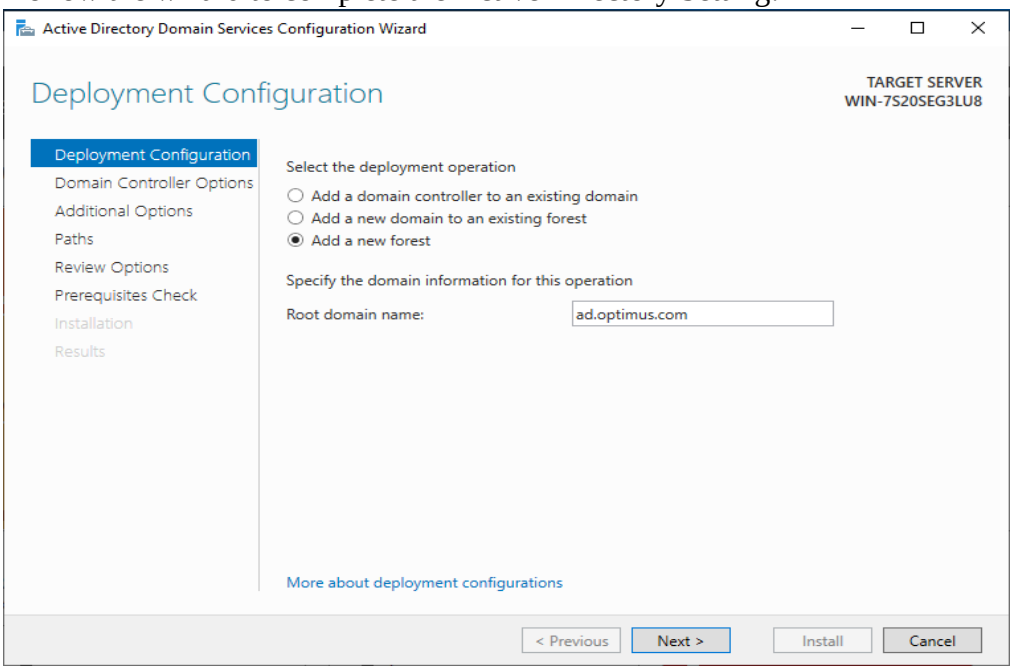


Figure 4 Active Directory Configuration

3. The Active Directory Service is ready after the system reboot when complete the configuration:

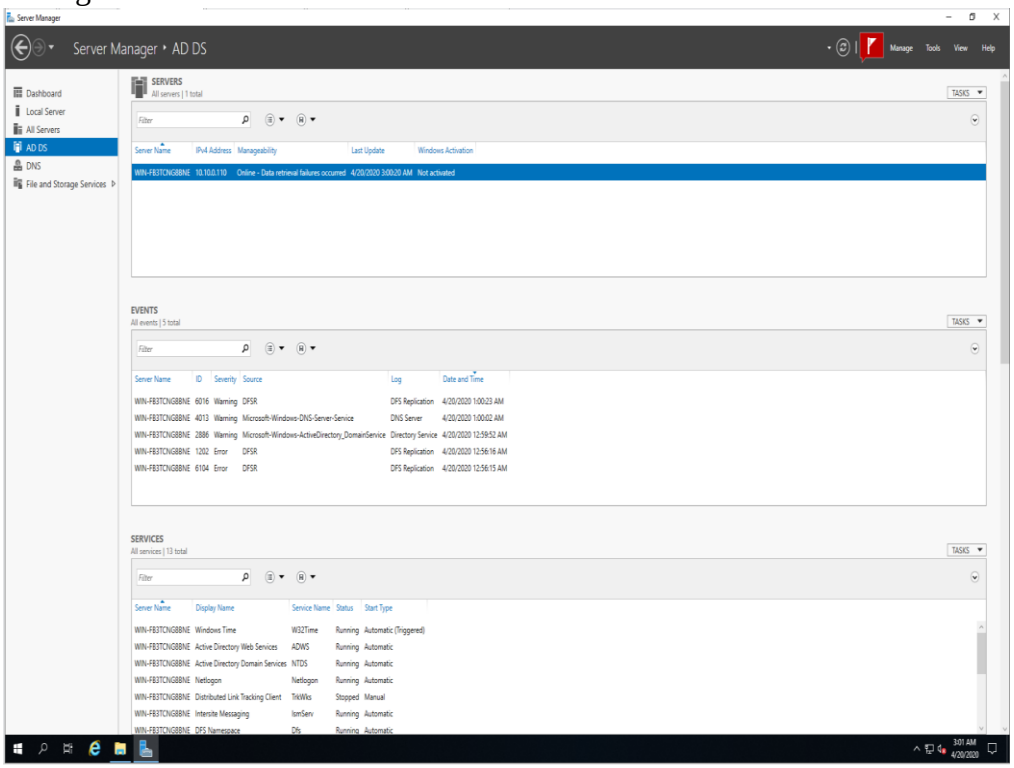


Figure 5 Active Directory Domain Controller

Step 4 Configuring ISCSI Target Services

1. Go to the ISCSI Section under the File and Storage Service Tab.
2. Create the ISCSI Disk Drive and ISCSI Target:

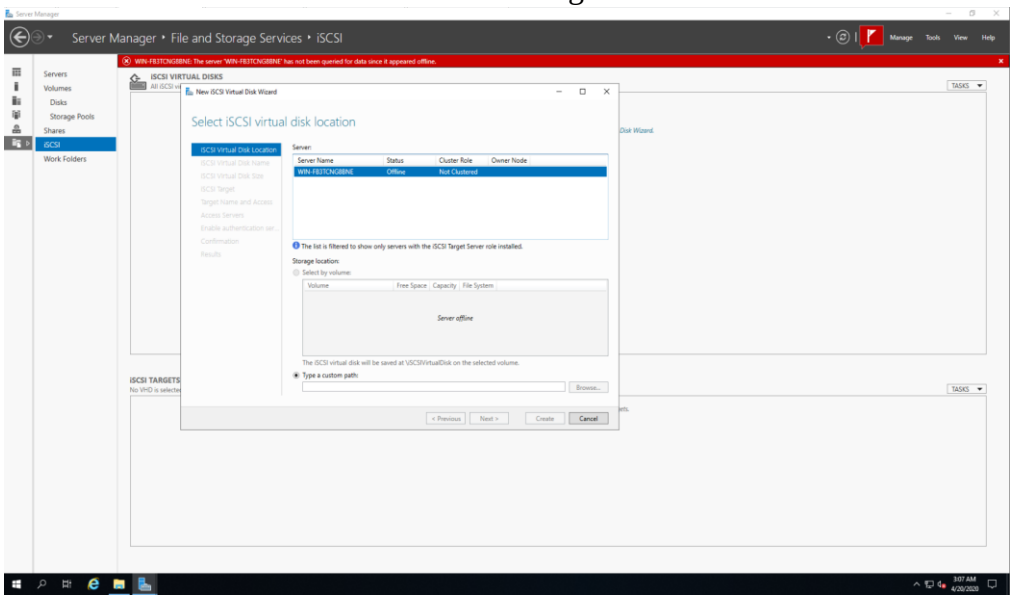


Figure 6 ISCSI Target Server

Step 5 Verify the ISCSI Disk and Target

1. All the ISCSI Configuration display under the File and Storage Services, ISCSI Tab:

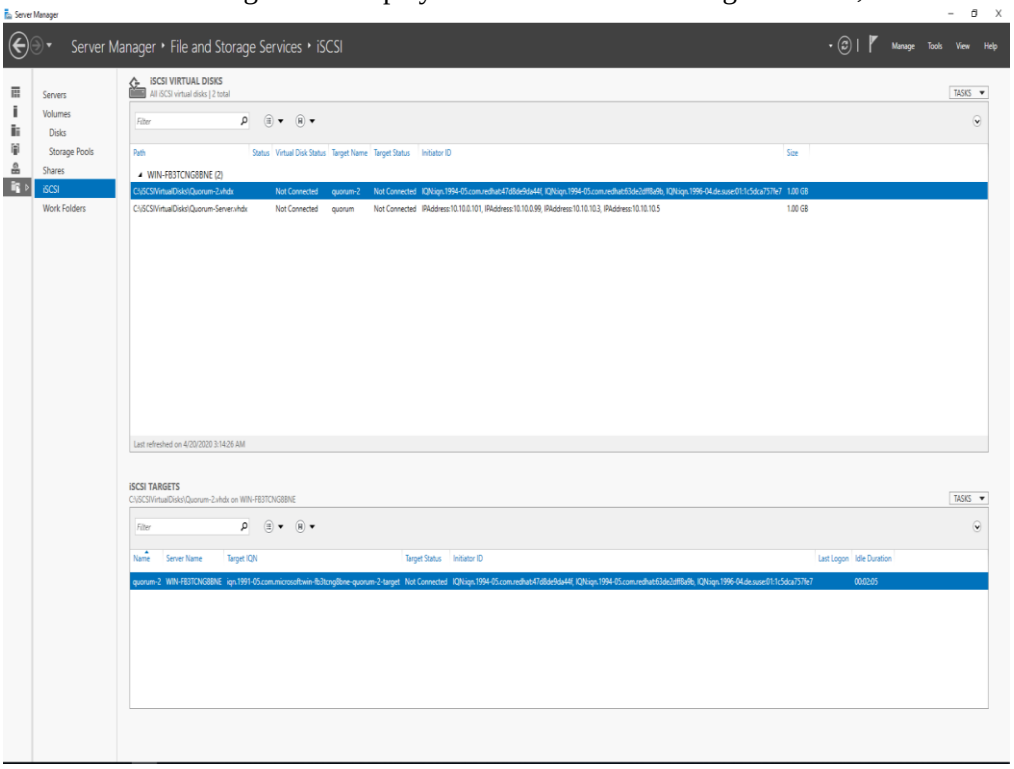


Figure 7 Verify ISCSI Disk and Target

5.0 Basic Configuration on Linux and Active Directory

5.1 Installing Linux

Step 1 Booting Up the Installation C/D

#Insert the Installation C/D into PC or Load it on VMware

Step 2 installing the system follow with the Graphic Guide

1. Follow the installation guide, complete the system installation on Master and Backup nodes:

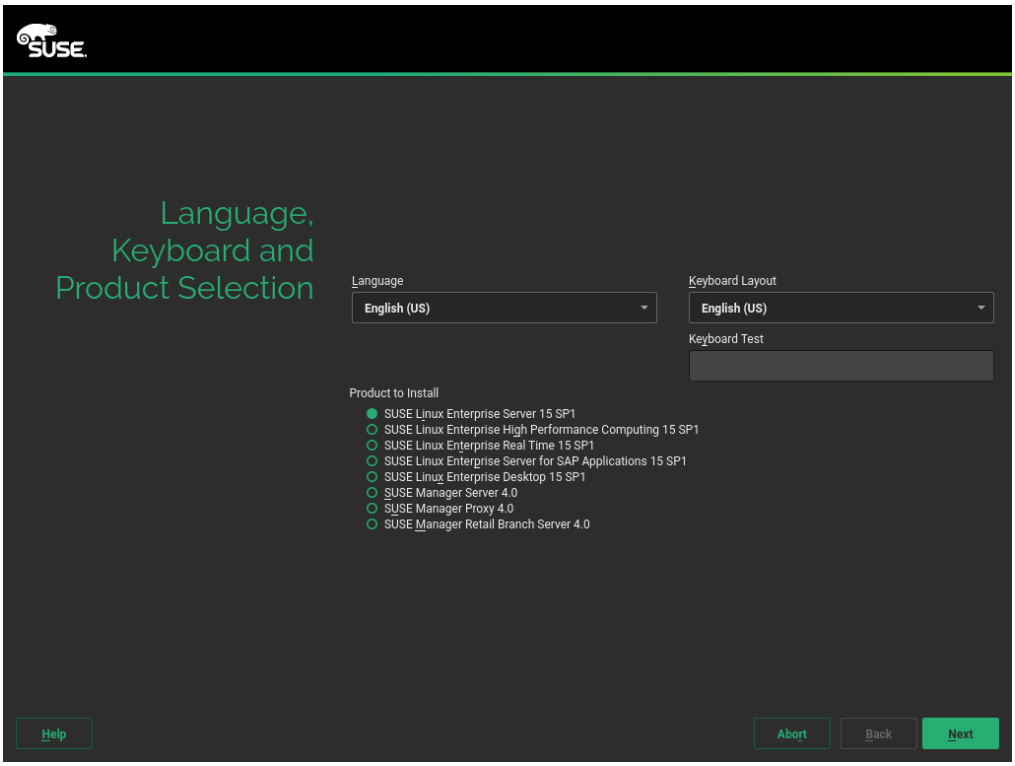


Figure 8 Figure 1 Language, Keyboard, and Product Selection

Figure 9 License Agreement

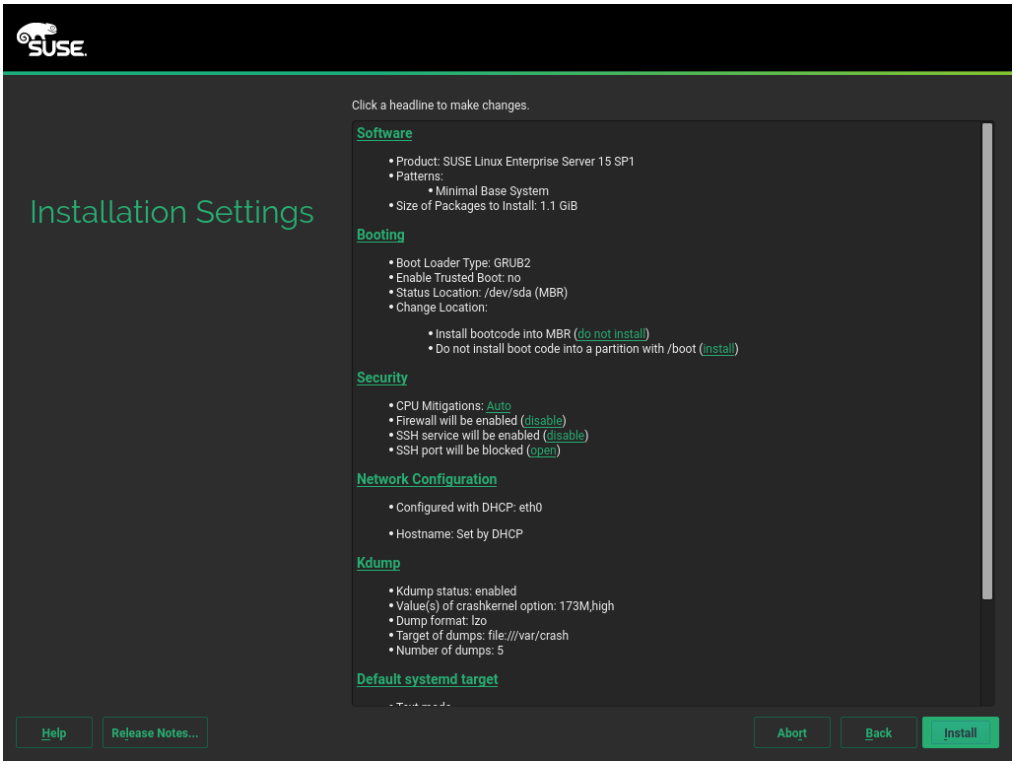


Figure 10 Installation

Step 3 Updating the system and Adding Extra Add-ons

1. Activate/Register the system by entering the license key in the Product Registration Software:

Figure 11 system registration

Step 4 Updating the system and Adding Extra Add-ons

1. **Add the extra extension package to SUSE Linux**

Navigate to the Software Yast and Select the High-Availability and Package Hub Extension

2. **Update the system via CLI Terminal**

#zypper update

5.2 Creating High-Availability Cluster with Pacemaker

Step 1 Installing essential Software and dependencies

1. **Install the High-Availability Software Package.**

#zypper install -t pattern ha_sles

Step 2 Disabling the Firewall

1. **Firewall feature will be overleaped, if it is running on the Linux System.**

#systemctl disable firewalld.service

#systemctl stop firewalld.service

Step 3 Configure corosync file

Edit the file /etc/corosync/corosync.conf with following setting.

```
totem {
        version: 2
        cluster_name: Optimus-Server
        transport: udpu
        crypto_cipher: aes256
        crypto_hash: sha1
        interface {
                ringnumber: 0
                bindnetaddr: 10.10.0.0
                ttl: 1
        }
}
```

```
logging {
        fileline: off
        to_stderr: yes
        to_logfile: yes
        logfile: /var/log/cluster/corosync.log
        to_syslog: yes
        debug: off
        logger_subsys {
                subsys: QUORUM
                debug: off
        }
}
quorum {
        provider: corosync_votequorum
        two_node: 1
}

nodelist {

                        node {
                                        name: HA-HAMILTON-MASTER
                                        nodeid: 1
                                        ring0_addr: 10.10.0.99
        }
                        node {
                                        name: HA-HAMILTON-BACKUP
                                        nodeid: 2
                                        ring0_addr: 10.10.0.101
        }
}
```

Step 4 Auth Key Creation and file Synchronize

1. **Generate an Auth Key from the Master node.**

#corosync-keygen

2. **Copy the file to the second node.**

 # scp /etc/corosync/corosync.conf root@ha-backup:/etc/corosync/corosync.conf

 # scp /etc/corosync/authkey root@ha-backup:/etc/corosync/authkey

Step 5 Hosts File Configuration

1. Configure the Hosts file [/etc/hosts], which identify the a Static IP for a Specific hostname.

10.10.0.99 HA-Master.ad.optimus.com Master HA-Master

10.10.0.101 HA-Backup.ad.optimus.com Backup HA-Backup

Step 6 High-Availability Cluster Creation

1. **Start the Server Cluster Service.**

 # systemctl start pacemaker

 # systemctl enable pacemaker

Step 6 Verifying the Status of Cluster Server

1. Display the Cluster Status.

 # crm status

Stack: corosync

Current DC: HA-HAMILTON-MASTER (version 2.0.1+20190417.13d370ca9-3.9.1-2.0.1+20190417.13d370ca9) - partition with quorum

Last updated: Sun Apr 19 20:39:46 2020

Last change: Sun Apr 19 20:39:35 2020 by hacluster via crmd on HA-HAMILTON-MASTER

2 nodes configured

0 resources configured

Online: [HA-HAMILTON-BACKUP HA-HAMILTON-MASTER]

No resources

Step 7 Adding Virutal-IP and Apache Web Service for Cluster Resources

1. Import the following Setting in crm configure mode.

```
#crm configure
    primitive Virtual-IP ocf:heartbeat:IPaddr2  \
        params ip="10.10.0.100" nic="eth0" cidr_netmask="24"  \
        meta migration-threshold=2 \
        op monitor interval=20 timeout=60 on-fail=restart
    primitive Apache ocf:heartbeat:apache  \
        meta migration-threshold=2  \
        op monitor interval=20 timeout=60 on-fail=restart
    colocation lb-loc inf: Virtual-IP Apache
    order lb-ord inf: Virtual-IP Apache
    commit
```

5.3 Creating Split Brain Detection as Quorum

Step 1 Connecting Quorum Drive via ISCSI from Admin Server

1. Connect the ISCSI Drive from both nodes.

 # iscsiadm --mode discovery --type st --portal 10.10.0.110

10.10.0.110:3260,1 iqn.1991-05.com.microsoft:win-fb3tcng8bne-quorum-target

 # iscsiadm --mode node --login

Logging in to [iface: default, target: iqn.1991-05.com.microsoft:win-fb3tcng8bne-quorum-target, portal: 10.10.0.110,3260] (multiple)

Login to [iface: default, target: iqn.1991-05.com.microsoft:win-fb3tcng8bne-quorum-target, portal: 10.10.0.110,3260] successful.

2. Verify the Disk.

 # fdisk -l

Disk /dev/sdb: 1 GiB, 1073741824 bytes, 2097152 sectors

Units: sectors of 1 * 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 4096 bytes

I/O size (minimum/optimal): 4096 bytes / 4096 bytes

Step 2 Enabling the Software Watchdog Device

1. Set Up the Software Watchdog.

#echo softdog > /etc/modules-load.d/watchdog.conf

2. Enable the Watchdog by restart the module.

#systemctl restart systemd-modules-load

3. Verify the Watchdog.

 # lsmod | grep softdog

softdog 16384 0

Step 3 Creating SBD Device

1. Install SBD Software.

#zypper in sbd

2. Initialize the SBD device with the following command.

#sbd -d /dev/sdb create -4 80 -1 60

Initializing device /dev/sdb

Creating version 2.1 header on device 4 (uuid: 430911db-6d3c-4748-b580-1a4382a05e3a)

Initializing 255 slots on device 4

Device /dev/sdb is initialized.

3. Check what has been written to the device:

 # sbd -d /dev/sdb dump

==Dumping header on disk /dev/sdb

Header version : 2.1

UUID : 430911db-6d3c-4748-b580-1a4382a05e3a

Number of slots : 255

Sector size : 512

Timeout (watchdog) : 60

Timeout (allocate) : 2

Timeout (loop) : 1

Timeout (msgwait) : 80

==Header on disk /dev/sdb is dumped

3. Configuring SBD file /etc/sysconfig/sbd on both nodes

SBD_DEVICE="/etc/sdb"

SBD_PACEMAKER=yes

SBD_DELAY_START=yes

SBD_WATCHDOG_DEV=/dev/watchdog

Mask the other setting option by #

4. Verifying SBD Status

#systemctl status sbd

Loaded: loaded (/usr/lib/systemd/system/sbd.service; enabled; vendor preset:>

Active: active (running) since Sun 2020-04-19 20:58:55 NZST; 5s ago

Docs: man:sbd(8)

Process: 20544 ExecStart=/usr/sbin/sbd $SBD_OPTS -p /var/run/sbd.pid watch (c>

Main PID: 20574 (sbd)

Step 4 Testing SBD Device Functionality

1. Display the SBD Device connected nodes.

#sbd -d /dev/sdb list

0 ha-backup clear

1 ha-master clear

2. Send the test message to Backup node from Master.

#sbd -d /dev/sdb message ha-backup test

May 03 16:08:31 ha-mster sbd[66139]: /dev/SBD: notice: servant: Received command test from bob on disk /dev/SBD

Step 5 Adding Fencing Agent to Cluster Server

1. Import the following Setting in crm configure mode.

property no-quorum-policy=ignore

property stonith-enabled=yes

property stonith-watchdog-timeout=0

property stonith-timeout="120s"

*primitive fence_SBD stonith:external/sbd *

params pcmk_delay_max=30

commit

2. Verify the Running Resources.

#crm status

Full list of resources:

Virtual-IP (ocf::heartbeat:IPaddr2): Started HA-HAMILTON-BACKUP

Apache (ocf::heartbeat:apache): Stopping HA-HAMILTON-BACKUP

fence_SBD (stonith:external/sbd): Starting HA-HAMILTON-BACKUP

5.4 Creating Samba Share with Active Directory Authentication

Step 1 Editing the Samba Configuration File for Authentication features on File Share

1. Copy the following Settings into /etc/samba/smb.conf file on Master and Backup node.

```
[global]
                netbios name = HA-MASTER      #Depends on Node
                socket options = TCP_NODELAY SO_RCVBUF=16384
SO_SNDBUF=16384
                idmap uid = 10000-20000
                winbind enum users = yes
                winbind gid = 10000-20000
                workgroup = AD
                os level = 20
                winbind enum groups = yes
                socket address = 10.10.0.110
                password server = *
                preferred master = no
                winbind separator = +
                max log size = 50
                log file = /var/log/samba/log.%m
                encrypt passwords = yes
                dns proxy = no
                realm = AD.OPTIMUS.COM
                security = ADS
                wins server = 10.10.0.110
                wins proxy = no
[WorkShare]
                comment = WorkShare
                path = /mnt/WorkShare
                read only = No
                browseable = Yes
                inherit acls = yes
                inherit permissions = yes
```

Step 2 Editing the Kerberos File for connecting the Domain

1. **Editing the /etc/krb5.conf file with the following Settings on both nodes with a few changes**

```
[libdefaults]
                        dns_canonicalize_hostname = false
                        rdns = false
                        default_realm = AD.OPTIMUS.COM
                        default_ccache_name = FILE:/tmp/krb5cc_%{uid}
                        clockskew = 300

[realms]
                        AD.OPTIMUS.COM = {
                         kdc = SERVER-AD.ad.optimus.com
                         default_domain = ad.optimus.com
                         admin_server = SERVER-AD.ad.optimus.com
                        }

[logging]
                        kdc = FILE:/var/log/krb5/krb5kdc.log
                        admin_server = FILE:/var/log/krb5/kadmind.log
                        default = SYSLOG:NOTICE:DAEMON

[domain_realm]
                        .ad.optimus.com = AD.OPTIMUS.COM

[appdefaults]
                        pam = {
                         ticket_lifetime = 1d
                         renew_lifetime = 1d
                         forwardable = true
                         proxiable = false
                         minimum_uid = 1
                        }
```

Step 3 Joining the Windows Domain on Linux Servers

1. Join the Windows Domain

 # net ads join -U admin

Enter admin's password:

Using short domain name -- AD

Joined 'HA-BACKUP' to dns domain 'ad.optimus.com'

DNS update failed: NT_STATUS_UNSUCCESSFUL

Step 4 Verifying the Domain Computers on the Windows Server

1. Navigate to the Server Manager and Open Active Directory Users and Computers under tools:

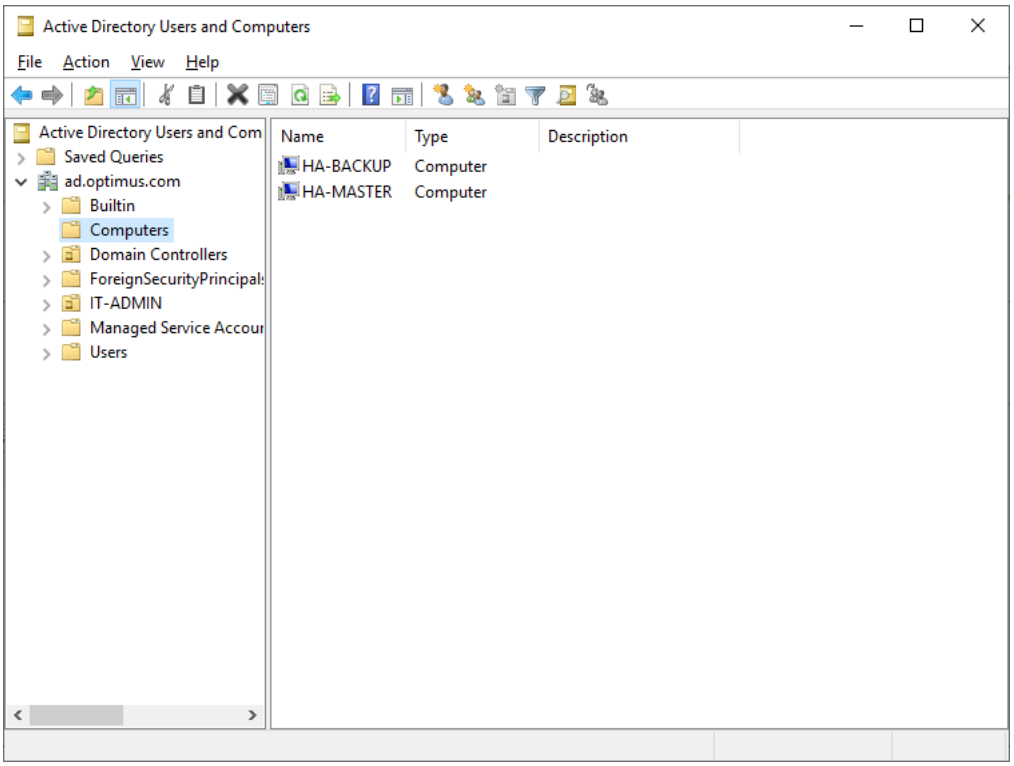


Figure 12 Active Directory Users and Computers

5.5 Creating Active Directory Users and OUs (Organization Unite)

Step 1 Adding the Organization Unite in Active Directory

1. Return to the Active Directory Users and Computers under the tools in Server Manager.
2. Right Click the Active Directory Domain Name and Create OUs followed by the Active Directory Diagram or Figure 14.

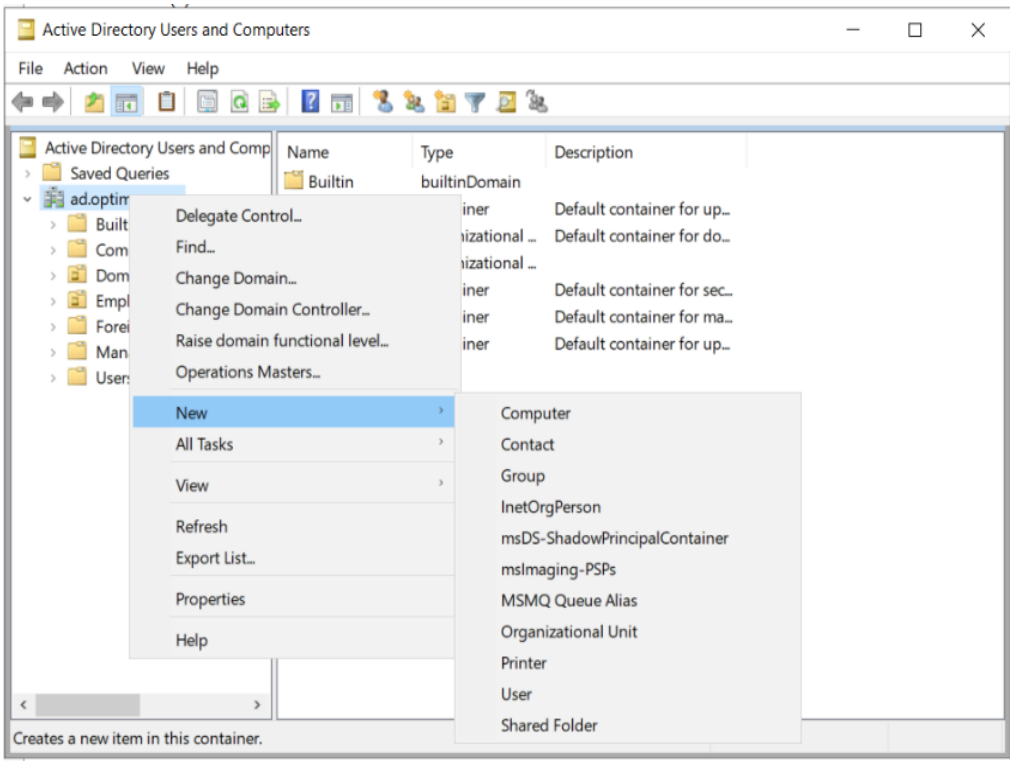


Figure 13 Creating OUs

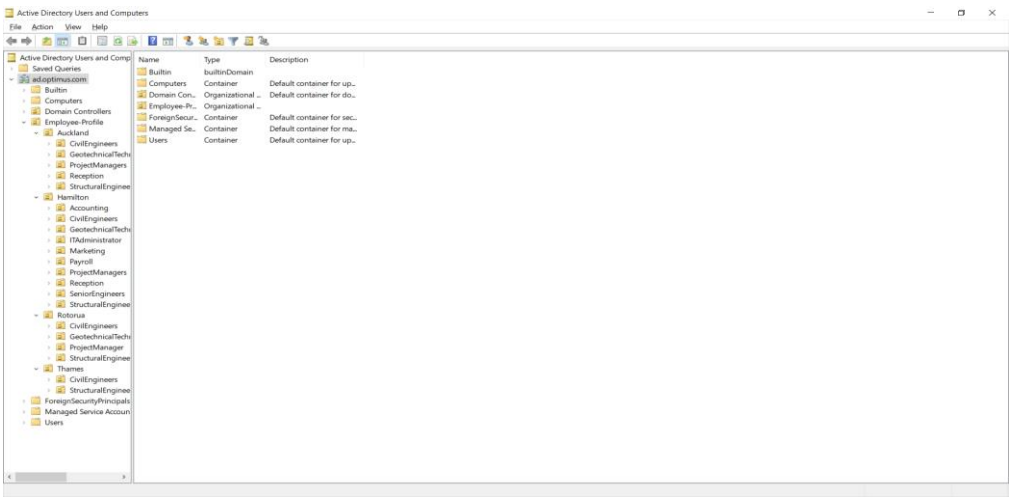


Figure 14 Organization Unites

Step 2 Importing the users by PowerShell Scripting

1. **Save the Script which import the Users that defined in the CSV file into the Active Directory.**

```
Import-Module ActiveDirectory

#Location need to be contingent on the situation
$users = Import-csv "C:\Users\Administrator\Desktop\tested\AD.csv"


ForEach ($user in $users) {

    $Username    = $user.username
    $Password    = $user.password
    $Firstname   = $user.firstname
    $Lastname    = $user.lastname
    $Department  = $user.department
    $OU1         = $user.ou1
    $OU2         = $user.ou2
    $OU3         = $user.ou3
    $dc1         = $user.dc1
    $dc2         = $user.dc2
    $dc3         = $user.dc3


    New-ADUser -Name "$Firstname $Lastname" -GivenName $Firstname -
Surname $Lastname -Department $Department -UserPrincipalName
"$Firstname.$Lastname" -Path "$OU1,$OU2,$OU3,$dc1,$dc2,$dc3" -
AccountPassword (convertto-securestring $user.password -AsPlainText -Force) -
ChangePasswordAtLogon $True

    echo "$Firstname $Lastname Account Created in AD"
```

Step 3 Creating CSV file

1. Follow the format of this documents and Modify with own preferences:

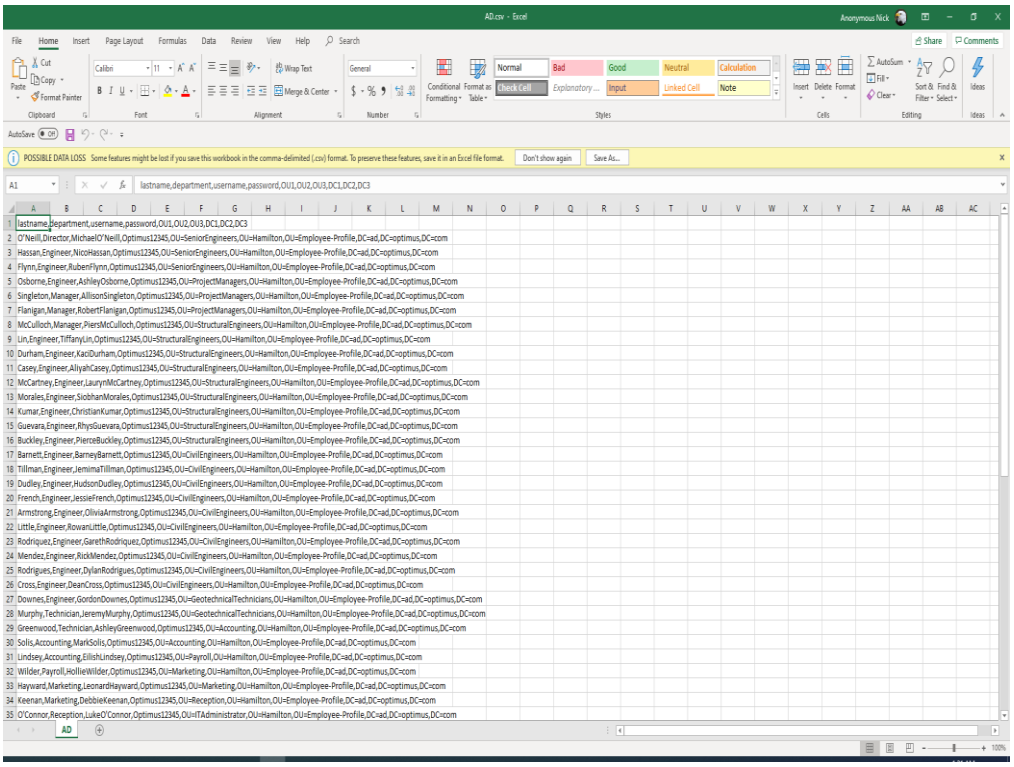


Figure 15 Active Directory CSV File

Step 4 Executing the Script in PowerShell

1. Paste the script into the PowerShell with Administrator Permissions:

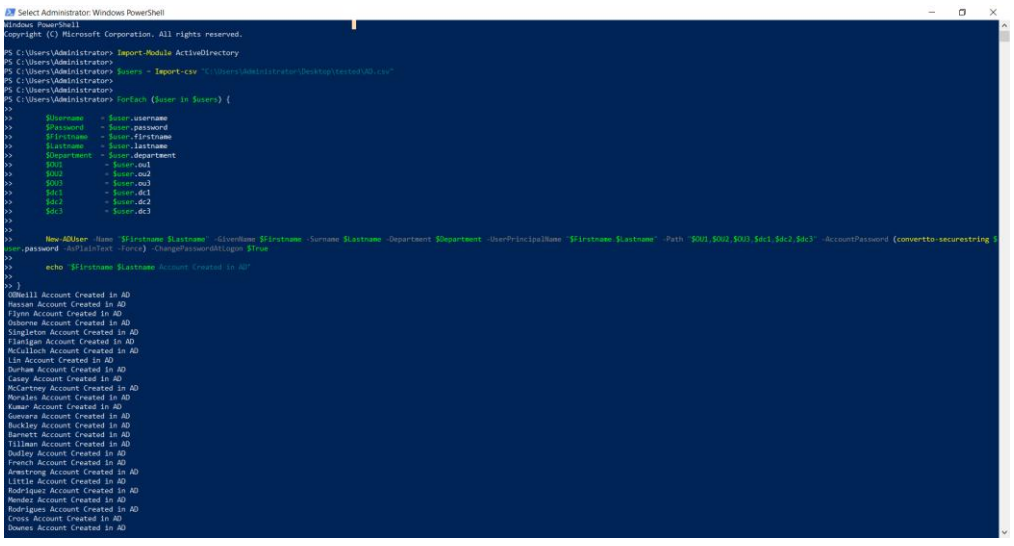


Figure 16 PowerShell

Step 5 Verifying the Active Directory Users

1. Return to the Active Directory Users and Computers, expand all the OUs that we created:

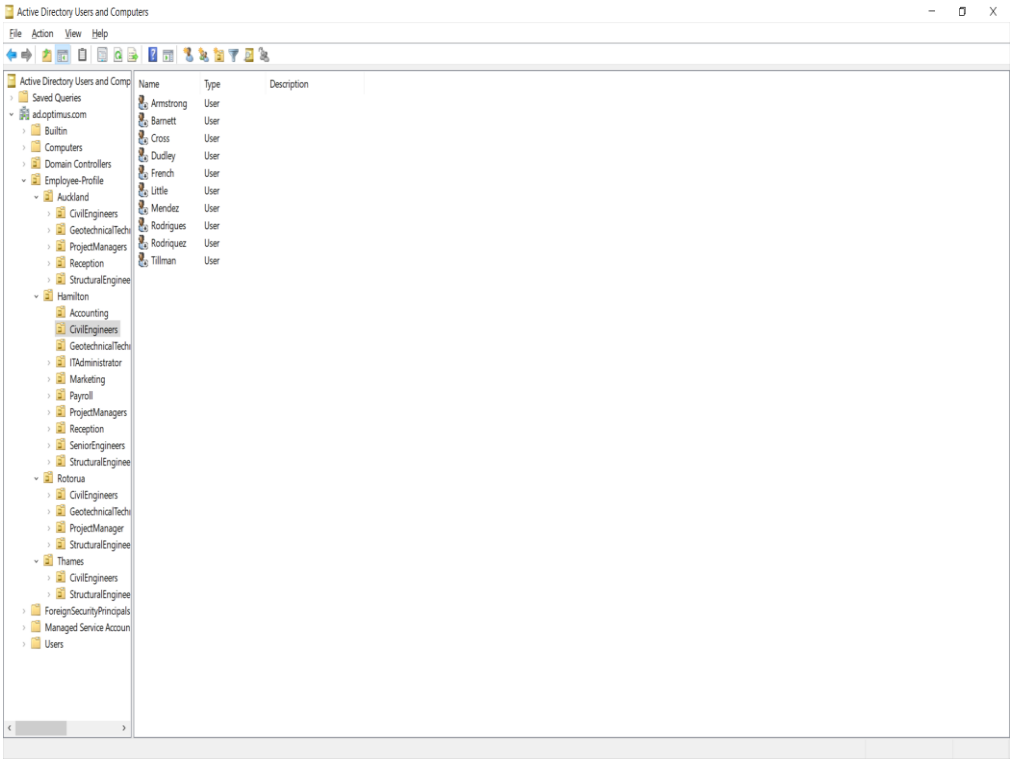


Figure 17 Verify Active Directory Users

5.6 Synchronization the folder between Master and Backup Node via Resilio-Sync

Step 1 Download and unzip the Resilio-Sync from the official website

1. Access to the website https://www.resilio.com/

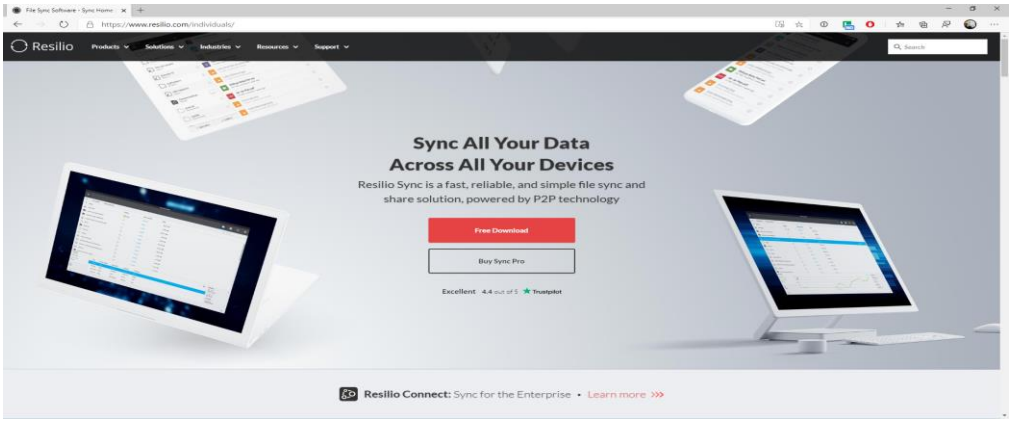


Figure 18 Resilio-Sync Website

2. Download the appropriate version of software, unzip the file and executing.

1. Unzip the file.

#tar -zxvf /home/server/Downloads/resilio-sync_x64.tar.gz

2. Execute the file.

 # ./rslsync

By using this application, you agree to our Privacy Policy, Terms of Use and End User License Agreement.

https://www.resilio.com/legal/privacy

https://www.resilio.com/legal/terms-of-use

https://www.resilio.com/legal/eula

Step 2 Access the resilio-sync via Browser

1. Open the browser and access http://127.0.0.1:8888/gui/ to resilio-sync:

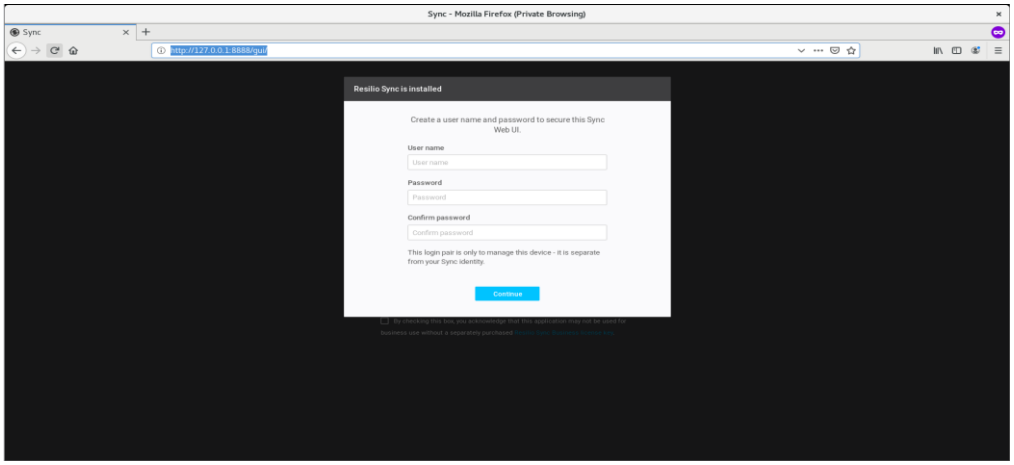


Figure 19 Resilio-Sync Web

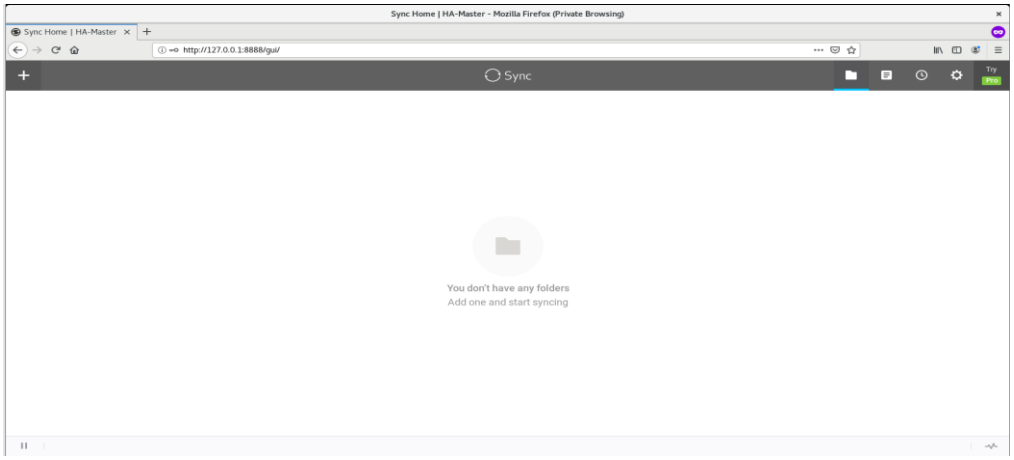


Figure 20 Resilio Sync Main Page

Step 3 Activating the Licences of Resilio-Sync

1. Navigate to the Setting and Click Apply Licence:

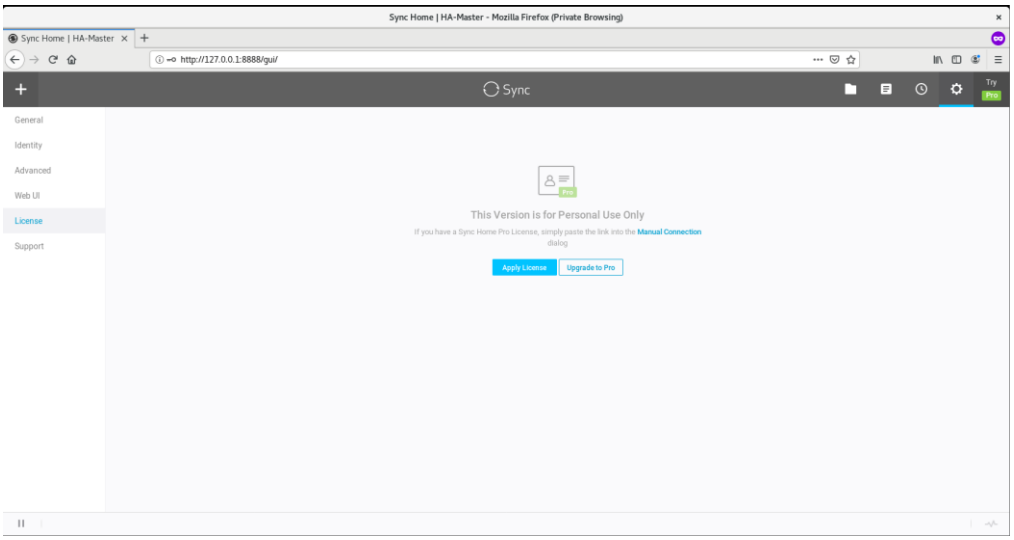


Figure 21 Applying Licence

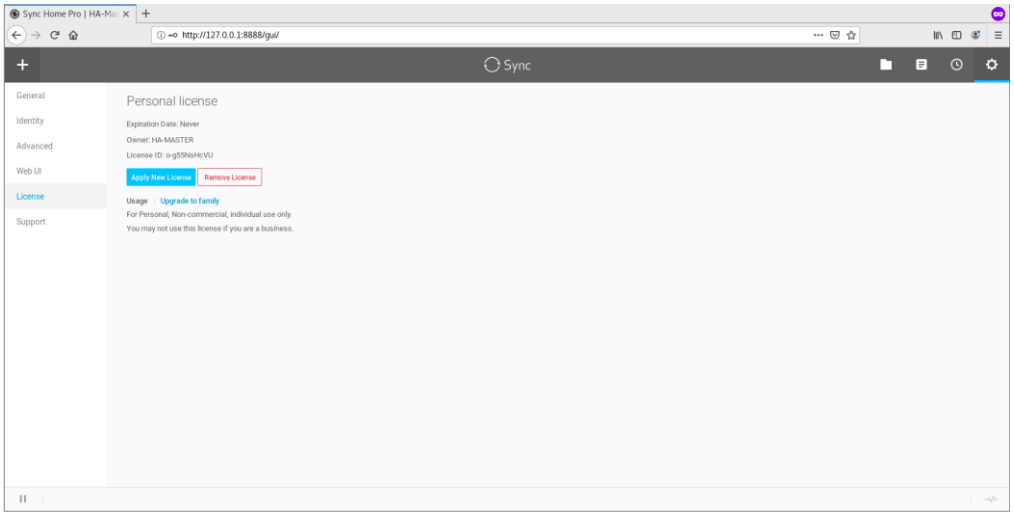


Figure 22 Review Licence

Step 4 Link two nodes for synchronization

1. Navigate to the identity tab and Click link Devices:

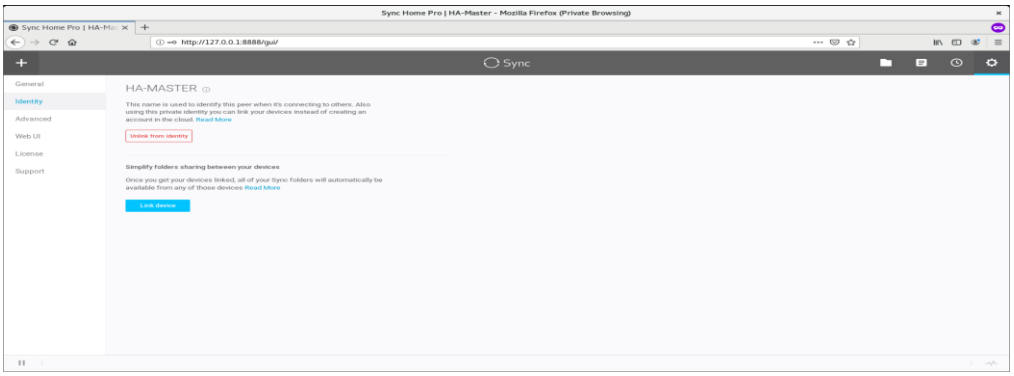


Figure 23 Resilio Sync Identity Section

2. Link the Master and Backup node together:

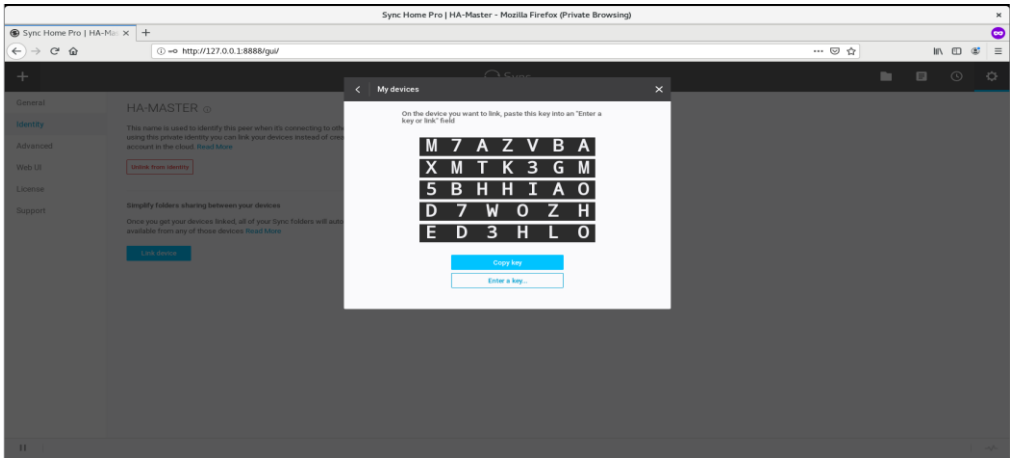


Figure 24 Link Devices Manually

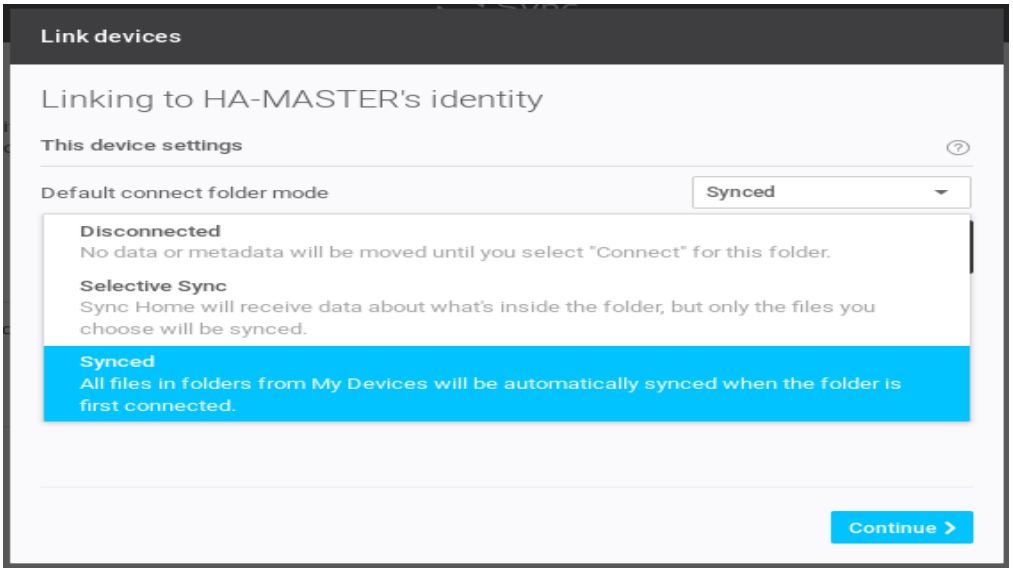


Figure 25 Devices Sync Mode

Step 5 Configuring frequency of sync time

1. Navigate to the Open Power User Preferences under the Advance Section and configure the folder_rescam_interval to 30s:

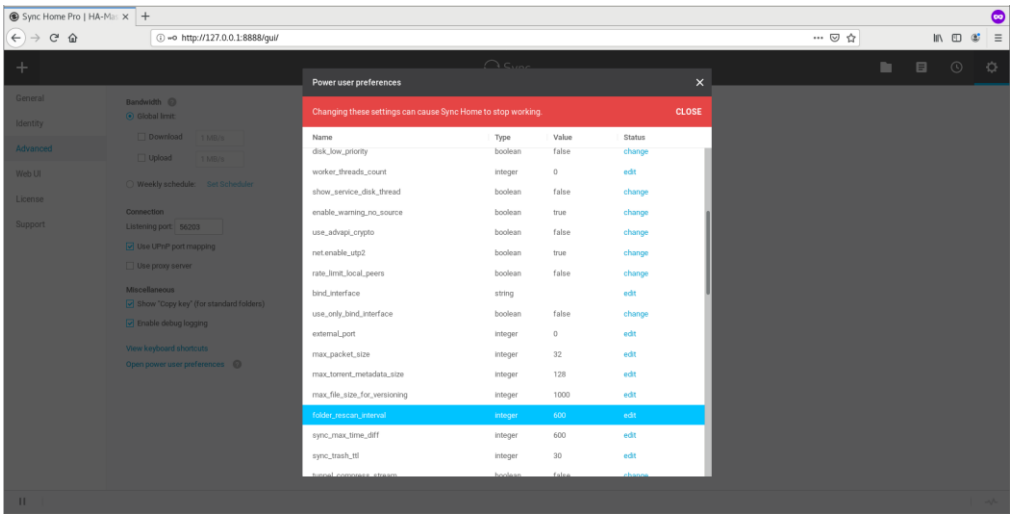


Figure 26 Open Power User Preferences

Step 6 Configuring Synchronization folder

1. Click the Plus Button and Add a Directory for sync and Copy the share link to the second node:

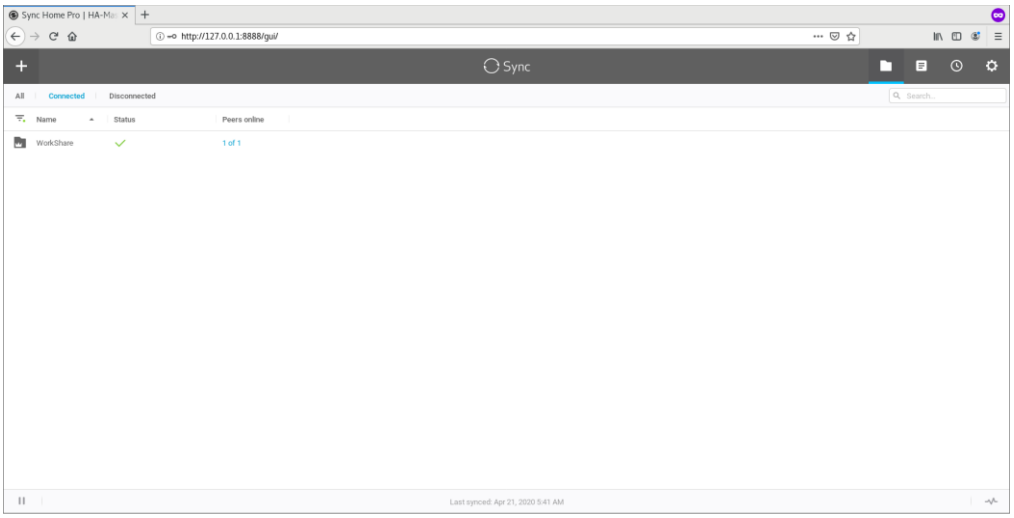


Figure 27 Sync Folder

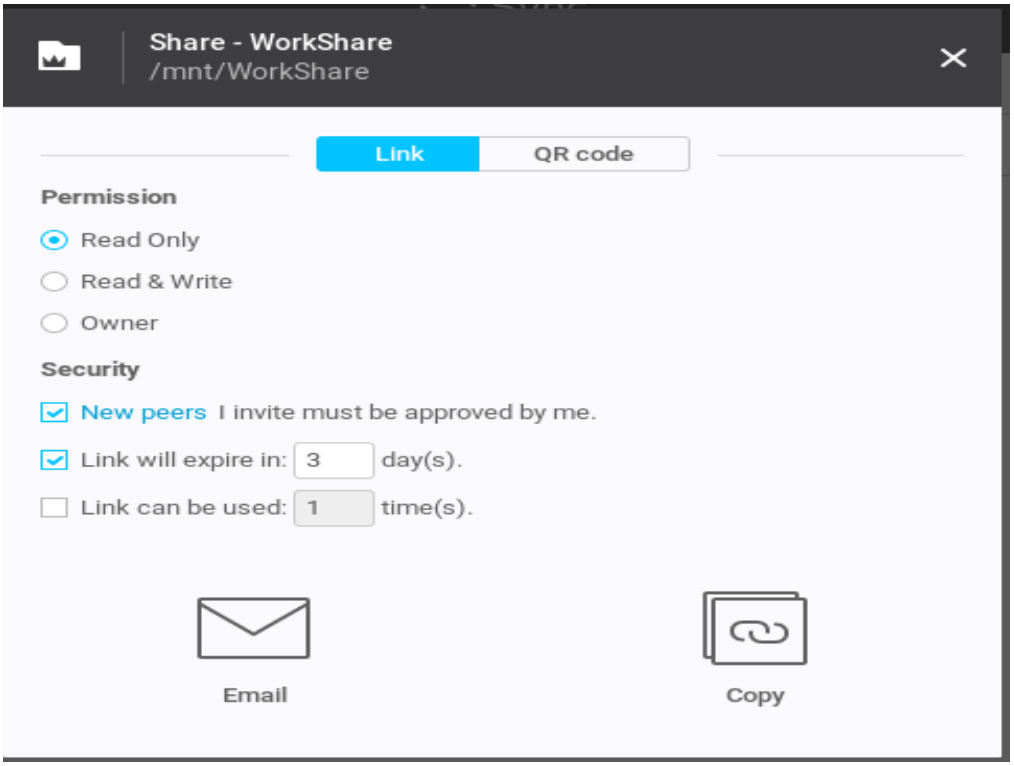


Figure 28 Share link

2. Verify the Synchronization history

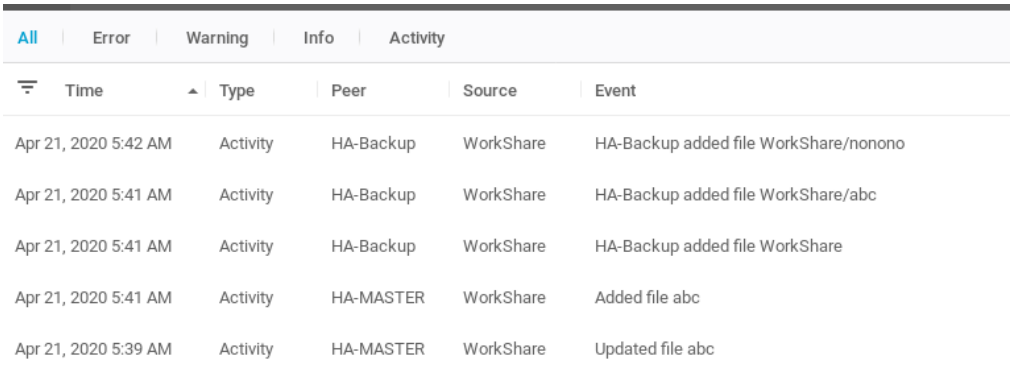


Figure 29 Synchronization history

6.0 Configuration on Samba Share and its permissions

6.1 Configuring Active Directory Group for Users

Step 1 Grouping the Users to appropriate Group

1. **Group the Users to the Appropriate Groups:**

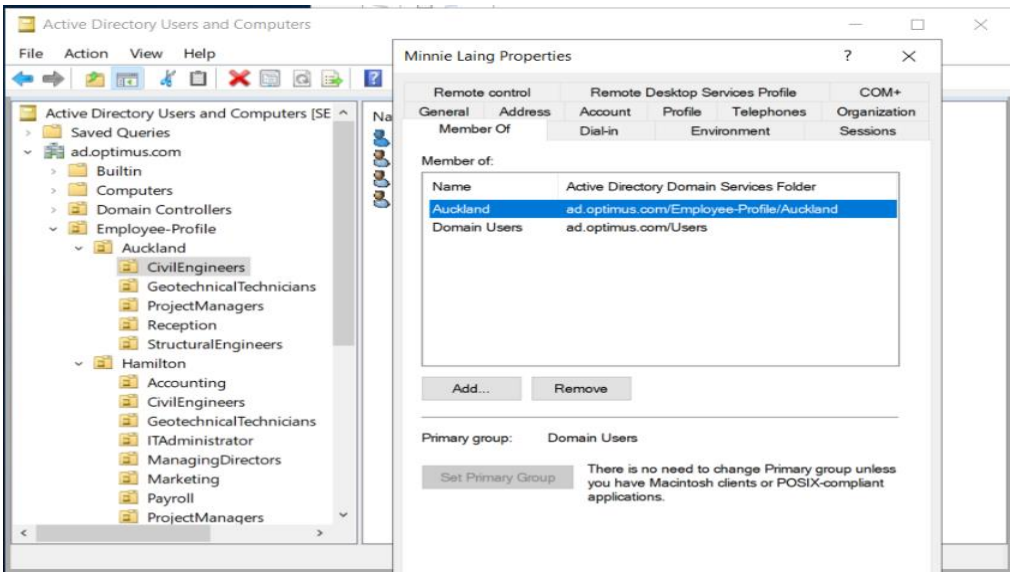


Figure 30 Grouping Users

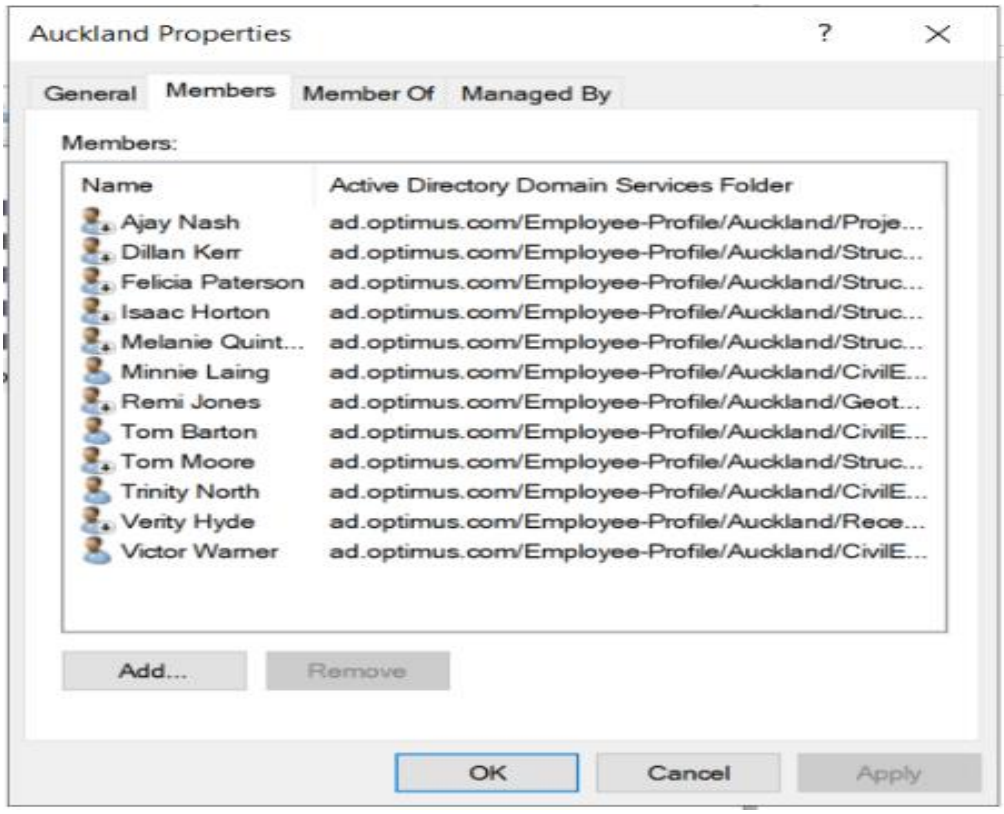


Figure 31 Group Members

Step 2 Verifying the Groups and Users on Linux Server

1. **Verify the Groups.**

#wbinfo -g

2. **Verify the Users.**

#wbinfo -u

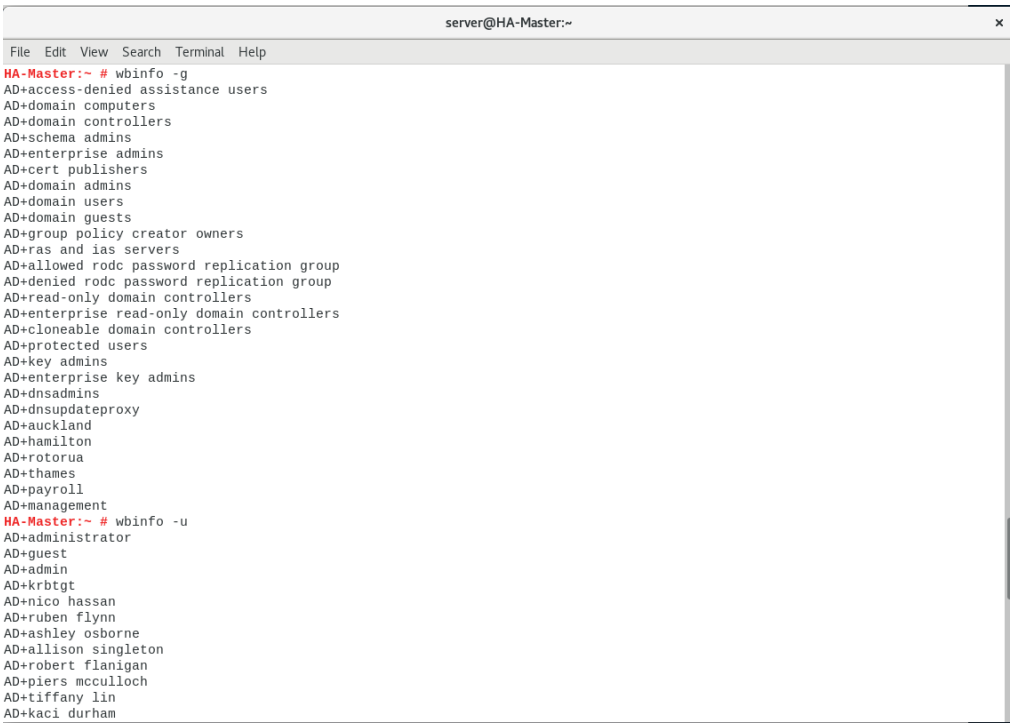


Figure 32 Verify the Groups and Users

6.2 Configuring the Permission on Samba Share

Step 1 Paste the Setting on Both nodes

1. Add the following Setting at the end of the file /etc/samba/smb.conf

```
[WorkFolder]
        comment = WorkShare
        path = /mnt/WorkShare/WorkShare
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+Domain Admins"
        admin users = @"AD+Domain Admins"
        hide unreadable = yes
        access based share enum = true
[Auckland]
        comment = Auckland
        path = /mnt/WorkShare/WorkShare/Auckland
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+auckland"
        admin users = @"AD+Domain Admins"
        access based share enum = true
[Hamilton]
        comment = Hamilton
        path = /mnt/WorkShare/WorkShare/Hamilton
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+hamilton"
```

```
        admin users = @"AD+Domain Admins"
        access based share enum = true
[Rotorua]
        comment = Rotorua
        path = /mnt/WorkShare/WorkShare/Rotorua
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+rotorua"
        admin users = @"AD+Domain Admins"
        access based share enum = true
[Thames]
        comment = Thames
        path = /mnt/WorkShare/WorkShare/Thames
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+thames"
        admin users = @"AD+Domain Admins"
        access based share enum = true
[Payroll]
        comment = Payroll
        path = /mnt/WorkShare/WorkShare/Payroll
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+payroll"
        admin users = @"AD+Domain Admins"
        access based share enum = true
[Share]
        comment = Share
        path = /mnt/WorkShare/WorkShare/Share
```

```
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+domain users"
        admin users = @"AD+Domain Admins"
[Management]
        comment = Management
        path = /mnt/WorkShare/Management
        read only = no
        browseable = yes
        inherit acls = yes
        inherit permissions = yes
        valid users = @"AD+management"
        admin users = @"AD+management"
        access based share enum = true
```

Step 2 Reboot the SMB Services

```
# service smb restart
```

Step 3 Verifying the Permission

1. Login to a normal employee account:

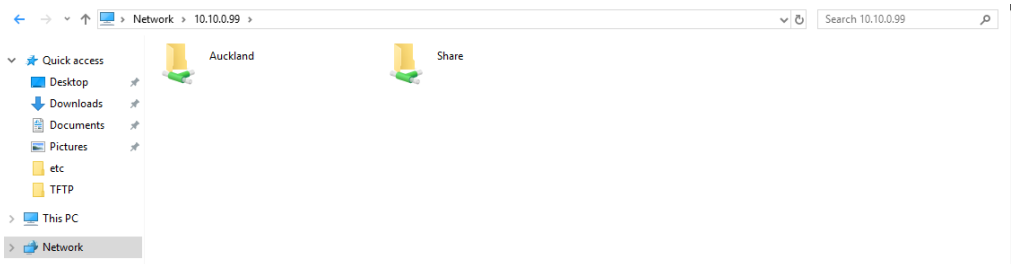


Figure 33 Verify Permission - 1

2. Login to Management Account:

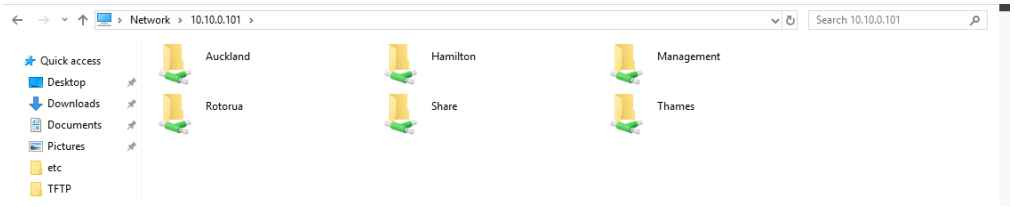


Figure 34 Verify Permission - 2

7.0 Configuration on Proxy Server

7.1 Creating AnyConnect VPN on ASA Device

Step 1 Enabling HTTP on ASA

```
ASA>http server enable
ASA>http 10.10.0.110 255.255.255.255 inside
```

Step 2 Installing ASDM and Accessing to the ASA

1. Open a browser on SERVER-AD and access to the ASA via HTTPS Protocol:

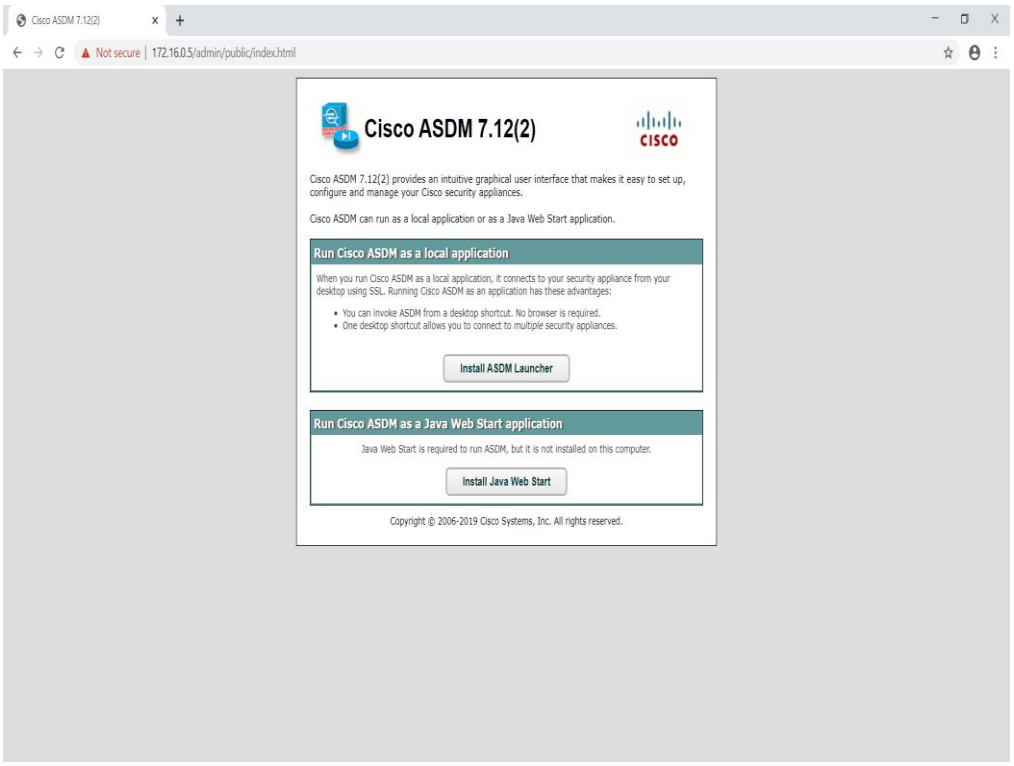


Figure 35 ASDM

2. Accessing ASA via ASDM

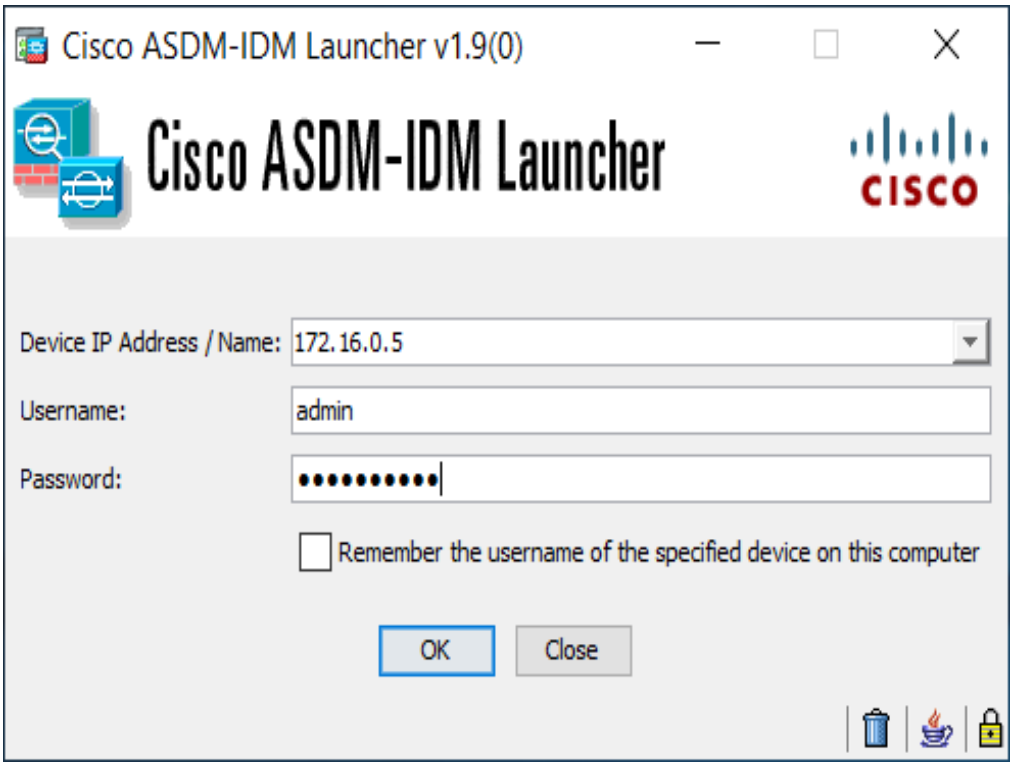


Figure 36 Cisco ASDM

Step 3 Configuring the Basic Setting on ASA

1. **Follow the instruction on the previous ASA section to configurate.**

Step 4 Configuring AnyConnect VPN

1. Click the AnyConnect VPN Wizard under the VPN Wizards:

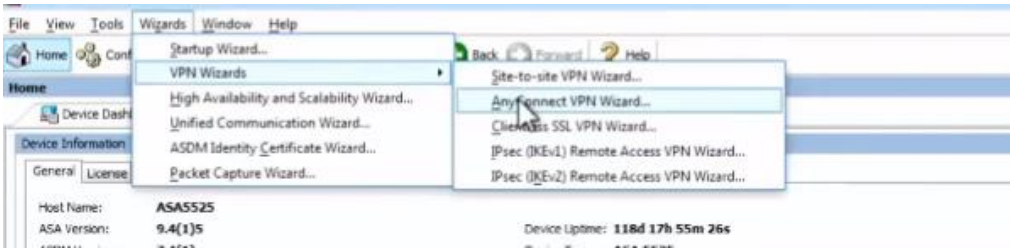


Figure 37 AnyConnect Wizard

2. Setting a Profile name and click Next:

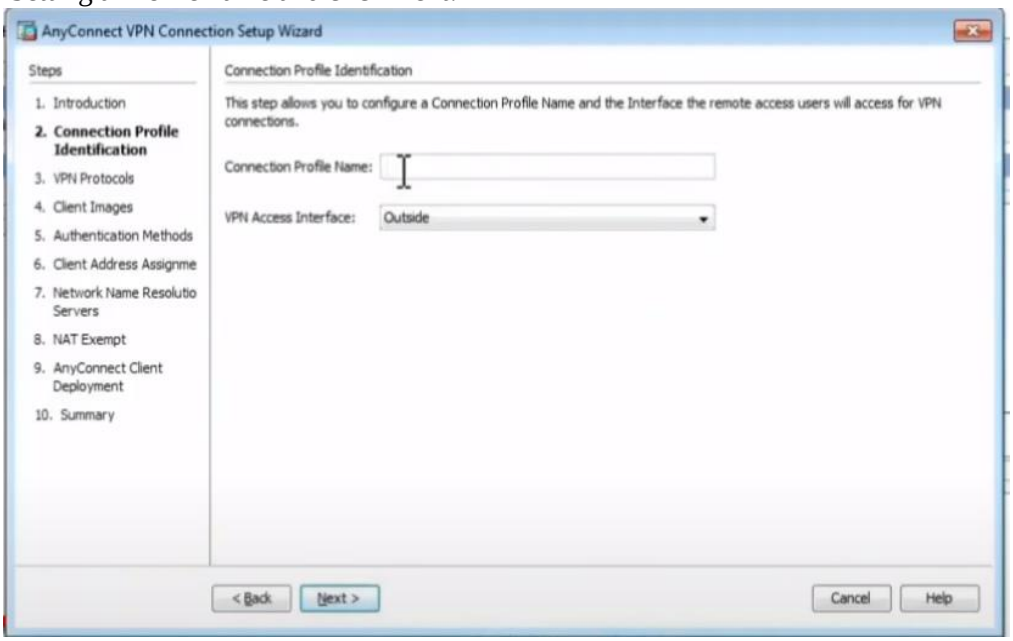


Figure 38 AnyConnect VPN Wizard

3. Select SSL Protocol and Click Next:

Figure 39 VPN Protocol

4. Click Add and select the image in order to add AnyConnect Client Image for Client to install (name: anyconnect-win-XXX-webdeploy-k9.pkg):

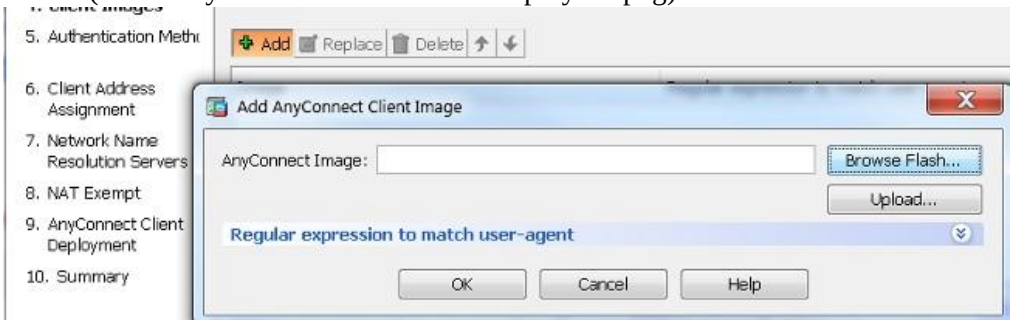


Figure 40 AnyConnect Client Image

5. Setting Up the Users for AnyConnect VPN:

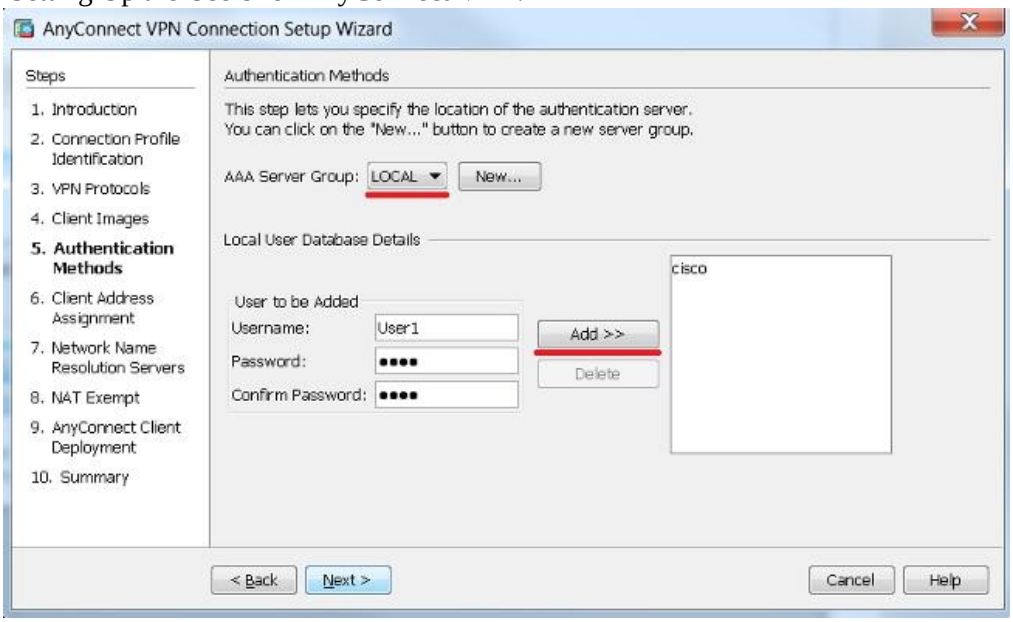


Figure 41 Adding Users

6. Assign the IP Address Range for AnyConnect VPN:

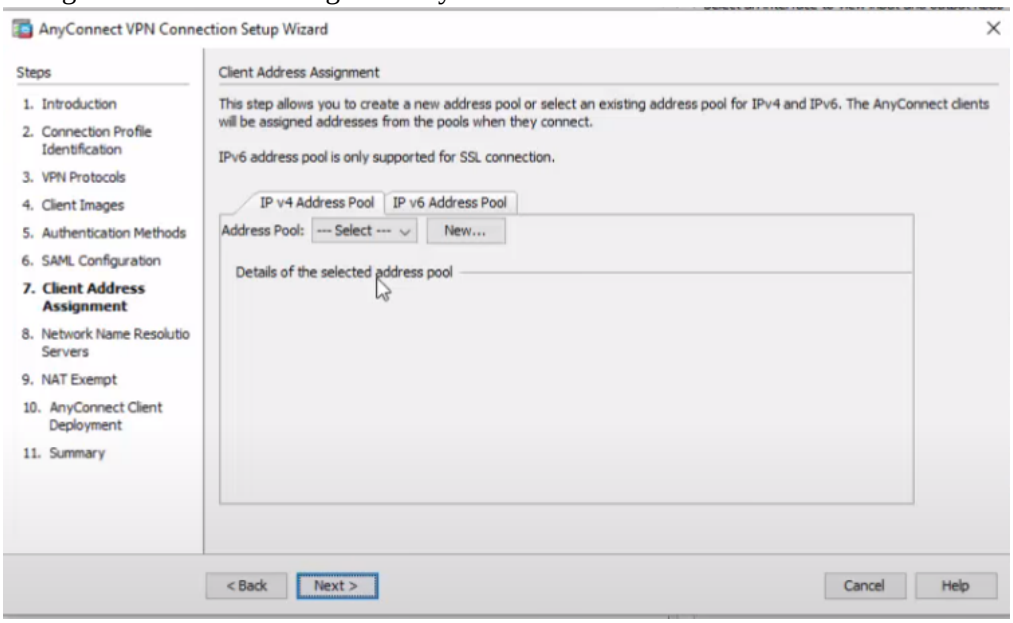
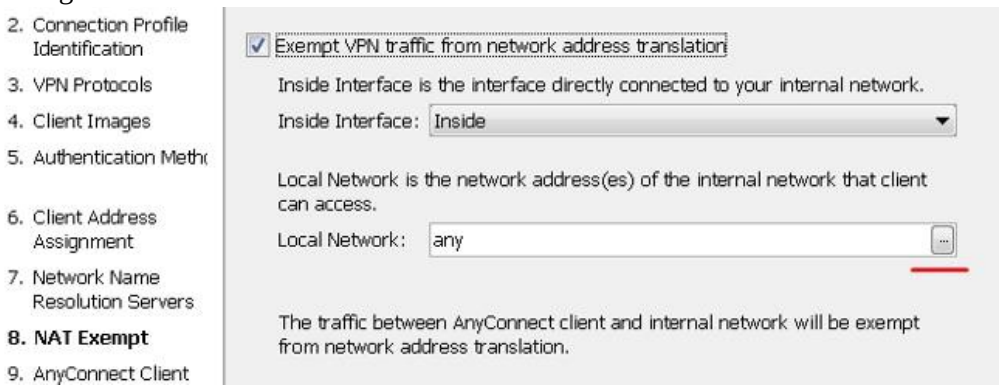


Figure 42 IP Address Pool

7. Check the Exempt VPN traffic from network address translation check box and configure the LAN and WAN interfaces:



Step 5 Configuring Split Tunnel mode

1. Edit the AnyConnect Profile and Uncheck the Policy and Network List:

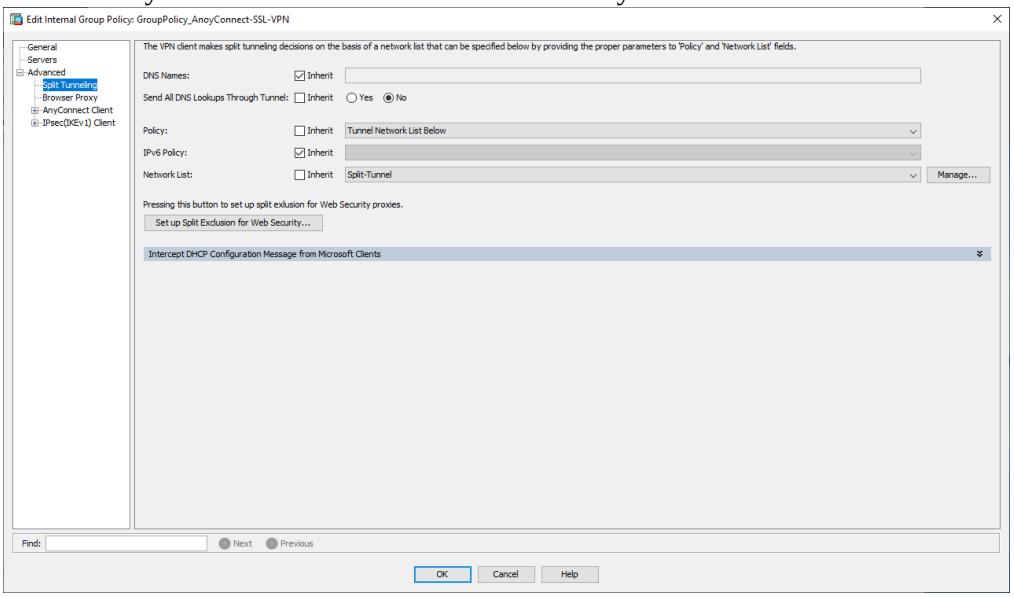


Figure 43 Policy Configuration

2. Adding an ACE and ACL for Split Tunnel, the IP Address will be the inside LAN Address:

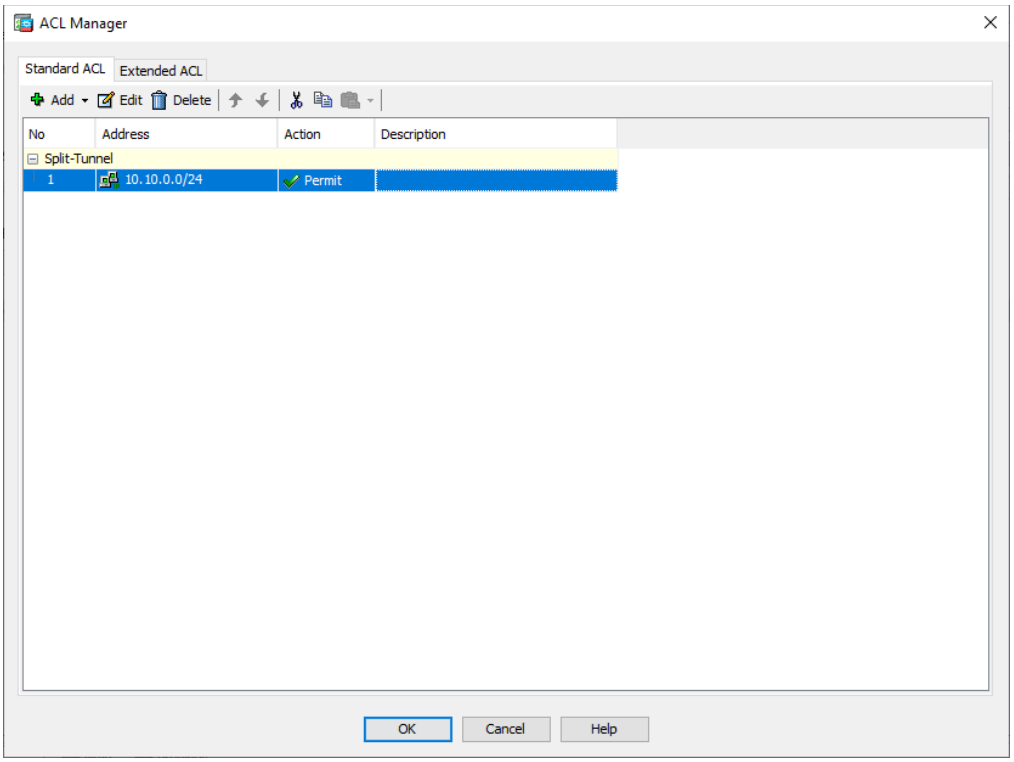


Figure 44 ACL Manager

3. Select the ACE and Save the Configuration:

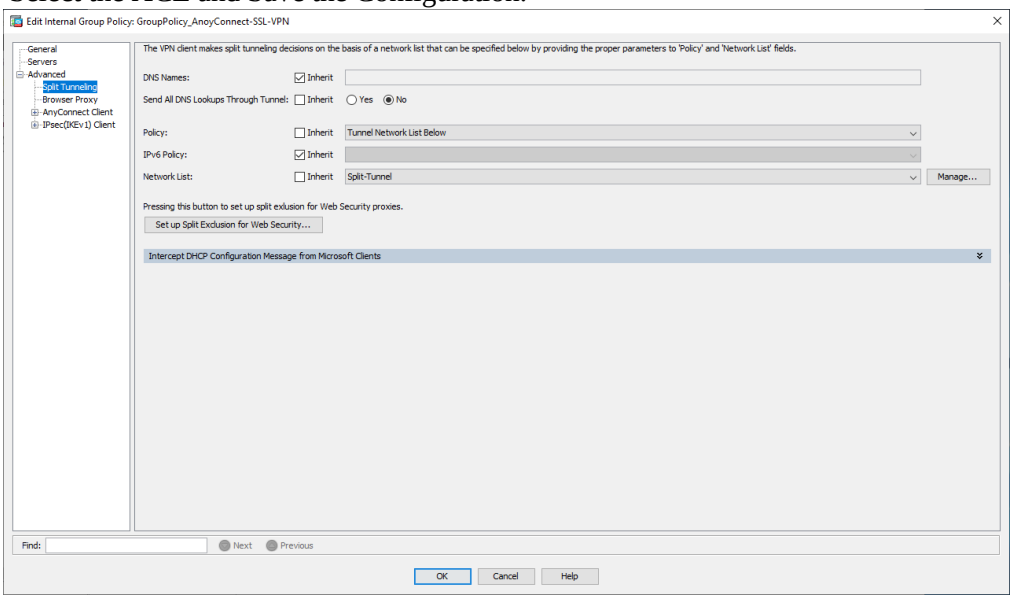


Figure 45 Save the Configuration

Step 6 Connecting the Proxy Server via remote users

1. Access the Public IP Address from the remote users to the Proxy Server:

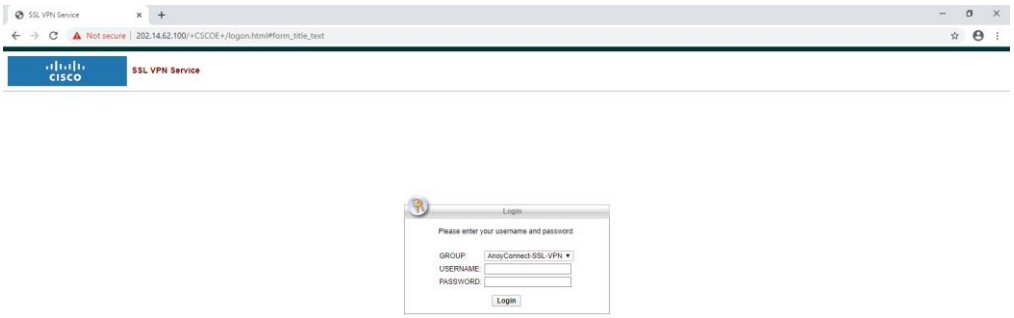


Figure 46 AnyConnect Protol

2. Install the AnyConnect VPN Client on the Remote PCs:

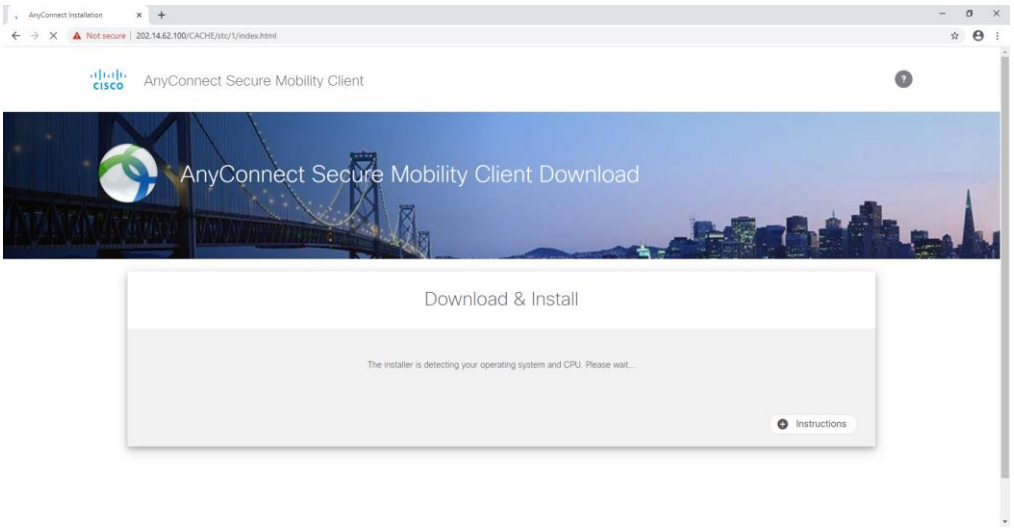


Figure 47 Install VPN Client

3. Connect the VPN to the Company Network

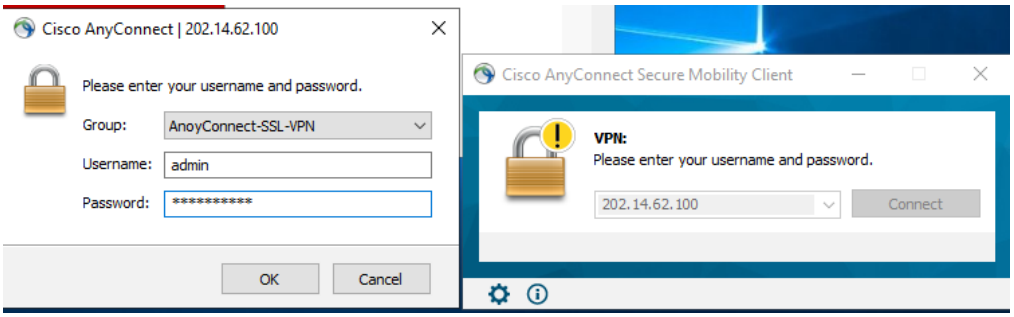


Figure 48 Connecting VPN

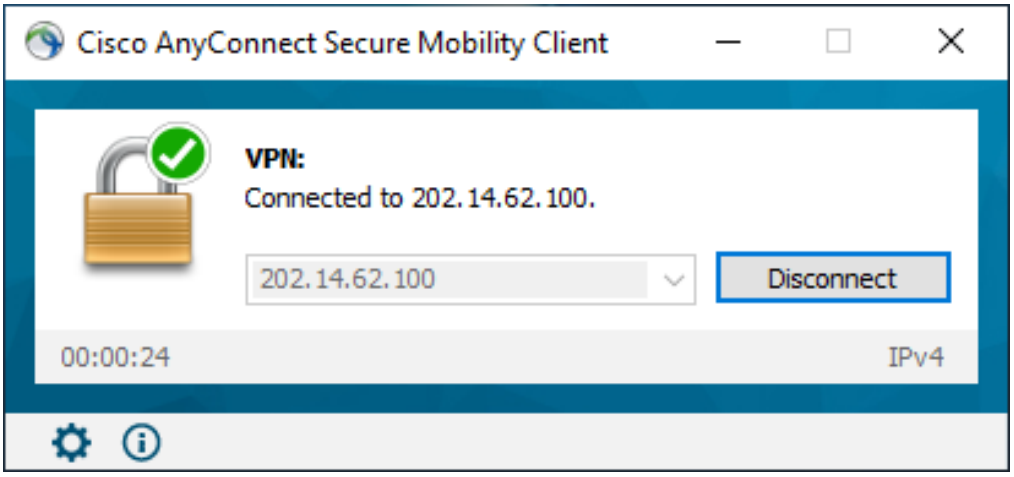


Figure 49 VPN Connected

8.0 Configuration on WDS and DHCP Service

8.1 Configuring WDS and DHCP Service

Step 1 Install the WDS and DHCP Service

1. Open the Add Roles and Features Wizard and Select the Services:

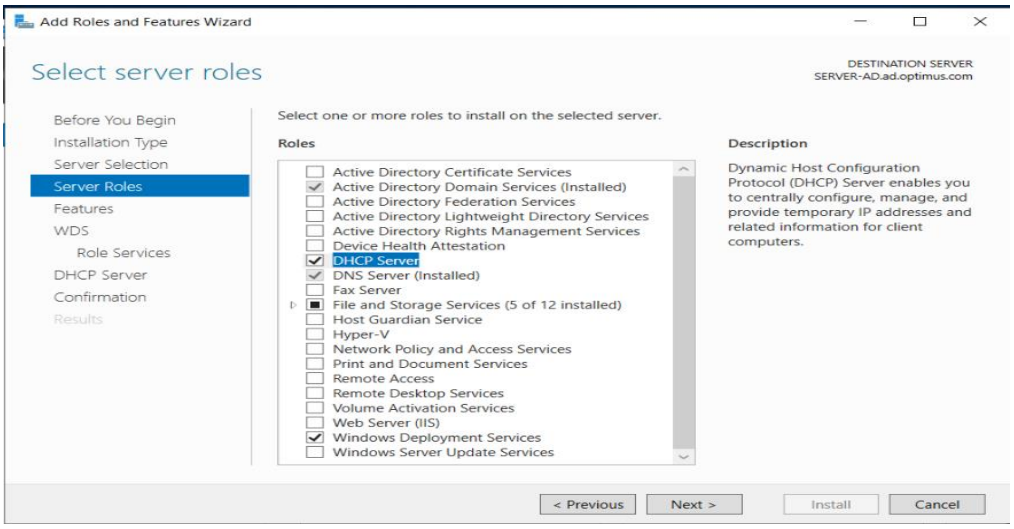


Figure 50 Install DHCP and WDS Service

Step 2 Configuring DHCP Service

1. Navigate to the DHCP Post-Install Wizard and Check Skip AD Authorization box:

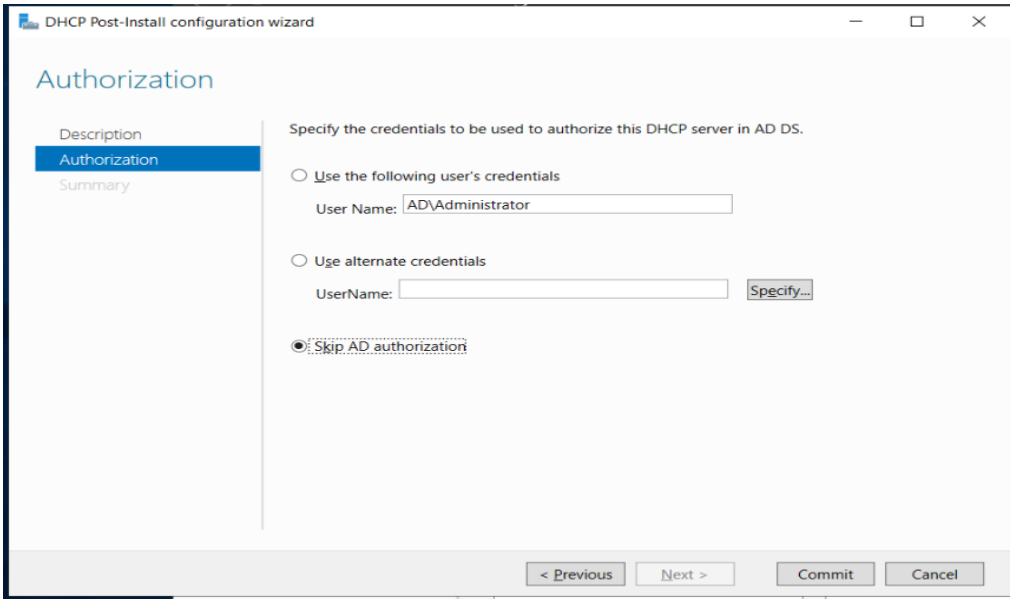


Figure 51 DHCP Post-Install Wizard

2. Navigate to the DHCP Management tool and Create a new Scope:

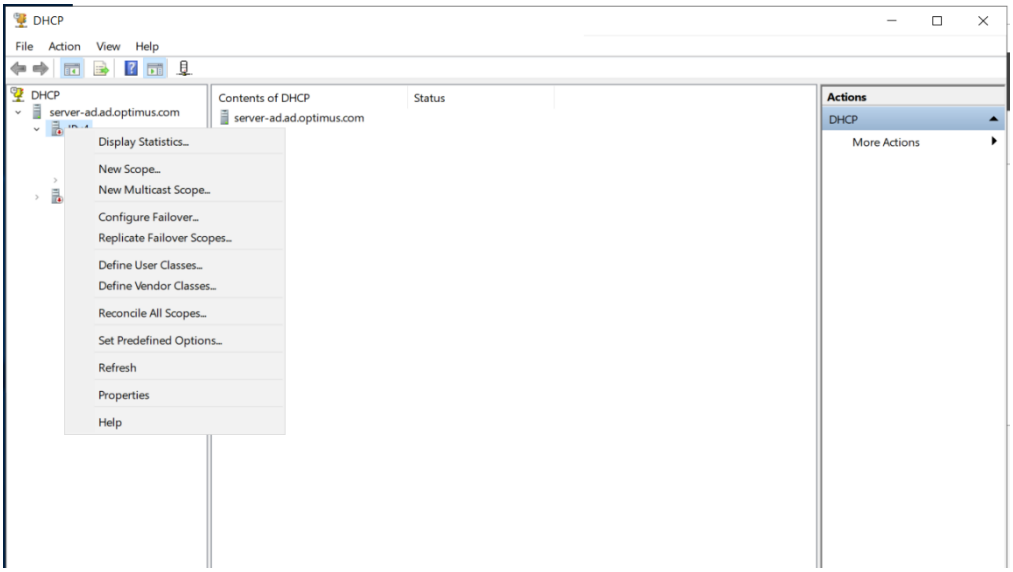


Figure 52 DHCP Management

3. Set up the name of the Scope:

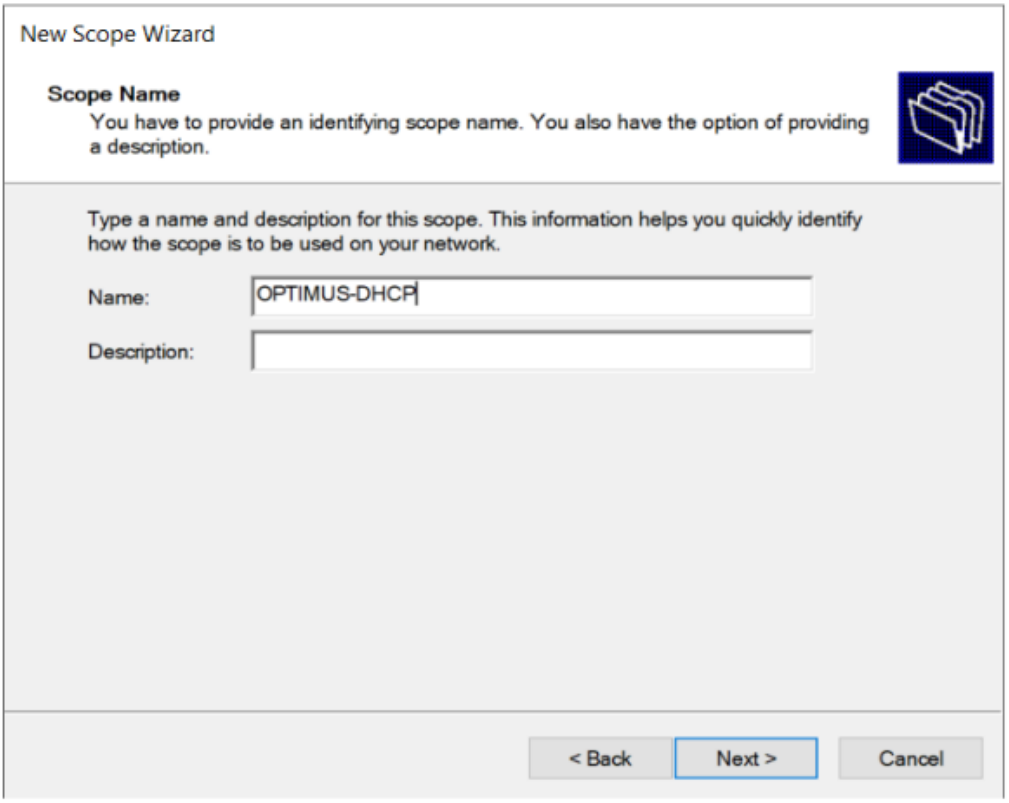


Figure 53 DHCP SCOPE - 1

4. Configure DHCP IP range and Subnet mask:

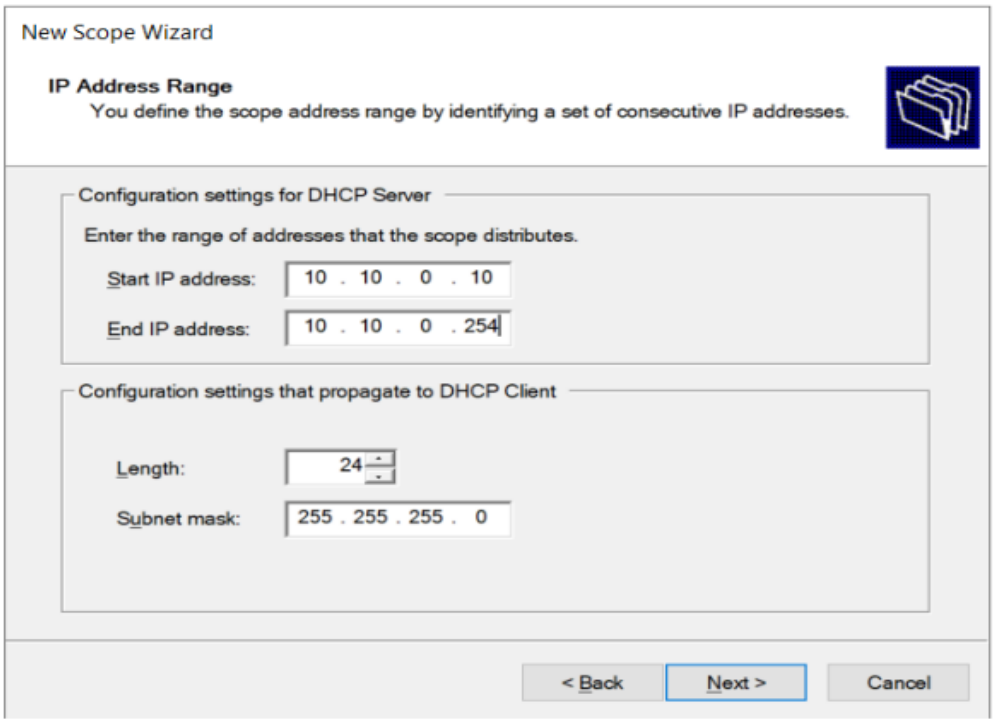


Figure 54 DHCP SCOPE - 2

5. Configure Exclusion IP Address:

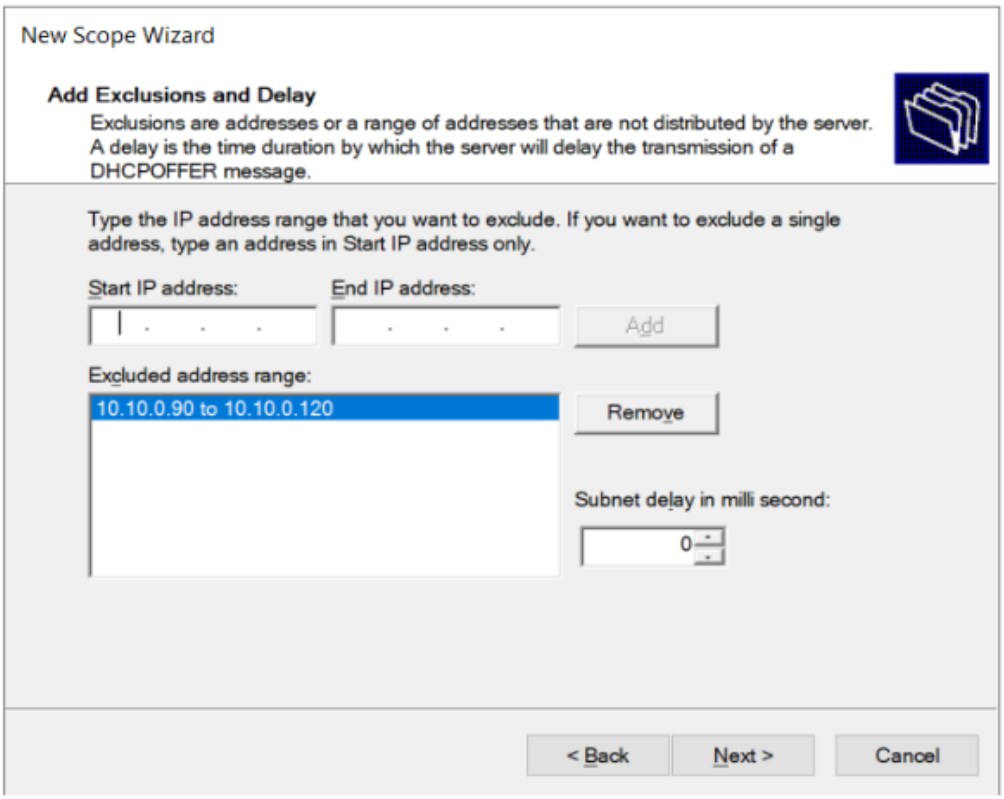


Figure 55 IP Address Exclusion

6. Set the Lease Duration to 2 hours:

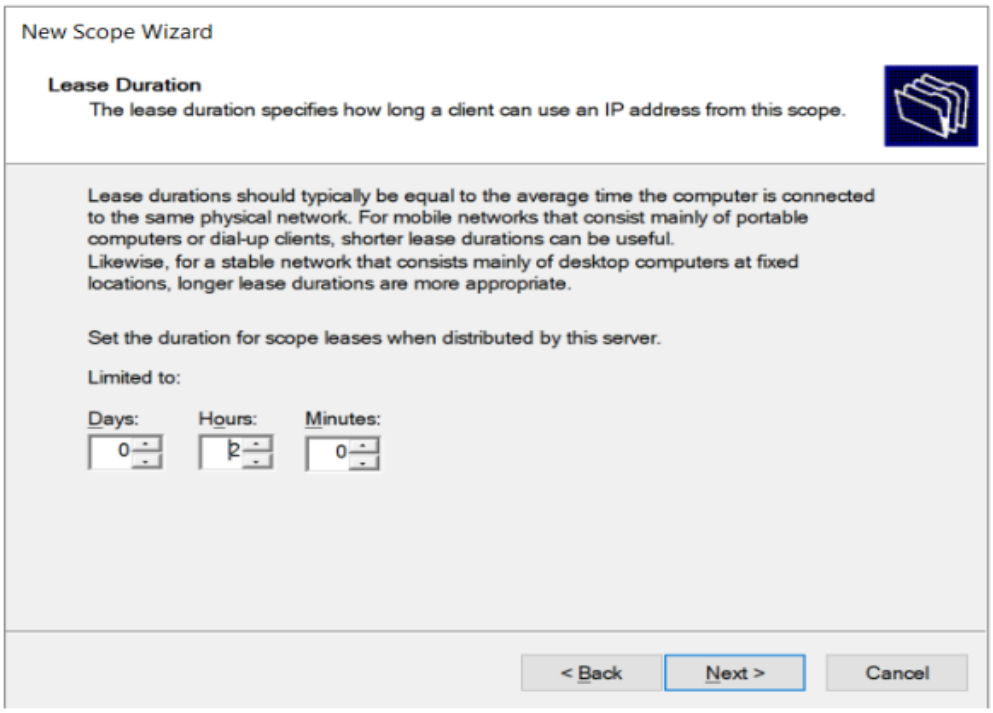


Figure 56 Lease Duration

7. Set up the Default Gateway:

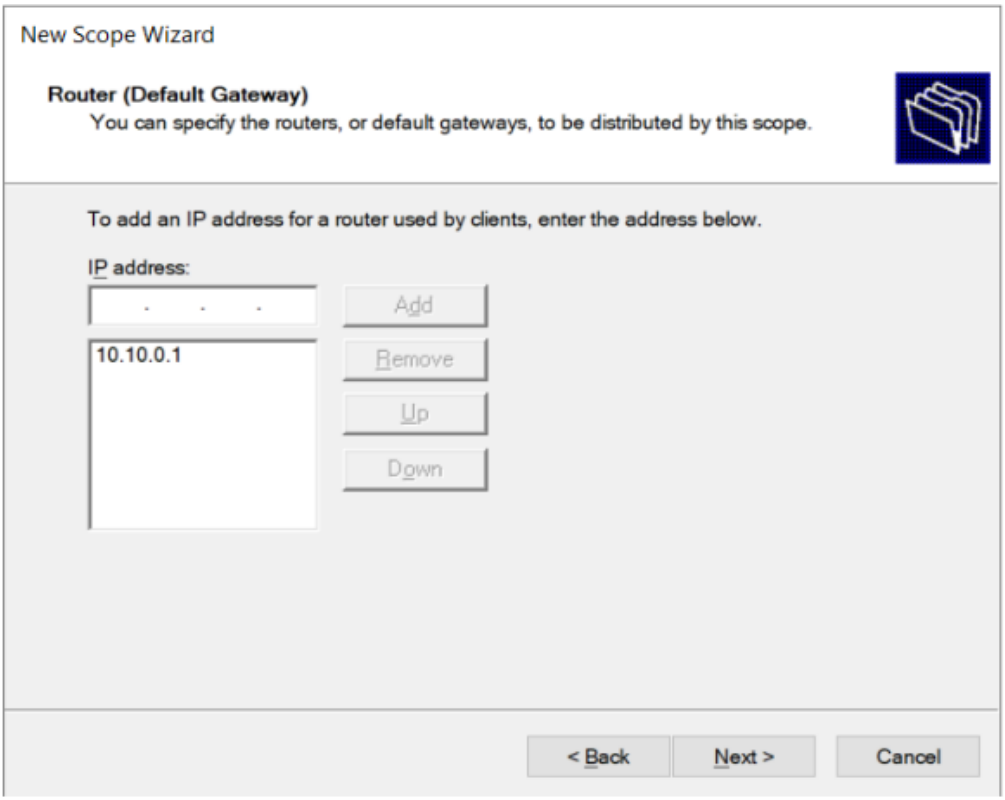


Figure 57 Scope Default Gateway

8. Configure the DNS server for DHCP Client:

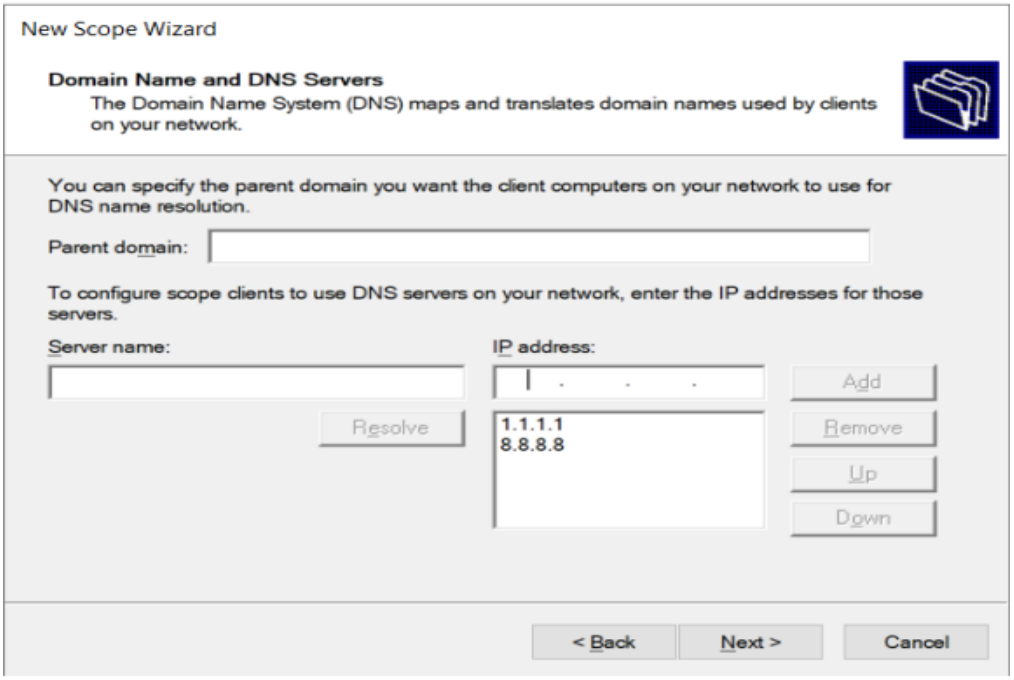


Figure 58 DNS For DHCP

9. Click Next until the Wizard finished.

Step 3 Configuring WDS Service

1. Navigate to the Windows Deployment Services Tool and Open the Configuration Wizard:

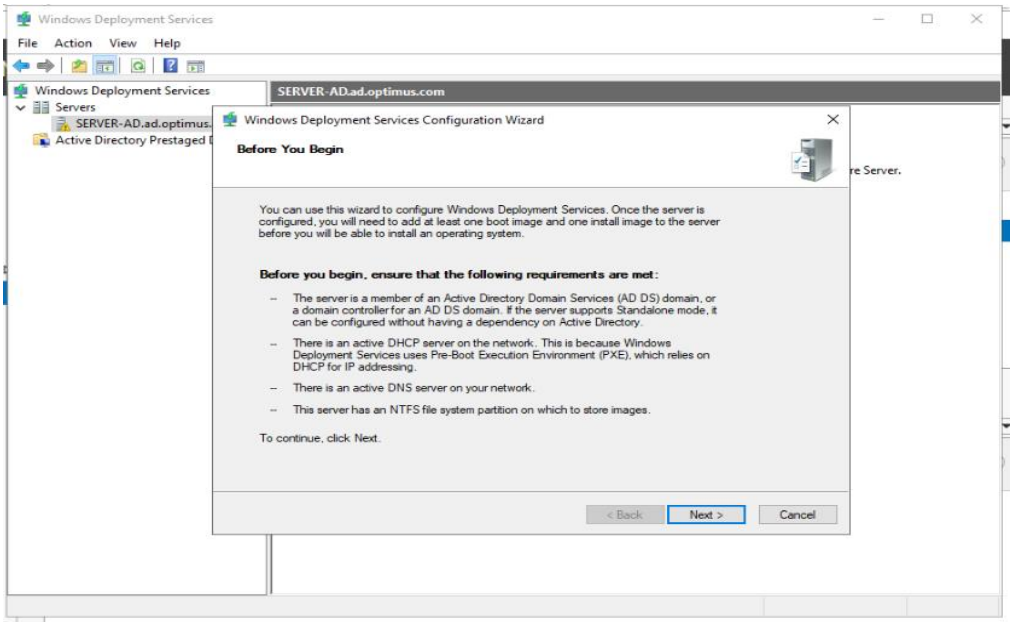


Figure 59 Windows Deployment Services Configuration Wizard

2. Select the Standalone Server:

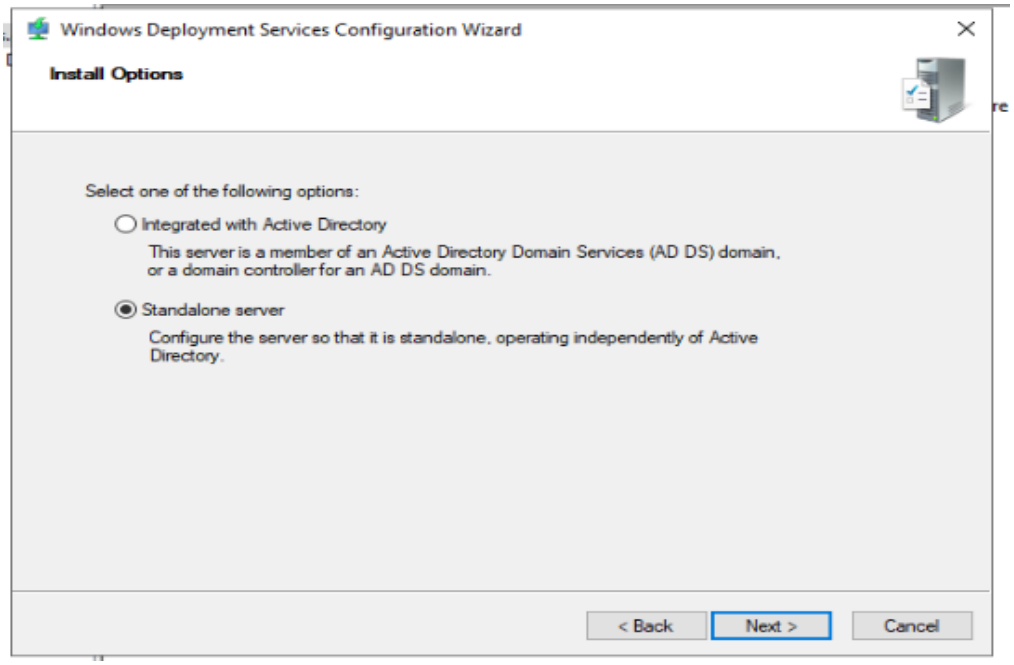


Figure 60 Windows Deployment Services Configuration Wizard - 2

3. Check the Respond to All Client Computers box:

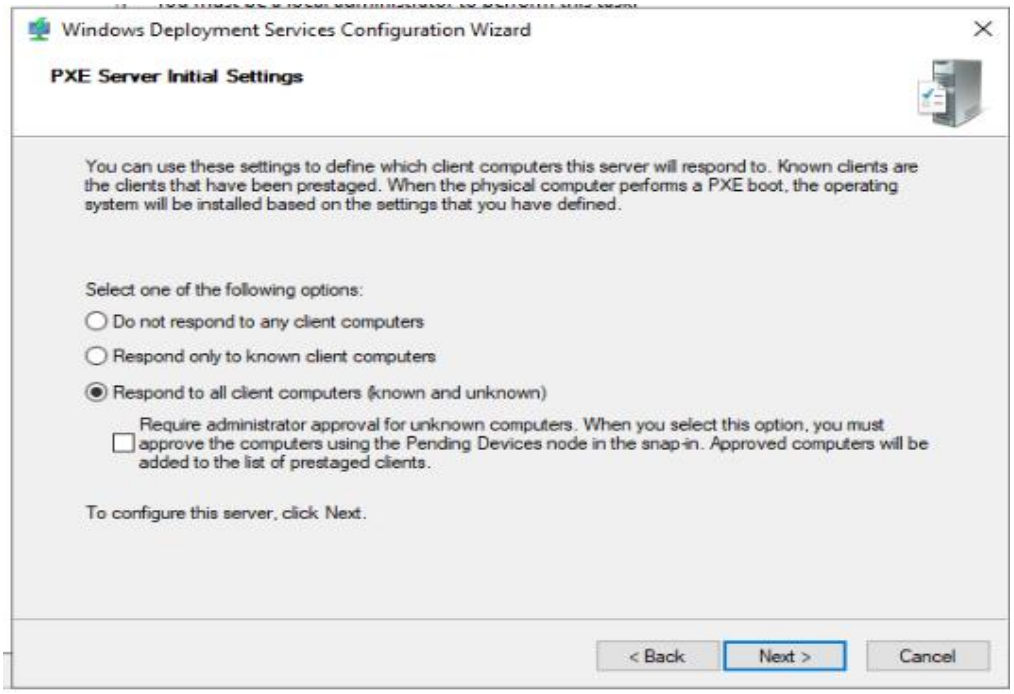


Figure 61 PXE Server Initial Settings

4. Click Next until finish.

5. Add install images to WDS Services:

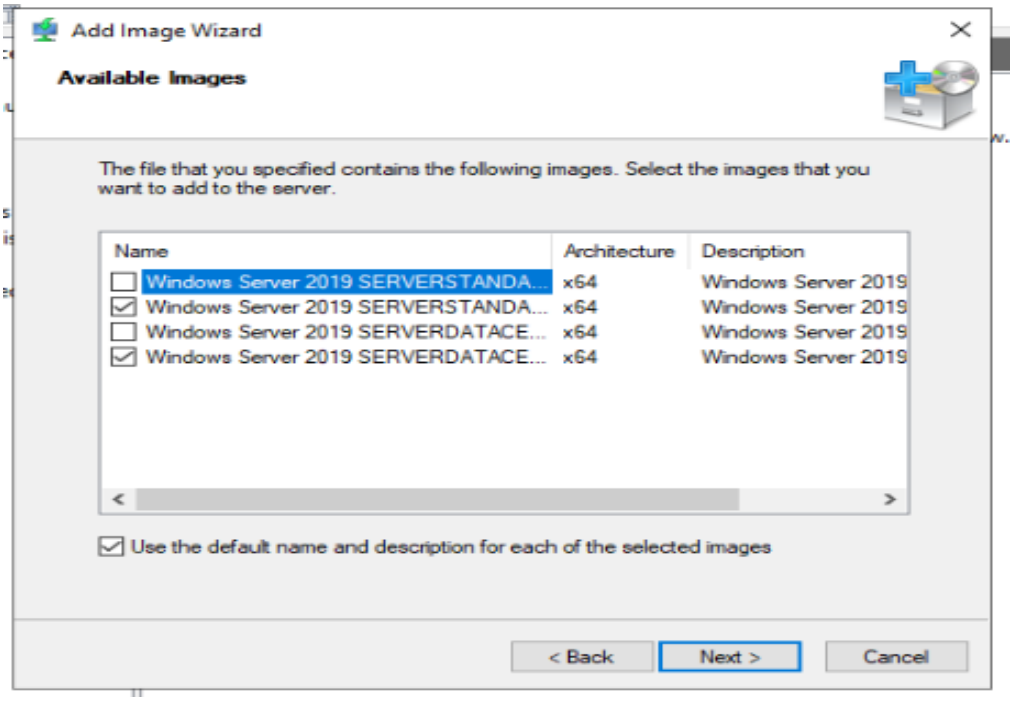


Figure 62 Add Images

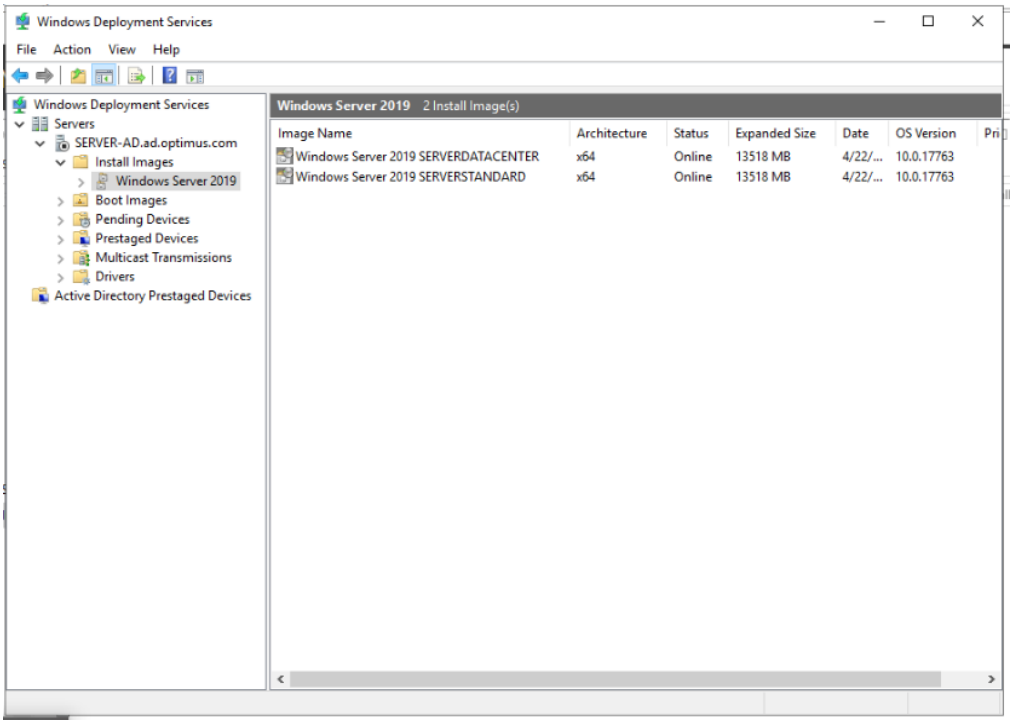


Figure 63 Windows Server Install Images

6. Add the Boot Image:

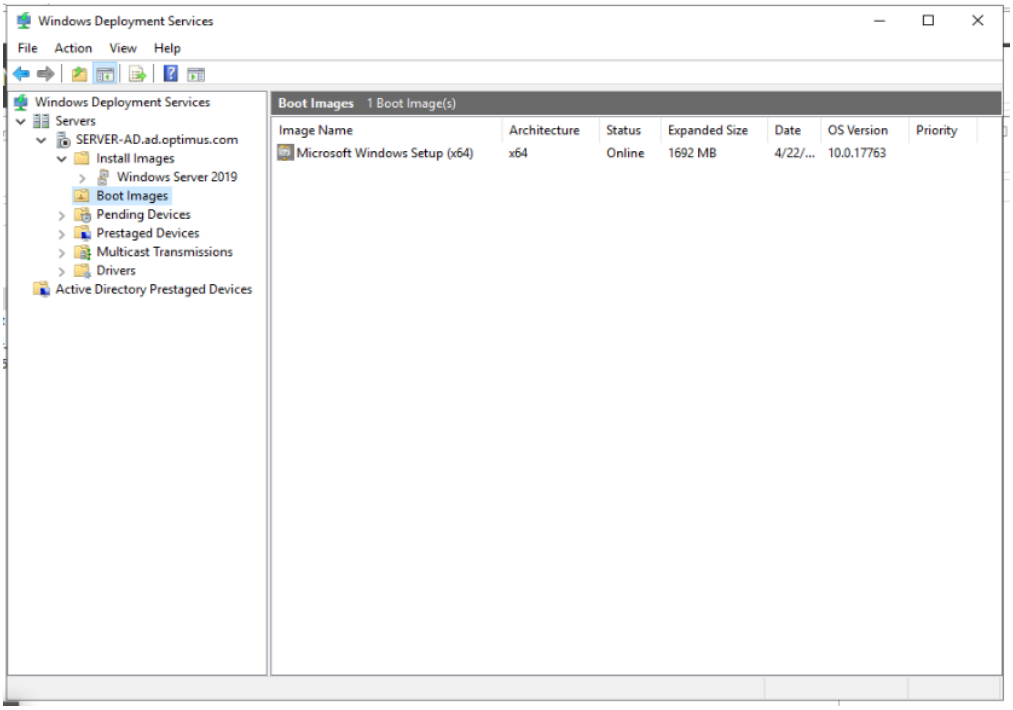


Figure 64 Boot Image

7. Start the WDS Service.

Step 4 Verifying the WDS Services

1. Use Network Boot from PC:

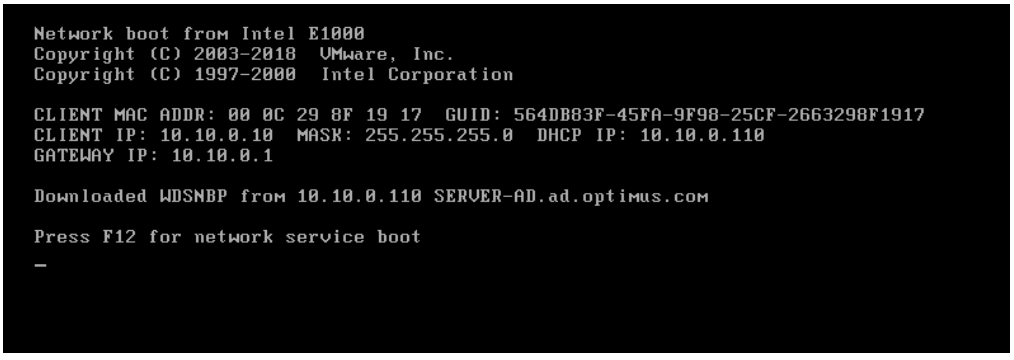


Figure 65 Network Boot

2. Press F12 for PXE Boot Mode:

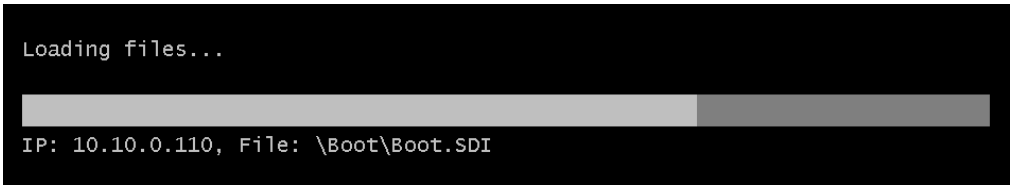


Figure 66 Loading Image

Figure 67 PXE BOOT