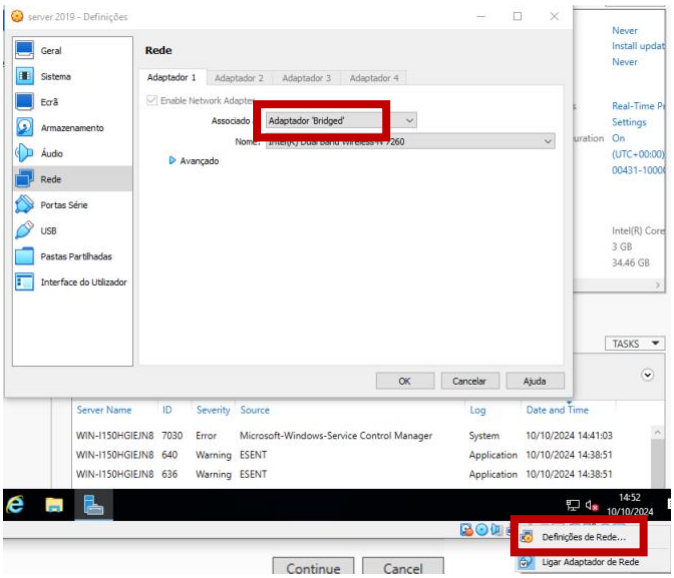
MODALIDADE:	Campeonato das profissões	Não aplicável	
ÁREA:	Cibersegurança		
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Saber como instalar e configurar servidor RADIUS com o Active Directory
- Configuração dos serviços no Windows Server 2022
- Segurança nas redes informáticas de acesso com redes informáticas

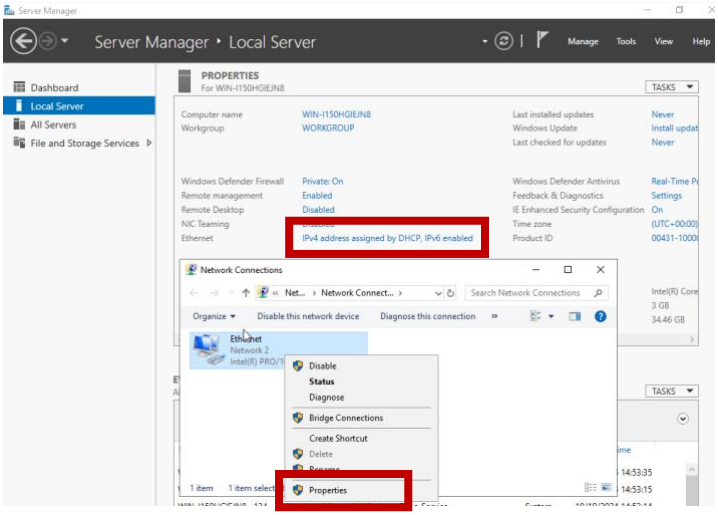
Parte 1 – Configuração da rede

Passo 1 – Ativar modo bridge Adapter (máquina física e virtual tem dois endereços IP diferentes):

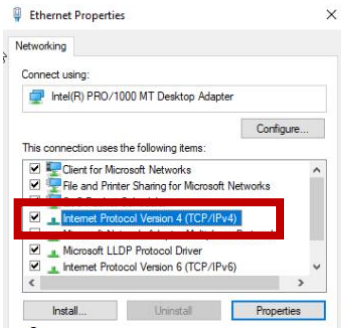


Passo 2 – Fazer apenas se ainda não tiver endereço IP fixo:

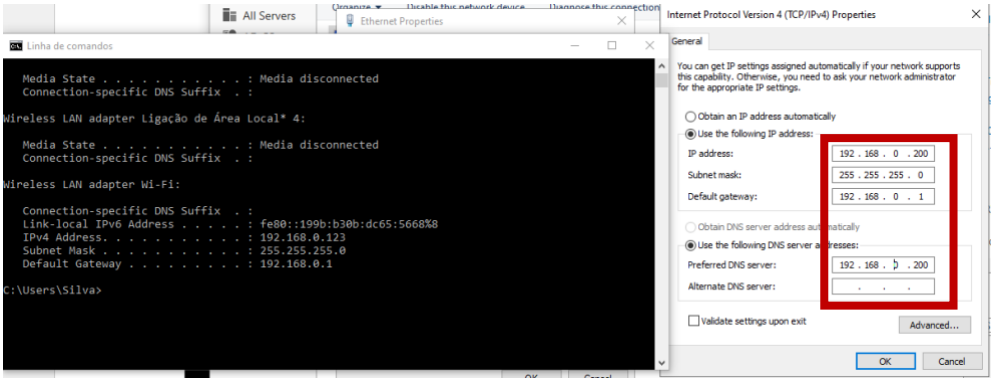
Passo 2.1 - Abra as propriedades de gestão do servidor, clique na opção onde esta "Ethernet" e na nova janela será exibida as ligações de rede. Clique em cima da ligação de rede com o lado direito do rato e selecione a opção Properties:



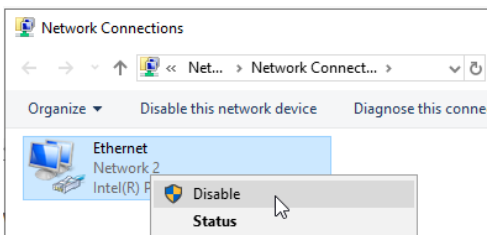
Passo 2.2 – Na nova janela, selecione as propriedades do protocolo IPv4:

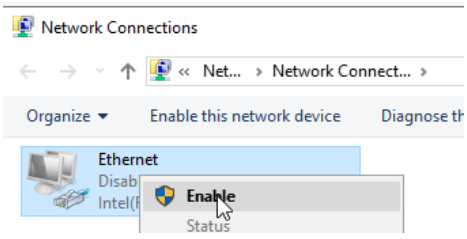


Passo 2.3 – Altere os valores do endereço (pois é necessário que o servidor tenha um endereço privado):



Passo 2.4 – Depois feche a janela e de seguida desabilite e volte a habilitar as novas alterações:

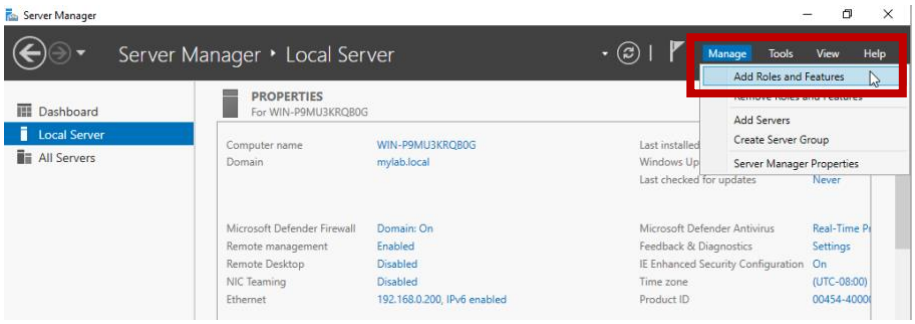




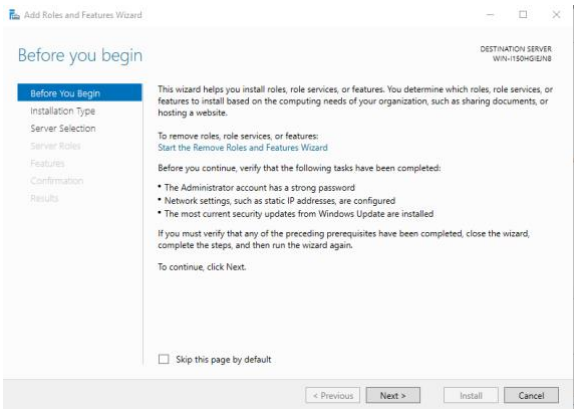
Parte 2 – Configuração AD, DNS e NPAS

Vamos instalar o Activity Diretory (para criar utilizadores e grupos), o DNS (sistema que contém uma lista de nomes de domínio e permite que os utilizadores encontrem um sistema/página web por meio desses nomes) e Network Policy and Acess Services (para configurar as políticas de acesso a rede e serviços).

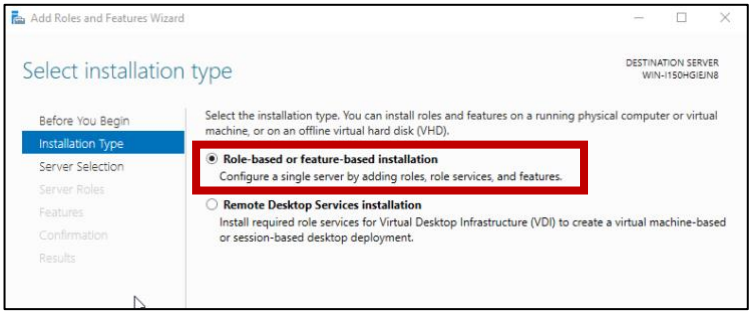
Passo 1 – Como tal, vamos começar por instalar os serviços clicar na opção "Manage" →"Add roles and features":



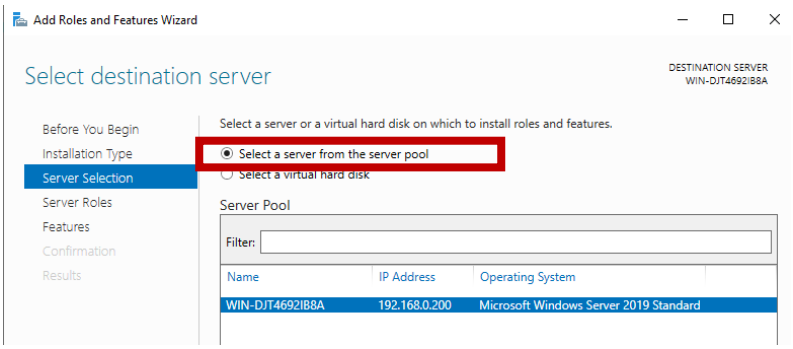
Passo 2 – Aceitar as políticas de utilização de serviços antes de começar a instalar serviços:



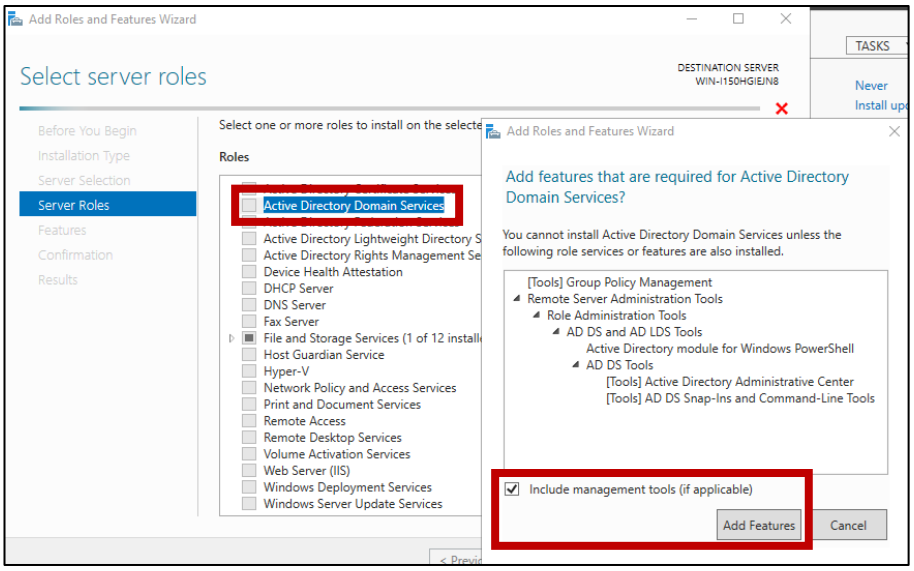
Passo 3 – Pedir para instalar os serviços neste servidor (físico):



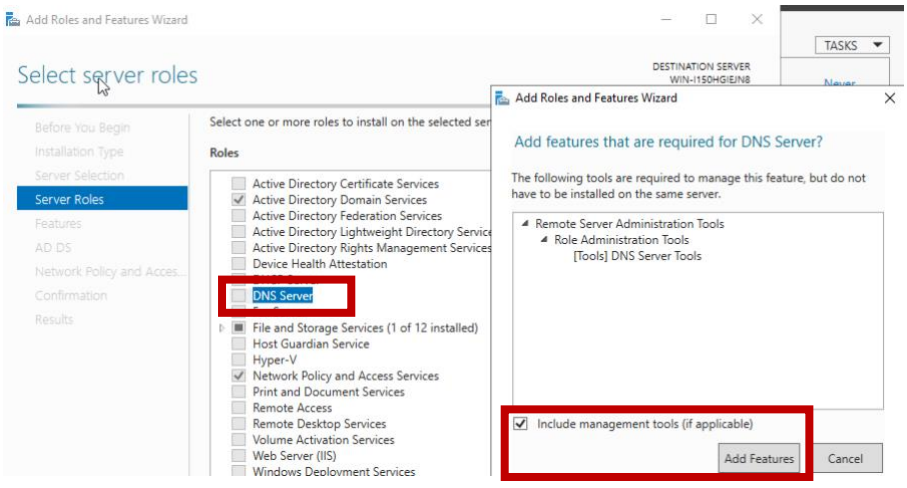
Passo 4 – Selecionar qual a instância no servidor (neste caso só é 1):



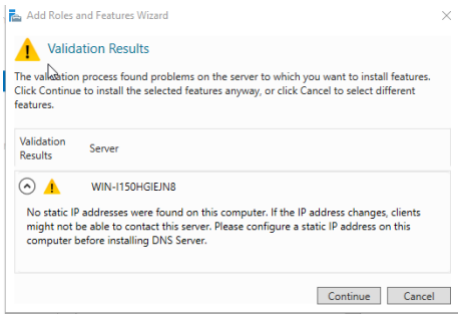
Passo 5 – Pedir para instalar o **Active Diretory Domain Services** (para configurar utilizadores e grupos):



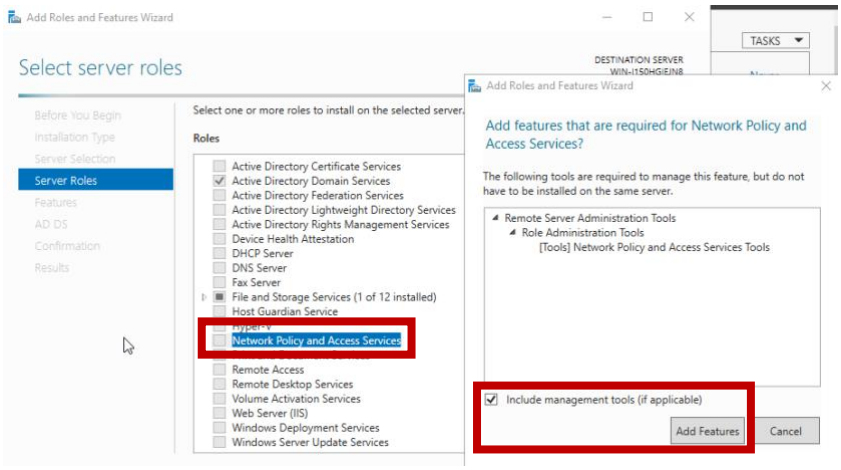
Passo 6 – Pedir para instalar o **DNS Server**:



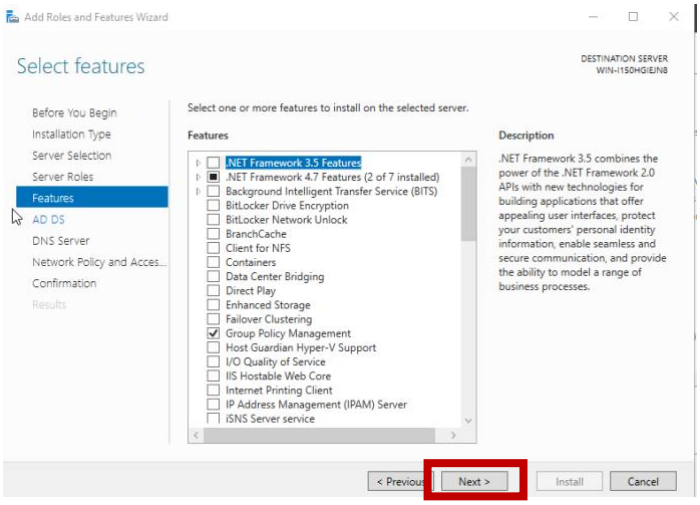
Se aparecer a seguinte mensagem, significa que ainda não tem endereço IP fixo:



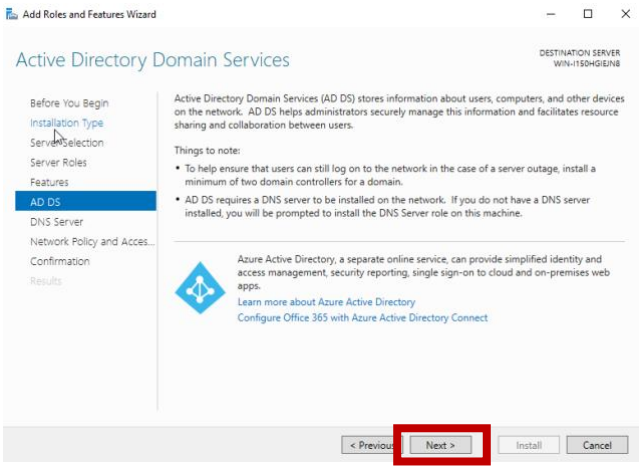
Passo 7 – Instalar a ferramenta "**Network Policy and Acess Services**":



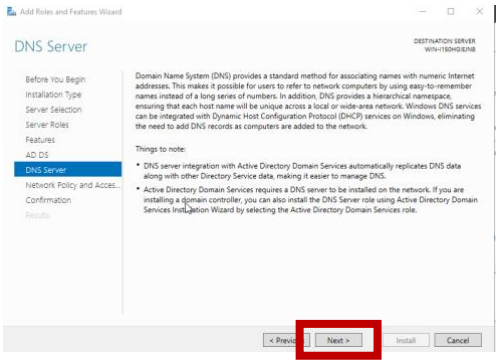
Passo 8 – Por enquanto, não será preciso instalar mais serviços adicionais para este contexto. Como tal, clique em Next:



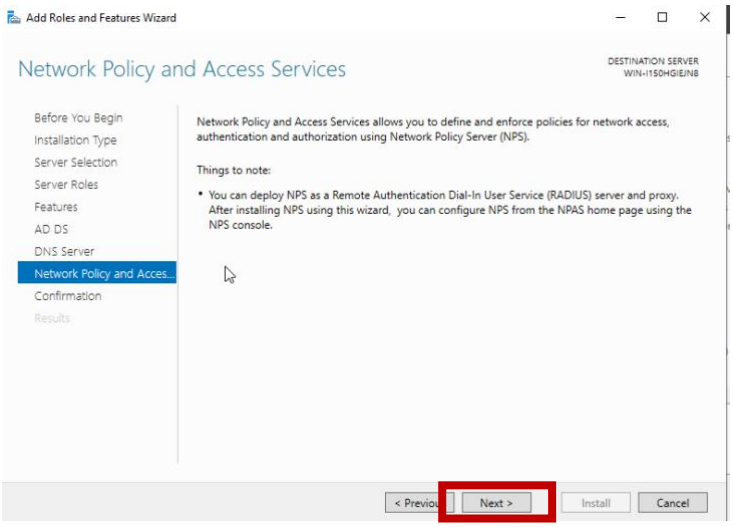
Passo 9 – Concordar com a instalação do Active Directory:



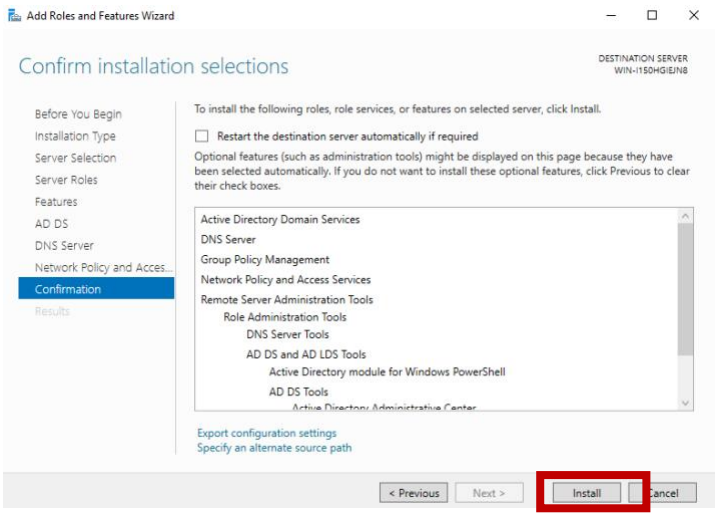
Passo 10 – Concordar com a instalação do DNS Server:



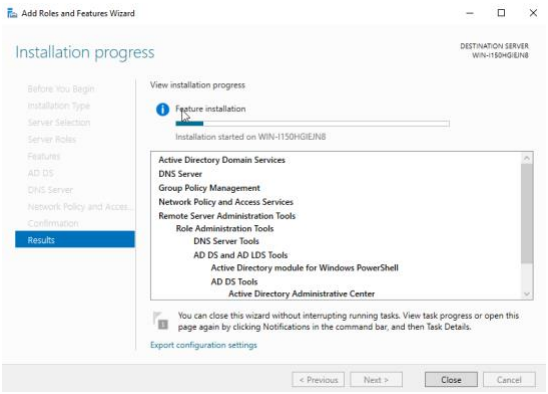
Passo 11 – Concordar com a instalação do Network Policy and Access Services:



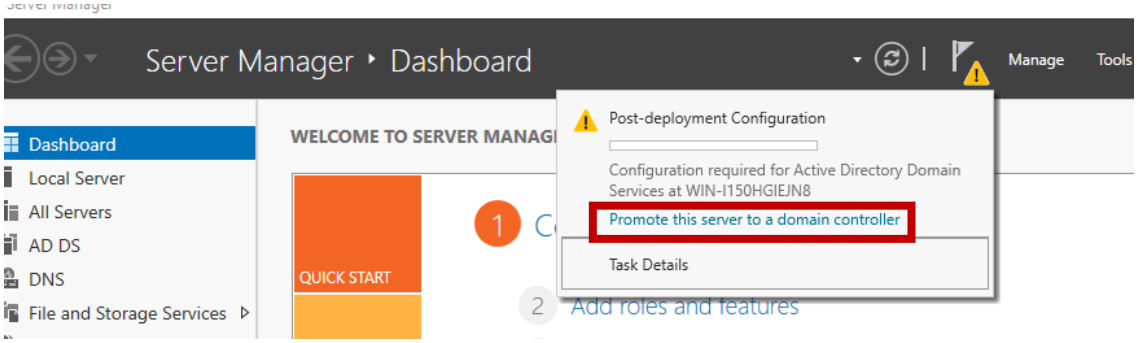
Passo 12 – Confirmar as ações anteriores e instalar:



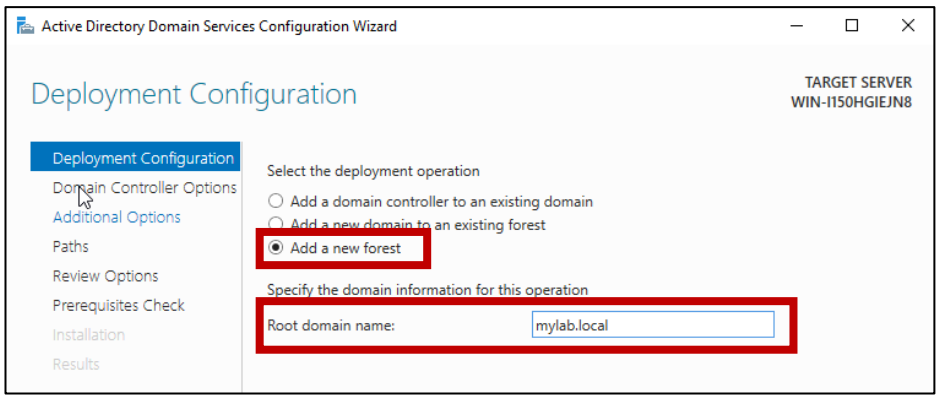
Passo 13 – Aguardar pelo processo da instalação:



Passo 14 – Reinicie a máquina virtual e de seguida, clique na opção "Promote this server to a domain controller":

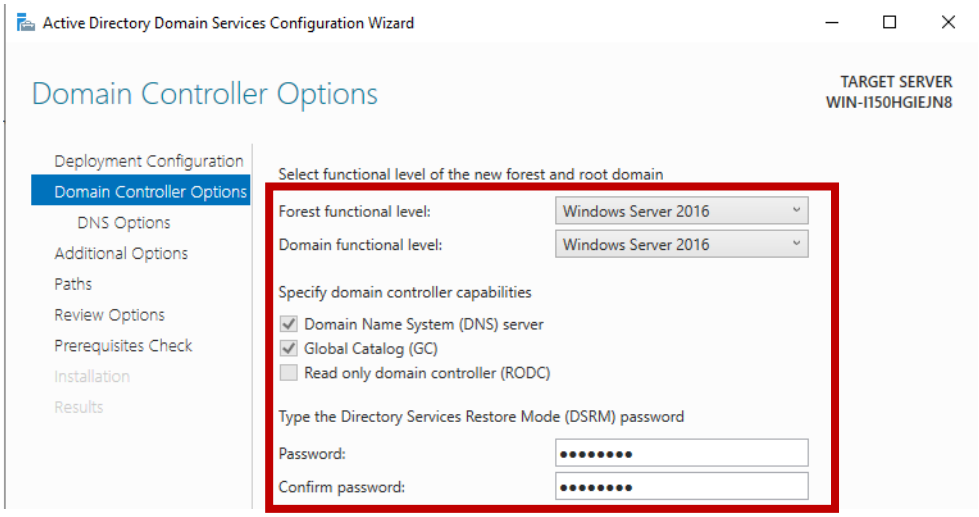


Passo 15 – Vamos configurar o Active Directory. Como tal, vamos criar uma nova floresta e de seguida coloque o nome "mylab.local":

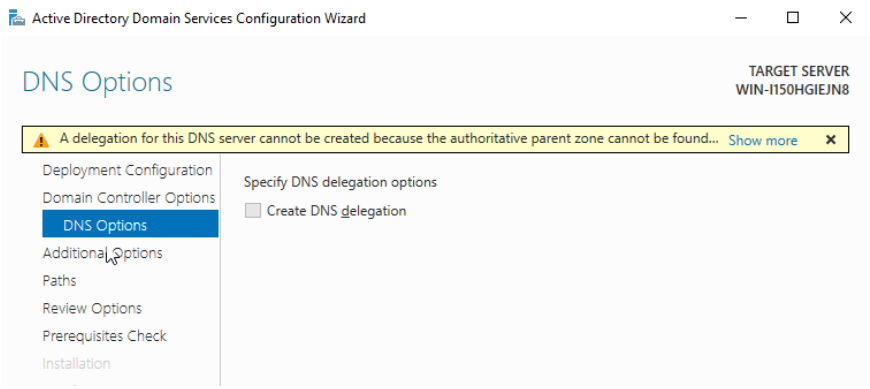


Passo 16 – Colocar/confirmar os seguintes valores:

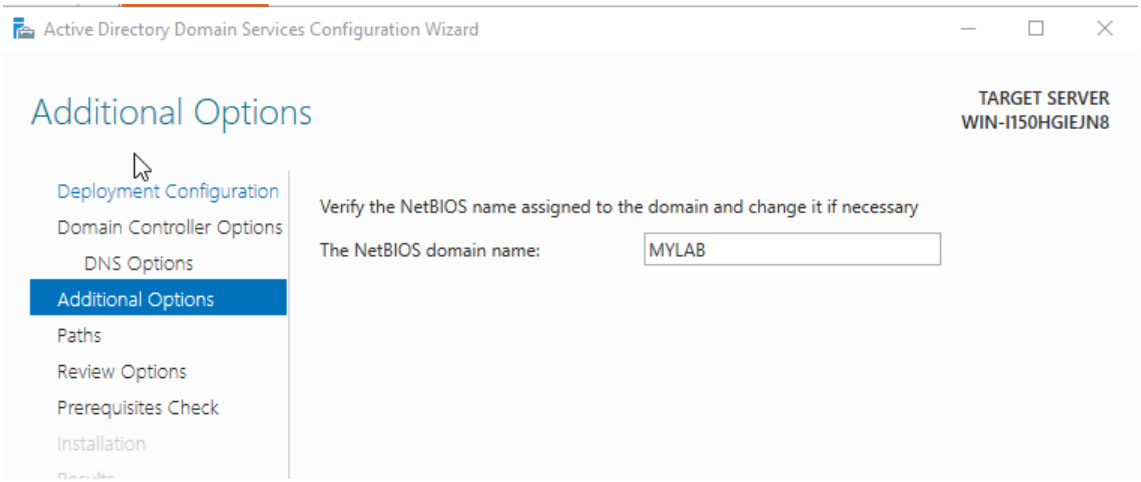
- Forest Funcional Level: compatibilidade com Sistema Windows Server 2016;
- Domain Funcional Level: compatibilidade com Sistema Windows Server 2016;
- Ativar as opções:
  - Domain Name System (DNS) server
  - Global Catalog (GC)
- Definir uma nova password e repetir a mesma;



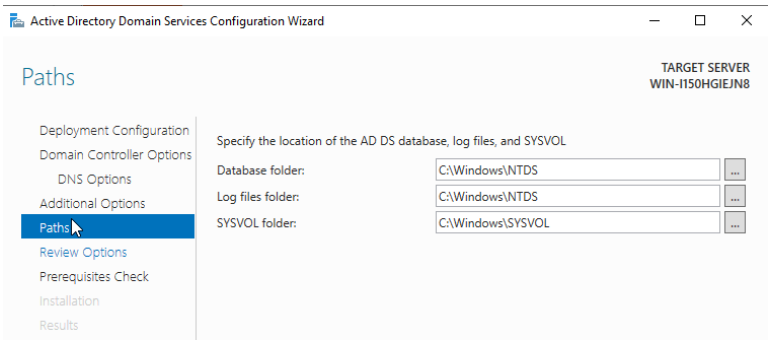
Passo 17 – Ignorar a criação do DNS delegation:



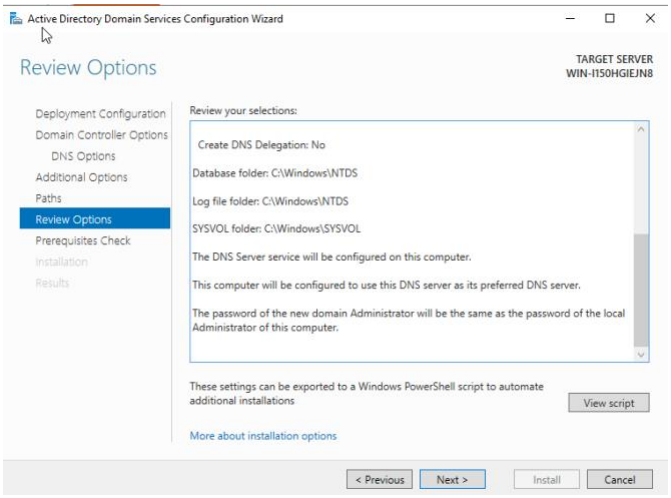
Passo 18 – Confirmar o nome do domínio na NETBIOS (neste caso será o nome MYLAB que foi definido anteriormente):



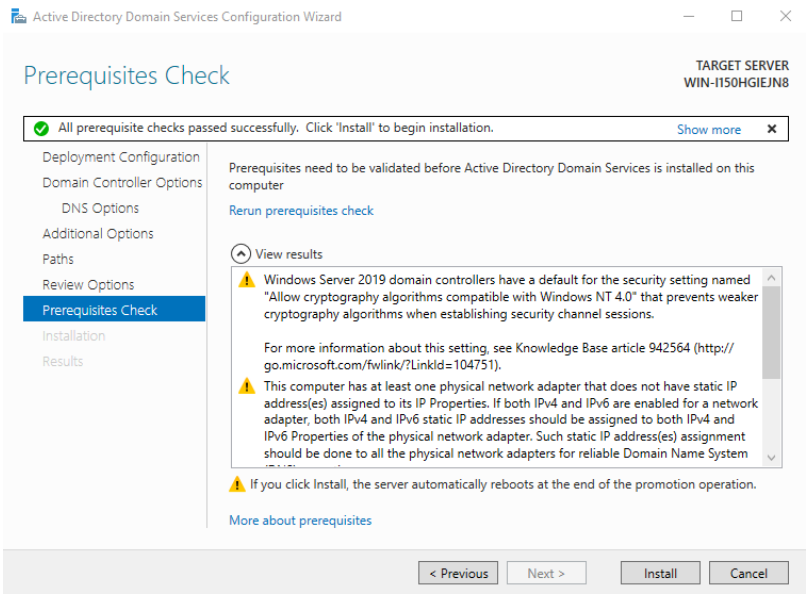
Passo 19 – Confirmar os locais onde vai armazenar os dados das configurações:



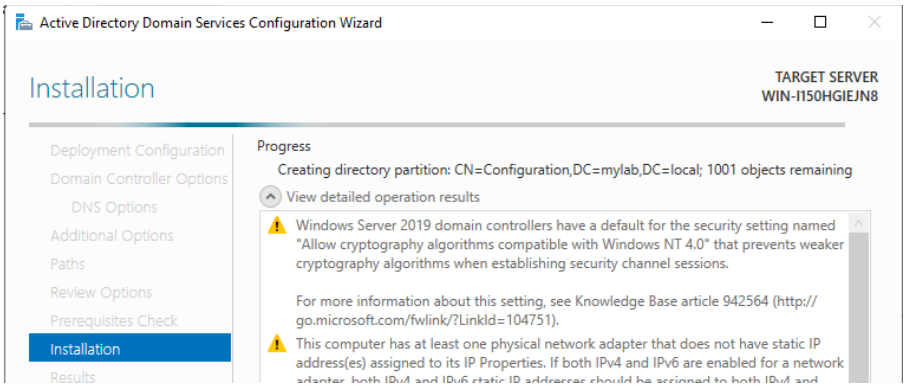
Passo 20 – Rever todas as opções da personalização do serviço:



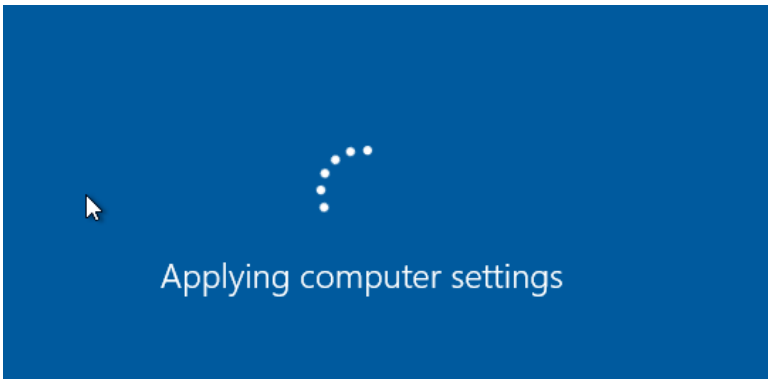
Passo 21 – Verificar se todos os requisitos passaram na validação e pedir para instalar:



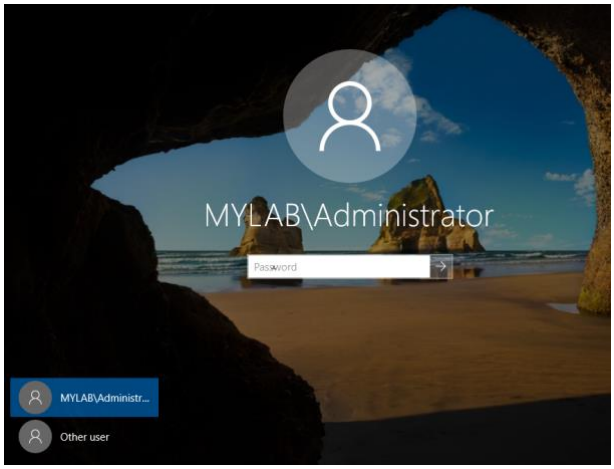
Passo 22 – Deixar a instalação finalizar:



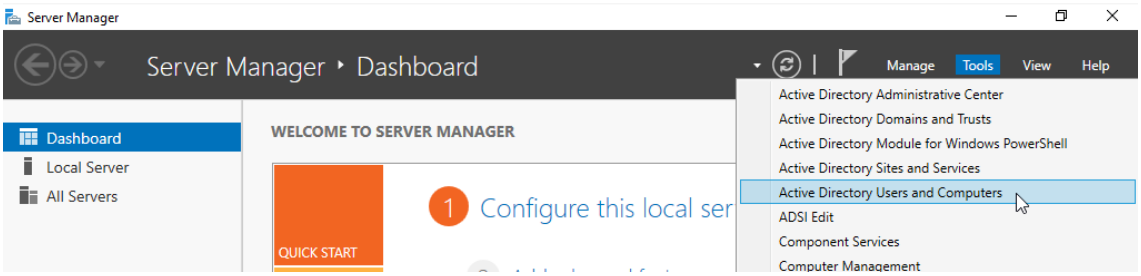
Após a personalização e instalação dos serviços, as contas e domínios vão ser atualizados e inseridos no novo domínio:



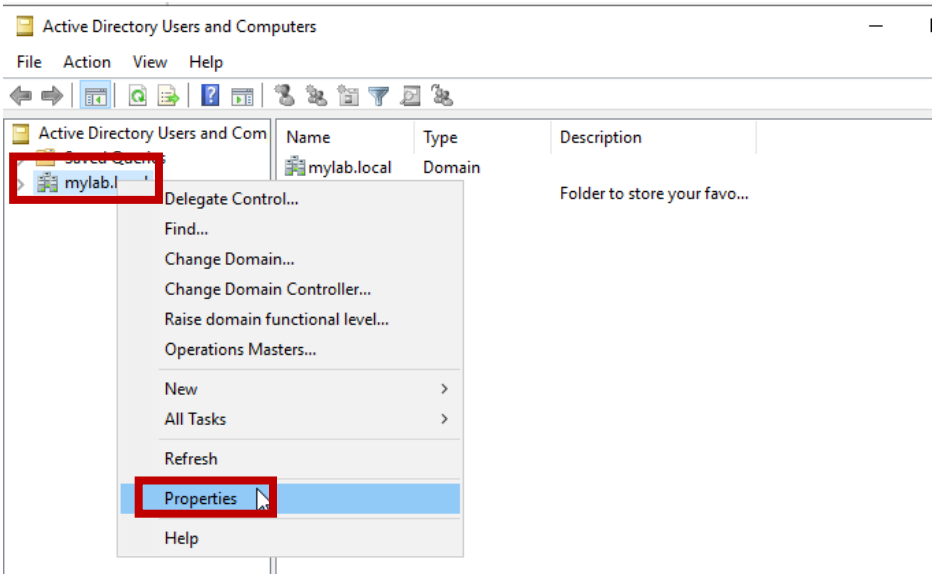
Passo 23 – Após a configuração, repare na tela do login a informar que agora pertence ao domínio MYLAB e logo a seguir qual a conta do utilizador que está a aceder. Faça o login na conta do administrador:

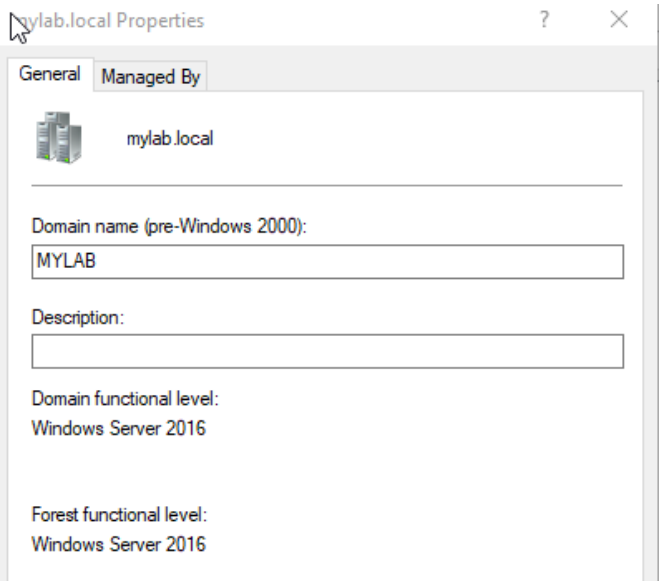


Passo 24 – Para verificar se ficou tudo em condições, vamos ao Server Manager e nas opções do menu superior deve selecionar Tools → Active Directory Users and Computers:



Verificar se instalou tudo em condições (abrindo as propriedades do AD):

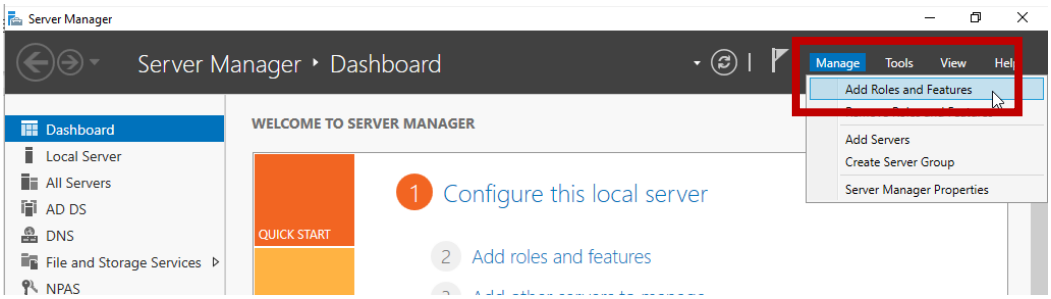

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
mylab.l
Name
Type
Description
mylab.local
Domain
Folder to store your favo...
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Properties
Help


mylab.local Properties
General
Managed By
mylab.local
Domain name (pre-Windows 2000):
MYLAB
Description:
Domain functional level:
Windows Server 2016
Forest functional level:
Windows Server 2016

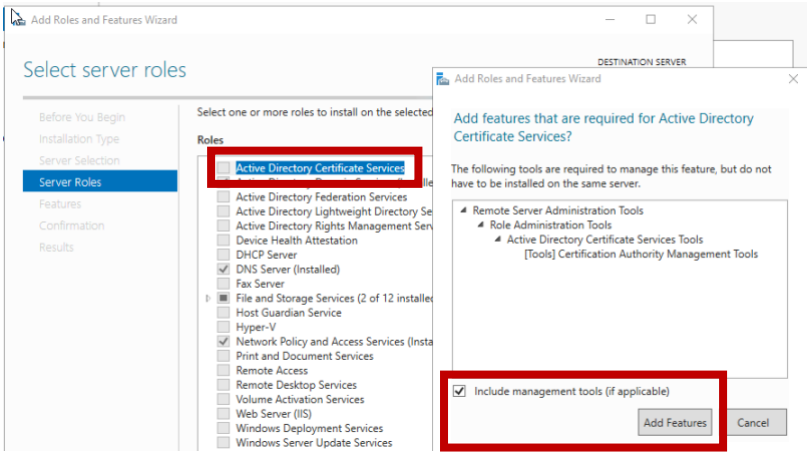
Parte 3 – Instalação de certificados Active Directory

O AD *Certificate Services* (Serviços de Certificados do Active Directory) é uma função do Windows Server para emitir e gerir certificados para os protocolos de autenticação e comunicação segura. Isto será útil para ajudar a proteger os acessos via RADIUS.

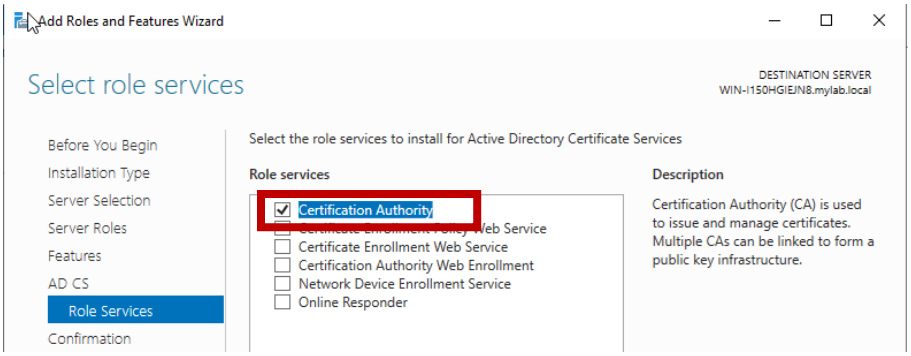
Passo 1 – Para instalar certificados AD, vamos ao menu Manage → Add Roles and Features:



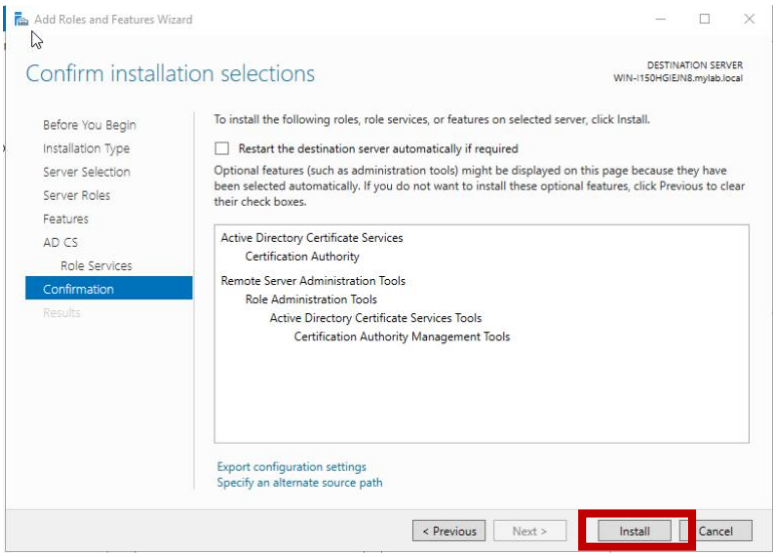
Passo 2 – Selecione a opção "Active Directory Domain Services" e confirme a operação:



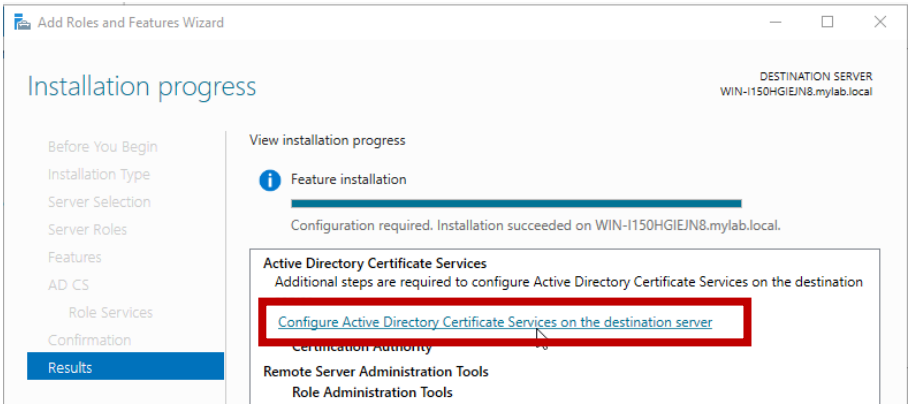
Passo 3 – Verificar se a opção "Certification Authority" está selecionada:



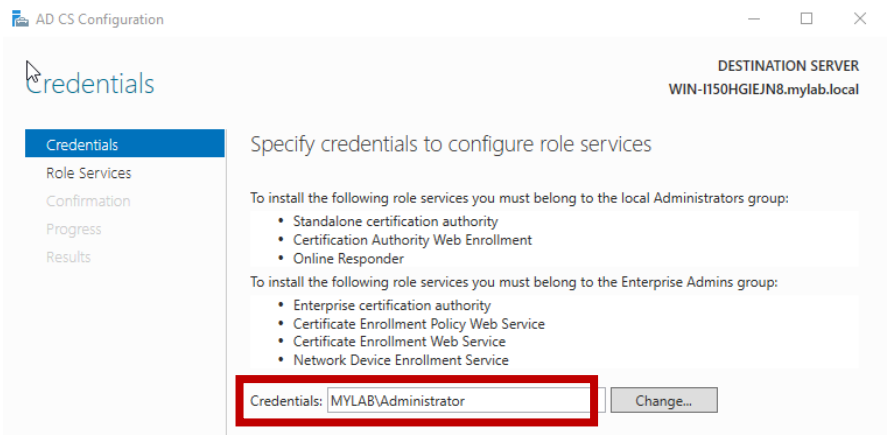
Passo 4 – Pedir para instalar a nova funcionalidade:



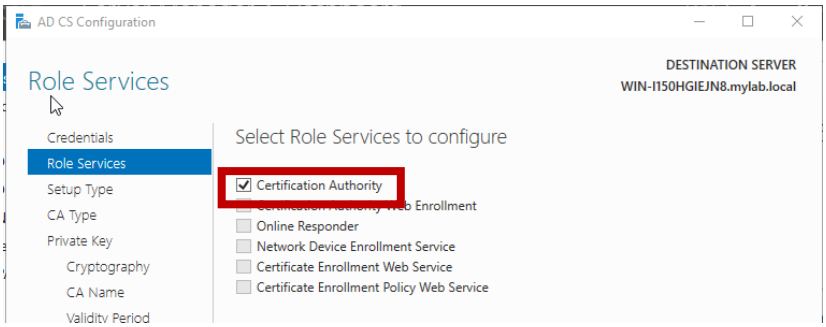
Passo 5 – Após a instalação, clique na opção para configurar o serviço instalado:



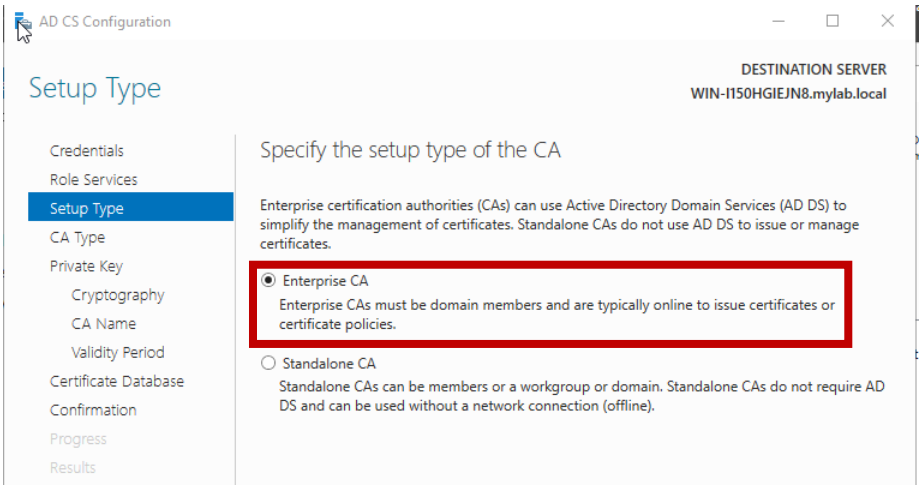
Passo 6 – Confirmar que estão a utilizar as credenciais da conta administrador:



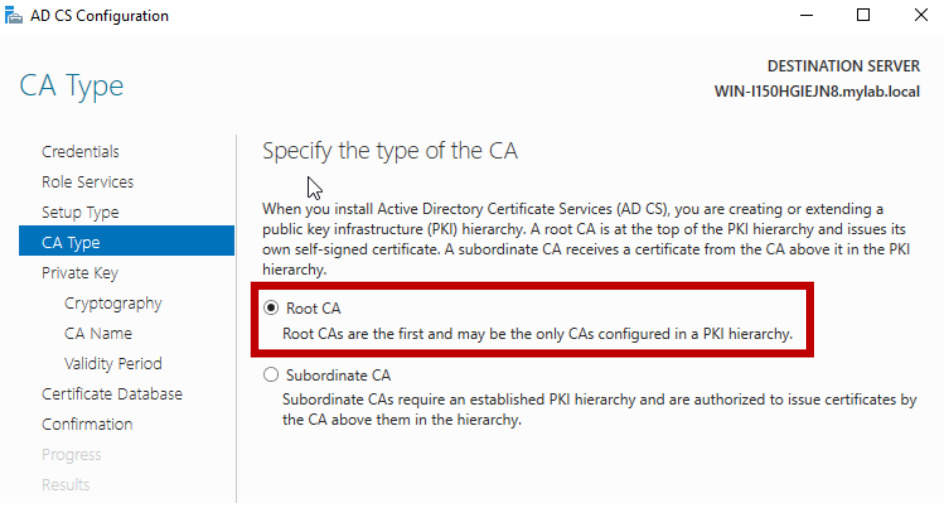
Passo 7 – Selecionar a configuração da opção "Certification Authority":



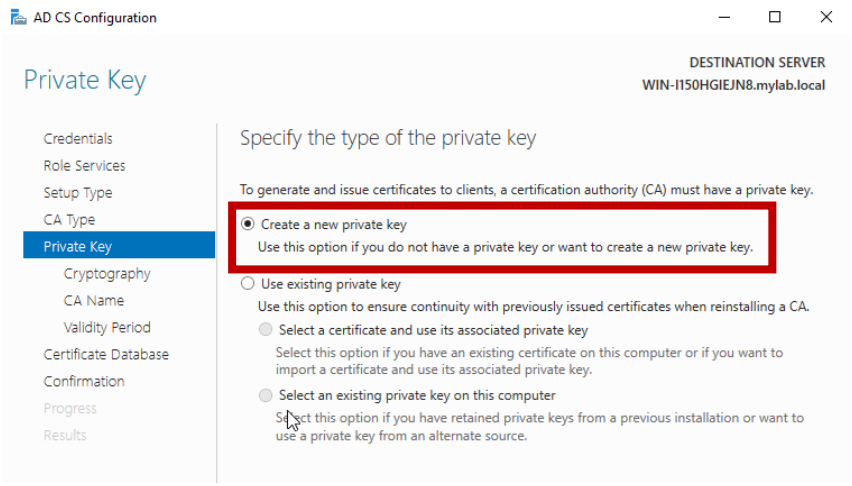
Passo 8 – Selecionar a opção Enterprise-CA:



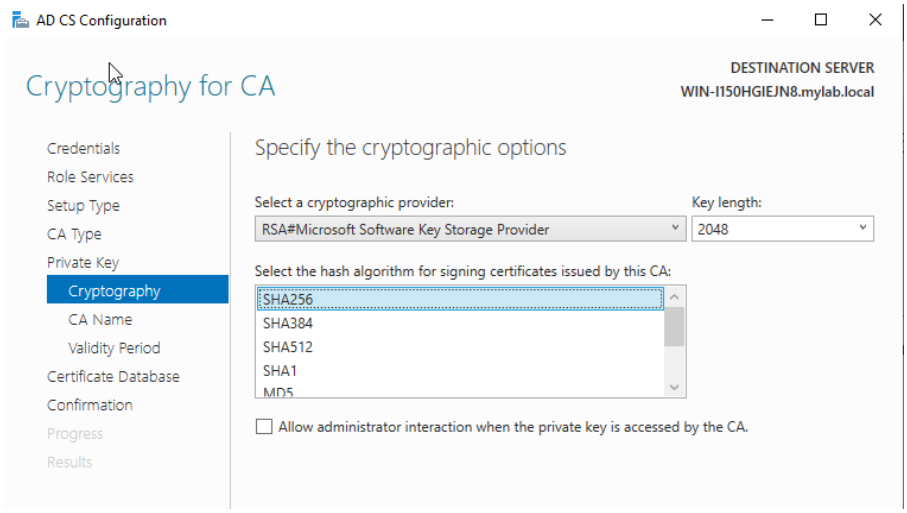
Passo 9 – Selecionar a opção Root CA:



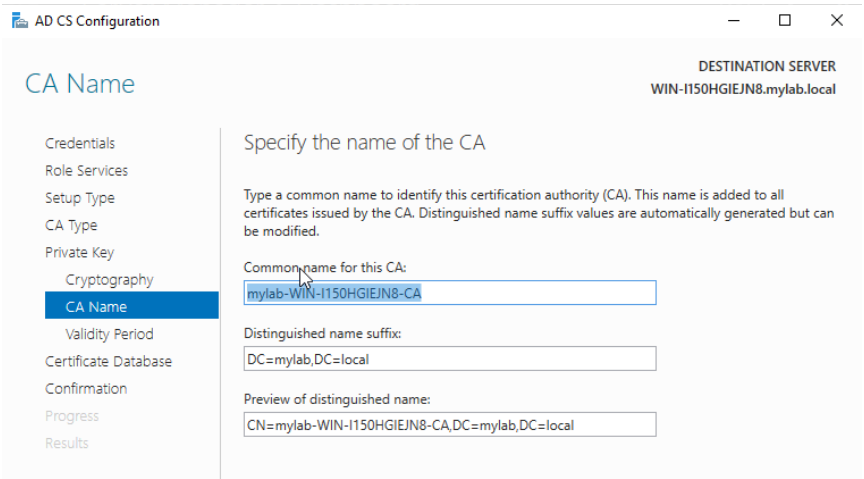
Passo 10 – Pedir para gerar uma nova chave privada:



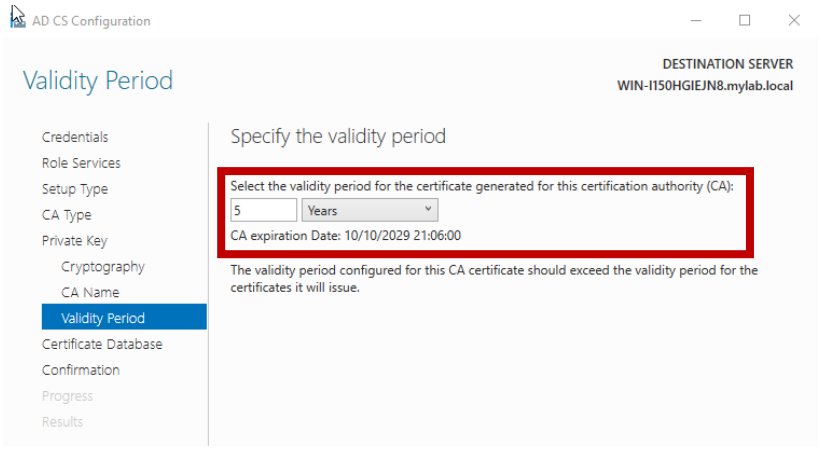
Passo 11 – Selecionar a criptografia RSA com 2048 bits e HASH: SHA256



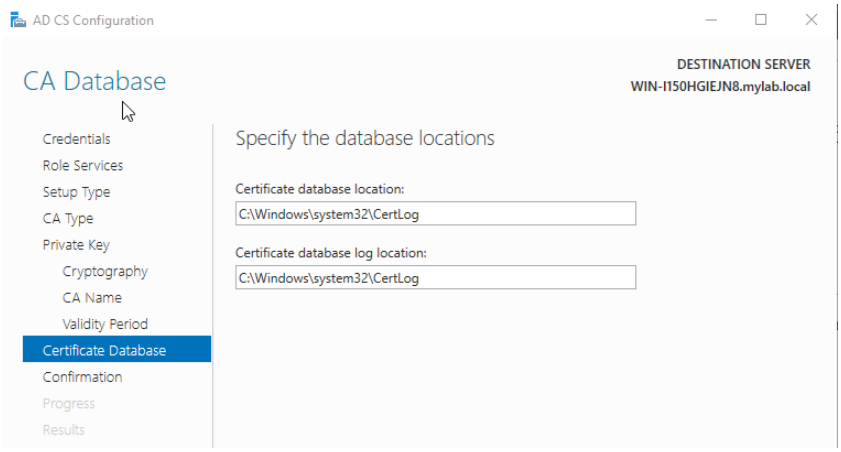
Passo 12 – Confirmar os dados com a associação do domínio nos dados da chave privada:



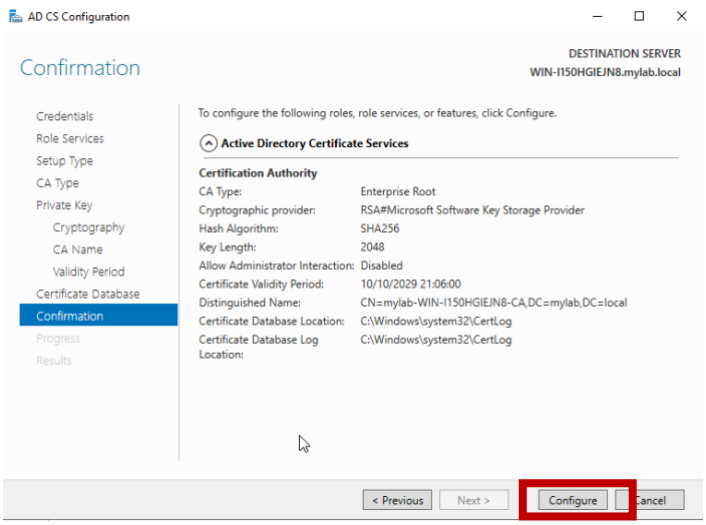
Passo 13 – Definir o período de validade da chave a ser gerada (vamos assumir 5 anos):



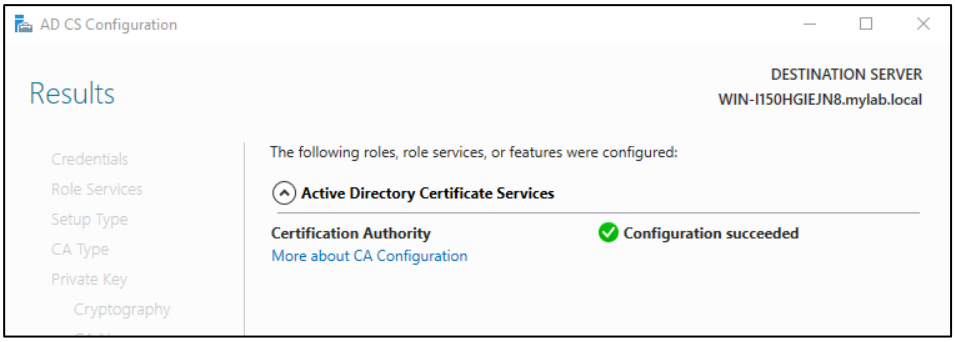
Passo 14 – Confirmar onde vão ficar os dados de registo e logs:



Passo 15 – Confirmar os dados da instalação e instalar:



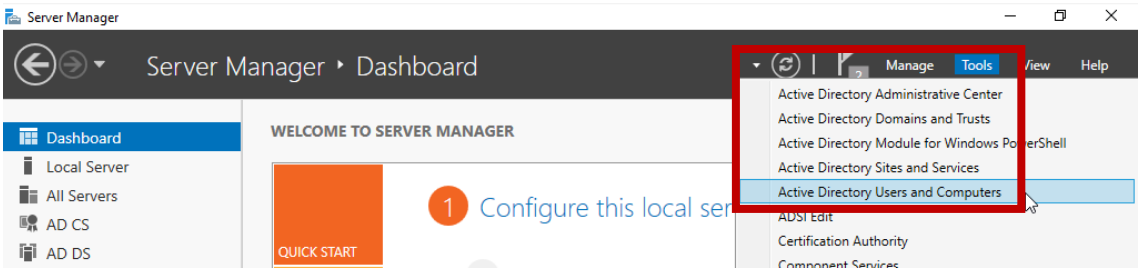
Se tudo correr bem, será exibida a mensagem de confirmação:



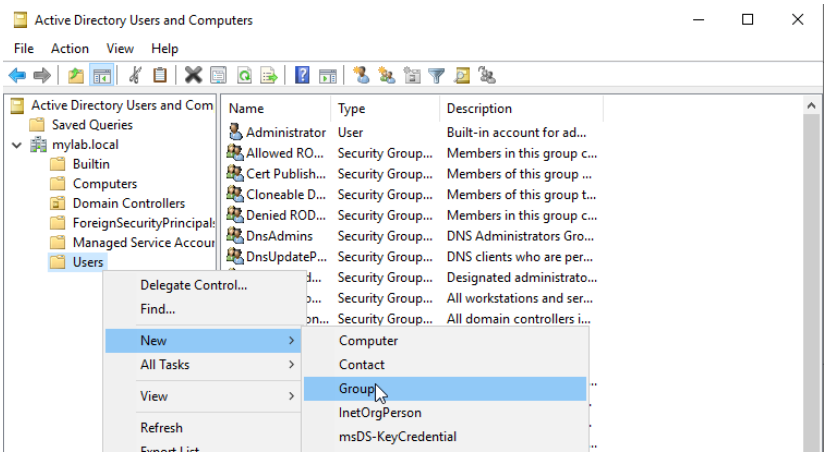
Parte 4 – Criação de Grupos e Utilizadores

Antes de ir para as configurações do servidor, vamos adicionar utilizadores e grupos específicos para este trabalho.

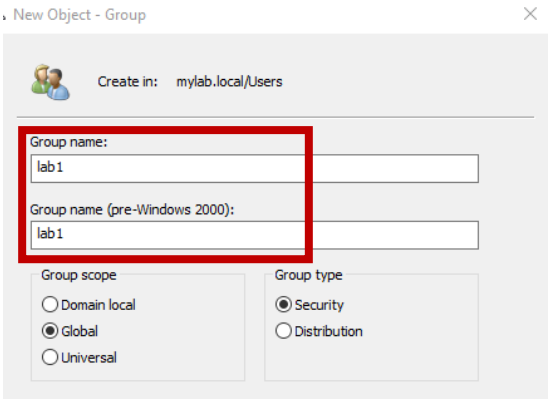
Passo 1 – Selecionar a opção Tools → Active Directory Users and Computers:



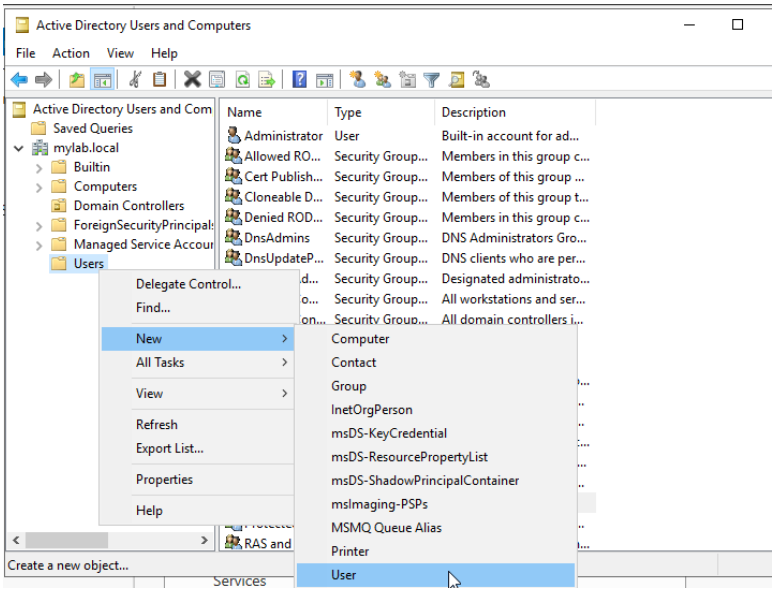
Passo 2 – Clicar com o lado direito do rato em cima da pasta Users e selecionar as opções New → Group:



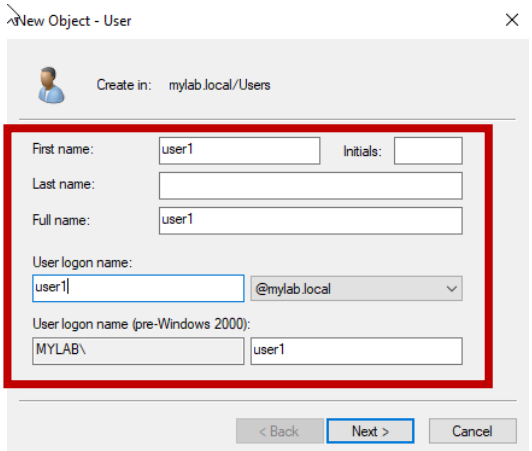
Passo 3 – Criar o grupo com o nome "lab1":



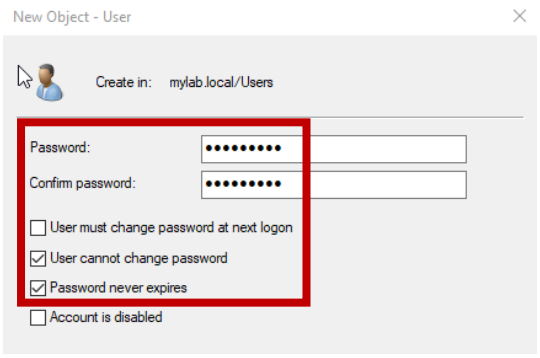
Passo 4 – Clicar com o lado direito do rato em cima da pasta Users e selecionar as opções New → User:



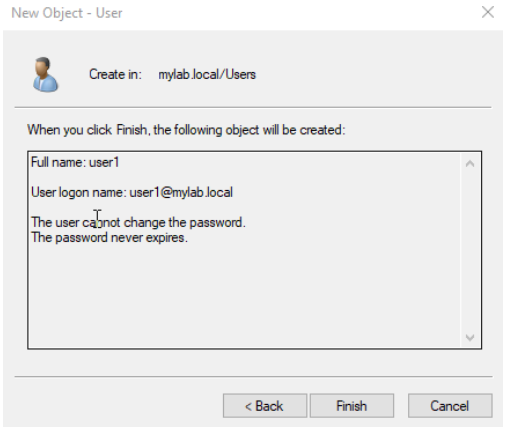
Passo 5 – Criar o utilizador "user1" e carregar em seguinte:



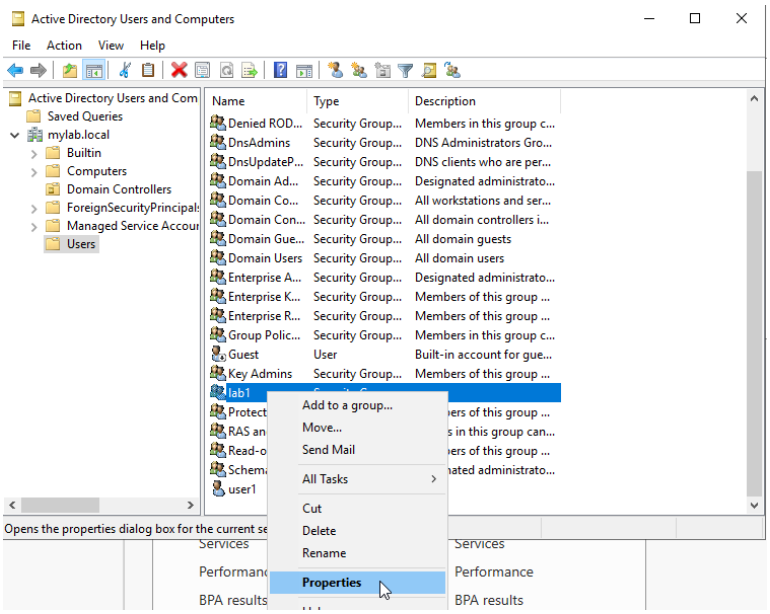
Passo 6 – Definir a password e selecionar as opções para não alterar password e que nunca expira:



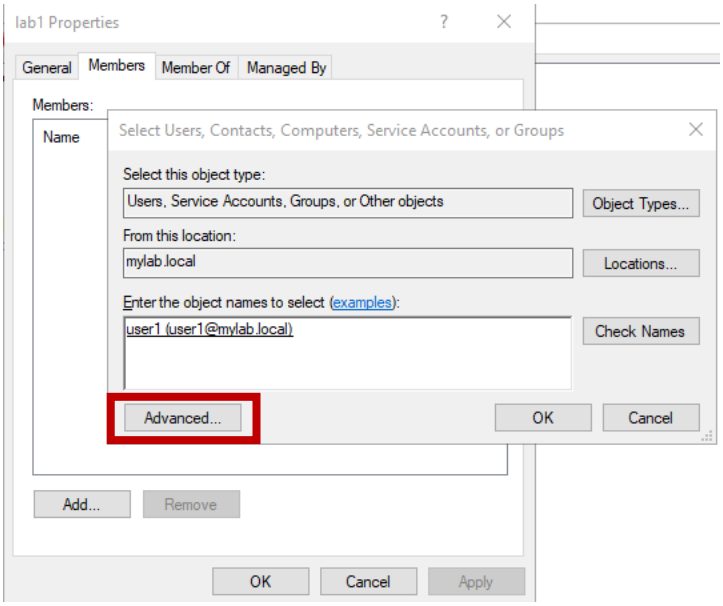
Passo 7 – Confirmar as operações:



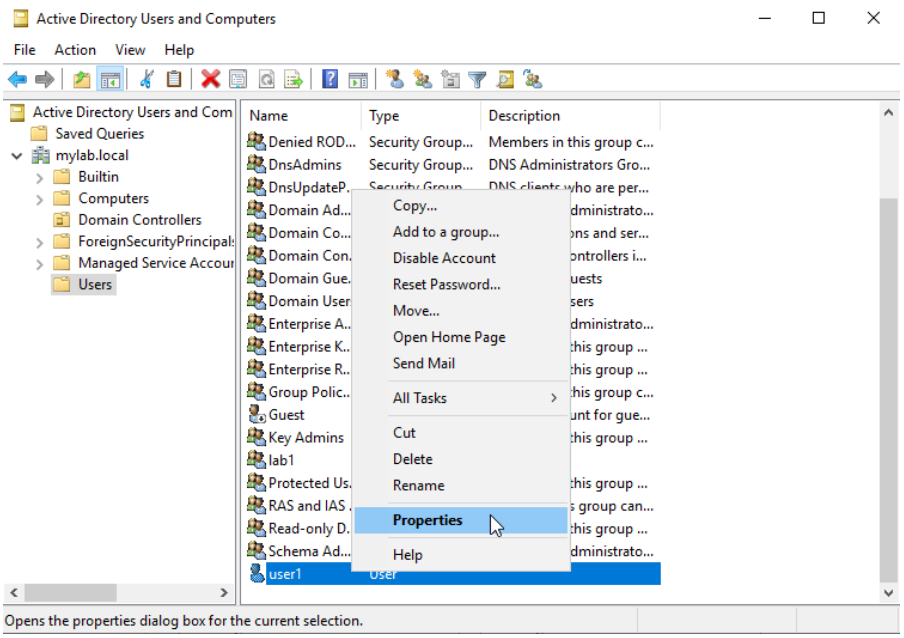
Passo 8 – Clicar com o lado direito do rato na pasta Users, selecionar o grupo lab1 e abrir as propriedades:



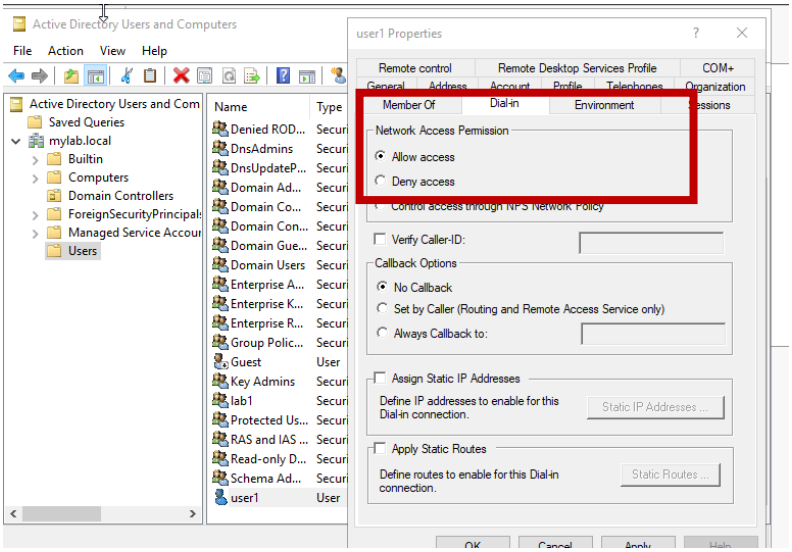
Passo 9 – Selecione o separador Members e depois mais abaixo o botão Add. Na nova janela, clique no botão Advanced e adicione o user1:



Passo 10 – De seguida, vamos clicar para abrir as propriedades do "user1":

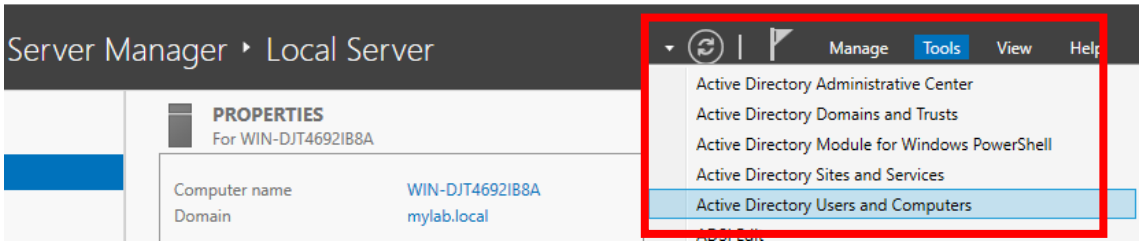


Passo 11 – Nas propriedades do utilizador, selecione o separador Dial-in e verifique se nas propriedades de Network Access Permission tem a opção Allow Access selecionada:

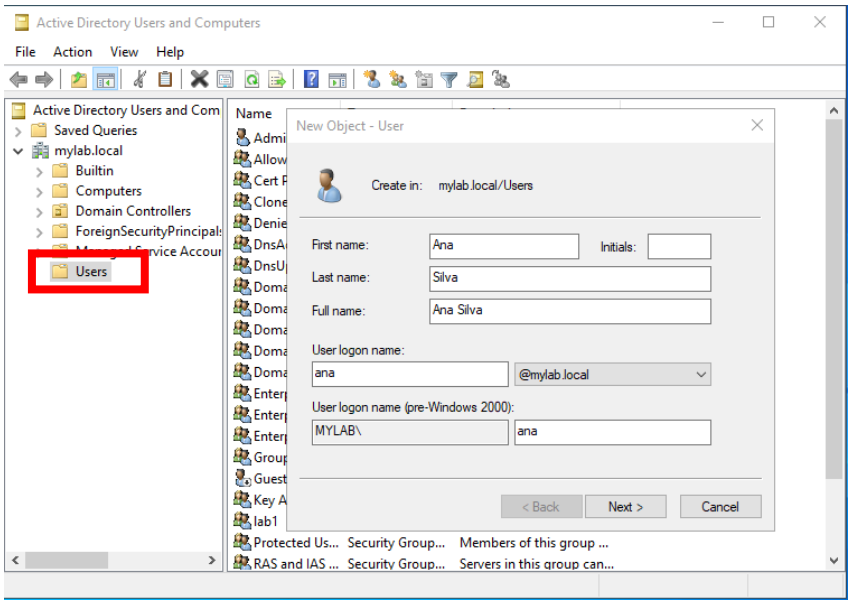


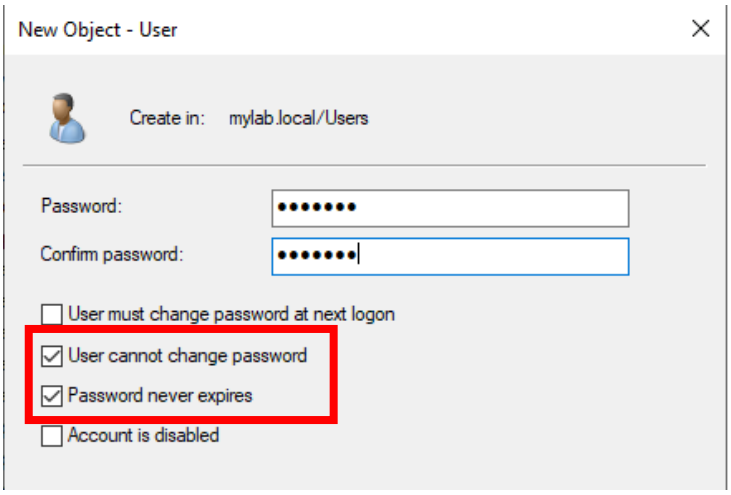
Parte 5 – Configurar Acesso Remoto

Passo 1 – Vamos entrar na seção dos utilizadores e computadores do active directory:

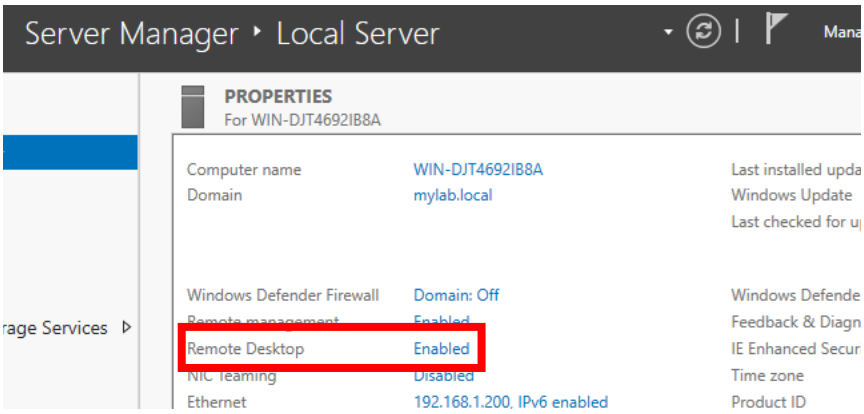


Dentro da gestão de utilizadores, deve clicar com o lado direito do rato em cima da pasta Users e adicionar a utilizadora Ana, como demonstra as seguintes imagens:



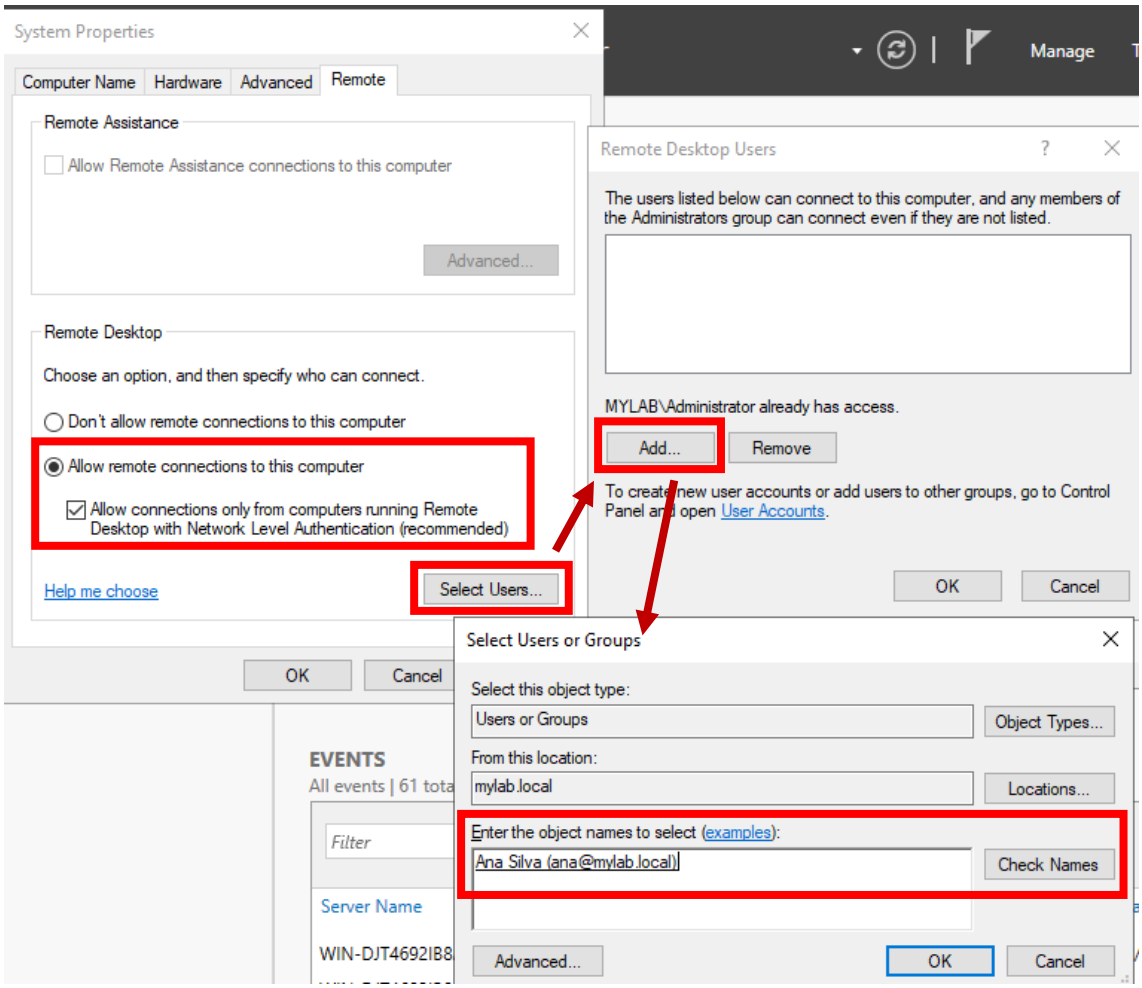


Passo 2 – Verificar se a opção de acesso remoto está ativo (Enabled):



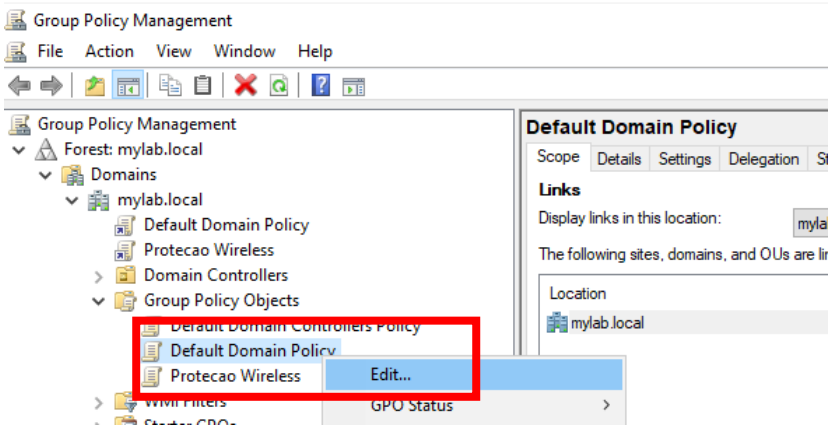
Passo 3 – Verificar se tem permissões ativadas (Allow remote connections to this computer) e carregue no botão Select Users.

Dentro desta seção deve adicionar a utilizadora Ana:



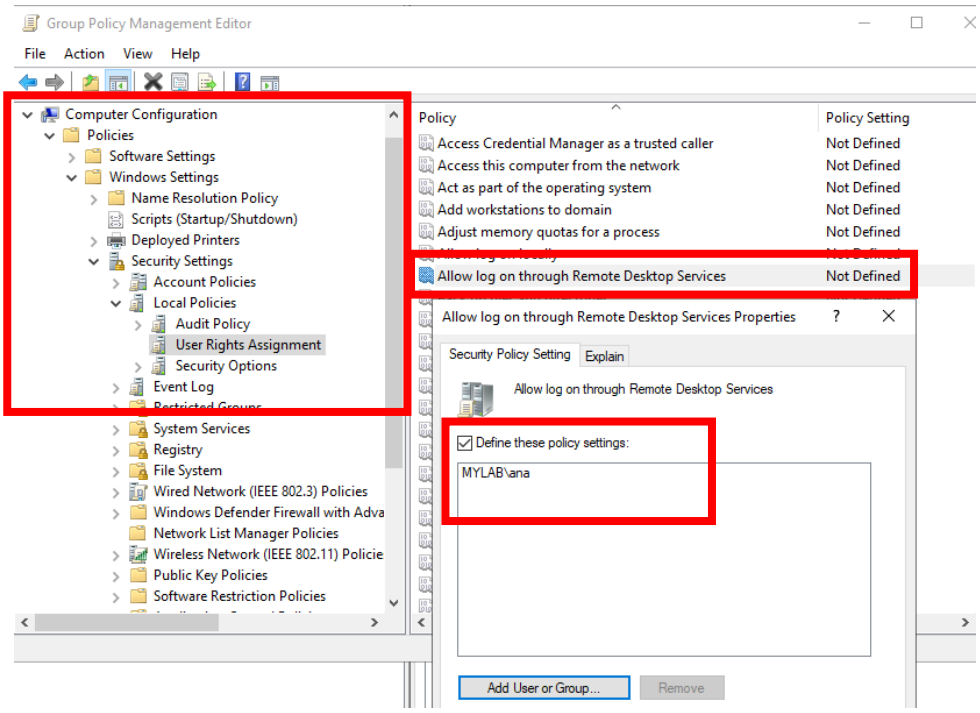
Passo 4 – O passo anterior ainda não chega para dar as permissões de acesso remoto. Como tal, vamos ter de atribuir a política de segurança para ligar remotamente.

Vamos ao Group Policy Management, clicar com o lado direito do rato nas políticas por defeito e selecionar a opção editar:



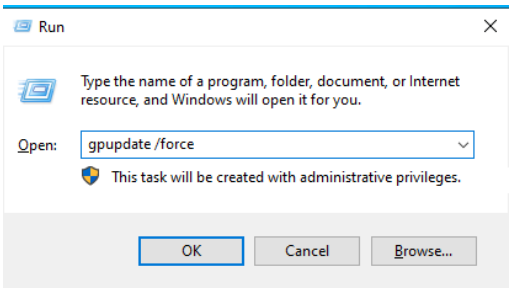
Navegue as seguintes pastas: Computer Configuration → Policies → Windows Settings → Security Settings → LocalPolicies → User Rights Assignment.

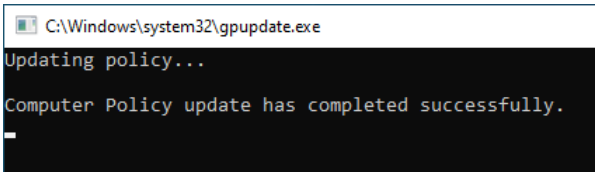
Depois selecione a opção Aloow log on trough Remote Desktop Services, ative esta opção e adicione a utilizadora que criou mais acima:



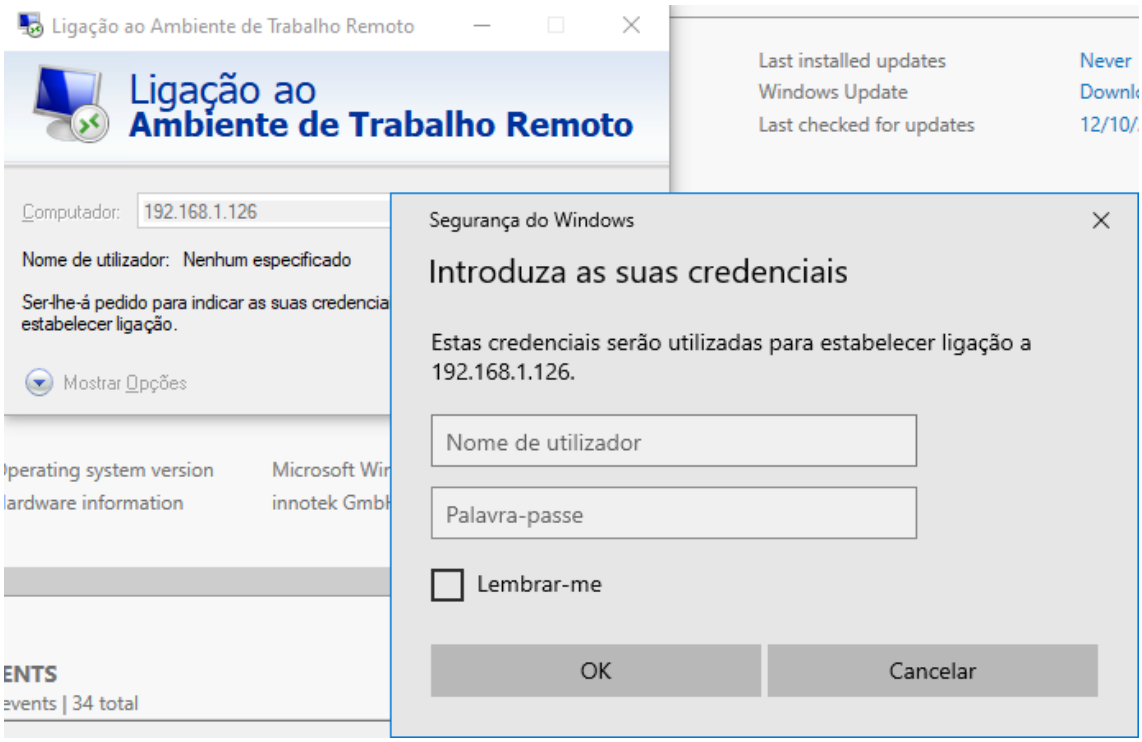
Testar as novas alterações:

Vamos atualizar a política de segurança através da aplicação “Executar” ou “Run” e colocar o código para atualizar as novas políticas de segurança:





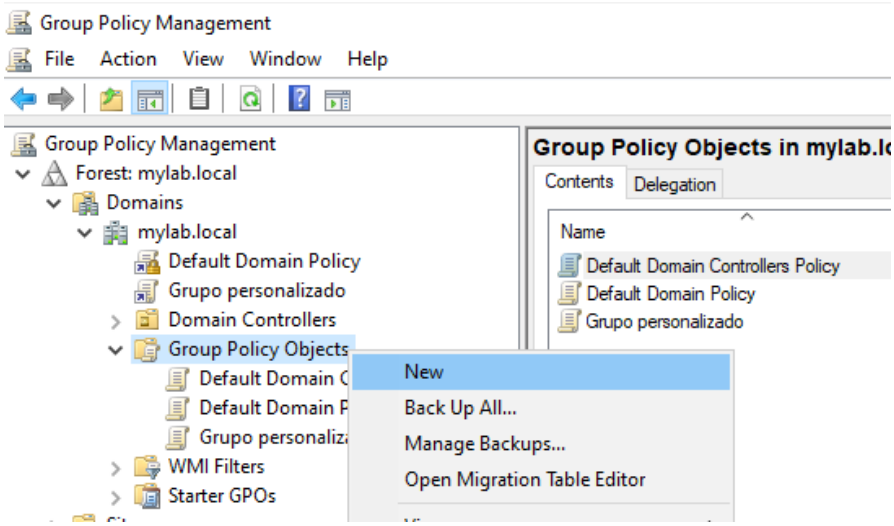
No computador original (físico), tente fazer conexão remota para a máquina virtual e entre com os dados de acesso da Ana:



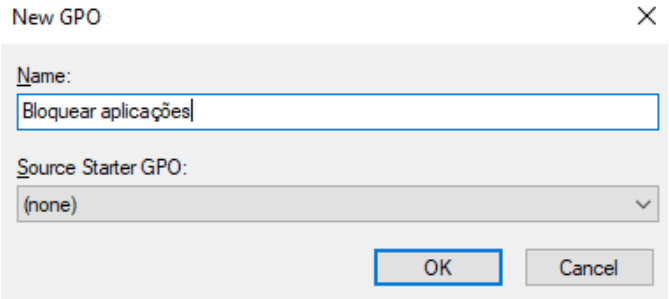
Exercício: Tente aceder as opções de rede, mais especificamente as propriedades do adaptador e verifique se as regras do exercício anterior estão aplicadas!

5 - Restrições de instalação de software

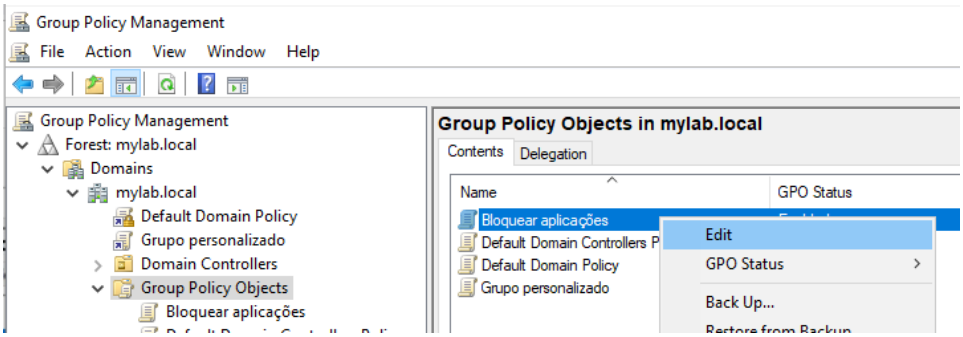
Passo 1 - Vamos criar outro grupo de política de segurança, mas desta vez, vamos dar nomes personalizados:



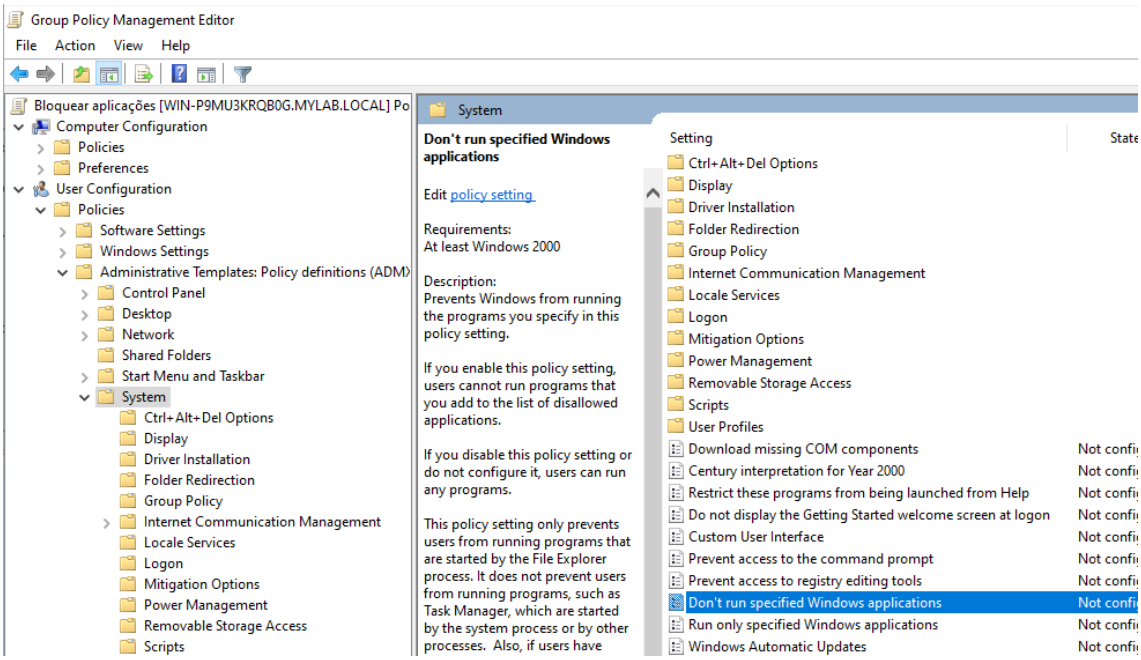
Coloque o nome “Bloquear aplicações”:



Passo 2 - Edite as políticas na nova regra:

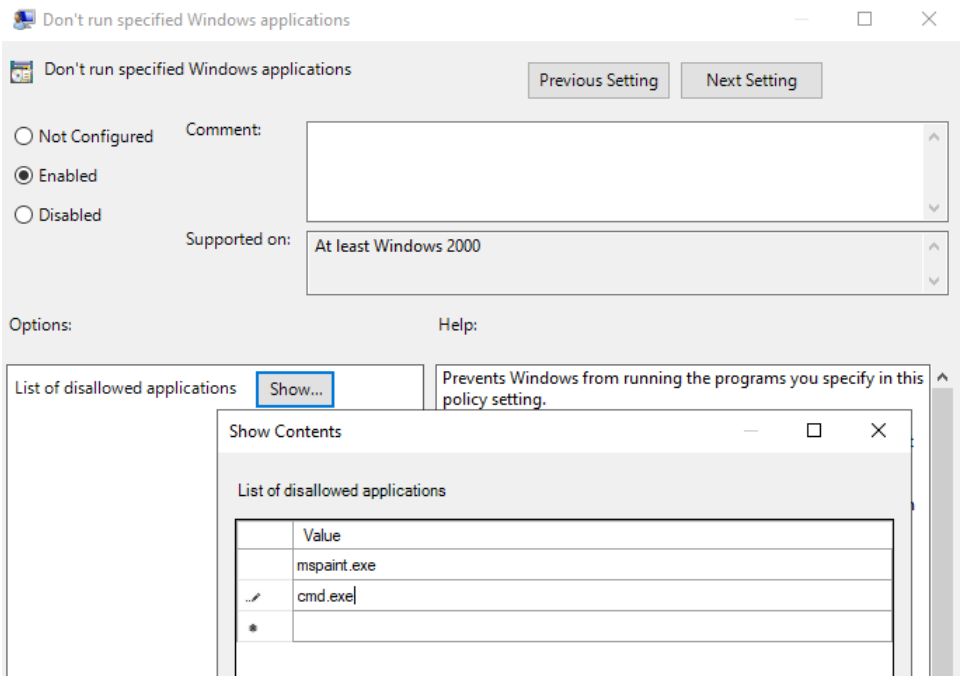


Passo 3 – Navegue até ao diretório User Configuration → Policies → Administrative Templates → System. No lado direito deve selecionar a opção "Don't run specified Windows Applications":

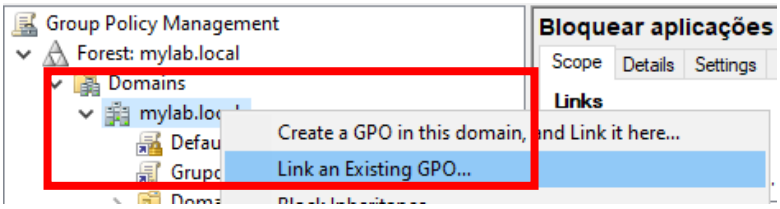


Passo 4 – Ative a funcionalidade e no botão Show, deve colocar os seguintes programas:

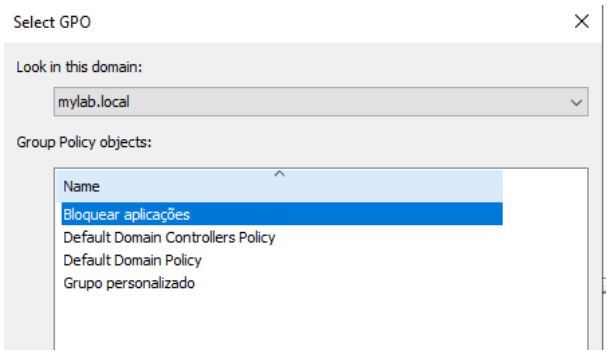
- Cmd.exe (abrir linha de comandos/terminal);
- Mspaint.exe (abrir o editor de imagens do Windows);

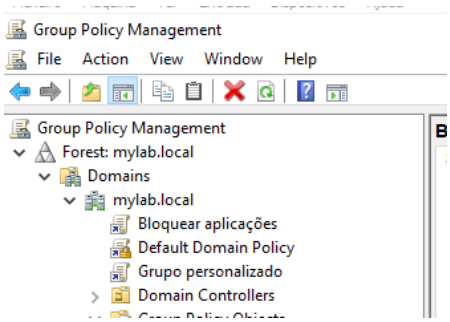


Passo 5 – Como este passo foi uma nova regra, temos de importar e associar a mesma para dentro das políticas GPO do Windows Server. Como tal, vamos clicar com o lado direito do rato em cima do domínio mylab.local e selecionar a seguinte opção:



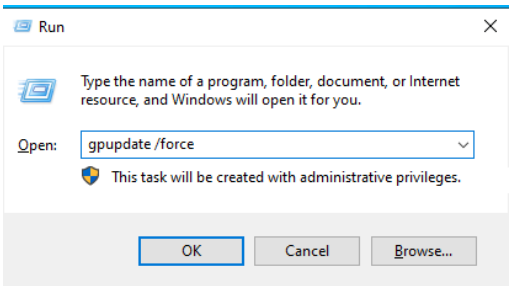
Passo 6 – Verificar se estamos no domínio mylab.local e de seguida, vamos selecionar e associar a nova regra dentro da politica do grupo GPO:

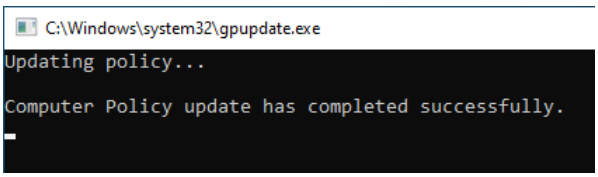




Testar as novas alterações:

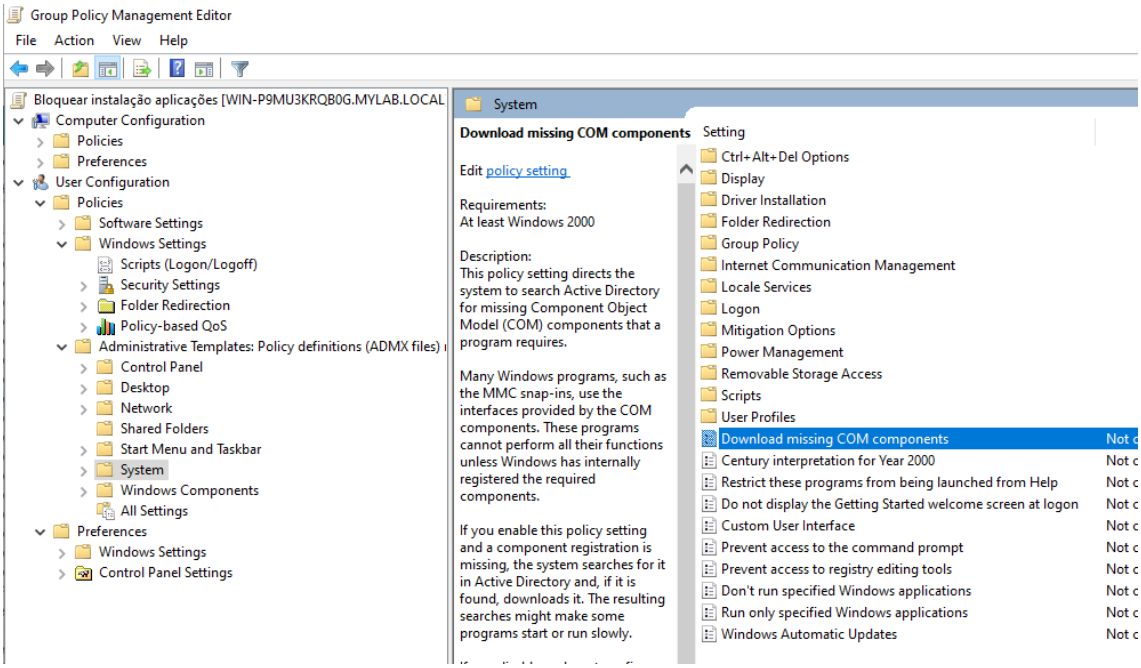
Vamos atualizar a política de segurança através da aplicação "Executar" ou "Run" e colocar o código para atualizar as novas políticas de segurança:





Tarefa: Faça logout da conta do cliente atual e volte a iniciar a sessão. Verifique se consegue abrir as aplicações que foram bloqueadas!

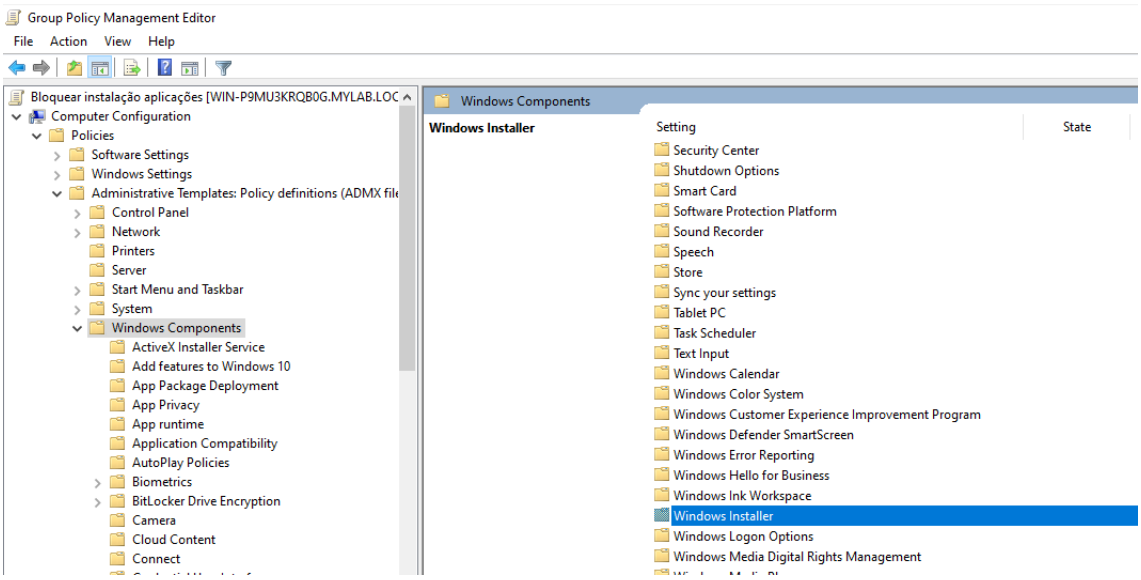
Para além disso ainda tem outras opções adicionais para políticas de segurança, como por exemplo, Windows Updates, bloquear portas USB, execuções especificas, entre outras opções:



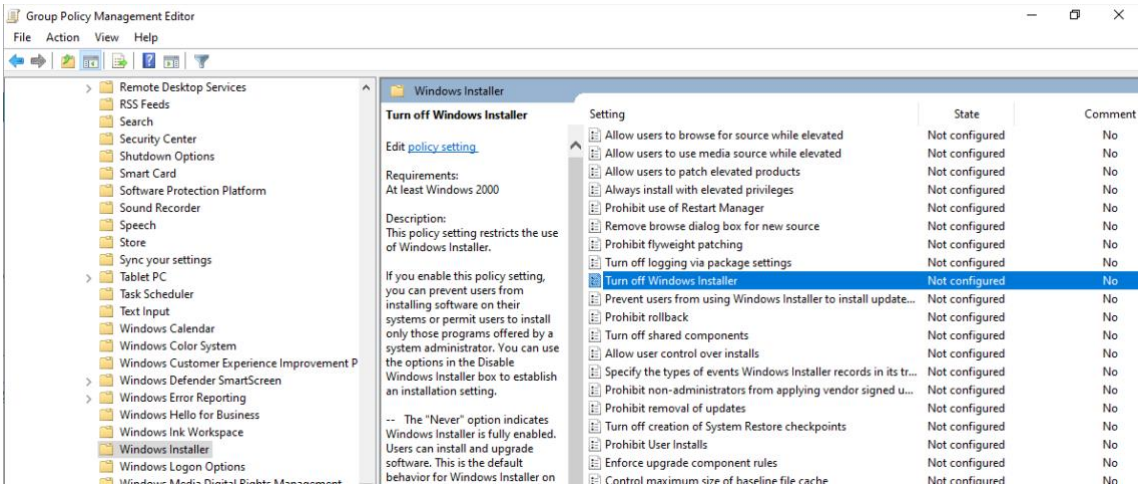
6 - Bloquear instalação de software

Vamos observar como bloquear as instalações de programas no Windows. Siga os seguintes passos:

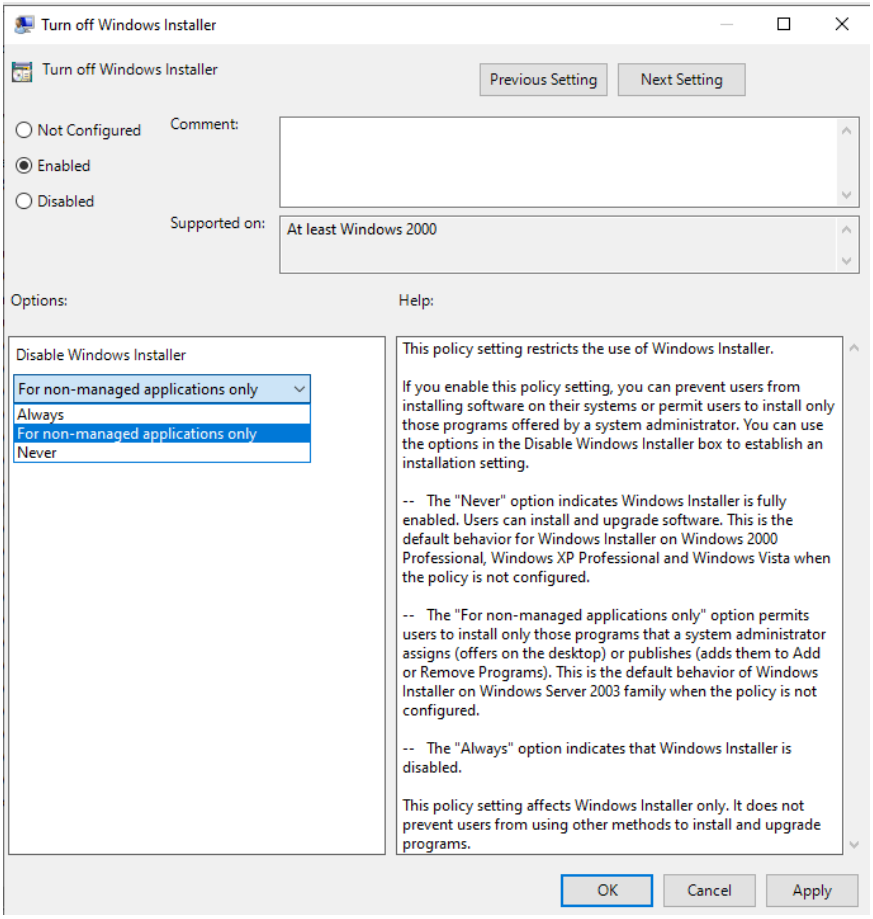
Passo 1 – Crie uma nova regra GPO com o nome "Bloquar instalações de aplicações" e de seguida, edite a regra e vamos navegar até ao diretório Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Installer:



Passo 2 – Dentro desta pasta, vamos ativar a opção "Turn off Windows Installer" (mas repare que há mais opções):

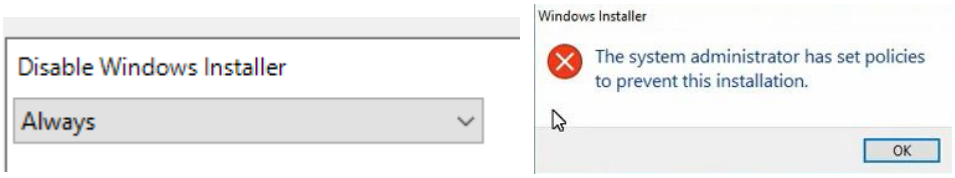


Passo 3 – Ative a funcionalidade e logo abaixo, temos a opção "Disable Windows Installer".

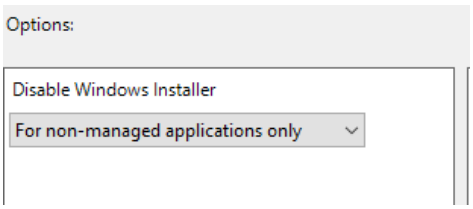


Passo 4 - Nesta caixa de seleção, temos duas opções:

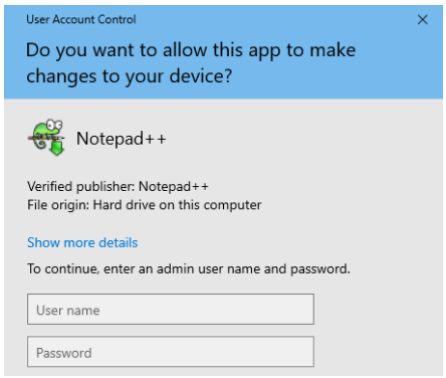
- Always → bloqueia a instalação para os utilizadores;



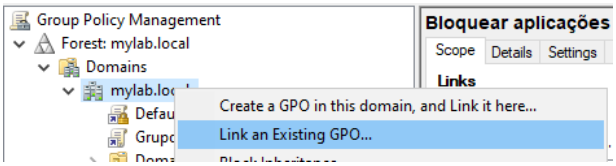
- For non-managed aplications only → permite instalar software com uma conta de permissão elevada

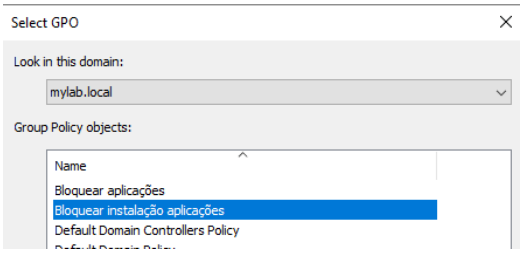


Tarefa: Ative a opção For-non-managed applications only



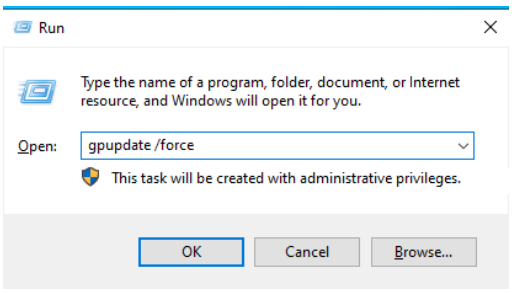
Passo 5 - Aplicar novas atualizações:

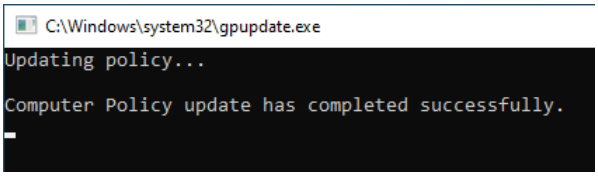




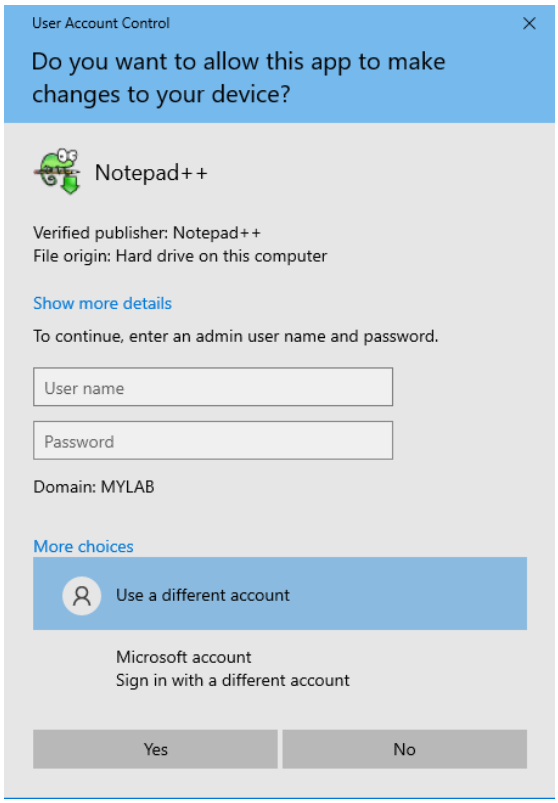
Testar as novas alterações:

Vamos atualizar a política de segurança através da aplicação "Executar" ou "Run" e colocar o código para atualizar as novas políticas de segurança:





Entre na conta da Ana e tente instalar aplicações:


User Account Control
Do you want to allow this app to make changes to your device?
Notepad++
Verified publisher: Notepad++
File origin: Hard drive on this computer
Show more details
To continue, enter an admin user name and password.
User name
Password
Domain: MYLAB
More choices
Use a different account
Microsoft account
Sign in with a different account
Yes
No