MCSA Project

By : Nasim Daghash

lecturer: Eliran Berkovich

INT College

Introduction:

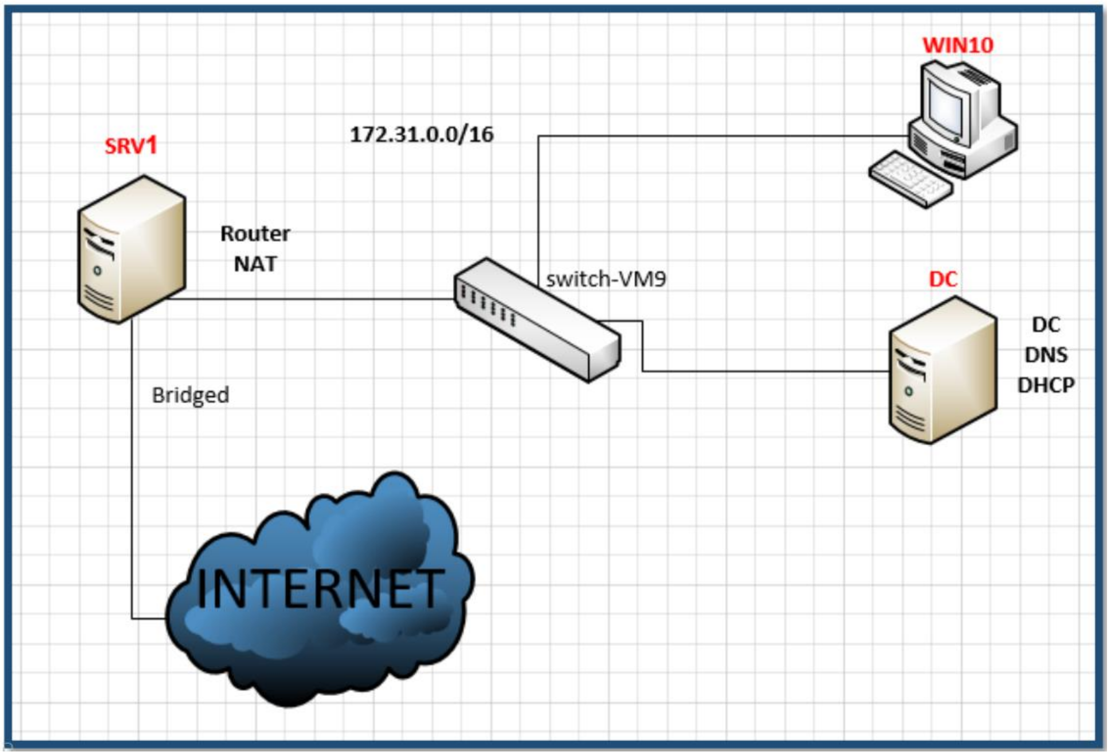
This project shows the steps of the production and configuration of devices, in a local area network (LAN) in a Microsoft environment, which contains three devices, the devices in the network are:

1. **DC** - Windows server Active directory with domain controller, DHCP and DNS.

2. **SRV1** - Windows server which functioning as a router with NAT.

3. **WIN10** - client computer on the LAN.

Here is a diagram that shows the network (the switch is not included in this project)



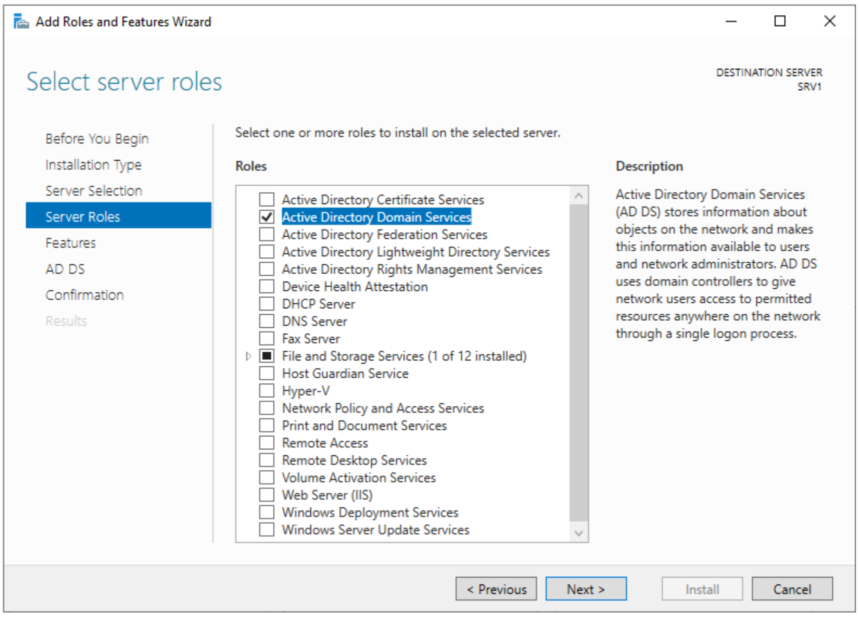
Definitions:

- **Active directory:** Active Directory is a suite of utilities developed by Microsoft for managing networks in organizations. The package includes services such as: directory services based on the LDAP protocol, Authentication services based on Kerberos protocol, DNS services, and Group Policy enforcement on computers or users in the organization. The Active Directory enables central management of the computer network in organizations.
- **LDAP protocol:** Lightweight Directory Access Protocol is an open communication protocol at the application layer, which allows access and management of Directory service over IP networks. These services are essential in the construction and management of internal and Internet networks, and they enable sharing of information about users, systems, networks and services in the network.
- **Kerberos protocol:** It is an authentication protocol, which allows server/client based communication applications to securely verify identities' as well as conduct secure communication using secret encryption keys over an open network. Today this protocol is the most common protocol for authentication, integrity and confidentiality of information.
- **Domain controller:** A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft Windows environments (see Domain controller (Windows)), where it is the centerpiece of the Windows Active Directory service.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address, and other related configuration information, such as the subnet mask and default gateway.
- **DNS:** Domain Name System (DNS) is one of the industry-standard suite of protocols that comprise TCP/IP, and together the DNS Client and DNS Server provide computer name-to-IP address mapping name resolution services to computers and users.
- **NAT:** Network address translation (NAT) is a method of mapping an IP address space into another, by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

Stage 1: Setting up Domain Controller and Active Directory:

Install Active Directory Domain Services and DNS. The DNS is automatically installed with the Active Directory.

Manage ->Add Roles and Features Wizard -> Role-based or Feature-based installation -> Select server roles -> Active Directory Domain Services



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SRV1

Select one or more roles to install on the selected server.

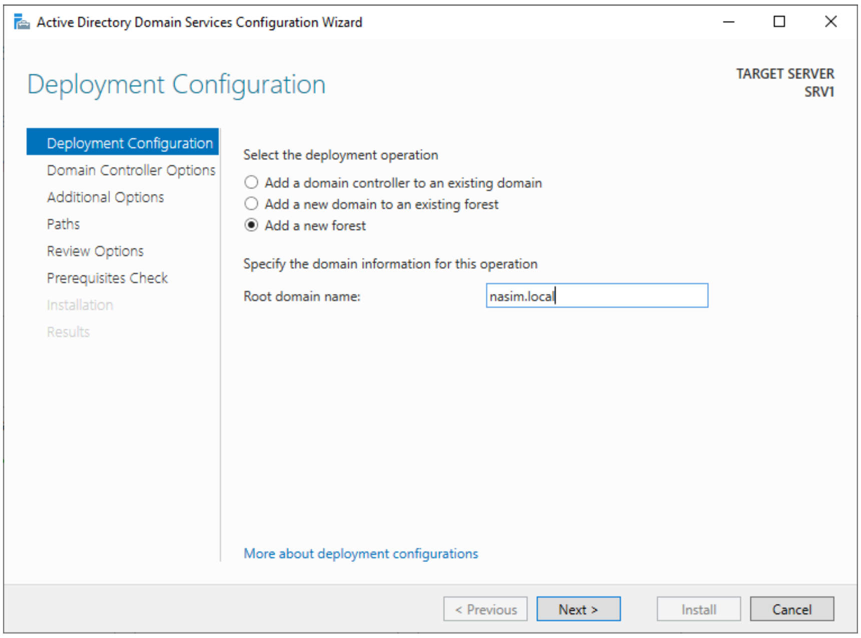
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

->Promote this server to a domain controller (this will install also the DNS).



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SRV1

Select the deployment operation

- ○ Add a domain controller to an existing domain
- ○ Add a new domain to an existing forest
- ● Add a new forest

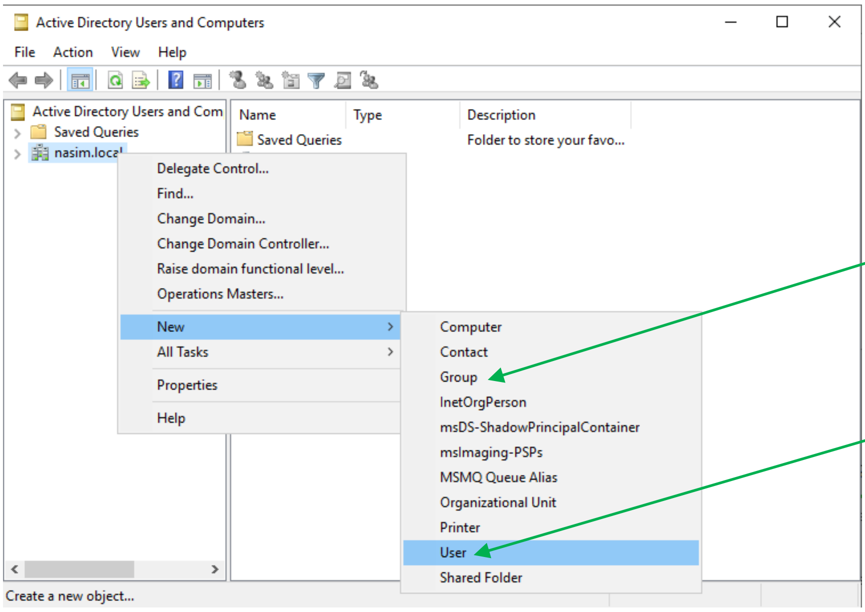
Specify the domain information for this operation

Root domain name: nasim.local

Create two organizational units (OU), one for the Sales department and the other for the SysAdmin department.

I created two users named USER3 and USER4 and a group named sysadmin; I added the users to the group and added the group as a member of the domain admins group.

Tools -> Active Directory Users and Groups

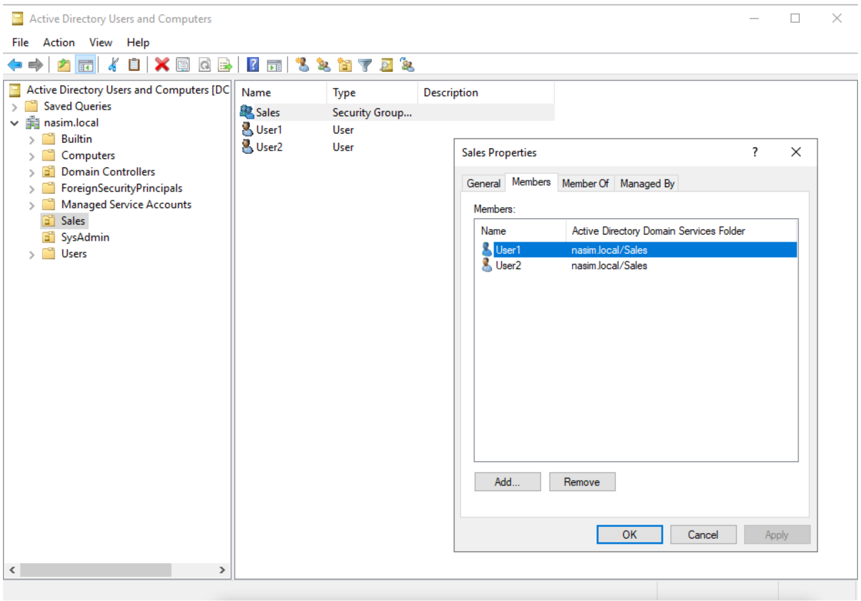


Name	Type	Description
Saved Queries		Folder to store your favo...

Select the Group option to create a new group.

Select the User option to create a new user.

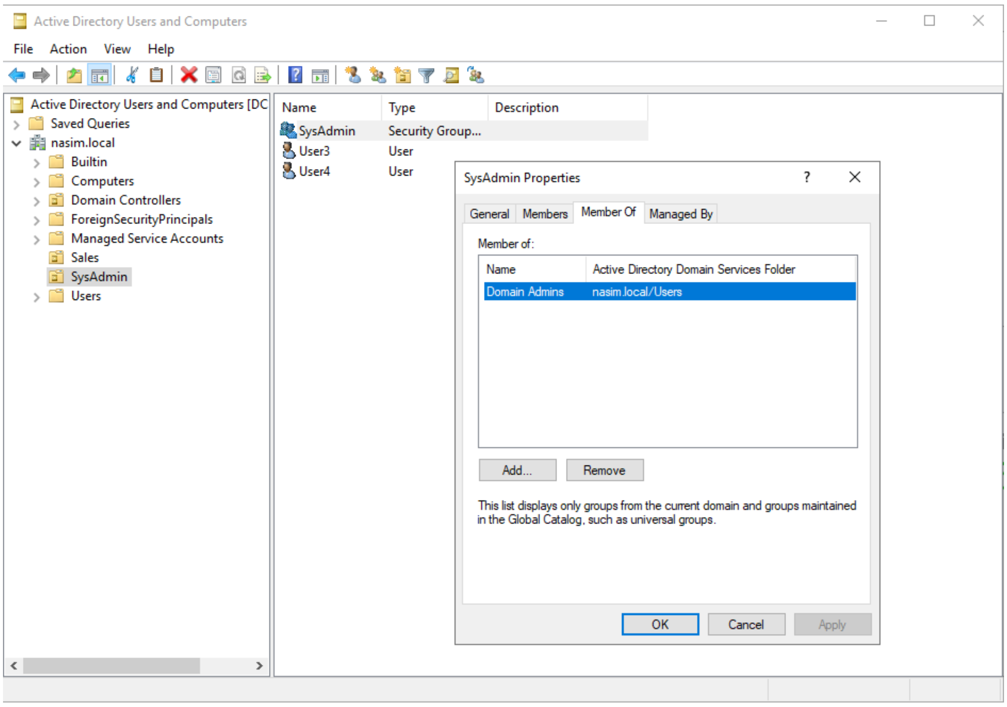
The Sales group:



Name	Type	Description
Sales	Security Group...	
User1	User	
User2	User	

Name	Active Directory Domain Services Folder
User1	nasim.local/Sales
User2	nasim.local/Sales

The SysAdmin group member of the domain admins group .



- Active Directory Users and Computers [DC
  - Saved Queries
  - nasim.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Sales
    - SysAdmin
    - Users

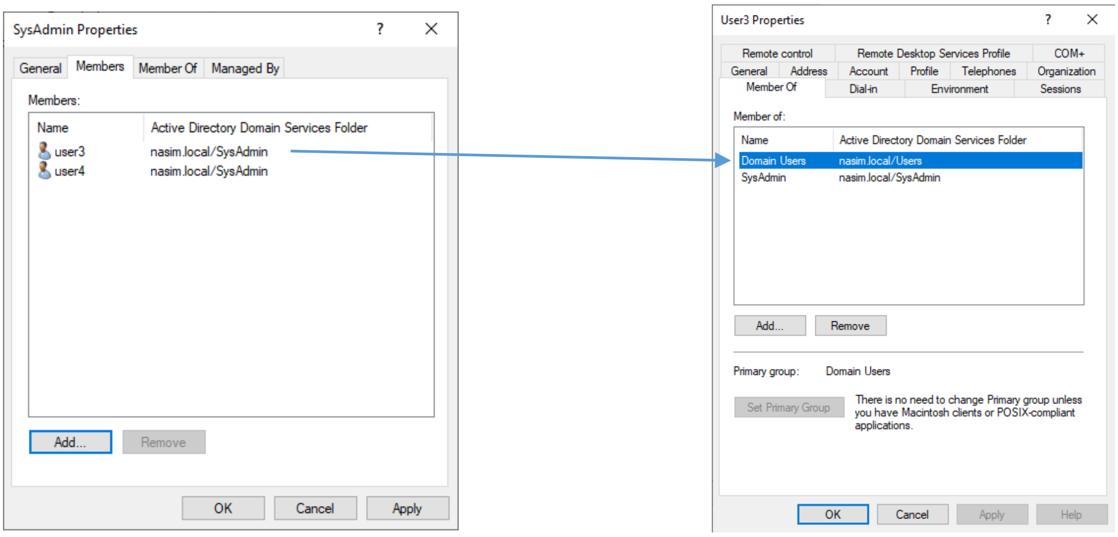
Name	Type	Description
SysAdmin	Security Group...	
User3	User	
User4	User	

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	nasim.local/Users

This list displays only groups from the current domain and groups maintained in the Global Catalog, such as universal groups.

Each SysAdmin group member will also be a member of the domain controller group, because the group is member of the domain controller.



Members:

Name	Active Directory Domain Services Folder
user3	nasim.local/SysAdmin
user4	nasim.local/SysAdmin

Member of:

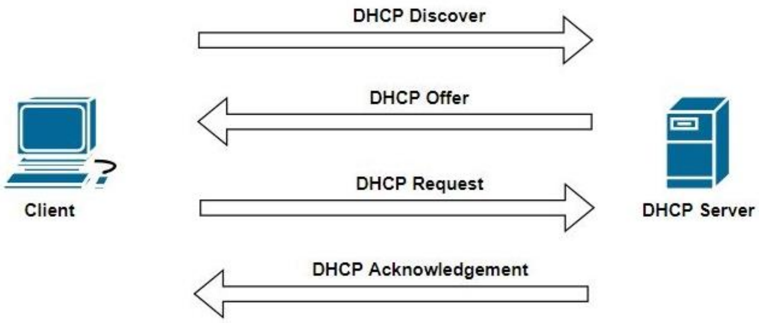
Name	Active Directory Domain Services Folder
Domain Users	nasim.local/Users
SysAdmin	nasim.local/SysAdmin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Stage 2: Setting up the DHCP server

The process of obtaining an IP address from a DHCP server includes four steps called DORA



Step 1: DHCP Discover Message: DHCP client will find the server by sending DHCP discover message.

Step 2: DHCP Offer Message: DHCP server receives the discover message and it replays the DHCP client with the DHCP offer request. The server sends a DHCP offer message with filled information. It has information about the IP address and duration of time that a host can use.

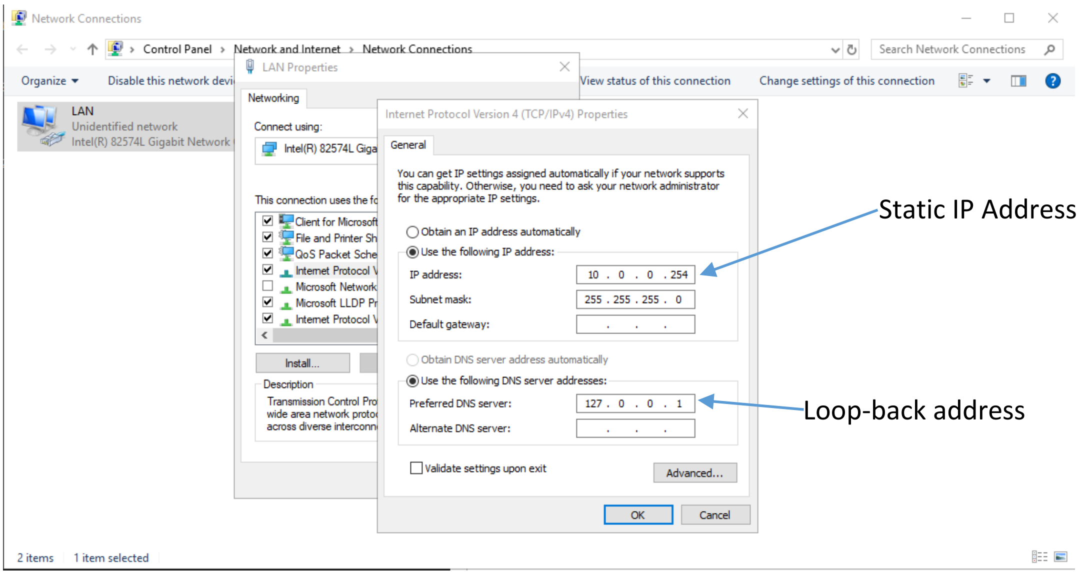
Step 3: DHCP Request Message: DHCP clients send the request message to the server when it receives a DHCP offer message from the server. This message tells the server that it accepts the IP address given by the server.

Step 4: DHCP Acknowledge Message: This is the last step or message in the DORA process. The DHCP server sends Acknowledge Message to the client when it receives the request message from the DHCP client. This message will contain the IP address and subnet mask that the server assigns to the client. Source IP address will be the IP address of the server.

In order to configure a DHCP server, you should give the DC server a static IP address

ncpa.cpl -> Network Connections -> LAN properties -> Internet Protocol Version 4 (TCP/IPv4)

I set the DC's IP to 10.0.0.254, the subnet to 255.255.255.0 and the preferred DNS server to the loop-back address 127.0.0.1 (which is DC itself, it's the same as setting it to 10.0.0.254)



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 254

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

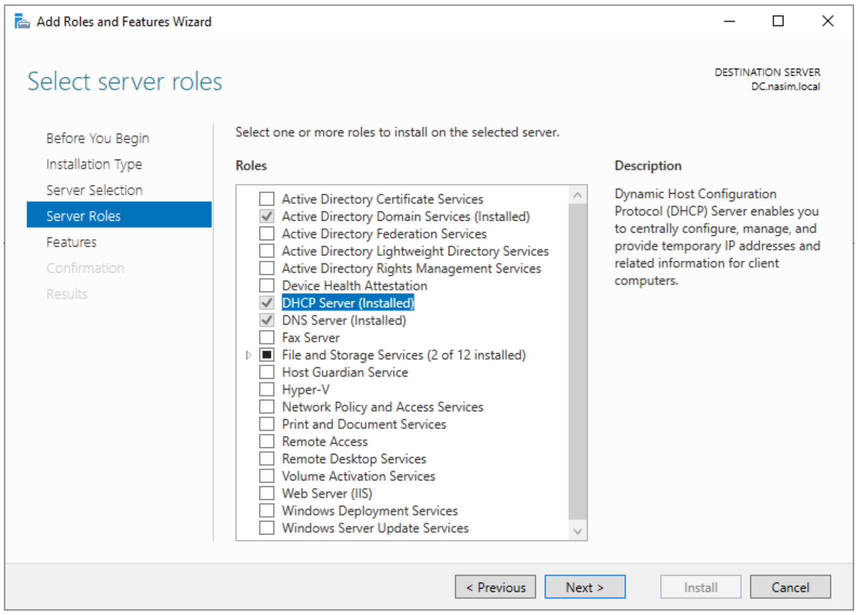
☐ Validate settings upon exit

Static IP Address

Loop-back address

Setup DHCP Server:

Manage ->Add Roles and Features Wizard -> Role-based or Feature-based installation -> Select server roles -> DHCP Server



Select server roles

DESTINATION SERVER
DC.nasim.local

Select one or more roles to install on the selected server.

Roles

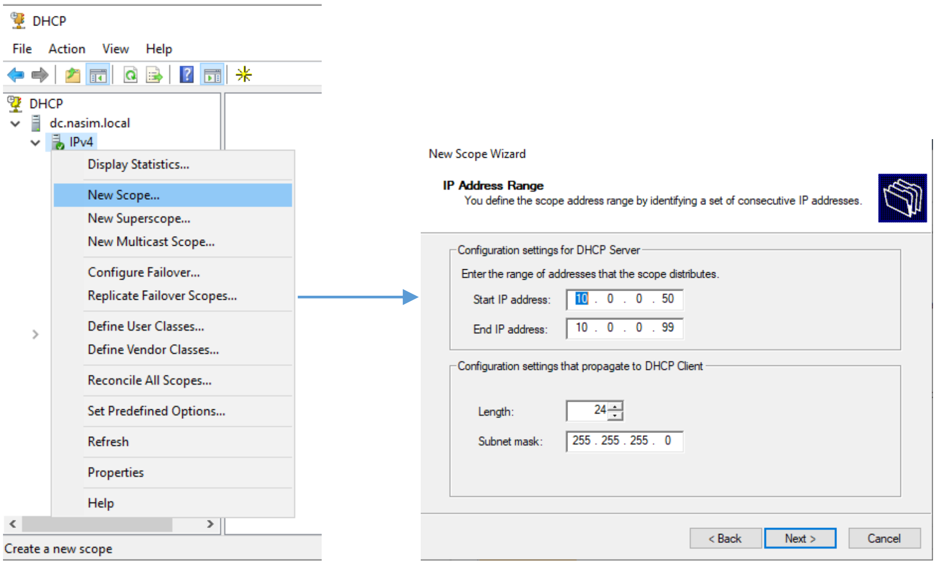
☐ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☑ DHCP Server (Installed)
☑ DNS Server (Installed)
☐ Fax Server
■ File and Storage Services (2 of 12 installed)
☐ Host Guardian Service
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

DHCP SERVER configuration:

Each DHCP must have a scope, scope is a consecutive range of IP addresses that a DHCP server can draw on to fulfill an IP address request from a DHCP client. By defining one or more scopes on your DHCP server, the server can manage the distribution and assignment of IP addresses to DHCP clients. I defined scope from address 10.0.0.50 – 10.0.0.99 (50 addresses)



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 0 . 0 . 50

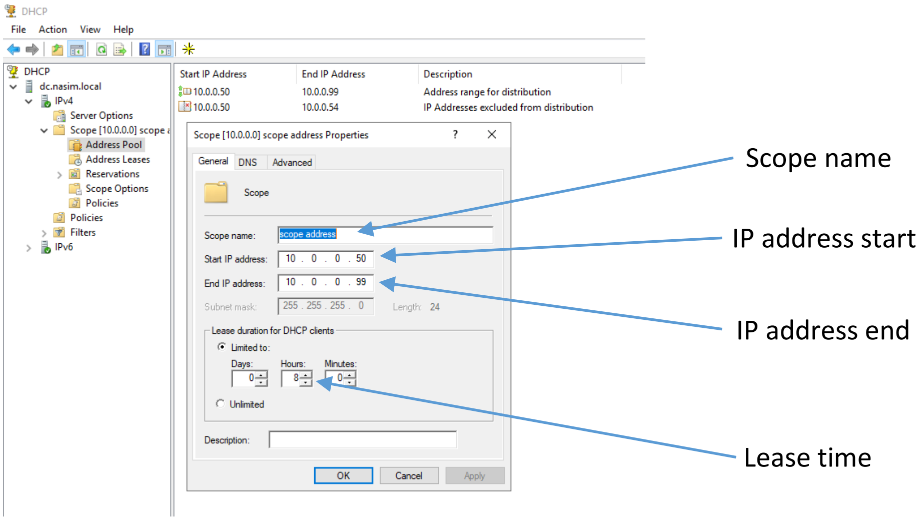
End IP address: 10 . 0 . 0 . 99

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

During the scope creation, I have also defined lease time, router, DNS, and the domain.



Start IP Address	End IP Address	Description
10.0.0.50	10.0.0.99	Address range for distribution
10.0.0.50	10.0.0.54	IP Addresses excluded from distribution

Scope [10.0.0.0] scope address Properties

Scope name: scope address

Start IP address: 10 . 0 . 0 . 50

End IP address: 10 . 0 . 0 . 99

Subnet mask: 255 . 255 . 255 . 0 Length: 24

Lease duration for DHCP clients

● Limited to:

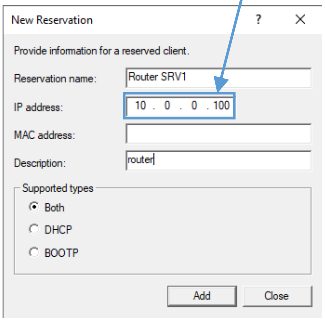
Days: 0 Hours: 8 Minutes: 0

○ Unlimited

Description:

Lease time: The DHCP-assigned IP address is not permanent and expires in a predetermined time. This is called DHCP lease time. The biggest advantage with DHCP lease time is that the same IP address is not stuck to a device forever and is available for other devices too, when needed. I have set the lease time to 8 hours.

In addition, I did IP reservation for SRV1 cause it is router.



New Reservation

Provide information for a reserved client.

Reservation name: Router SRV1

IP address: 10 . 0 . 0 . 100

MAC address:

Description: router

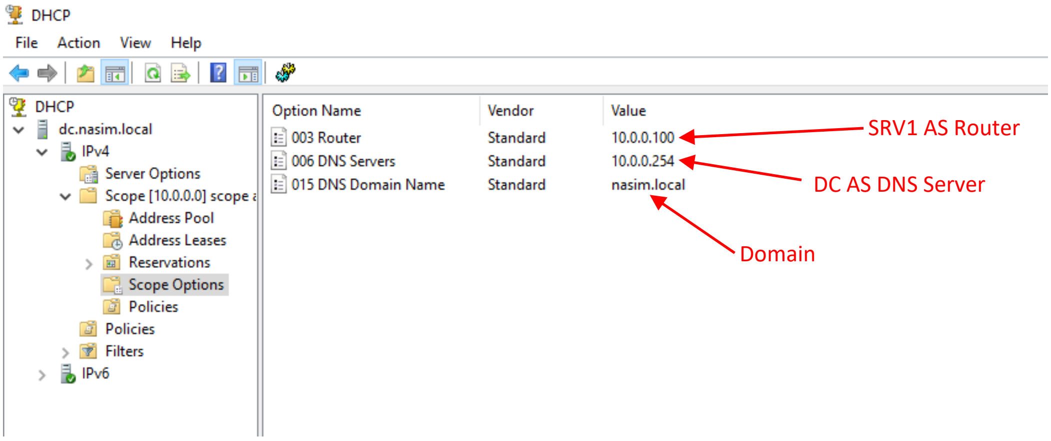
Supported types

● Both

○ DHCP

○ BOOTP

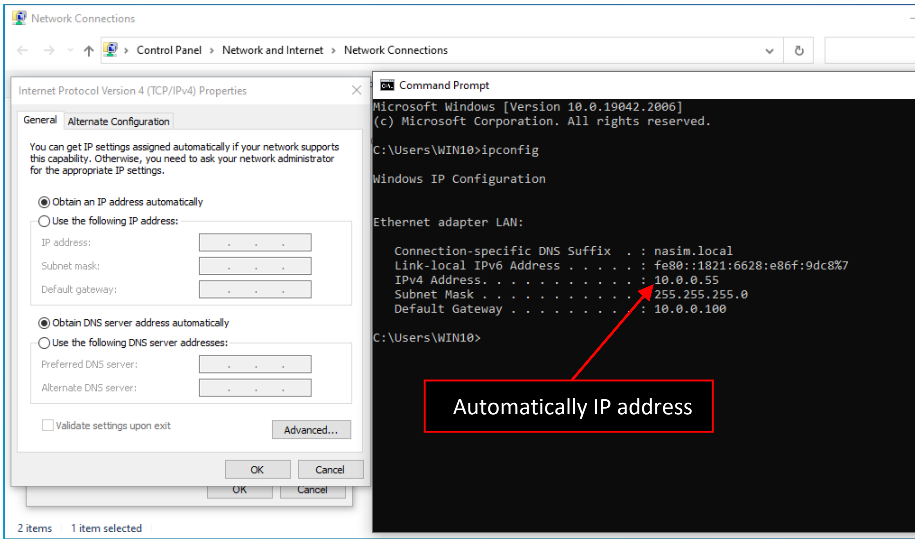
Scope options:



Option Name	Vendor	Value
003 Router	Standard	10.0.0.100
006 DNS Servers	Standard	10.0.0.254
015 DNS Domain Name	Standard	nasim.local

Now we need to do some checks:

Client (WIN10) get automatically IP address from DHCP and SRV1 get the reserved IP:



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

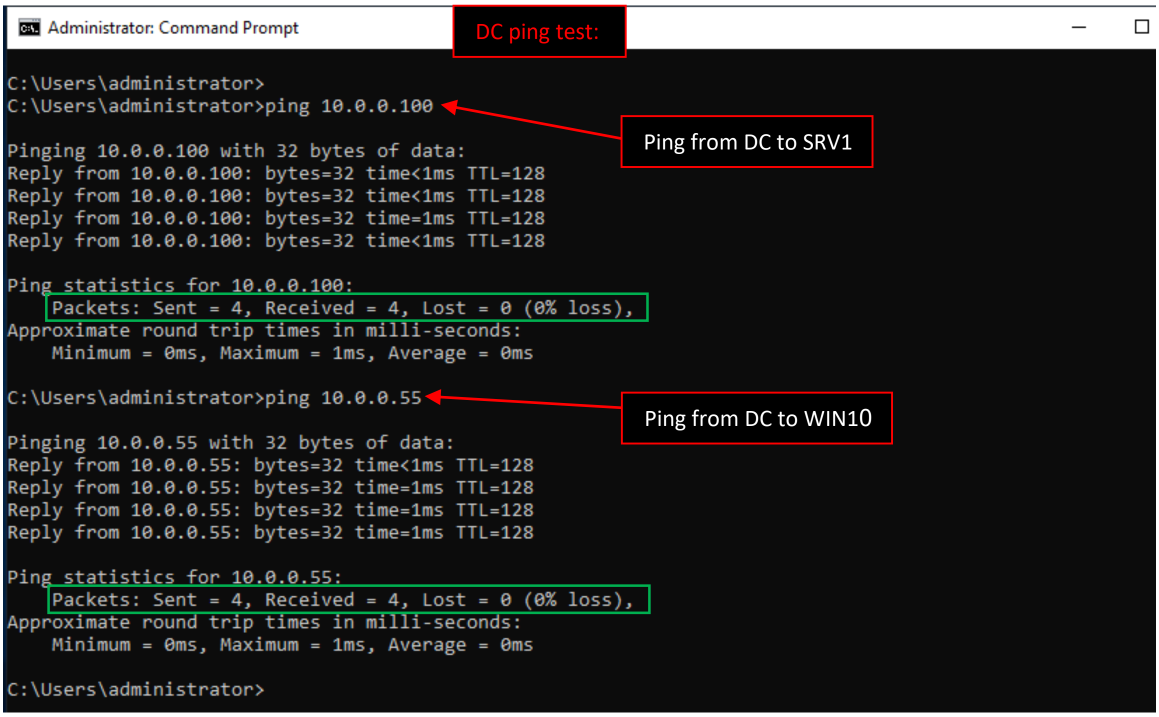
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

```
Microsoft Windows [Version 10.0.19042.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\WIN10>ipconfig

Windows IP Configuration


Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : nasim.local
   Link-local IPv6 Address . . . . . : fe80::1821:6628:e86f:9dc8%7
   IPv4 Address. . . . . . . . . . . : 10.0.0.55
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.100

C:\Users\WIN10>
```

Connectivity between all the devices, and communication from SRV1 to the Internet. Therefore, we will perform ping command tests between the devices and ping from SRV1 to the Internet.

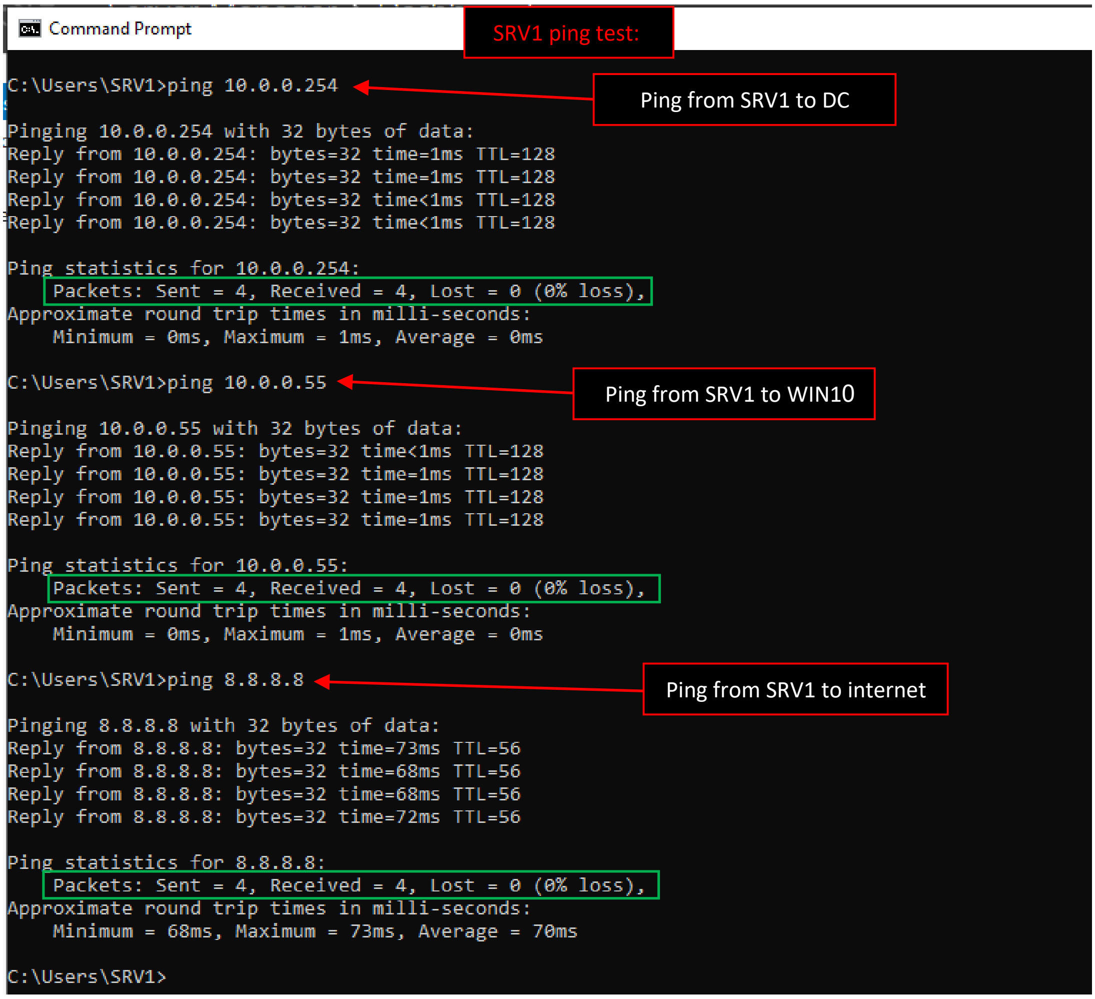


DC ping test:

Ping from DC to SRV1

Ping from DC to WIN10

```
C:\Users\administrator>
C:\Users\administrator>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time<1ms TTL=128
Reply from 10.0.0.100: bytes=32 time<1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=1ms TTL=128
Reply from 10.0.0.100: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\administrator>ping 10.0.0.55

Pinging 10.0.0.55 with 32 bytes of data:
Reply from 10.0.0.55: bytes=32 time<1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\administrator>
```



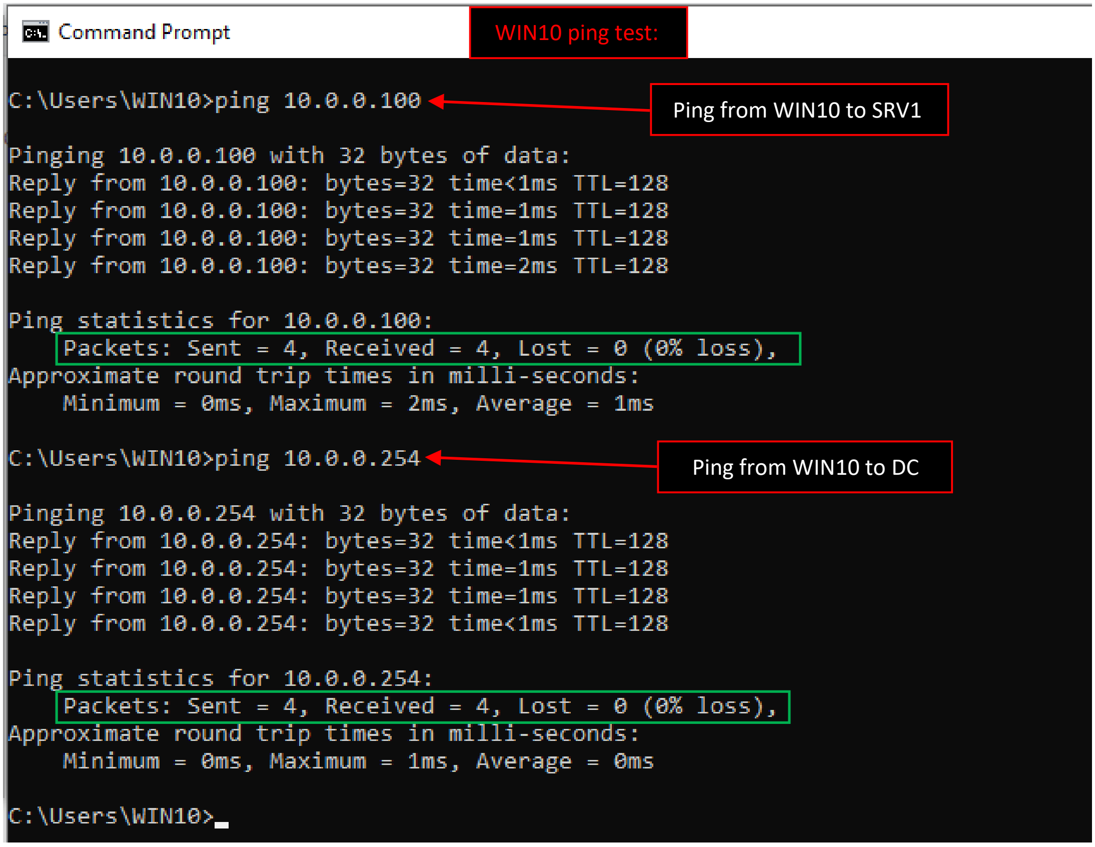
SRV1 ping test:

Ping from SRV1 to DC

Ping from SRV1 to WIN10

Ping from SRV1 to internet

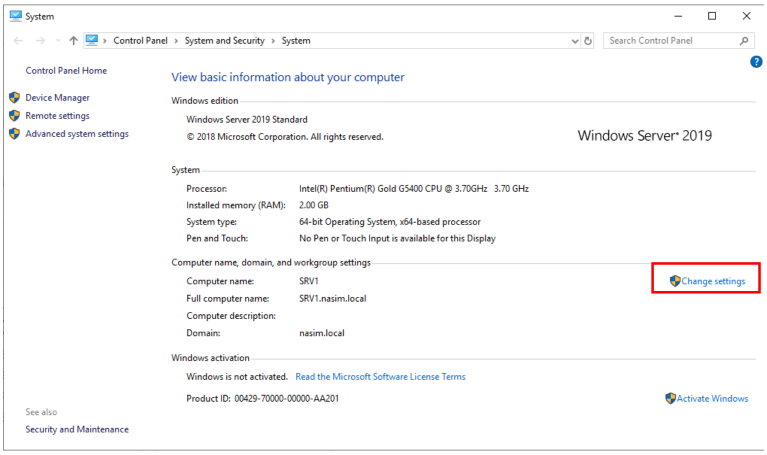
```
C:\Users\SRV1>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:
Reply from 10.0.0.254: bytes=32 time=1ms TTL=128
Reply from 10.0.0.254: bytes=32 time=1ms TTL=128
Reply from 10.0.0.254: bytes=32 time<1ms TTL=128
Reply from 10.0.0.254: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\SRV1>ping 10.0.0.55

Pinging 10.0.0.55 with 32 bytes of data:
Reply from 10.0.0.55: bytes=32 time<1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128
Reply from 10.0.0.55: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\SRV1>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=73ms TTL=56
Reply from 8.8.8.8: bytes=32 time=68ms TTL=56
Reply from 8.8.8.8: bytes=32 time=68ms TTL=56
Reply from 8.8.8.8: bytes=32 time=72ms TTL=56

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 73ms, Average = 70ms

C:\Users\SRV1>
```



```
C:\Users\WIN10>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time<1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=2ms TTL=128

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\WIN10>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:
Reply from 10.0.0.254: bytes=32 time<1ms TTL=128
Reply from 10.0.0.254: bytes=32 time=1ms TTL=128
Reply from 10.0.0.254: bytes=32 time=1ms TTL=128
Reply from 10.0.0.254: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\WIN10>_
```

Stage 3: Join devices to domain

File Explorer-> properities -> Control Panel -> System and Security -> System



View basic information about your computer

Windows edition

Windows Server 2019 Standard

© 2018 Microsoft Corporation. All rights reserved.

Windows Server® 2019

System

Processor: Intel(R) Pentium(R) Gold G5400 CPU @ 3.70GHz 3.70 GHz

Installed memory (RAM): 2.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: SRV1

Full computer name: SRV1.nasim.local

Computer description:

Domain: nasim.local

Change settings

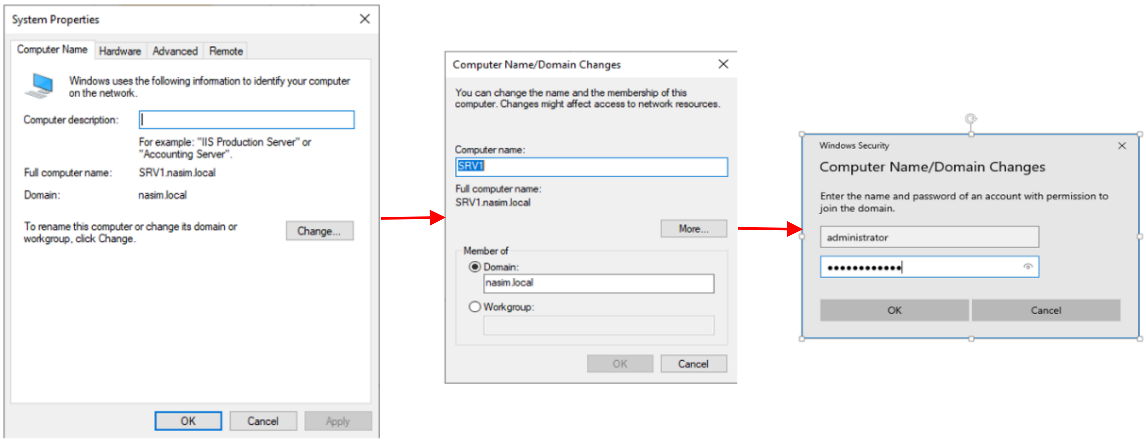
Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00429-70000-00000-AA201

Activate Windows

In order to join domain you need to have domain permissions (enter domain valid Name and password)



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: SRV1.nasim.local

Domain: nasim.local

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: SRV1

Full computer name: SRV1.nasim.local

Member of

● Domain: nasim.local

○ Workgroup:

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

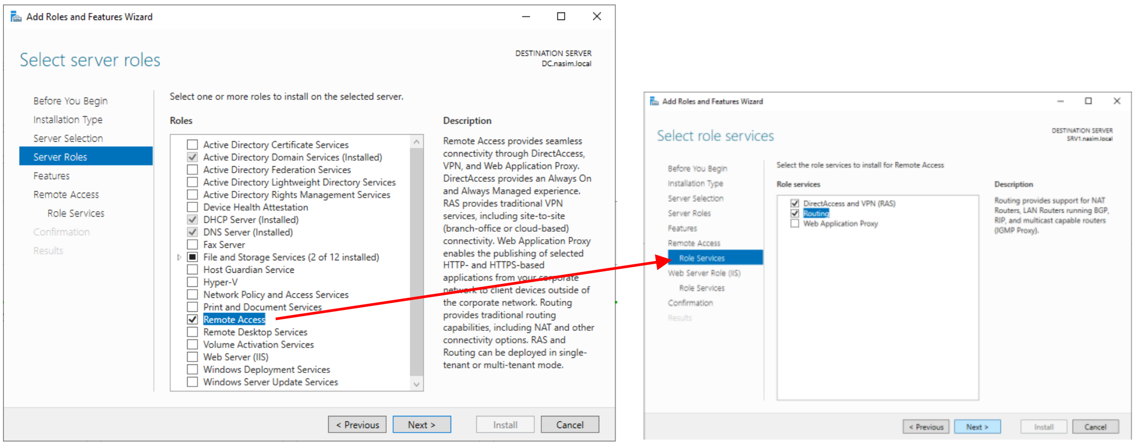
administrator

••••••••••••

Stage 4: Configuring routing and PAT:

Add remote access to SRV1

Manage ->Add Roles and Features Wizard -> Role-based or Feature-based installation -> Select server roles -> Remote Access



Select server roles

DESTINATION SERVER
DC.nasim.local

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- ☑ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

Select role services

DESTINATION SERVER
SRV1.nasim.local

Select the role services to install for Remote Access

Role services

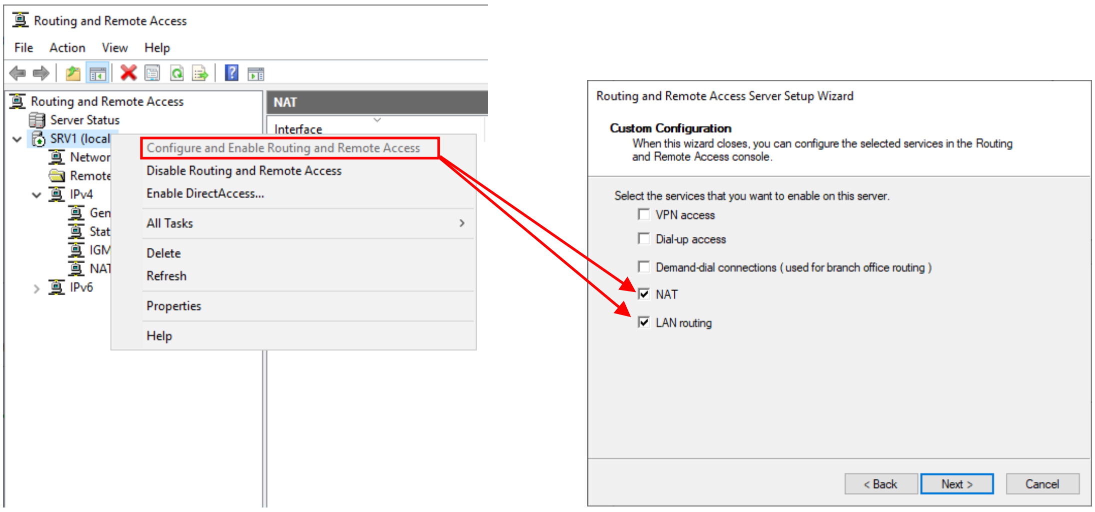
- ☑ DirectAccess and VPN (RAS)
- ☑ Routing
- □ Web Application Proxy

Description

Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).

Configure the NAT: The service must be activated.

Tools -> Routing and Remote Access -> configure and Enable Routing and Remote Access



Routing and Remote Access Server Setup Wizard

Custom Configuration

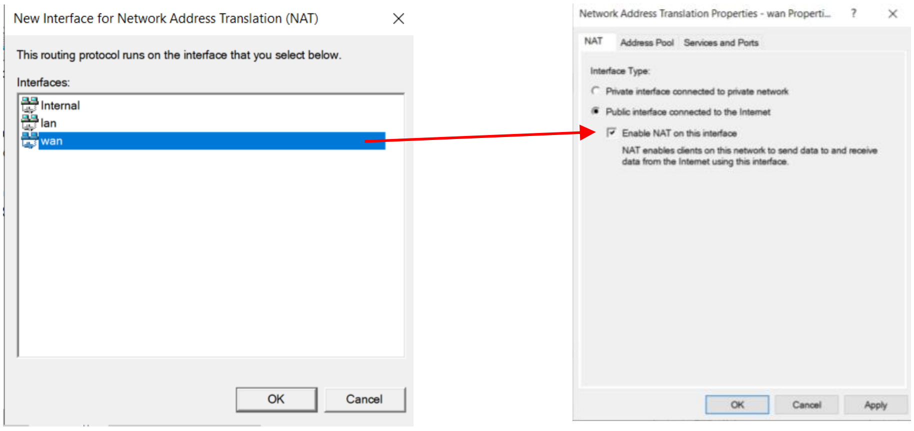
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

- □ VPN access
- □ Dial-up access
- □ Demand-dial connections (used for branch office routing)
- ☑ NAT
- ☑ LAN routing

IPv4 -> NAT ->New Interface -> WAN

Selected WAN as the interface for the NAT service to be connected to.



New Interface for Network Address Translation (NAT)

This routing protocol runs on the interface that you select below.

Interfaces:

Internal
lan
wan

Network Address Translation Properties - wan Properti...

Interface Type:

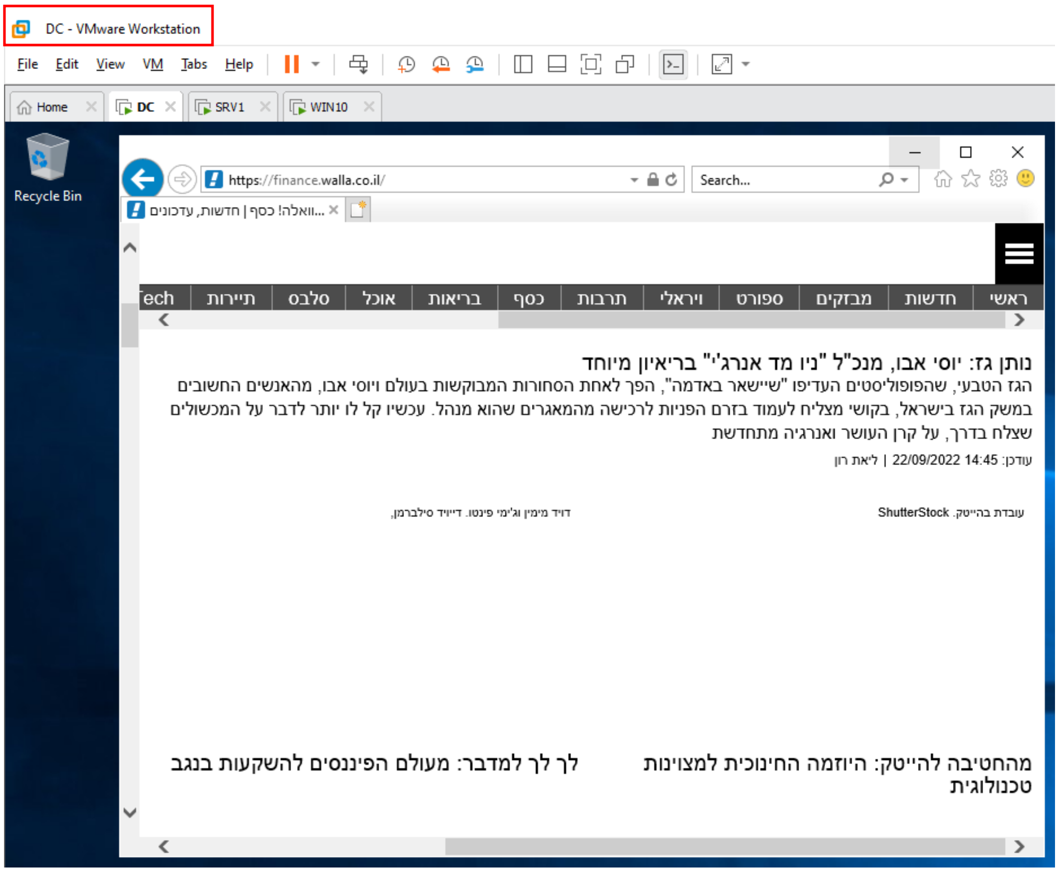
○ Private interface connected to private network

● Public interface connected to the Internet

☑ Enable NAT on this interface

NAT enables clients on this network to send data to and receive data from the Internet using this interface.

Although WAN is not connected, there is a connectivity to the Internet through SRV1 in both WIN10 and DC



DC - VMware Workstation

https://finance.walla.co.il/

וואלה! כסף | חדשות, עדכונים...

נותן גז: יוסי אבו, מנכ"ל "ניו מד אנרג'י" בריאיון מיוחד

הגז הטבעי, שהפופוליסטים העדיפו "שיישאר באדמה", הפך לאחת הסחורות המבוקשות בעולם ויוסי אבו, מהאנשים החשובים במשק הגז בישראל, בקושי מצליח לעמוד בזרם הפניות לרכישה מהמאגרים שהוא מנהל. עכשיו קל לו יותר לדבר על המכשולים שצלח בדרך, על קרן העושר ואנרגיה מתחדשת

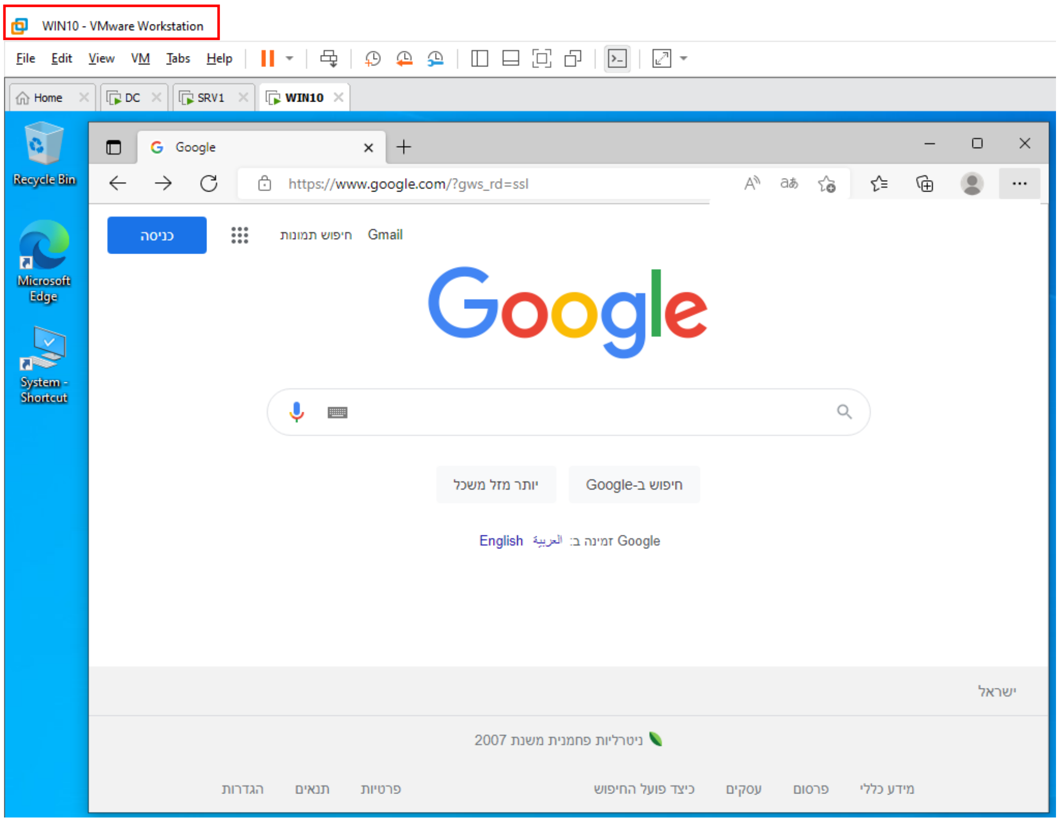
עודכן: 22/09/2022 14:45 | ליאת רון

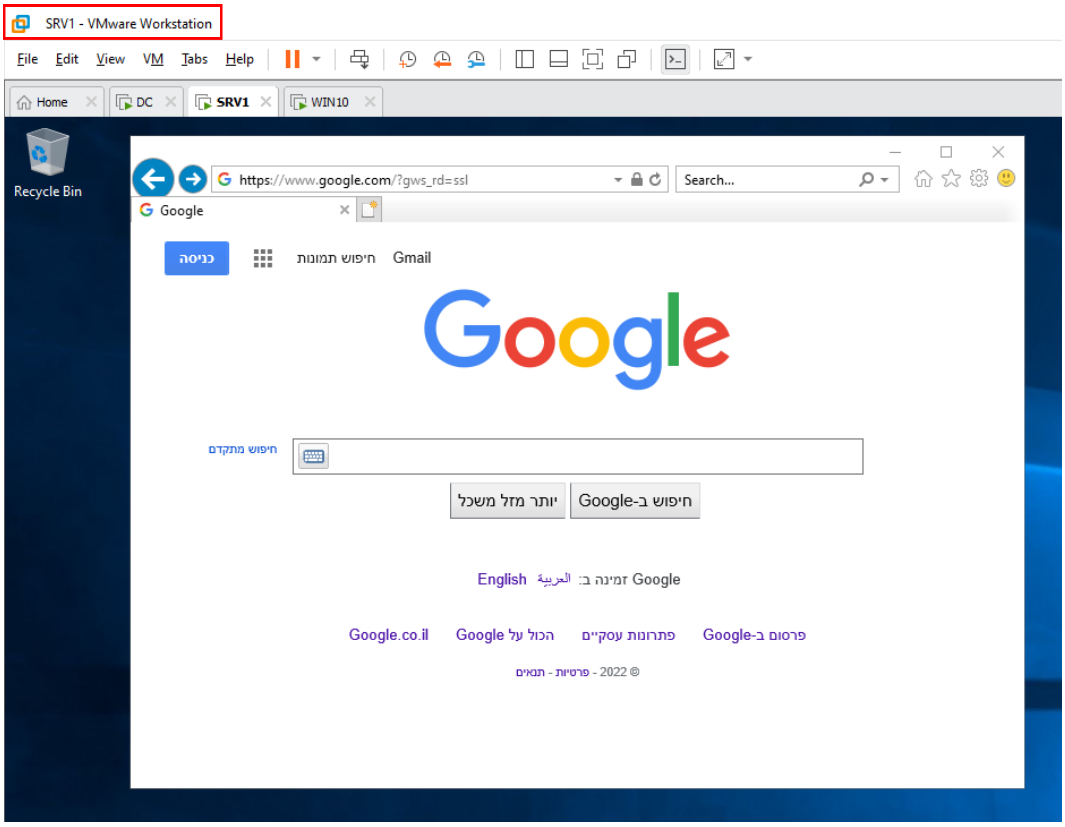
עובדת בהייטק. ShutterStock

דויד מימין וג'ימי פינטו. דייויד סילברמן,

מהחטיבה להייטק: היוזמה החינוכית למצוינות טכנולוגית

לך לך למדבר: מעולם הפיננסים להשקעות בנגב

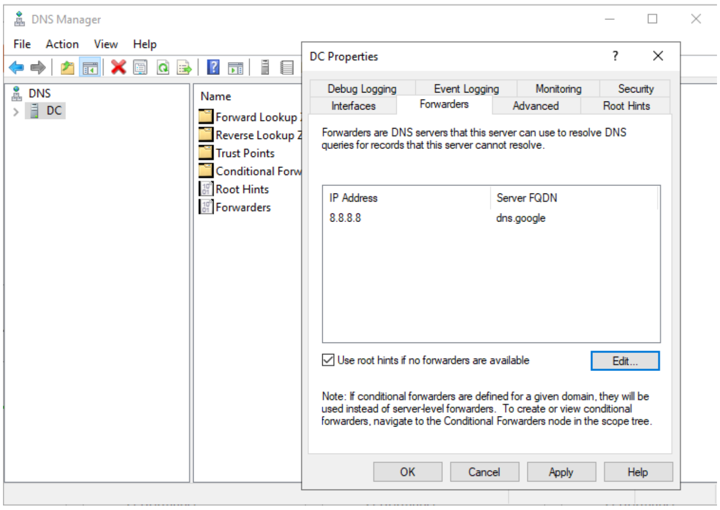

WIN10 - VMware Workstation
File Edit View VM Tabs Help
Home
DC
SRV1
WIN10
Recycle Bin
Microsoft Edge
System - Shortcut
Google
https://www.google.com/?gws_rd=ssl
כניסה
חיפוש תמונות
Gmail
Google
יותר מזל משכל
חיפוש ב-Google
Google זמין ב: العربية English
ישראל
ניטרליות פחמנית משנת 2007
הגדרות
תנאים
פרטיות
כיצד פועל החיפוש
עסקים
פרסום
מידע כללי


SRV1 - VMware Workstation
File Edit View VM Tabs Help
Home
DC
SRV1
WIN10
Recycle Bin
https://www.google.com/?gws_rd=ssl
Search...
Google
כניסה
חיפוש תמונות
Gmail
Google
חיפוש מתקדם
יותר מזל משכל
חיפוש ב-Google
Google זמין ב: العربية English
Google.co.il
הכול על Google
פתרונות עסקיים
פרסום ב-Google
© 2022 - פרטיות - תנאים

Stage 5: DNS Definitions:

After we configured all devices to use DC DNS, we set the forwards to 8.8.8.8

Tools -> DNS -> DC -> properties



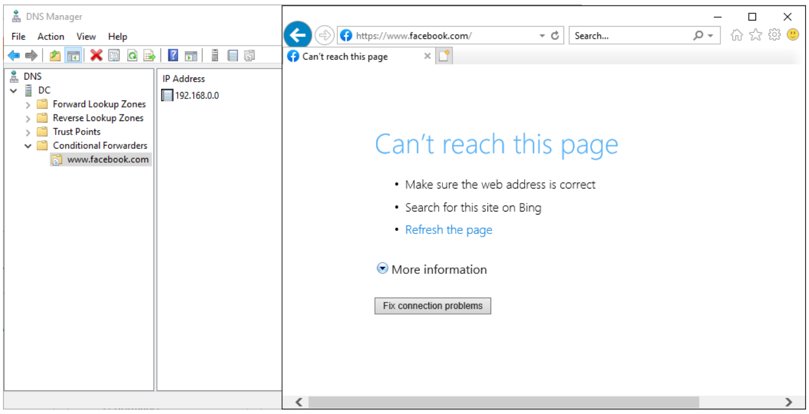
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
8.8.8.8	dns.google

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

Prevent access to the Facebook website:

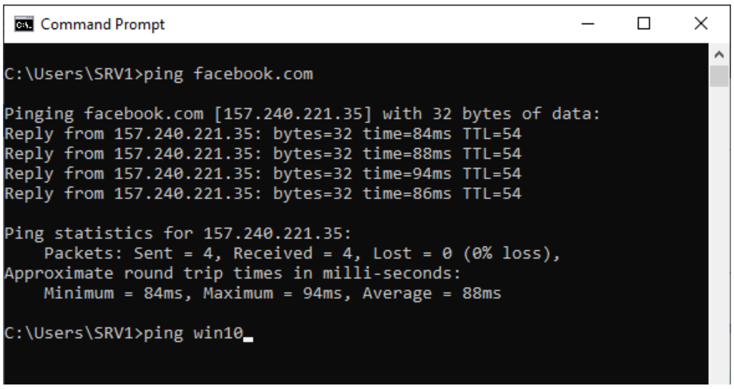


Can't reach this page

- Make sure the web address is correct
- Search for this site on Bing
- Refresh the page

More information

Even though Facebook is blocked, check that it returns a ping:

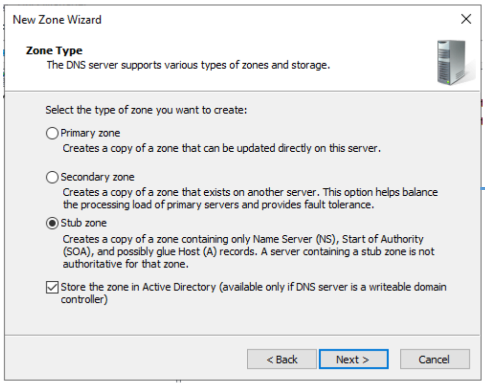


```
C:\Users\SRV1>ping facebook.com

Pinging facebook.com [157.240.221.35] with 32 bytes of data:
Reply from 157.240.221.35: bytes=32 time=84ms TTL=54
Reply from 157.240.221.35: bytes=32 time=88ms TTL=54
Reply from 157.240.221.35: bytes=32 time=94ms TTL=54
Reply from 157.240.221.35: bytes=32 time=86ms TTL=54

Ping statistics for 157.240.221.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 84ms, Maximum = 94ms, Average = 88ms

C:\Users\SRV1>ping win10_
```

<u>Stub Zone:</u> A stub zone is a copy of a Domain Name System (DNS) zone that contains only resource records that identify the DNS servers for that zone.

Stub Zone for google.com:

Tools -> DNS -> Forward Lookup Zone -> New Zone ->



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

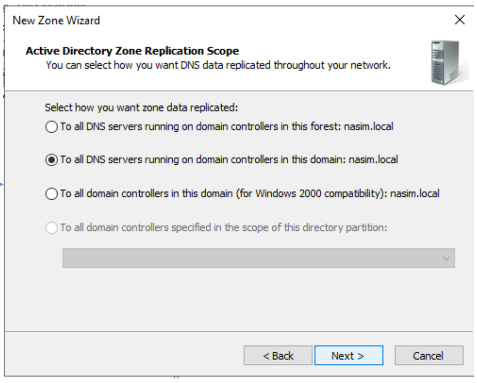
Select the type of zone you want to create:

○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

● Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)



New Zone Wizard

Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

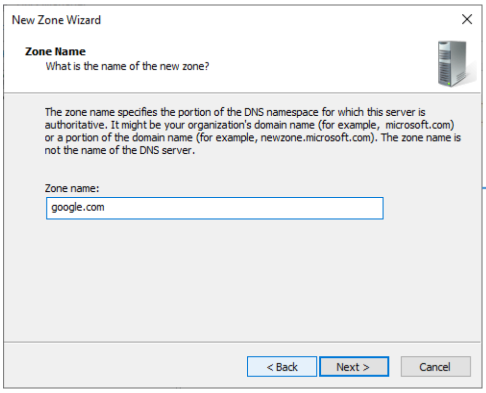
Select how you want zone data replicated:

○ To all DNS servers running on domain controllers in this forest: nasim.local

● To all DNS servers running on domain controllers in this domain: nasim.local

○ To all domain controllers in this domain (for Windows 2000 compatibility): nasim.local

○ To all domain controllers specified in the scope of this directory partition:

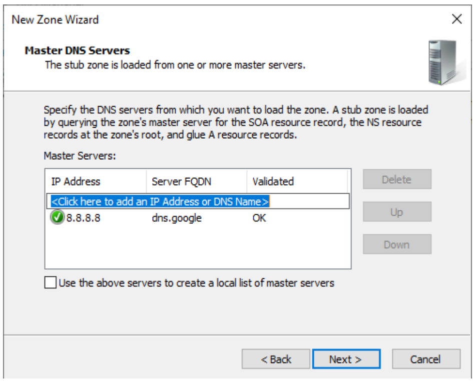


New Zone Wizard

Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:
google.com



New Zone Wizard

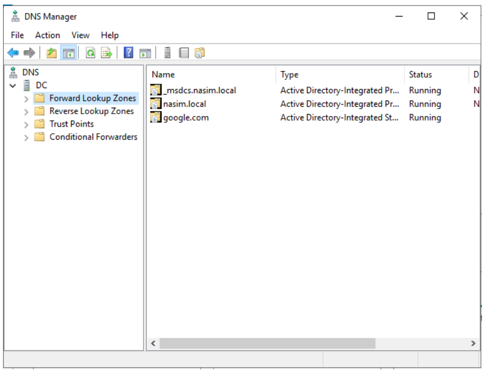
Master DNS Servers
The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

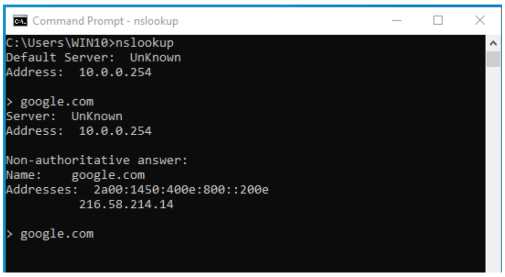
IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✓ 8.8.8.8	dns.google	OK

□ Use the above servers to create a local list of master servers



Name	Type	Status	D
_msdcs.nasim.local	Active Directory-Integrated Pr...	Running	N
nasim.local	Active Directory-Integrated Pr...	Running	N
google.com	Active Directory-Integrated St...	Running	

Open the client station (WIN10), use the NSLOOKUP command and verify that the server is able to translate the address google.com

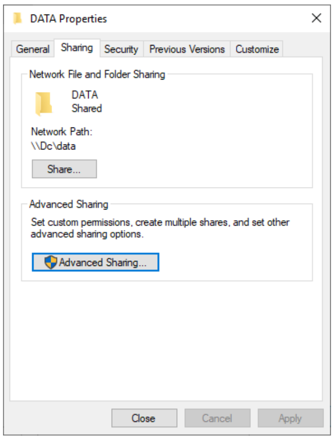


Command Prompt - nslookup

```
C:\Users\WIN10>nslookup
Default Server:  UnKnown
Address:  10.0.0.254

> google.com
Server:  UnKnown
Address:  10.0.0.254

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:400e:800::200e
          216.58.214.14

> google.com
```

Stage 6: Sharing and Mapping

Create shared folder called DATA with permissions



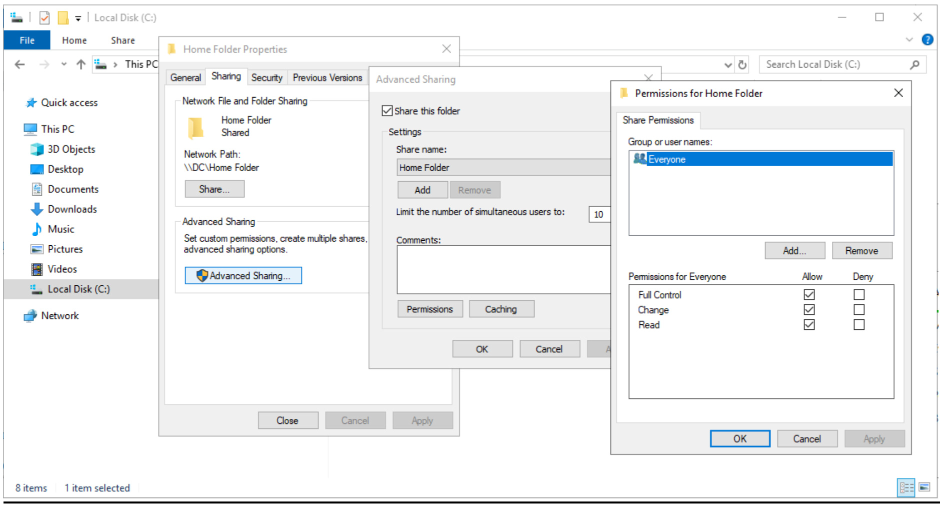
Network File and Folder Sharing

DATA
Shared

Network Path:
\\Dc\data

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.



Network File and Folder Sharing

Home Folder
Shared

Network Path:
\\DC\Home Folder

Advanced Sharing

Set custom permissions, create multiple shares, advanced sharing options.

☑ Share this folder

Settings

Share name:
Home Folder

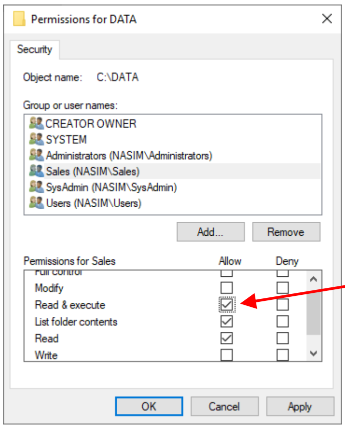
Limit the number of simultaneous users to: 10

Comments:

Group or user names:
Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

The permission for the sale group is Read & execute, the permission for the SysAdmin group is Modify:

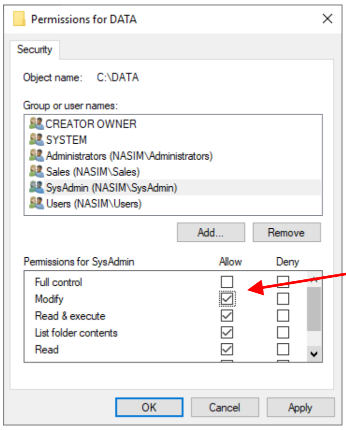


Object name: C:\DATA

Group or user names:
CREATOR OWNER
SYSTEM
Administrators (NASIM\Administrators)
Sales (NASIM\Sales)
SysAdmin (NASIM\SysAdmin)
Users (NASIM\Users)

Permissions for Sales	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	□	□

Sales group



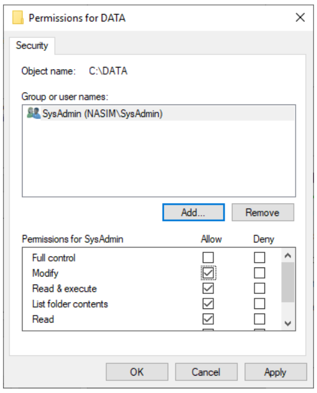
Object name: C:\DATA

Group or user names:
CREATOR OWNER
SYSTEM
Administrators (NASIM\Administrators)
Sales (NASIM\Sales)
SysAdmin (NASIM\SysAdmin)
Users (NASIM\Users)

Permissions for SysAdmin	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

SysAdmin group

Data folder access permissions:



Permissions for DATA

Security

Object name: C:\DATA

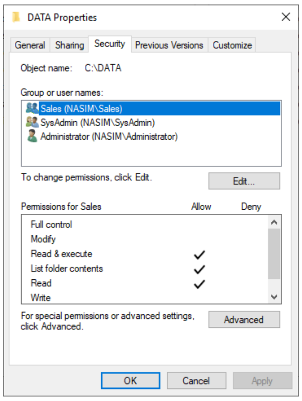
Group or user names:

SysAdmin (NASIM\SysAdmin)

Add... Remove

Permissions for SysAdmin	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

OK Cancel Apply



DATA Properties

General Sharing Security Previous Versions Customize

Object name: C:\DATA

Group or user names:

Sales (NASIM\Sales)
SysAdmin (NASIM\SysAdmin)
Administrator (NASIM\Administrator)

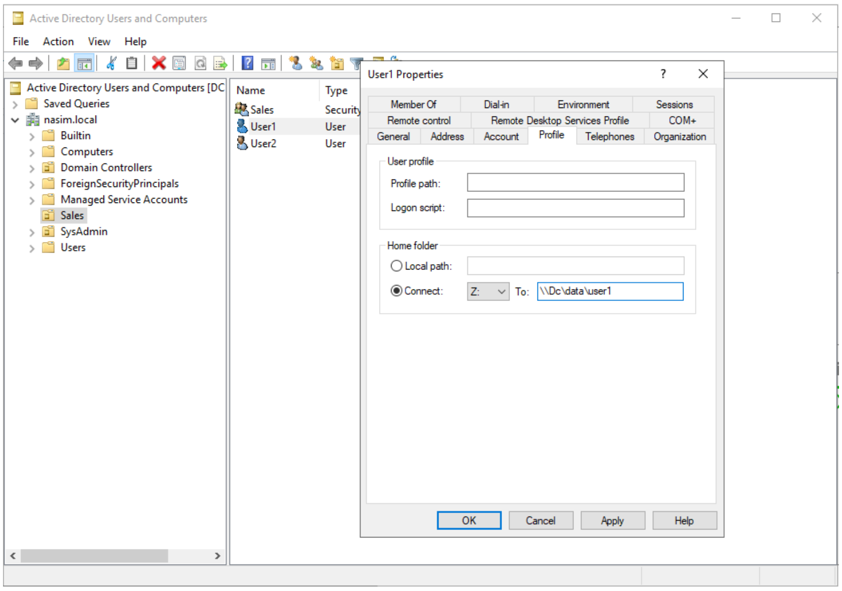
To change permissions, click Edit. Edit...

Permissions for Sales	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

For each user create a folder that only he can access:



Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [DC
Saved Queries
nasim.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Sales
SysAdmin
Users

Name	Type
Sales	Security
User1	User
User2	User

User1 Properties

Member Of Dial-in Environment Sessions
Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization

User profile

Profile path:

Logon script:

Home folder

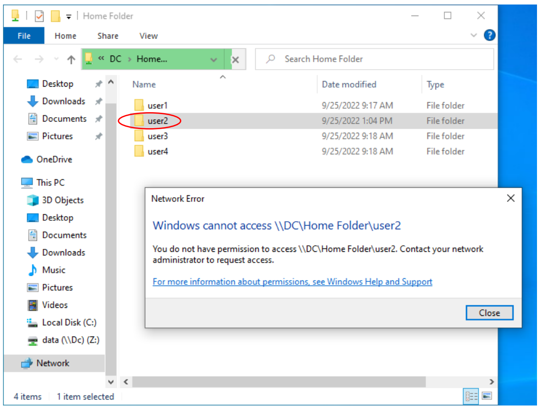
○ Local path:

● Connect: Z: To: \\Dc\data\user1

OK Cancel Apply Help

Each user allowed accessing only his own folder:

For example, user1 try to access the three other folders



Home Folder

File Home Share View

DC › Home...

Search Home Folder

Name	Date modified	Type
user1	9/25/2022 9:17 AM	File folder
user2	9/25/2022 1:04 PM	File folder
user3	9/25/2022 9:18 AM	File folder
user4	9/25/2022 9:18 AM	File folder

Network Error

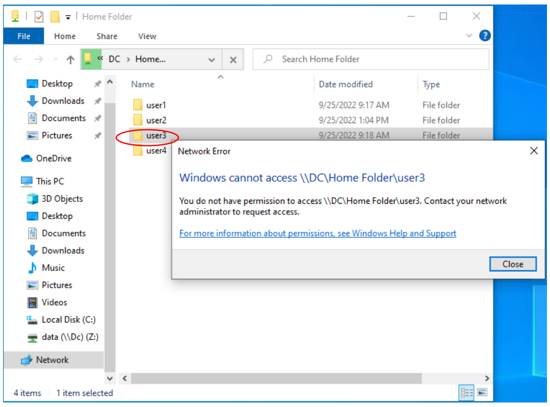
Windows cannot access \\DC\Home Folder\user2

You do not have permission to access \\DC\Home Folder\user2. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

Close

4 items 1 item selected



Home Folder

File Home Share View

DC › Home...

Search Home Folder

Name	Date modified	Type
user1	9/25/2022 9:17 AM	File folder
user2	9/25/2022 1:04 PM	File folder
user3	9/25/2022 9:18 AM	File folder
user4		

Network Error

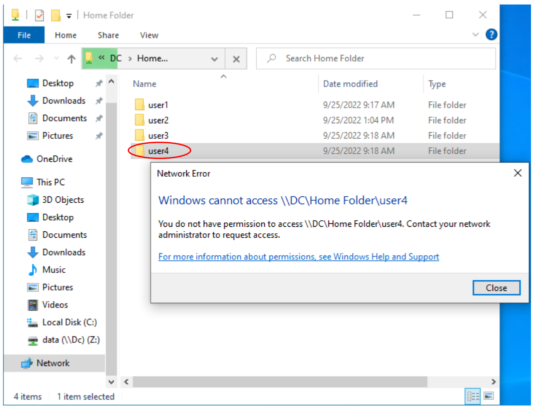
Windows cannot access \\DC\Home Folder\user3

You do not have permission to access \\DC\Home Folder\user3. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

Close

4 items 1 item selected



Name	Date modified	Type
user1	9/25/2022 9:17 AM	File folder
user2	9/25/2022 1:04 PM	File folder
user3	9/25/2022 9:18 AM	File folder
user4	9/25/2022 9:18 AM	File folder

Network Error

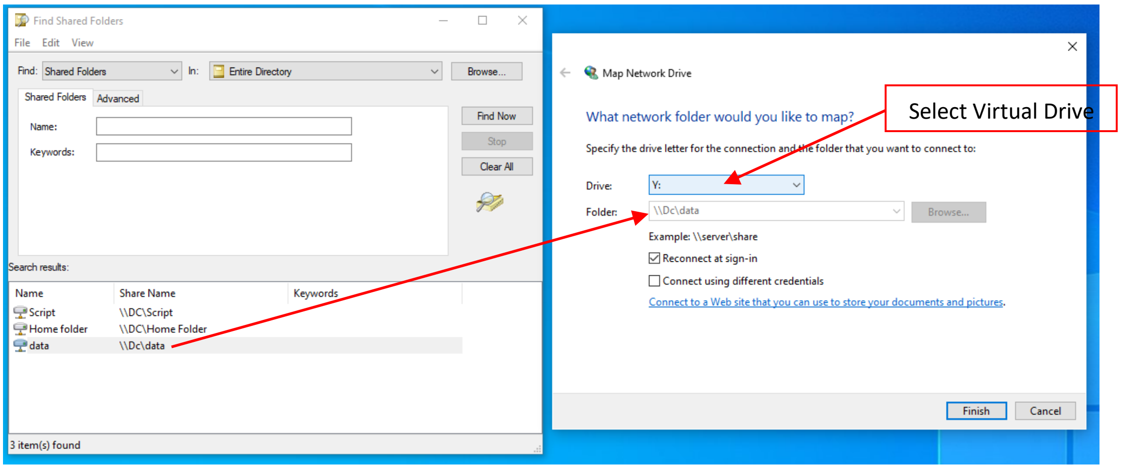
Windows cannot access \\DC\Home Folder\user4

You do not have permission to access \\DC\Home Folder\user4. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

Mapping:

Network ->Search Active Directory ->Fined Shared Folders -> Map Network Drive



Find: Shared Folders In: Entire Directory

Name:

Keywords:

Name	Share Name	Keywords
Script	\\DC\Script	
Home folder	\\DC\Home Folder	
data	\\Dc\data	

3 item(s) found

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

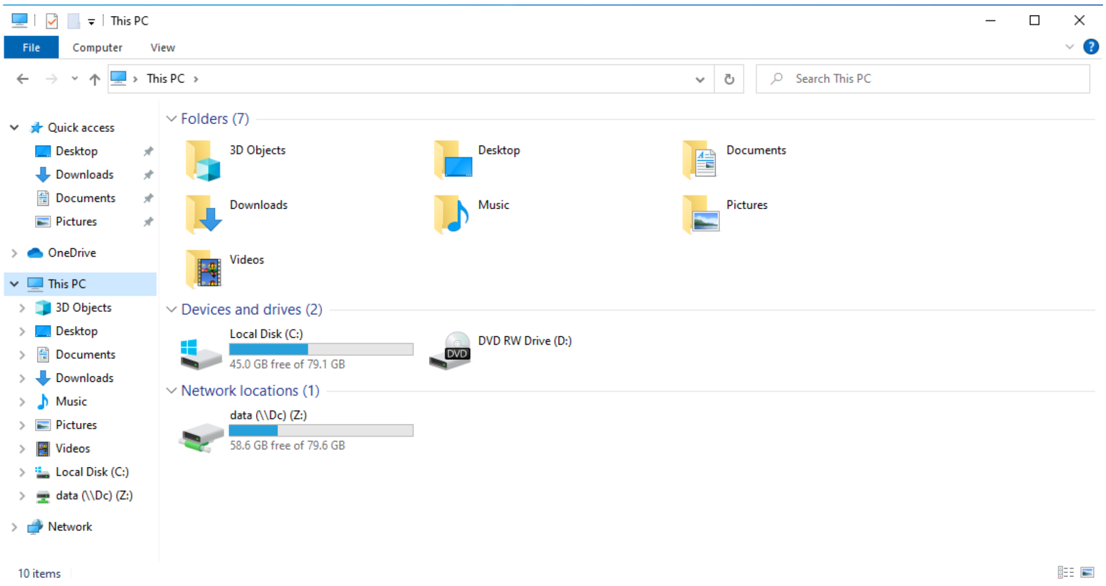
Folder: \\Dc\data

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

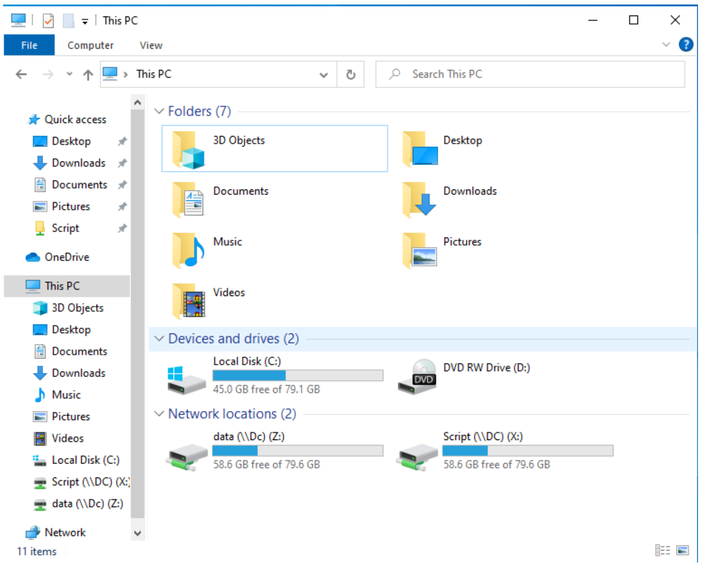


Local Disk (C:) 45.0 GB free of 79.1 GB

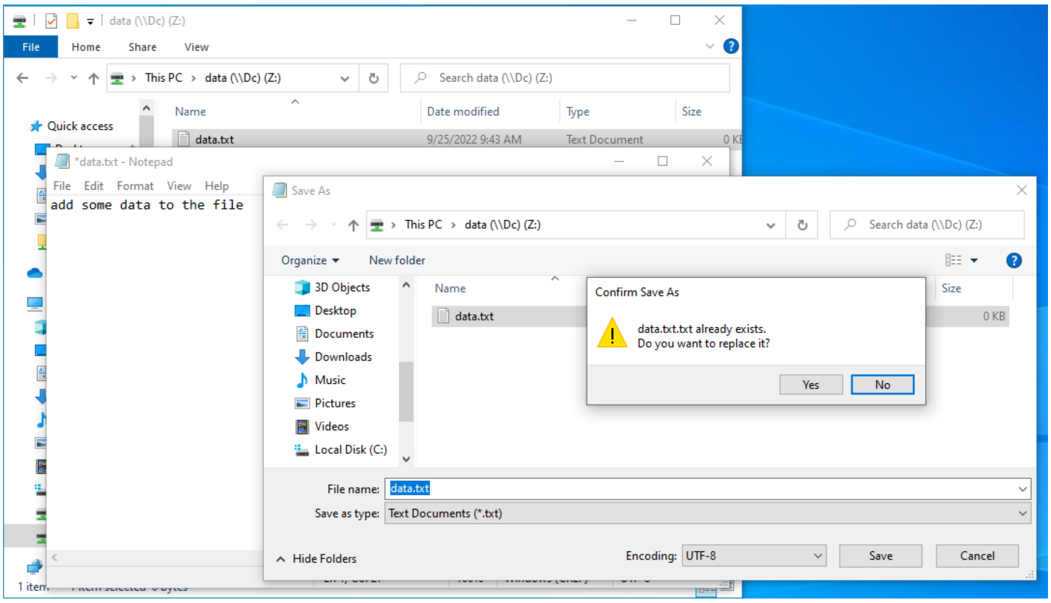
DVD RW Drive (D:)

data (\\Dc) (Z:) 58.6 GB free of 79.6 GB

Make Script directory with script.bat file in it, when the user run the file, it will map the Script directory to the user account.



Logged with user1 member of Sales group, trying to change the file data.txt (an empty text file) in the shared folder data, when I try to save the changes I get "Save As" option, I tried to replace the existing file:



```
add some data to the file
```

Confirm Save As

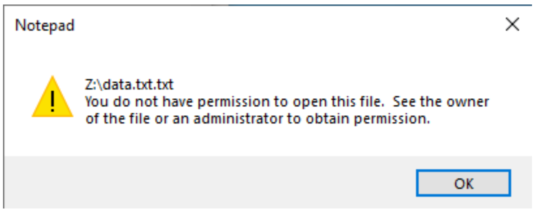
data.txt.txt already exists.
Do you want to replace it?

File name: data.txt

Save as type: Text Documents (*.txt)

Encoding: UTF-8

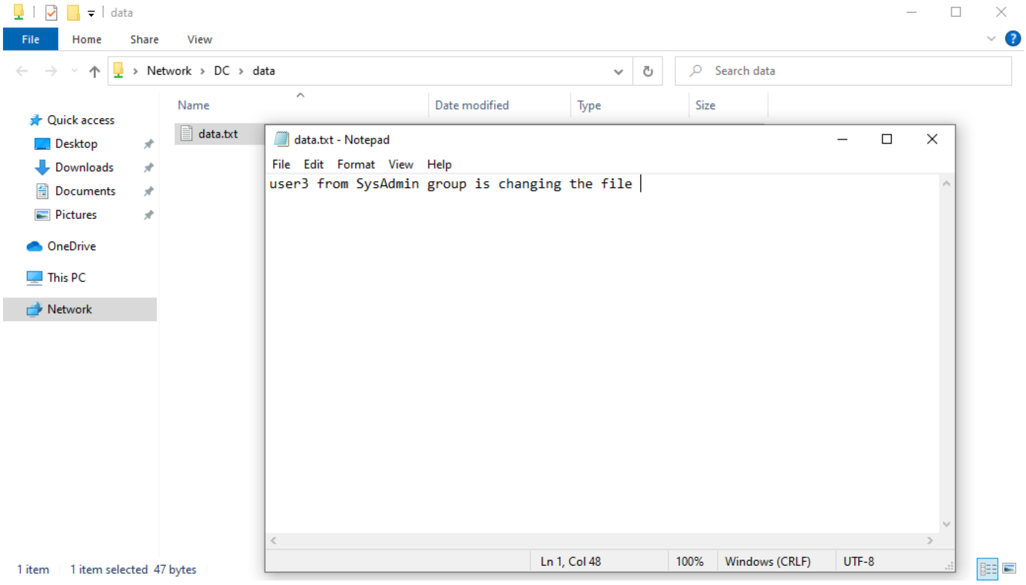
I got rejected:



Notepad

Z:\data.txt.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.

Logged with User3 member of SysAdmin group, trying to change dat.txt file , the file was saved successfully.



data.txt

```
user3 from SysAdmin group is changing the file
```

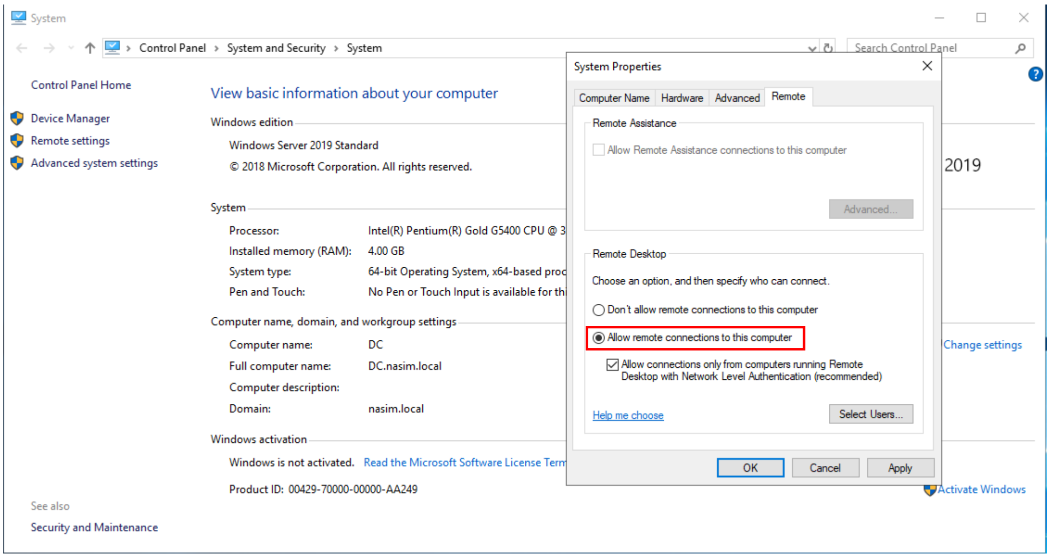
Ln 1, Col 48 | 100% | Windows (CRLF) | UTF-8

1 item 1 item selected 47 bytes

Stage 7: Remote Desktop:

In the domain controller

This pc -> properties -> Remote settings -> allow remote connections to this computer -> Select Users -> Add



View basic information about your computer

Windows edition

Windows Server 2019 Standard

© 2018 Microsoft Corporation. All rights reserved.

2019

System

Processor: Intel(R) Pentium(R) Gold G5400 CPU @ 3

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based proc

Pen and Touch: No Pen or Touch Input is available for th

Computer name, domain, and workgroup settings

Computer name: DC

Full computer name: DC.nasim.local

Computer description:

Domain: nasim.local

Windows activation

Windows is not activated. Read the Microsoft Software License Term

Product ID: 00429-70000-00000-AA249

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

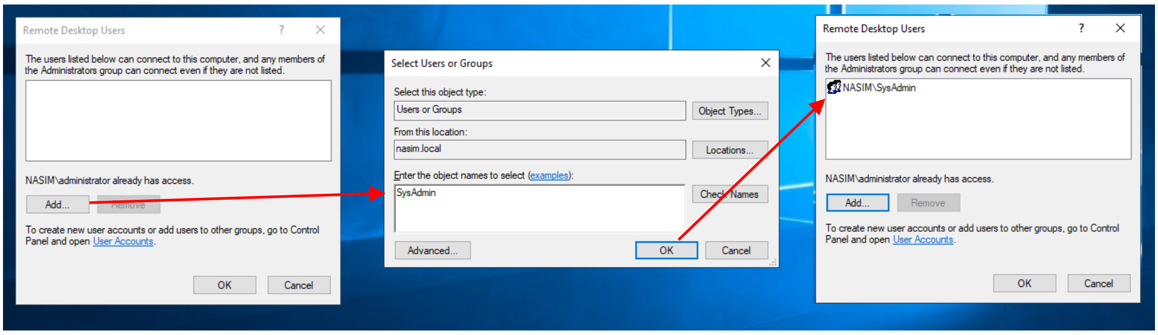
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

I added the entire SysAdmin group:



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

NASIM\administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

Select Users or Groups

Select this object type: Users or Groups

From this location: nasim.local

Enter the object names to select (examples): SysAdmin

Remote Desktop Users

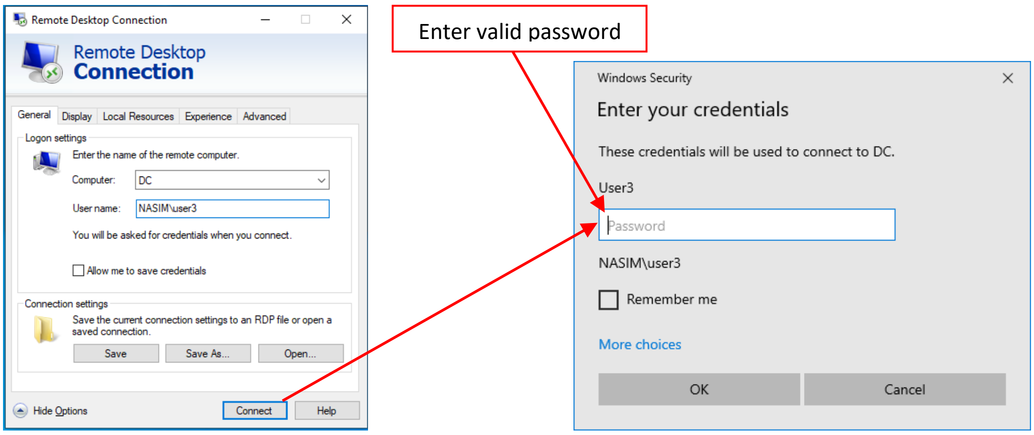
The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

NASIM\SysAdmin

NASIM\administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

In the client station (WIN10) logged as User3 (member of SysAdmin), check if he can take over the domain control/SRV1 remotely.



Enter valid password

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: DC

User name: NASIM\user3

You will be asked for credentials when you connect.

☐ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Windows Security

Enter your credentials

These credentials will be used to connect to DC.

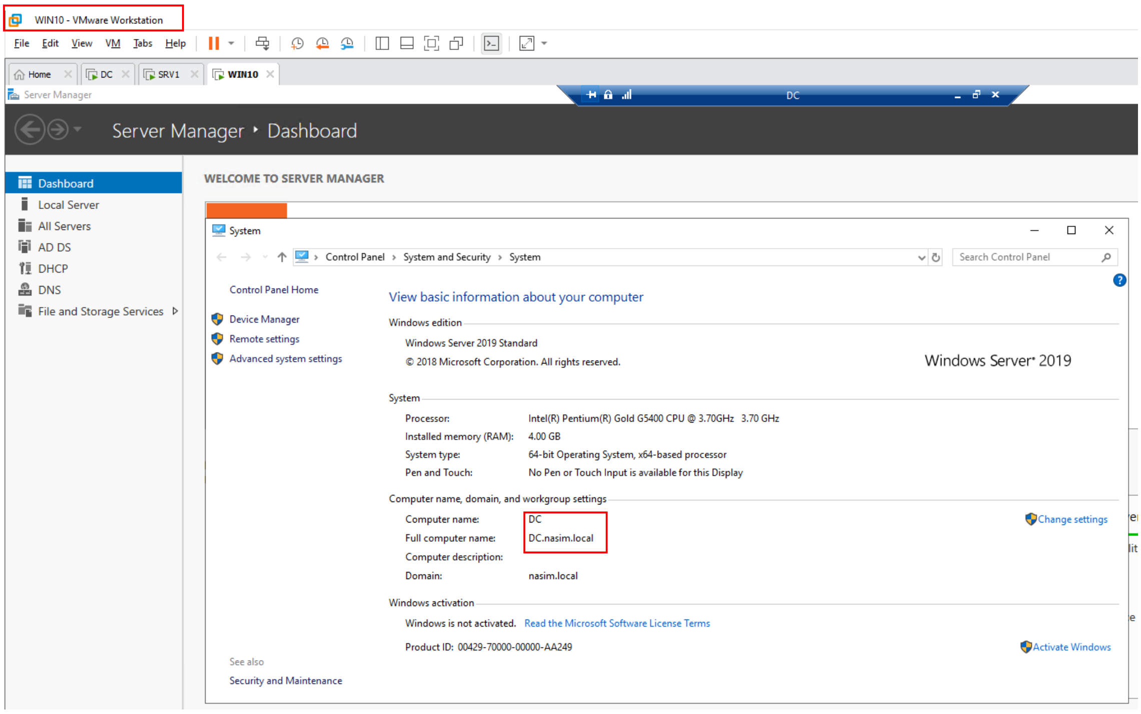
User3

Password

NASIM\user3

☐ Remember me

Log in to DC from WIN10 was made successfully.



WIN10 - VMware Workstation

Server Manager ‣ Dashboard

WELCOME TO SERVER MANAGER

System

Control Panel › System and Security › System

View basic information about your computer

Windows edition

Windows Server 2019 Standard

© 2018 Microsoft Corporation. All rights reserved.

Windows Server® 2019

System

Processor: Intel(R) Pentium(R) Gold G5400 CPU @ 3.70GHz 3.70 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: DC

Full computer name: DC.nasim.local

Computer description:

Domain: nasim.local

Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00429-70000-00000-AA249

Stage 8: Group Policy Objects:

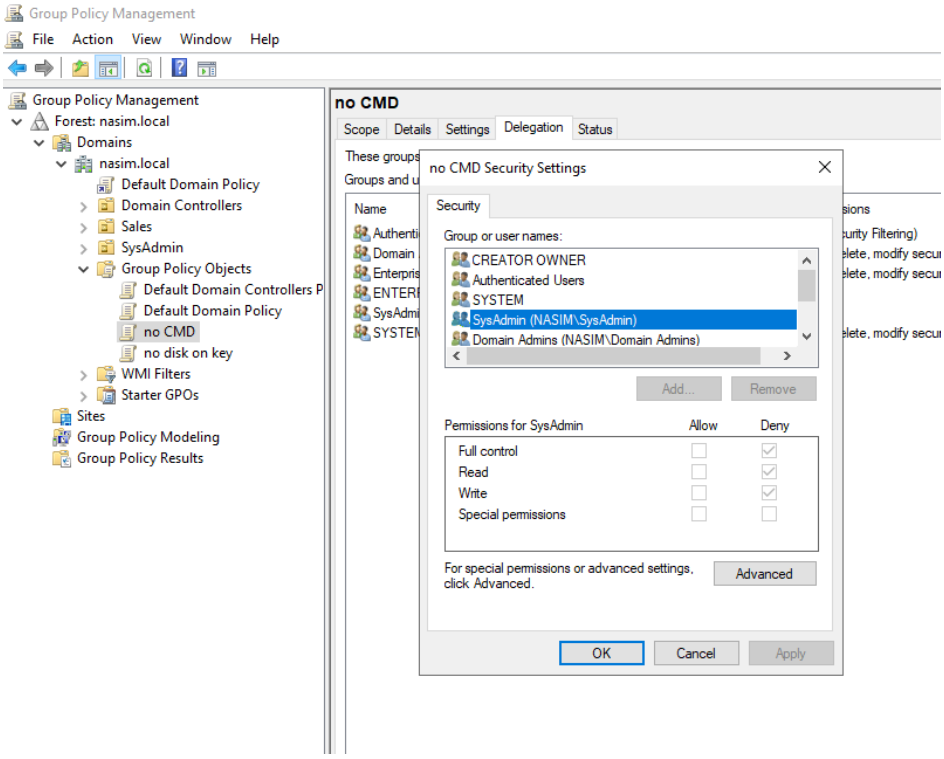
Exclusion of SysAdmin group from command Prompt and control panel GPO; prevent all users except SysAdmin from opening command prompt or Control Panel, prevent Disk-on-key for all users.

For command prompt:

no CMD -> Edit -> User Configuration -> Policies -> Administrative Templates -> System -> Prevent access to command prompt

For Disk-on-key:

no disk on key -> User Configuration -> Policies -> Administrative Templates -> System -> Removable Storage Access -> All Removable Storage classes: Deny all access



no CMD Security Settings

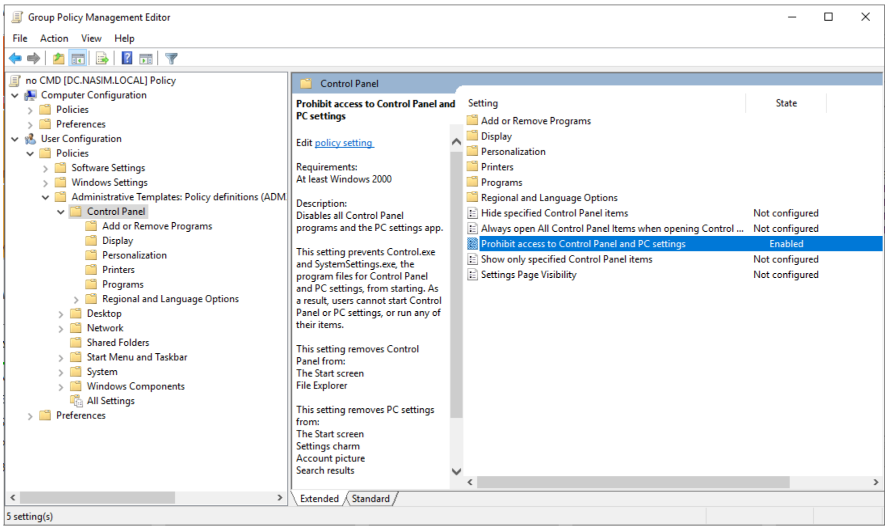
Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- SysAdmin (NASIM\SysAdmin)
- Domain Admins (NASIM\Domain Admins)

Permissions for SysAdmin	Allow	Deny
Full control	☐	☑
Read	☐	☑
Write	☐	☑
Special permissions	☐	☐

For special permissions or advanced settings, click Advanced.

no Control Panel -> Edit -> User Configuration -> Policies -> Administrative Templates -> Control Panel -> Prohibit access to Control Panel and PC settings



Prohibit access to Control Panel and PC settings

Edit policy setting

Requirements:
At least Windows 2000

Description:
Disables all Control Panel programs and the PC settings app.

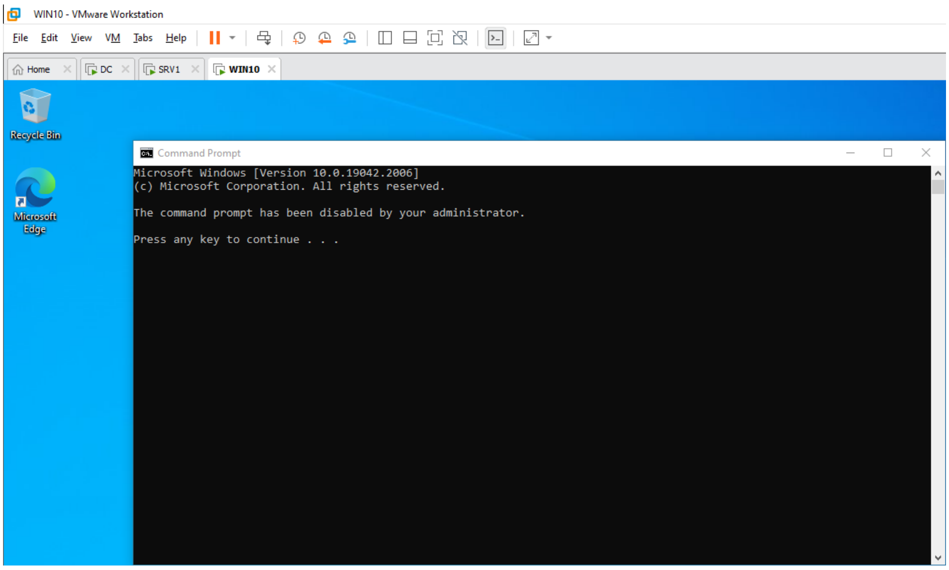
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

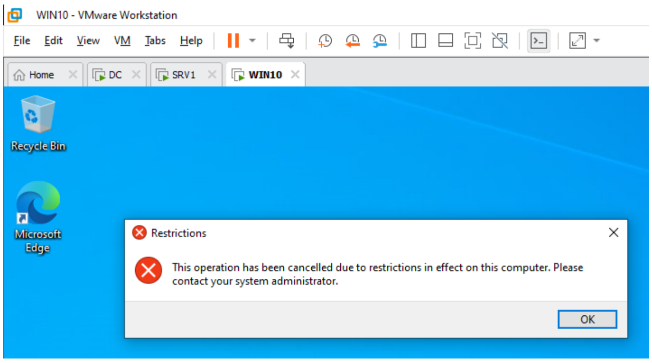
This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

Setting	State
Add or Remove Programs	
Display	
Personalization	
Printers	
Programs	
Regional and Language Options	
Hide specified Control Panel items	Not configured
Always open All Control Panel Items when opening Control ...	Not configured
Prohibit access to Control Panel and PC settings	Enabled
Show only specified Control Panel items	Not configured
Settings Page Visibility	Not configured

Log in with Sales group member – User1:

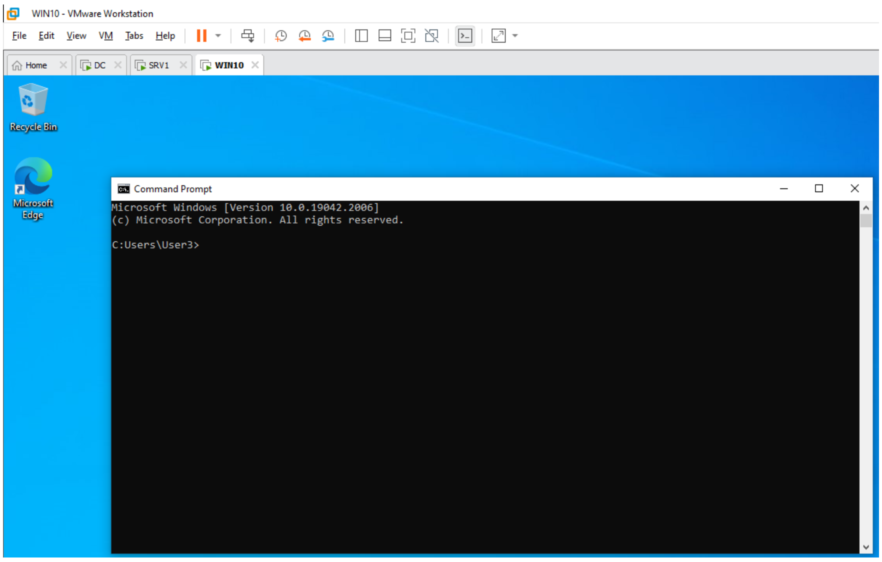


```
Microsoft Windows [Version 10.0.19042.2006]
(c) Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

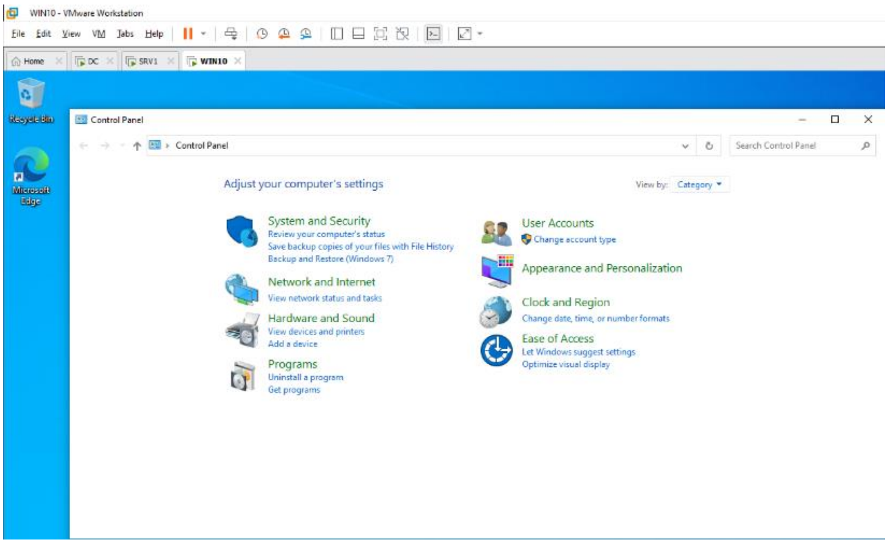


This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

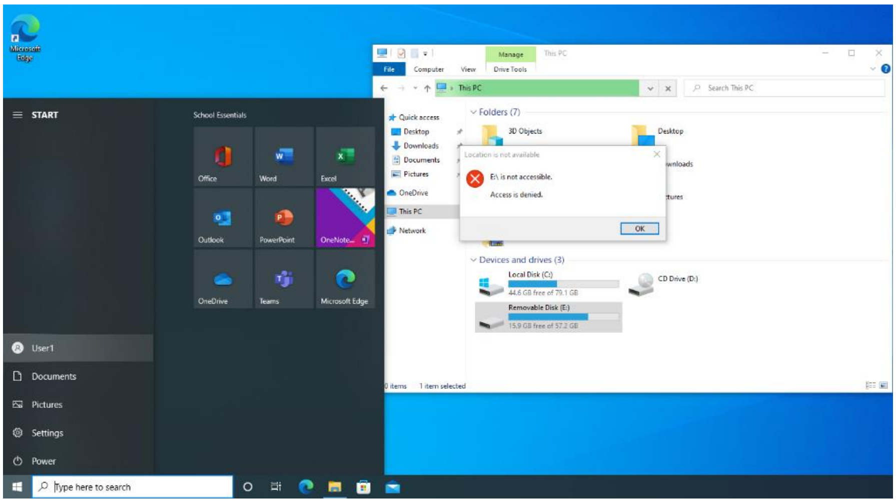
Log in with SysAdmin member – User3:



```
Microsoft Windows [Version 10.0.19042.2006]
(c) Microsoft Corporation. All rights reserved.

C:Users\User3>
```


WIN10 - VMware Workstation
File Edit View VM Tabs Help
Home
DC
SRV1
WIN10
Recycle Bin
Microsoft Edge
Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
Get programs
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

For the disk-on-key:



Location is not available

E:\ is not accessible.

Access is denied.

OK