SANGFOR

IAM

Praktik Terbaik untuk Skenario_Aktivitas Domain Script SSO

Versi 12.0.42

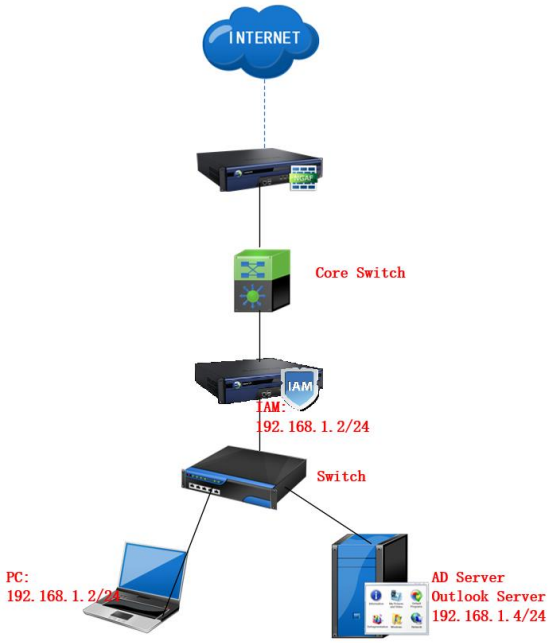
Catatan Perubahan

Tanggal	Deskripsi Perubahan
Agustus 4, 2020	Rilis Dokumen Versi 12.0.42.
Mei 17, 2021	Dokumen update Versi 12.0.42.

Daftar Isi

Bab 1 Skenario

Pelanggan menggunakan Microsoft AD server untuk mengelola pengguna intranet. Semua pengguna akhir adalah sistem Windows. Aplikasi kantor klien sebagian besar adalah aplikasi dari perusahaan Microsoft seperti Outlook; pelanggan ingin kontrol pengguna intranet dan memerlukan visualisasi kontrol, artinya, spesifik domain dapat dikueri. pengguna dan informasi traffic juga melakukan verifikasi identitas untuk pengguna intranet. Mengintegrasikan semua kebutuhan pelanggan, dan pada saat yang sama, pelanggan menggunakan Microsoft AD domain untuk mengelola pengguna. Diantara beberapa cara mengkombinasikan Microsoft AD domain authentication, script SSO memiliki tingkat keberhasilan tertinggi. Pelanggan diizinkan untuk mengirimkan skrip melalui Microsoft AD domain dan memerlukan tingkat keberhasilan SSO yang lebih tinggi, jadi pilih untuk menggunakan script SSO.



AD Server:

IP: 192.168.1.4

Domain Name: sangfor.com

Account/Password: administrator/@sangfor123

Test PC:

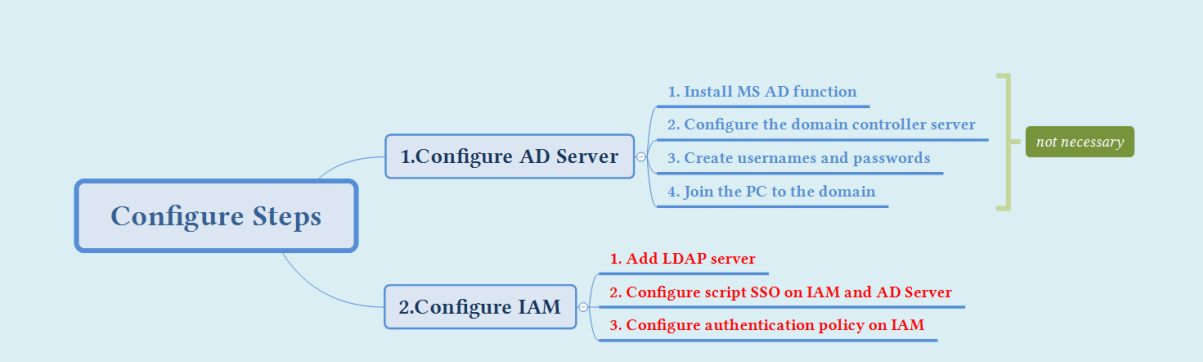
IP: 192.168.1.3

Account/Password: administrator/@sangfor123

Domain Account/Password: sangfortest/@sangfor123

1.1 Langkah Konfigurasi

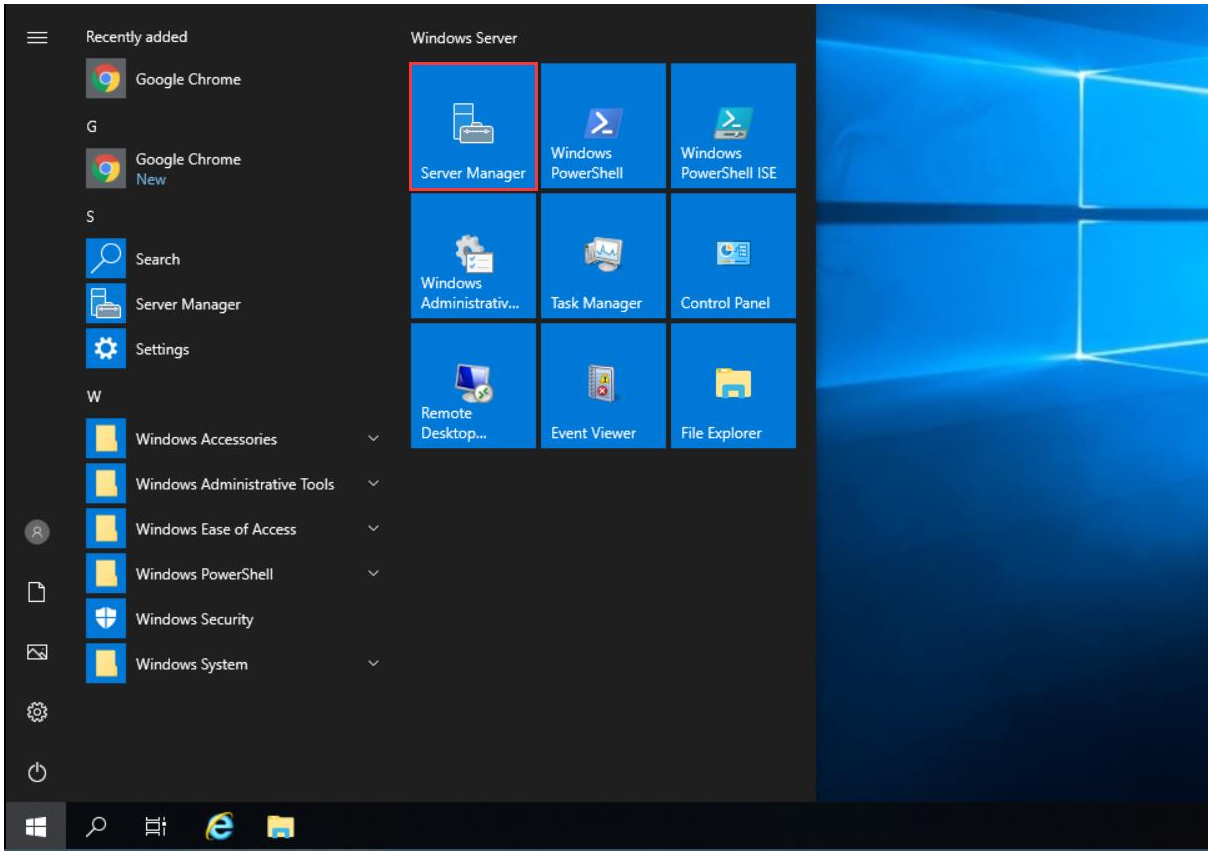
Langkah konfigurasi seperti yang ditunjukkan pada gambar di bawah ini. Perlu dicatat bahwa untuk membuat semua orang terbiasa dengan AD domain lebih cepat, kami menambahkan metode konfigurasi AD domain, yang merupakan bagian yang ditandai"tidak perlu". Jika pelanggan telah menggunakan AD domain sebelumnya dan tidak perlu konfigurasi ulang AD domain, maka hanya perlu konfigurasi bagian lain.



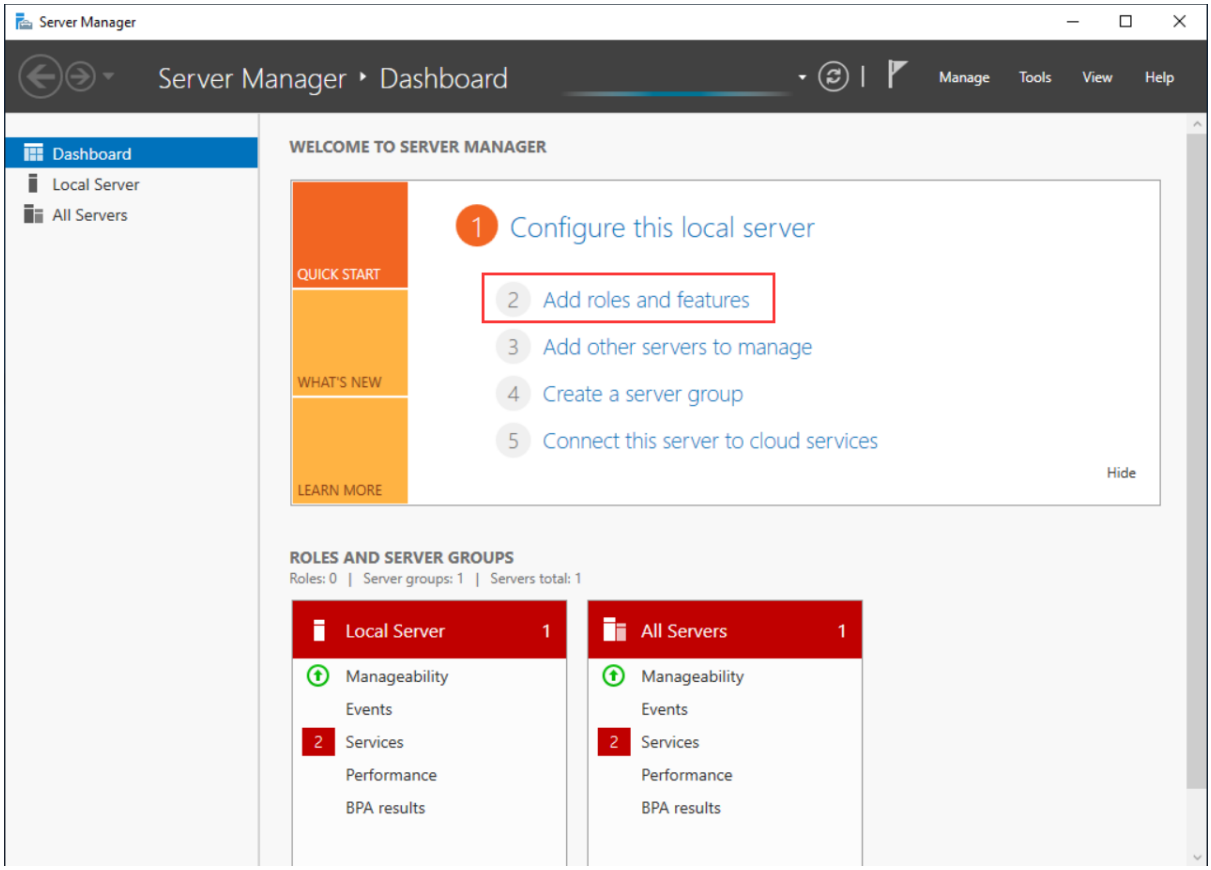
Bab 2 Bagaimana untuk Konfigurasi Aktivitas Domain Server

2.1 Instal fungsi MS AD

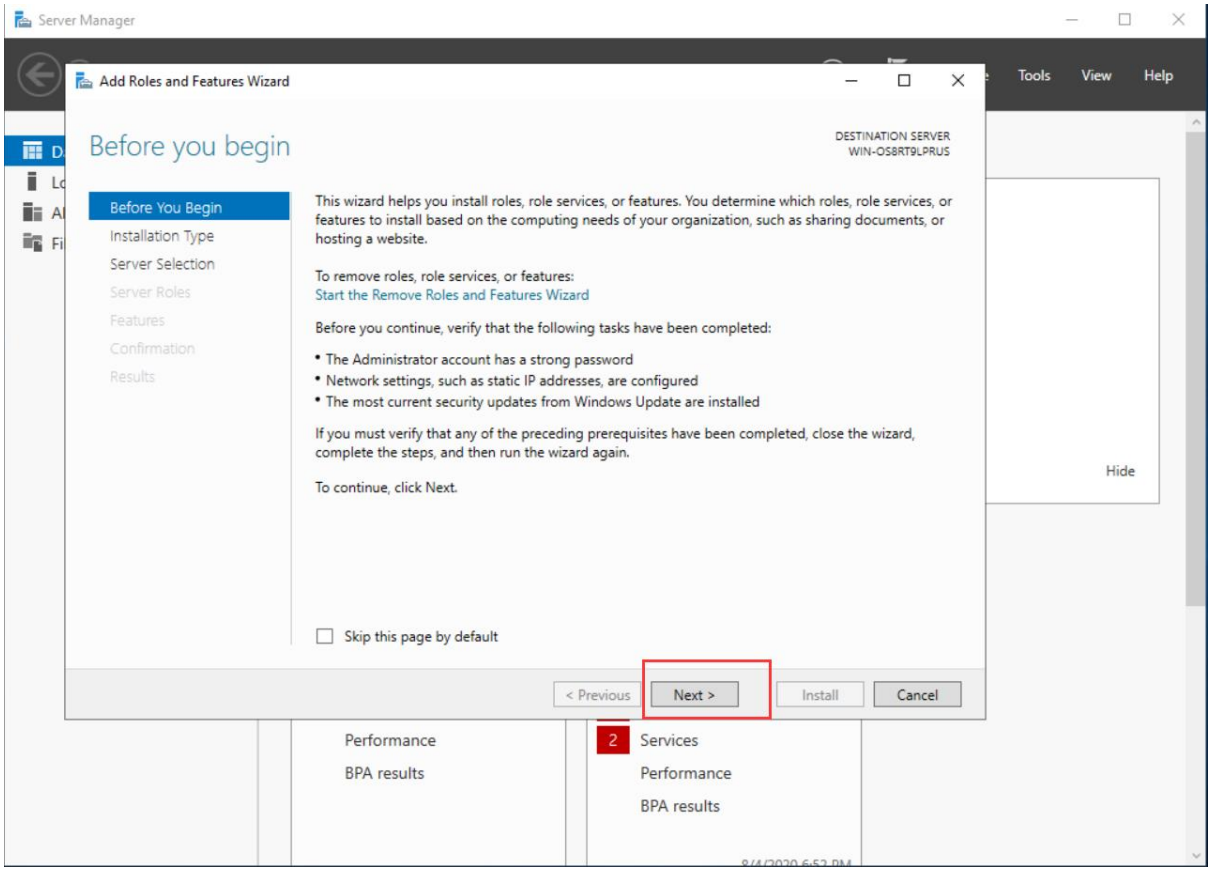
1. Buka Server Manager pada Windows Server 2019.



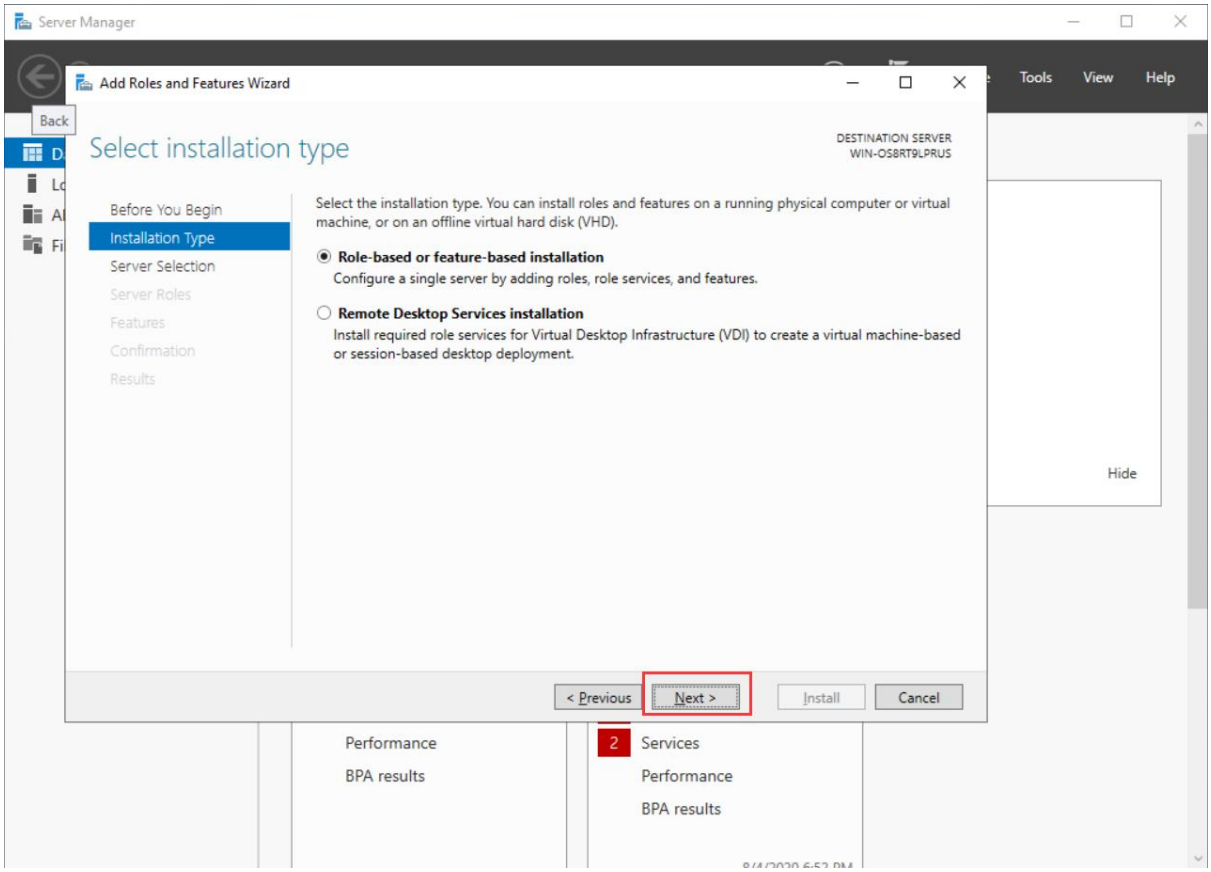
2.Klik "Add roles and features".



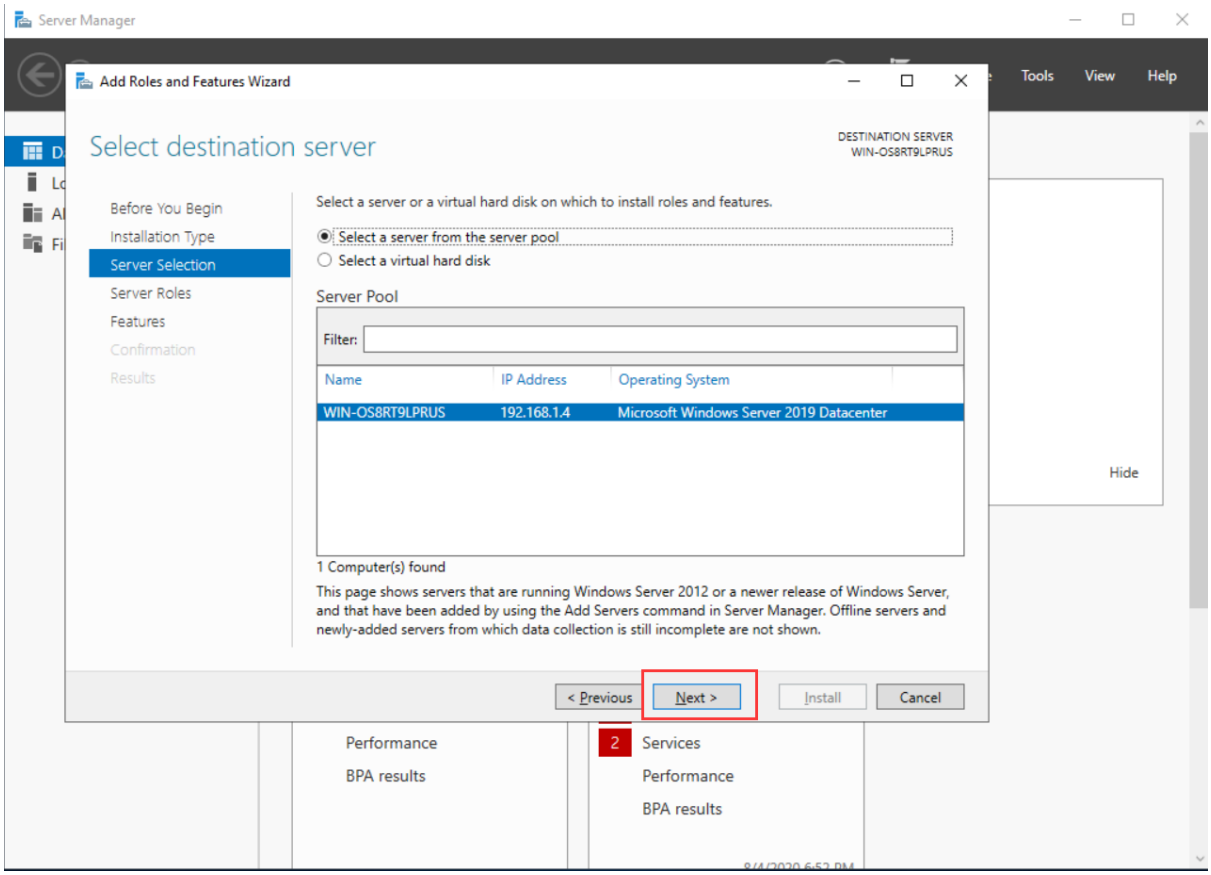
3.Klik "Next".



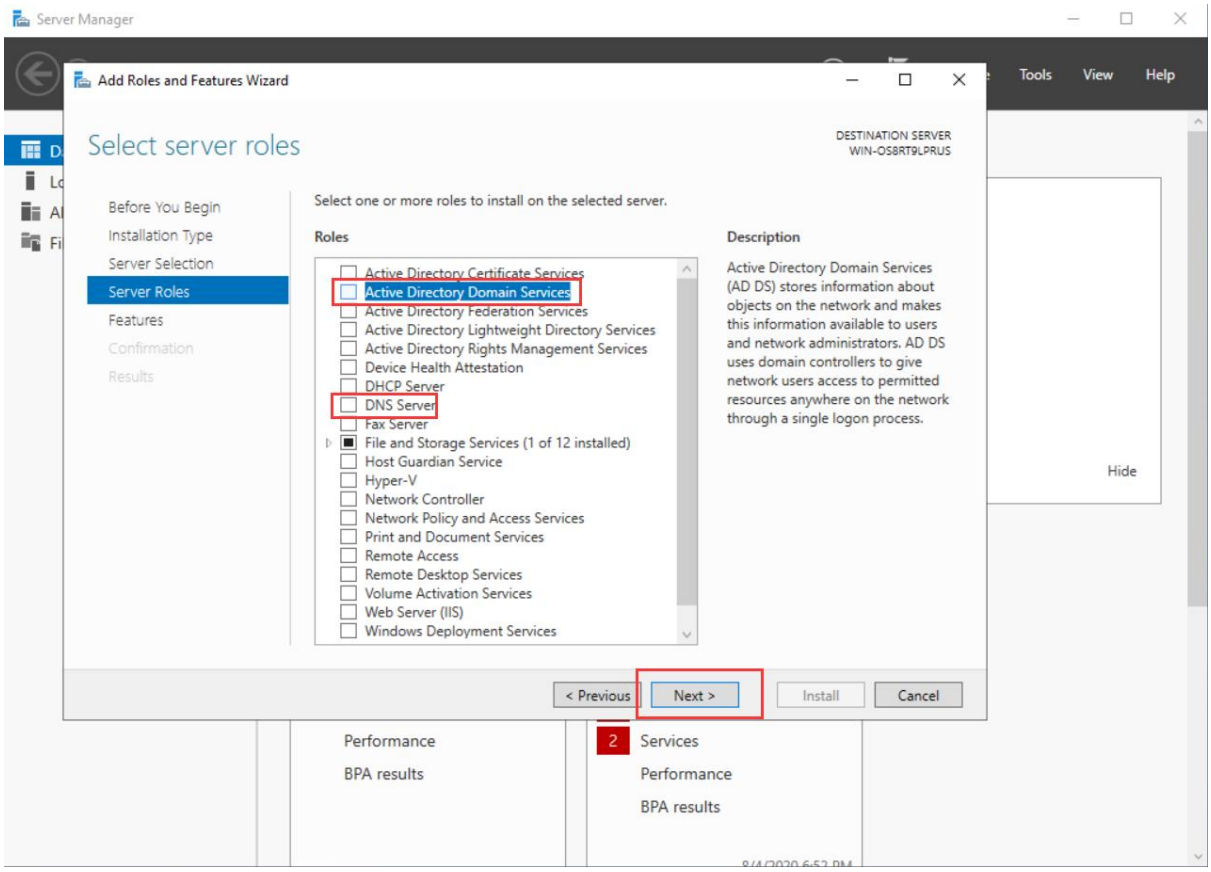
4. Klik "Next".

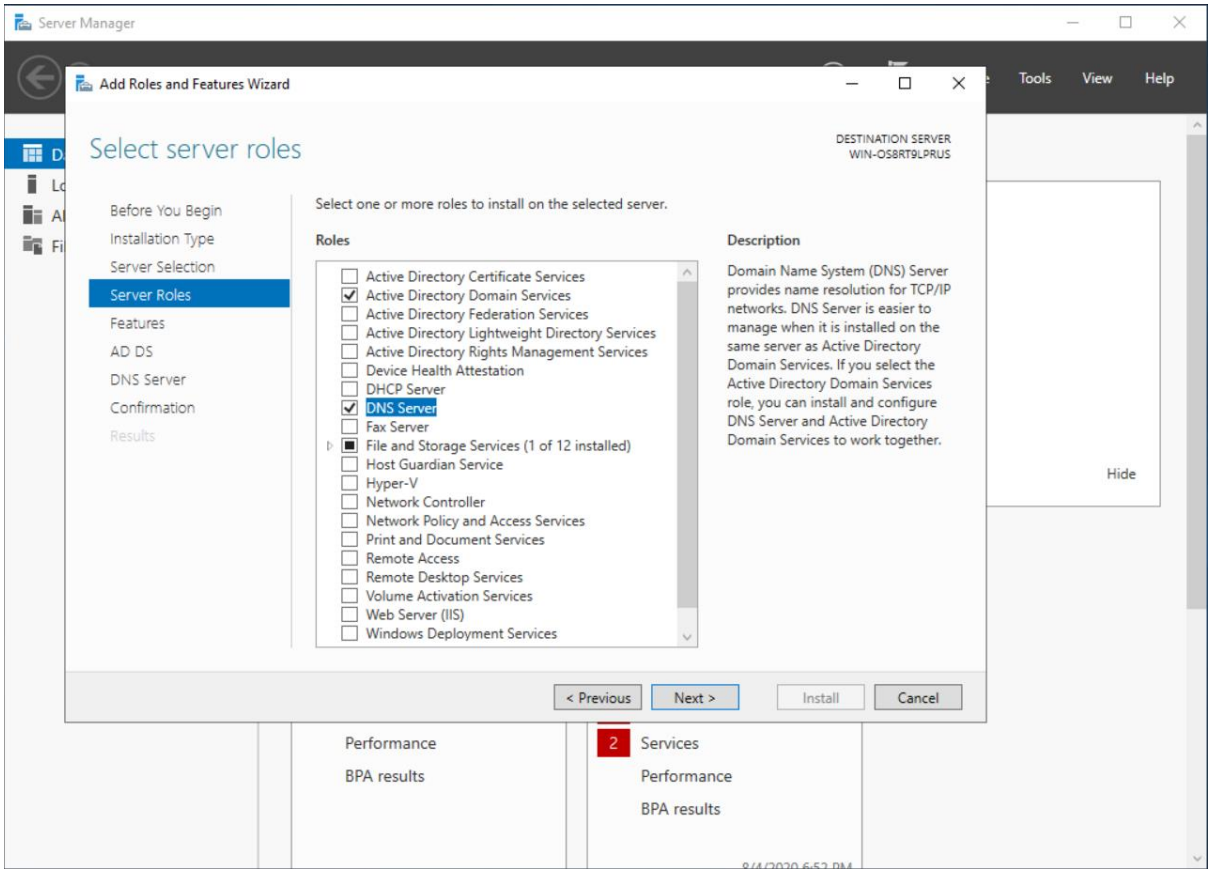

Server Manager
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
Services
Performance
BPA results

5. Klik "Next".

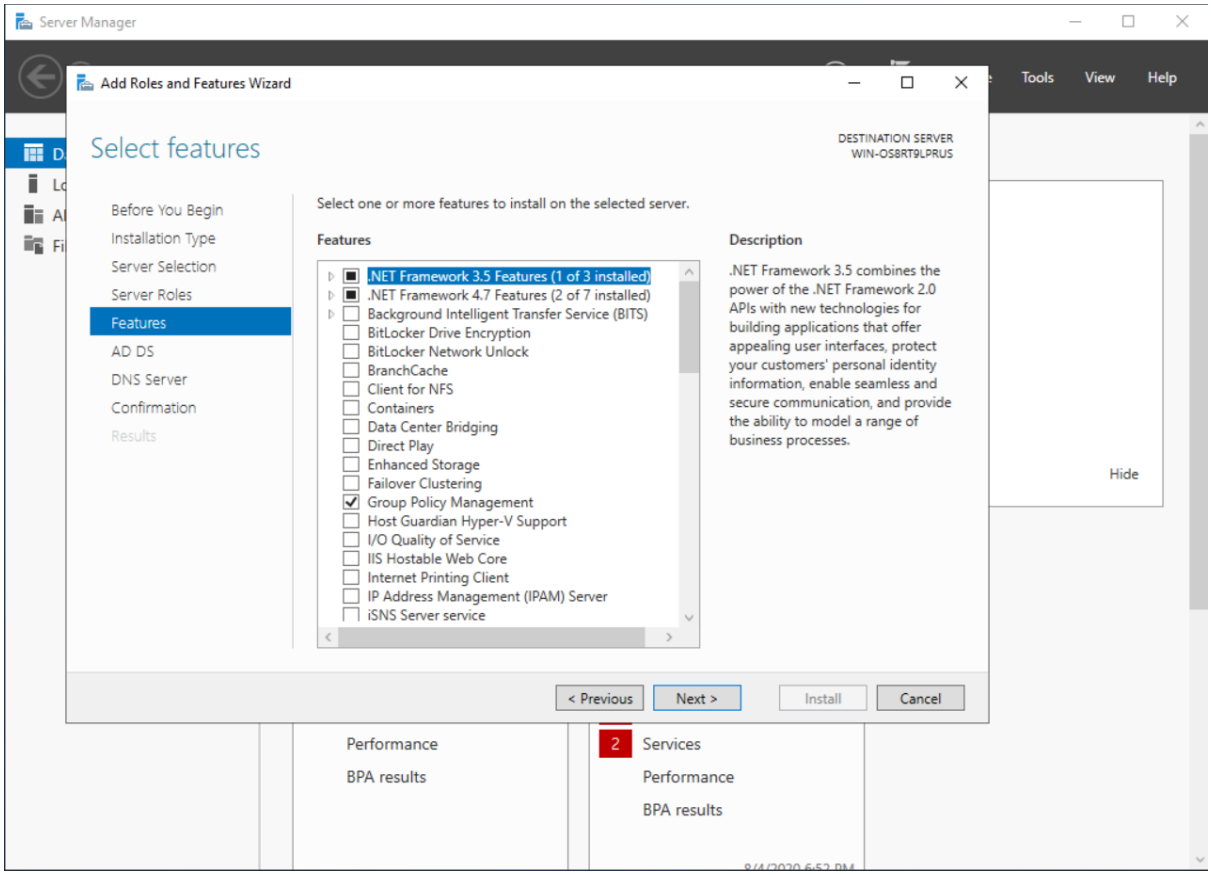

Server Manager
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-OS8RT9LPRUS
192.168.1.4
Microsoft Windows Server 2019 Datacenter
1 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
Tools
View
Help
Hide
Performance
BPA results
Services
Performance
BPA results

6. Pilih fungsi yang perlu diinstal "Active Directory Domain Services" dan "DNS Server", lalu klik "Next".

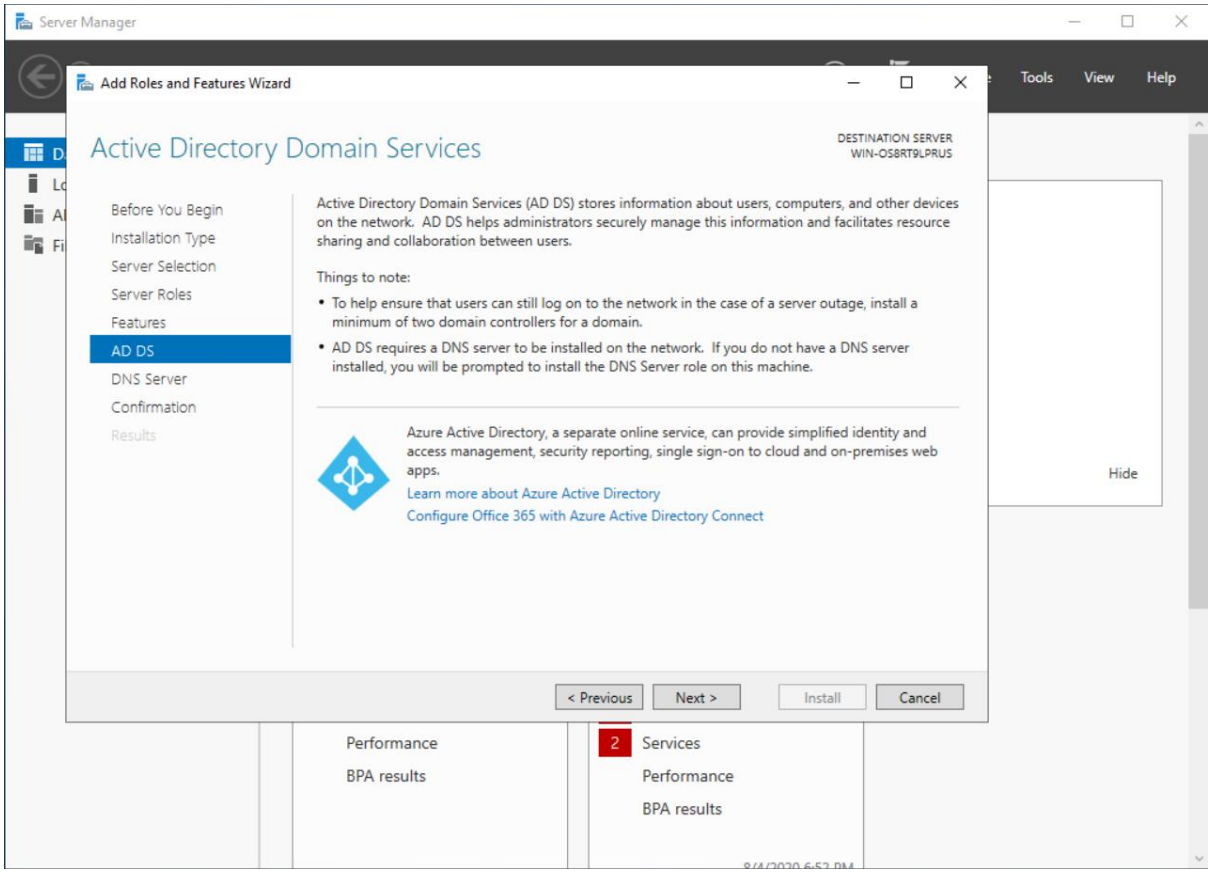



Server Manager
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate 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 Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results

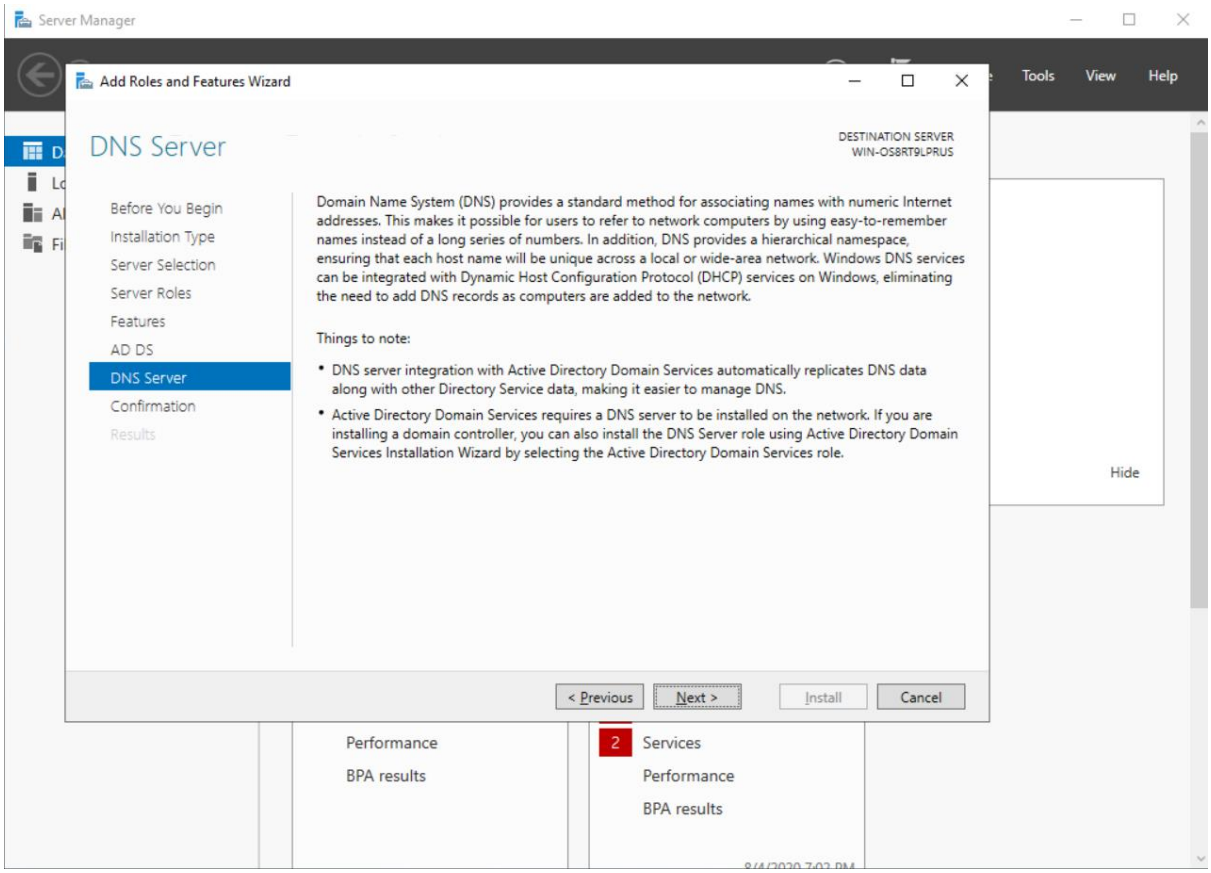
7. Klik "Next".


Server Manager
Add Roles and Features Wizard
Select features
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features (1 of 3 installed)
.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
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results

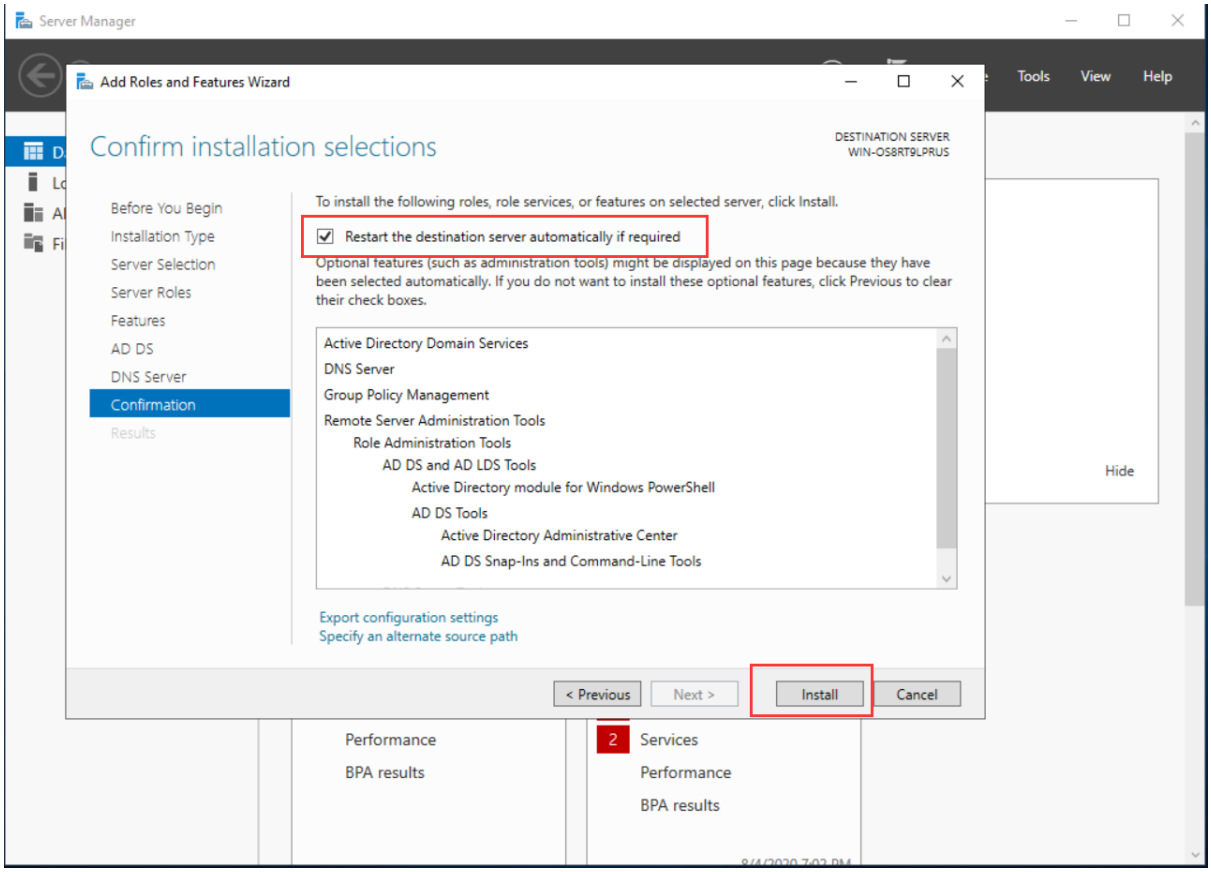
8. Klik "Next".

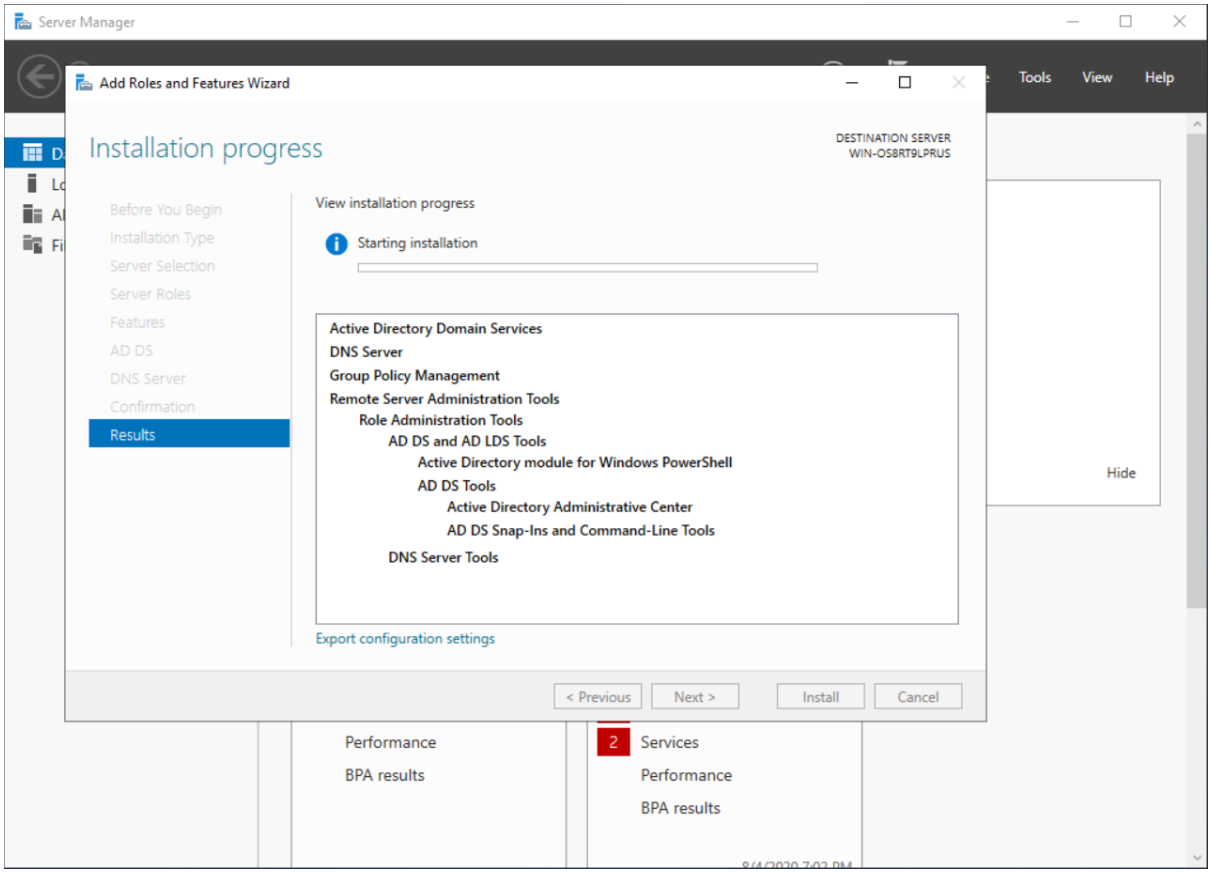


9. Klik "Next".

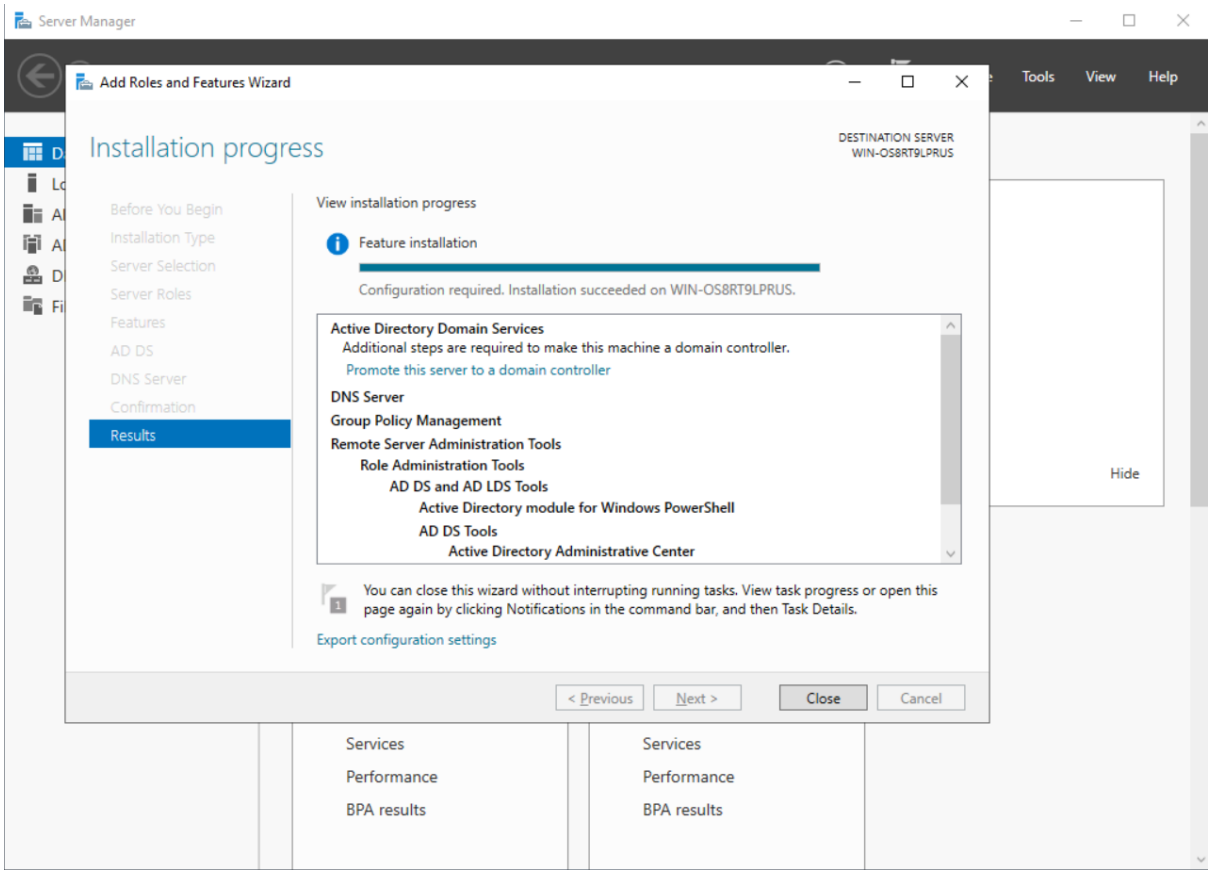


10. Klik "Install".



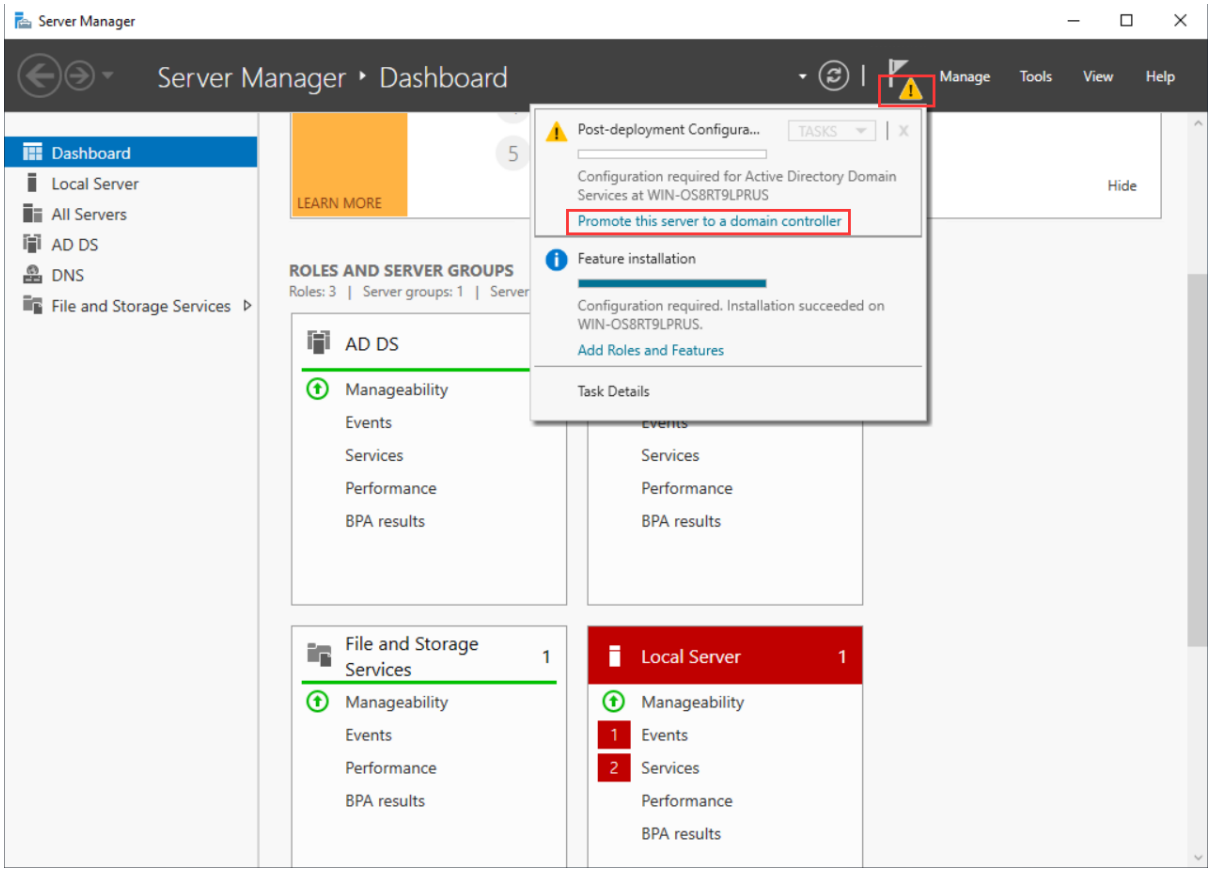


11. Klik "Close" setelah instalasi.

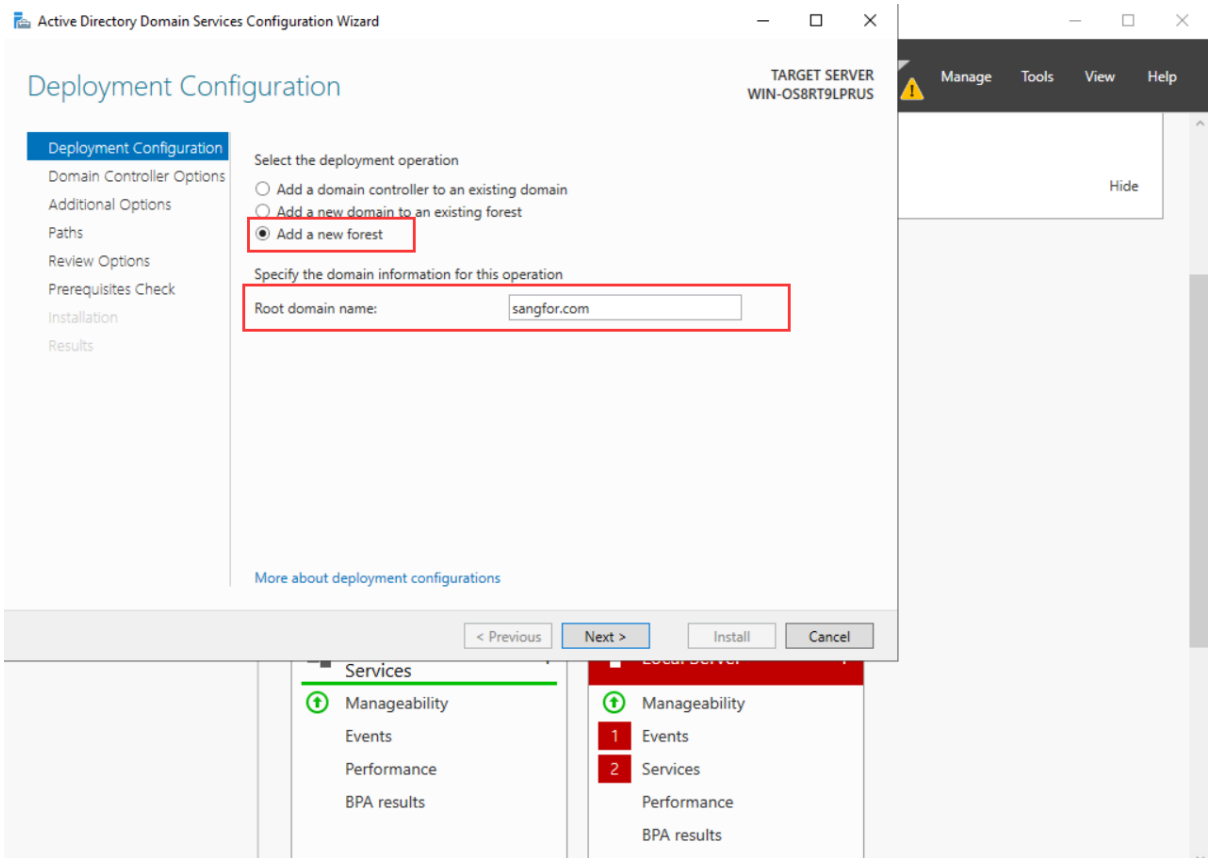


2.2 Konfigurasi domain controller server

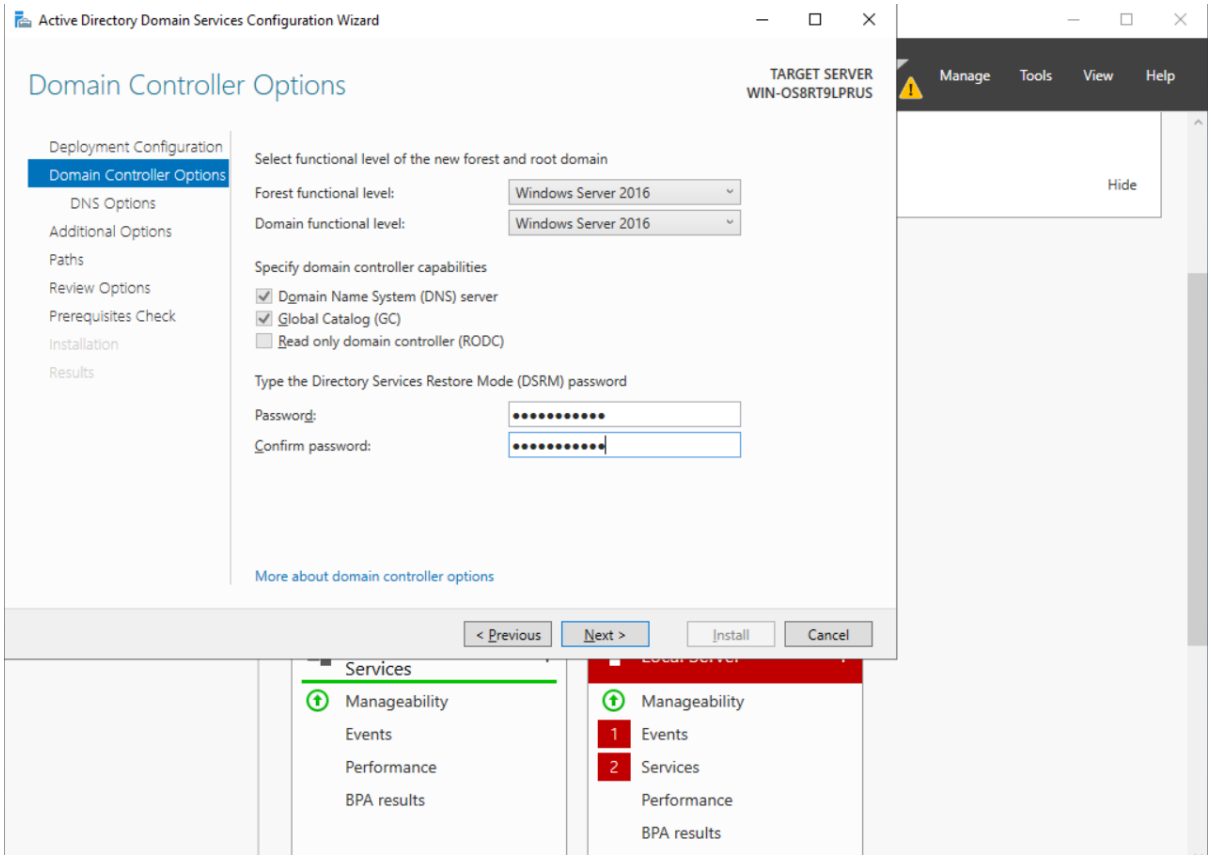
1. Menurut gambar berikut, pilih "Promote this server to a domain controller".



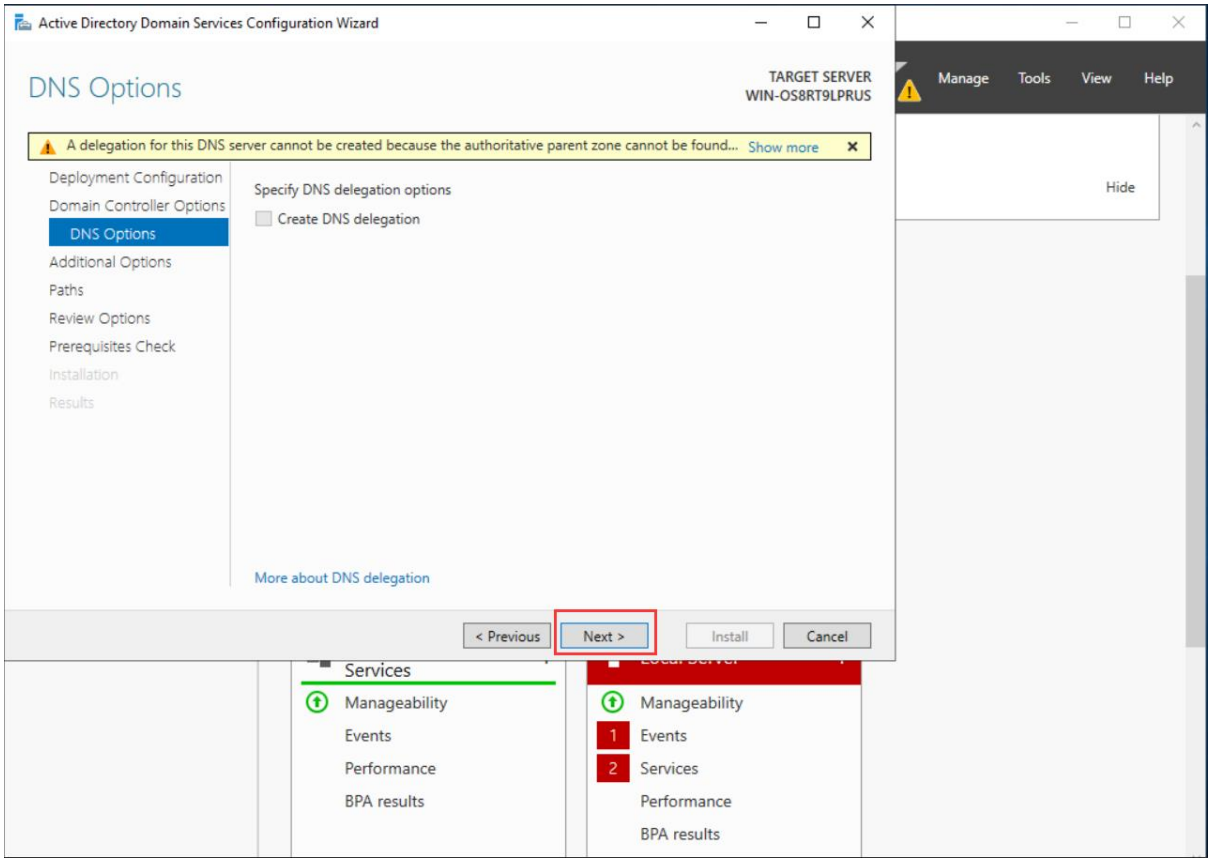
2. Konfigurasi domain name untuk AD domain, seperti sangfor.com.



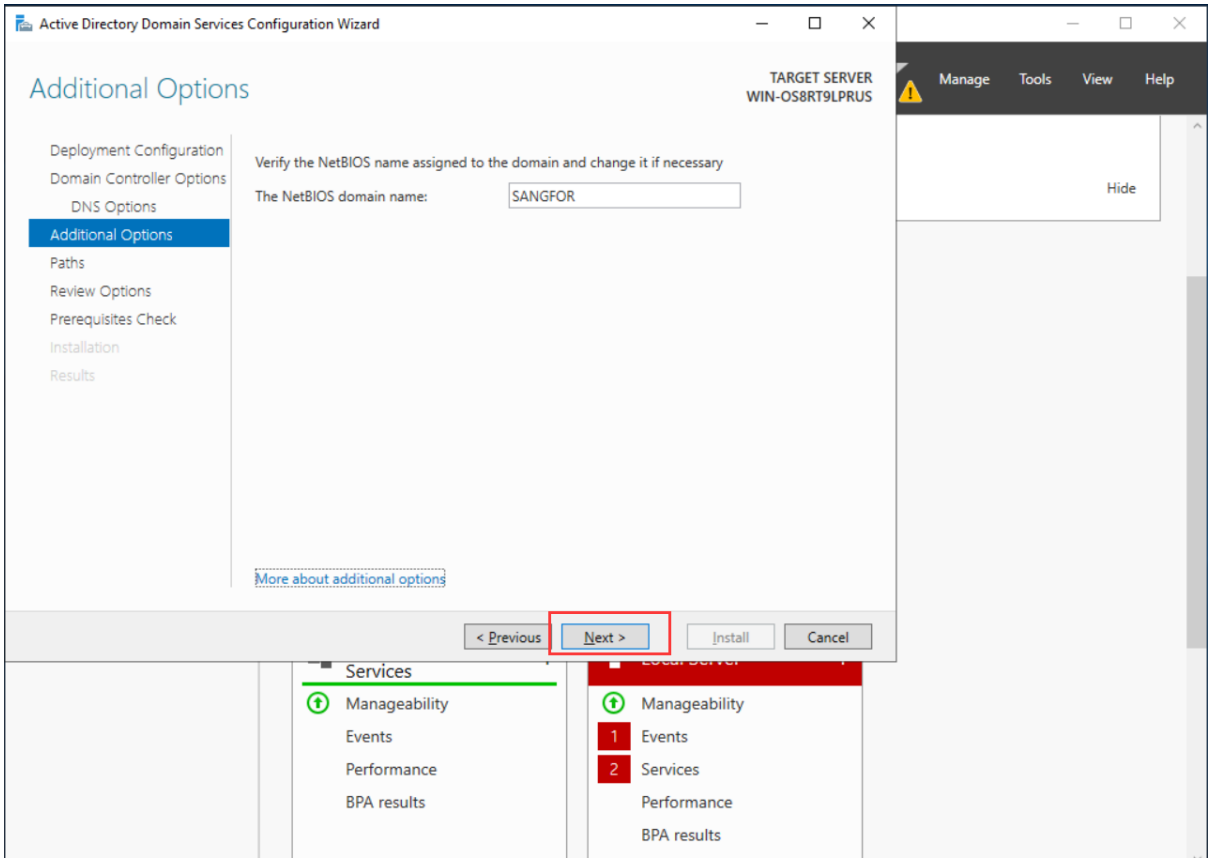
3. Atur password, misalnya @sangfortest.



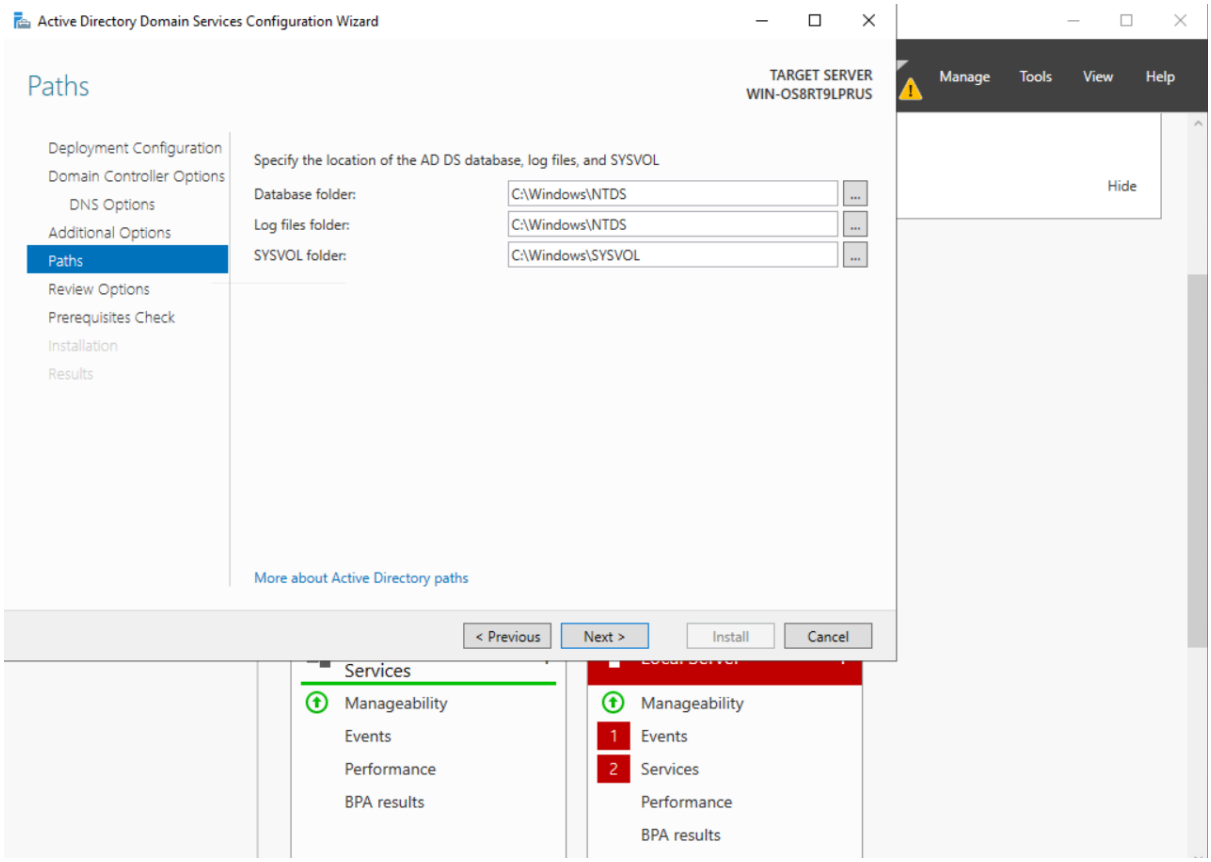
4.Klik "Next".



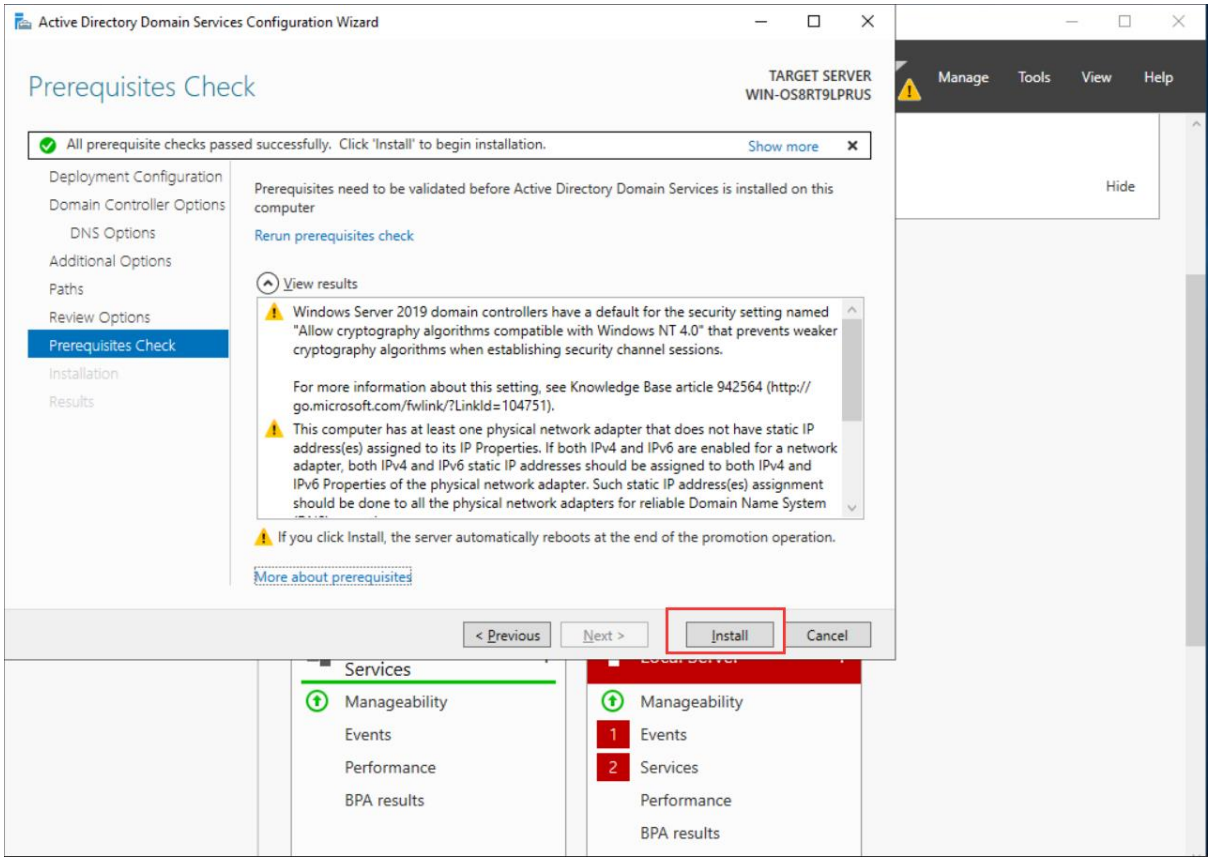
5. Atur NETBIOS Domain Name, Anda dapat menggunakan default SANGFOR.



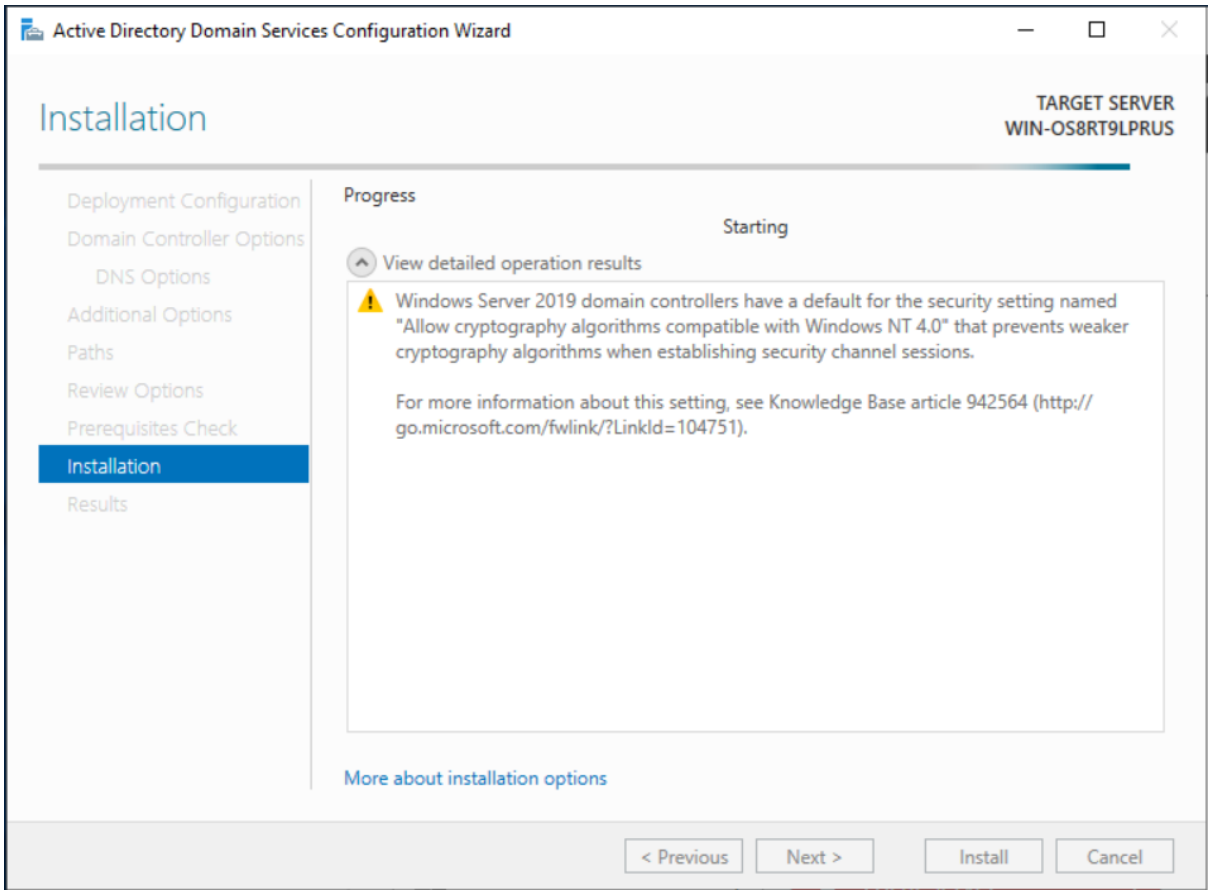
6.Klik "Next".



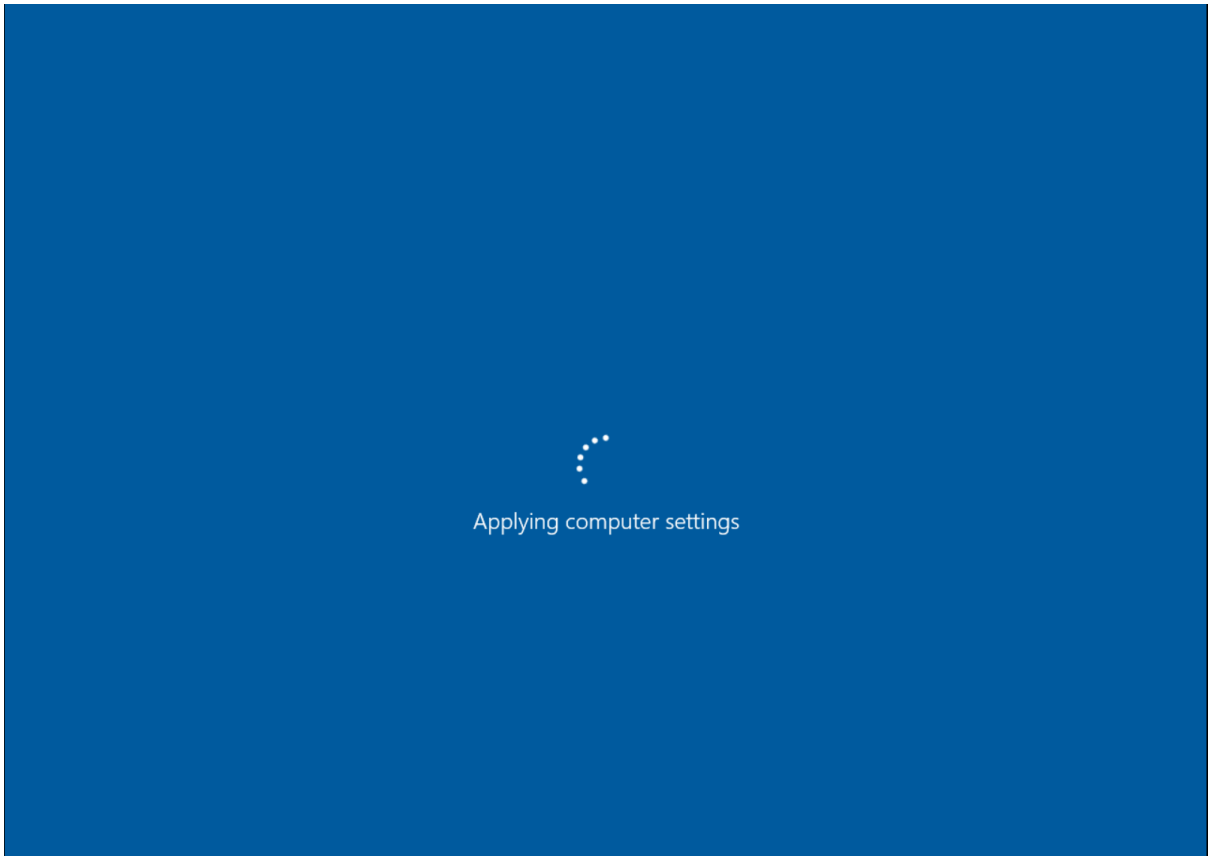
7.Pilih "Install".



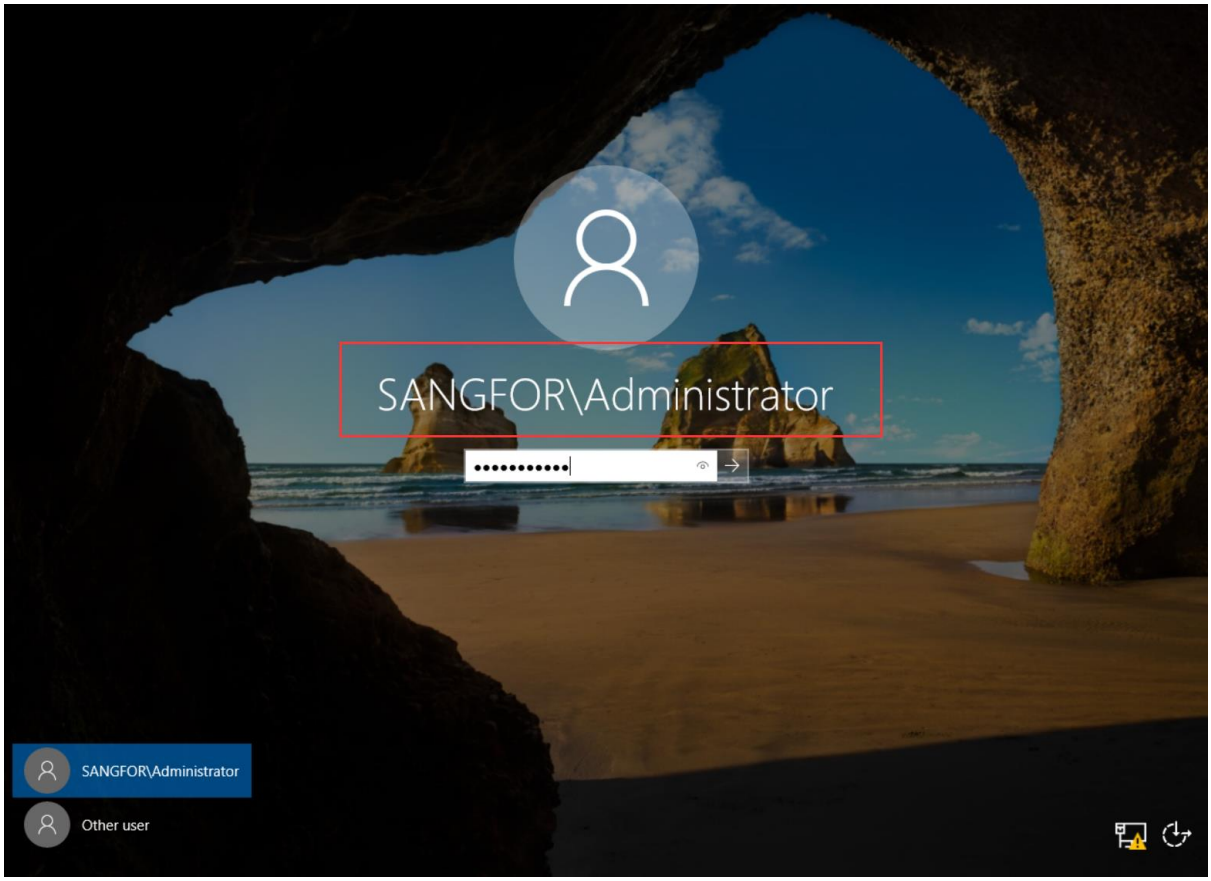
8. Tunggu peralatan untuk instal dan deploy fungsi yang berhubungan.



9. Setelah instalasi selesai, Windows Server secara otomatis akan restart.

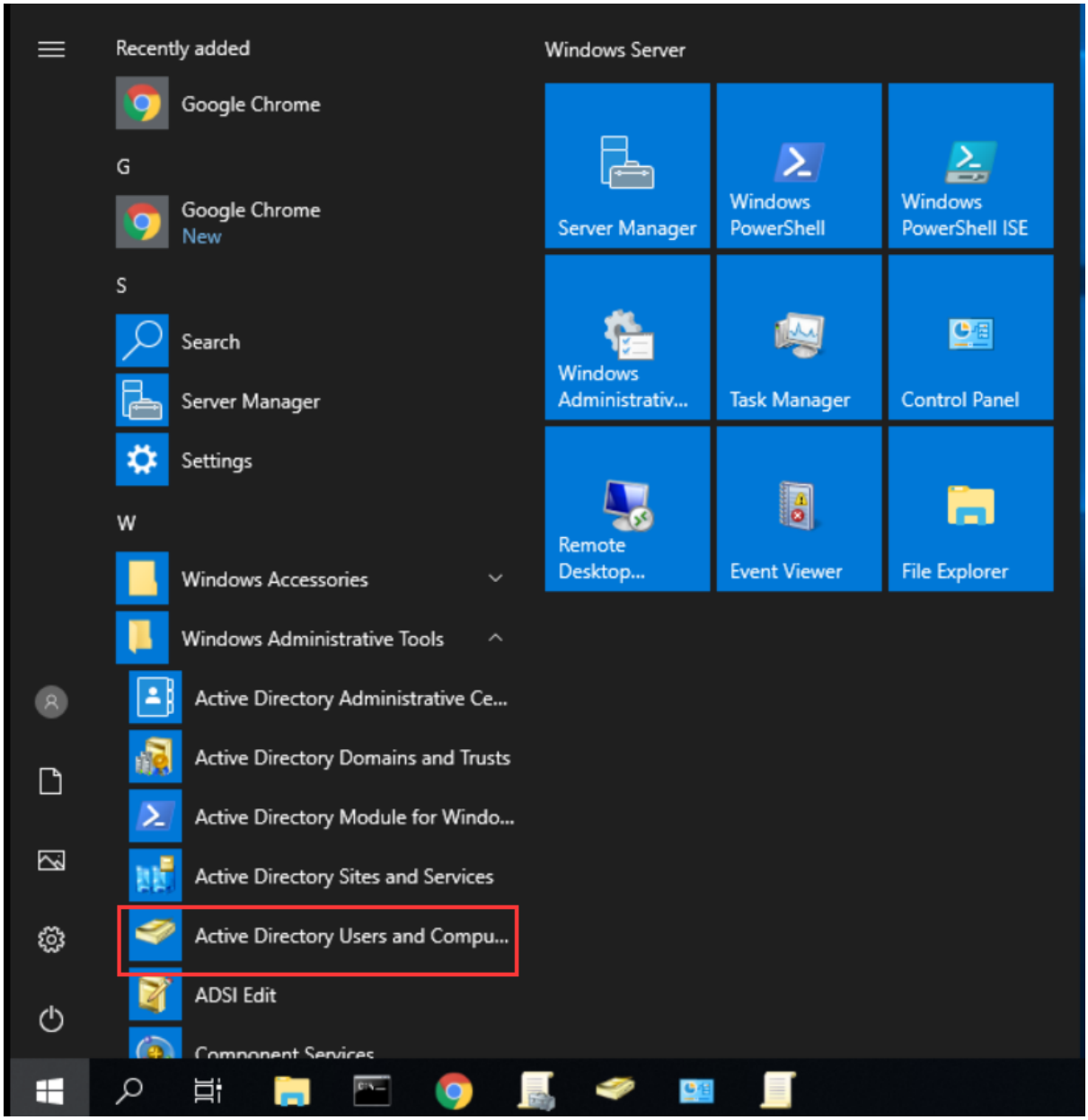


10. Setelah Windows Server restart, Anda dapat melihat di halaman login bahwa default local administrator yang masuk ke sistem operasi telah menjadi administrator di domain, dan login password sama dengan password dari akun administrator lokal.

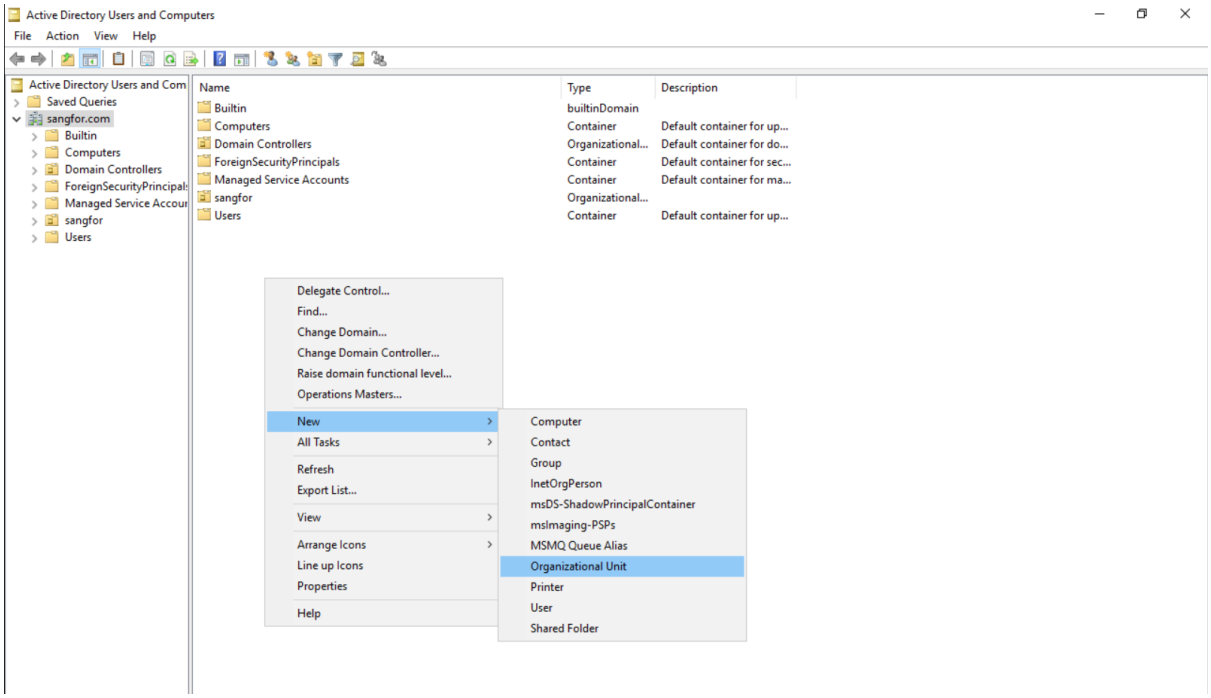


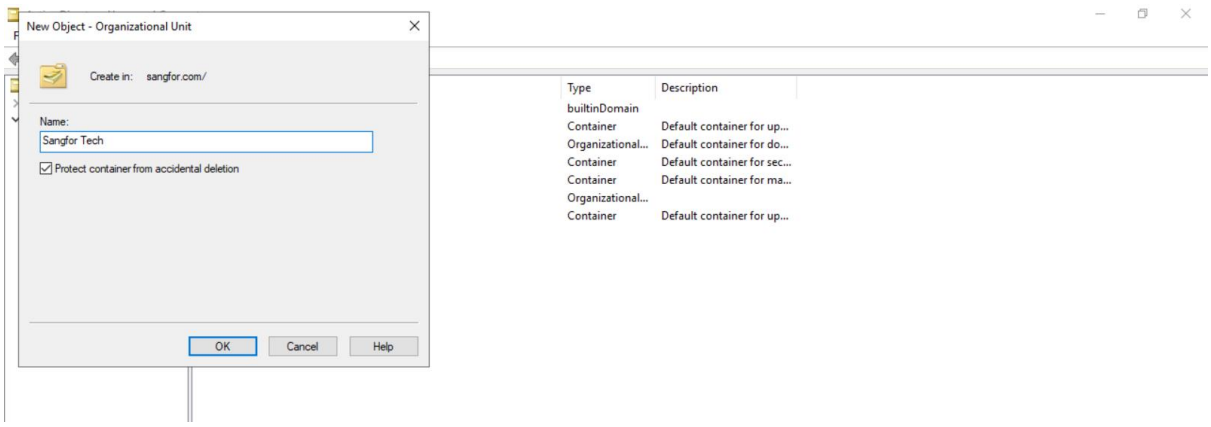
2.3 Buat usernames dan passwords untuk pengguna lain di domain

1.Buka "Active Directory Users and Computers".

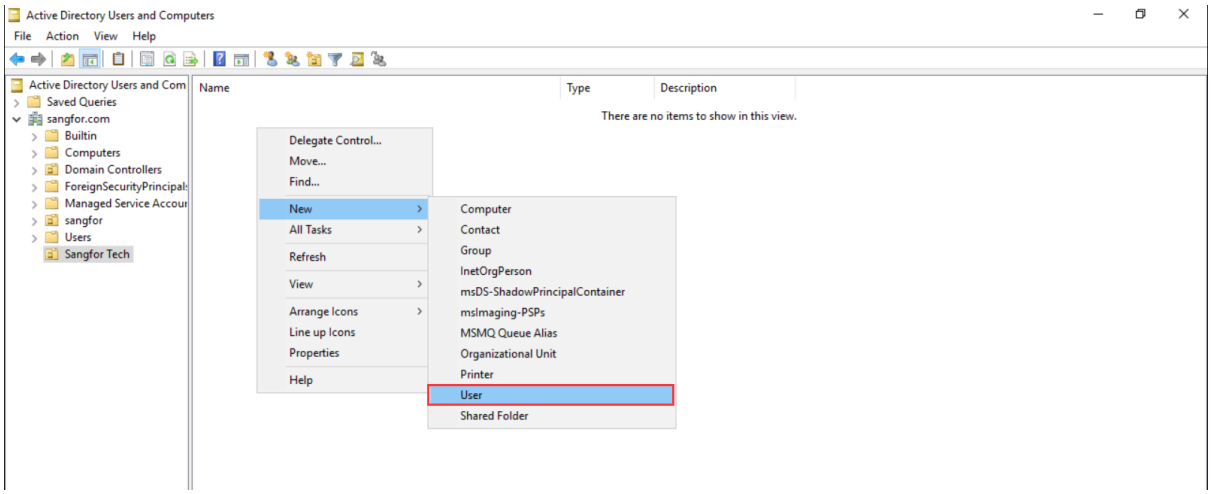


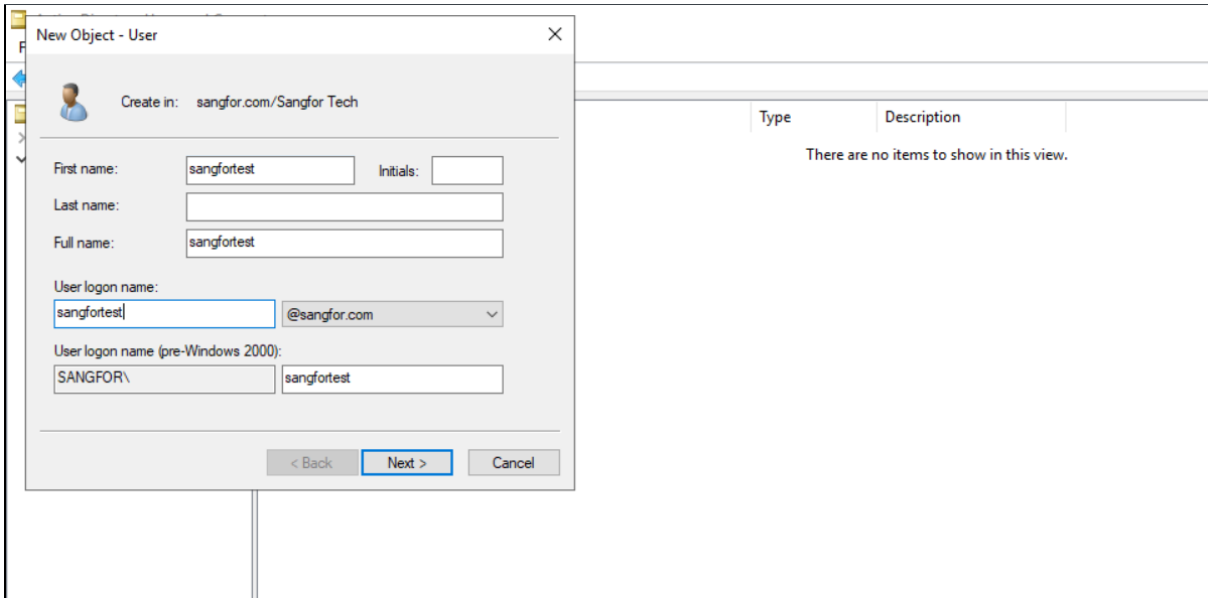
2. Dalam rangka untuk memfasilitasi manajemen pengguna menurut struktur organisasi perusahaan, logical container dibuat di sini untuk mewakili department. Misalnya, buat department bernama Sangfor Tech.



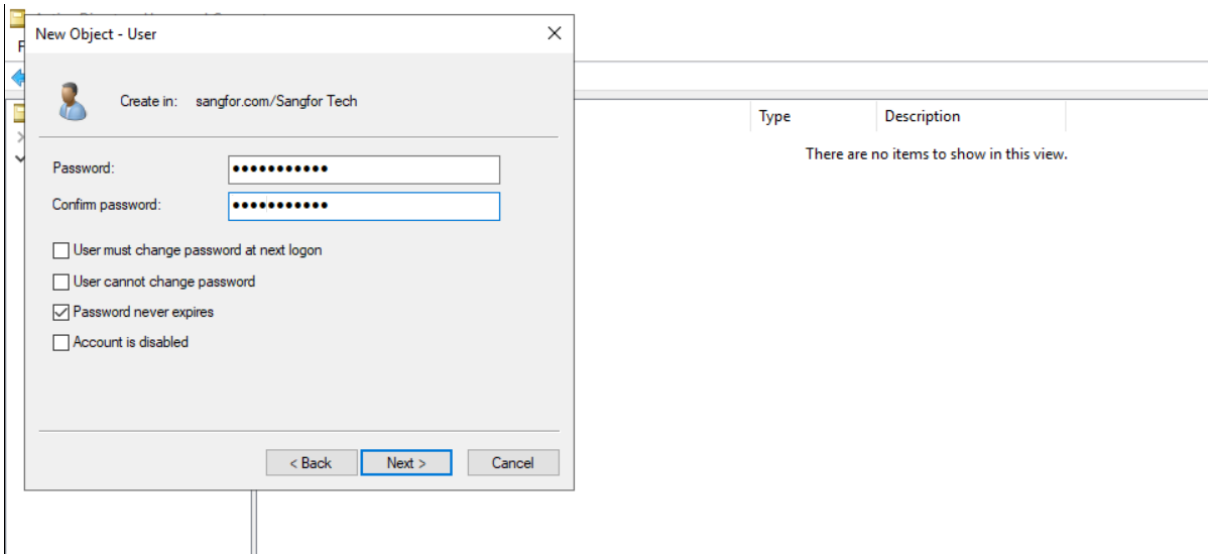


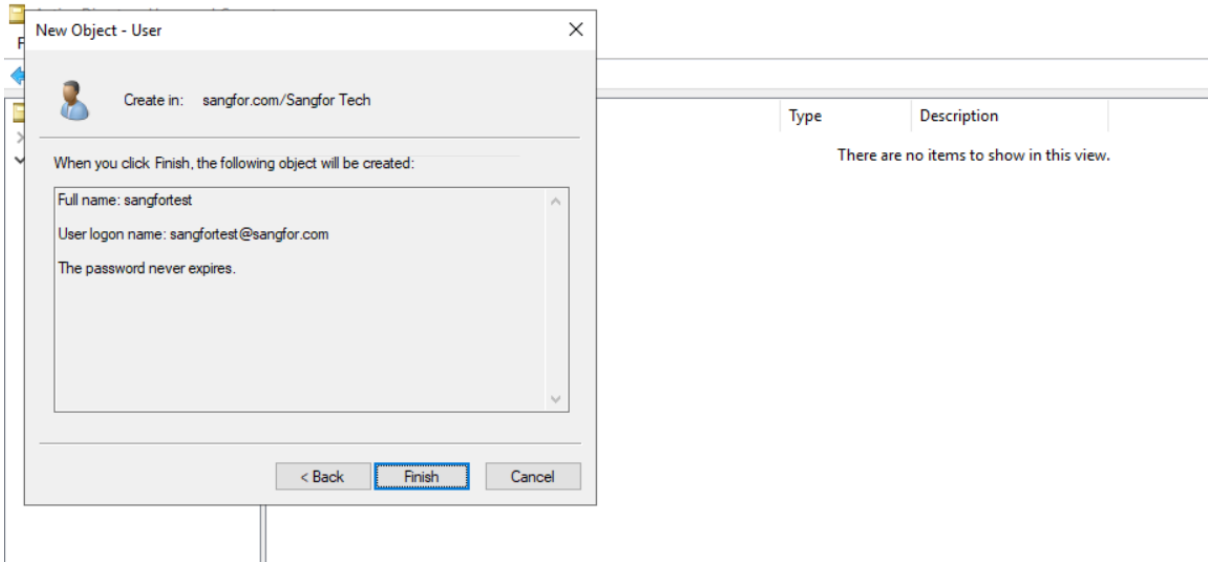
3. Buat pengguna di container, misalnya disebut sangfortest.





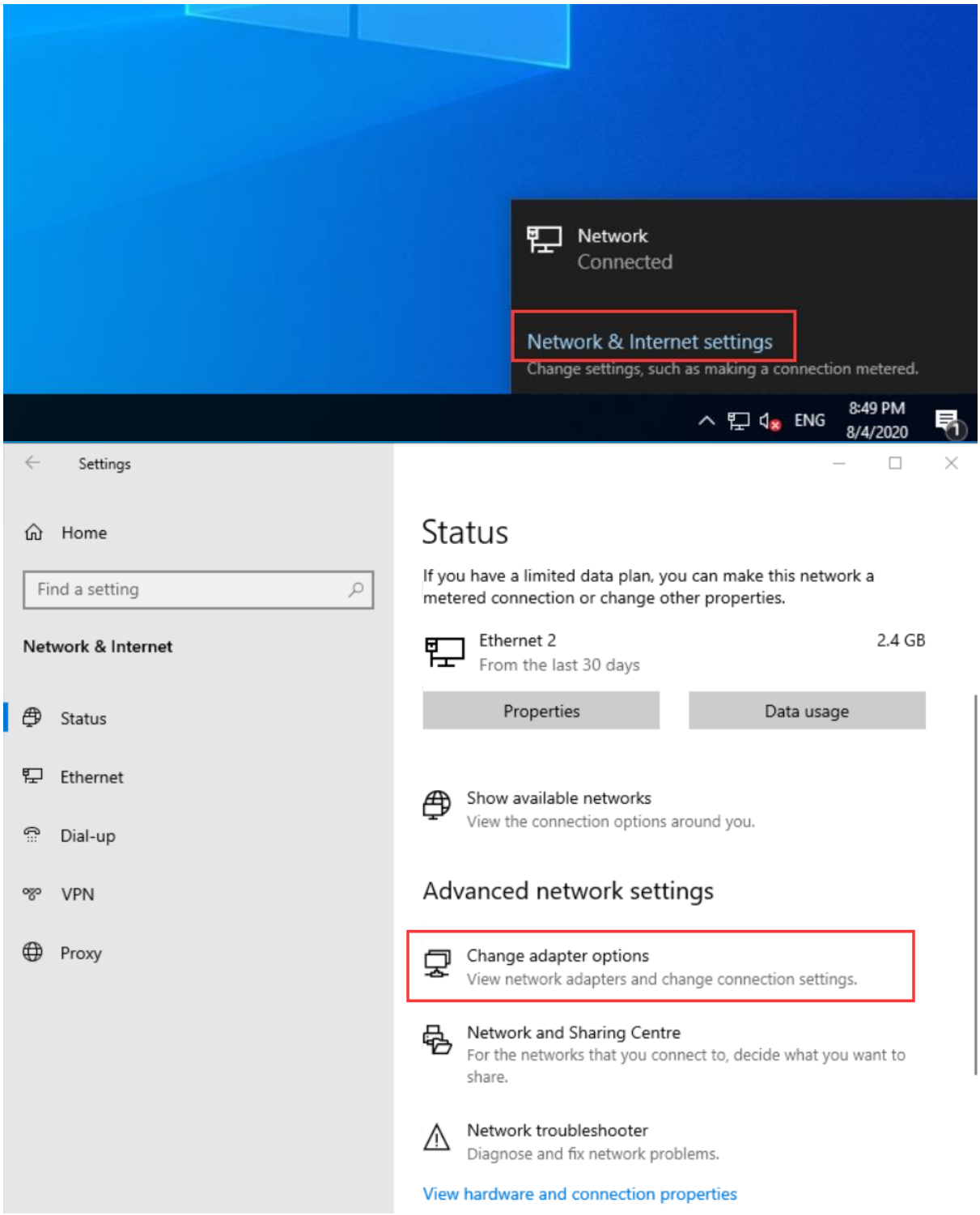
Atur login password untuk pengguna ini.

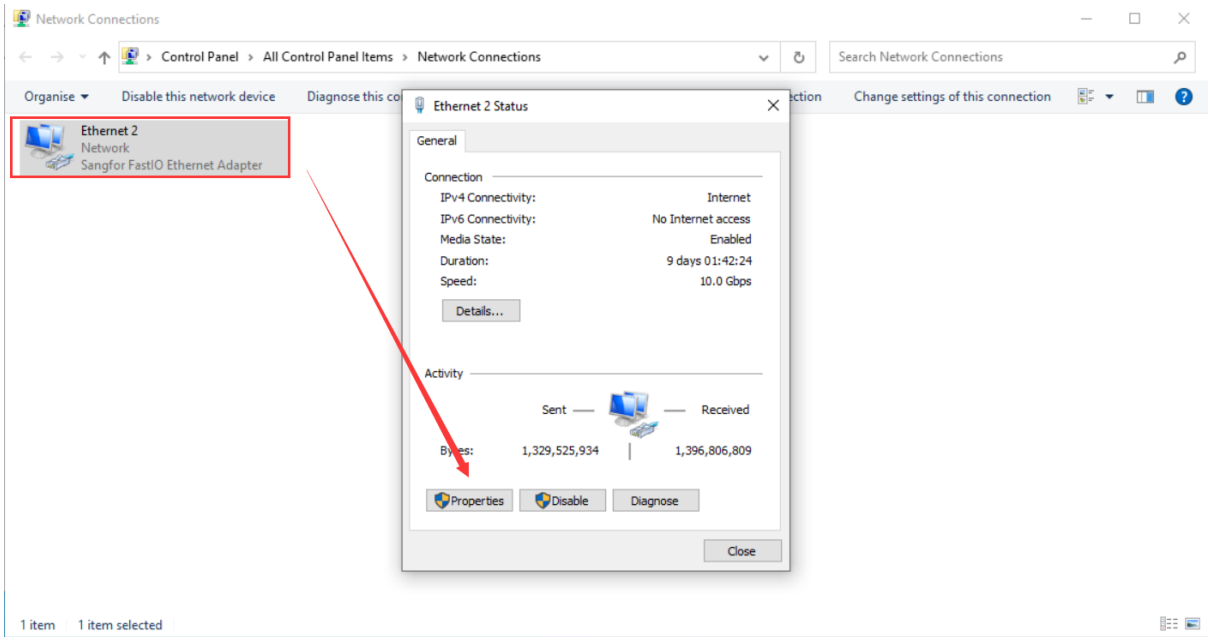


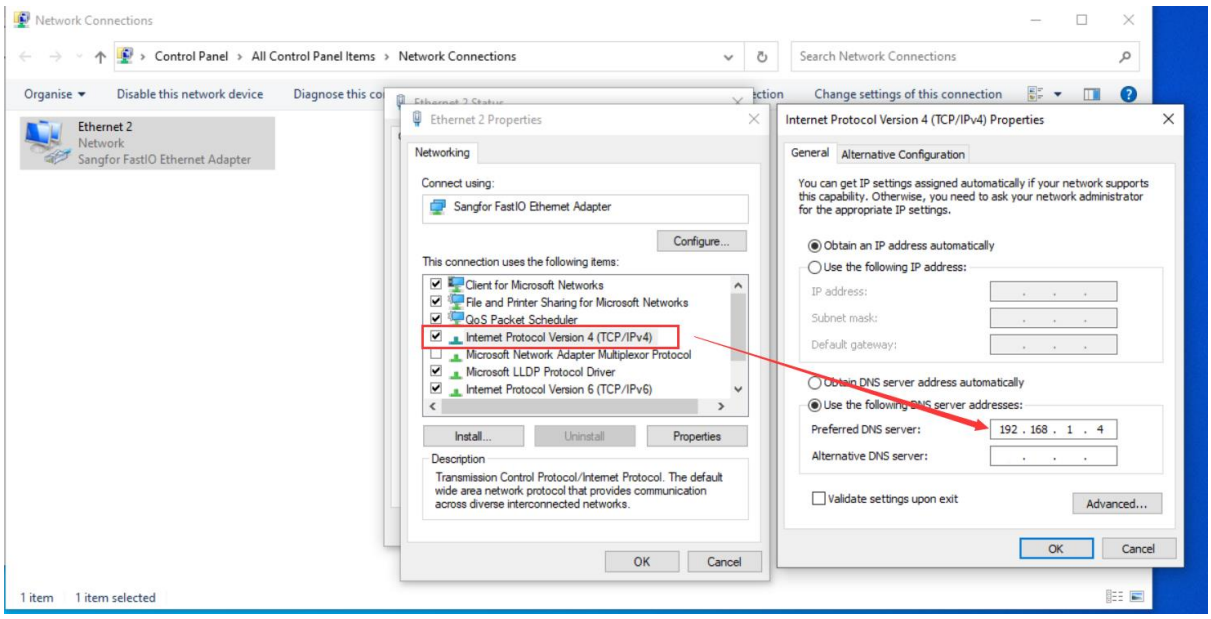


2.4 Bergabung PC ke domain

1. Konfigurasi network card PC, dan konfigurasi DNS sebagai IP dari domain kontrol server: 192.168.1.4.

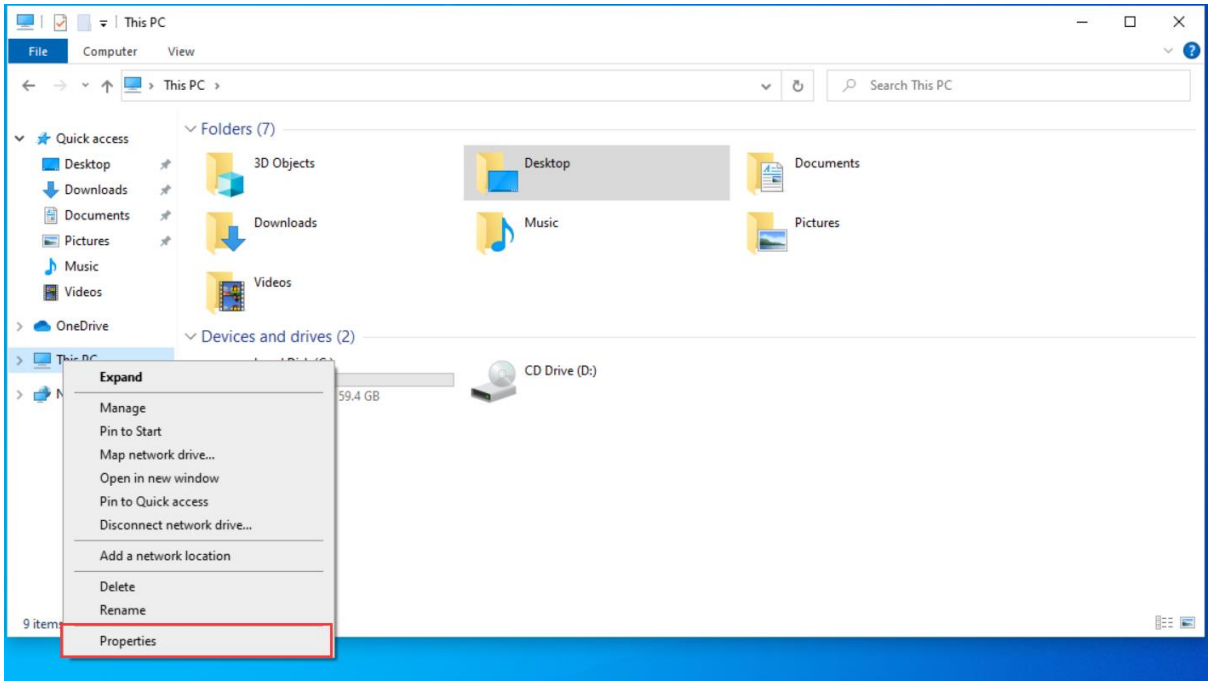


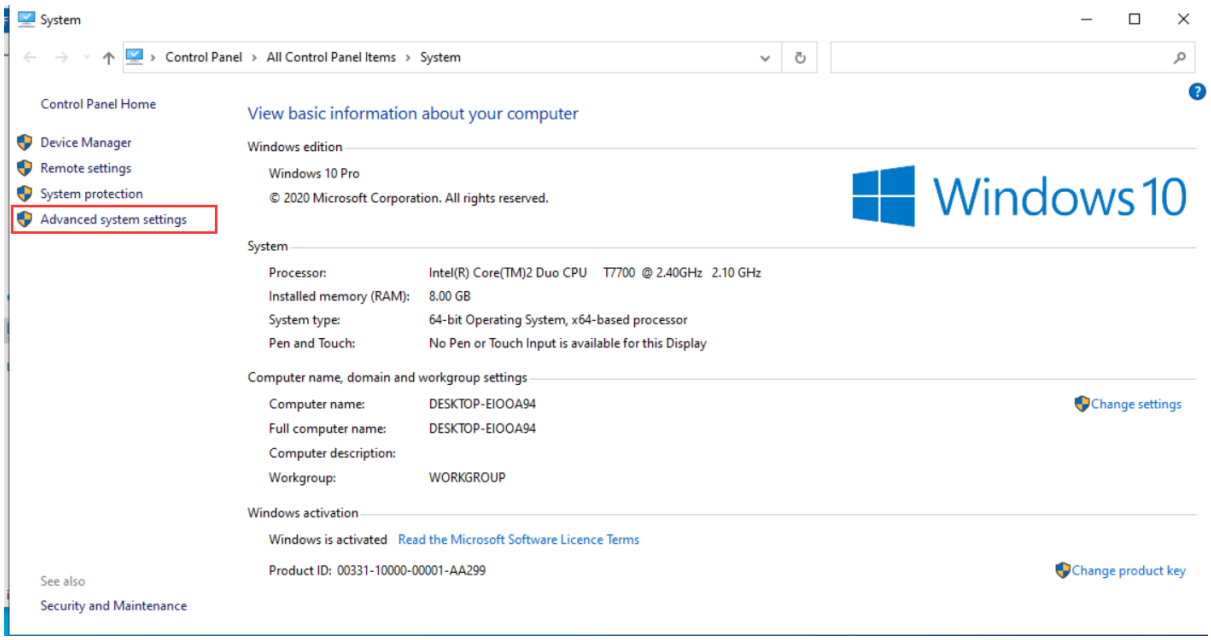


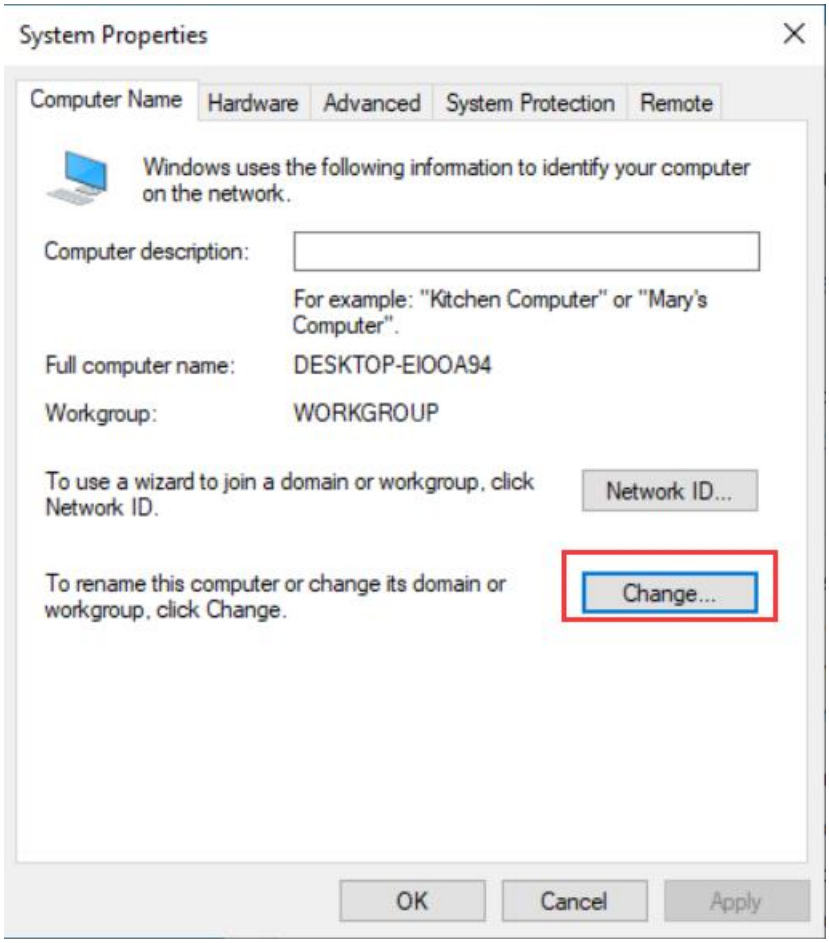


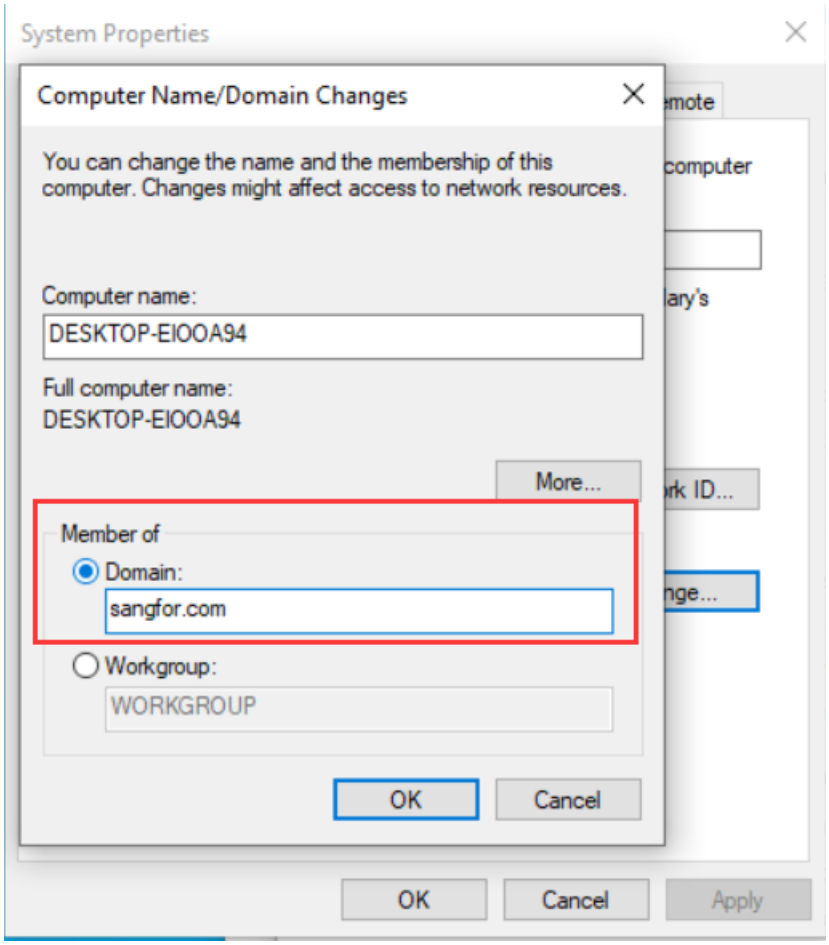
2. Bergabung PC ke domain.

Aktivitas Domain Script SSO

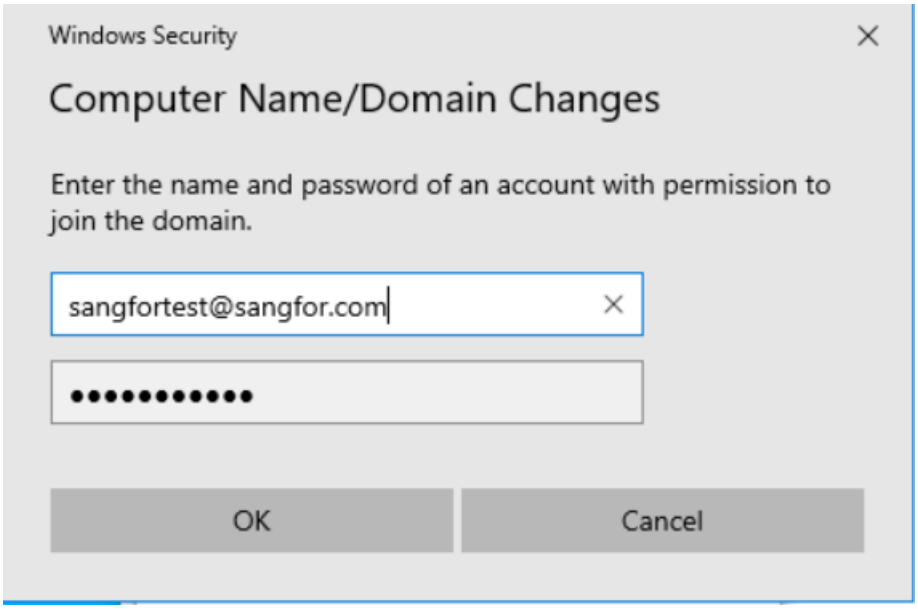




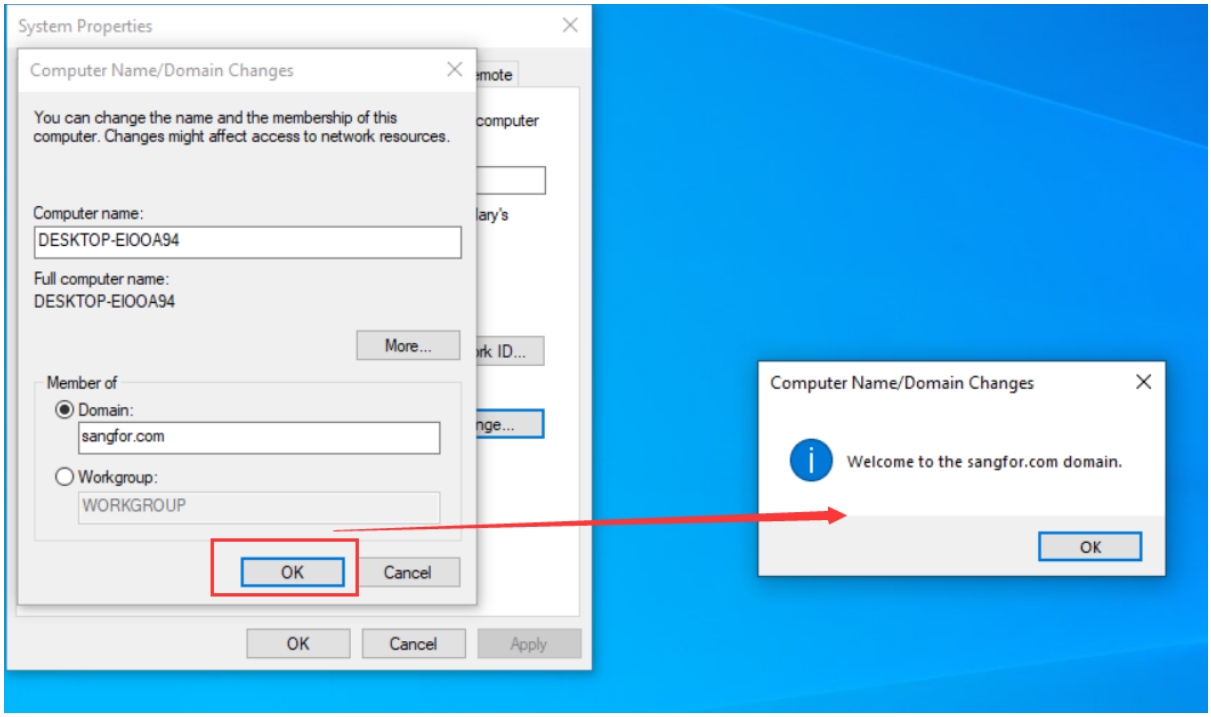

System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name:
DESKTOP-EIOOA94
Workgroup:
WORKGROUP
To use a wizard to join a domain or workgroup, click Network ID.
Network ID...
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply

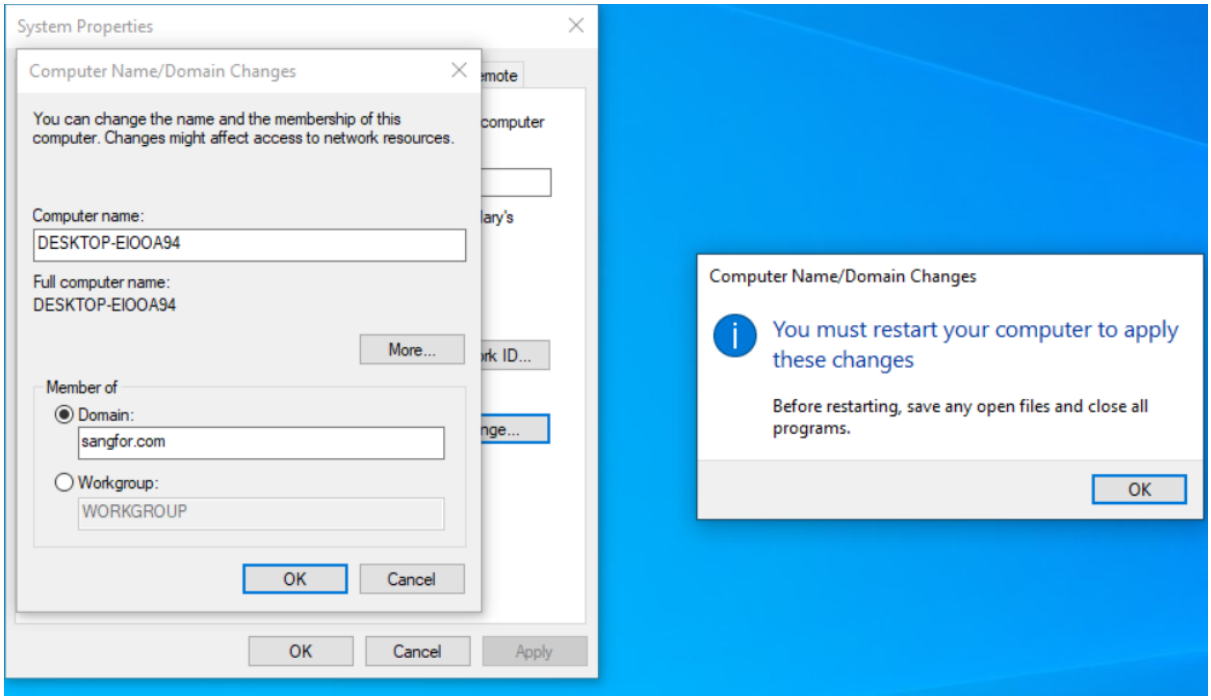


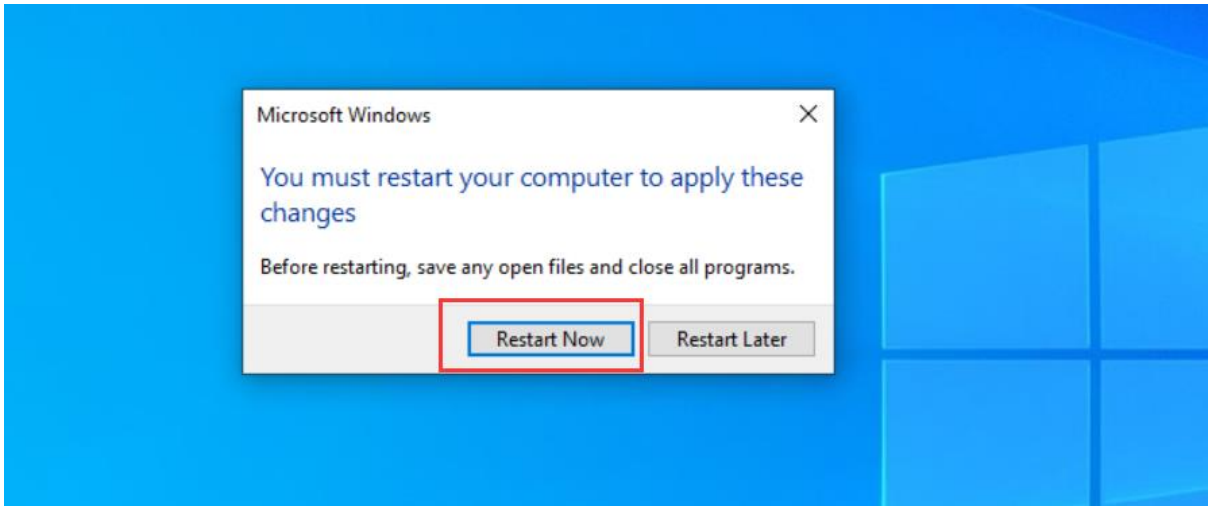
3. Dalam proses bergabung dengan domain, Anda perlu memverifikasi identitas Anda, cukup gunakan pengguna sangfortest yang dibuat pada AD domain control 192.168.1.4 untuk pengujian.



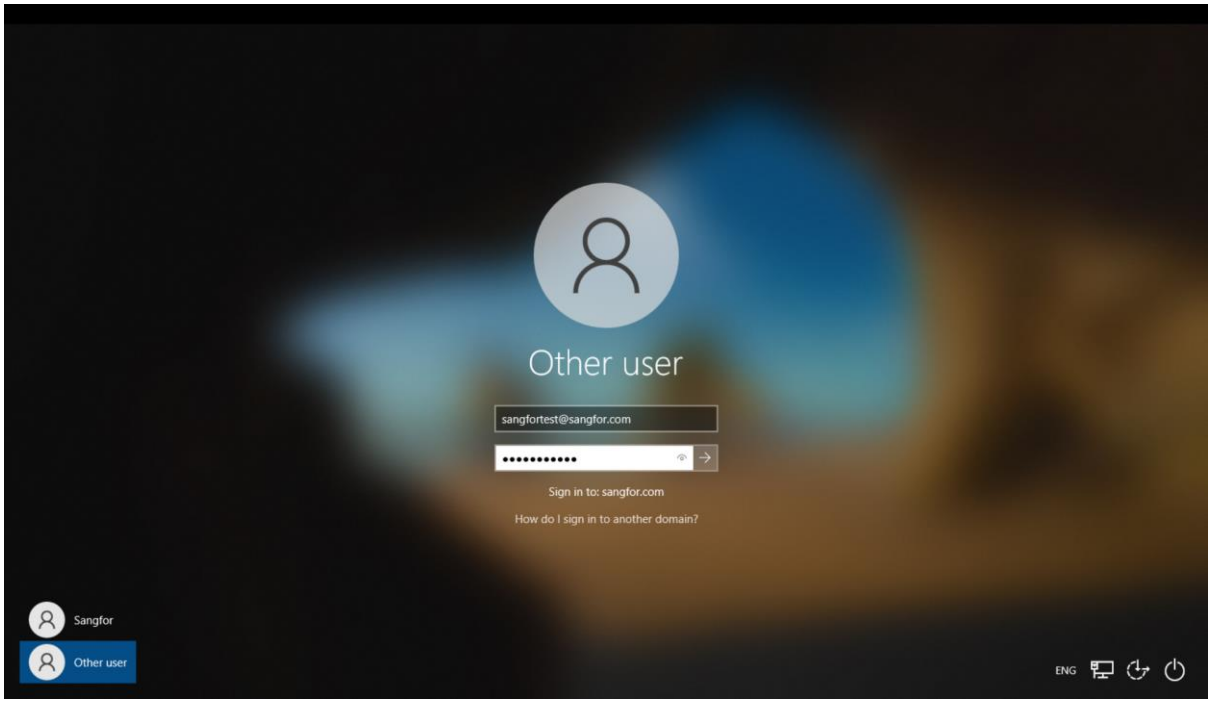
4. Setelah berhasil bergabung dengan domain, Anda perlu restart PC.


System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
DESKTOP-EIOOA94
Full computer name:
DESKTOP-EIOOA94
More...
Member of
Domain:
sangfor.com
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Computer Name/Domain Changes
Welcome to the sangfor.com domain.
OK


System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
DESKTOP-EIOOA94
Full computer name:
DESKTOP-EIOOA94
More...
Member of
Domain:
sangfor.com
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Computer Name/Domain Changes
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
OK



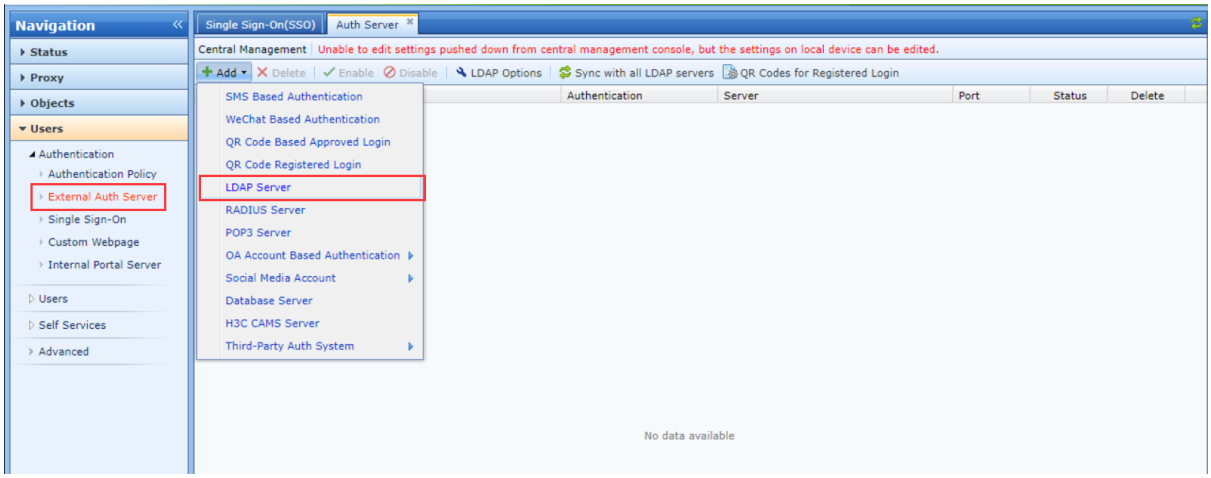
5. Setelah restart, Anda dapat melihat halaman login PC, pilih untuk menggunakan akun domain sangfortest untuk login.



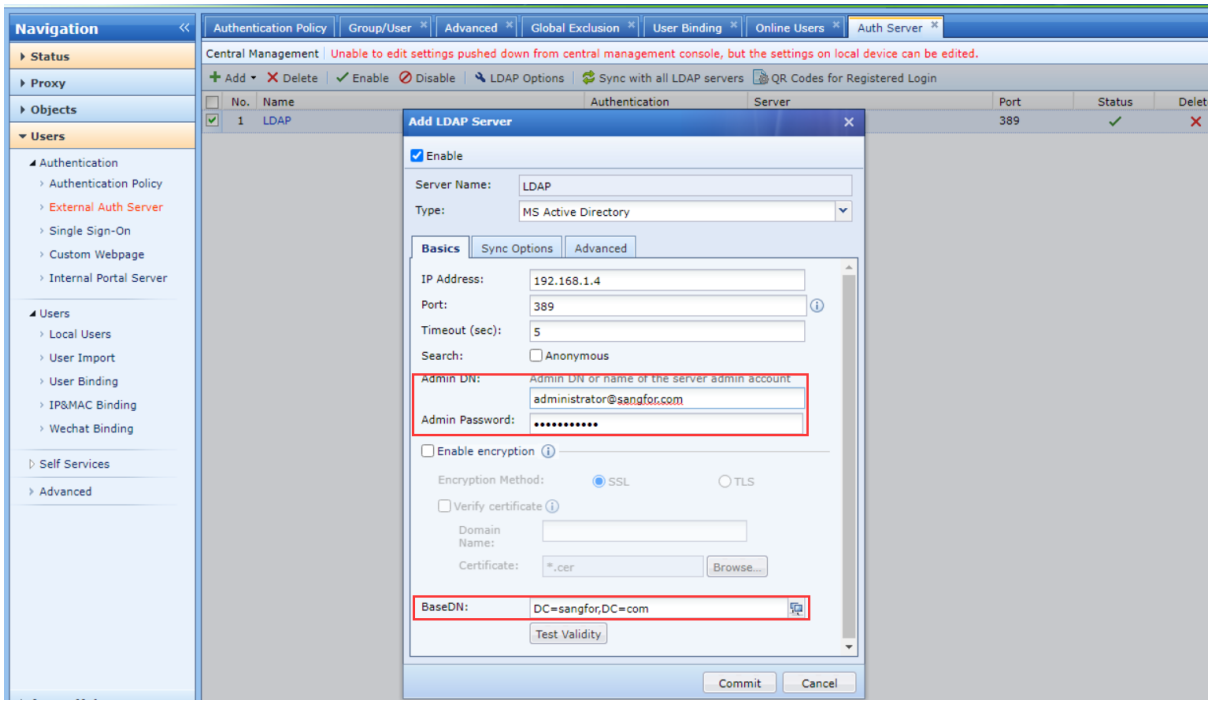
Bab 3 Bagaimana untuk Konfigurasi IAM

3.1 Tambah LDAP server

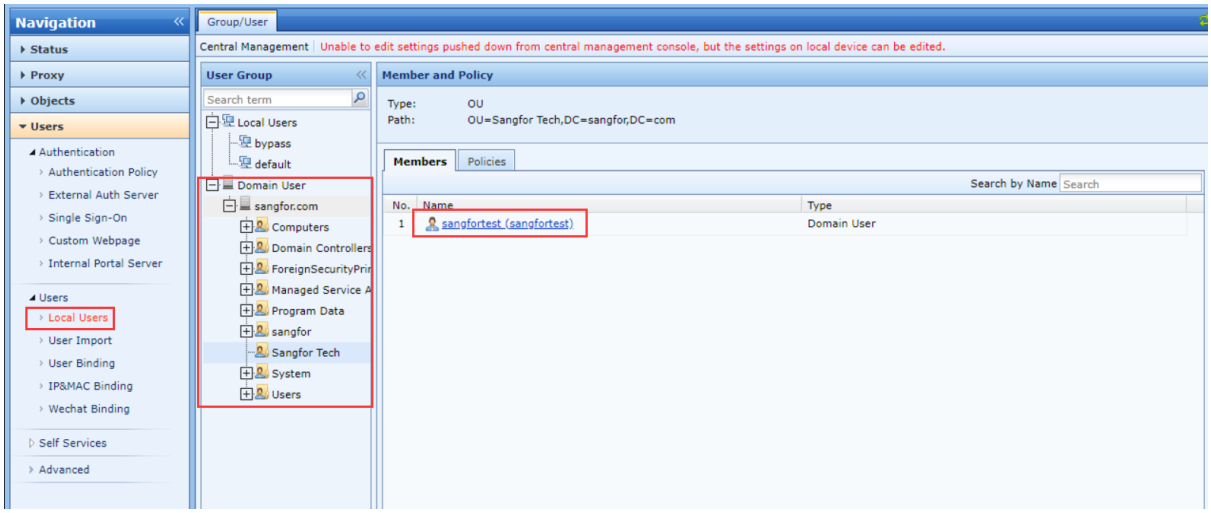
1. Tambah Microsoft AD server di IAM.



2. Perhatikan nama pengguna untuk memasukkan domain name lengkap, Anda dapat menggunakan yang dibuat sangfortest@sangfor.com, tetapi biasanya disarankan untuk menggunakan akun administrator, untuk menghindari kurangnya izin yang menyebabkan IAM tidak dapat berinteraksi dengan Microsoft AD server. BaseDN dapat memilih sangfor.

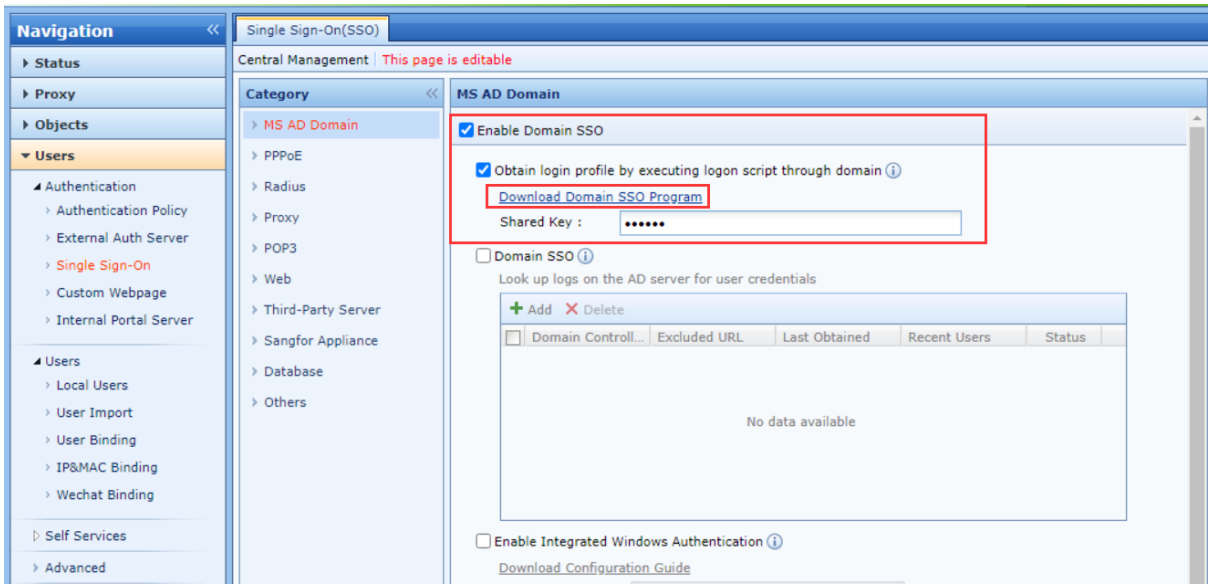


3. Jika IAM dan AD dapat berinteraksi secara normal, kemudian di pengguna lokal, Anda dapat melihat bahwa IAM telah memperoleh informasi pengguna domain dari AD server, termasuk pengguna sangfortest yang kami buat sebelumnya.

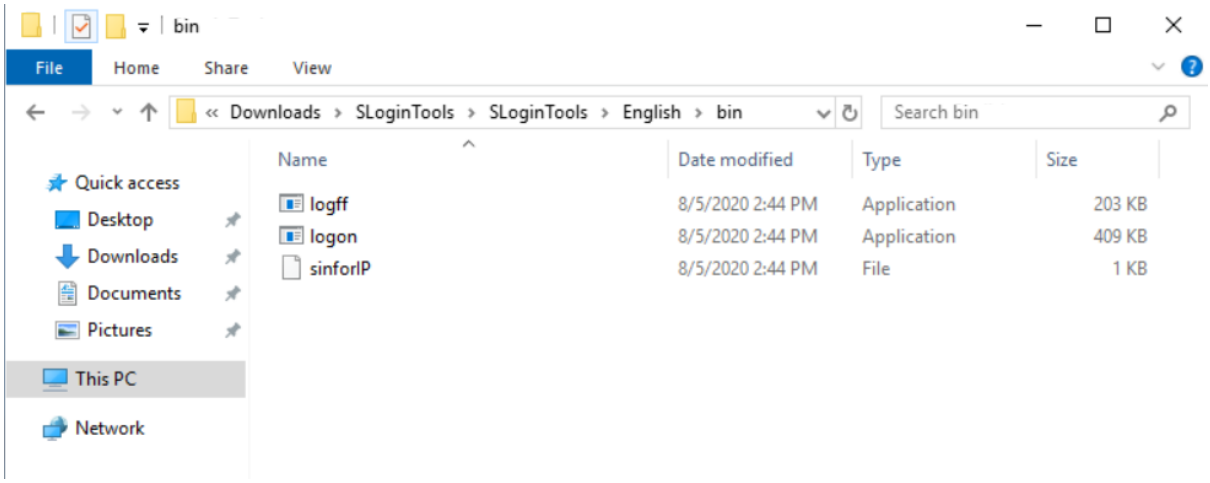


3.2 Konfigurasi script SSO di IAM dan AD Server

1. Hidupkan "Domain SSO" dan hidupkan script SSO. Di sini Anda perlu mengkonfigurasi kunci rahasia bersama untuk authentication, misalnya, itu diatur ke 123456.

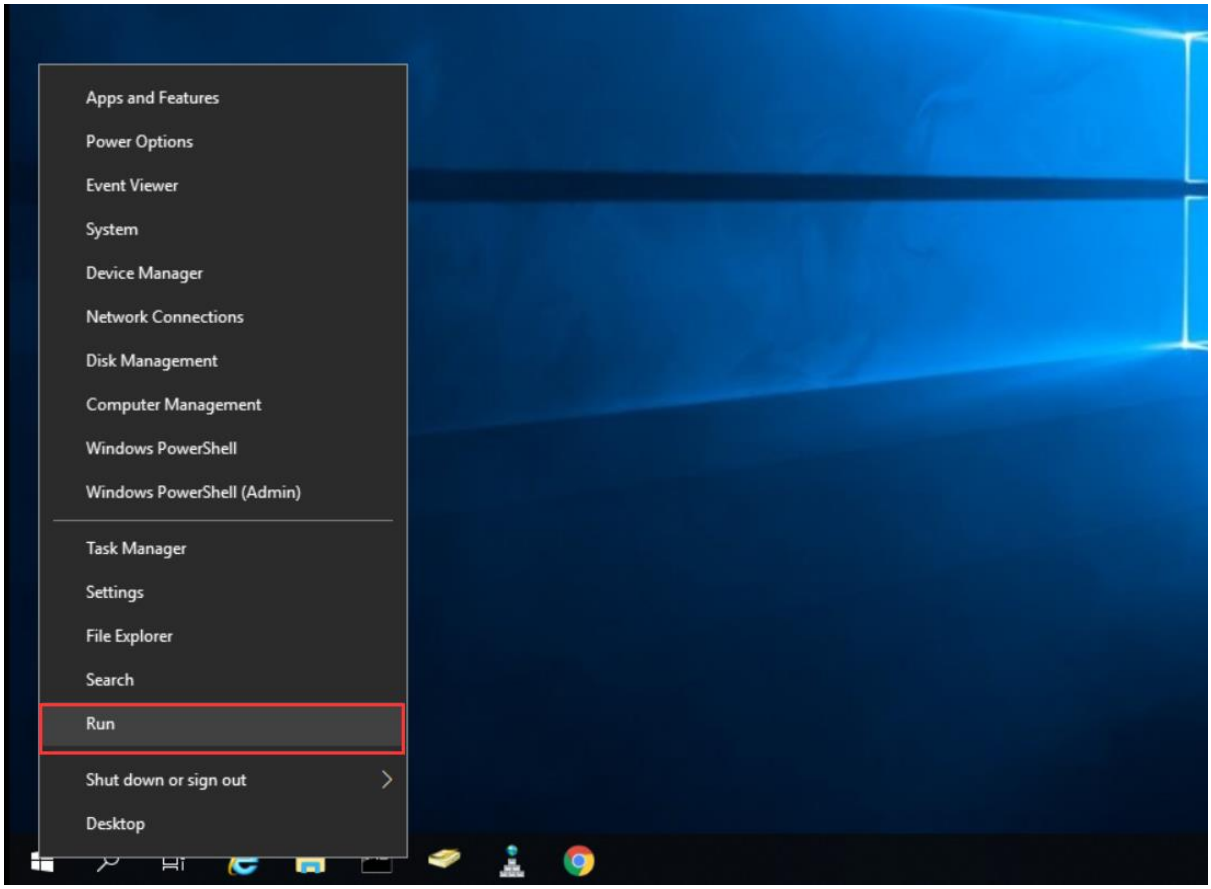


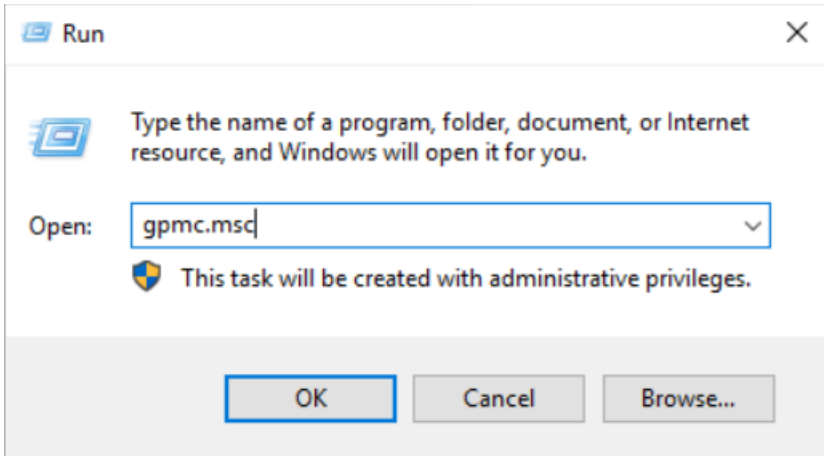
2. Download the program from the page, termasuk login script dan logout script.



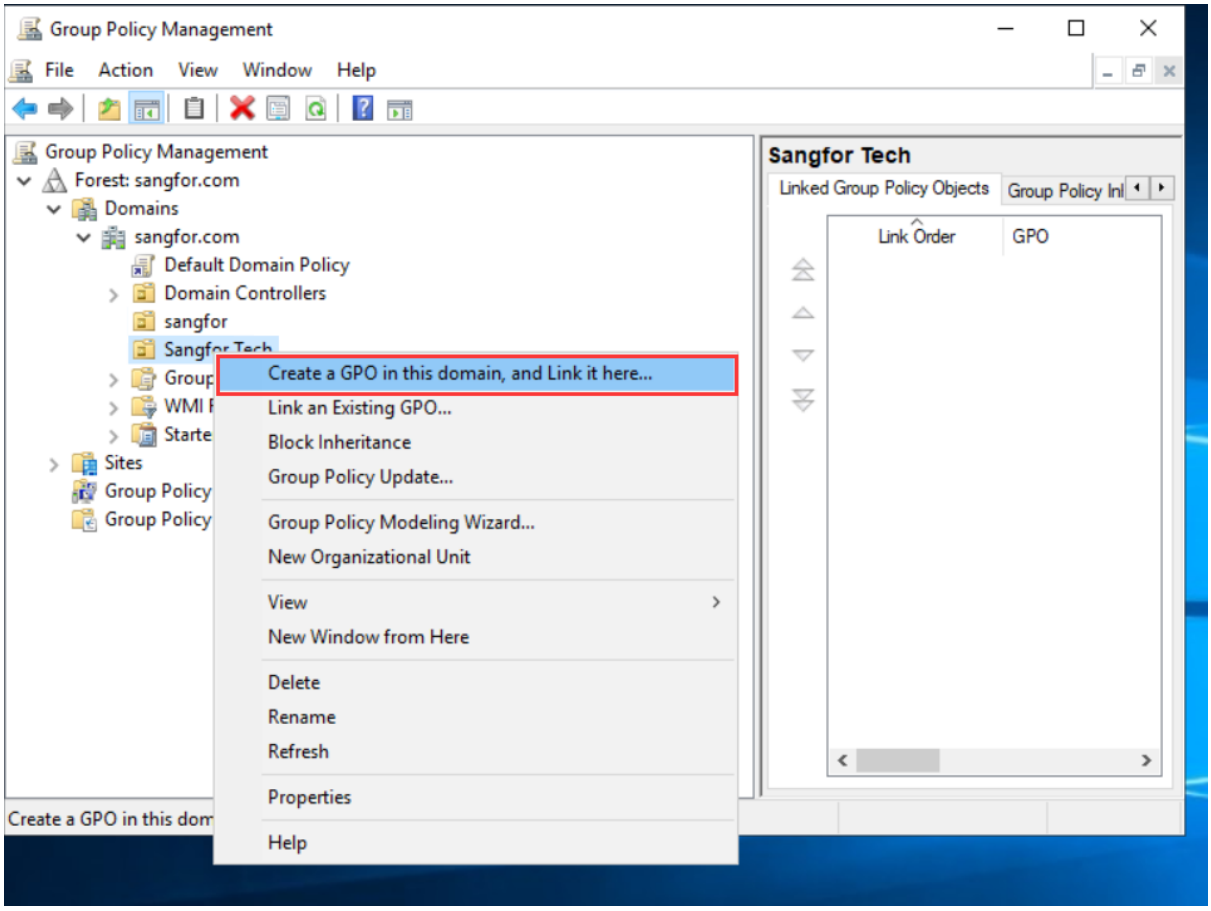
3.3 Konfigurasi login dan logout script di AD server

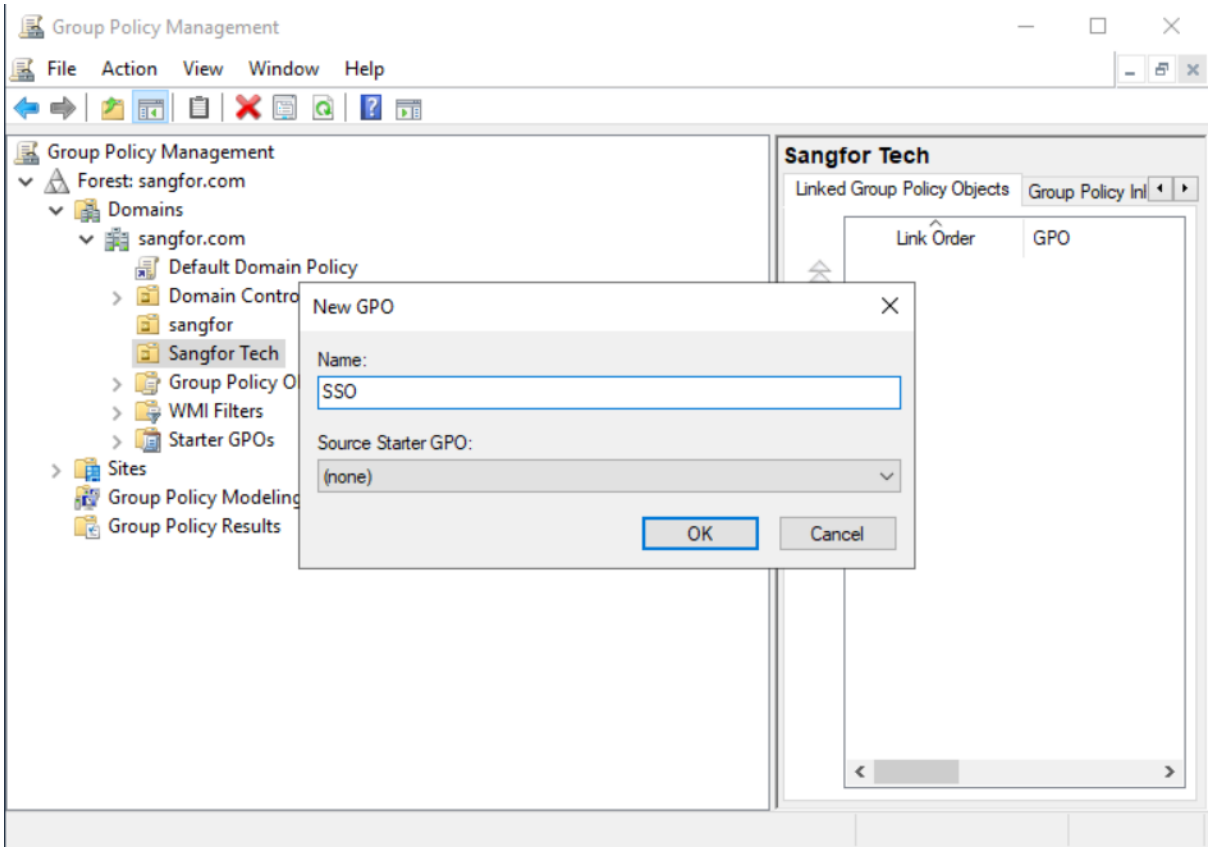
1. Buka "Group Policy Management" di "Run".



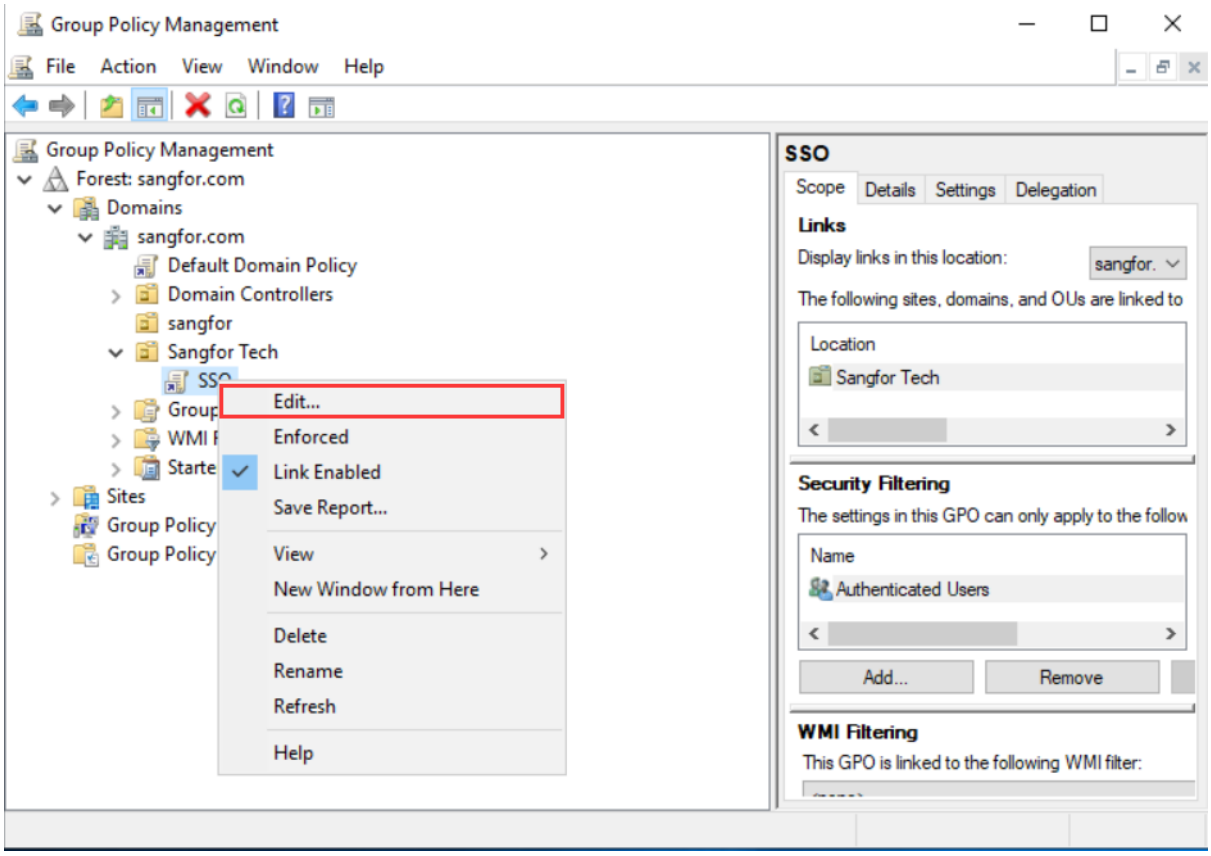


2. Buat sebuah GPO untuk container yang baru dibuat Sangfor Tech, dan buat nama untuk GPO.

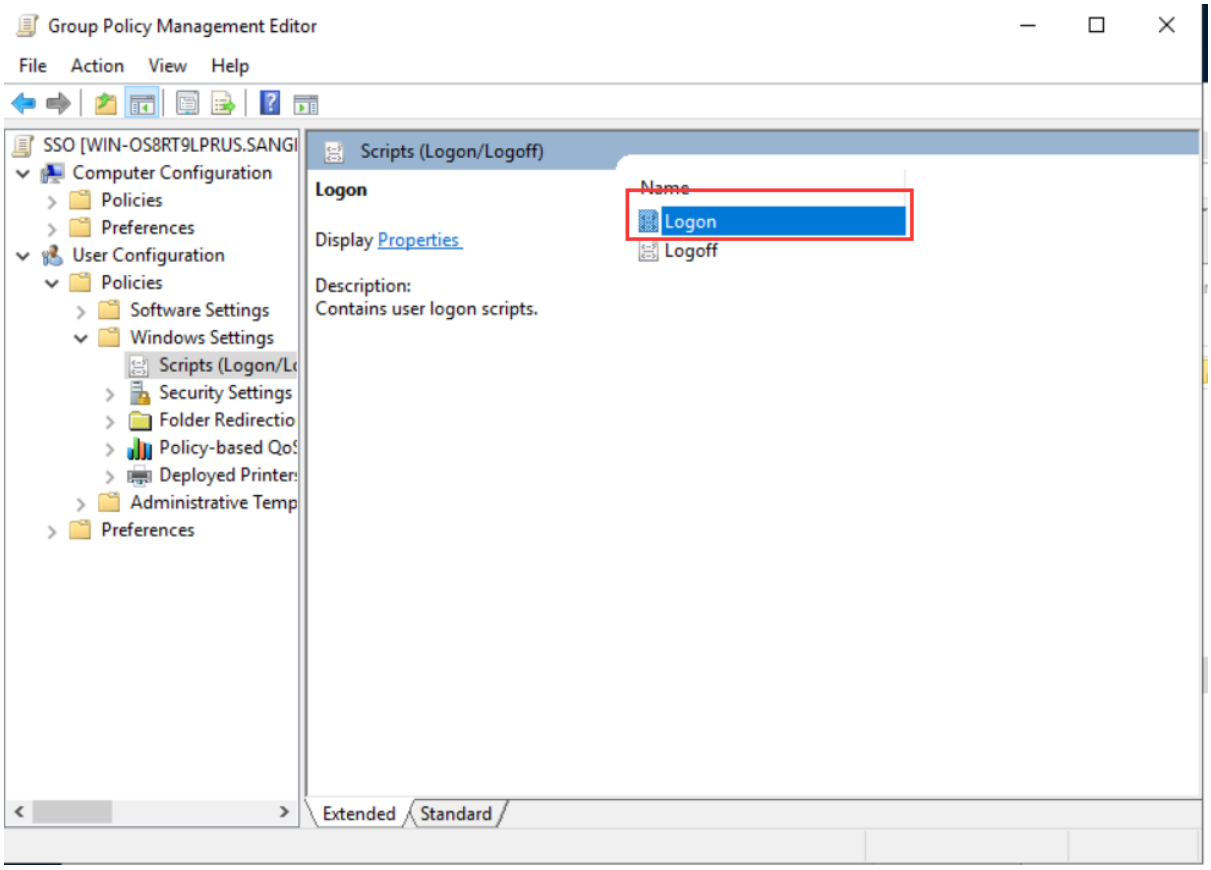




3. Gunakan tombol kanan mouse untuk memilih Edit GPO.

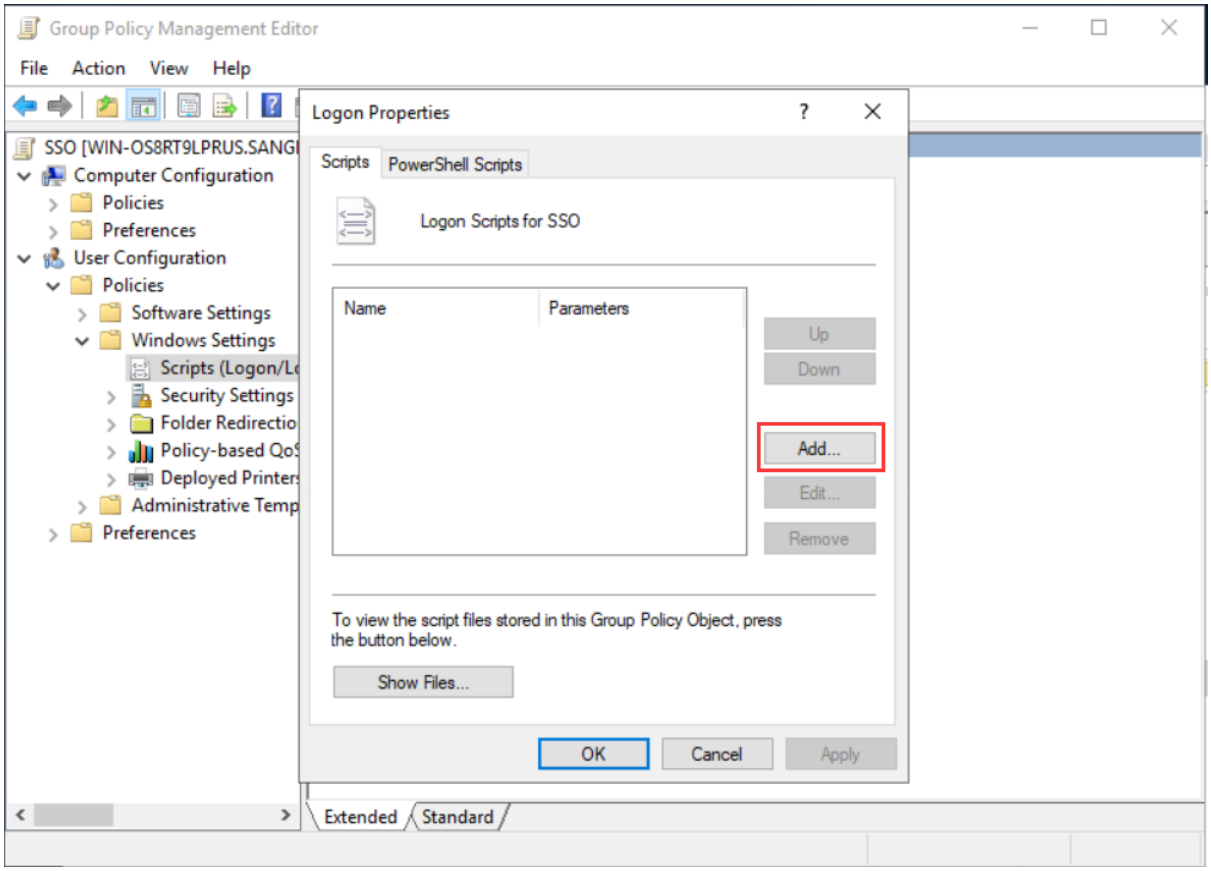


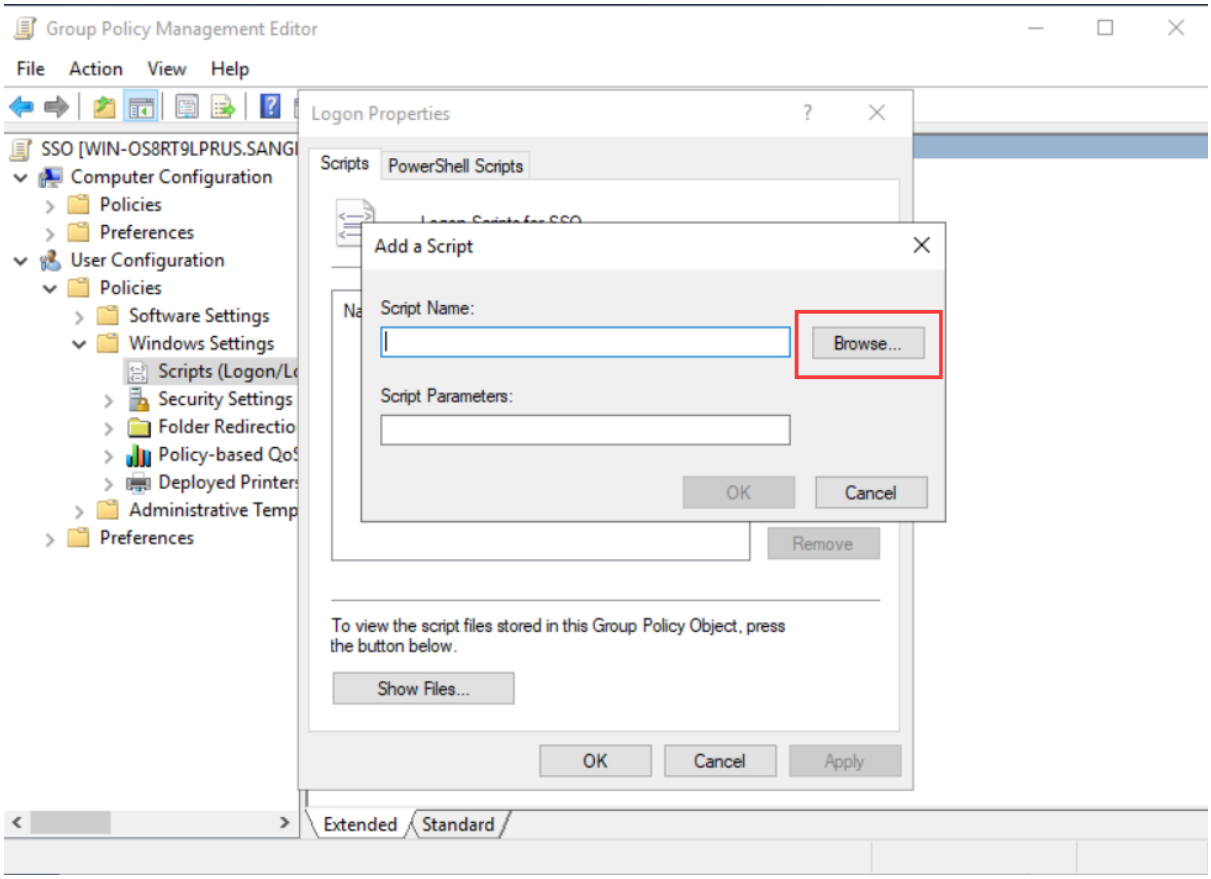
4. Cari konfigurasi login script di "User Configuration".

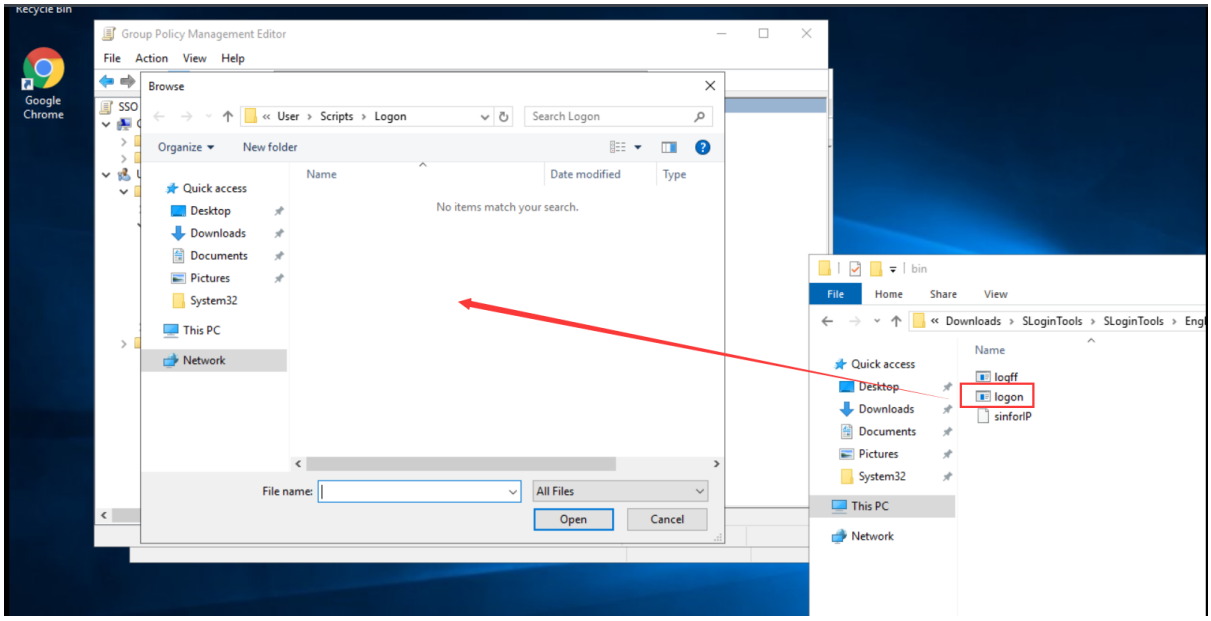


5. Pilih Logon script, klik "Add", dan kemudian pilih "Broswe" untuk copy login script yang kami unduh dari halaman IAM ke path yang ditentukan.

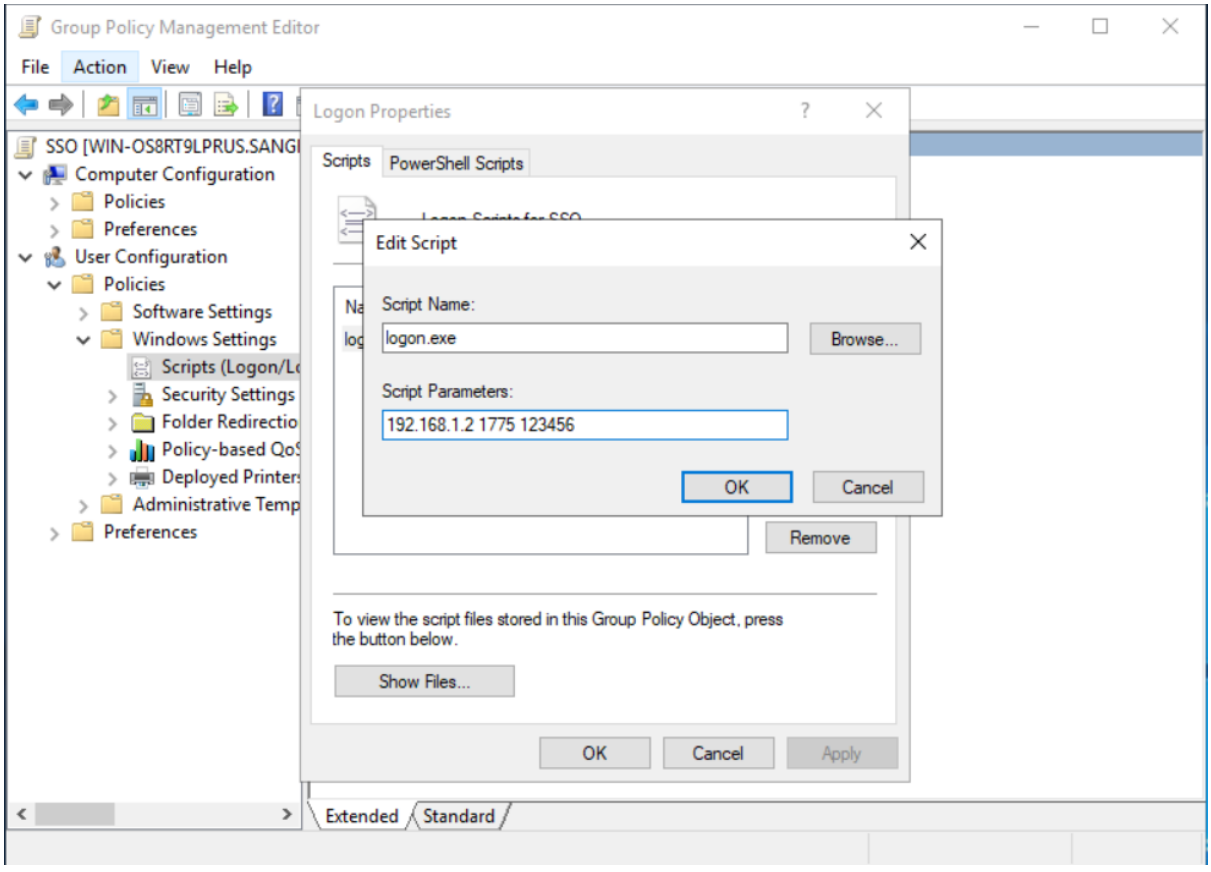
Aktivitas Domain Script SSO





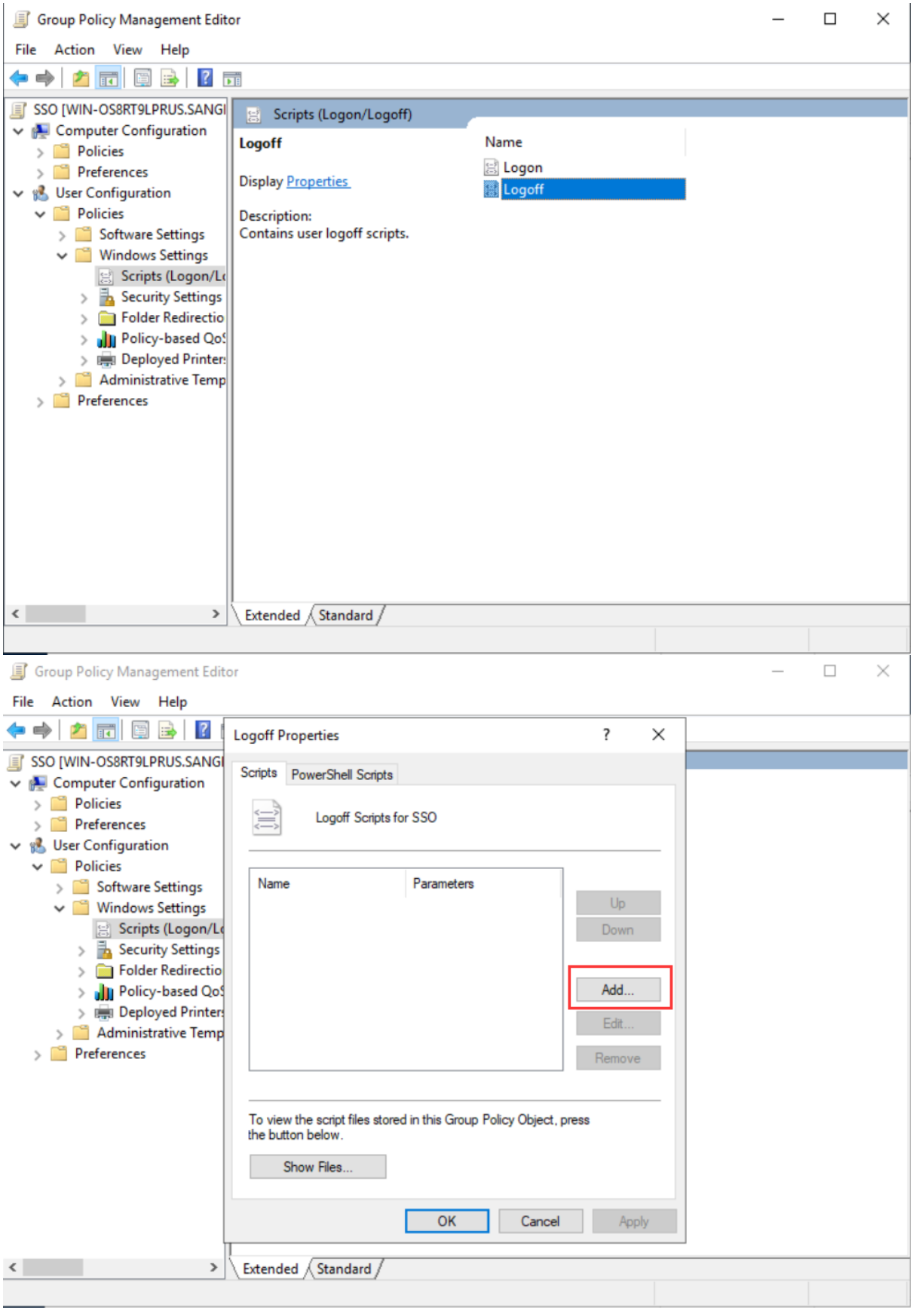


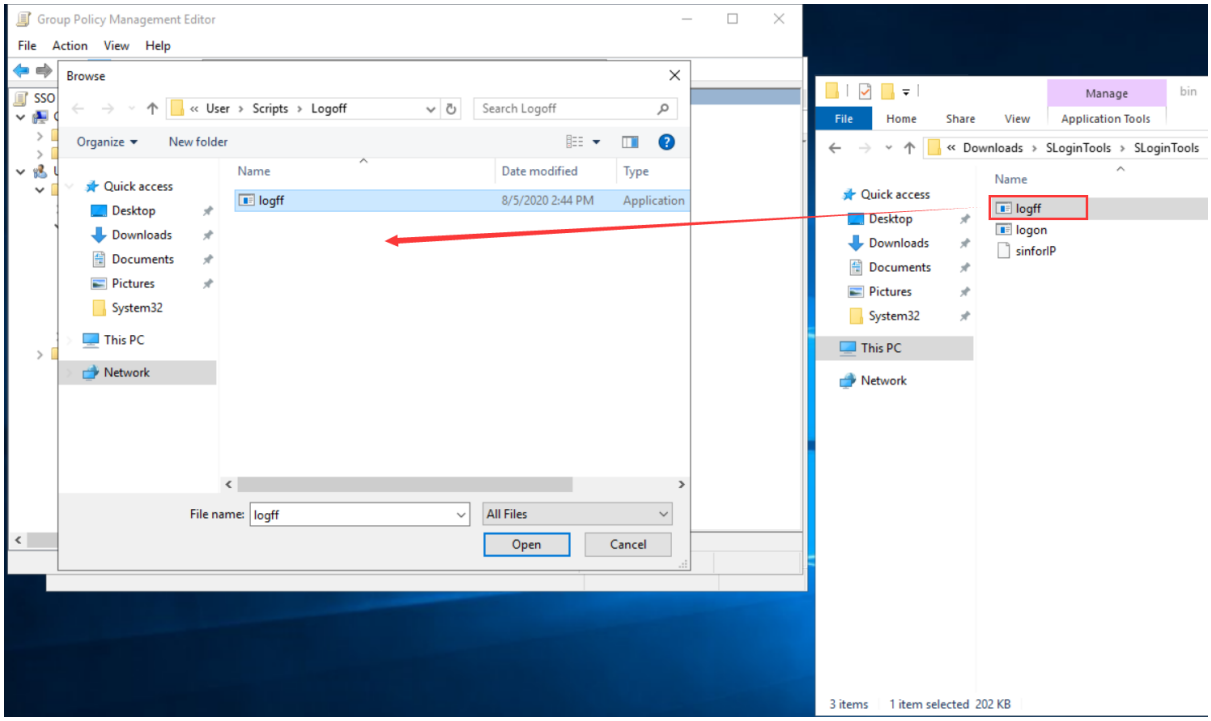
5. Atur parameter dari script single sign-on, pertama tulis IAM address 192.168.1.2 dan kemudian isi port 1775, IAM menggunakan port UDP 1775 untuk menerima informasi authentication yang aktif dikirimkan oleh PC, dan isi secret key bersama 123456 yang kami konfigurasi di halaman IAM.

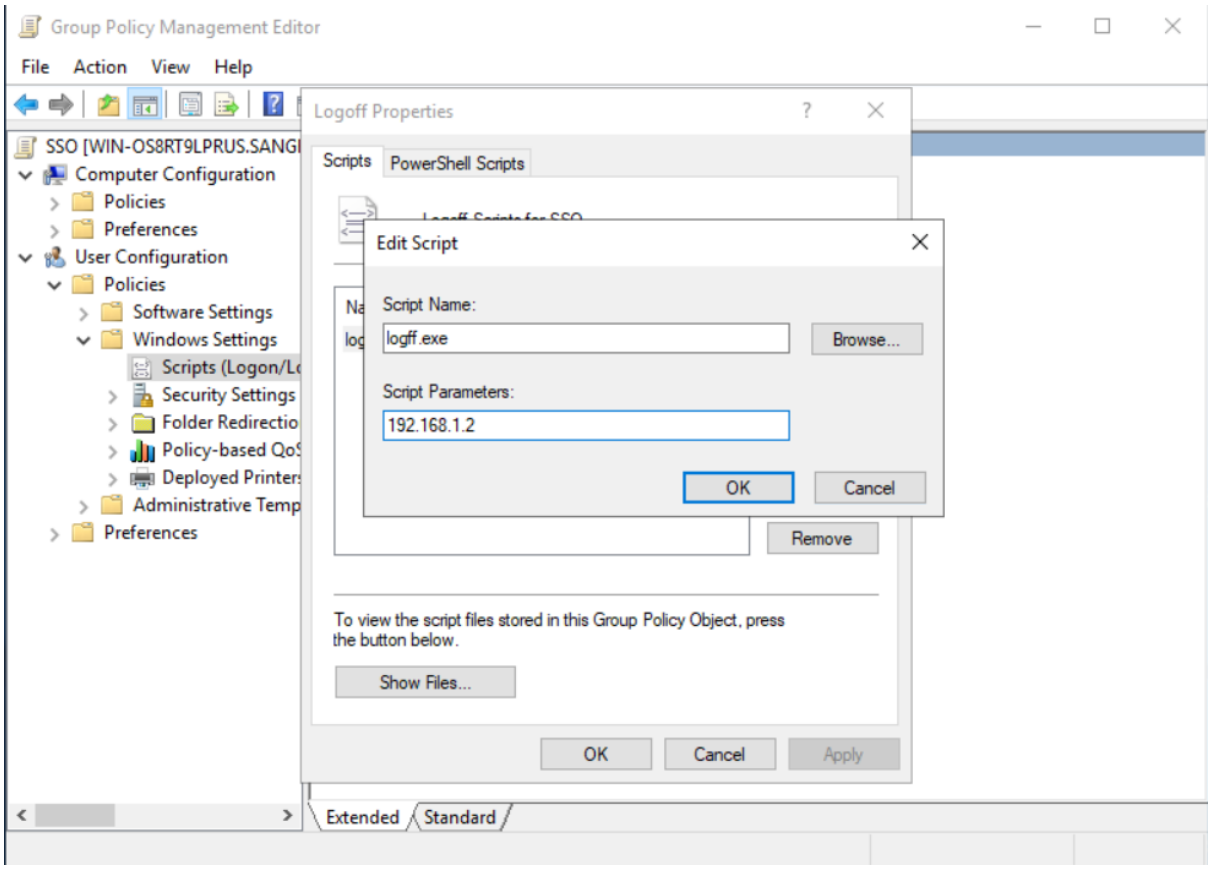


6. Untuk Logoff script, juga copy program Log off yang kita unduh dari halaman IAM ke path

yang ditentukan, dan isi parameter script IAM IP 192.168.1.2.



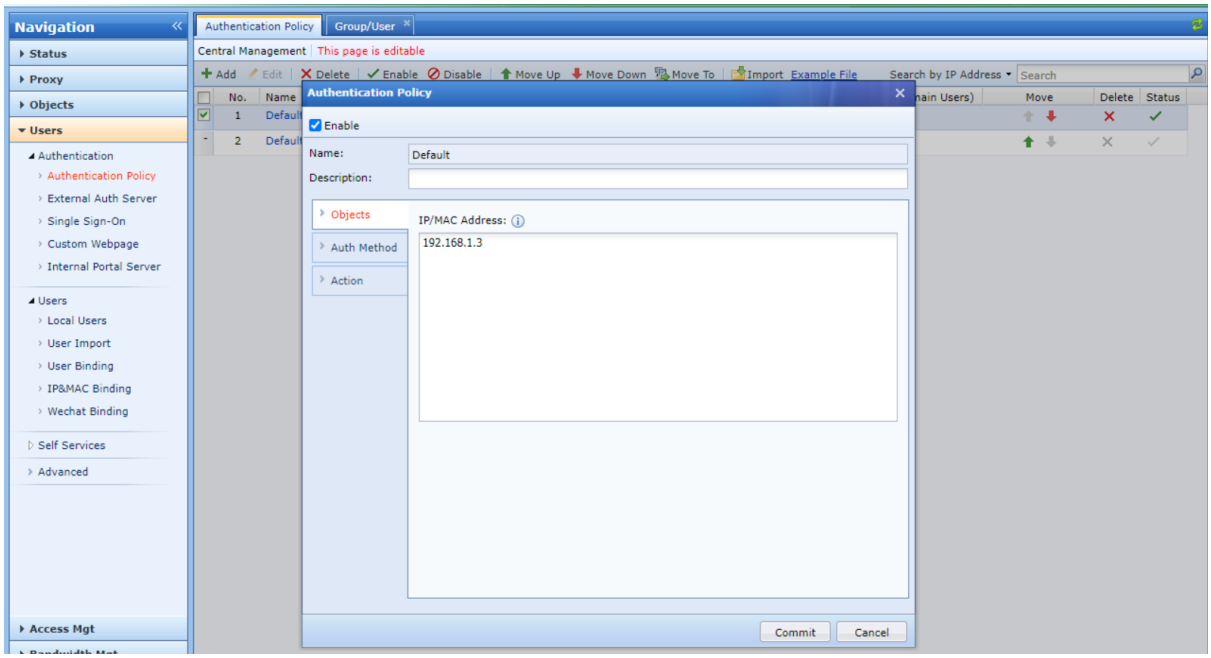




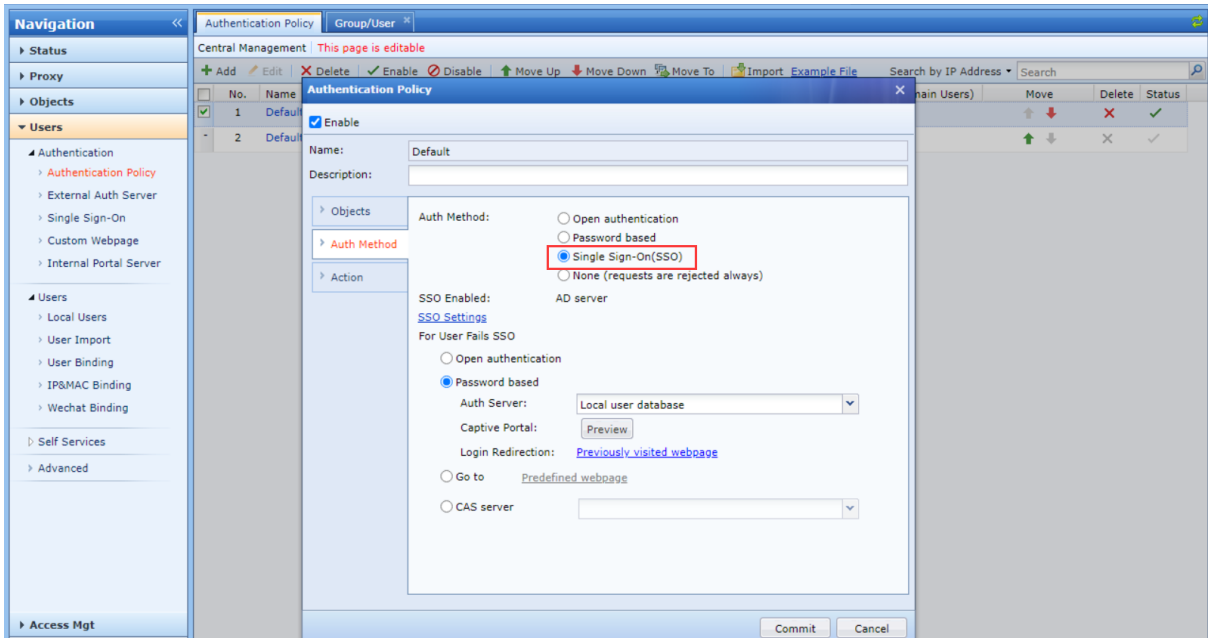
7. Setelah modifikasi AD domain server, gunakan perintah gpupdate/force untuk secara paksa menyegarkan semua kebijakan group.

3.4 Konfigurasi authentication policy pada IAM

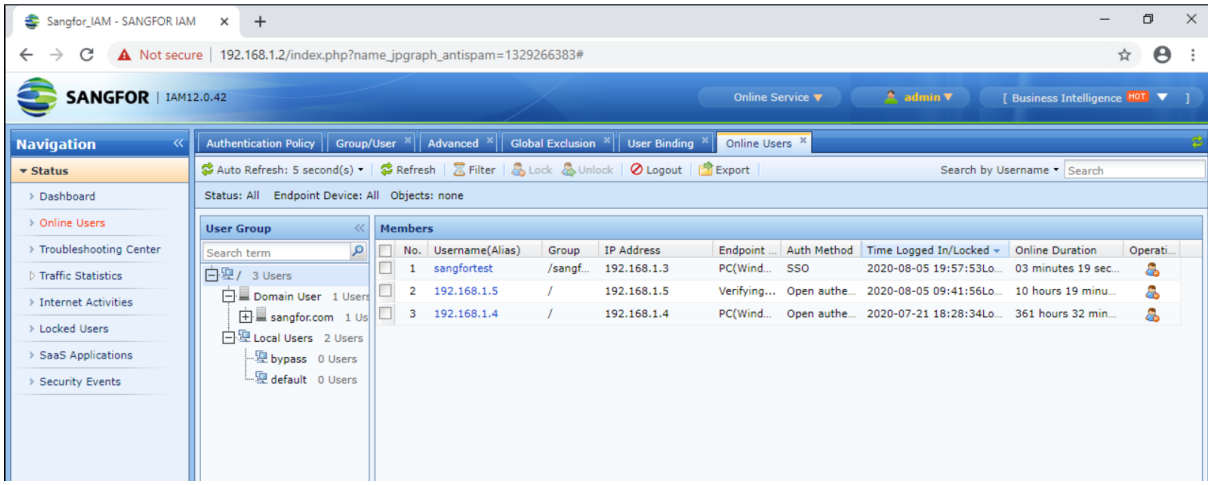
1. Atur scope dari authentication strategy, yaitu, IP mana yang harus cocok dengan authentication policy.



2. Pilih metode autentikasi sebagai "SSO".

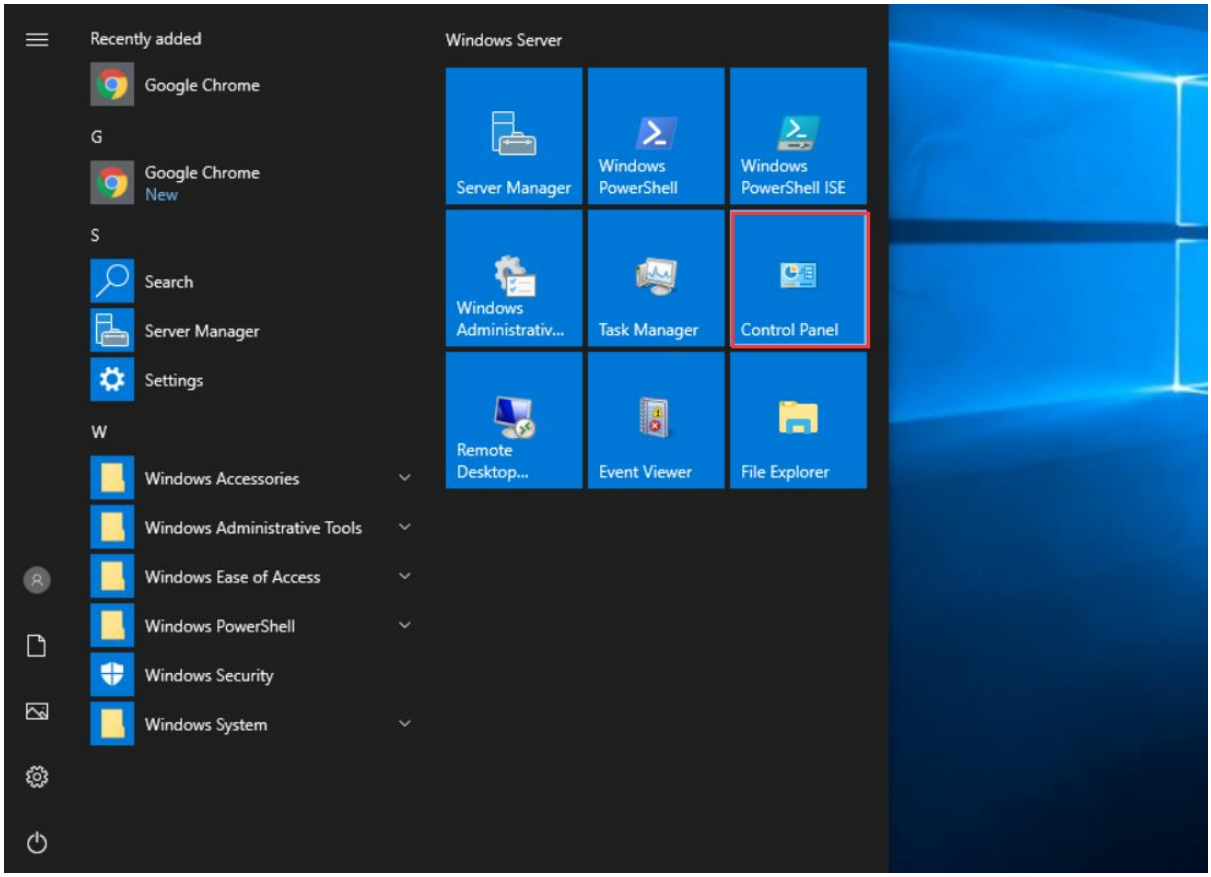


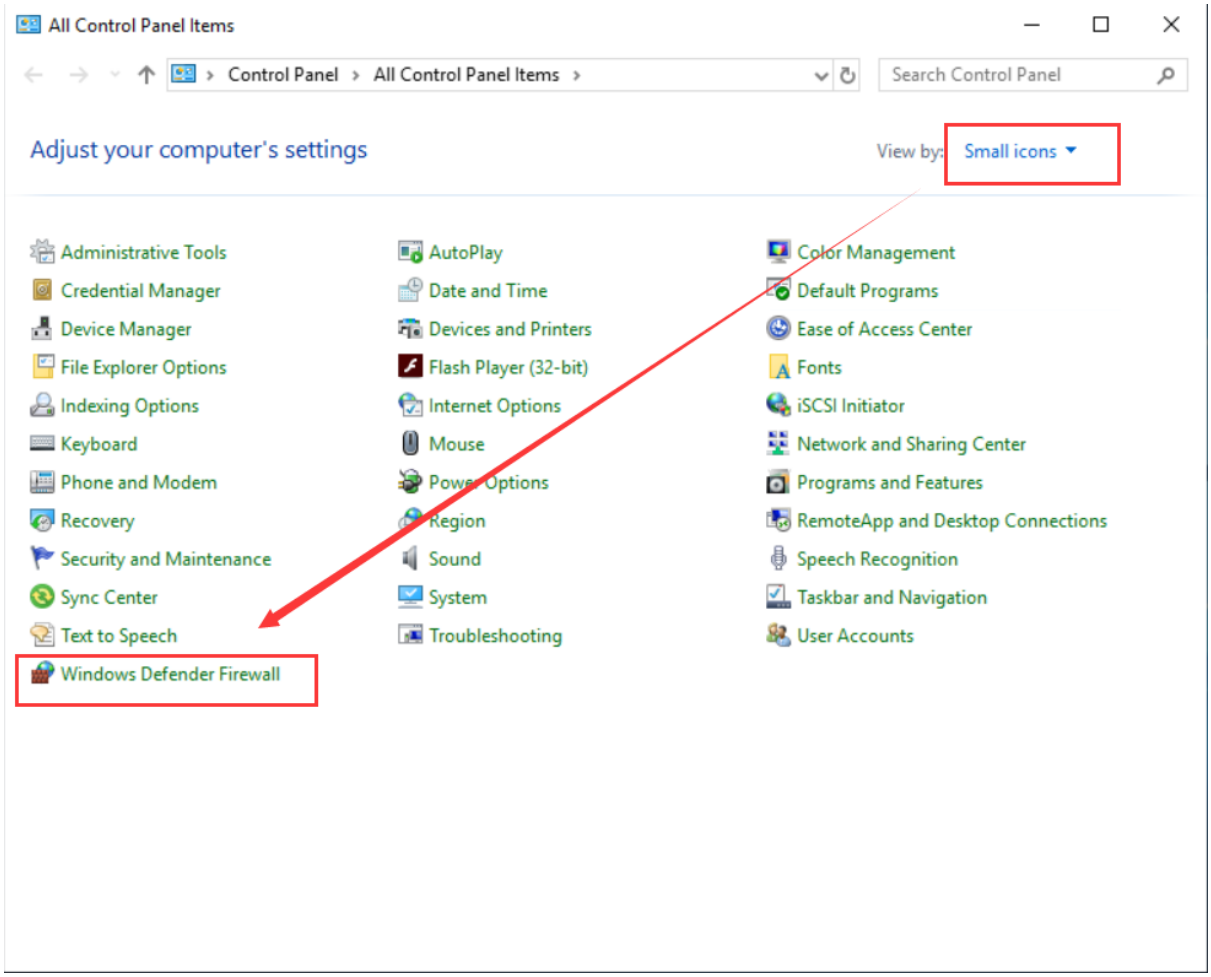
3. Restart test PC 192.168.1.3 dan login ke PC dengan akun domain. Anda dapat melihat bahwa PC 192.168.1.3 sedang online dan metode authentication adalah SSO di IAM.

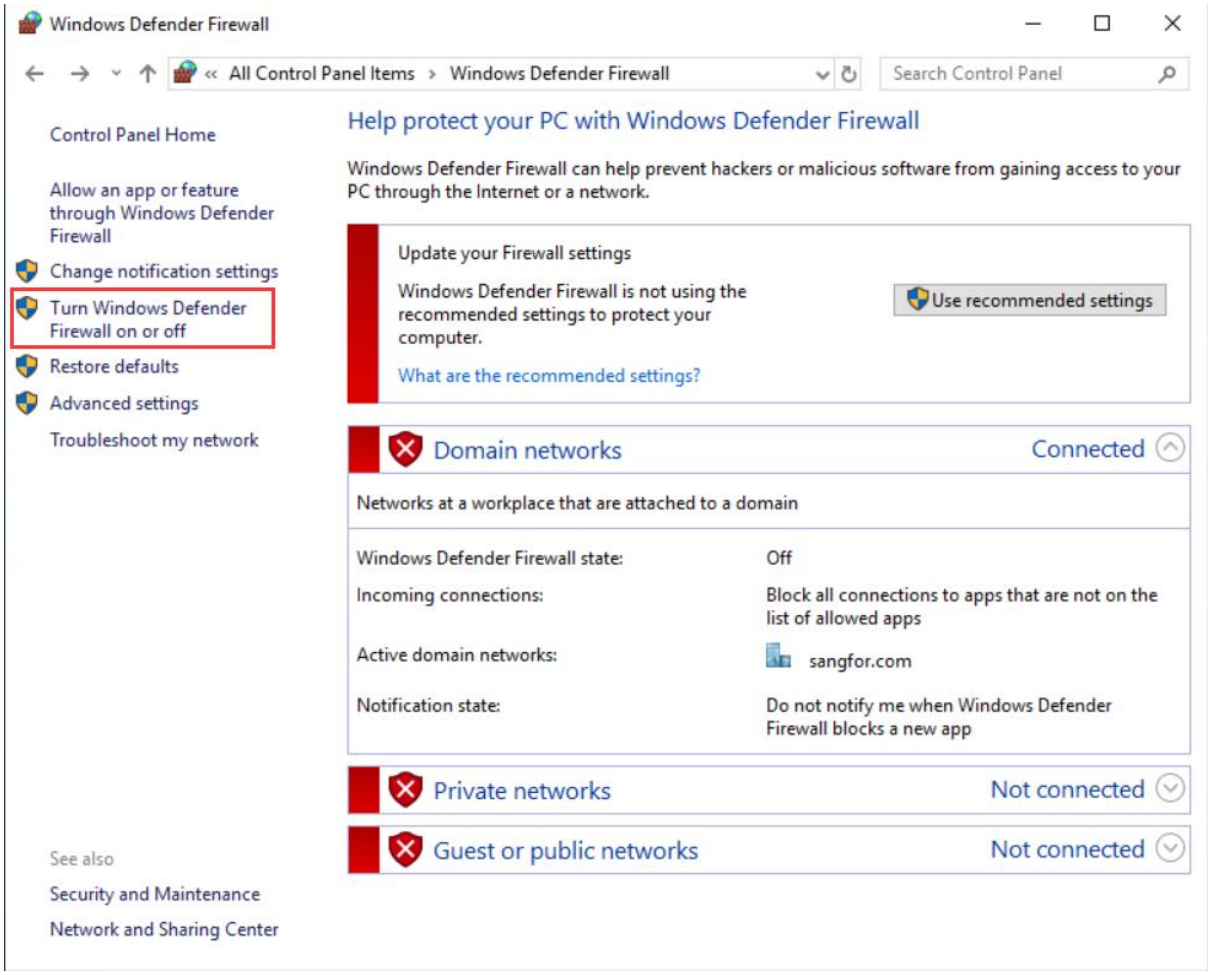


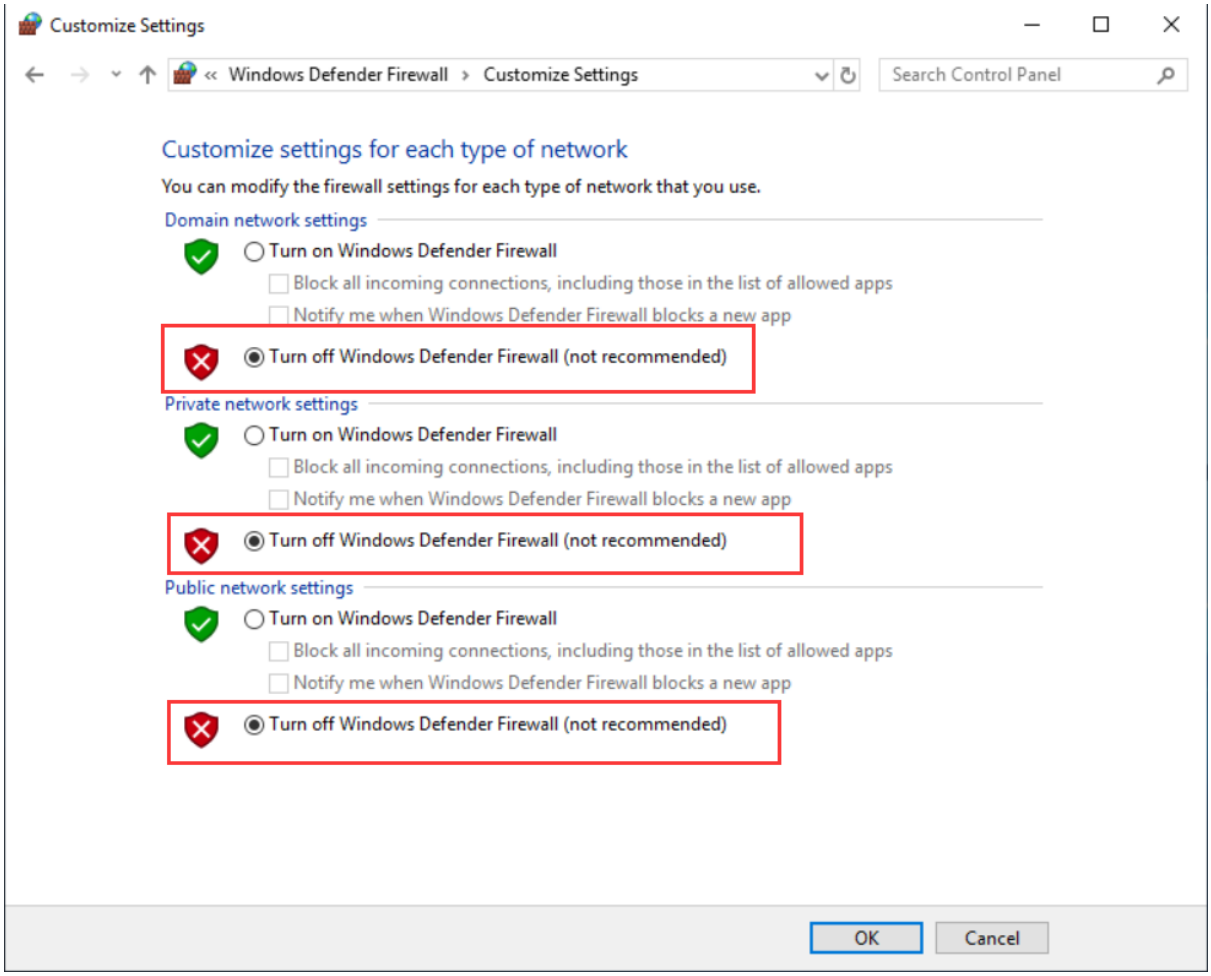
Bab 4 Tindakan Pencegahan

1. Biasanya disarankan untuk mematikan sistem firewall Windows Server, karena mekanisme keamanan Windows Server sangat ketat, yang biasanya menyebabkan perangkat lain tidak dapat memperoleh data yang relevan dari AD Server.

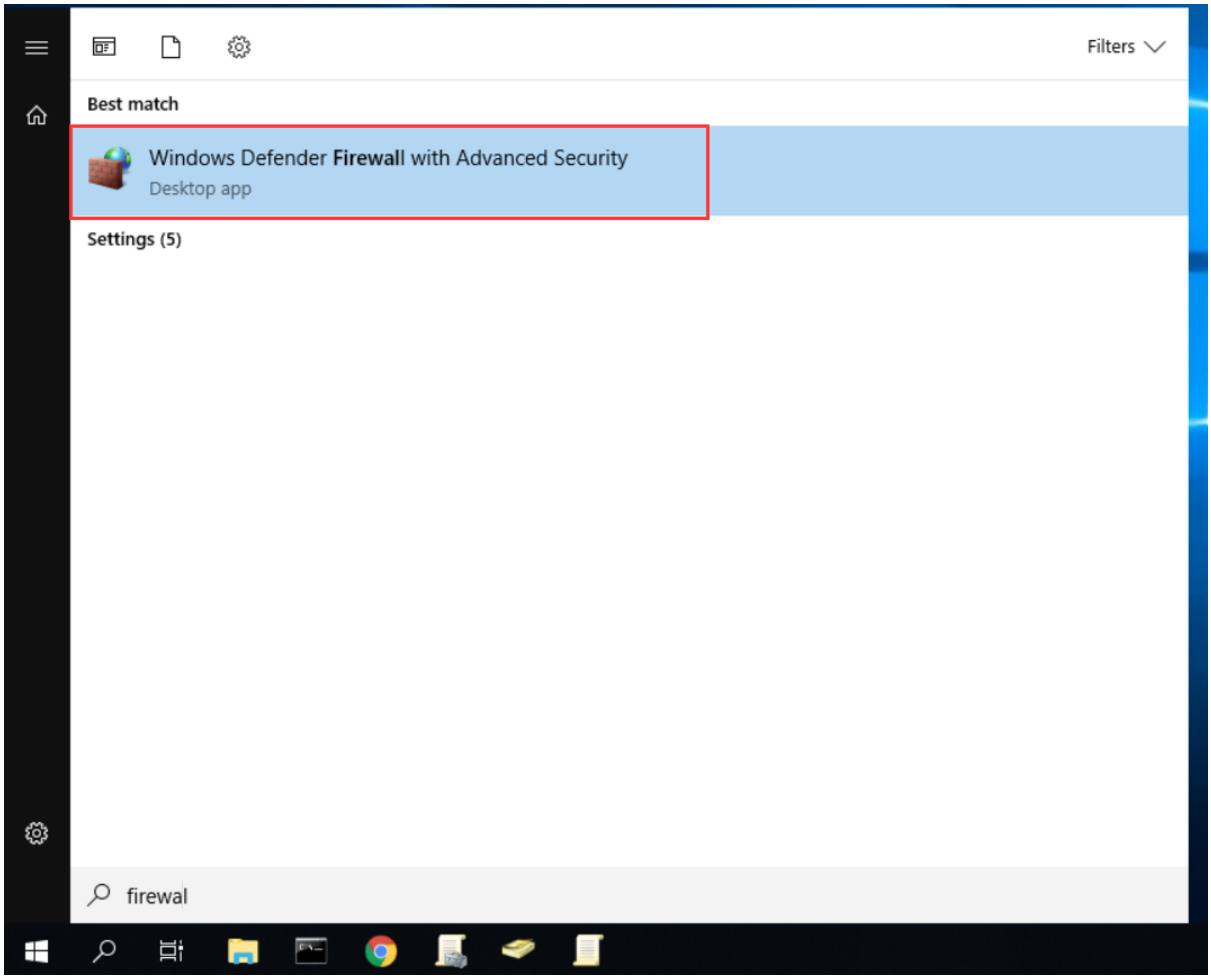

Recently added
Google Chrome
G
Google Chrome
New
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows System
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer


All Control Panel Items
Control Panel › All Control Panel Items ›
Search Control Panel
Adjust your computer's settings
View by: Small icons
Administrative Tools
Credential Manager
Device Manager
File Explorer Options
Indexing Options
Keyboard
Phone and Modem
Recovery
Security and Maintenance
Sync Center
Text to Speech
Windows Defender Firewall
AutoPlay
Date and Time
Devices and Printers
Flash Player (32-bit)
Internet Options
Mouse
Power Options
Region
Sound
System
Troubleshooting
Color Management
Default Programs
Ease of Access Center
Fonts
iSCSI Initiator
Network and Sharing Center
Programs and Features
RemoteApp and Desktop Connections
Speech Recognition
Taskbar and Navigation
User Accounts


Windows Defender Firewall
All Control Panel Items › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Defender Firewall is not using the recommended settings to protect your computer.
What are the recommended settings?
Use recommended settings
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Defender Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active domain networks:
sangfor.com
Notification state:
Do not notify me when Windows Defender Firewall blocks a new app
Private networks
Not connected
Guest or public networks
Not connected
See also
Security and Maintenance
Network and Sharing Center



Atau Anda dapat menambahkan aturan firewall secara manual untuk mengizinkan perangkat terkait untuk mengakses AD Server.


Filters
Best match
Windows Defender Firewall with Advanced Security
Desktop app
Settings (5)
firewal

Aktivitas Domain Script SSO