



IAM

Praktik Terbaik untuk

Skenario_Aktivitas Domain ADSSO

Versi 12.0.42



Catatan Perubahan

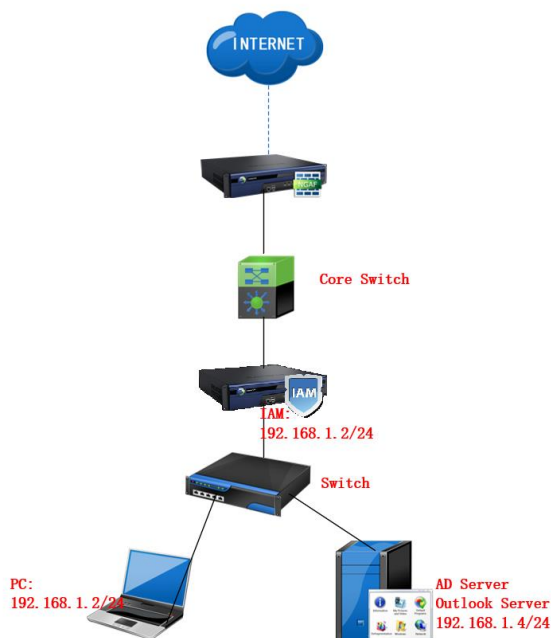
Tanggal	Deskripsi Perubahan
Agustus 4, 2020	Rilis Dokumen Versi 12.0.42.
Mei 17, 2021	Dokumen update Versi 12.0.42.

Daftar Isi

Bab 1 Skenario	1
1.1 Langkah Konfigurasi.....	错误!未定义书签。
Bab 2 Bagaimana untuk Konfigurasi Aktivitas Domain Server.....	2
2.1 Instal Fungsi MS AD	2
2.2 Konfigurasi domain controller server	10
2.3 Buat username dan passwords untuk pengguna lain di domain	16
2.4 Gabung PC ke domain.....	20
2.5 Aktifkan fungsi log audit dari AD Server	26
Bab 3 Bagaimana untuk Konfigurasi IAM.....	29
3.1 Tambah LDAP server.....	29
3.2 Konfigurasi option SSO authentication	30
3.3 Konfigurasi authentication policy pada IAM	31
Bab 4 Tindakan Pencegahan.....	32

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 Microsoft seperti Outlook; pelanggan ingin kontrol pengguna intranet dan memerlukan visualisasi kontrol, artinya, spesifik domain dapat dikueri. Perilaku online 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 ini adalah beberapa cara mengkombinasikan Microsoft AD domain authentication, script SSO memiliki tingkat keberhasilan tertinggi, tetapi pelanggan tidak mengizinkan untuk mengirimkan script melalui Microsoft AD domain, jadi kita bisa memilih metode ADSSO.



AD Server:

IP: 192.168.1.4

Domain Name: sangfor.com

Account/Password: administrator/@sangfor123

Test PC:

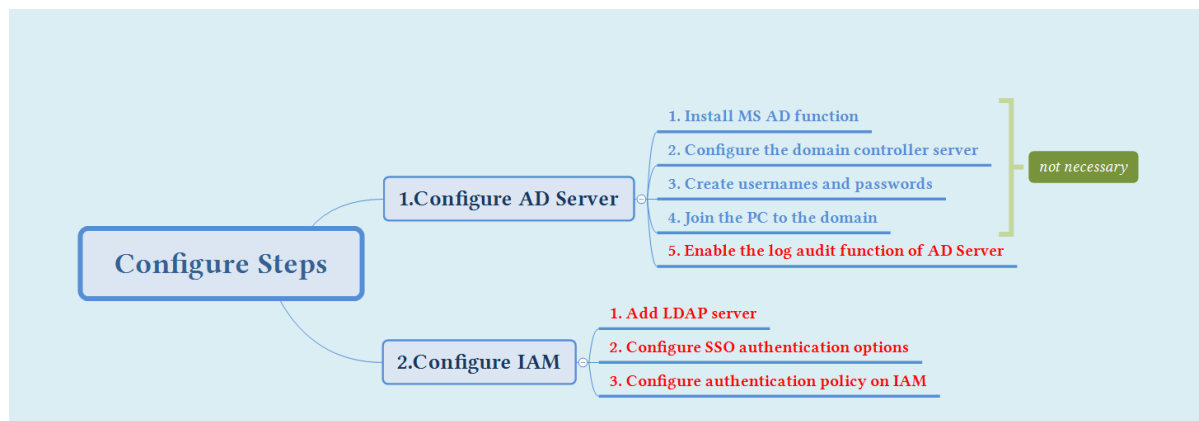
IP: 192.168.1.3

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.

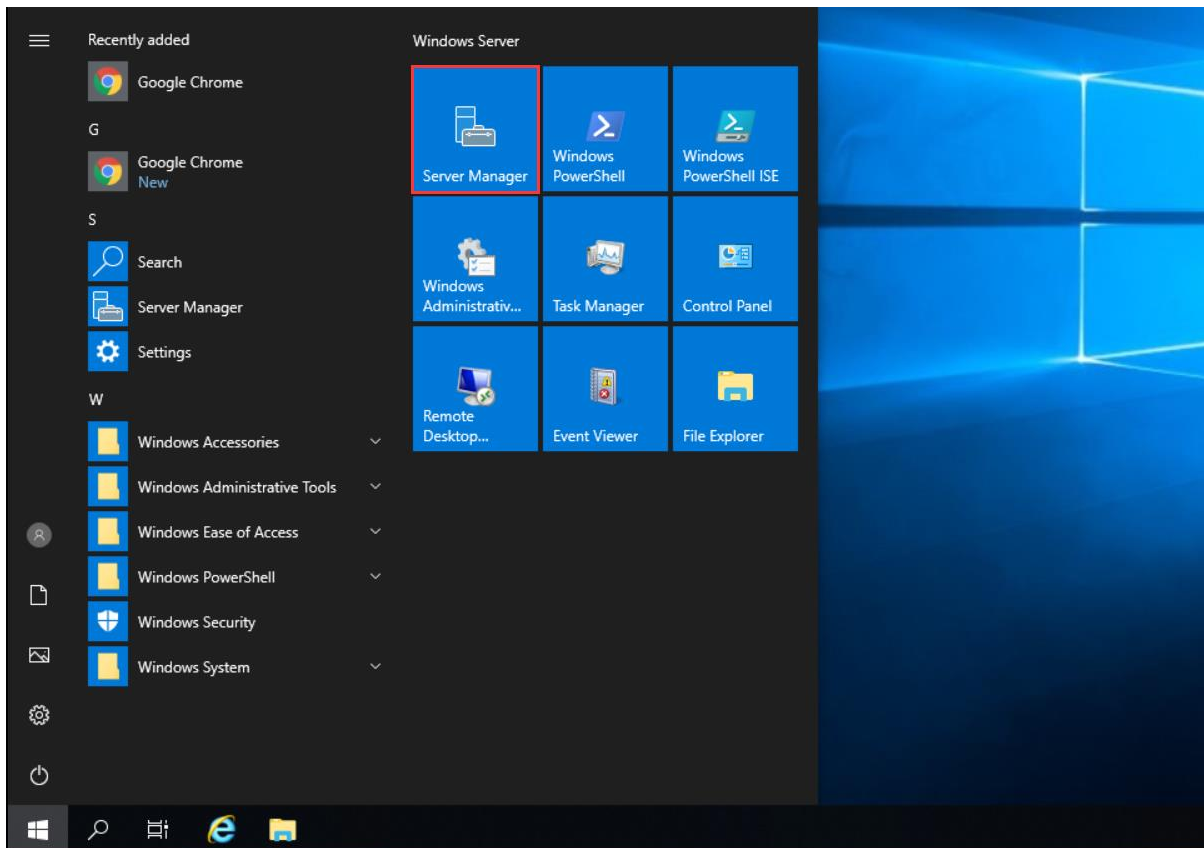


Bab 2 Bagaimana untuk Konfigurasi Aktivitas Domain Server

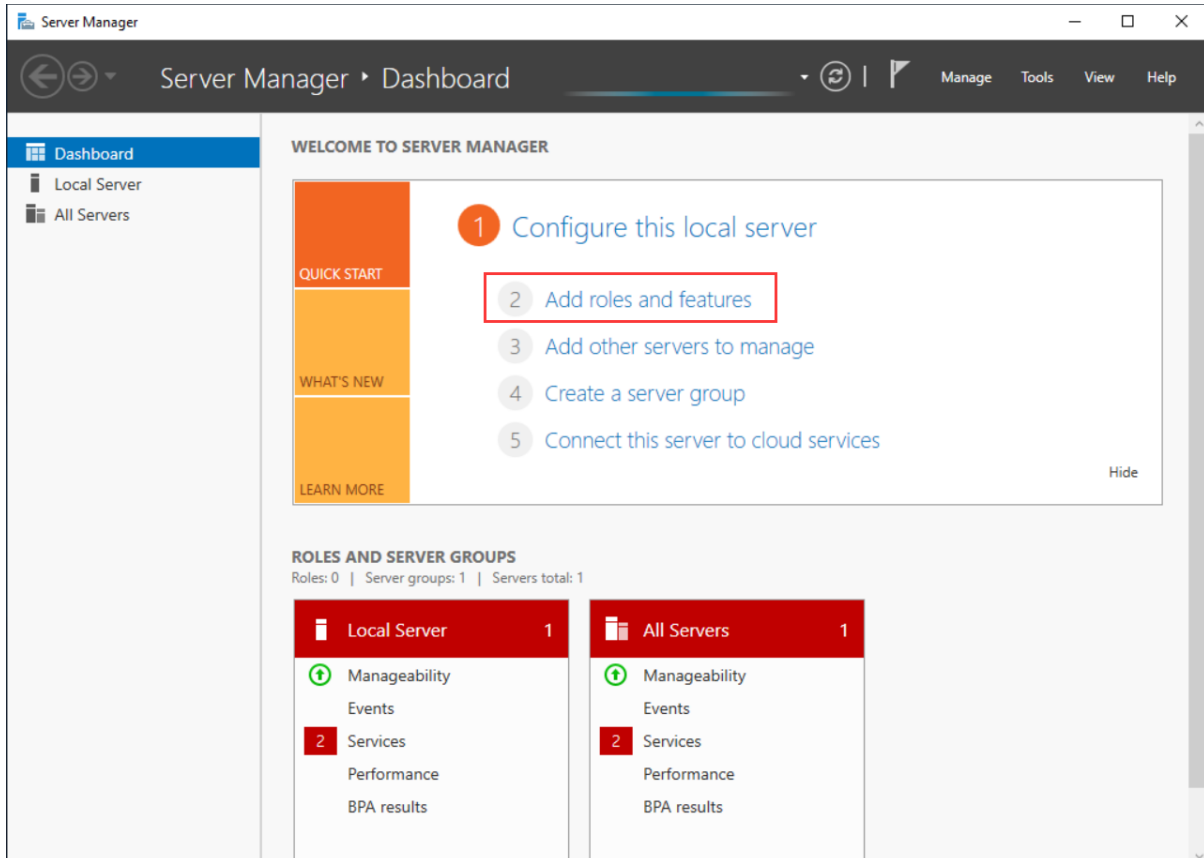
2.1 Instal Fungsi MS AD

1. Buka Server Manager pada Windows Server 2019.

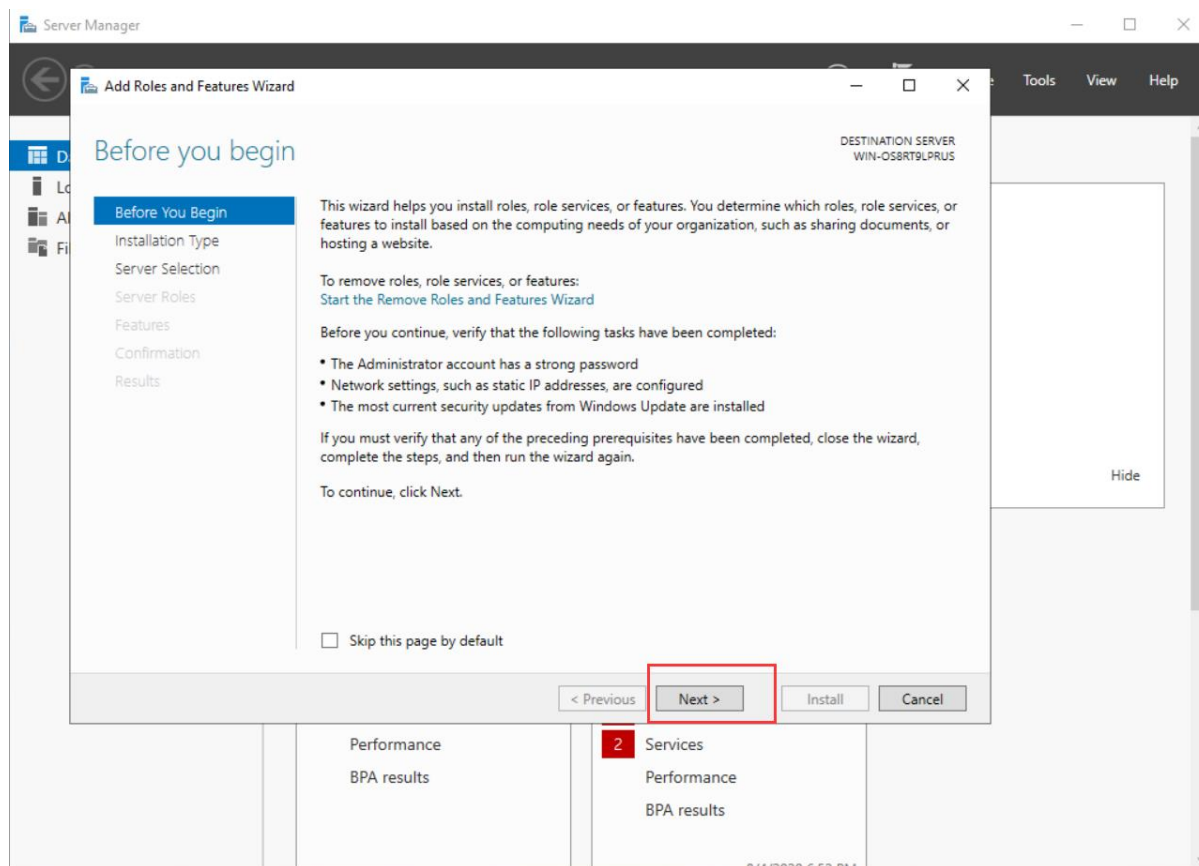
Aktivitas Domain ADSSO



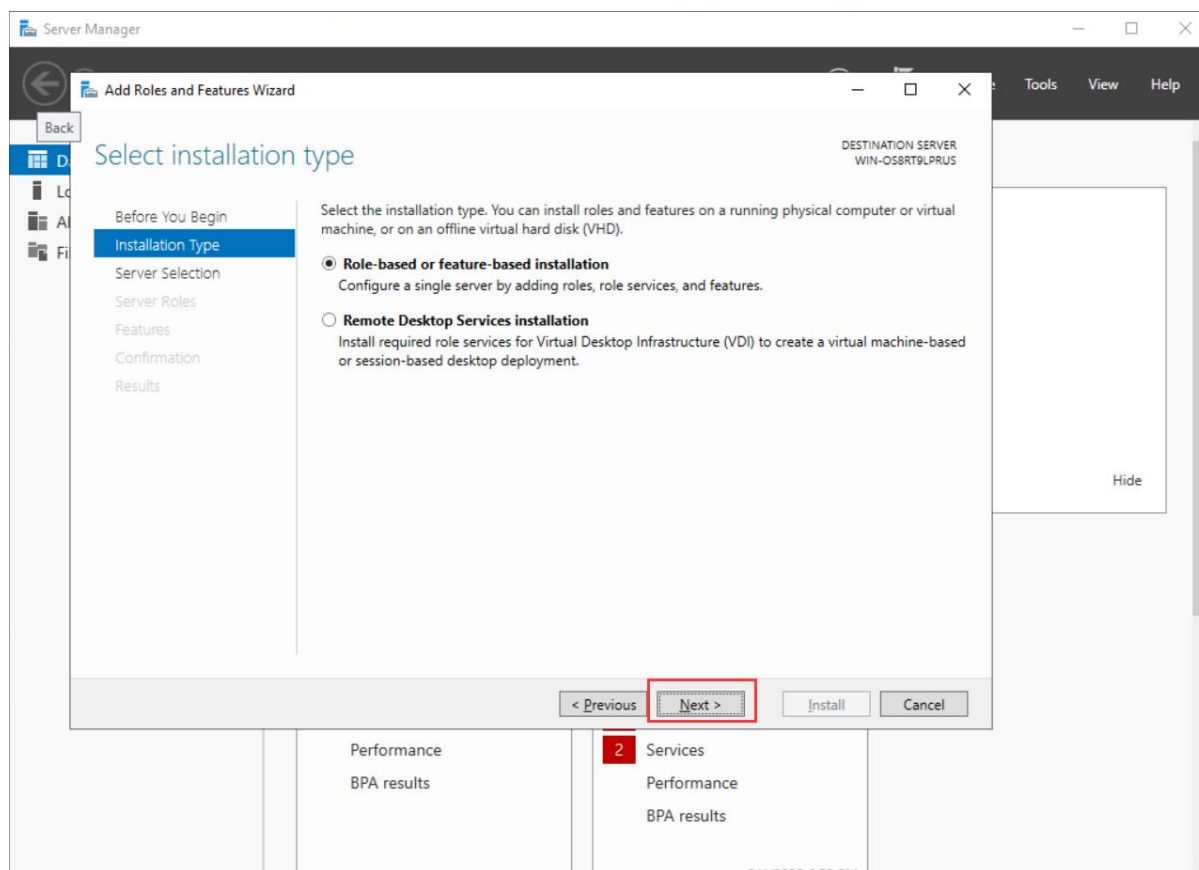
2.Klik "Add roles and features".



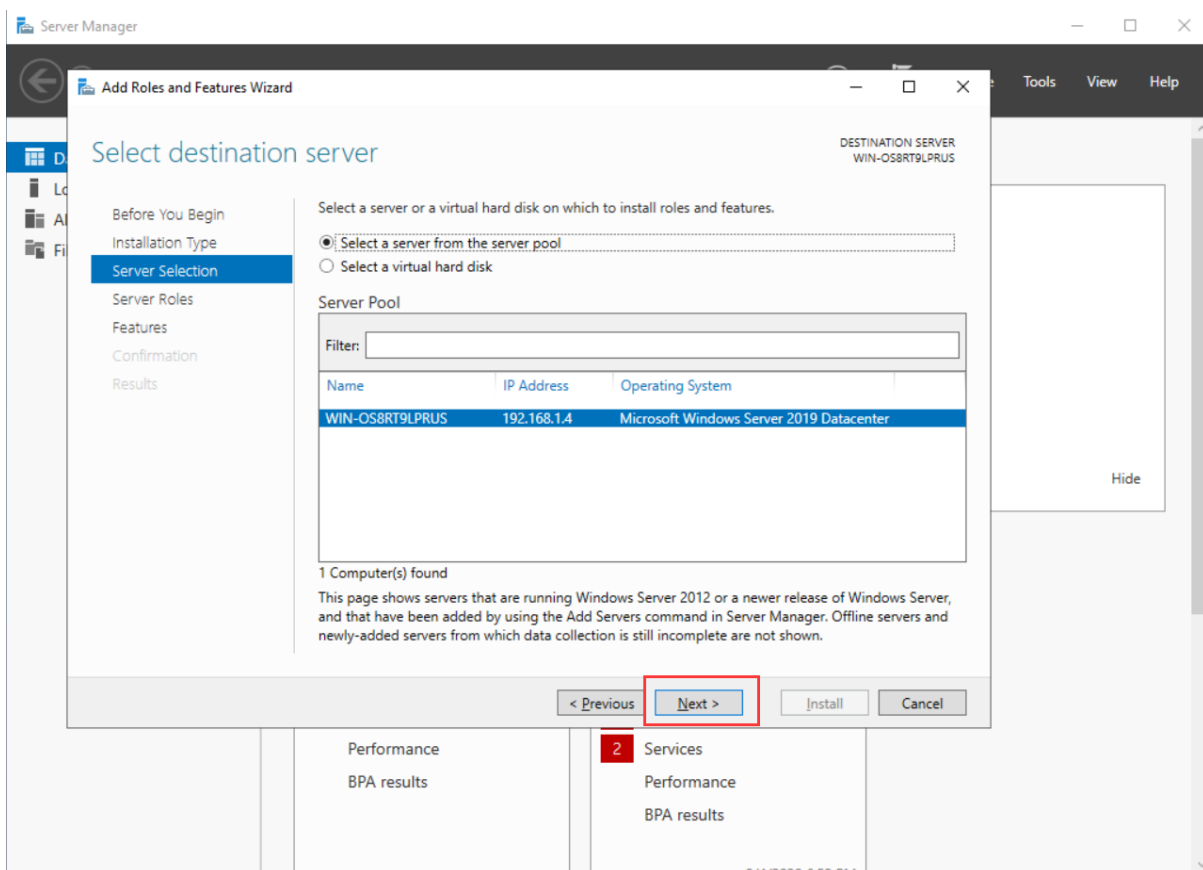
3.Klik "Next".



4. Klik "Next".

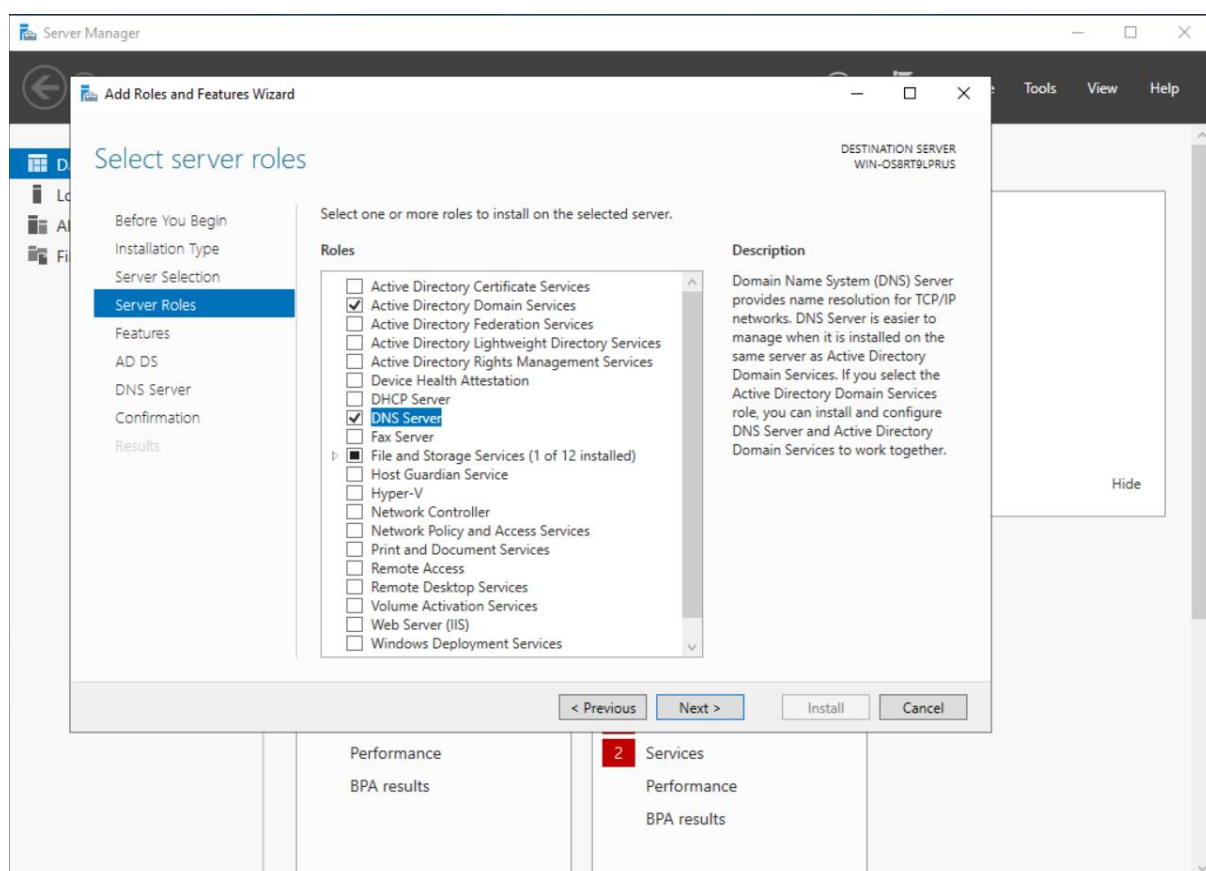
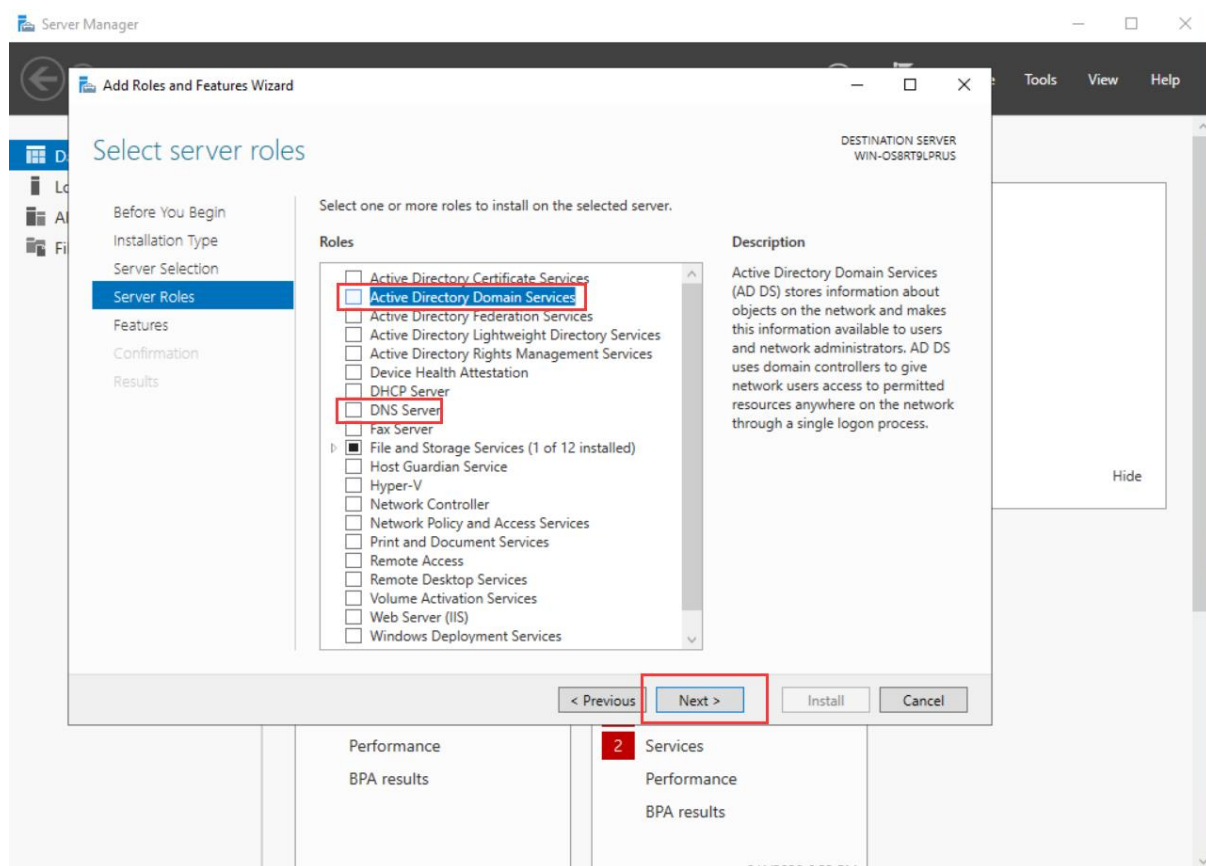


5. Klik "Next".

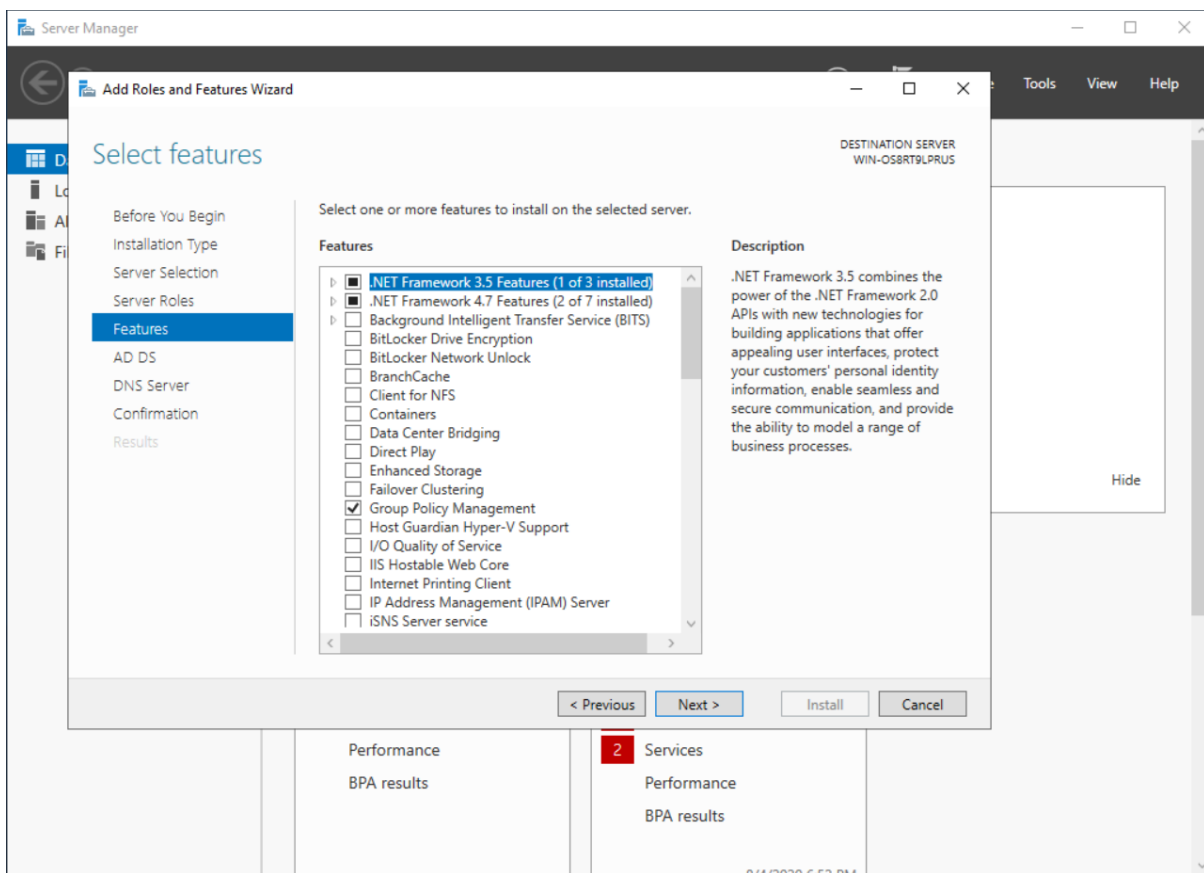


6. Pilih fungsi yang perlu diinstal "Active Directory Domain Services" dan "DNS Server", lalu klik "Next".

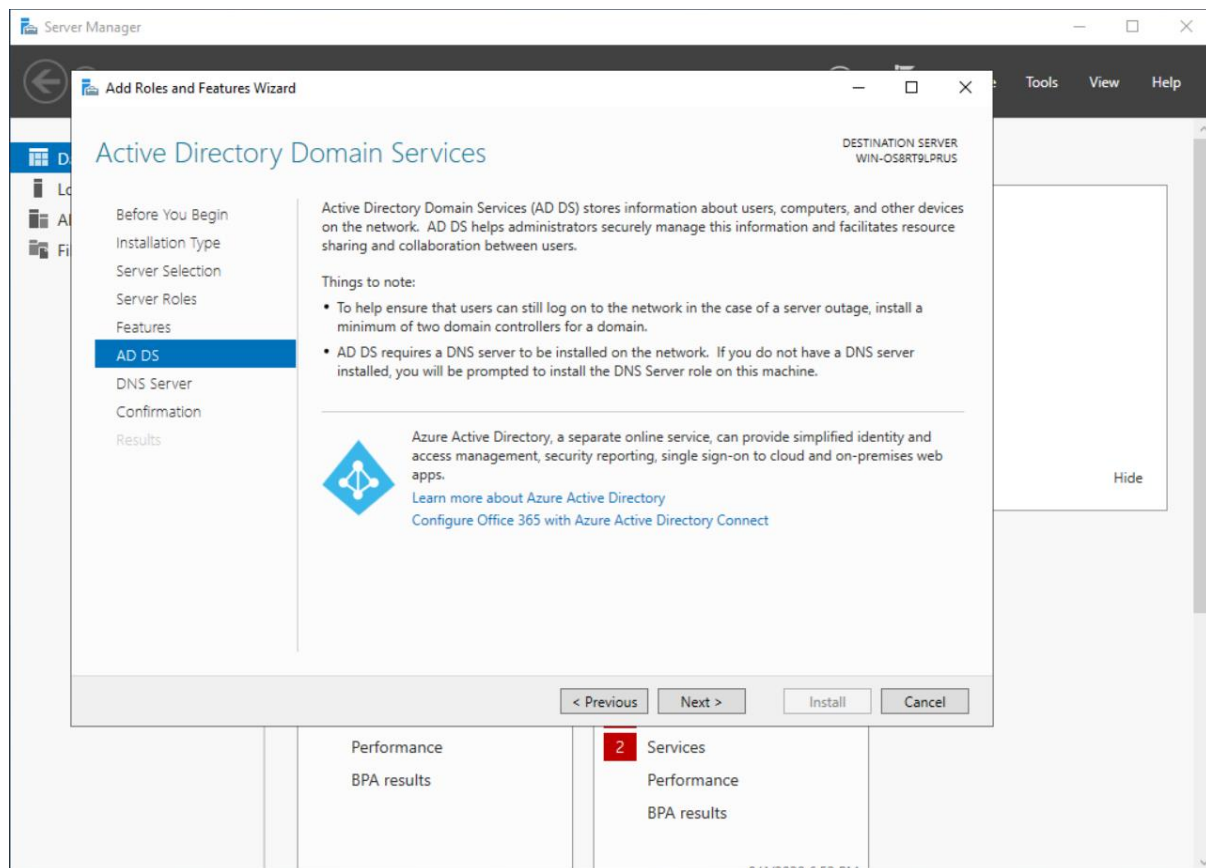
Aktivitas Domain ADSSO



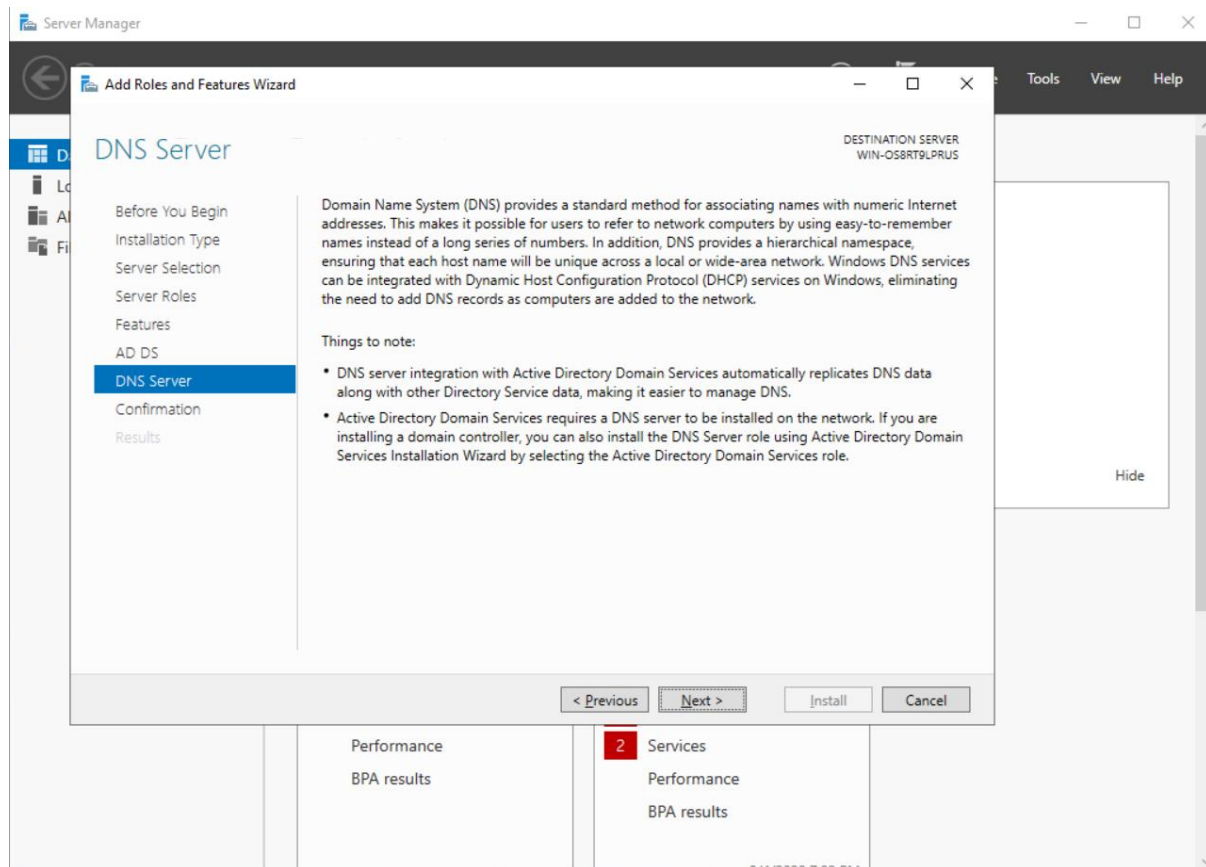
7. Klik "Next".



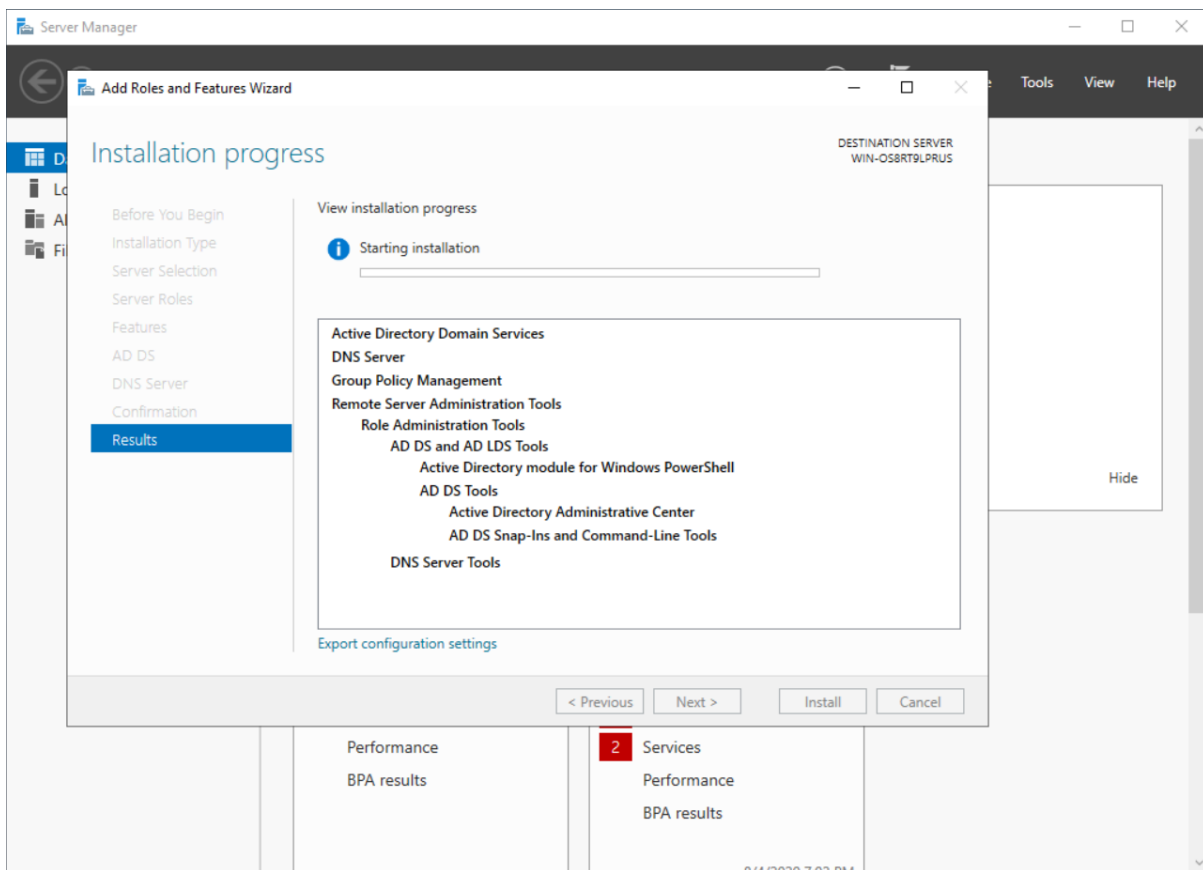
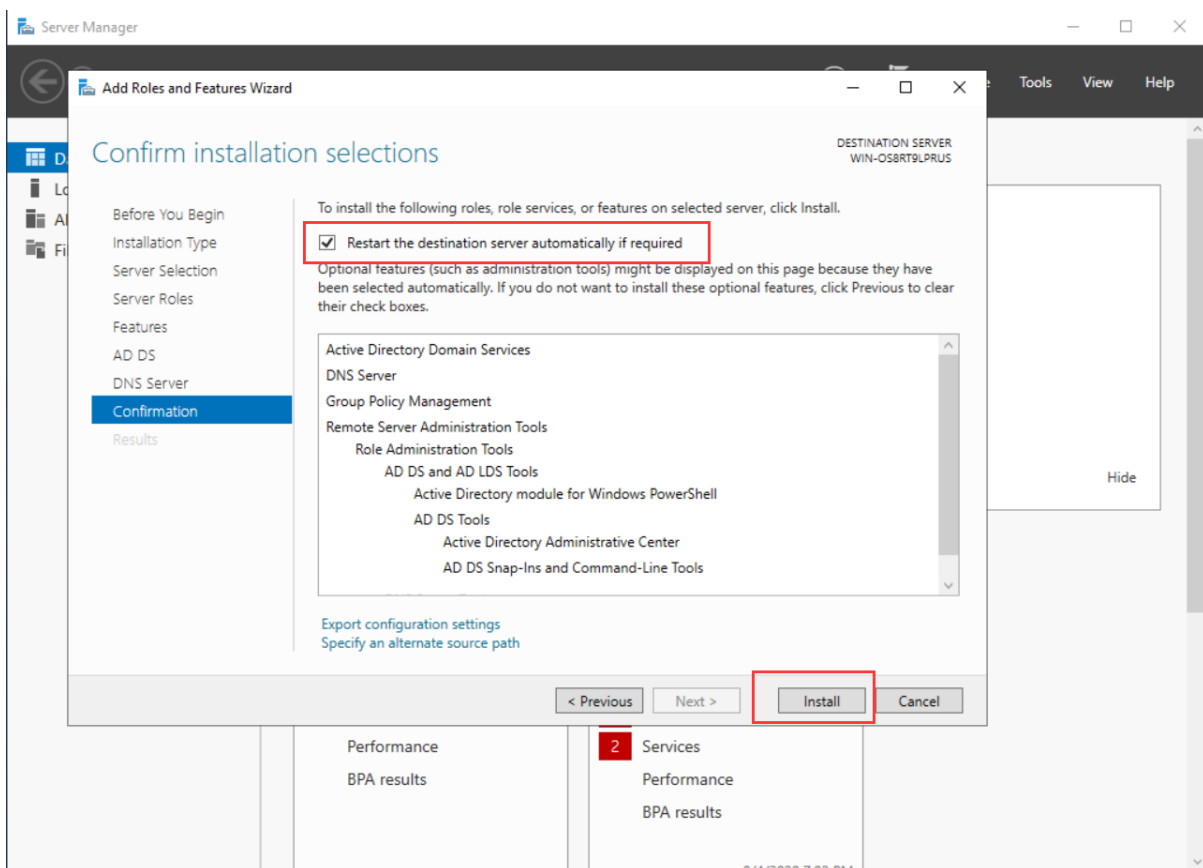
8. Klik "Next".



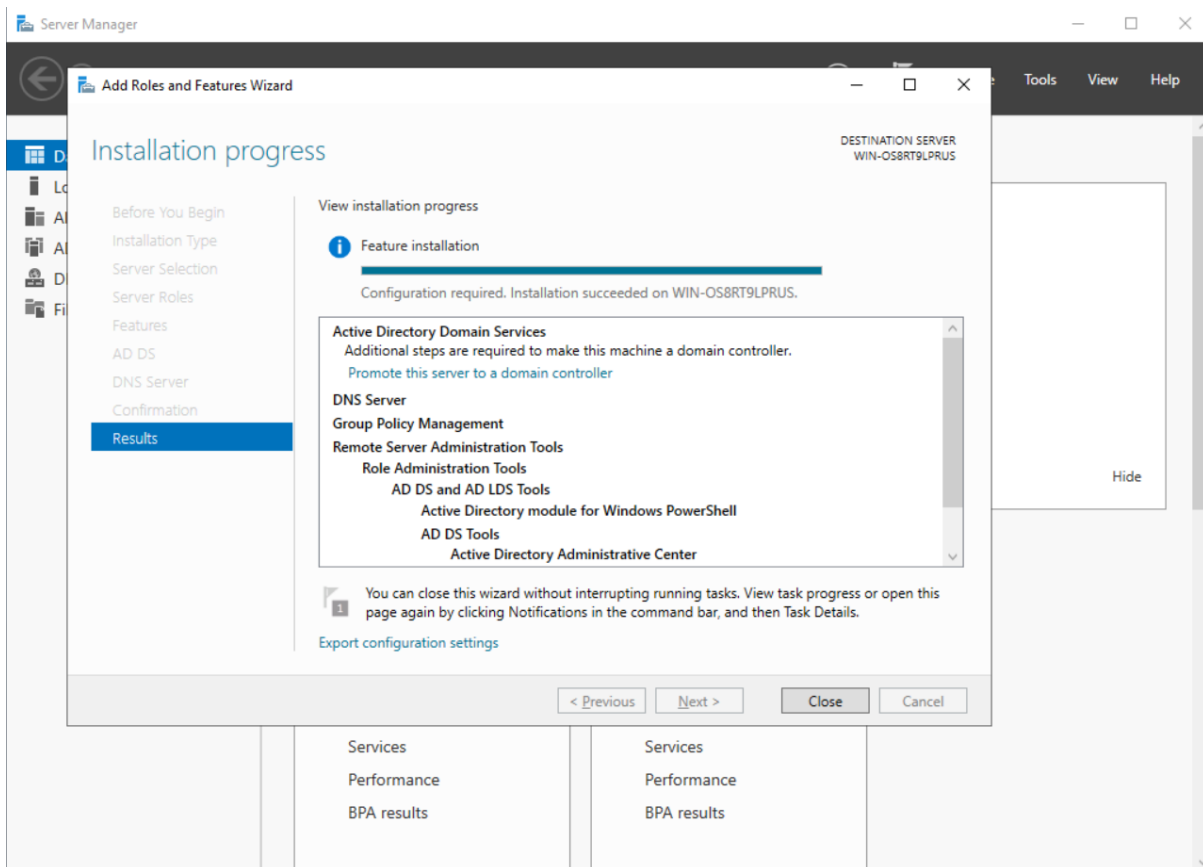
9. Klik "Next".



10. Klik "Install".



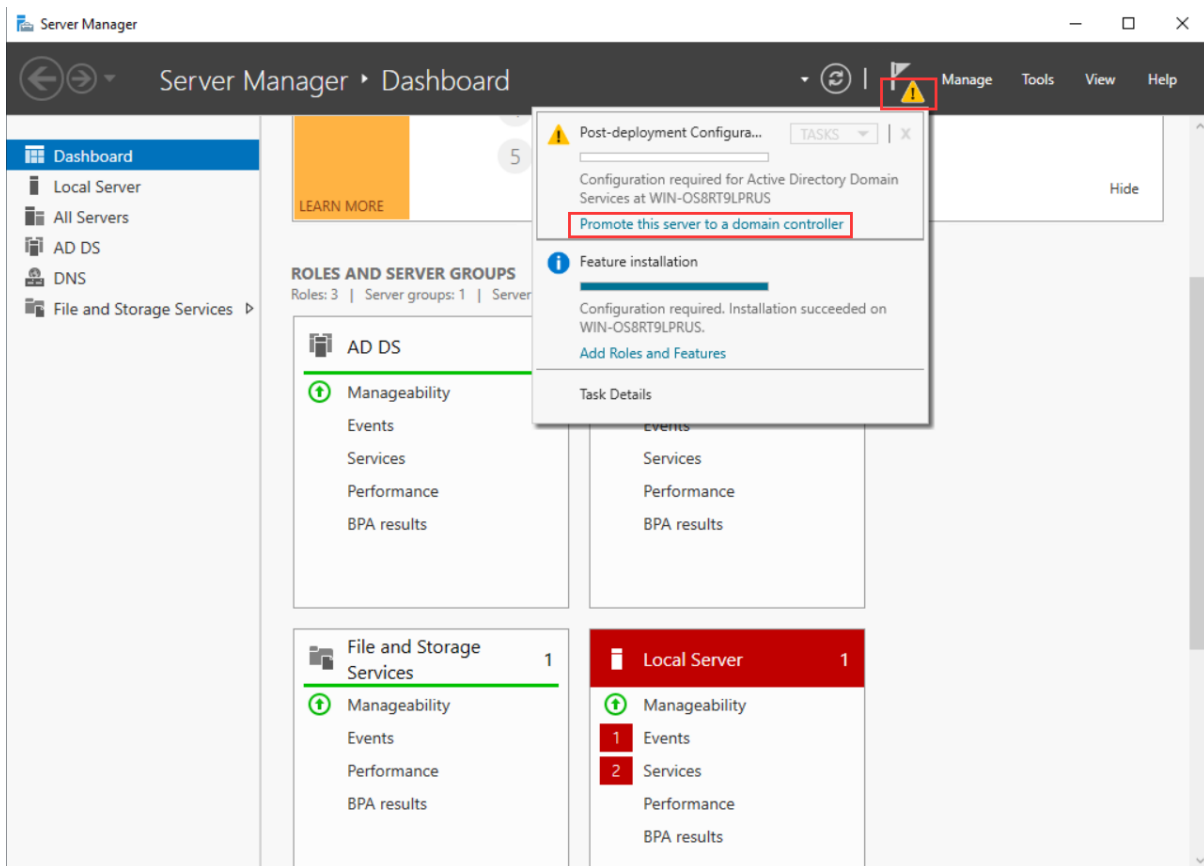
11. Klik "Close" setelah instalasi.



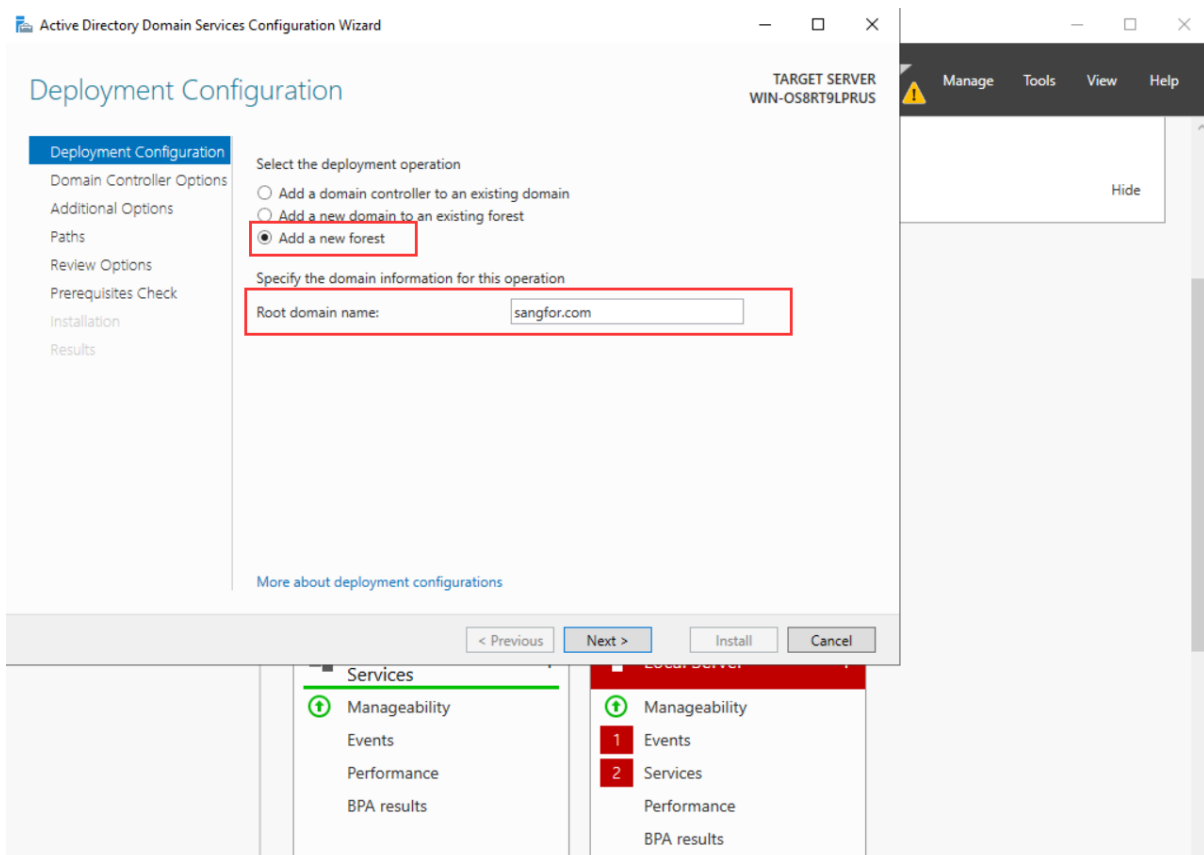
2.2 Konfigurasi domain controller server

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

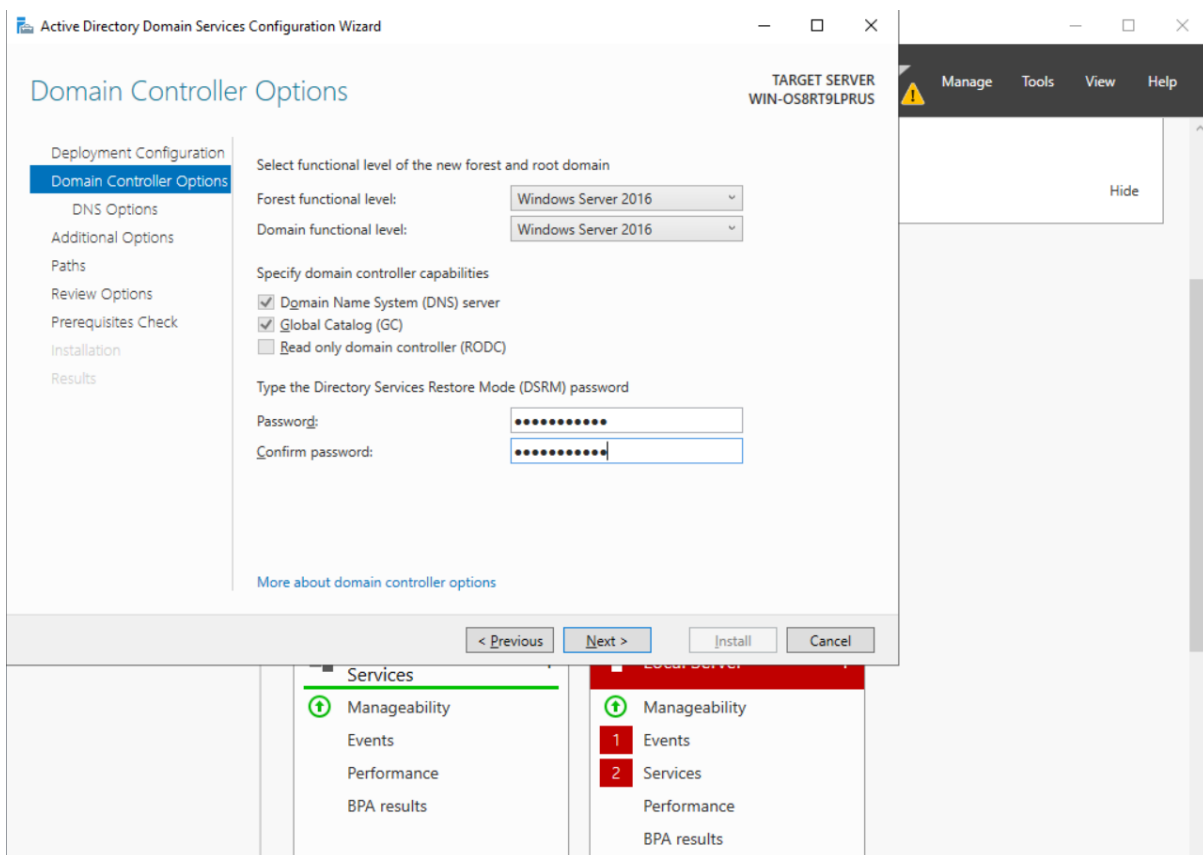
Aktivitas Domain ADSSO



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

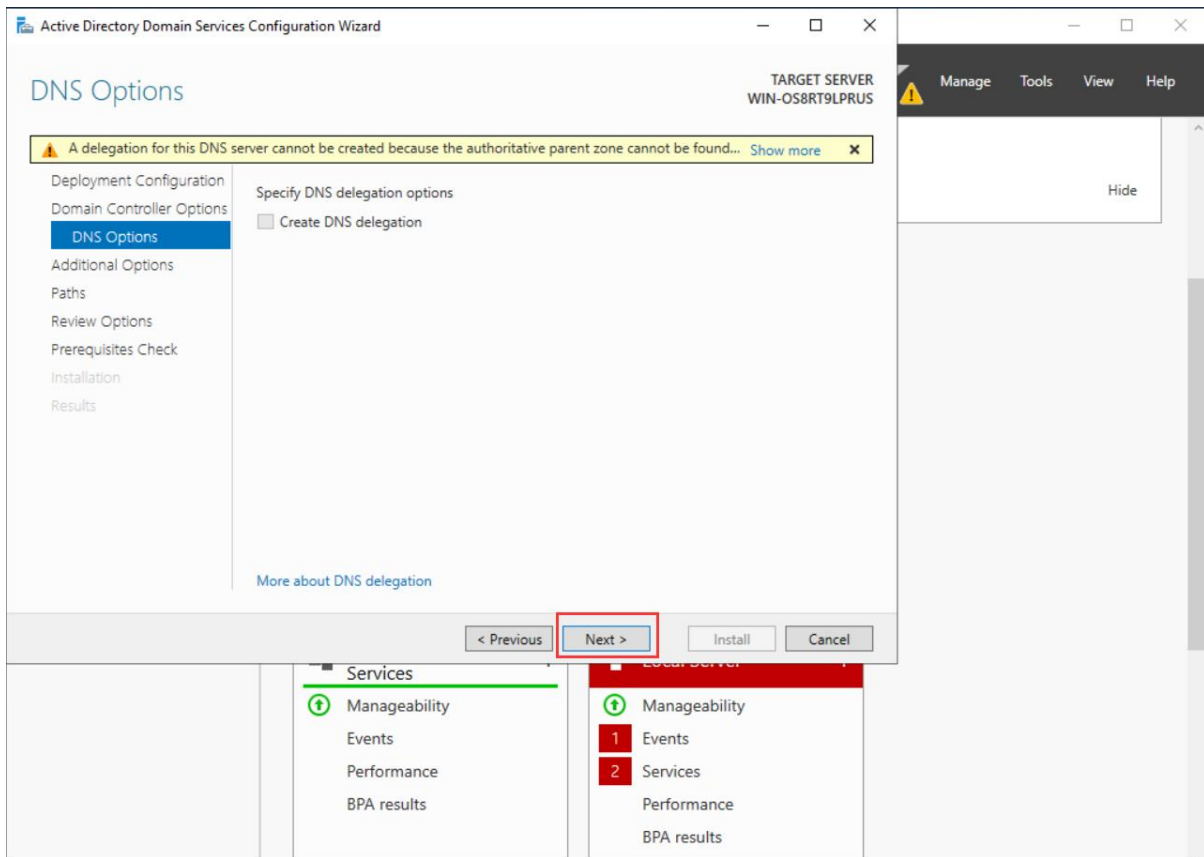


3. Atur password, misalnya @sangfortest.

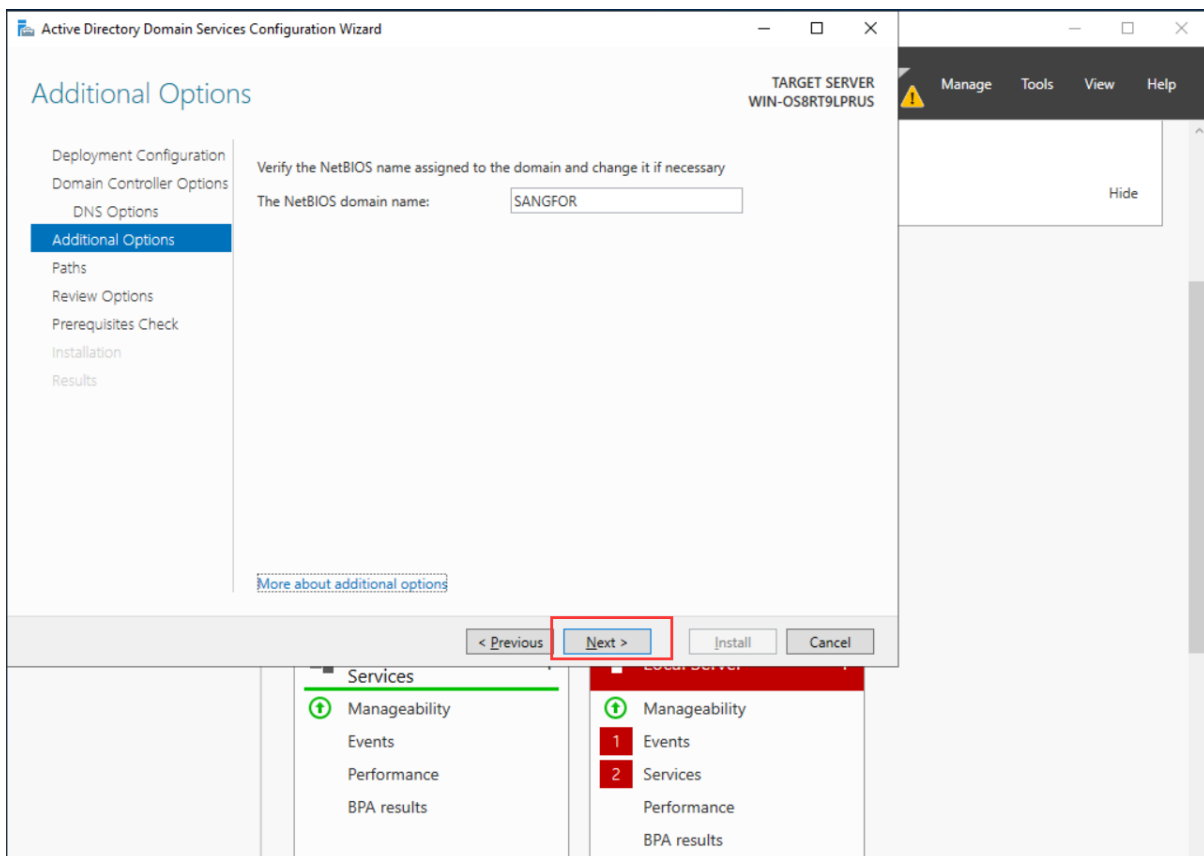


4. Klik "Next".

Aktivitas Domain ADSSO

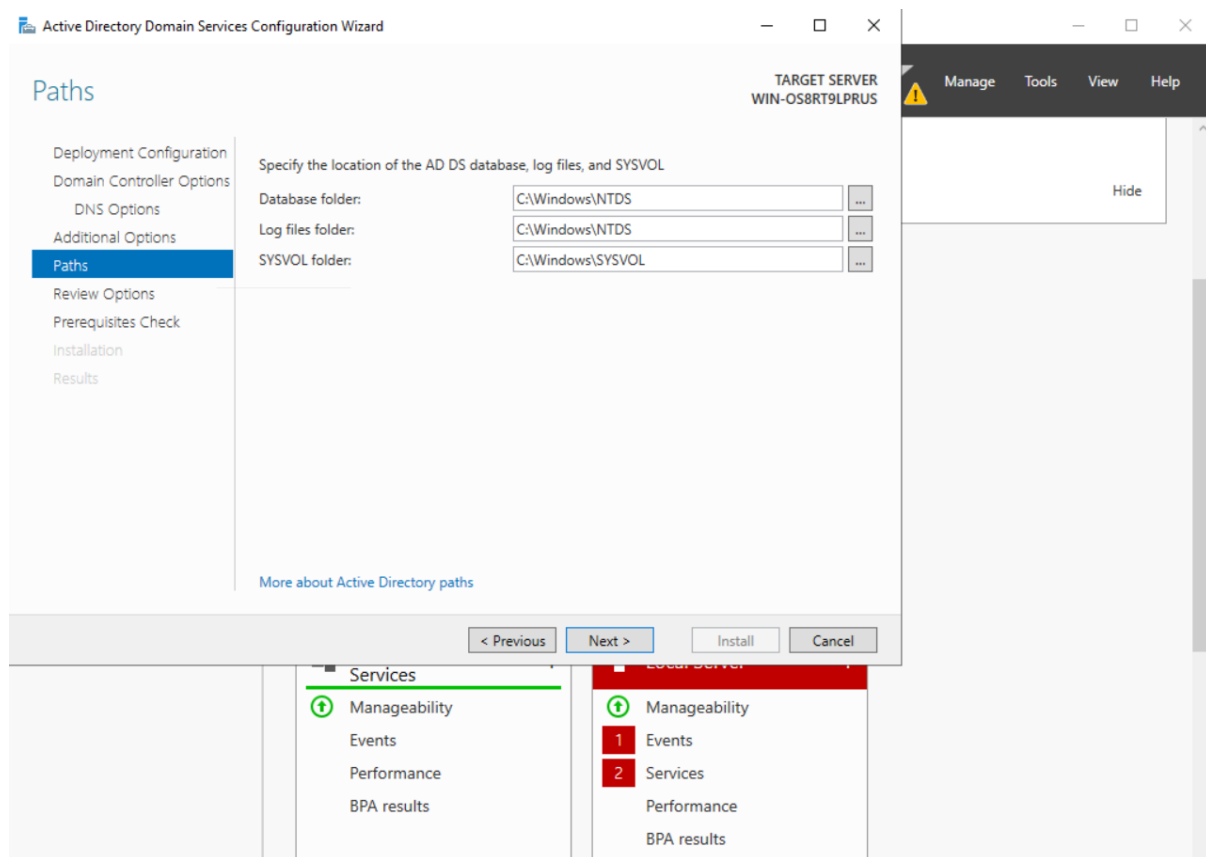


5. Atur NETBIOS Domain Name, Anda dapat menggunakan default SANGFOR.

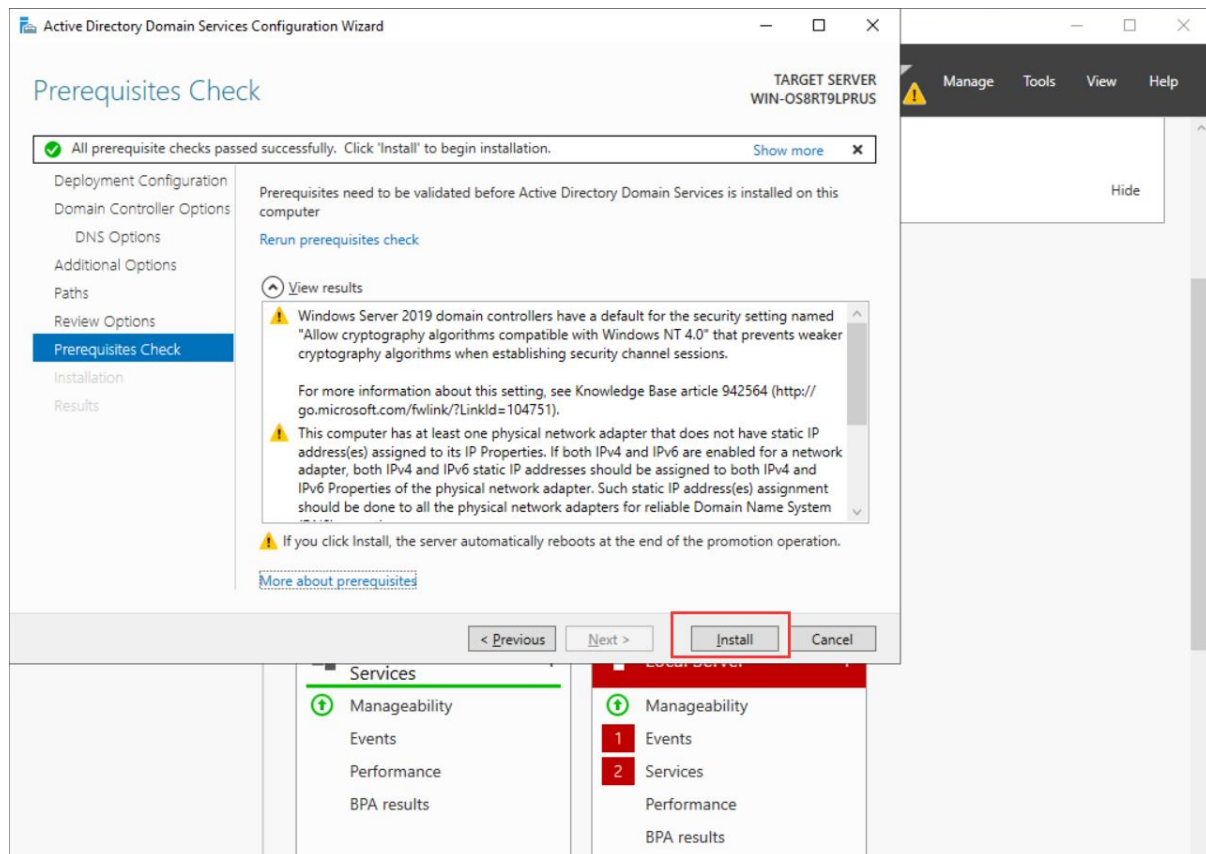


6. Klik "Next".

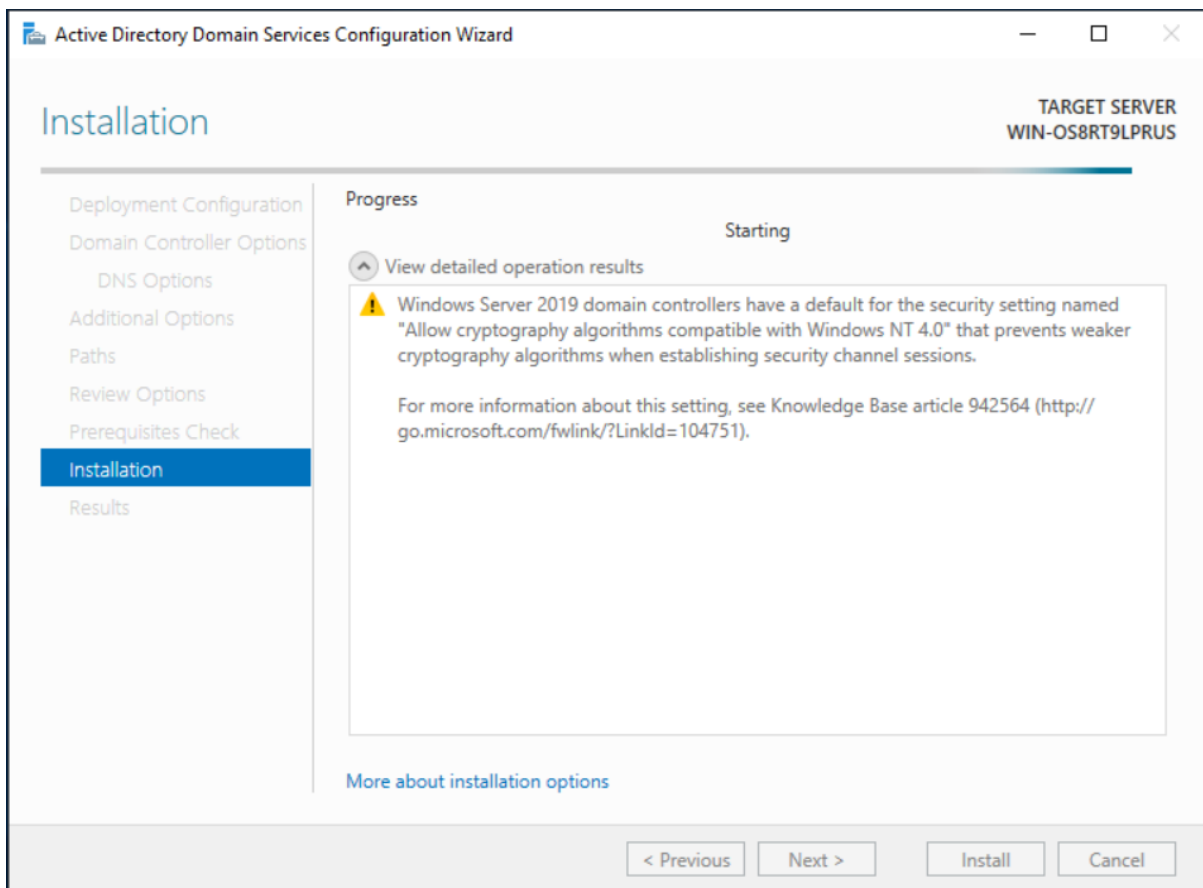
Aktivitas Domain ADSSO



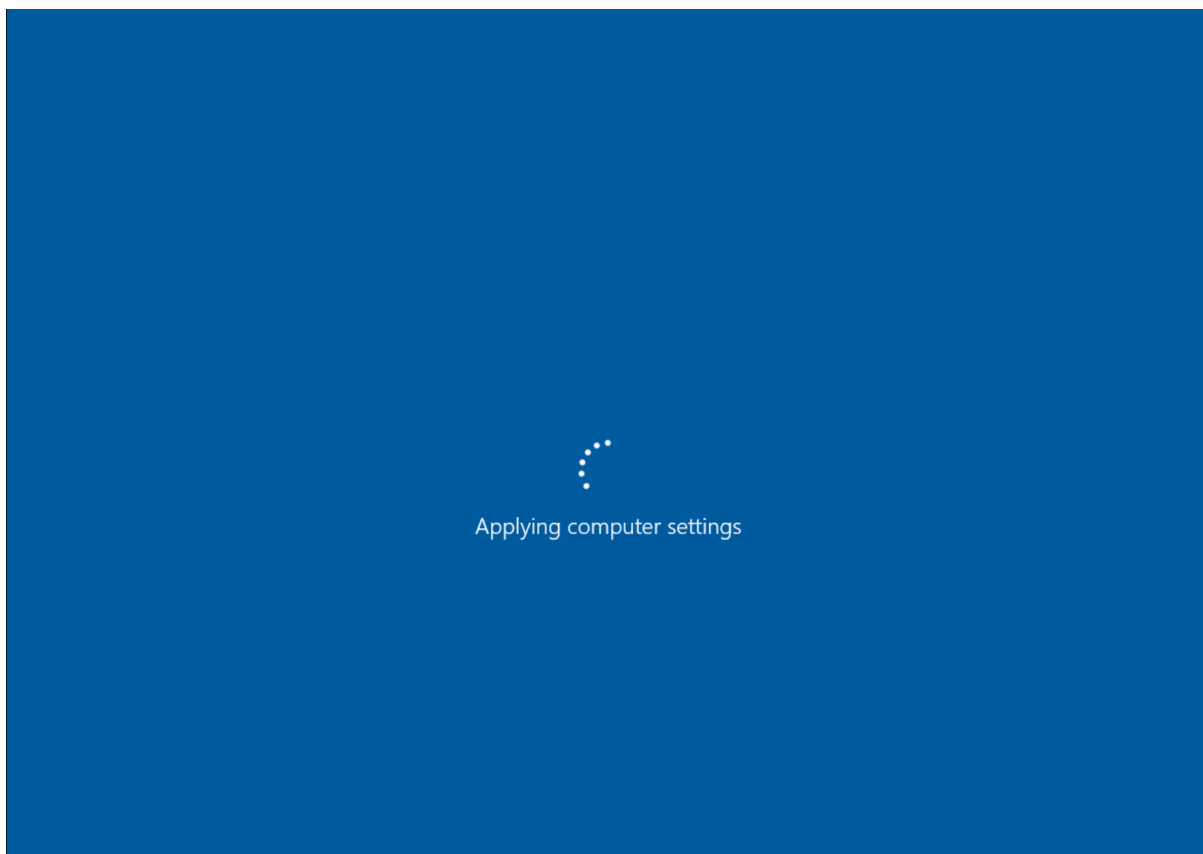
7. Pilih "Install".



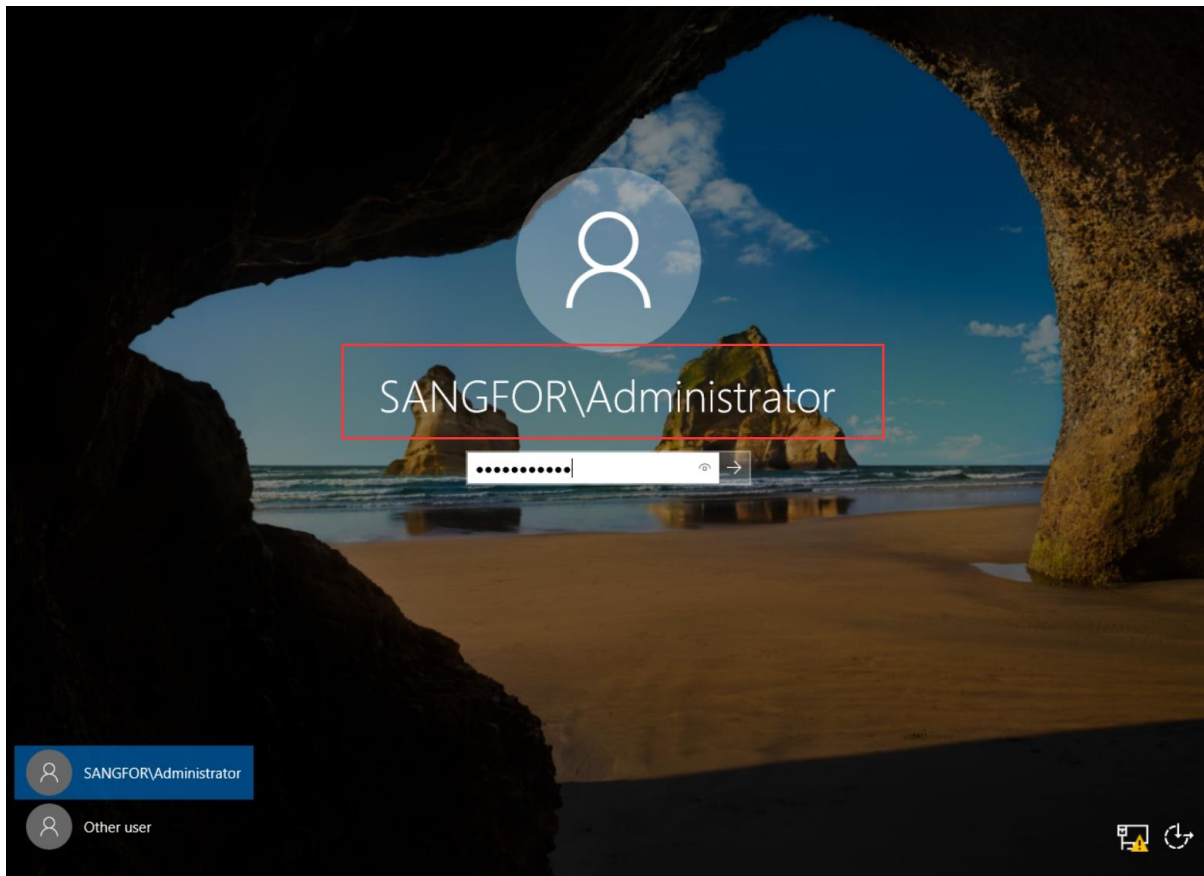
8. Tunggu peralatan untuk instal dan deploy fungsi yang berhubungan.



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

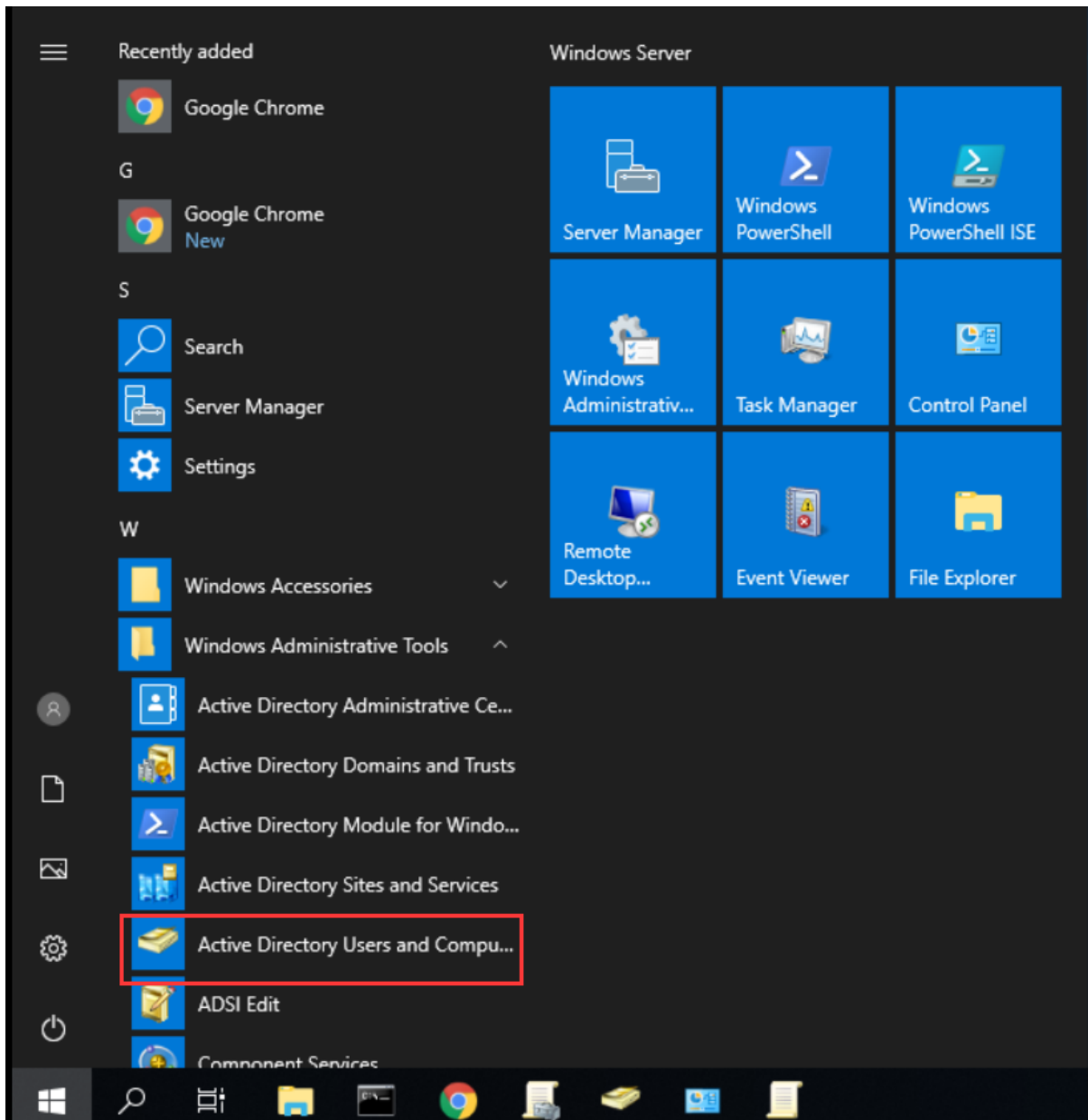


10. Setelah Windows Server restart, Anda dapat melihat di halaman login bahwa administrator yang masuk ke system operasi telah menjadi administrator di domain, dan login password sama dengan password dari akun administrator lokal.



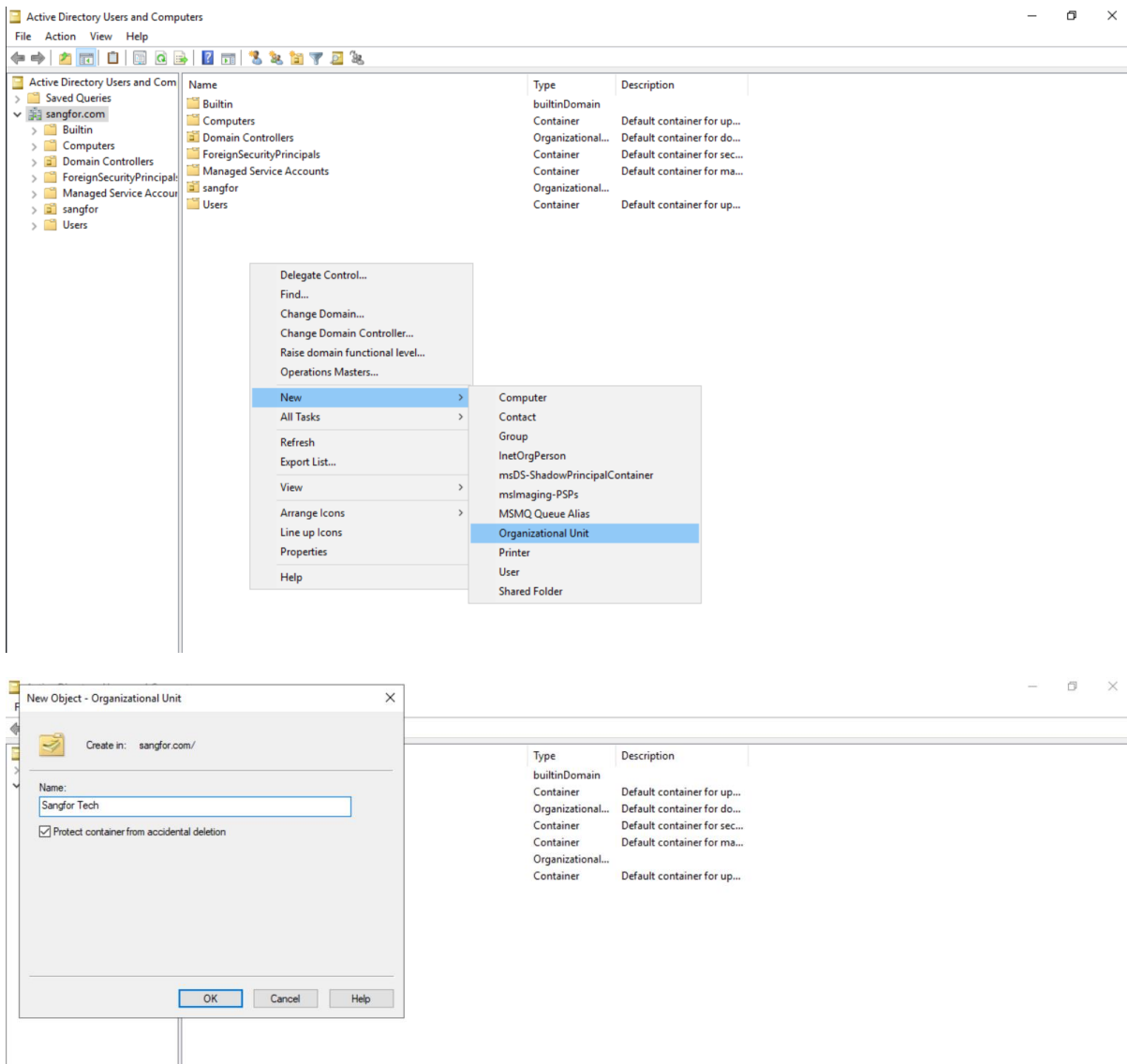
2.3 Buat usernames dan passwords untuk pengguna lain di domain

1. Buka "Active Directory Users and Computers".

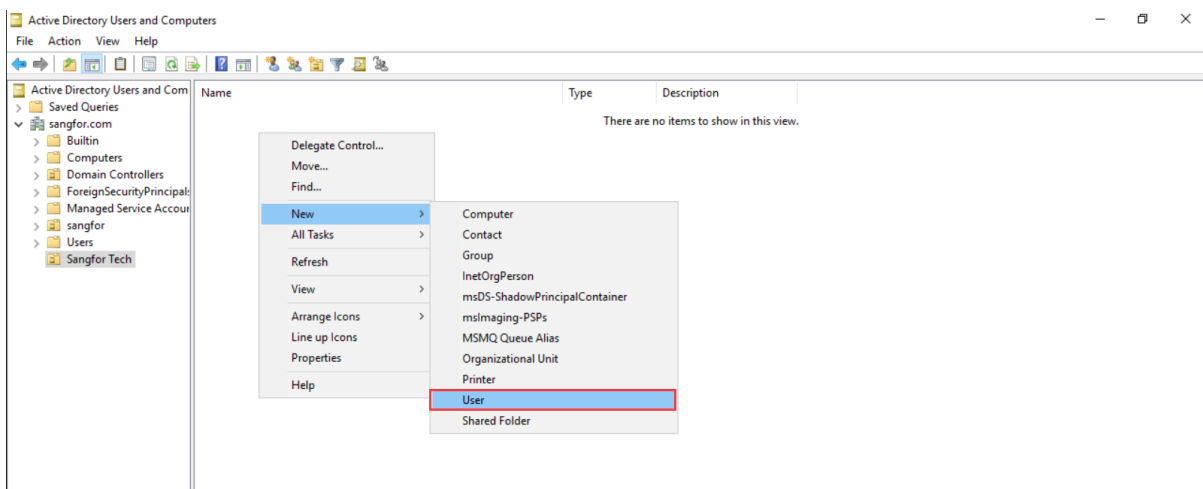


2. Dalam rangka untuk memfasilitasi manajemen pengguna menurut struktur organisasi perusahaan, logical container dibuat di sini untuk mewakili departemen. Misalnya, department disebut Sangfor Tech.

Aktivitas Domain ADSSO



3. Buat pengguna di container, misalnya disebut sangfortest.



Aktivitas Domain ADSSO

New Object - User

Create in: sangfor.com/Sangfor Tech

First name: sangfortest Initials:

Last name:

Full name: sangfortest

User logon name: sangfortest@sangfor.com

User logon name (pre-Windows 2000): SANGFOR\sangfortest

< Back Next > Cancel

Type	Description
There are no items to show in this view.	

Atur login password untuk pengguna ini.

New Object - User

Create in: sangfor.com/Sangfor Tech

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Type	Description
There are no items to show in this view.	

New Object - User

Create in: sangfor.com/Sangfor Tech

When you click Finish, the following object will be created:

Full name: sangfortest

User logon name: sangfortest@sangfor.com

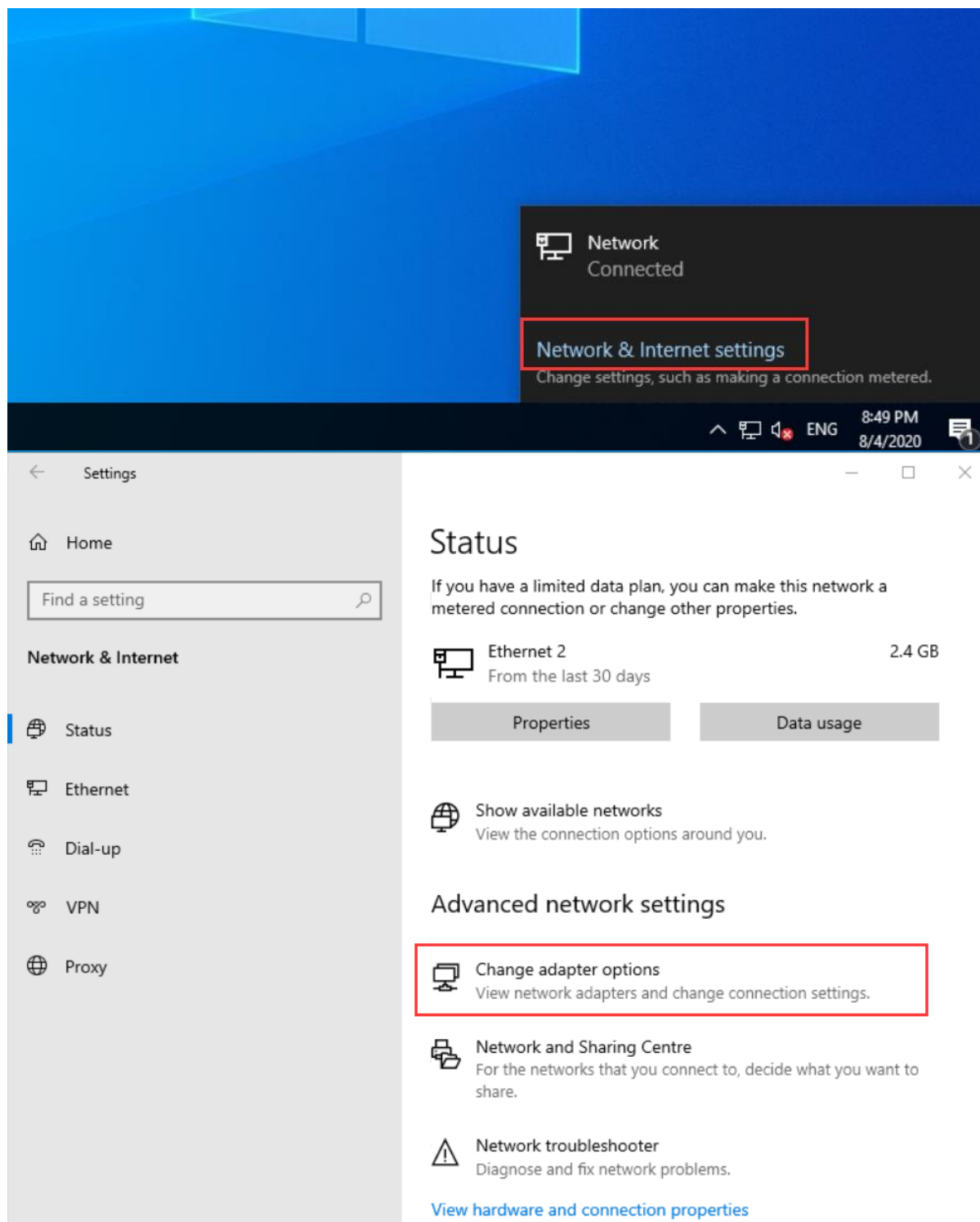
The password never expires.

< Back Finish Cancel

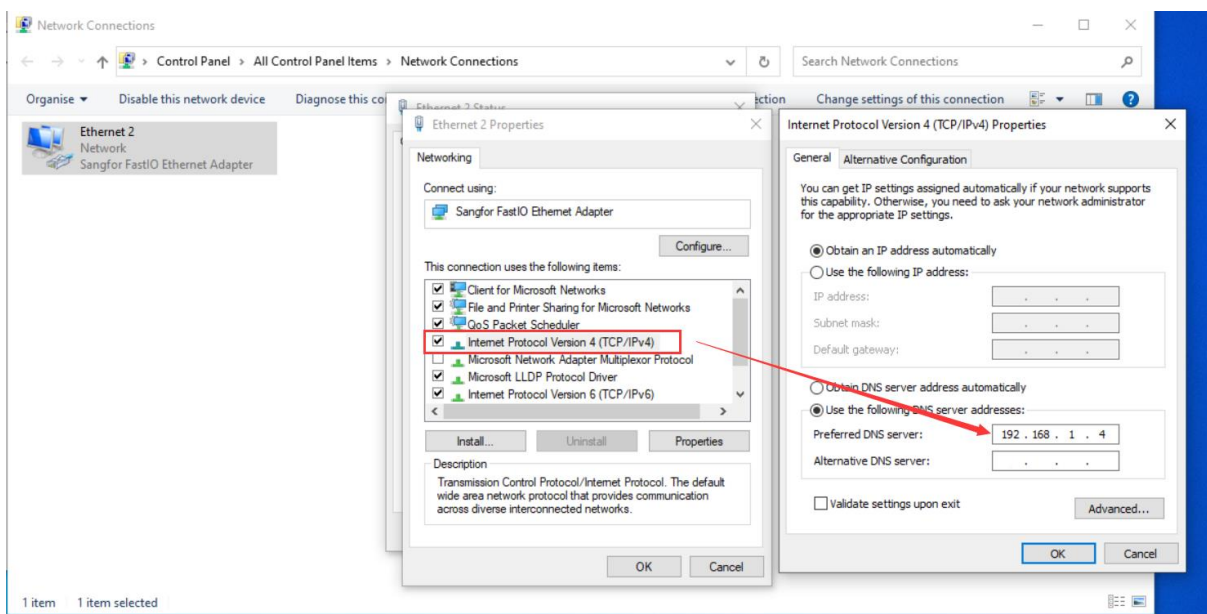
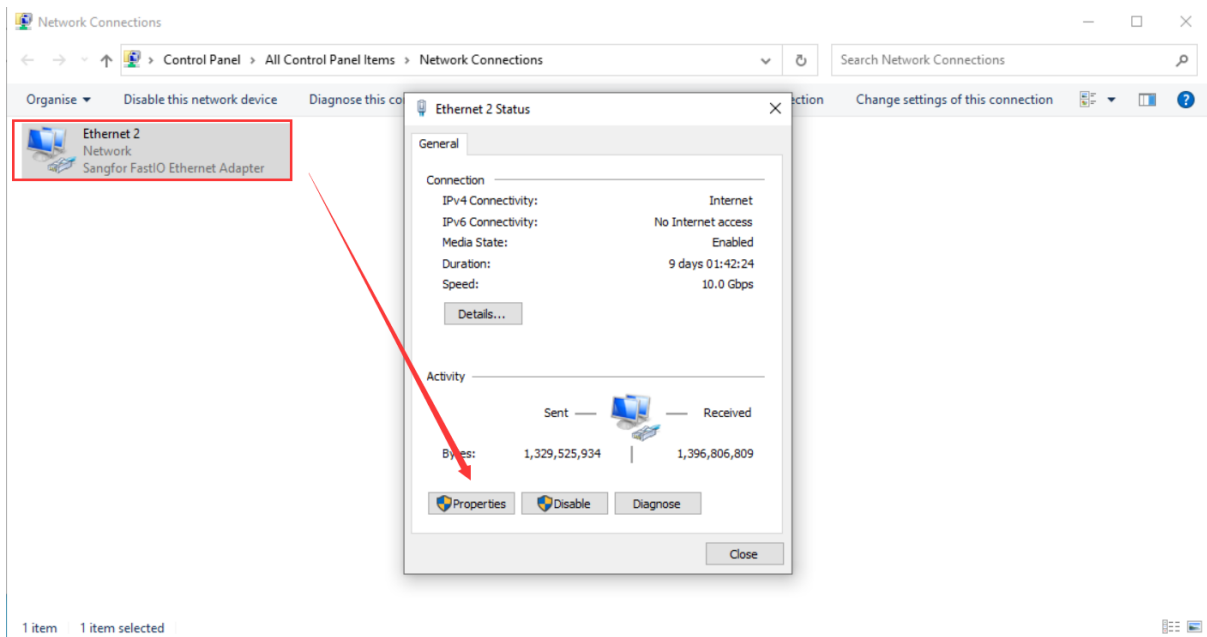
Type	Description
There are no items to show in this view.	

2.4 Gabung PC ke domain

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

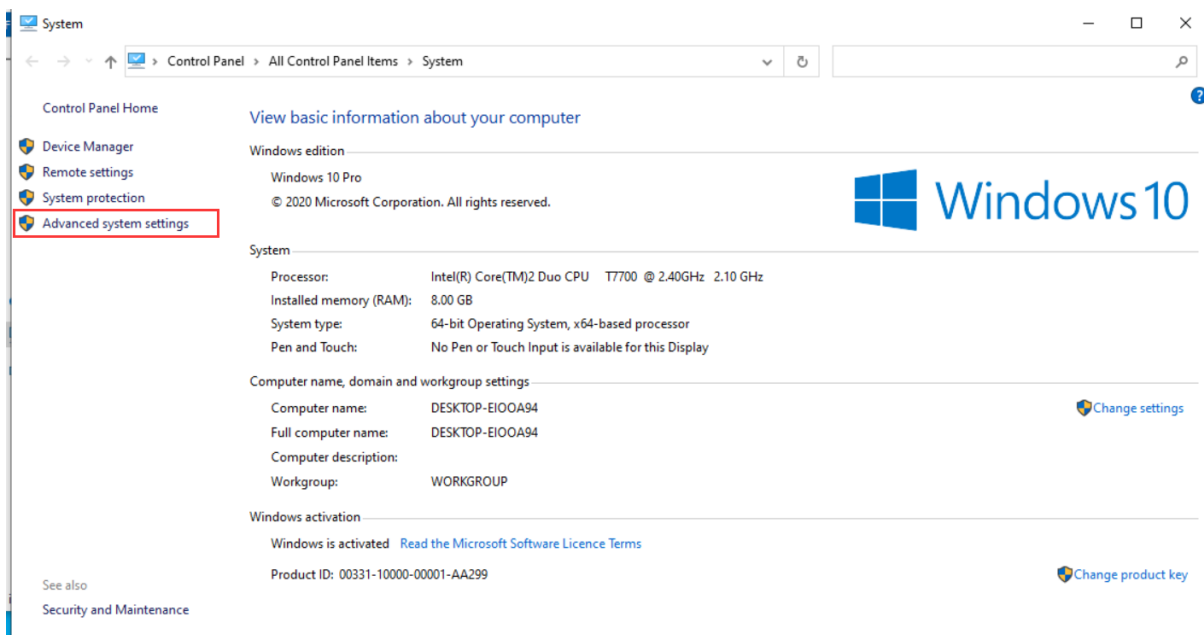
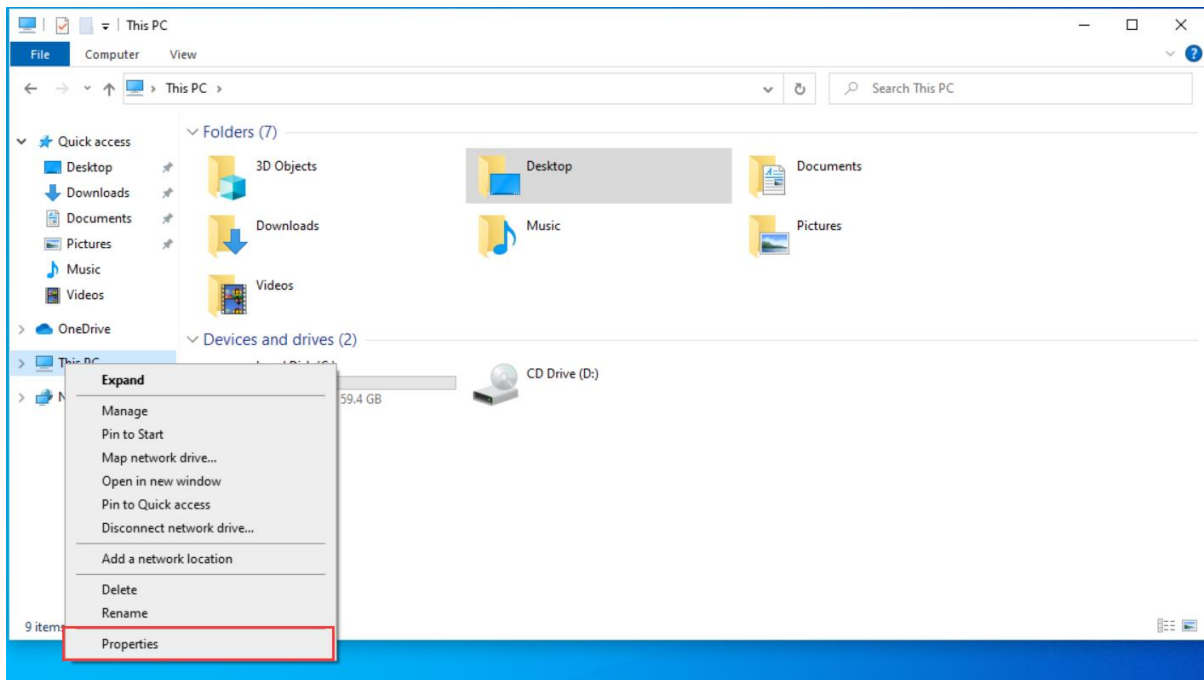


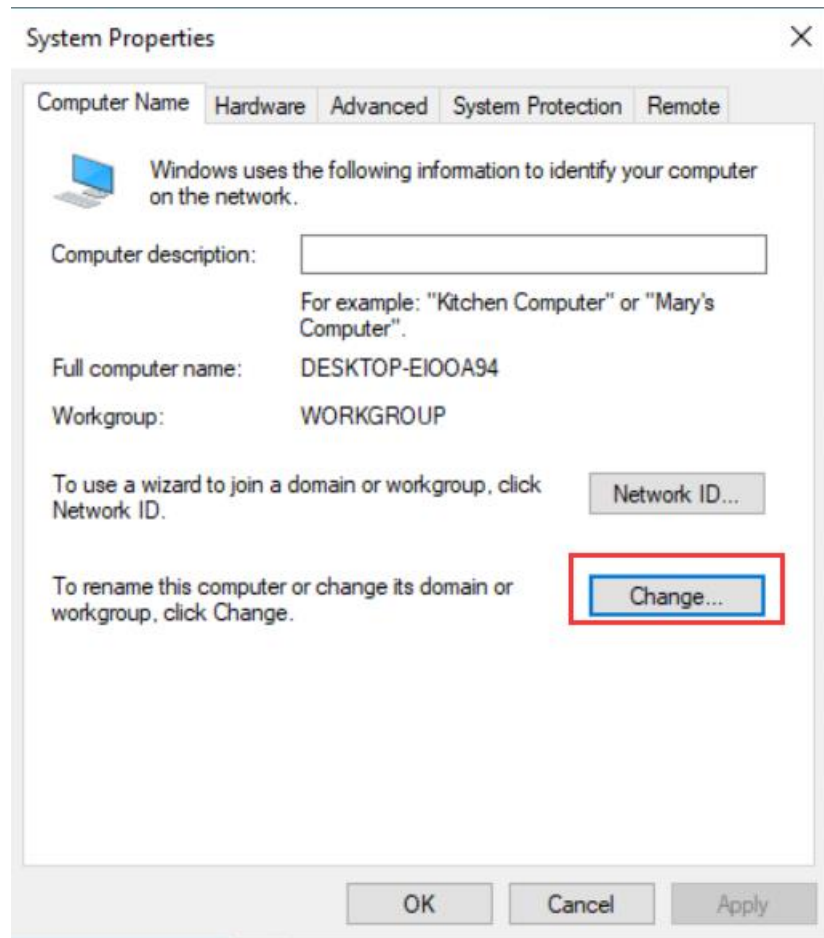
Aktivitas Domain ADSSO

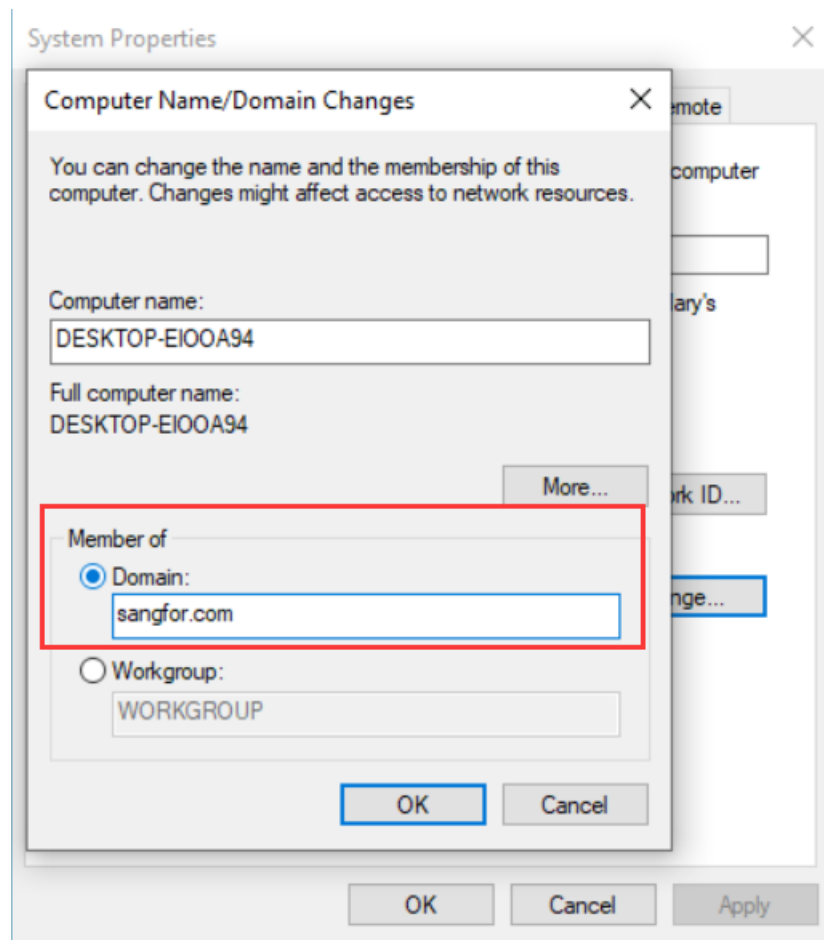


2. Sambungkan PC ke domain.

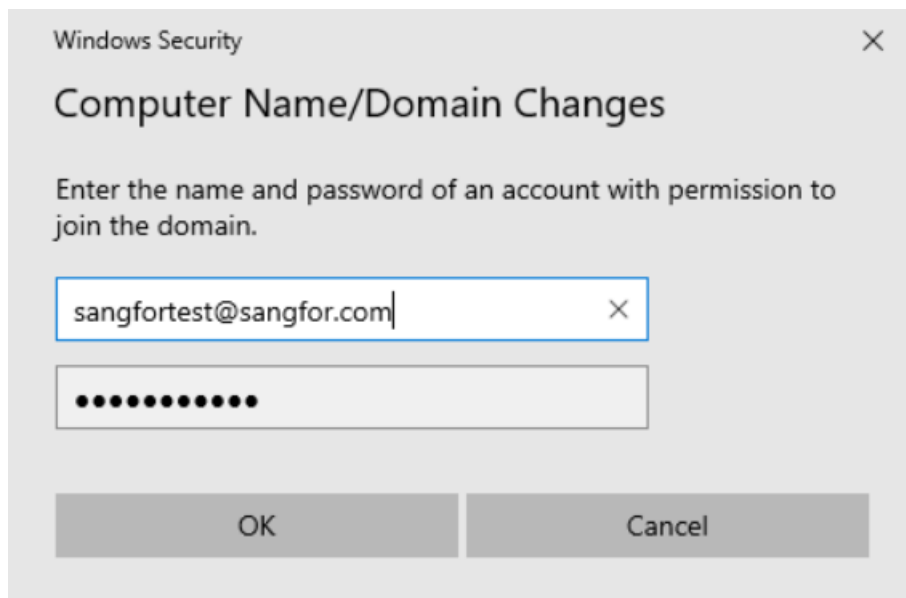
Aktivitas Domain ADSSO



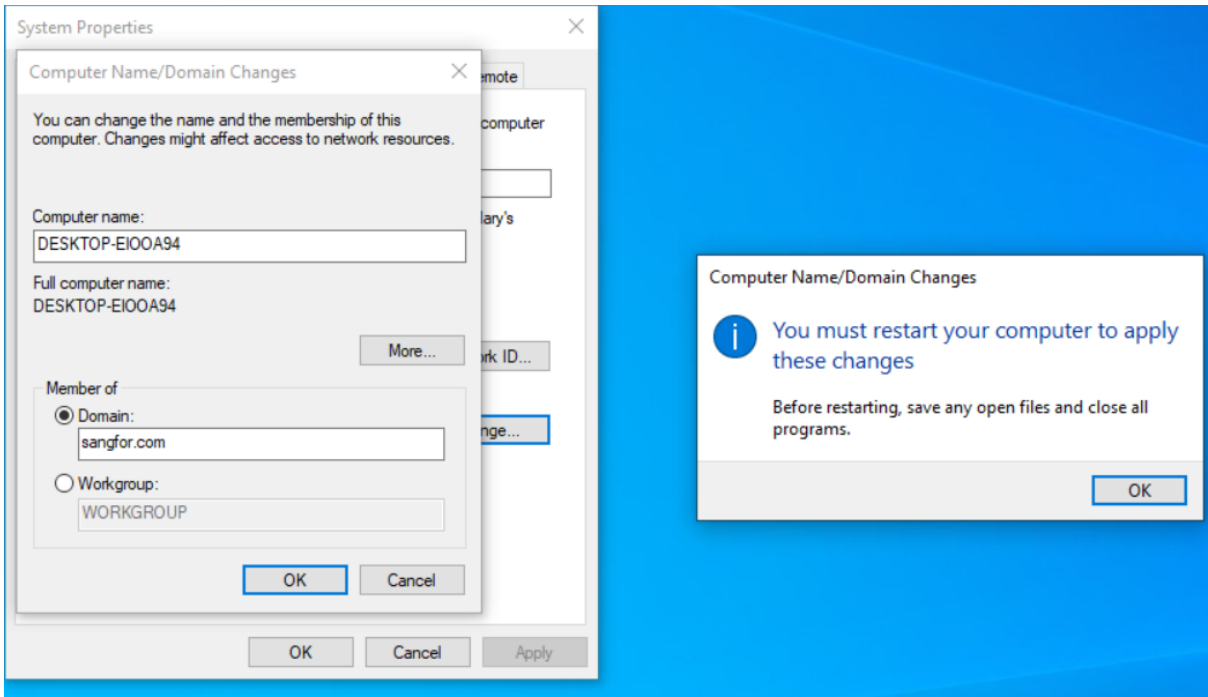
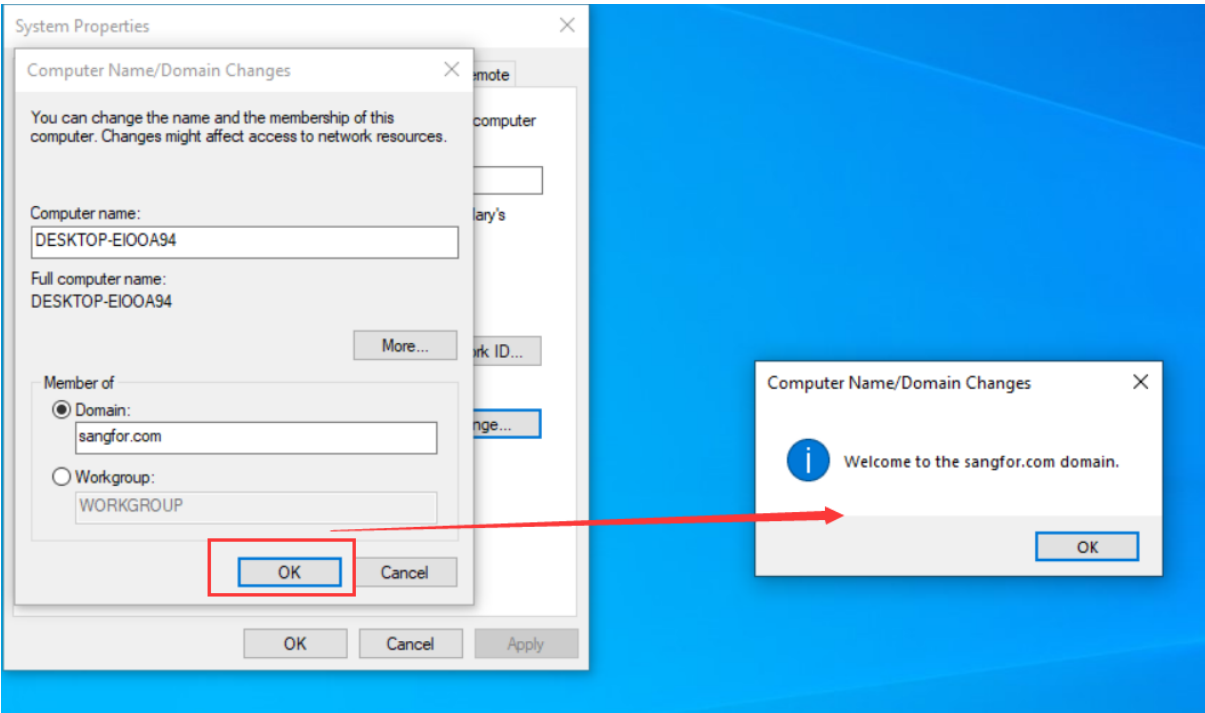


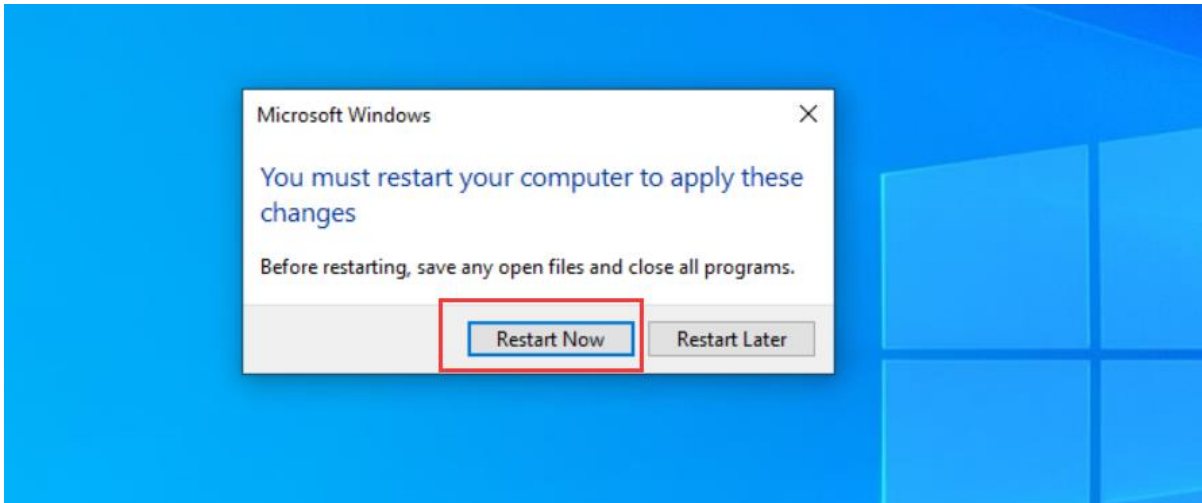


3. Dalam proses bergabung dengan domain, Anda perlu memverifikasi identitas Anda, cukup gunakan pengguna sangfortest yang dibuat pada AD domain control 192.168.1.4 untuk pengujian.

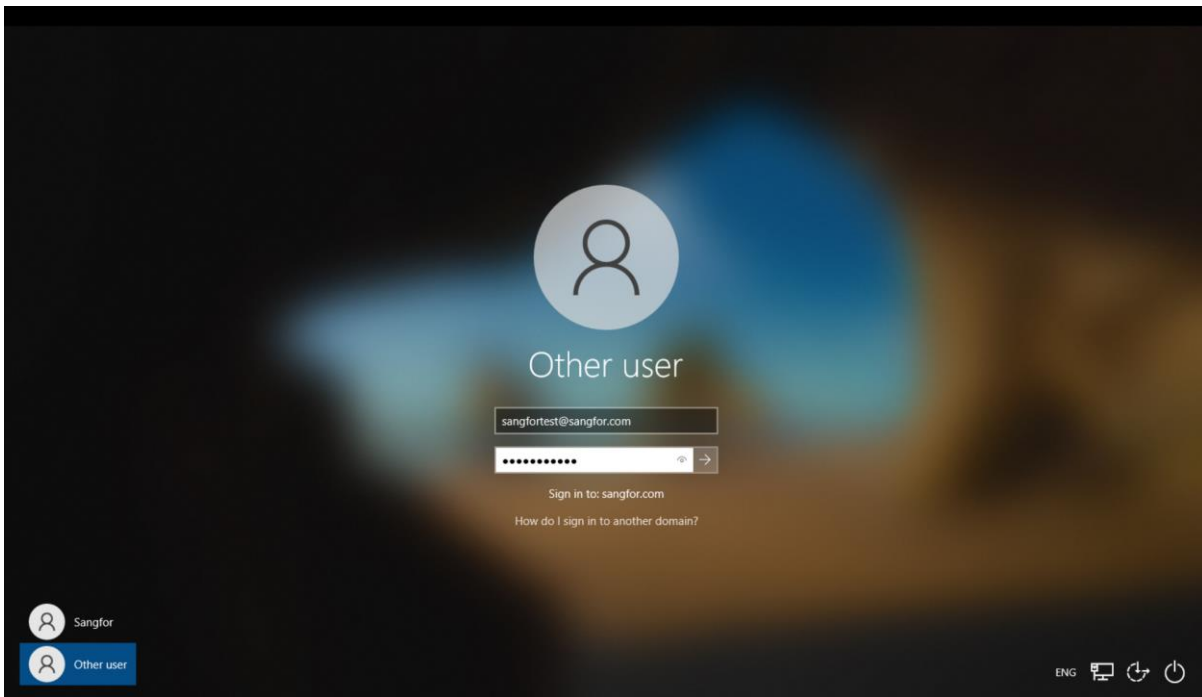


4. Setelah berhasil menggabungkan domain, Anda perlu restart PC.



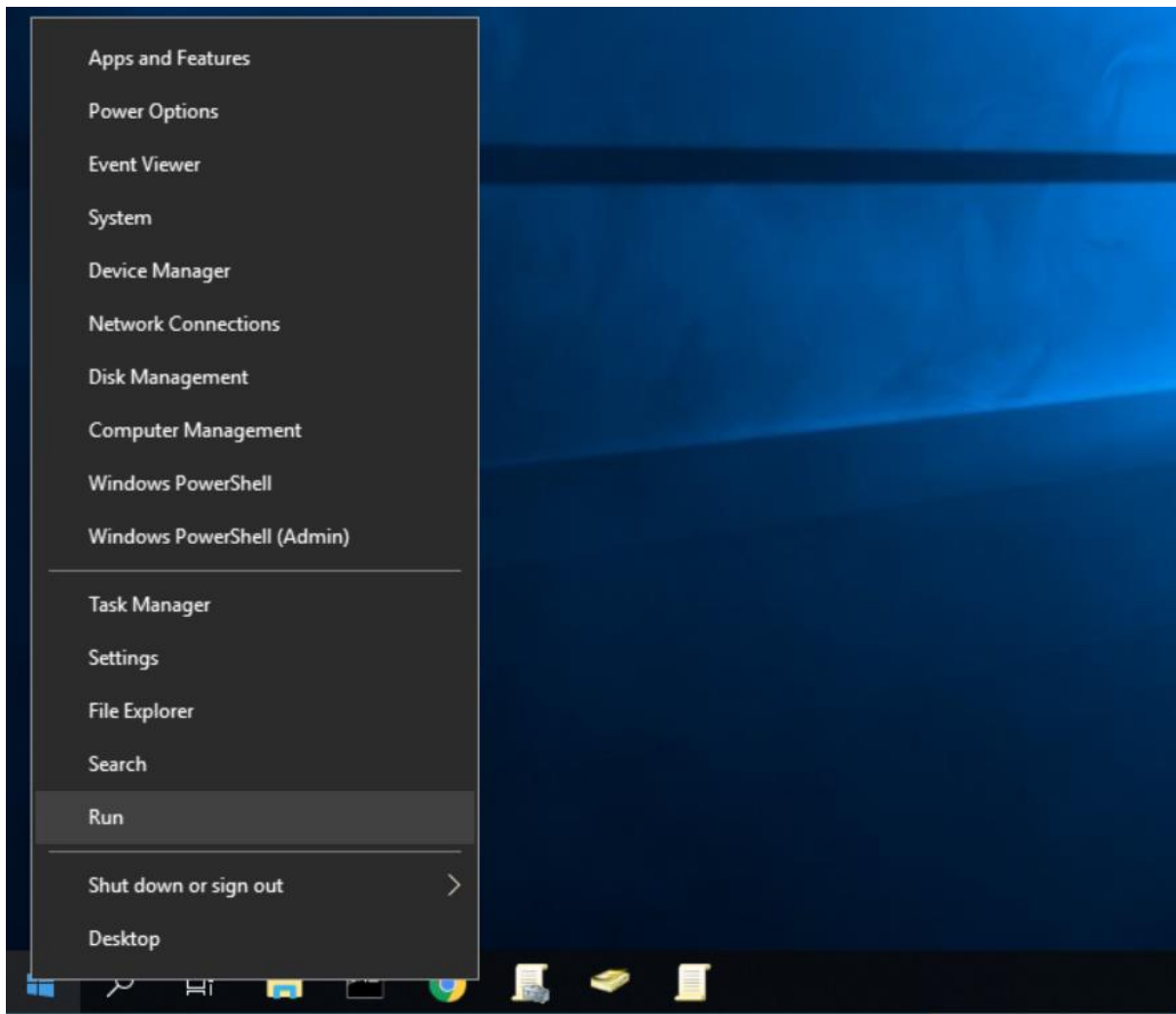


5. Setelah restart, Anda dapat melihat halaman login PC, pilih untuk menggunakan akun domain sangfortest untuk login.

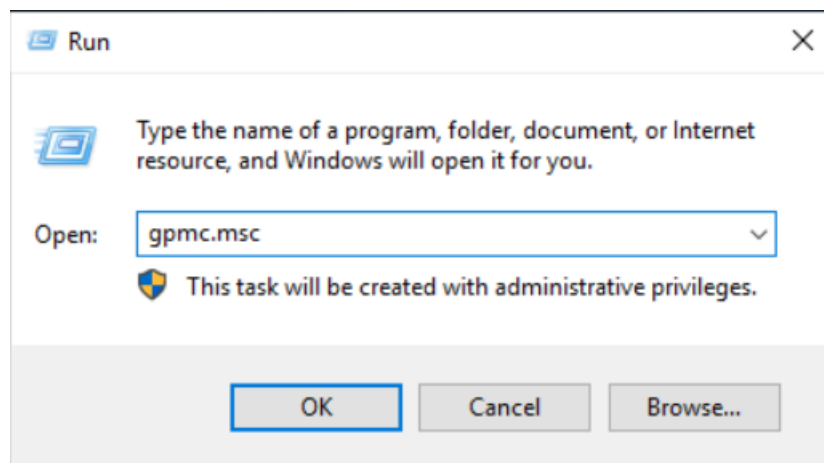


2.5 Aktifkan fungsi log audit dari AD Server

1. Buka "Run".

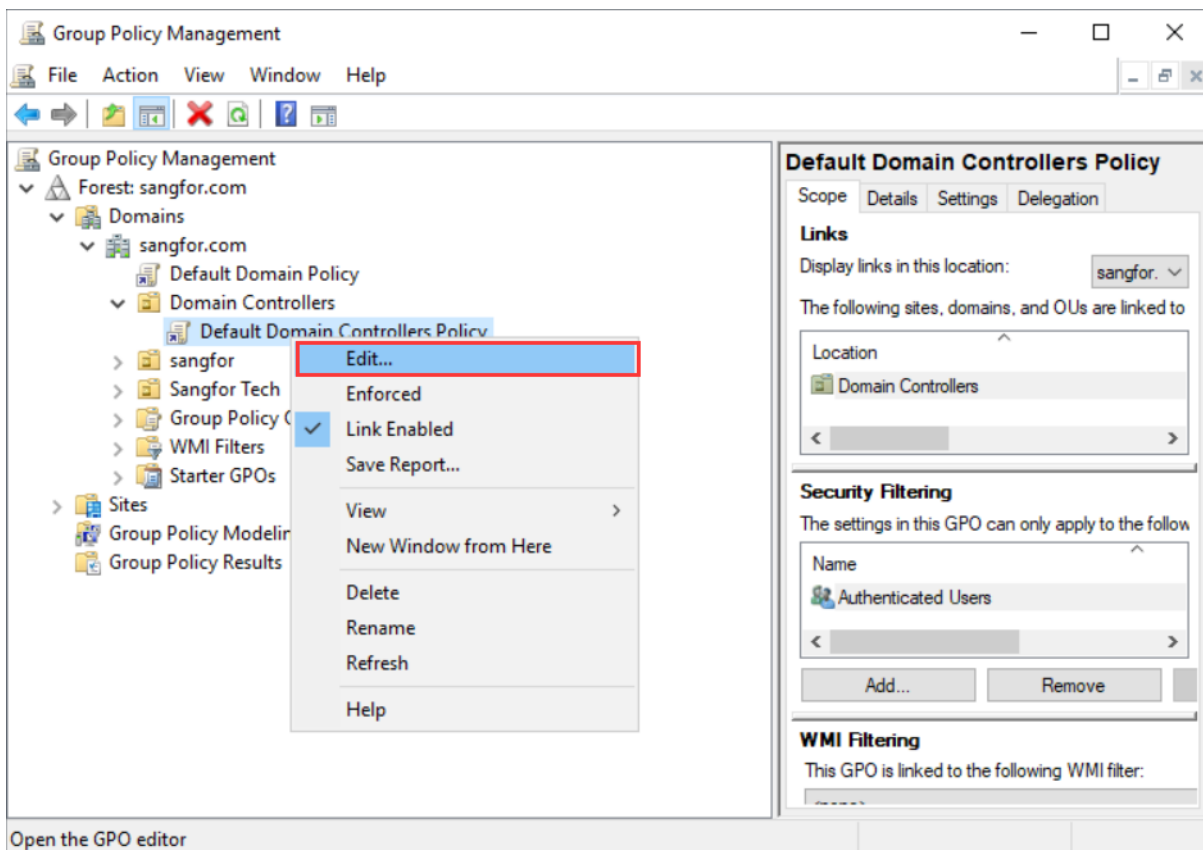


2. Enter "gpmmc.msc".

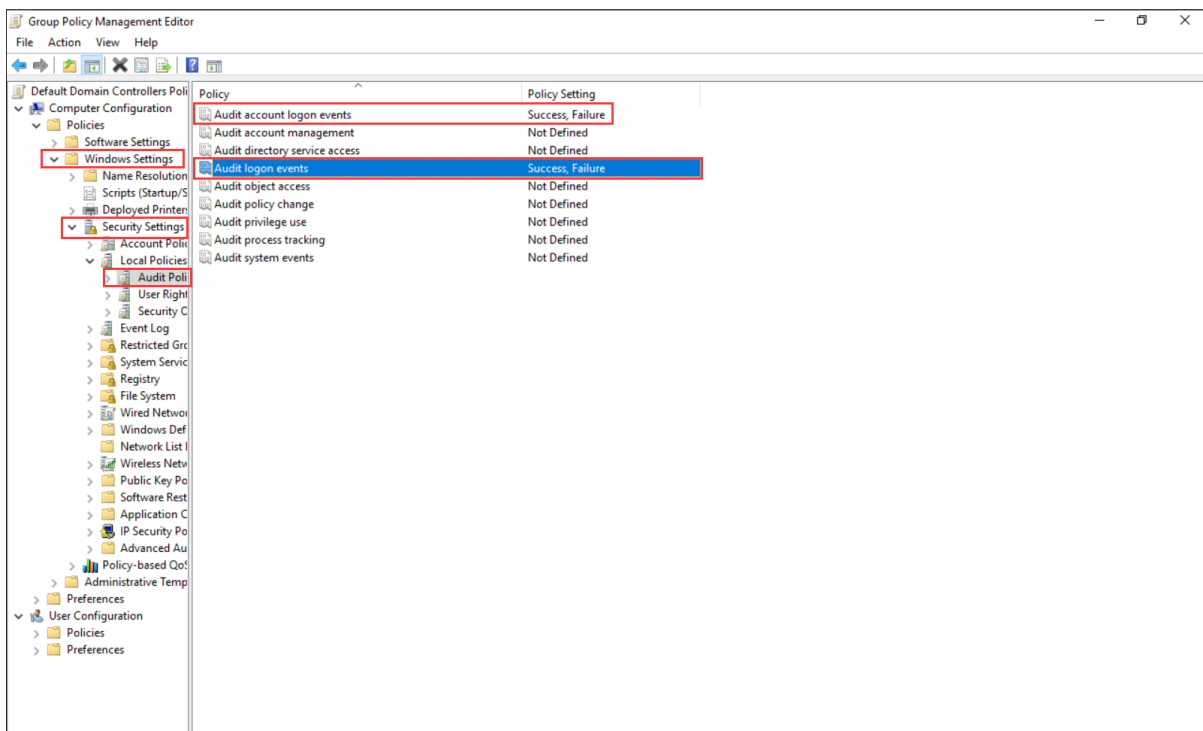


3. Klik kanan untuk edit "Default Domain Controllers Policy".

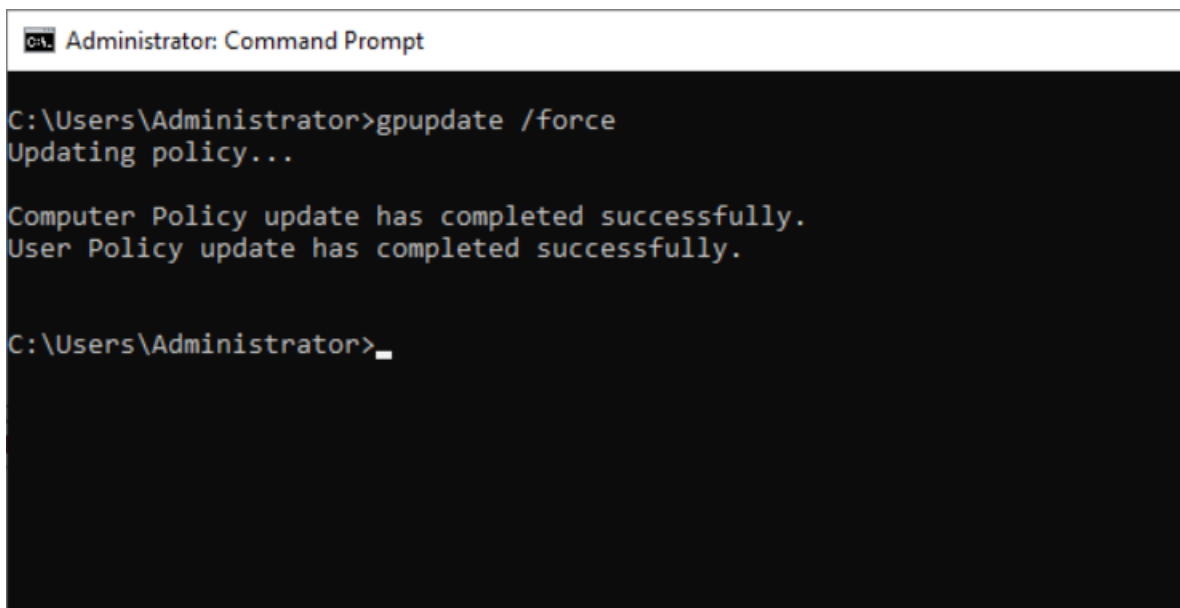
Aktivitas Domain ADSSO



4. Aktifkan "Audit account logon events" dan "Audit logon events".



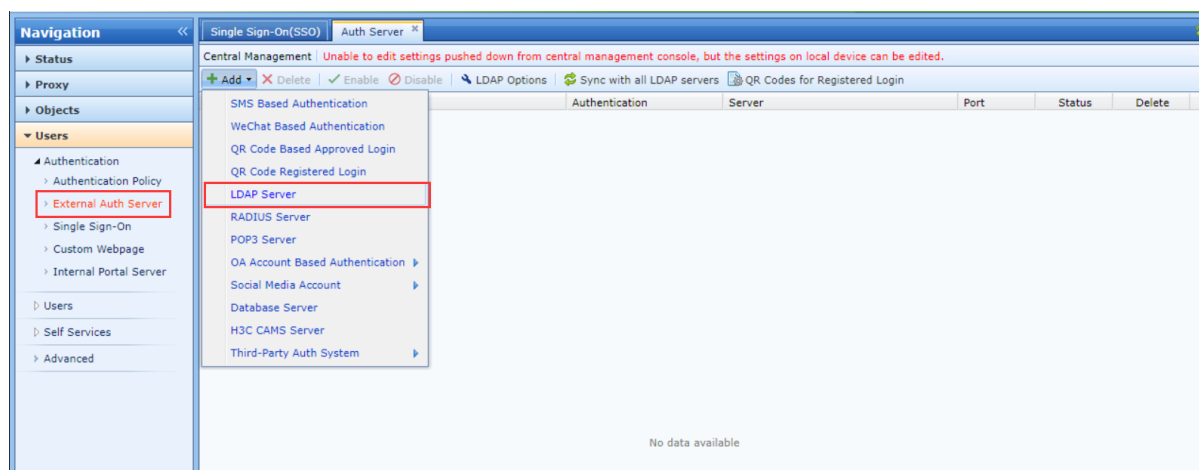
5. Enter "gpupdate /force" di CMD untuk force refresh group policy.



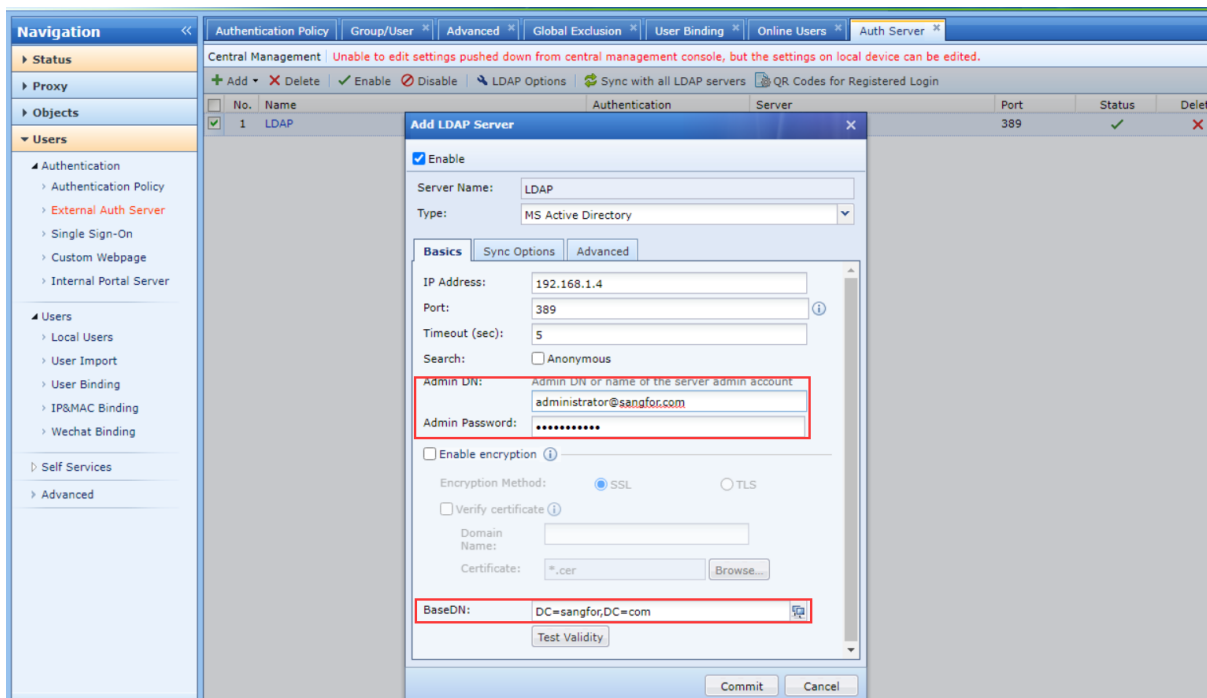
Bab 3 Bagaimana untuk Konfigurasi IAM

3.1 Tambah LDAP server

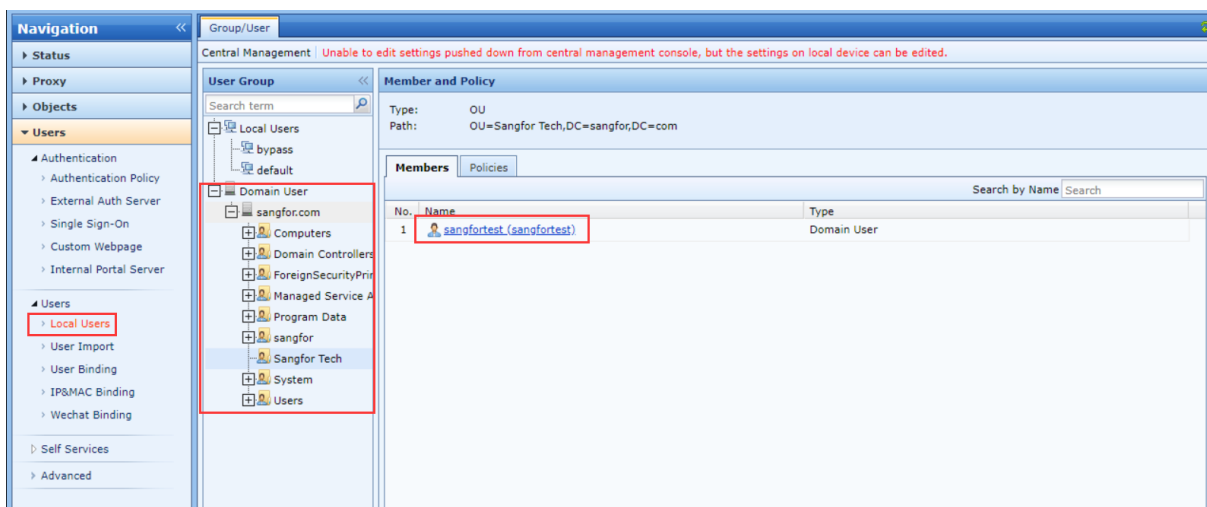
1. Tambahkan Microsoft AD server di IAM.



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 permission yang menyebabkan IAM tidak dapat berinteraksi dengan Microsoft AD server. BaseDN dapat memilih sangfor.

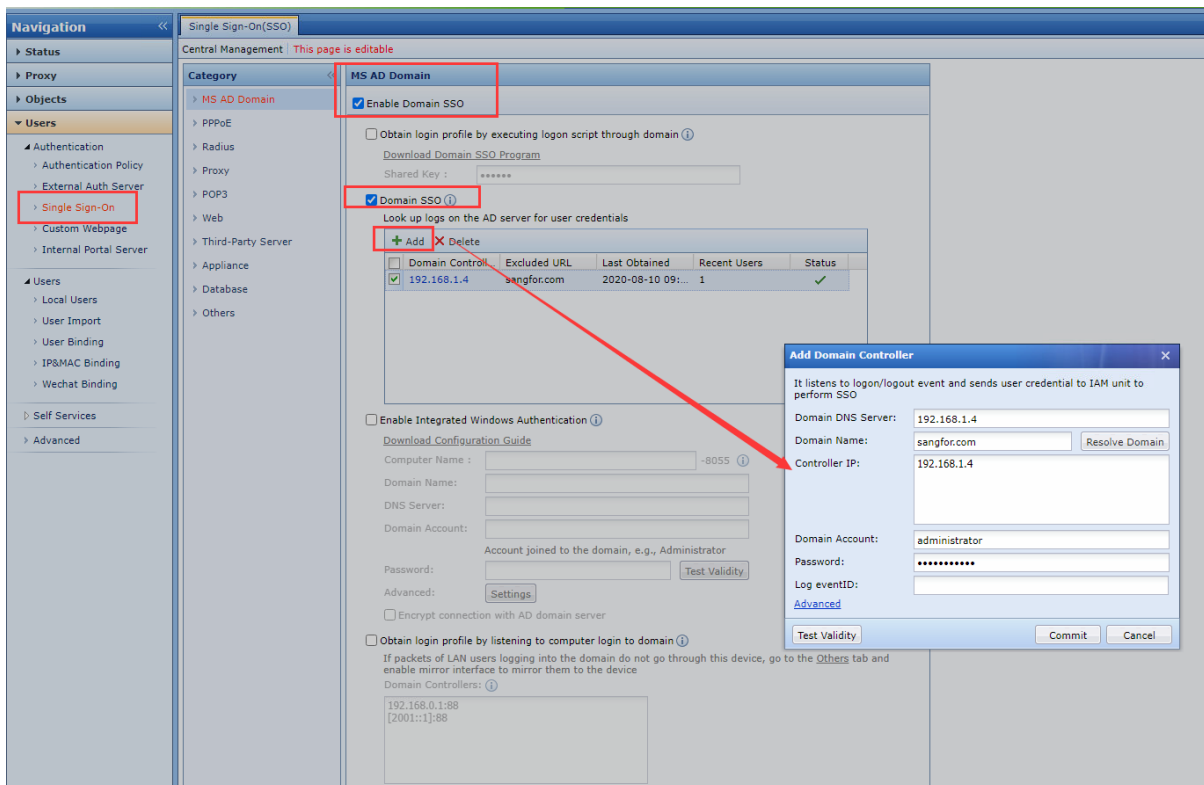


3. Jika IAM dan AD dapat berinteraksi secara normal, lalu di pengguna lokal, Anda dapat melihat bahwa IAM telah memperoleh informasi pengguna domain dari AD server, termasuk pengguna sangfortest yang kami buat sebelumnya.



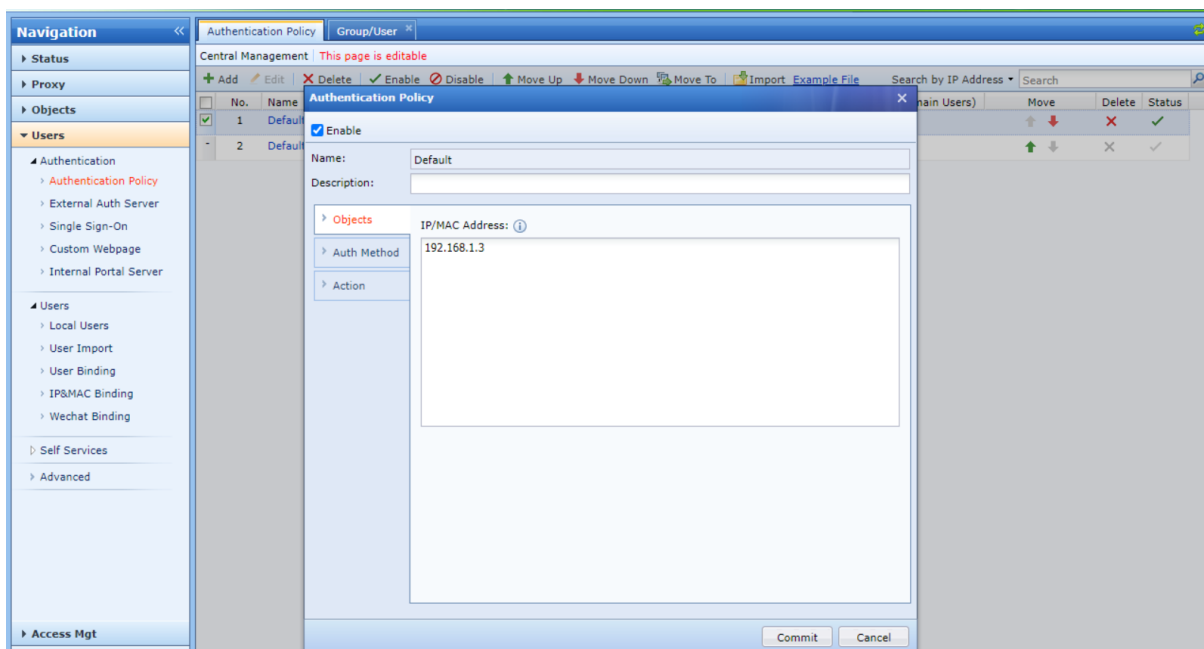
3.2 Konfigurasi option SSO authentication

1. Konfigurasi SSO authentication sesuai dengan informasi Microsoft AD Server yang telah ditetapkan sebelumnya.

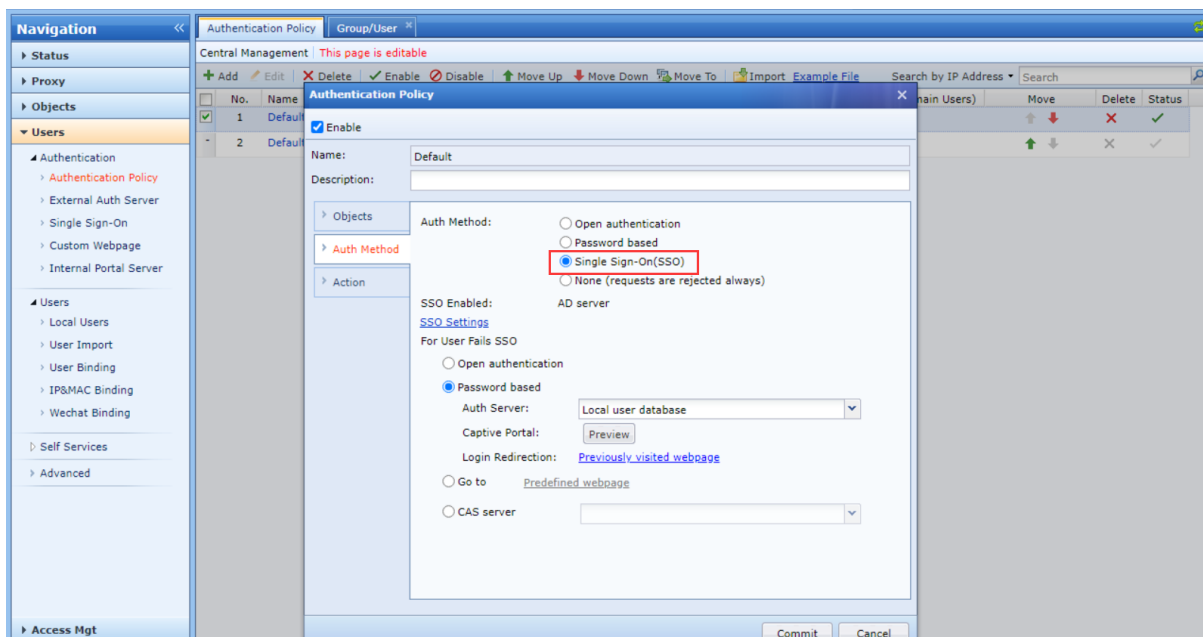


3.3 Konfigurasi authentication policy di IAM

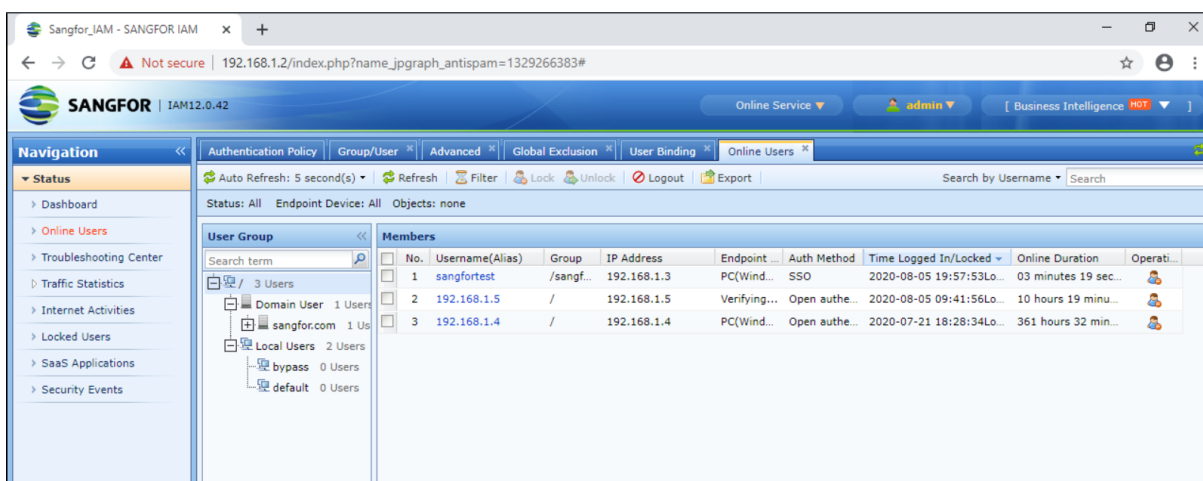
1. Atur scope dari authentication strategy, yaitu, IP mana yang harus cocok dengan authentication policy.



2. Pilih metode authentication sebagai "SSO".

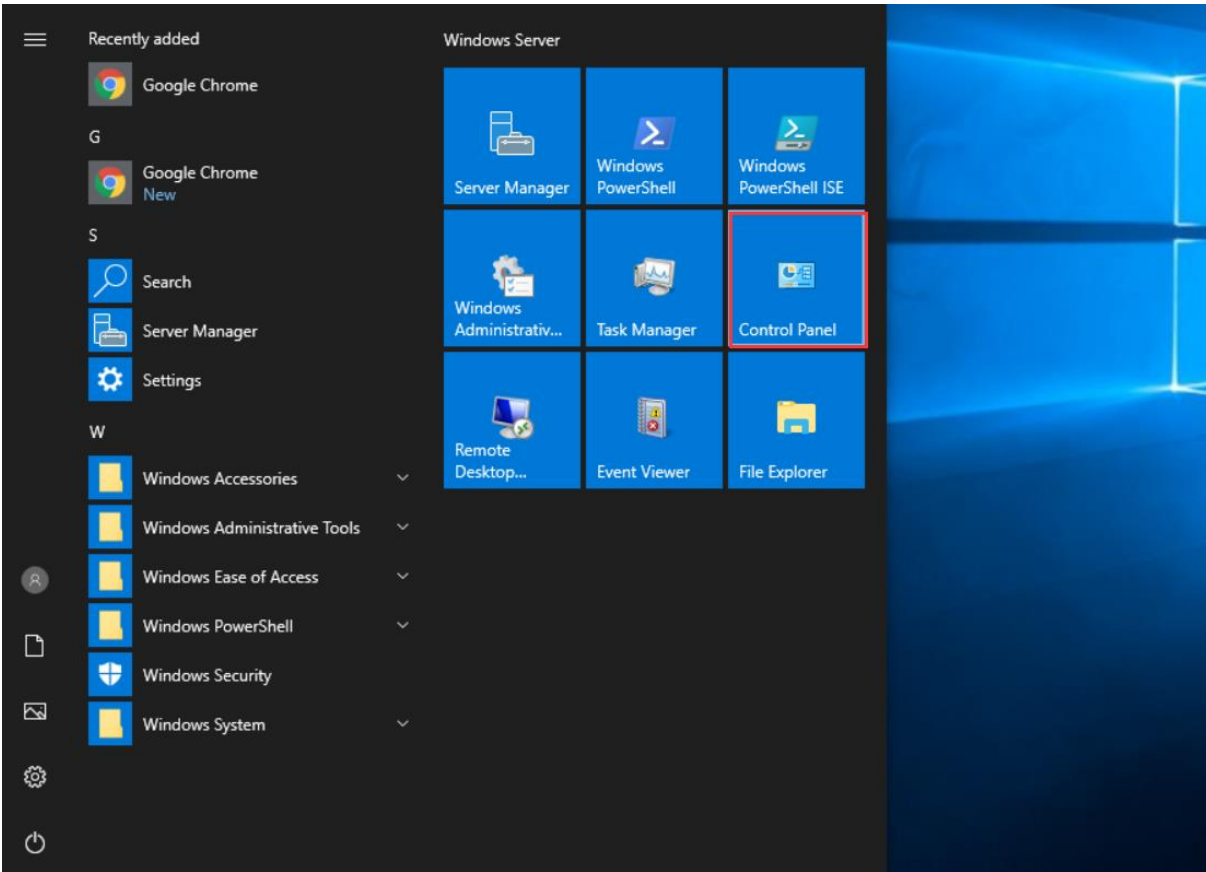


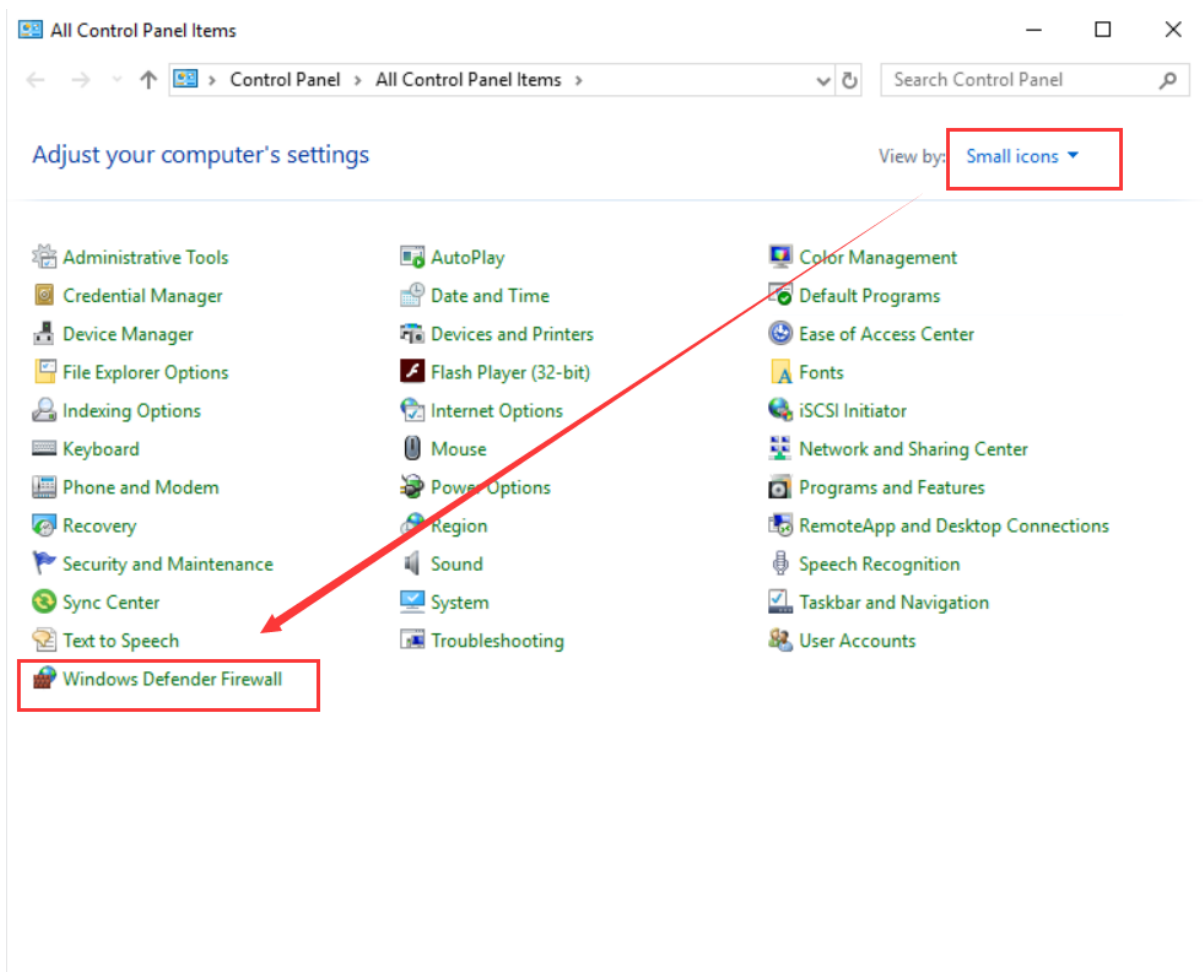
3. Restart test PC 192.168.1.3 dan login ke PC dengan akun domain . Anda dapat melihat bahwa PC 192.168.1.3 sedang online dan metode authentication adalah SSO di IAM.

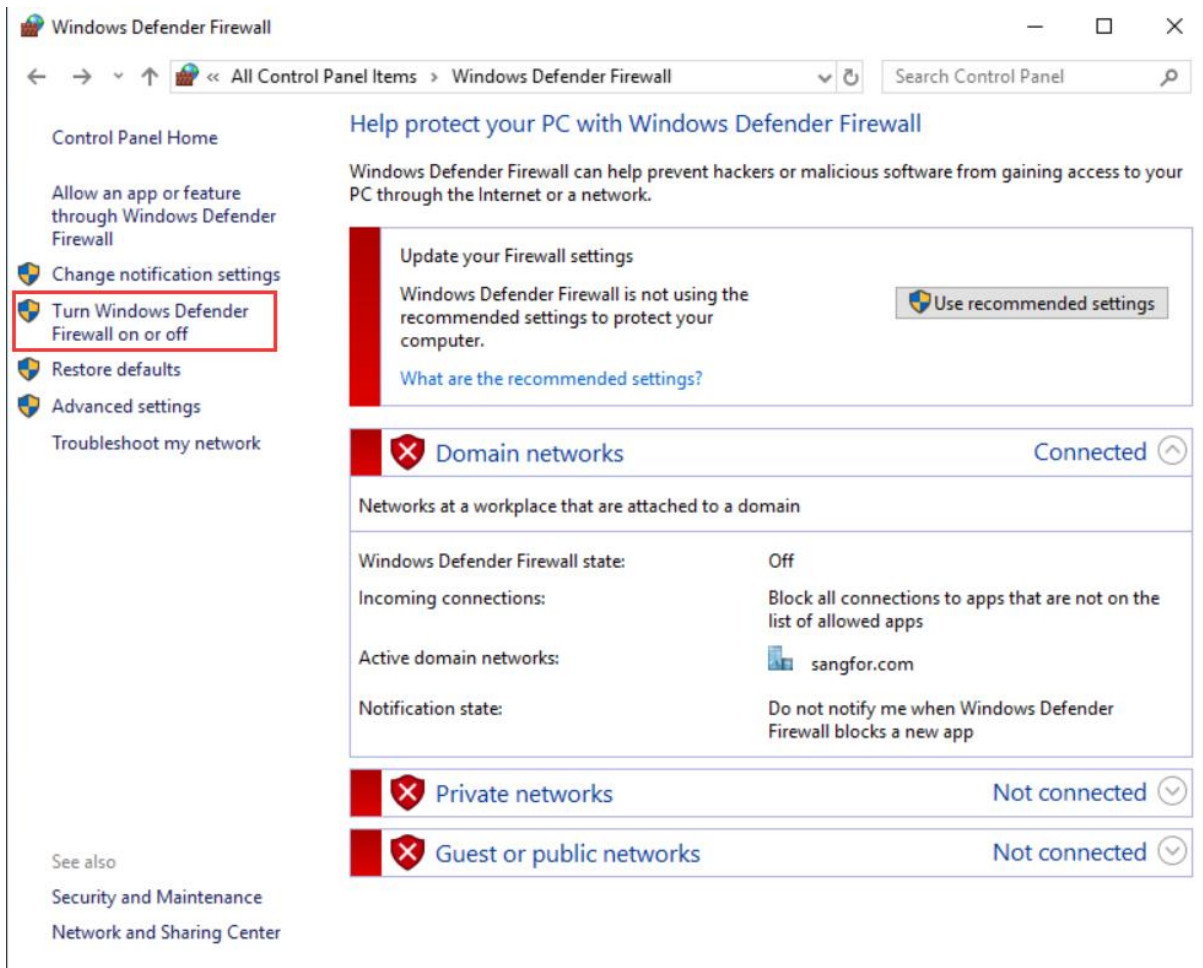


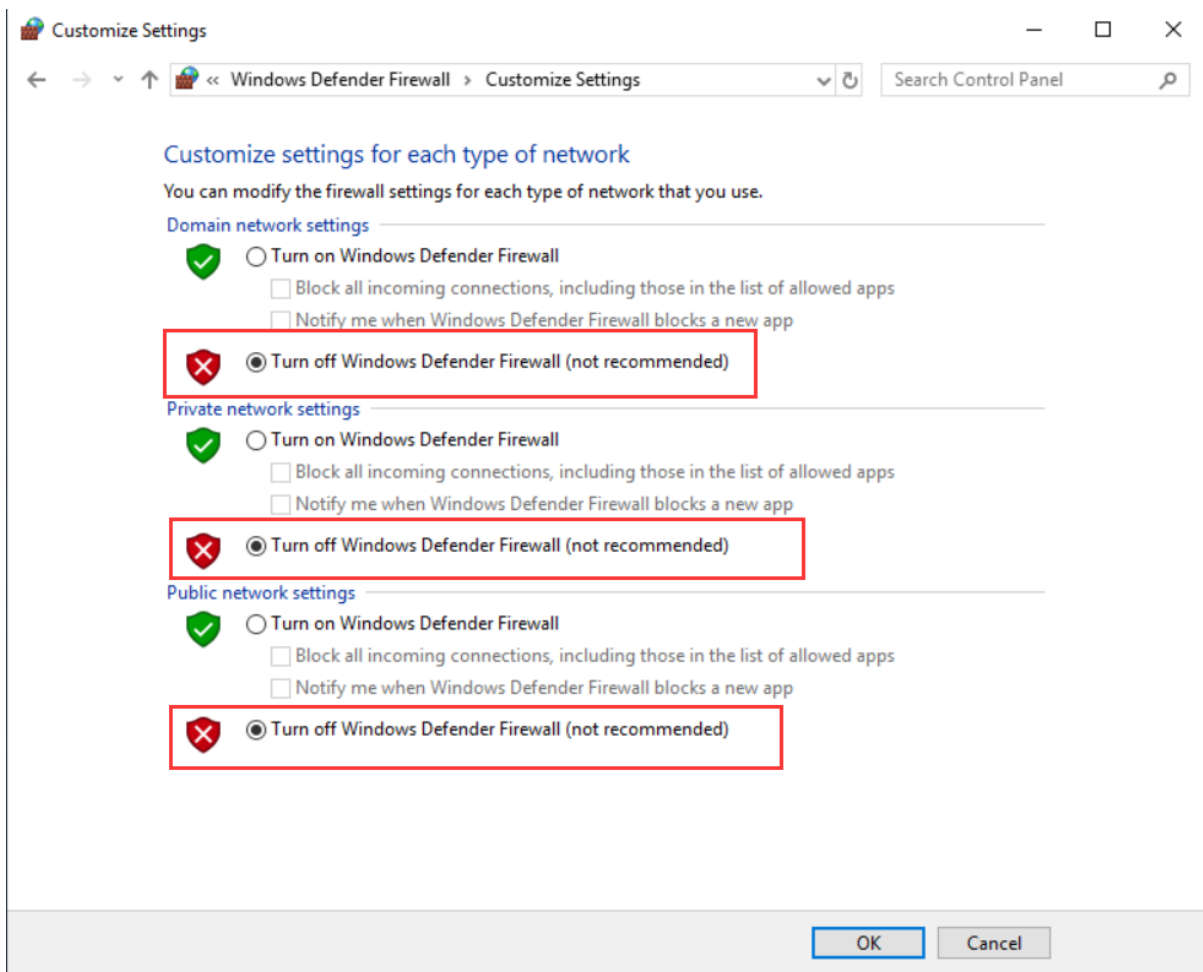
Bab 4 Tindakan Pencegahan

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

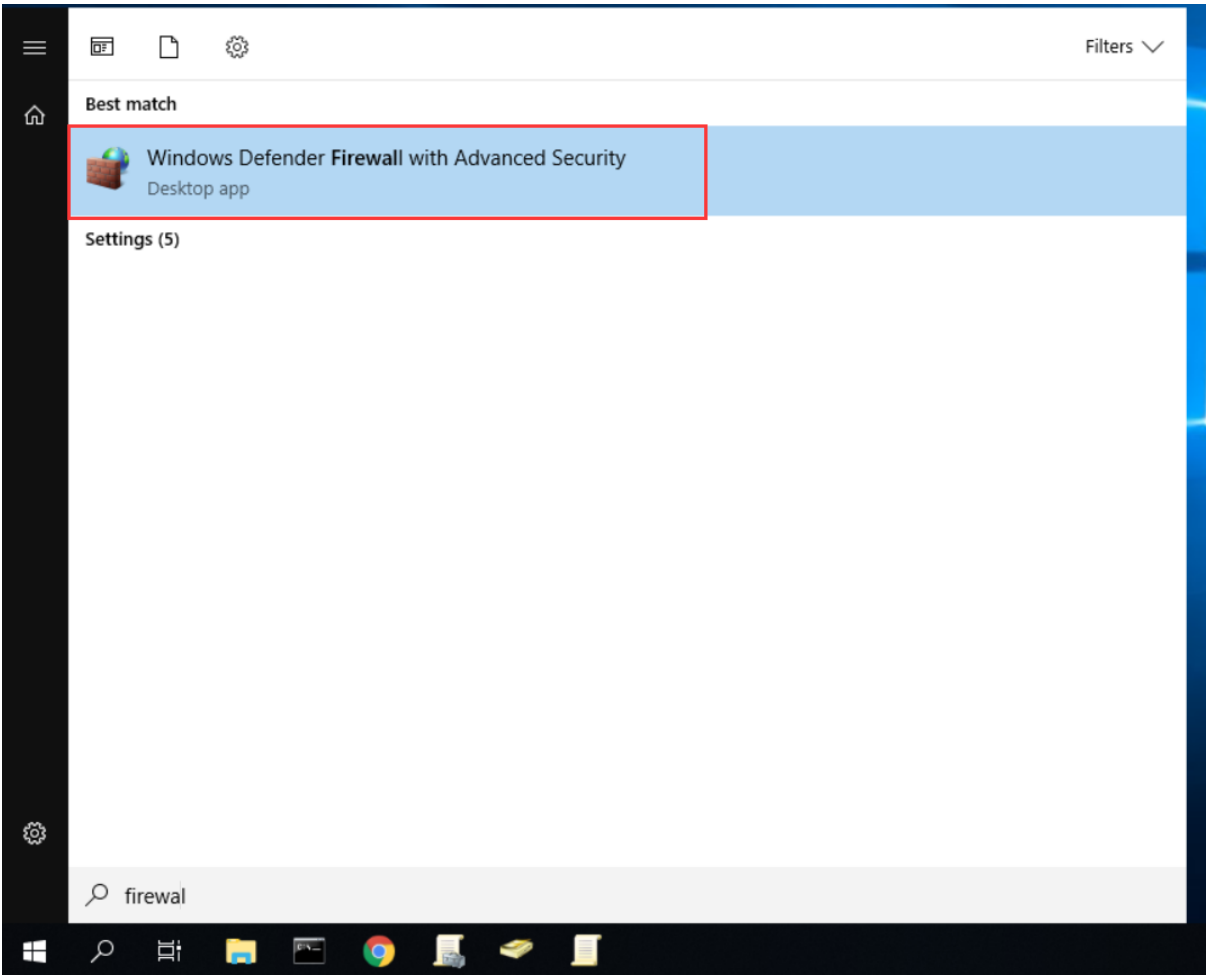


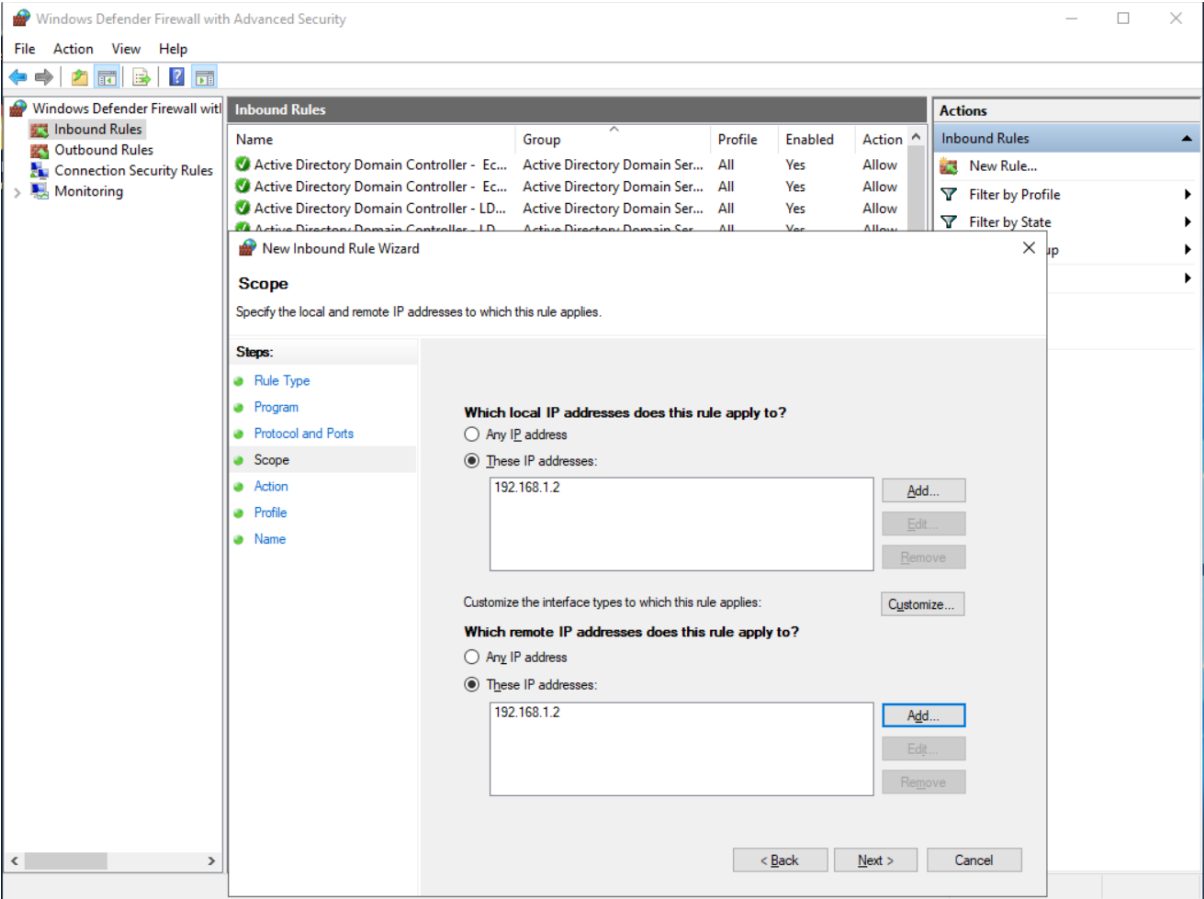






Atau Anda dapat secara manual menambahkan aturan firewall untuk mengizinkan perangkat terkait mengakses AD Server.







SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc