Domain Migration

Step 1: Configure the DNS on the Target PC and Source PC on all the Servers and Computers. and also add 8.8.8.8.

Step 2: Configuring Conditional Forwarding on both the Source and Target PC.

What is Conditional Forwarding?

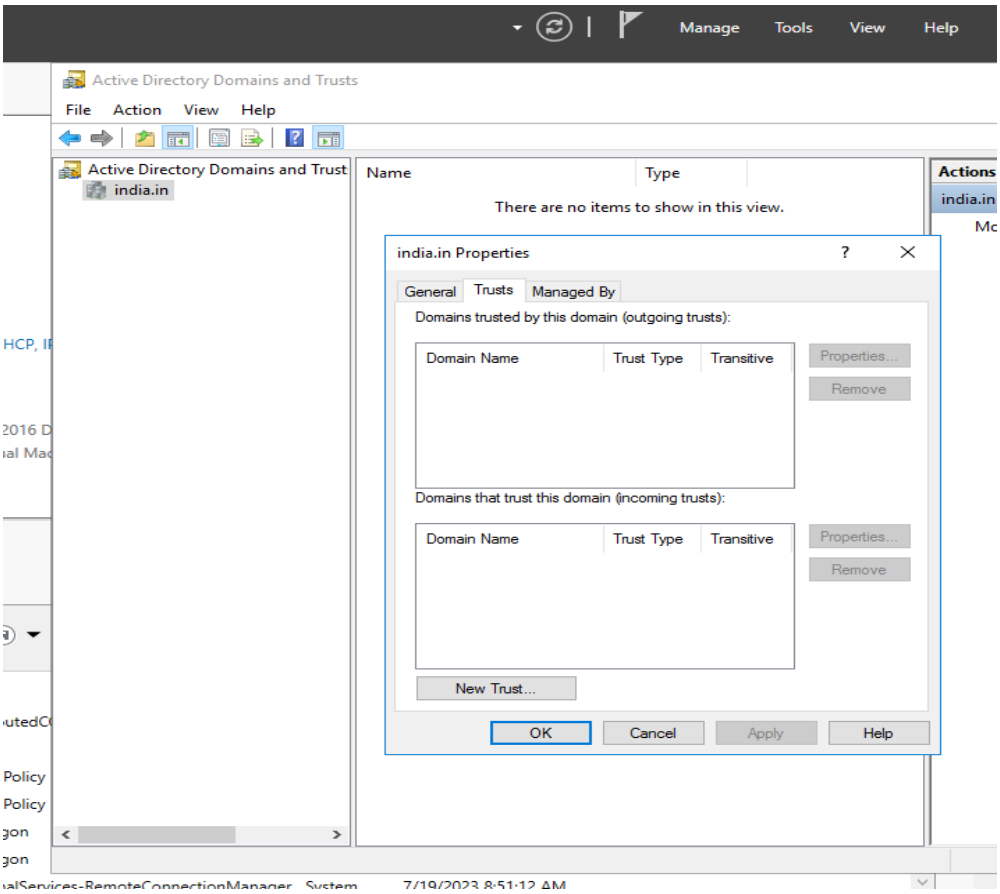
Conditional DNS forwarding is a method to direct DNS queries related to a specific domain to another DNS server. This is done by creating conditional DNS forwarders or rules on the DNS server. This is a simple and reliable method to resolve DNS queries belonging to an external domain.

Note: Ping both the target and source machine with domain name and IP addresses on both the sides.

Step 3: Creating Trust relationship and validate the incoming and outgoing trust.

To create Trust go to Tools→ Active Directory Domain and Trust → Right click on domain click on Properties→ click on Trust and create new Trust.

Enter the domain name of the source domain if performing from target→select two way→ both this domain and specified domain→enter the credentials for specified domain→ domain wide authentication→….-->Finish.



Step 4: Configuring the DNS Suffix search list.

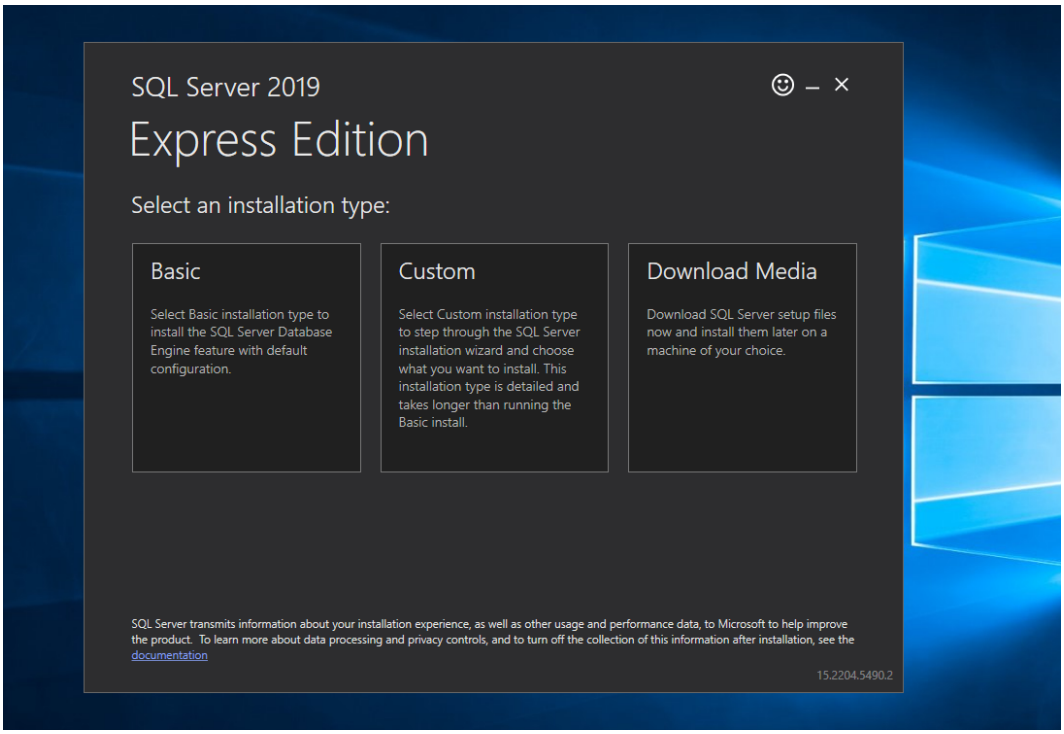
Go to tools→ Group Policy Management → Click on Forest → click on domain → Right click on default domain →Edit→Computer Configuration→Policies→Administrative Templates→Networks→DNS Client→Configure DNS Suffix Search List.

Note: Perform this steps on both source and target machine after that Run the command prompt by pressing Win+R cmd → Run **gpupdate** to update the group policy. And Run **ipconfig /all** .

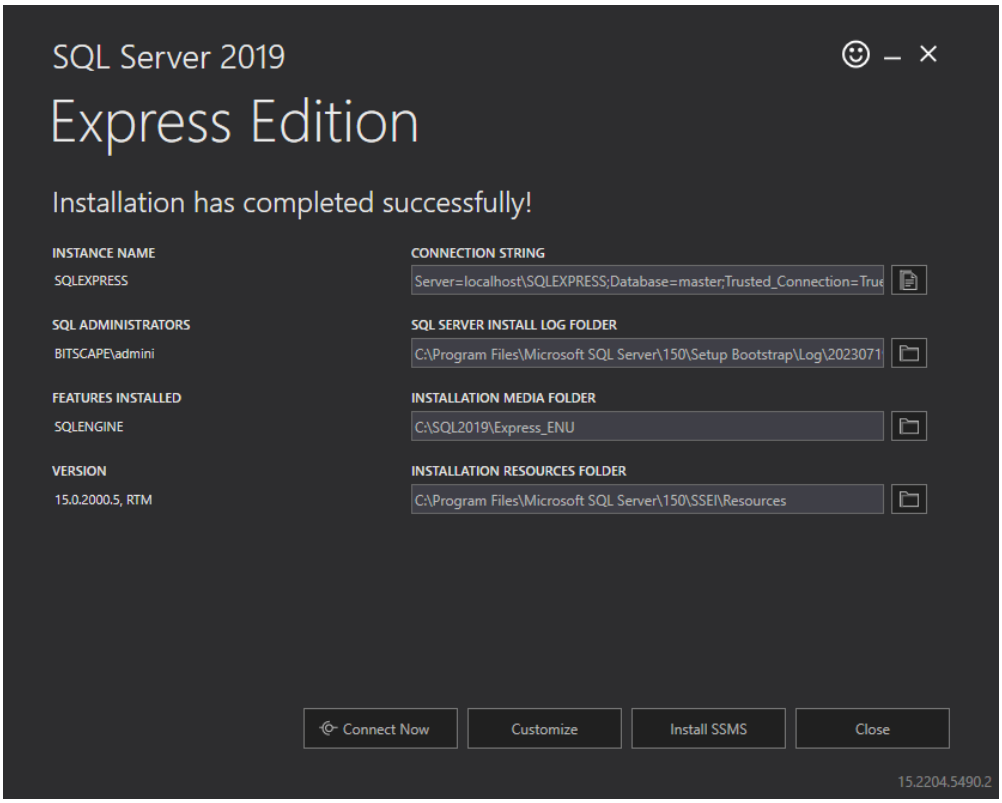
Step 5: Installing the SQL Express 2019 R2

https://www.microsoft.com/en-us/Download/details.aspx?id=101064

Select the Basic Installation

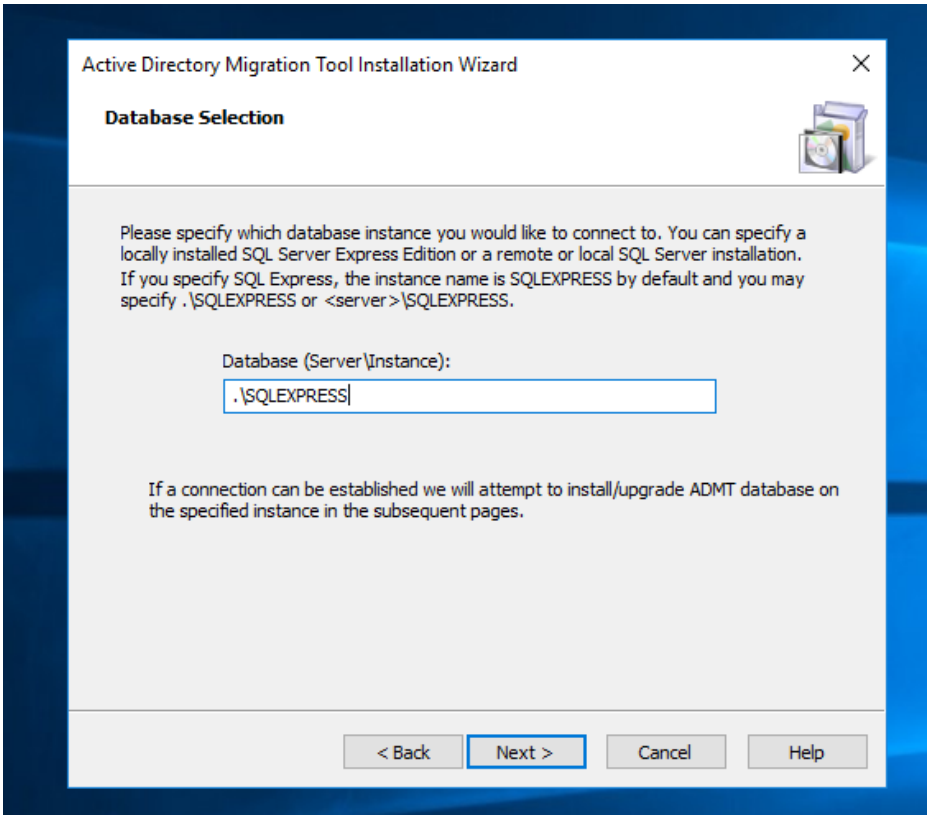


Now customize the Installation



Perform a new Installation of SQLServer 2019 →Instance Configuration: select default Instance →Authentication mode: select Windows Authentication mode.

Step 6: Now Install the ADMT Migration Tool and connect with the Database.



Note: You have to perform the Step 5 and Step 6 for both Source and Target Machine.

Step 7: Command to generate Encryption Key:

Encryption key is used to sync your password from old Domain to new Domain.

Now open the path where ADMT is installed and open CMD and run the following command: (Run the following command in Target Machine)

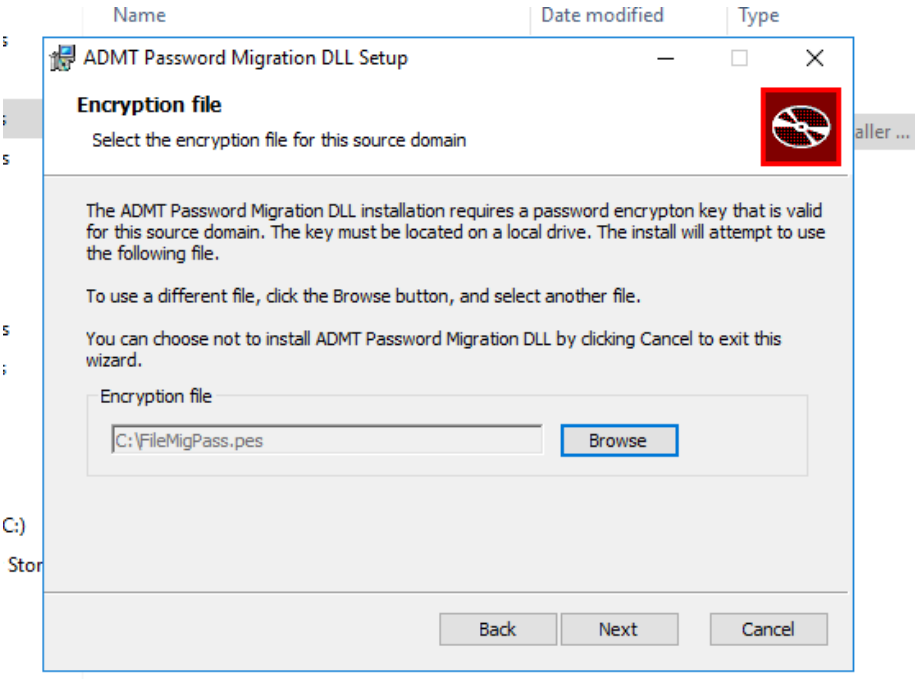
ADMT Key /Option:Create /SourceDomain:bitscape.ishan-kansara.in /KeyFile:C:\FileMigPass.pes /KeyPassword:Pass@123

After running this command the key will be generated paste it to the source domain.

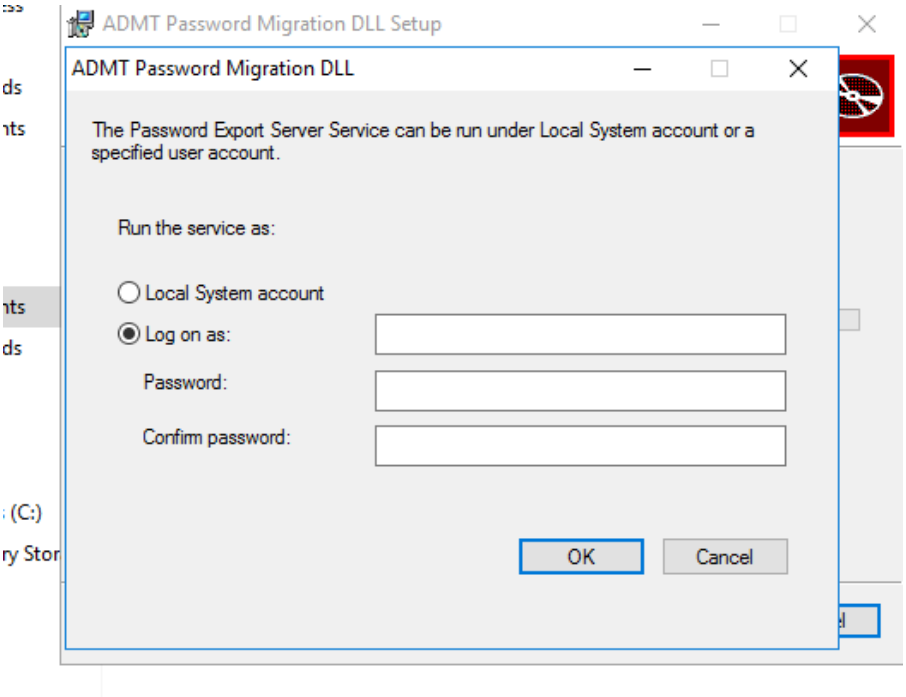
Step 8: Add ADMT Migration Account in Administrators Group

Go to Tools→Active Directory Users and Computers→ Click on Domain→Click on Builtin→in Administrator group add members→give administrative permission for both the domains on both the sides.

Step 9: Now Install ADMT Password DLL Tool on Source Domain.



Enter the Credentials of Target Domain



Step 10: Starting Password Export Server Service

Go to Tools on Source Domain → Services→ Select the Password Export Service and run it automatic, **Enable the service on both the machine.**

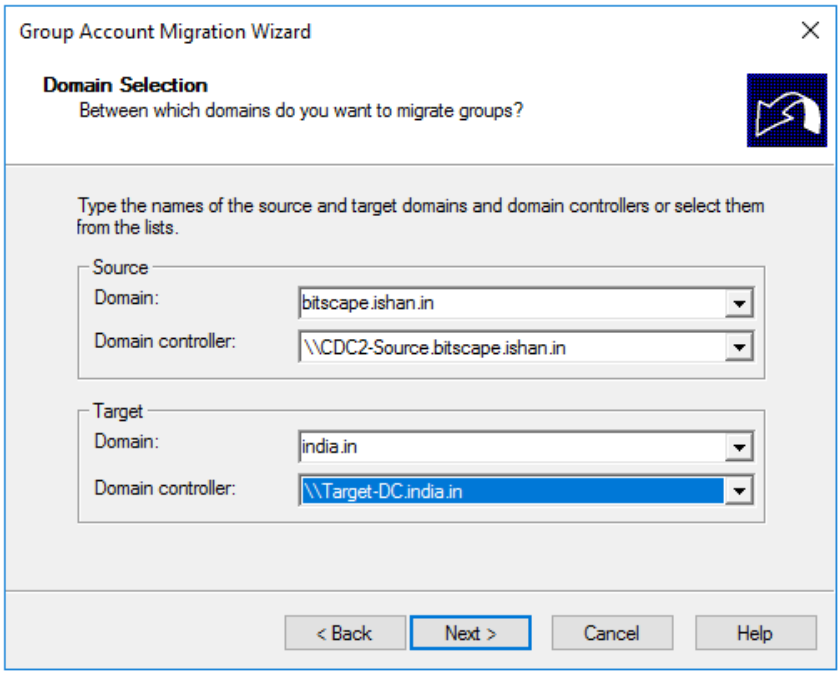
Step 11: Create OU in Target OU

Step 12: Migration Steps

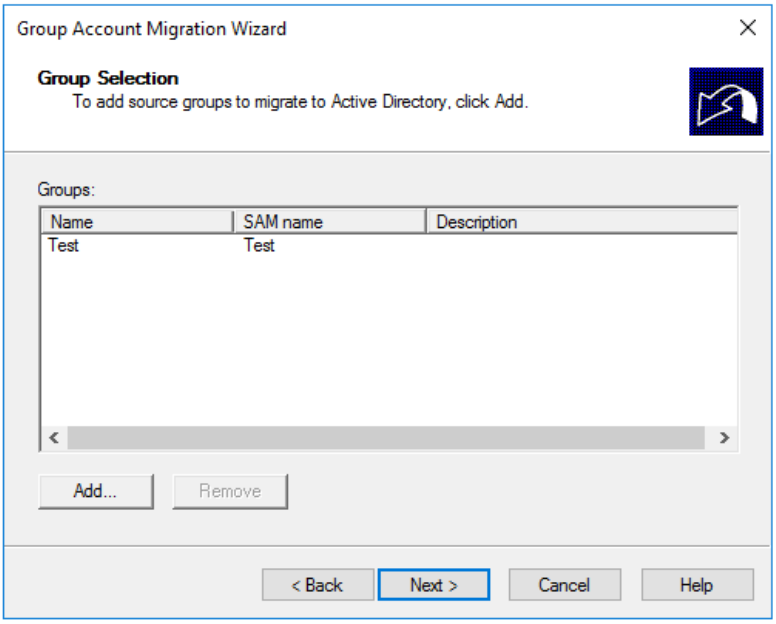
Now open Active Directory Migration Tool Kit on the Target Domain:

Right Click on it and Perform Group Migration.

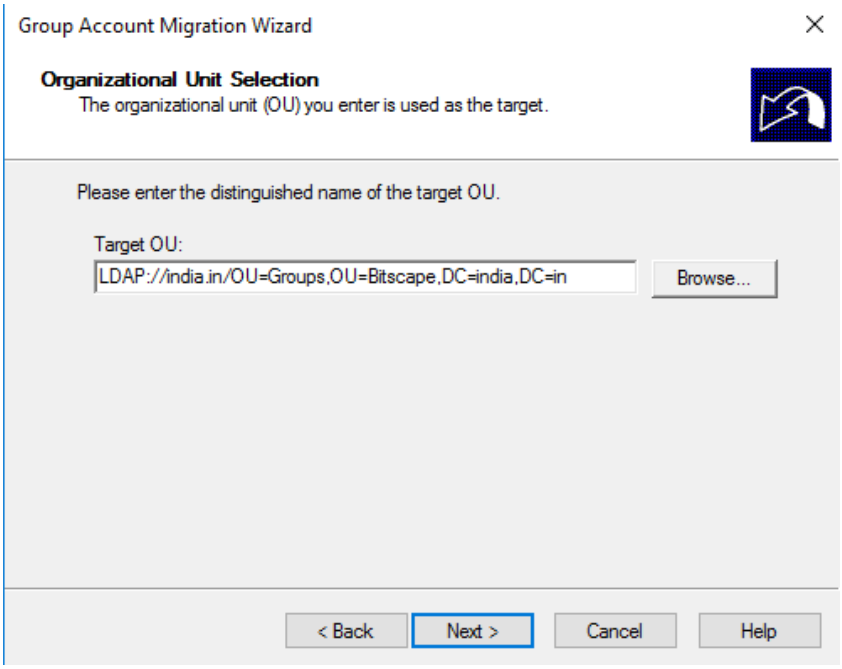
Domain Selection for Group Migration:



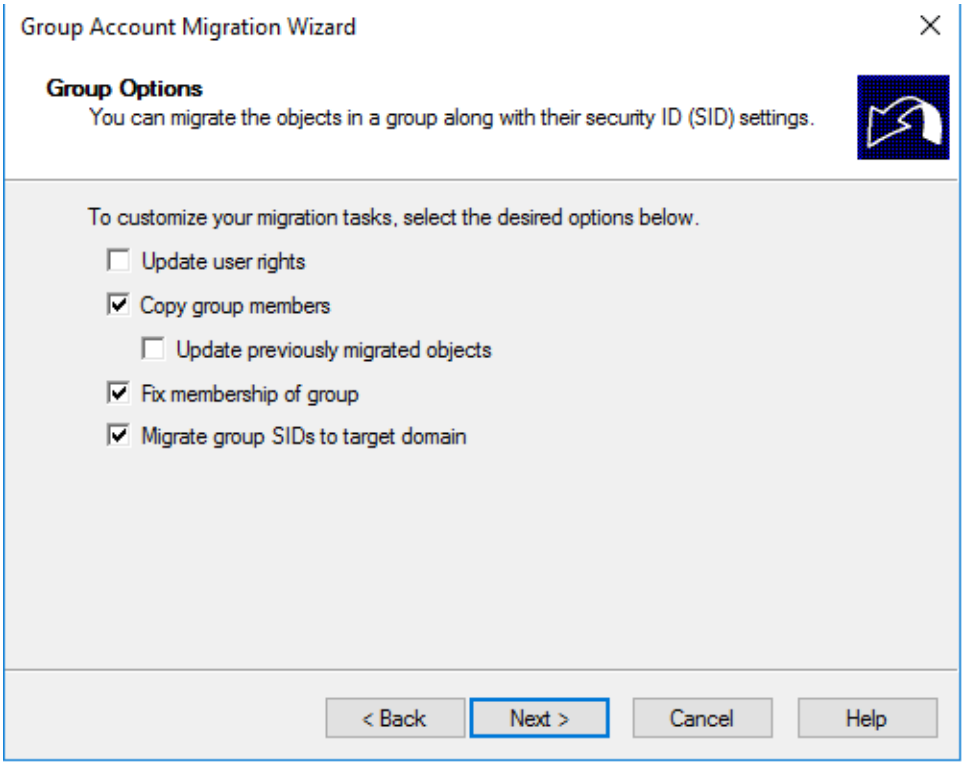
Perform the Group Selection:



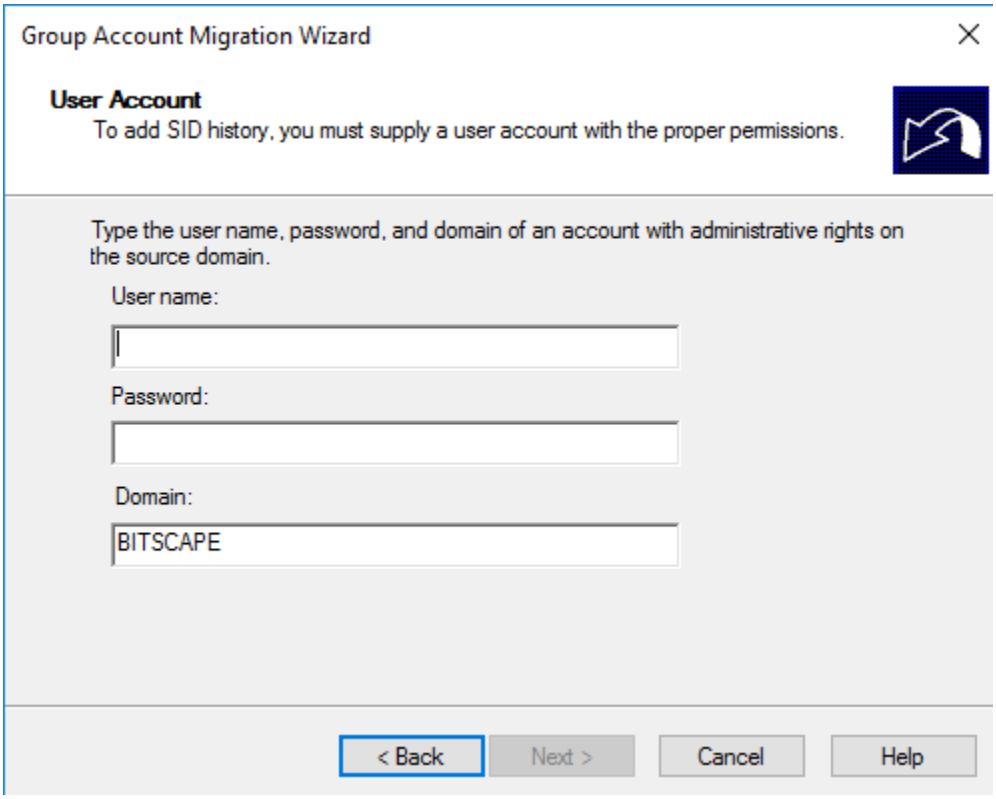
Select the Target OU:



Select Group Options:



Enter the Credentials for the source Domain



Same steps to be Performed for User Migration.

Security Translation Migration

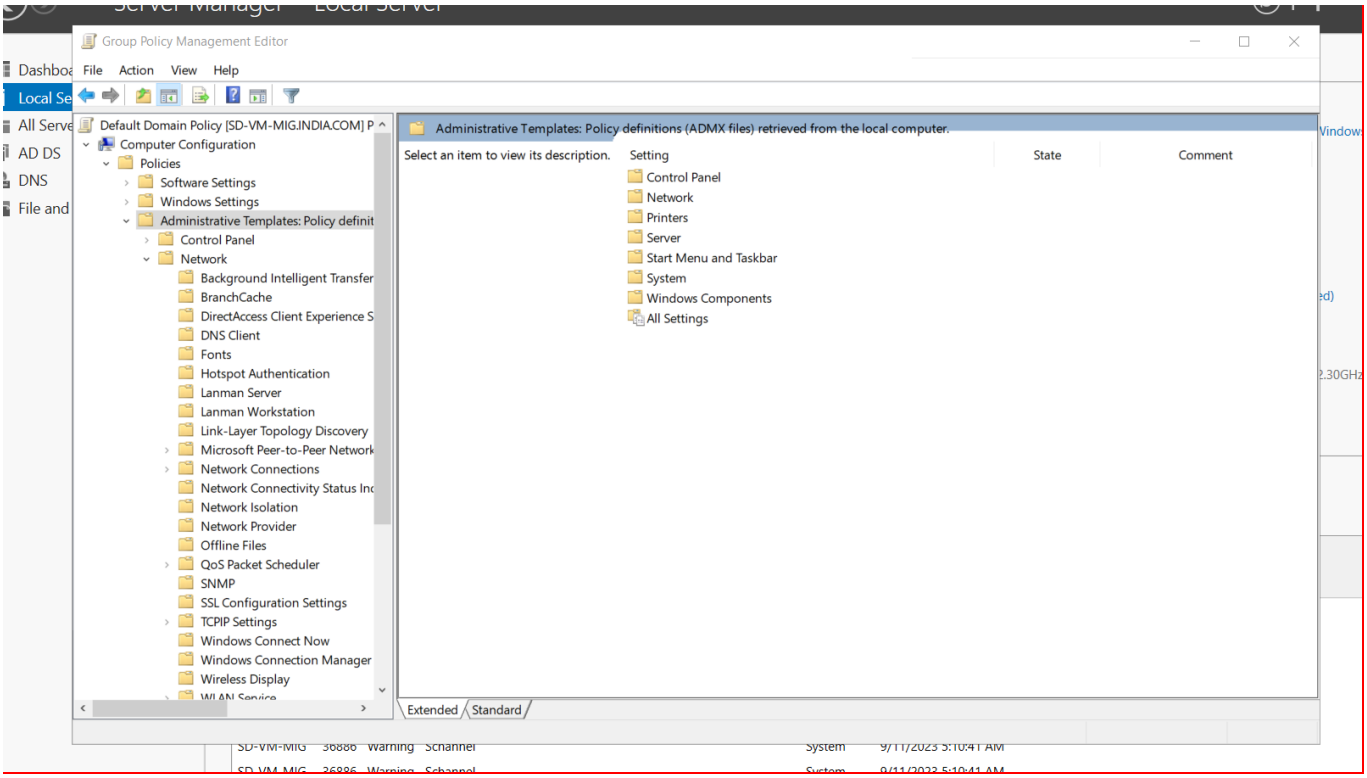
Now perform Security Translation is performed on a machine which you want to join in a new forest.

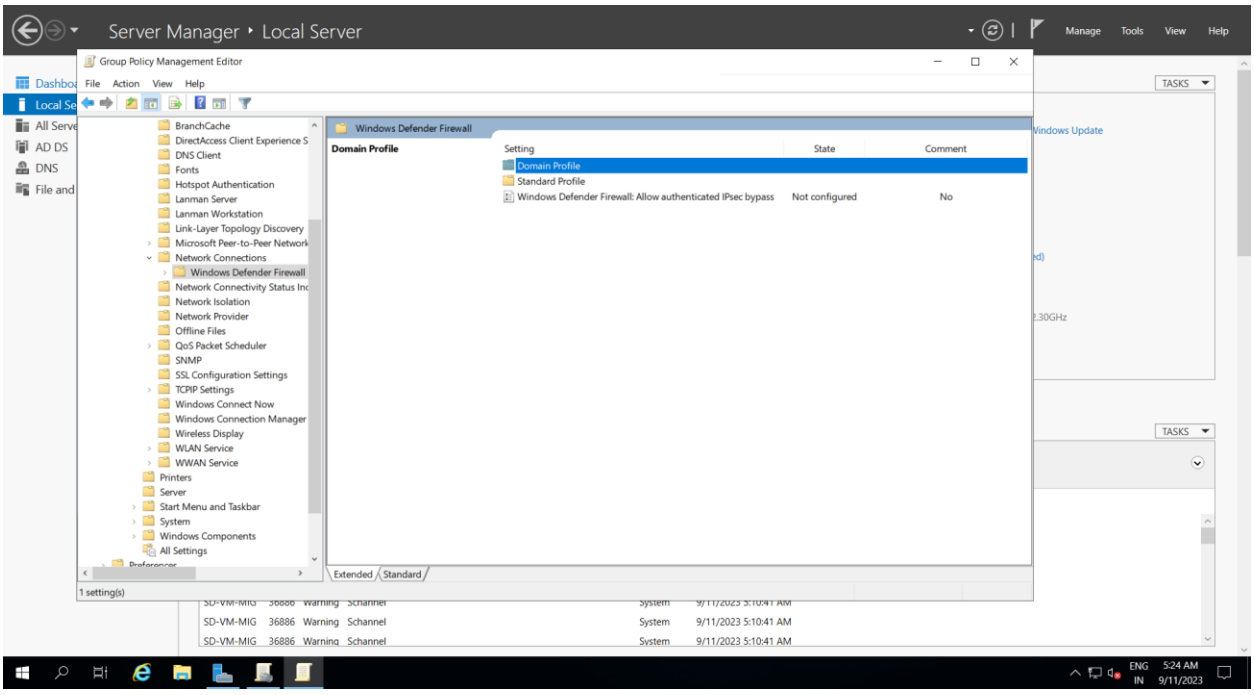
IN the machine which you want to migrate give the administrative permission to the Target domain and turn off the firewall.

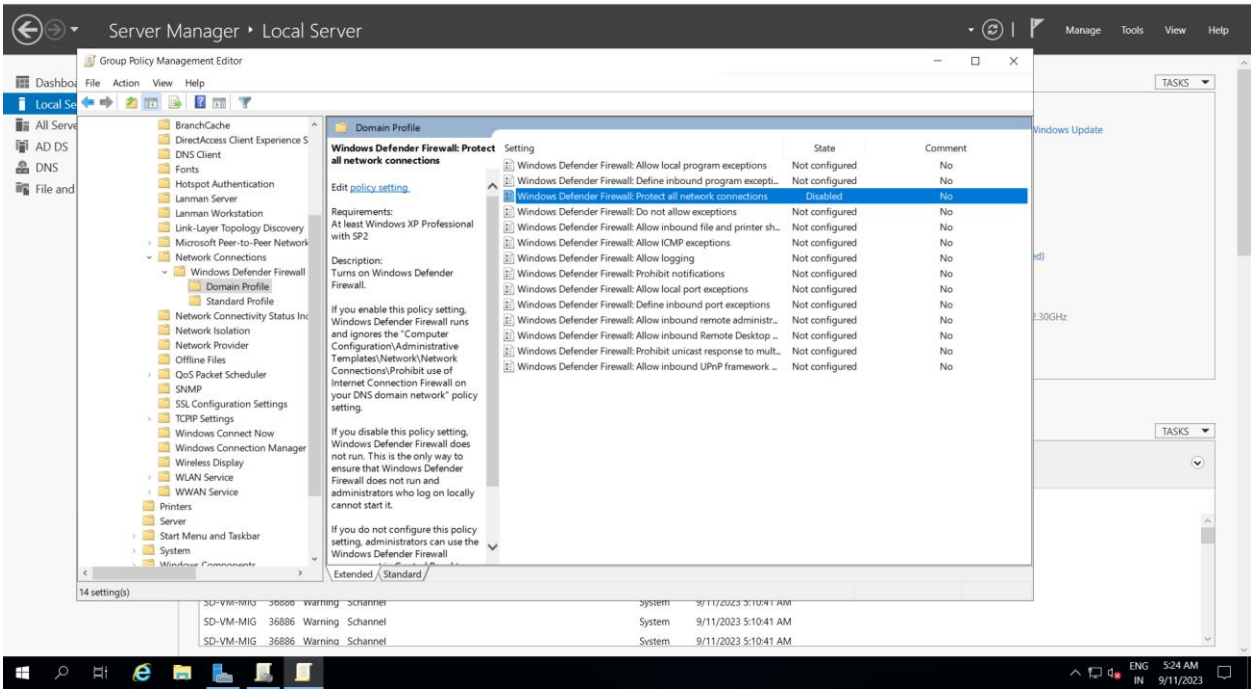
Now open the ADMT tool and perform the security Translation migration.

After that Perform the computer migration in ADMT.

How to turn off Firewall Using GPO?






Server Manager ▸ Local Server
Manage
Tools
View
Help
Group Policy Management Editor
File
Action
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
TASKS
Windows Update
BranchCache
DirectAccess Client Experience S
DNS Client
Fonts
Hotspot Authentication
Lanman Server
Lanman Workstation
Link-Layer Topology Discovery
Microsoft Peer-to-Peer Network
Network Connections
Windows Defender Firewall
Domain Profile
Standard Profile
Network Connectivity Status Ind
Network Isolation
Network Provider
Offline Files
QoS Packet Scheduler
SNMP
SSL Configuration Settings
TCPIP Settings
Windows Connect Now
Windows Connection Manager
Wireless Display
WLAN Service
WWAN Service
Printers
Server
Start Menu and Taskbar
System
Domain Profile
Windows Defender Firewall: Protect all network connections
Edit policy setting.
Requirements:
At least Windows XP Professional with SP2
Description:
Turns on Windows Defender Firewall.
If you enable this policy setting, Windows Defender Firewall runs and ignores the "Computer Configuration\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Firewall on your DNS domain network" policy setting.
If you disable this policy setting, Windows Defender Firewall does not run. This is the only way to ensure that Windows Defender Firewall does not run and administrators who log on locally cannot start it.
If you do not configure this policy setting, administrators can use the Windows Defender Firewall
Setting
State
Comment
Windows Defender Firewall: Allow local program exceptions
Not configured
No
Windows Defender Firewall: Define inbound program excepti...
Not configured
No
Windows Defender Firewall: Protect all network connections
Disabled
No
Windows Defender Firewall: Do not allow exceptions
Not configured
No
Windows Defender Firewall: Allow inbound file and printer sh...
Not configured
No
Windows Defender Firewall: Allow ICMP exceptions
Not configured
No
Windows Defender Firewall: Allow logging
Not configured
No
Windows Defender Firewall: Prohibit notifications
Not configured
No
Windows Defender Firewall: Allow local port exceptions
Not configured
No
Windows Defender Firewall: Define inbound port exceptions
Not configured
No
Windows Defender Firewall: Allow inbound remote administr...
Not configured
No
Windows Defender Firewall: Allow inbound Remote Desktop ...
Not configured
No
Windows Defender Firewall: Prohibit unicast response to mult...
Not configured
No
Windows Defender Firewall: Allow inbound UPnP framework ...
Not configured
No
Extended
Standard
14 setting(s)
SD-VM-MIG 36886 Warning Schannel System 9/11/2023 5:10:41 AM
SD-VM-MIG 36886 Warning Schannel System 9/11/2023 5:10:41 AM
SD-VM-MIG 36886 Warning Schannel System 9/11/2023 5:10:41 AM
ENG
IN
5:24 AM
9/11/2023