HW04 - Windows

UBNetDef Systems Security(SysSec)

September 30, 2021

UBNetDef

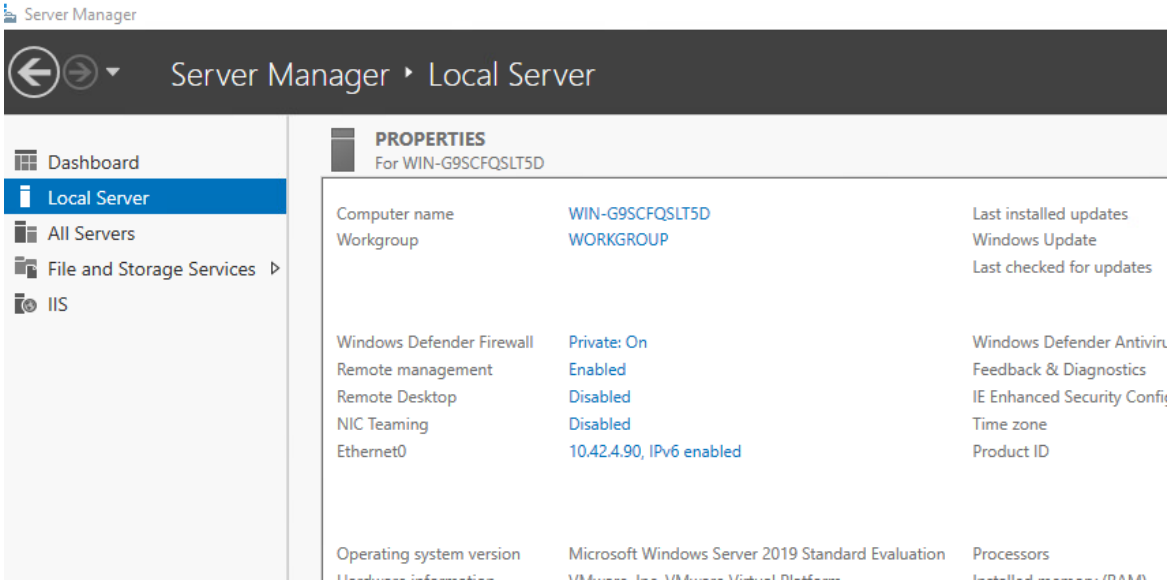
SUBMITTED BY
AKHILESH ANAND UNDRALLA

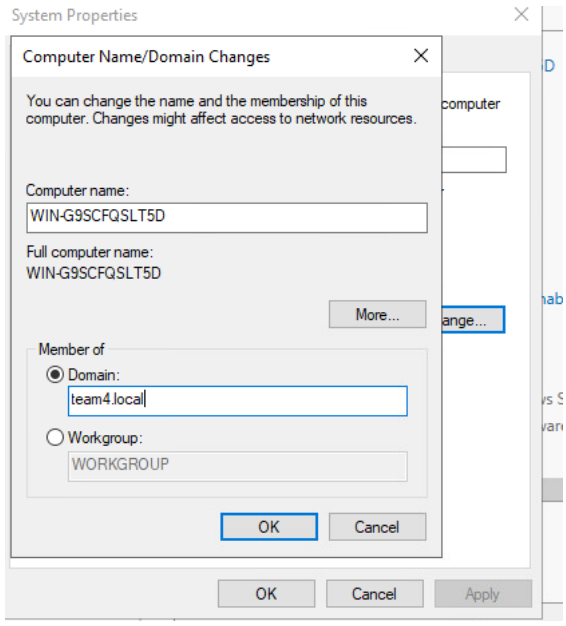
TABLE OF CONTENTS

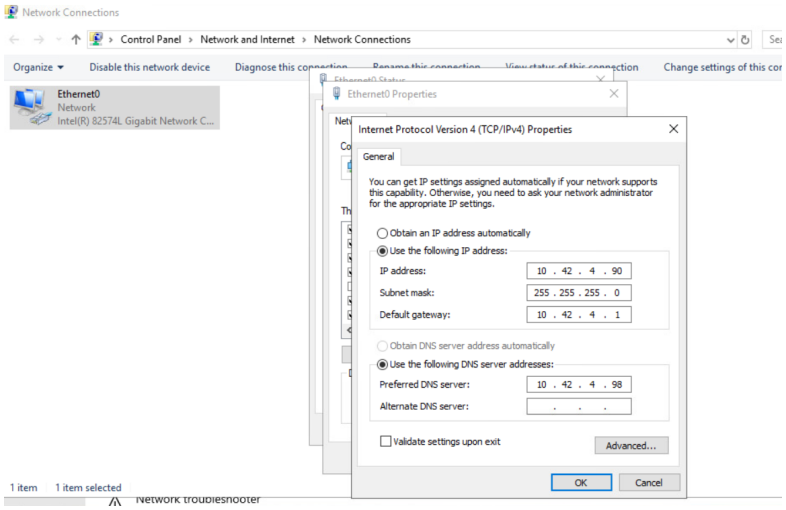
Join Windows Client and ServerGUI VM to your domain:

Join ServerGUI VM to Domain:
Give DNS of ServerGUI as 10.42.4.98 to point to the Domain Controller

Click on Computer name and click ‘Change and Select ‘Domain’ as team4.local



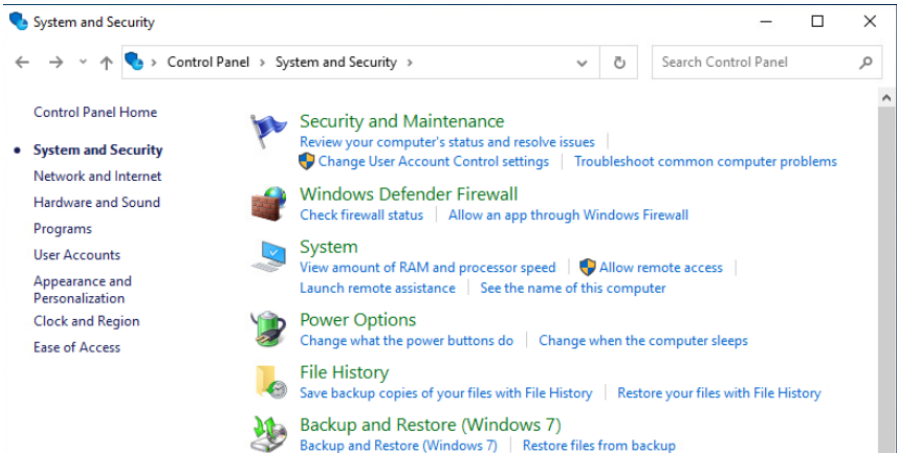


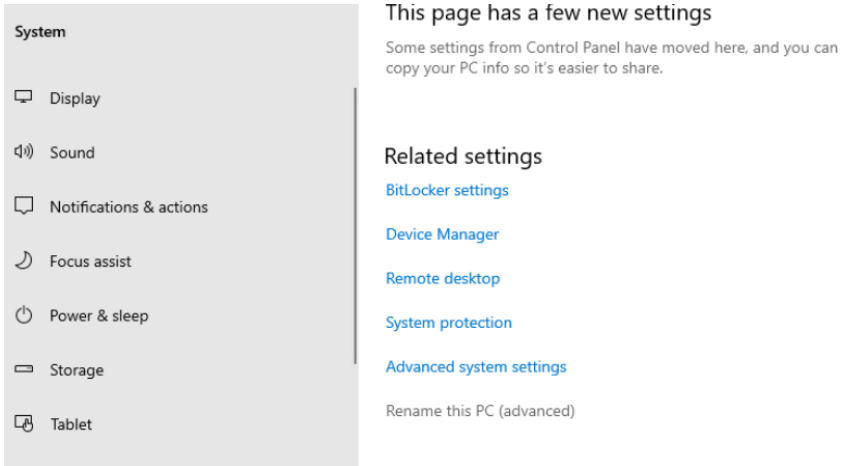


Screenshot of ServerGUI to point Domain Controller

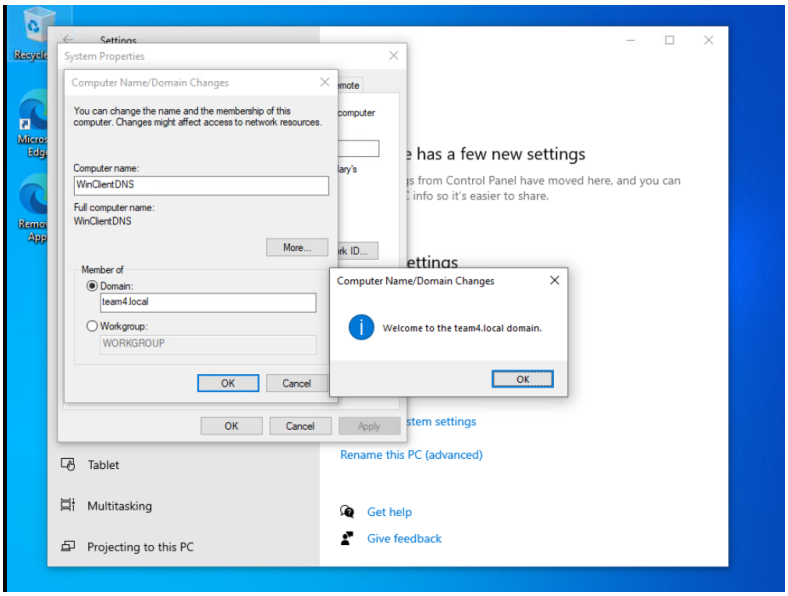
Join WindowsClient to Domain:

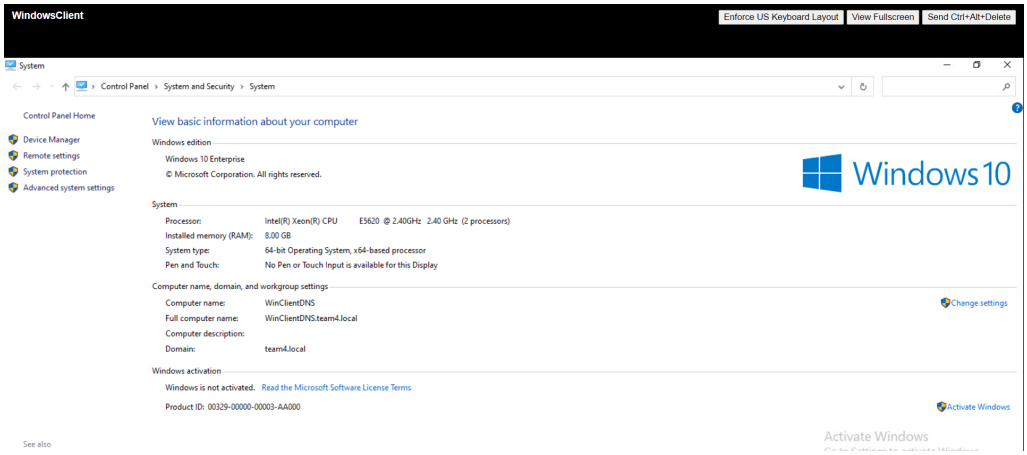
Go to Control Panel -> System and Security -> System -> Rename this PC (Advanced) at the bottom



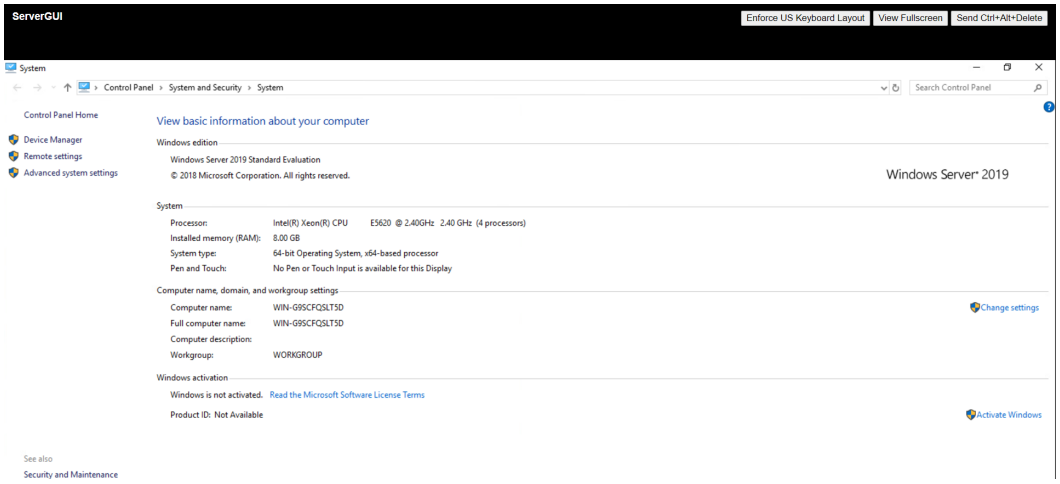


Click on ‘Change’ -> Select ‘Domain’ -> give the domain as ‘team4.local’ ->Click ‘OK’->Give ‘Administrator





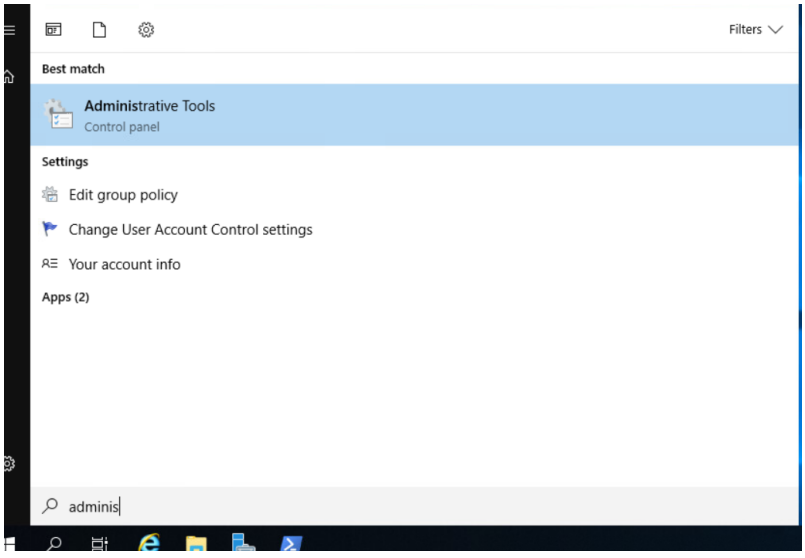
Screenshot of the “Properties” in “This Computer” after joining WindowsClient VM

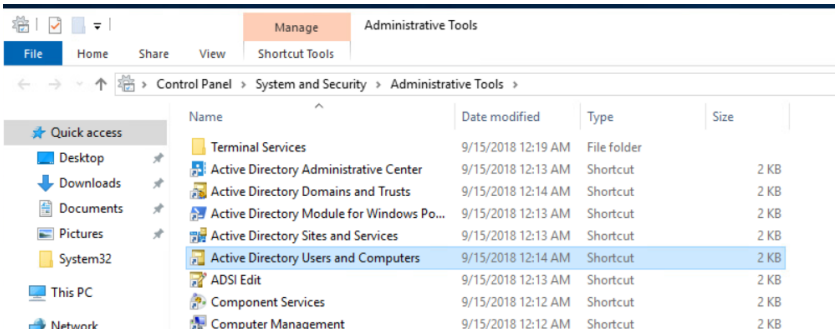


Screenshot of the “Properties” of “This Computer” after joining ServerGUI VM to the domain

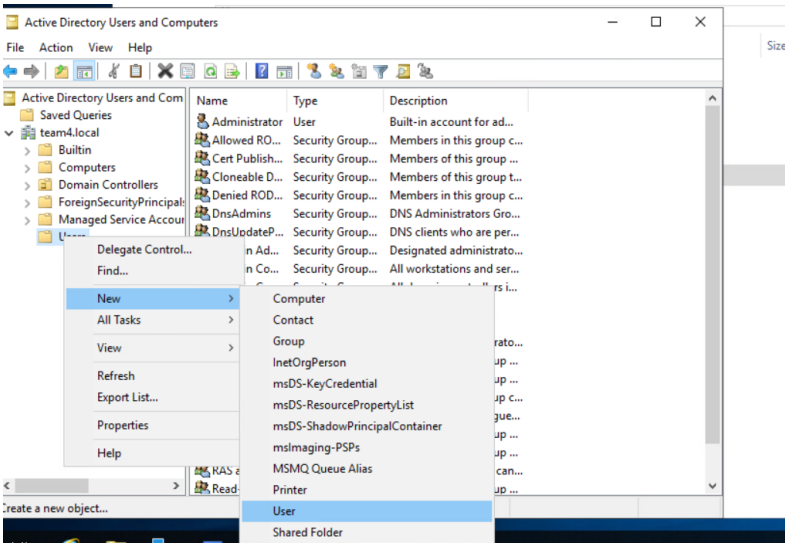
Create two users on your Windows Domain:

Search and Click ‘Administrative Tools’ -> Select ‘Active Directory Users and Computer’

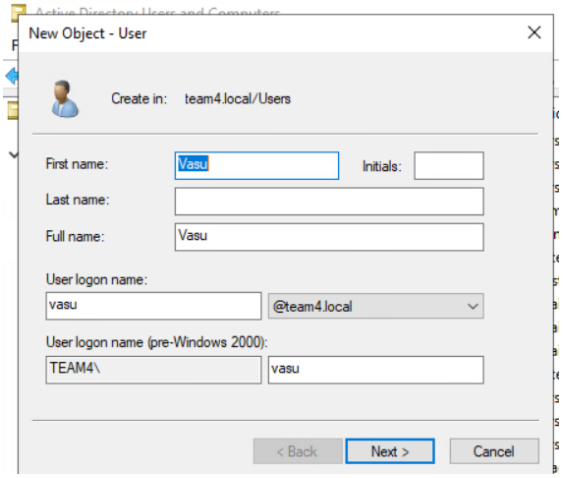


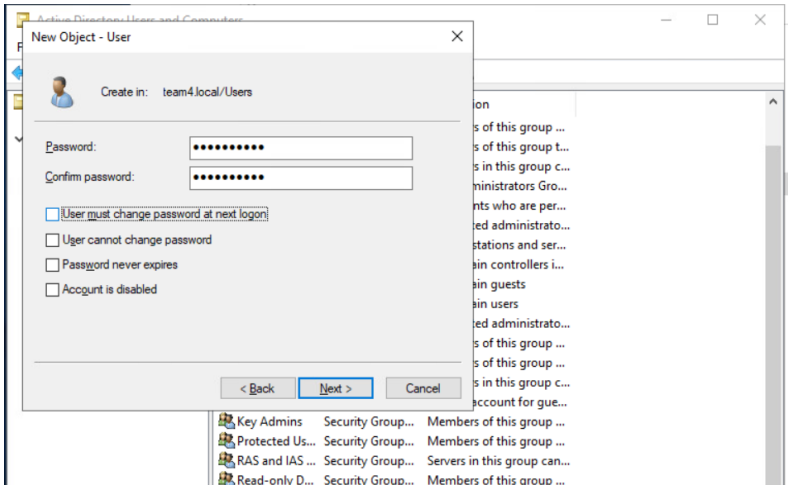


Expand ‘team4.local’ -> Right click on ‘Users’ -> Select ‘New’-> Select ‘User’

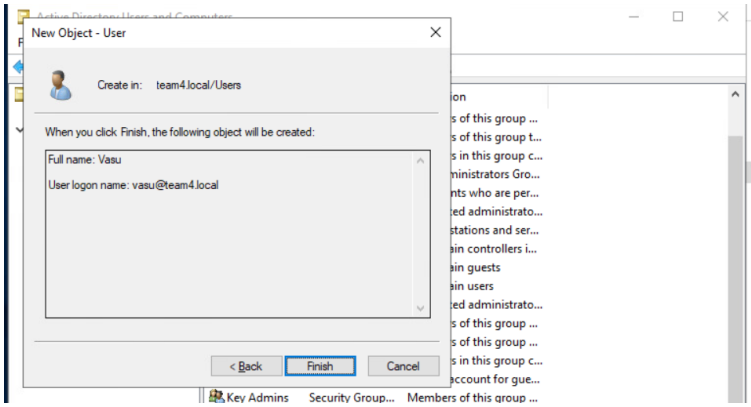


Give the First name and User logon name as ‘Vasu’ -> Click ‘Next’ -> Password:’Change.me!’->Uncheck all -> Click ‘Next’

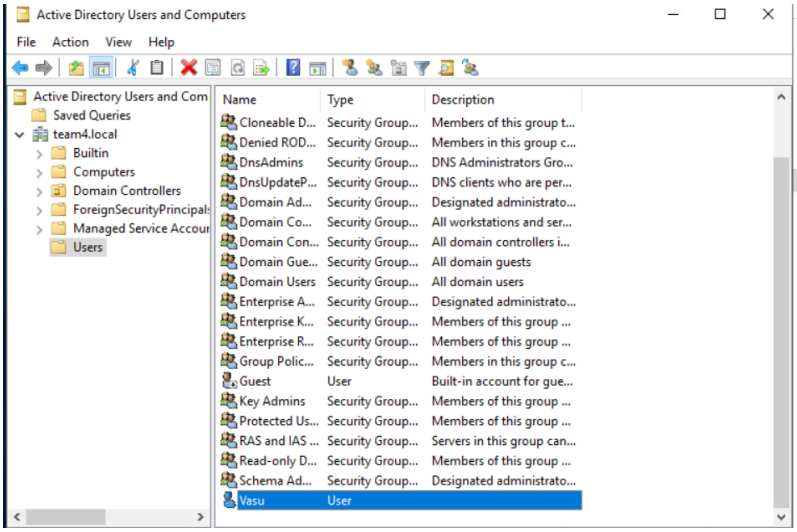


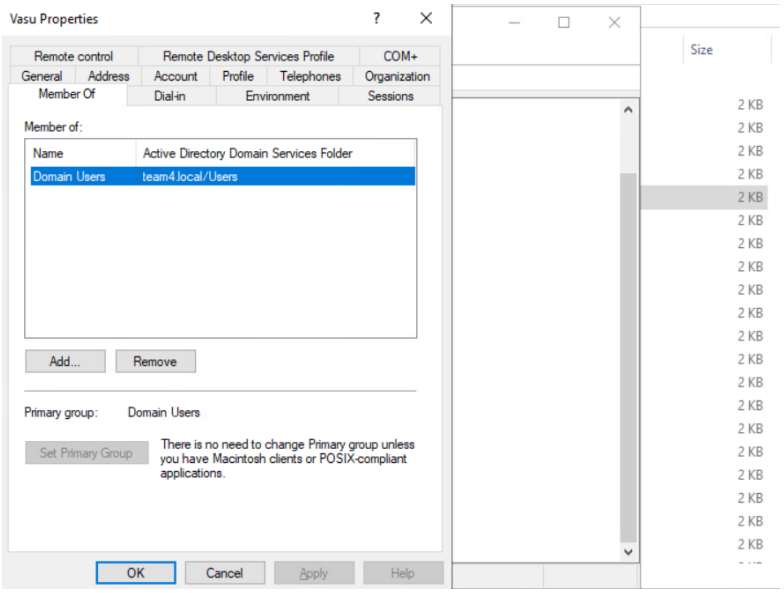


Click ‘Finish’ -> Type ‘Administrator’ as Username and Password as ‘Change.me!’ to authenticate

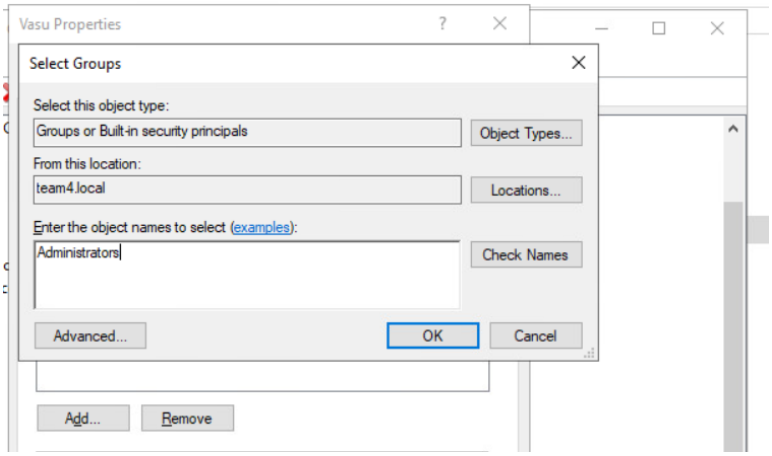


Double click on ‘Vasu’ -> Select ‘Member of’ -> Click ‘Add’



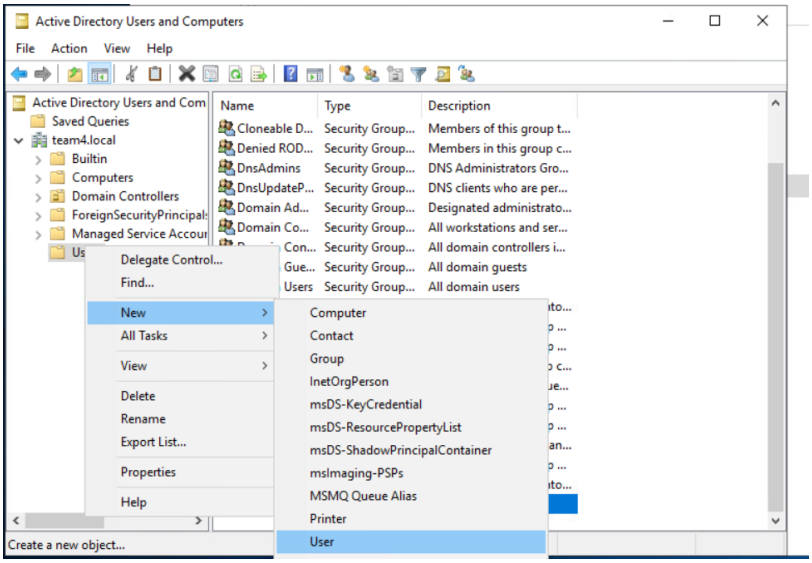


Enter the Object name as ‘Administrators’ -> Click ‘OK’

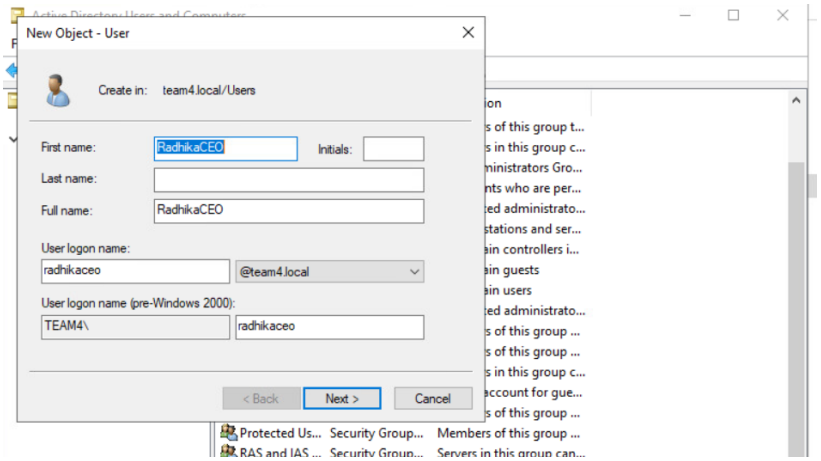


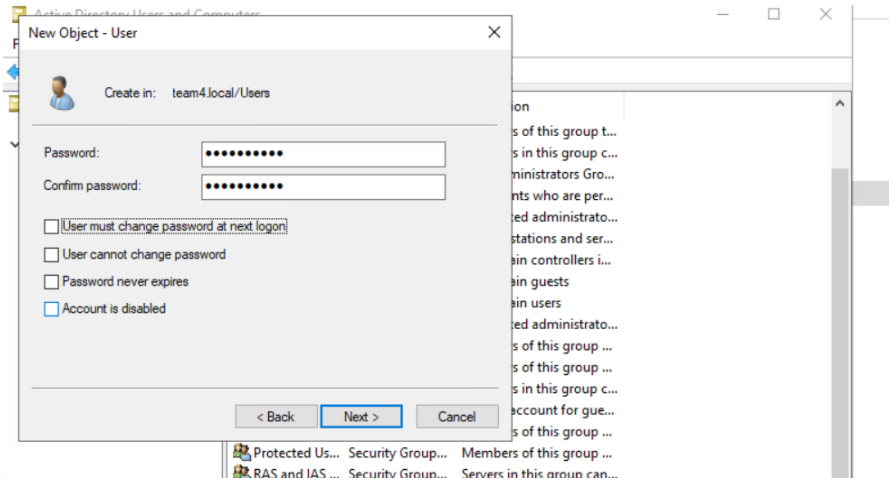
To create non administrative user:

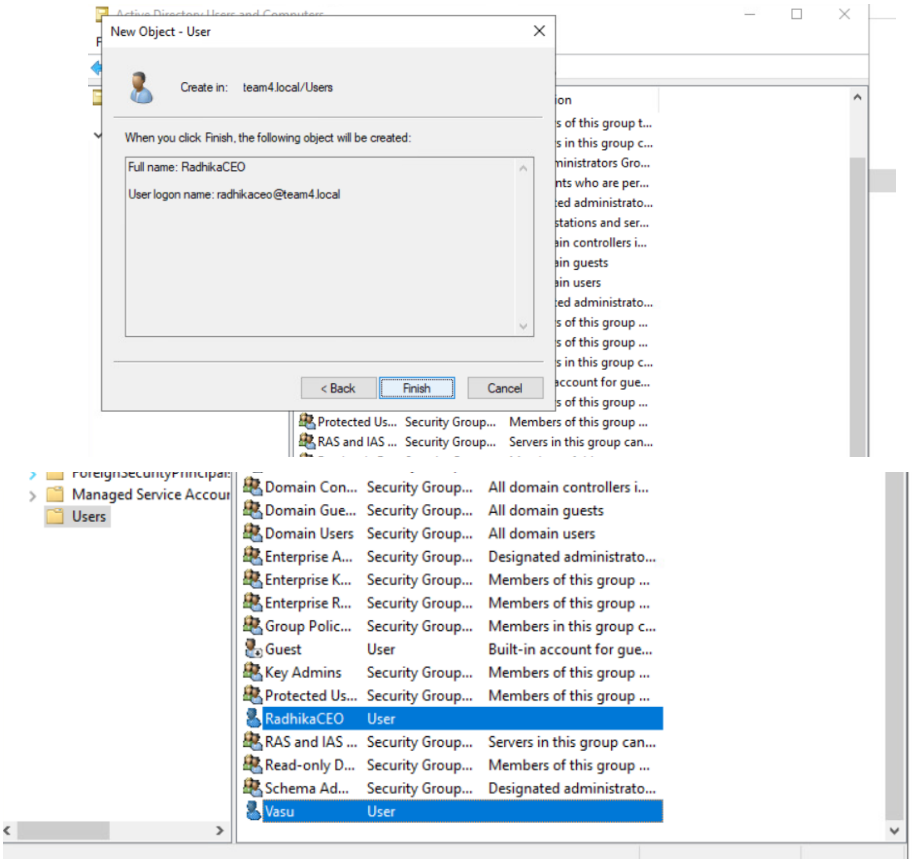
Right click on ‘Users’ -> Select ‘New’-> Select ‘User’



Give First name and User logon name as ‘RadhikaCEO’-> Click ‘Next’-> Uncheck all-> ‘Next’ -> ‘Finish’



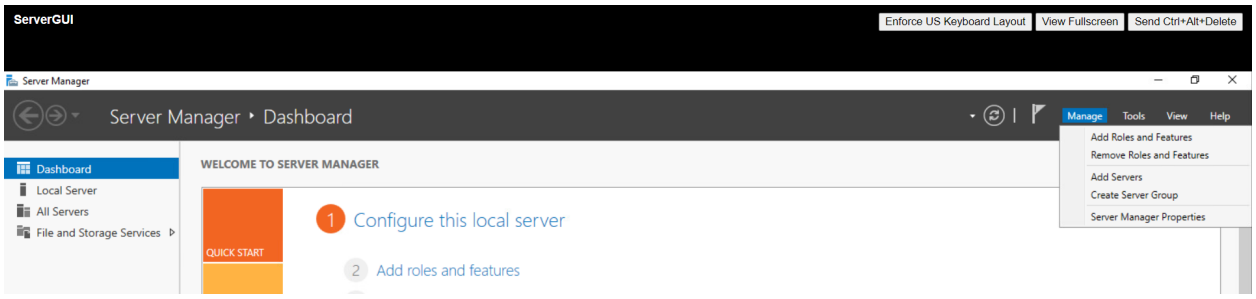


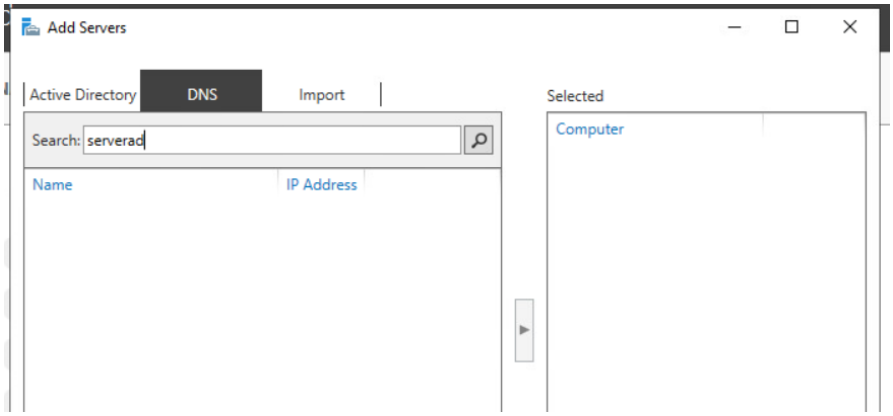


Screenshot of both users reflected on Windows Domain

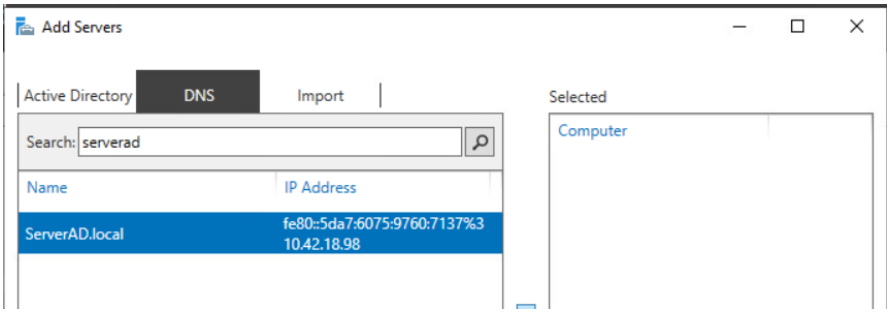
Add all servers into the Server Pool within Server Manager on ServerGUI:

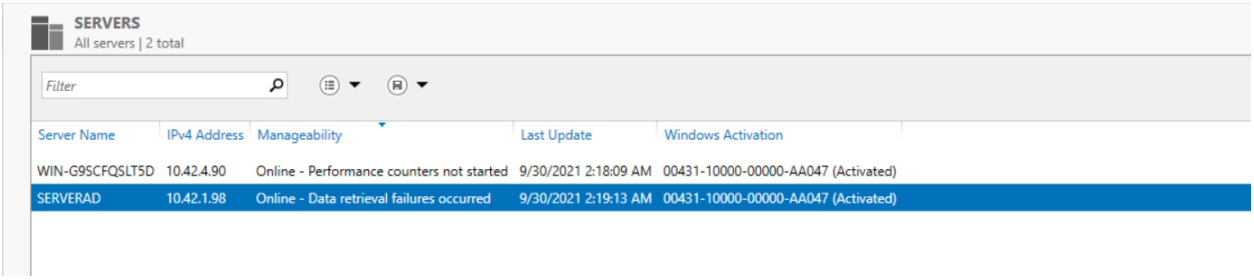
Open ServerGUI->Select ‘Manage’ from the menu (Top left)->Select ‘Add Servers’->’Select tab ’DNS’-> Search ‘ServerAD’





Click on right pointing arrow in the middle to move ‘ServerAD.local’ to the left pane

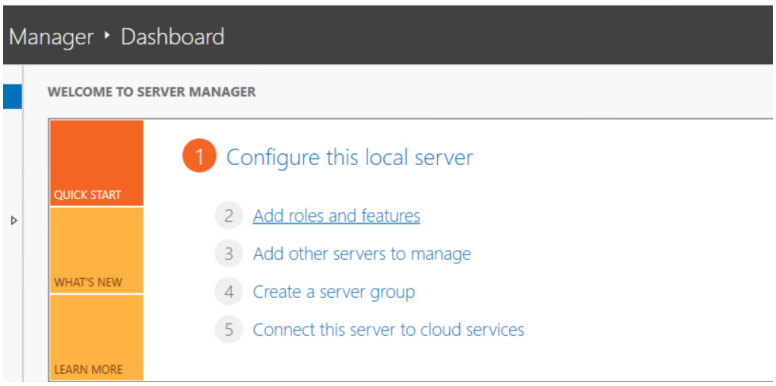




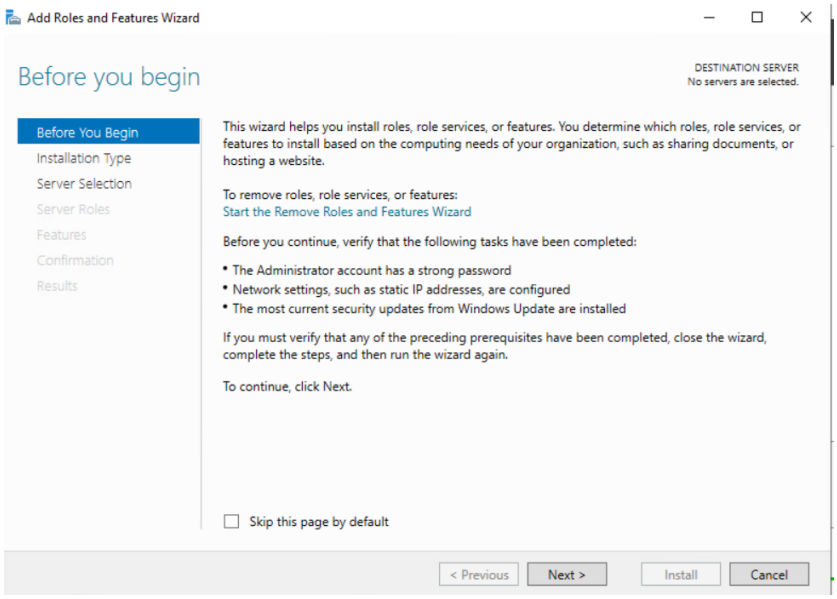
Screenshot of servers added to your server pool

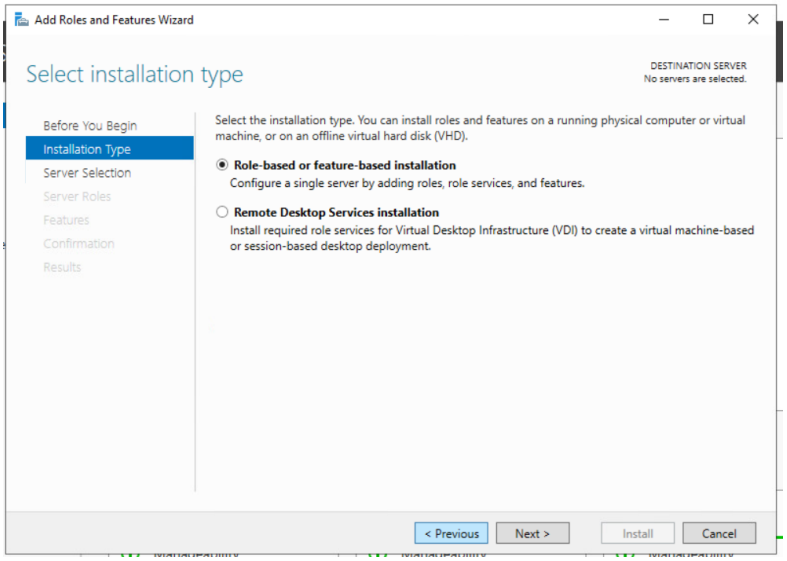
Install the Internet Information Service web server on your ServerGUI:

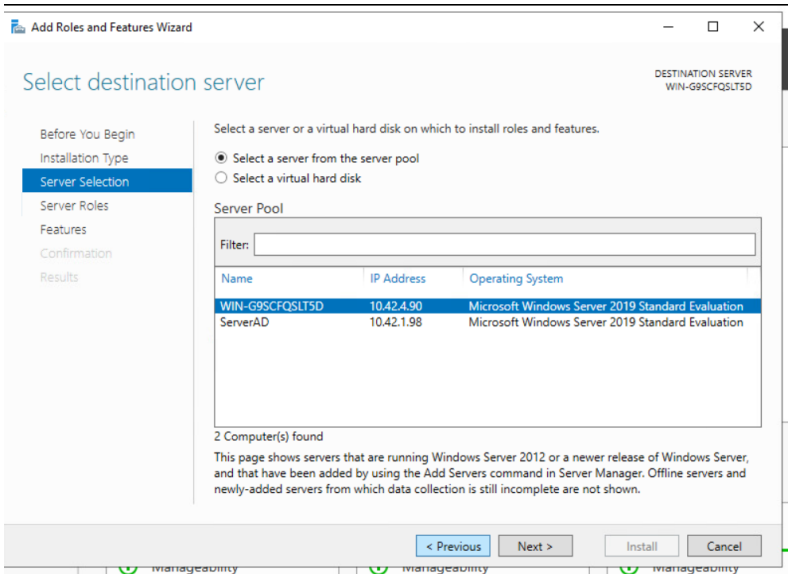
Steps required to set up Internet Information Services:
Select ‘Add roles and features’ from the Dashboard of Server Manager of ServerGUI

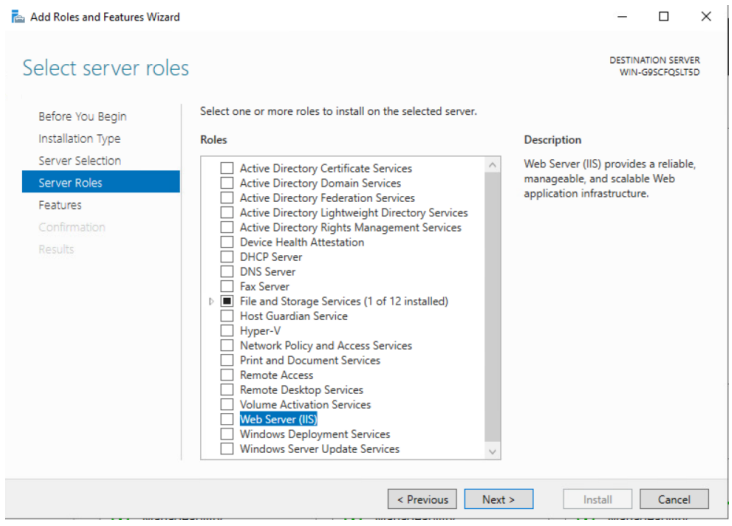


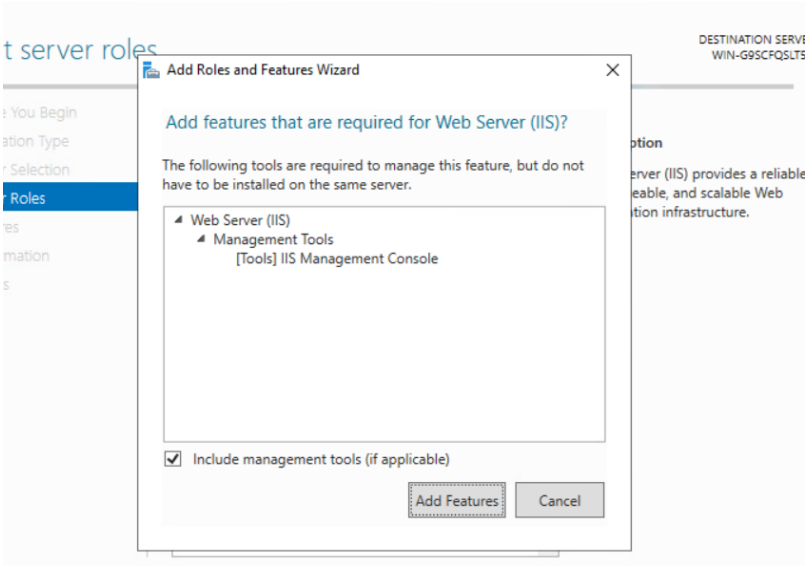
Click ‘Next’ -> Select ‘Role-based or feature-based installation’ for Installation type

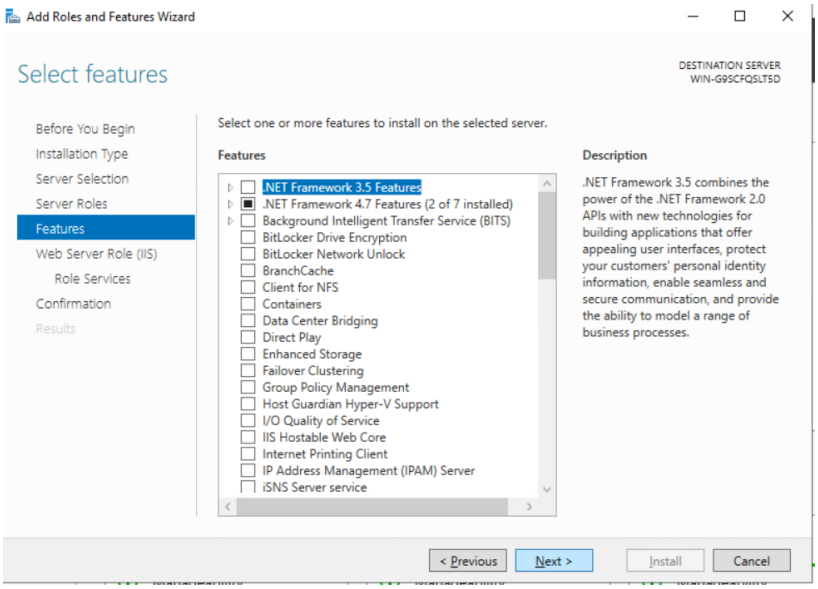


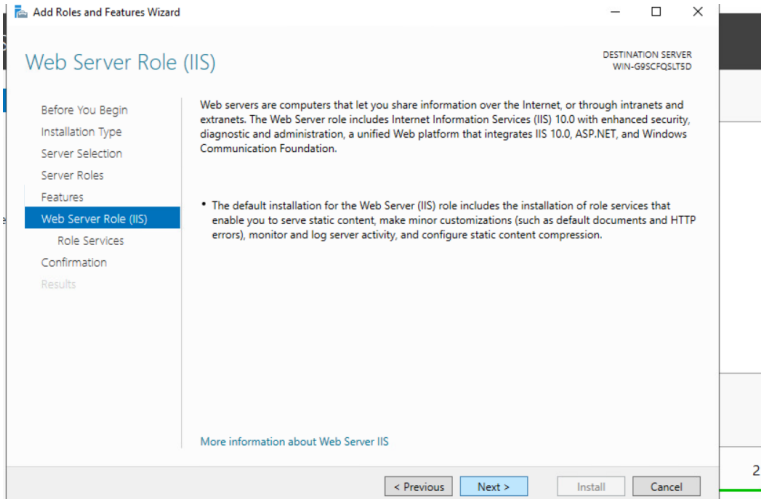


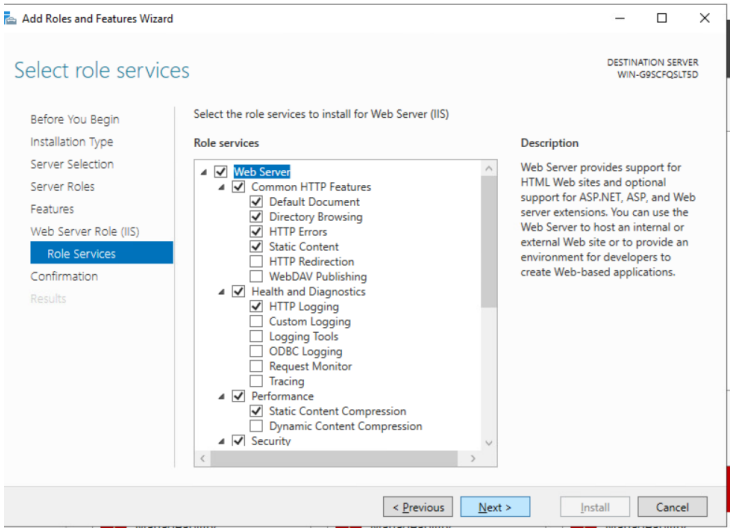

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-G9SCFQSLT5D
10.42.4.90
Microsoft Windows Server 2019 Standard Evaluation
ServerAD
10.42.1.98
Microsoft Windows Server 2019 Standard Evaluation
2 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

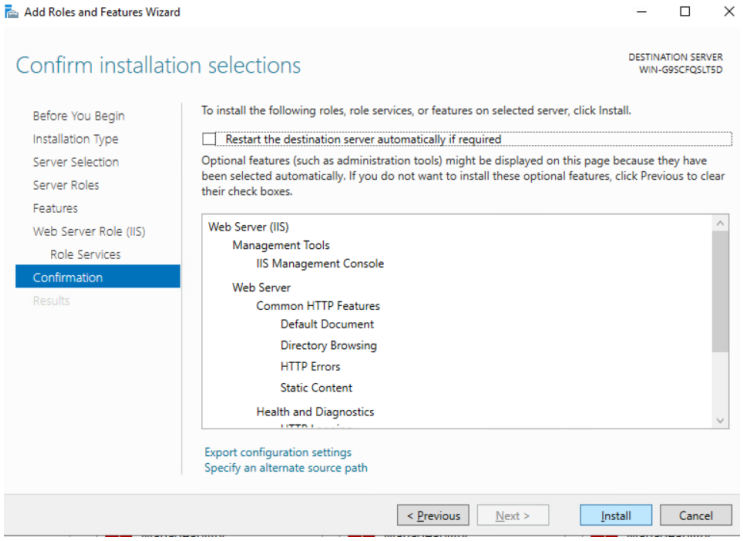

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory 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
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel

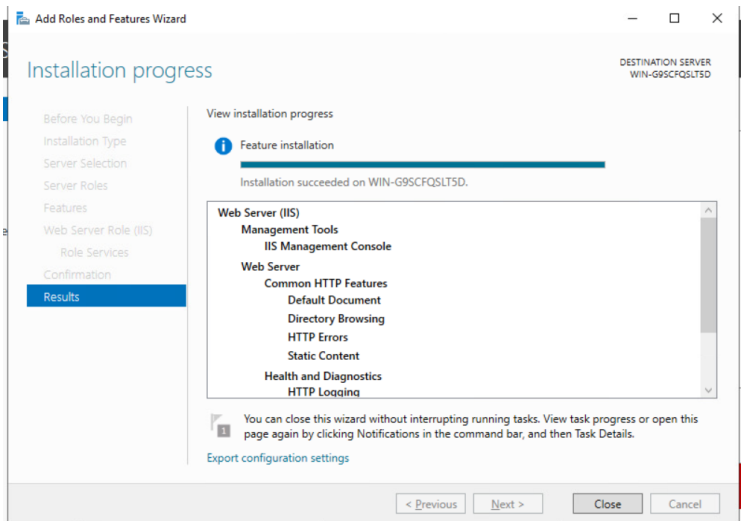

t server roles
DESTINATION SERVE
WIN-G9SCFQSLT5
You Begin
ation Type
Selection
Roles
es
mation
s
ption
erver (IIS) provides a reliable
eable, and scalable Web
tion infrastructure.
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel

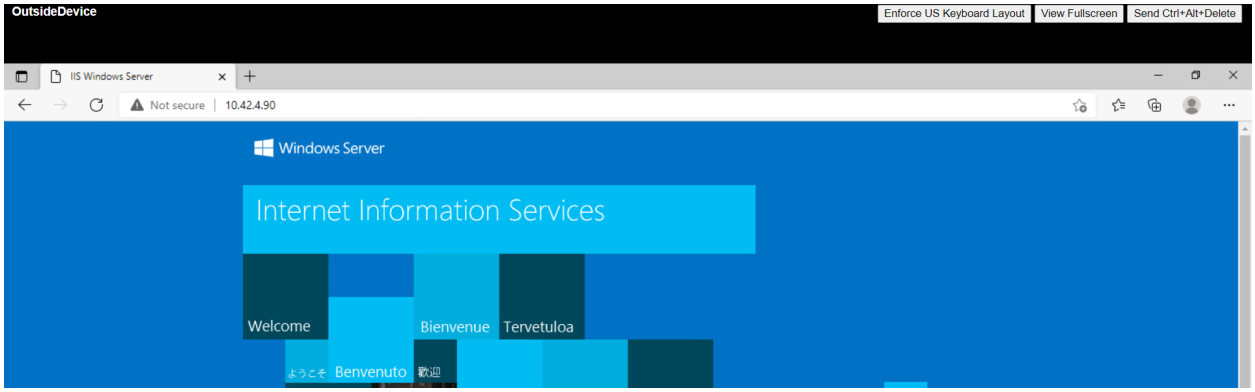

Add Roles and Features Wizard
Select features
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.7 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Web Server Role (IIS)
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.
The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
More information about Web Server IIS
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

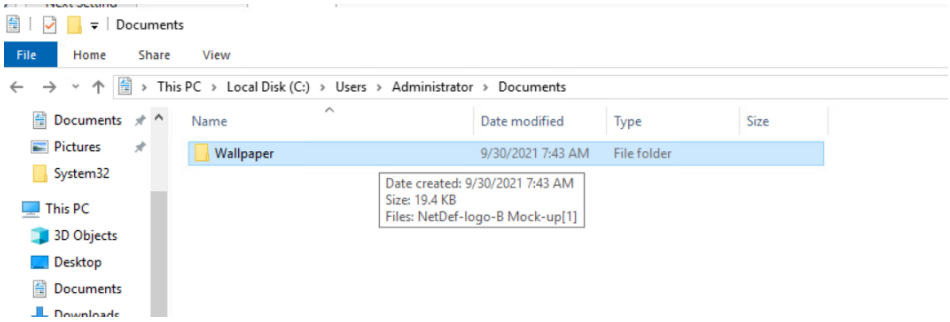

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-G9SCFQSLT5D
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on WIN-G9SCFQSLT5D.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

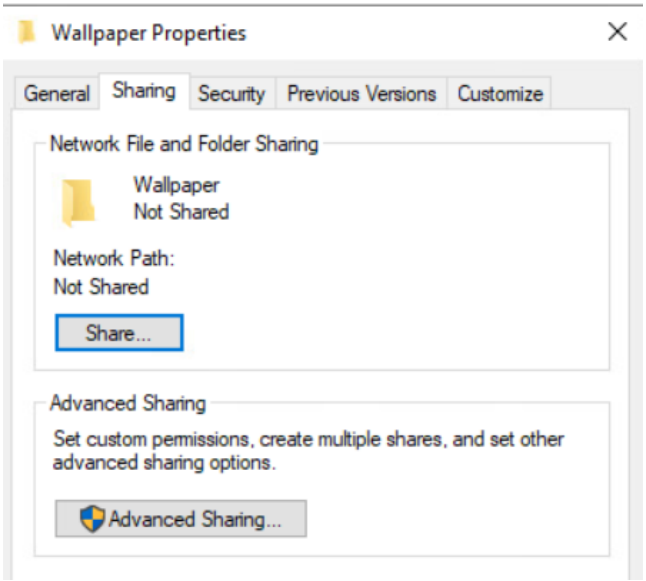


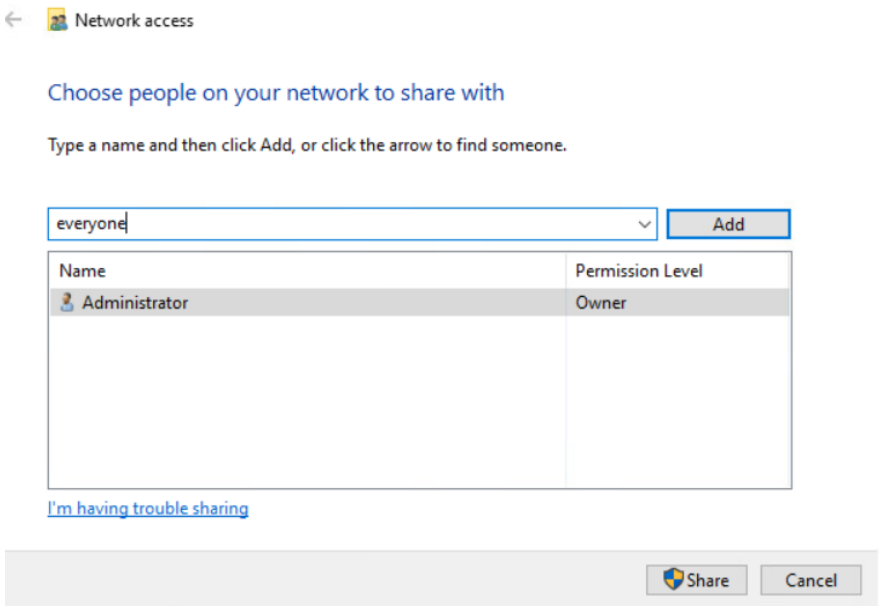
Screenshot of OutsideDevice visiting the webpage hosted by your IIS server

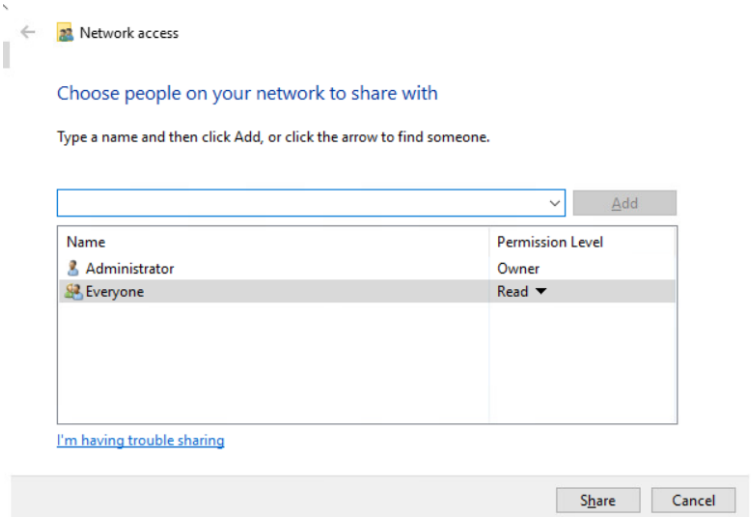
Enforce a background group policy:

Shared folder creation process:

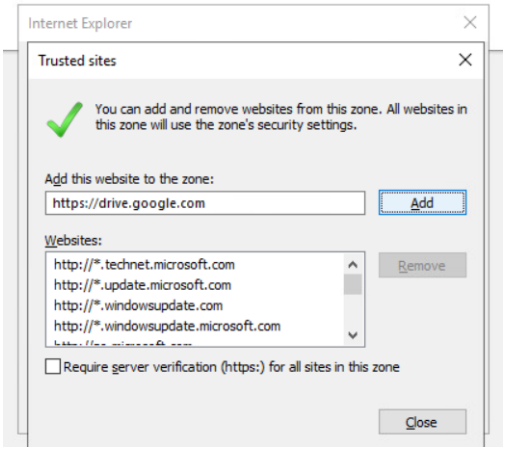


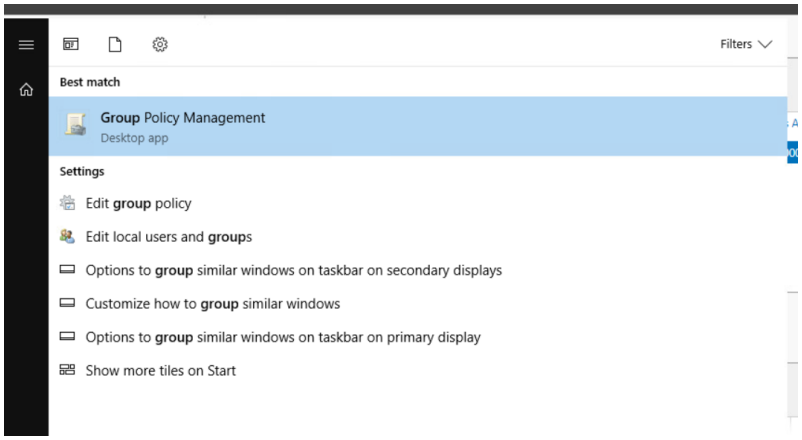


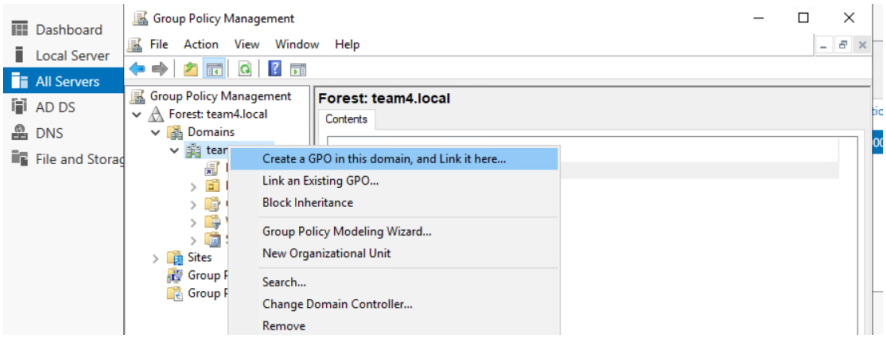


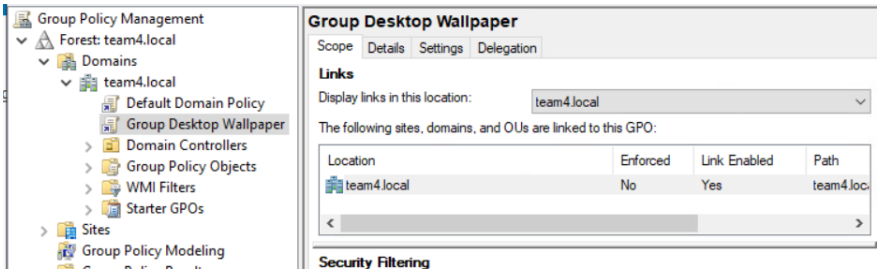


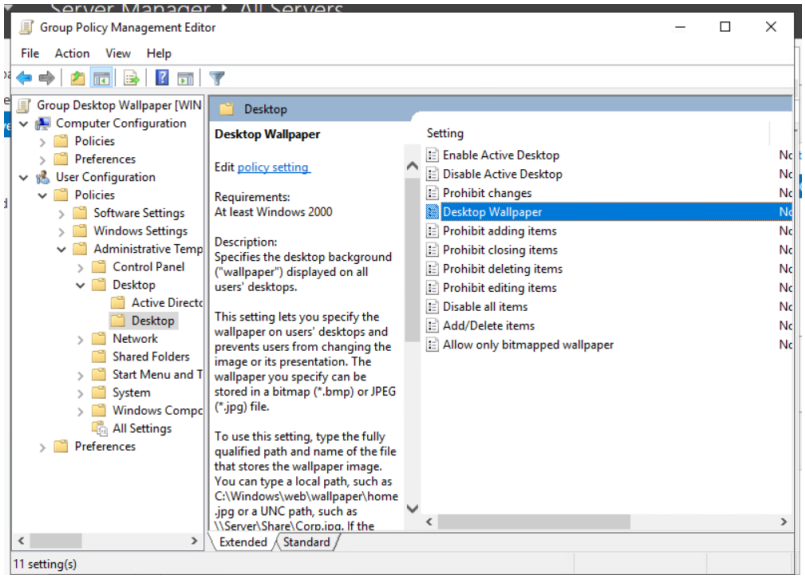
Creation of the background group policy:

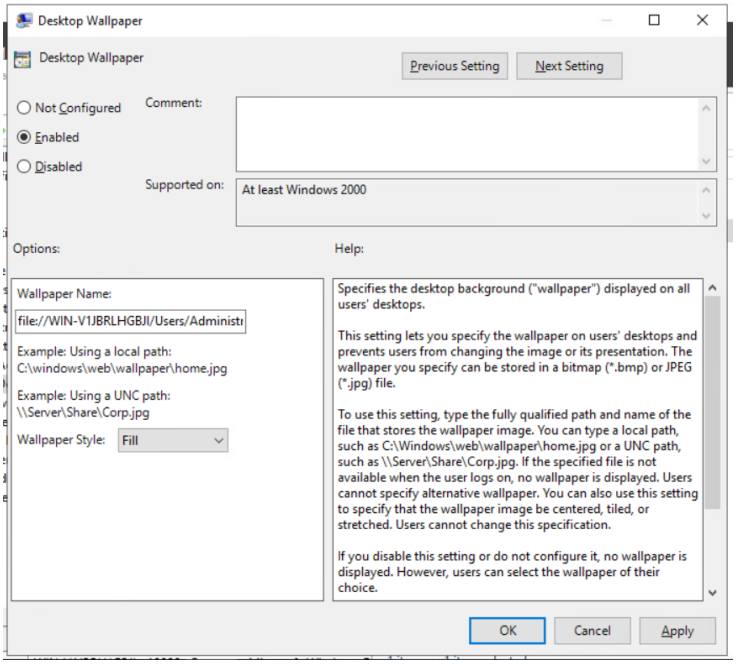



Filters
Best match
Group Policy Management
Desktop app
Settings
Edit group policy
Edit local users and groups
Options to group similar windows on taskbar on secondary displays
Customize how to group similar windows
Options to group similar windows on taskbar on primary display
Show more tiles on Start


Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: team4.local
Domains
Forest: team4.local
Contents
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Sites


Group Policy Management
Forest: team4.local
Domains
team4.local
Default Domain Policy
Group Desktop Wallpaper
Domain Controllers
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Desktop Wallpaper
Scope Details Settings Delegation
Links
Display links in this location: team4.local
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
team4.local No Yes team4.loc
Security Filtering


Group Policy Management Editor
File Action View Help
Group Desktop Wallpaper [WIN
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Active Directc
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
Desktop
Desktop Wallpaper
Edit policy setting
Requirements:
At least Windows 2000
Description:
Specifies the desktop background ("wallpaper") displayed on all users' desktops.
This setting lets you specify the wallpaper on users' desktops and prevents users from changing the image or its presentation. The wallpaper you specify can be stored in a bitmap (*.bmp) or JPEG (*.jpg) file.
To use this setting, type the fully qualified path and name of the file that stores the wallpaper image. You can type a local path, such as C:\Windows\web\wallpaper\home.jpg or a UNC path, such as \\Server\Share\Corp.jpg. If the
Setting
Enable Active Desktop
Disable Active Desktop
Prohibit changes
Desktop Wallpaper
Prohibit adding items
Prohibit closing items
Prohibit deleting items
Prohibit editing items
Disable all items
Add/Delete items
Allow only bitmapped wallpaper
Extended Standard
11 setting(s)



Backgrounds after group policy:

Setup PowerShell transcription using group policy:

Group policy creation process:

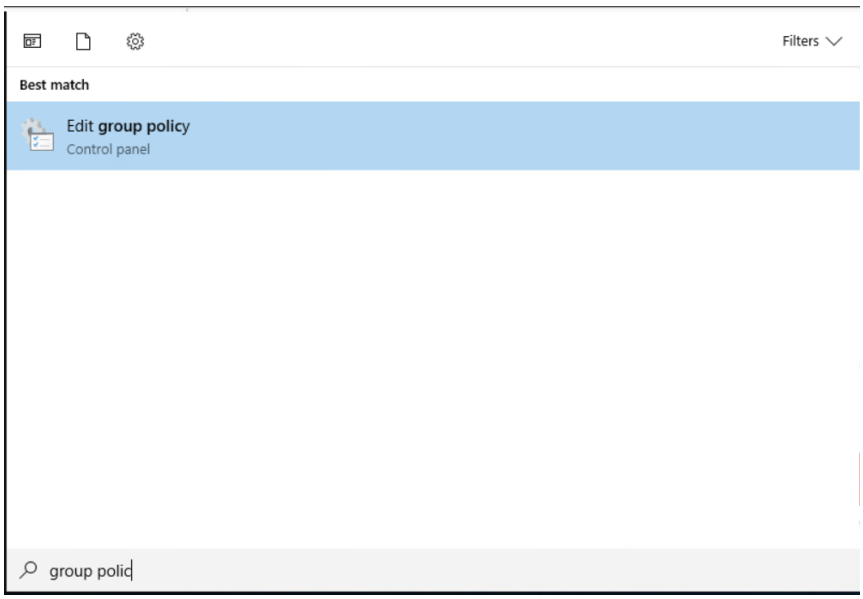
Search for ‘Edit Group Policy’ and Click

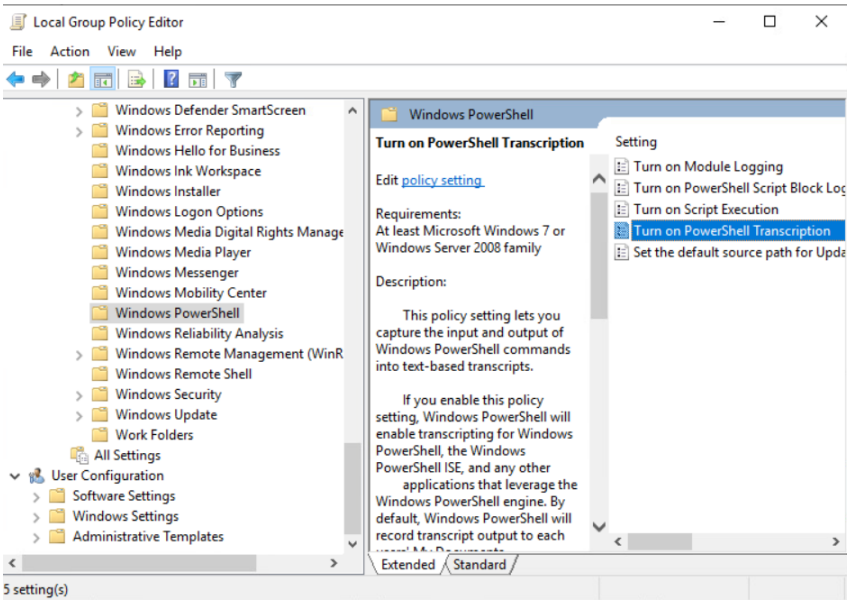
Navigate to Computer Configuration –> Administrative Templates –> Windows Components –> Windows PowerShell and Double-click on “Turn on PowerShell Transcription”

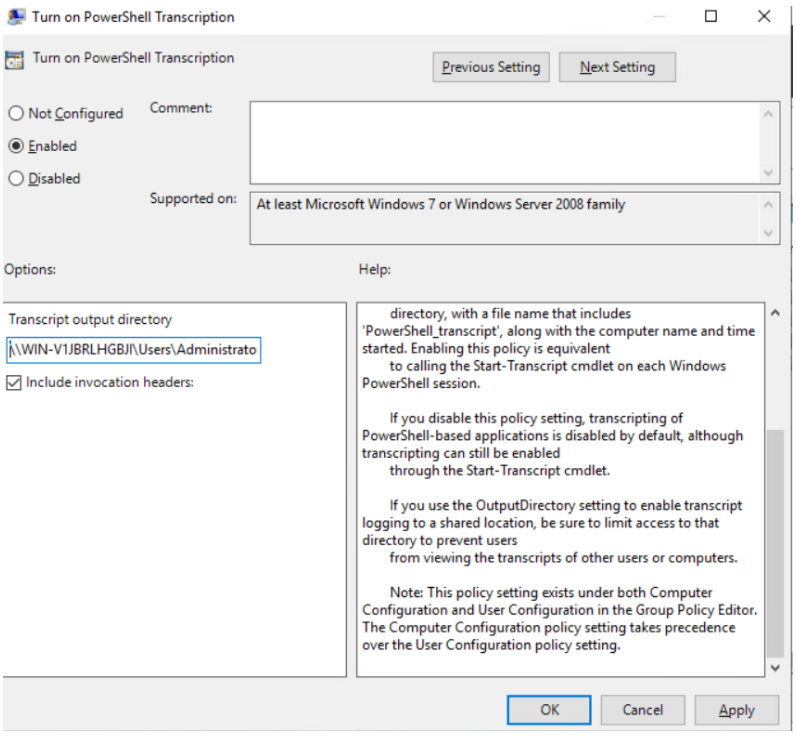
Click on Enable and enter your prefered Output Directory. You can also activate “Include invocation headers” to enable timestamps

Set a centralized transcript output directory as //WIN-V1JBRLHGBJI\Users\Administrator\Documents

And enforce gpupdate /force in cmd to update changes

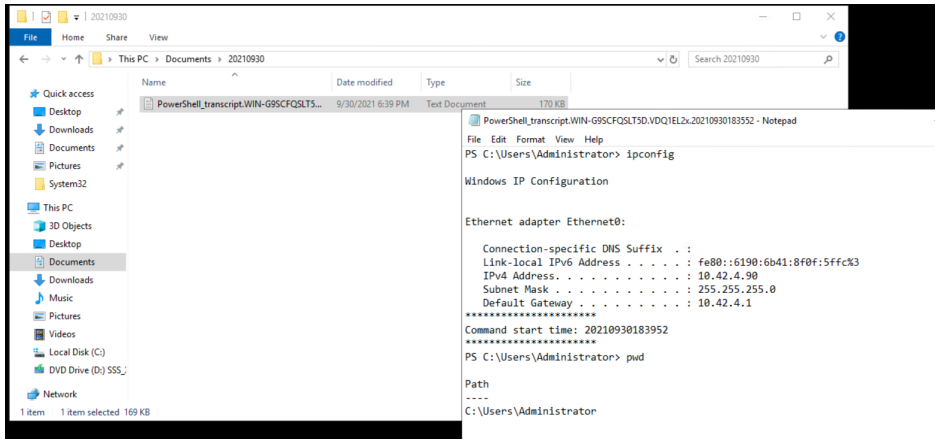



Local Group Policy Editor
File Action View Help
Windows Defender SmartScreen
Windows Error Reporting
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights Manage
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management (WinR
Windows Remote Shell
Windows Security
Windows Update
Work Folders
All Settings
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows PowerShell
Turn on PowerShell Transcription
Edit policy setting
Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family
Description:
This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.
If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each
Setting
Turn on Module Logging
Turn on PowerShell Script Block Log
Turn on Script Execution
Turn on PowerShell Transcription
Set the default source path for Upda
Extended Standard
5 setting(s)


Turn on PowerShell Transcription
Turn on PowerShell Transcription
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
Transcript output directory
\\WIN-V1JBRLHGBJI\Users\Administrato
Include invocation headers:
directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.
If you disable this policy setting, transcripting of PowerShell-based applications is disabled by default, although transcripting can still be enabled through the Start-Transcript cmdlet.
If you use the OutputDirectory setting to enable transcript logging to a shared location, be sure to limit access to that directory to prevent users from viewing the transcripts of other users or computers.
Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.
OK
Cancel
Apply

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>
```

```
PS C:\Users\Administrator> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=14ms TTL=112
Reply from 8.8.8.8: bytes=32 time=14ms TTL=112
Reply from 8.8.8.8: bytes=32 time=13ms TTL=112
Reply from 8.8.8.8: bytes=32 time=13ms TTL=112

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 14ms, Average = 13ms

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6190:6b41:8f0f:5ffc%3
   IPv4 Address. . . . . . . . . . . : 10.42.4.90
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.42.4.1

PS C:\Users\Administrator>
```



Screenshot of the PowerShell transcript created

Updated Topology: