LABORATÓRIO 5

Gestão de Acessos (IAM) com aplicação do princípio de Least Privilege

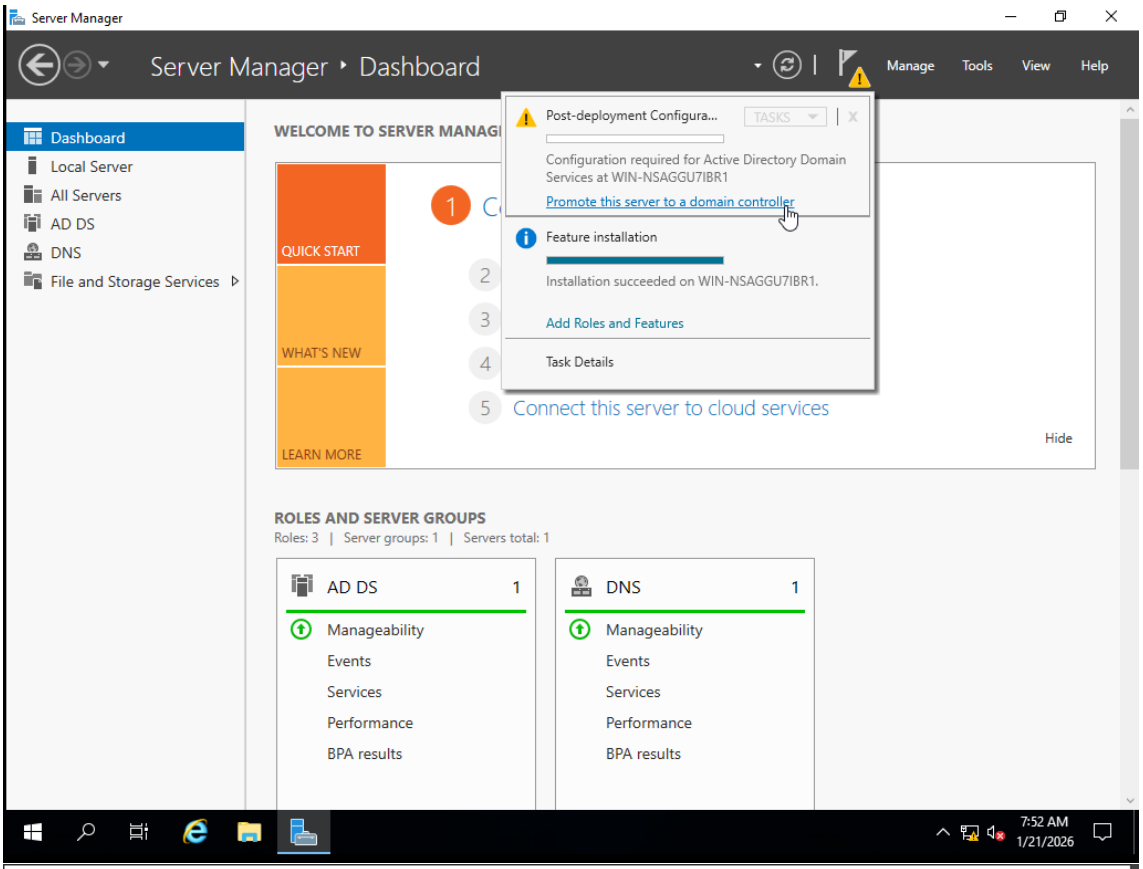
Data: 21/01/2026
Nome: Lucas Vieira Areal
Ambiente: Windows Server 2019
Repositório: https://github.com/sacullaera/Labs/tree/main/IAM-Governance

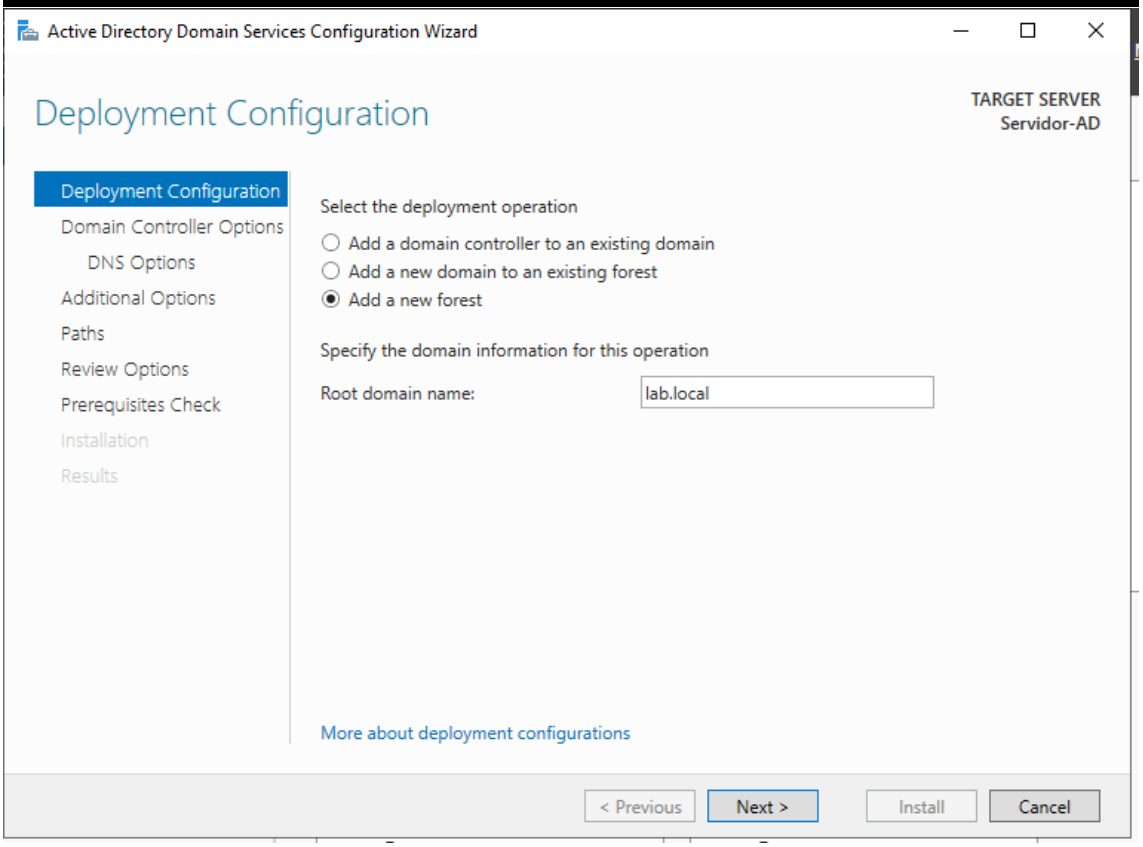
Este laboratório tem como objetivo a implementação de um servidor Microsoft Windows Server 2019 para gestão de acessos do Active Directory (AD) simulando dessa forma um programa completo de gestão de acessos (IAM) em um ambiente realista, incluindo:

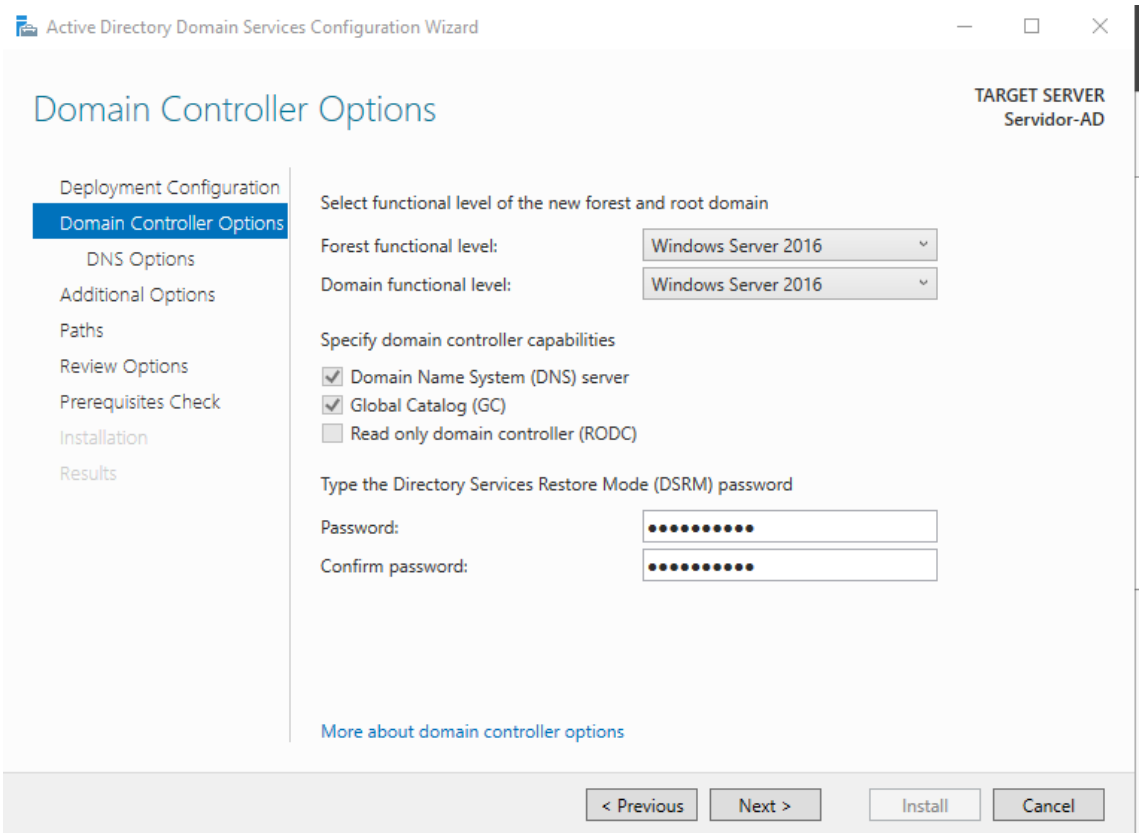
- Criação de domínio e GPOs com Active Directory;
- Onboarding de usuários com cargos e permissões;
- Aplicação do principío de least privilege;
- Revisão dos acessos acima de 90 dias após a última revisão;
- Offboarding de usuários seguro (desativação + revogação);
- Documentação alinhada com LGPD e boas práticas de governança.

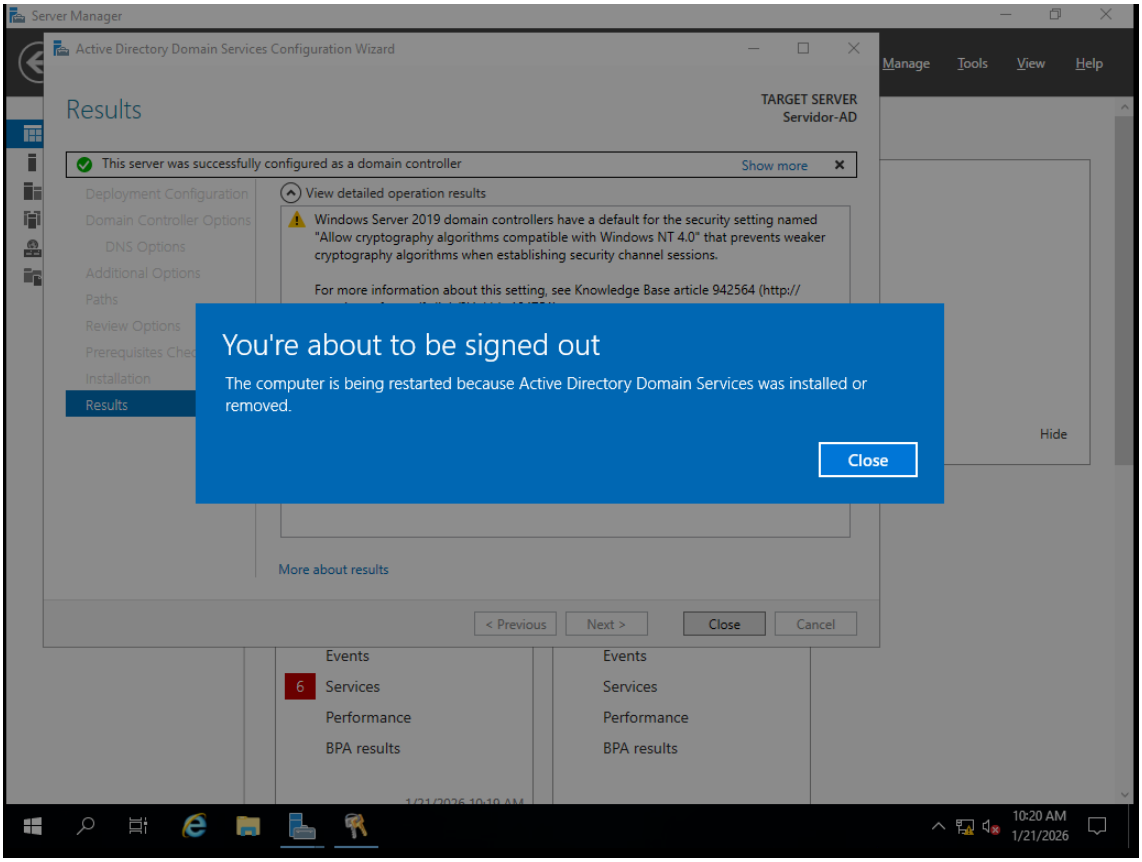
Configuração

A configuração do servidor foi feita com a implementação de IP estático para acessos externos ao servidor, implementação dos serviços Active Directory Domain Services (AD DS) e DNS e a alteração do nome do servidor para “Servidor-AD”. Após a instalação e as configurações é necessário reiniciar o servidor para que elas sejam aplicadas. É necessário agora promover o servidor a controlador de domínio para que ele possa gerenciar usuários, senhas, computadores e políticas (GPO) do AD DS. Clicando na bandeira com ícone amarelo ele vai abrir a tela de assistente de configuração e então poderemos criar uma nova floresta que iremos chamar de “**lab.local**” e iremos também definir uma senha para o Directory Service Restore Mode (DSRM) que será utilizado para reparar, restaurar ou recuperar o servidor em casos em que ele estiver corrompido e/ou inacessível. Após encerrar o processo basta clicar em seguinte e instalar e aguardar ele mesmo reiniciar o servidor.


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGI
QUICK START
WHAT'S NEW
LEARN MORE
1 C
2
3
4
5 Connect this server to cloud services
Hide
Post-deployment Configura...
TASKS
Configuration required for Active Directory Domain Services at WIN-NSAGGU7IBR1
Promote this server to a domain controller
Feature installation
Installation succeeded on WIN-NSAGGU7IBR1.
Add Roles and Features
Task Details
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS 1
Manageability
Events
Services
Performance
BPA results
7:52 AM
1/21/2026


Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
Servidor-AD
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
lab.local
More about deployment configurations
< Previous
Next >
Install
Cancel

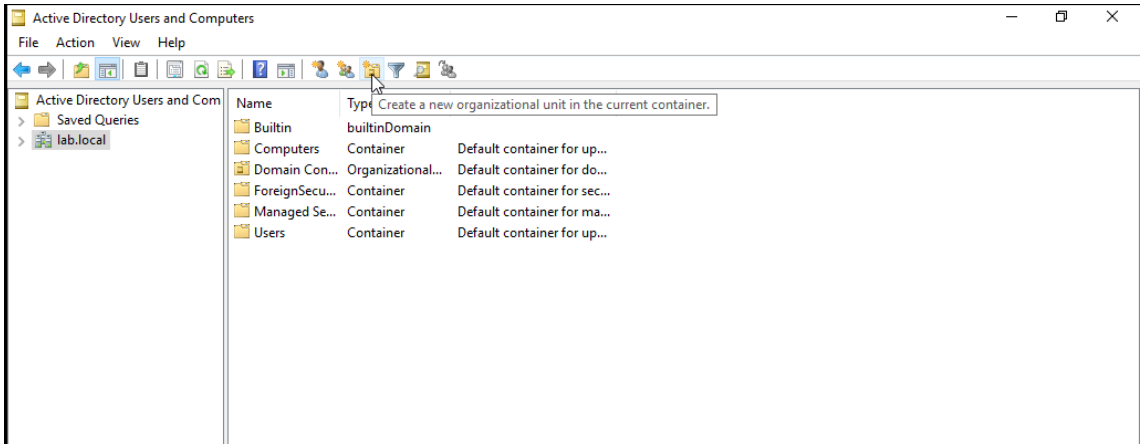

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
Servidor-AD
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel

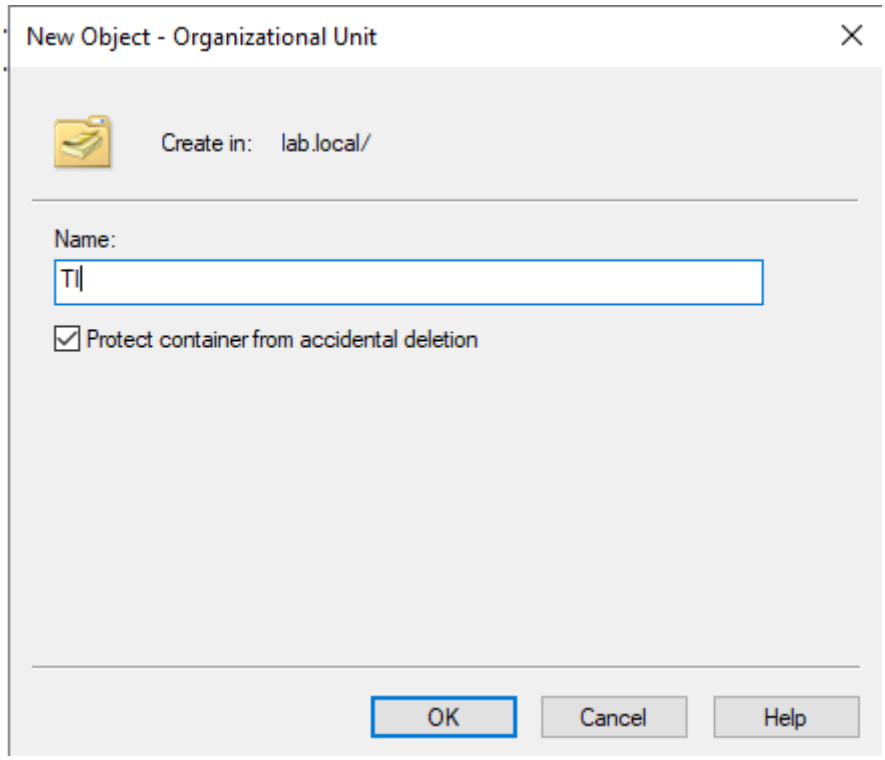

Server Manager
Active Directory Domain Services Configuration Wizard
Results
TARGET SERVER
Servidor-AD
This server was successfully configured as a domain controller
Show more
View detailed operation results
Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://
You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close
More about results
< Previous
Next >
Close
Cancel
Events
Services
Performance
BPA results
Manage
Tools
View
Help
Hide
10:20 AM
1/21/2026

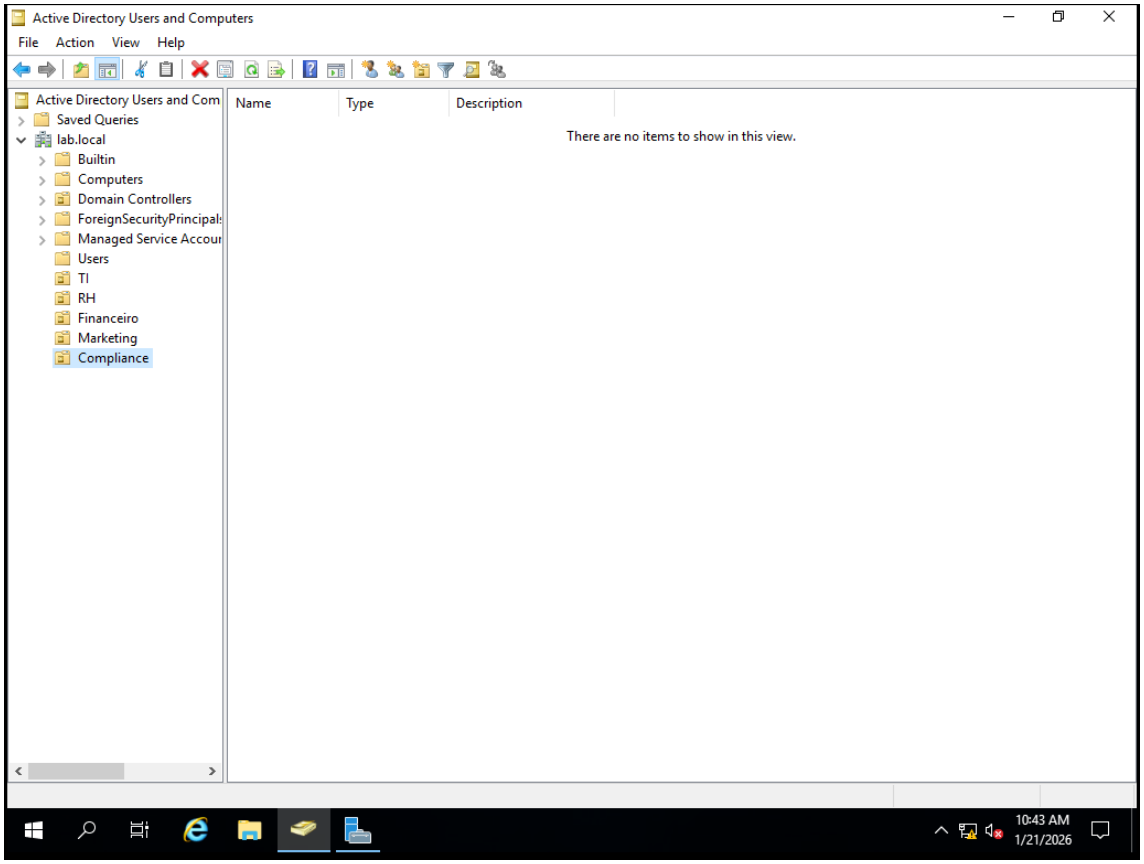
Gestão de Identidade e Acesso (IAM)

Criando Unidades Organizacionais (OUs)

A próxima etapa é a criação das unidades organizacionais que são responsáveis por agrupar os usuários e organizá-los em setores como RH, Marketing, Financeiro, TI e outros, permitindo o controle administrativo e a criação das GPOs que serão feitas mais a frente. Para começar o processo, pesquise no menu iniciar “Active Directory Users and Computers” e para facilitar sua localização futuramente anexe a barra de tarefas. Após abrir o AD podemos ver que temos nosso domínio que chamamos de **“lab.local”** e agora iremos criar nossa primeira OU selecionando primeiro o nosso domínio e em seguida a opção na barra superior “Criar um novo grupo organizacional no container atual” e iremos criar as Unidades Organizacionais das equipes de TI, Financeiro, RH, Marketing, Compliance e Ex-funcionarios e deixaremos marcada a opção de “Protect container from acidental deletion” para evitar que algum usuário com permissão exclua por equivoco a unidade organizacional. Podemos verificar as nossas OUs criadas na barra lateral esquerda, dentro do domínio **“lab.local”**.

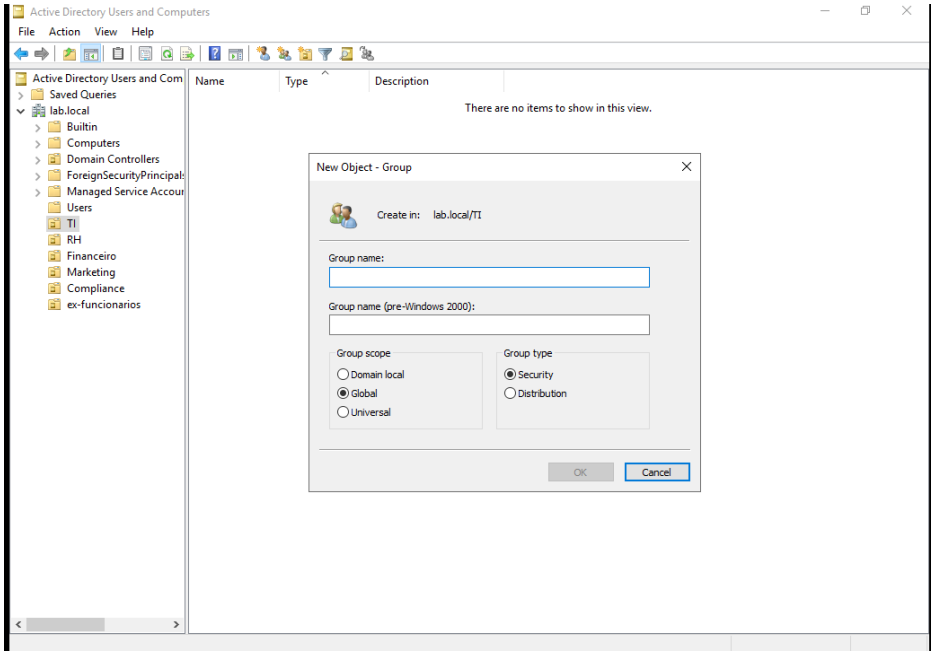


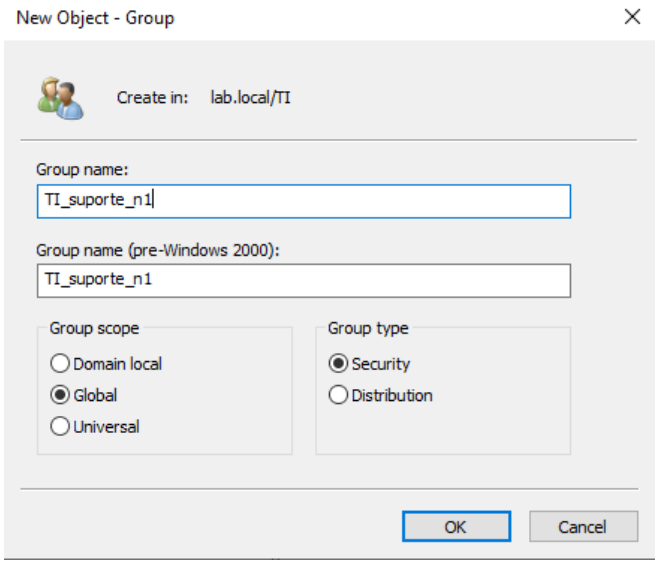

New Object - Organizational Unit
Create in: lab.local/
Name:
TI
Protect container from accidental deletion
OK
Cancel
Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
lab.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
TI
RH
Financeiro
Marketing
Compliance
Name
Type
Description
There are no items to show in this view.
10:43 AM
1/21/2026

Criando Grupos de Segurança

Após a criação das OUs devemos criar os grupos de segurança antes dos usuários, criando dessa o gerenciamento de acesso aos recursos, pastas, sites do SharePoint, aplicativos e dispositivos, com finalidade de simplificar a administração dos usuários. Iremos clicar dentro da unidade organizacional criada, selecionar a opção na barra superior **“Criar um novo grupo no container atual”** e então iremos nomear o grupo, manter ele no escopo “Global” para organizarem os usuários pelo departamento e sua função (ex: bruno é estagiário de TI e pertence ao grupo “TI_suporte_n1”) aplicando dessa forma o princípio de menor privilégio e manteremos a opção “Security”. Finalizando o cadastro dos grupos iremos para o cadastro dos usuários.





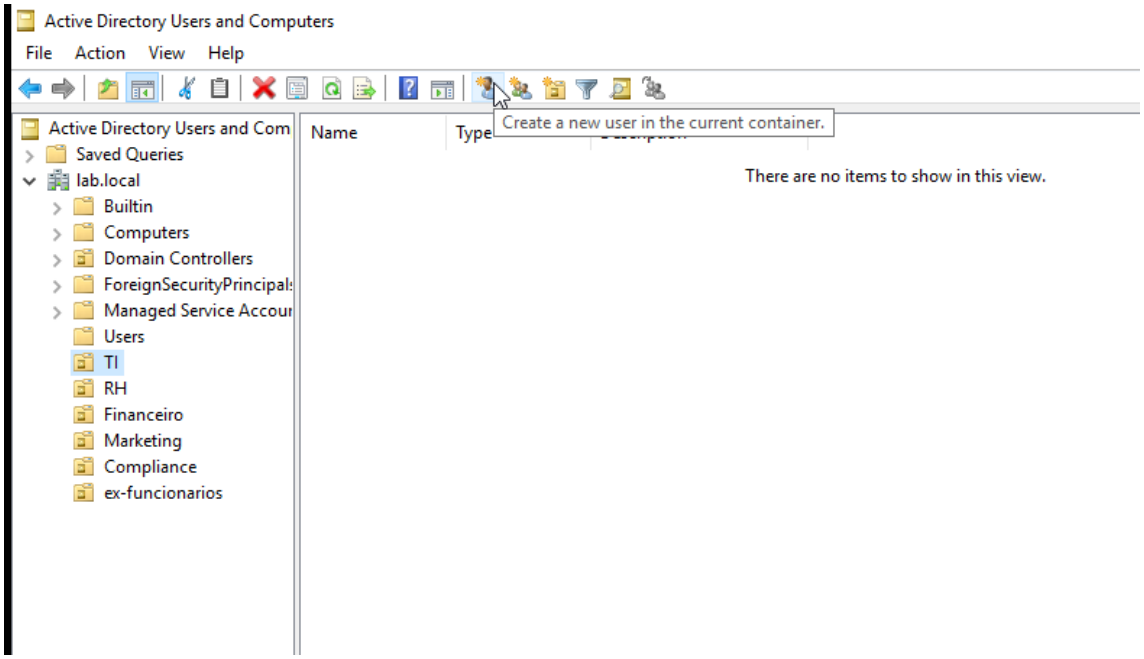
Onboarding dos Usuários

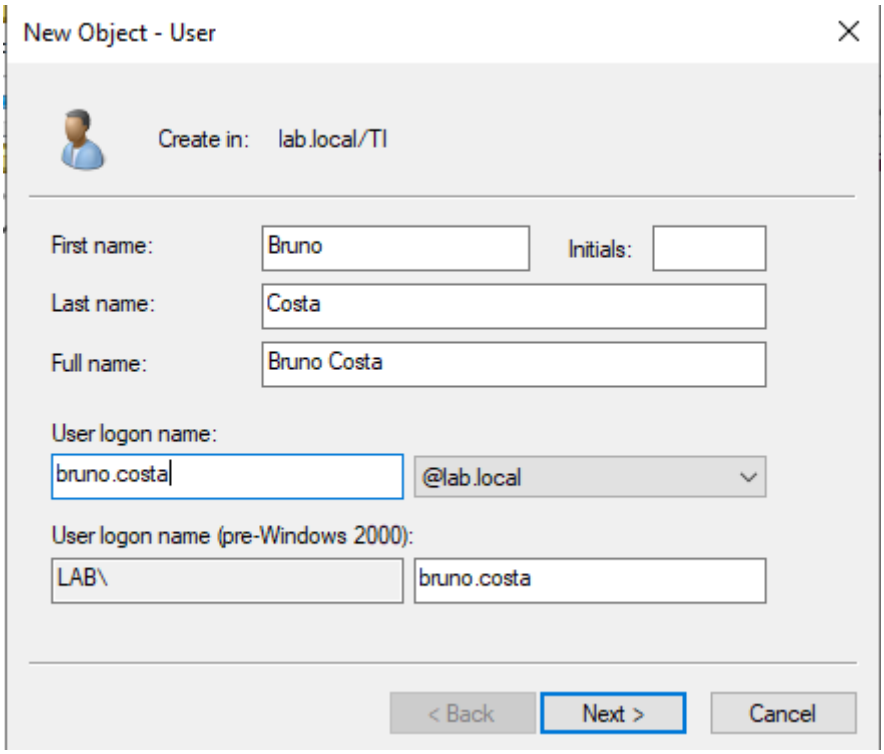
Para criar os primeiros usuários, iremos utilizar uma planilha fornecida pela nossa equipe fictícia de RH que forneceram os seguintes usuários a serem cadastrados:

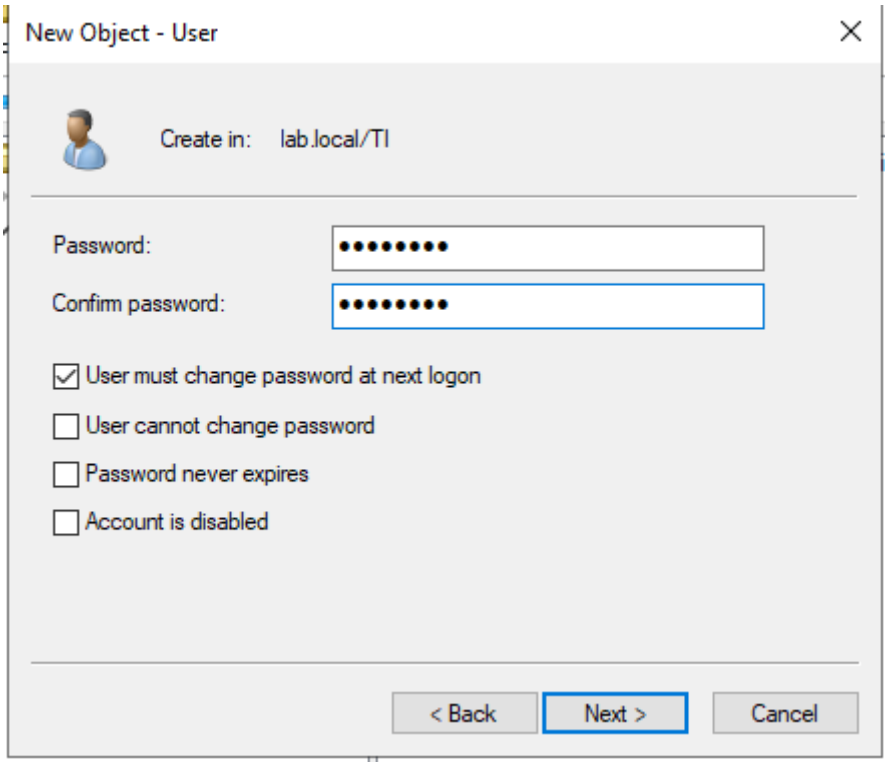
Nome	Cargo	Departamento	Sistemas Acessados	Data Admissão
Ana Silva	Analista Financeiro	Financeiro	ERP, BI, Pastas_Financeiro	16/05/2024
Bruno Costa	Estagiário TI	TI	AD, Servidores, Pastas_TI, ERP	01/06/2024
Carla Mendes	Gerente RH	RH	ERP, Pastas_RH, BI	04/12/2025
Juan Chavez	Analista de Marketing	Marketing	CRM, Pastas_MKT	10/11/2025
Elisa Rocha	Analista de Riscos	Compliance	ERP, BI, Pastas_Compliance, AD	04/04/2025

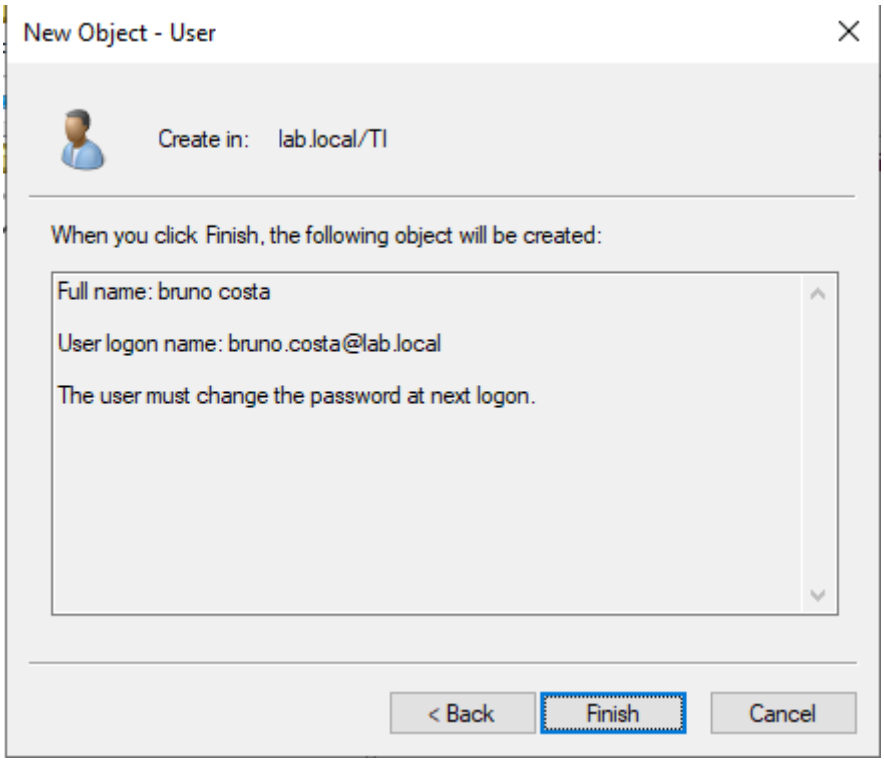
Para criar os usuários, devemos clicar na OU que ele pertence e em seguida na barra superior de ações na opção **“Criar um novo usuário no container atual”** e inserir os dados do usuário como **Nome e sobrenome, login do usuário, senha padrão e selecionar a opção “Usuário deverá alterar sua senha no próximo login”** para que o usuário selecione uma senha nova que não seja a padrão de criação. Iremos repetir o processo para os demais usuários na planilha fornecida pela equipe de RH.

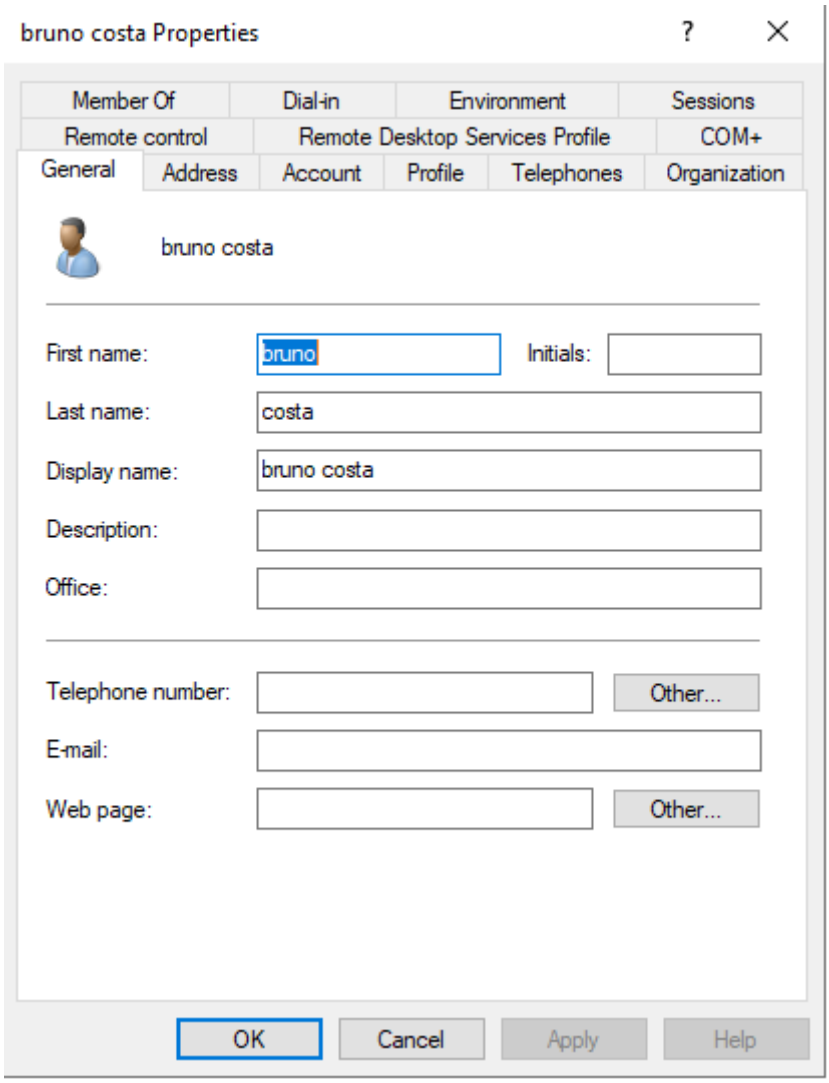
Quando finalizarmos o cadastro dos usuários, devemos atribuir a eles o seu grupo definindo quais recursos terão acesso, para isso devemos clicar duas vezes no usuário para abrir a tela de propriedades do usuário, selecionar **“Member of”** e em seguida **“Add”** para adicionarmos ao grupo **“TI_suporte_n1”.** Para localizar um grupo específico digite o início do nome do mesmo que ele vai autopreencher. Clique em “Ok” para fechar a tela e para finalizar **“Apply” e “Ok”.**

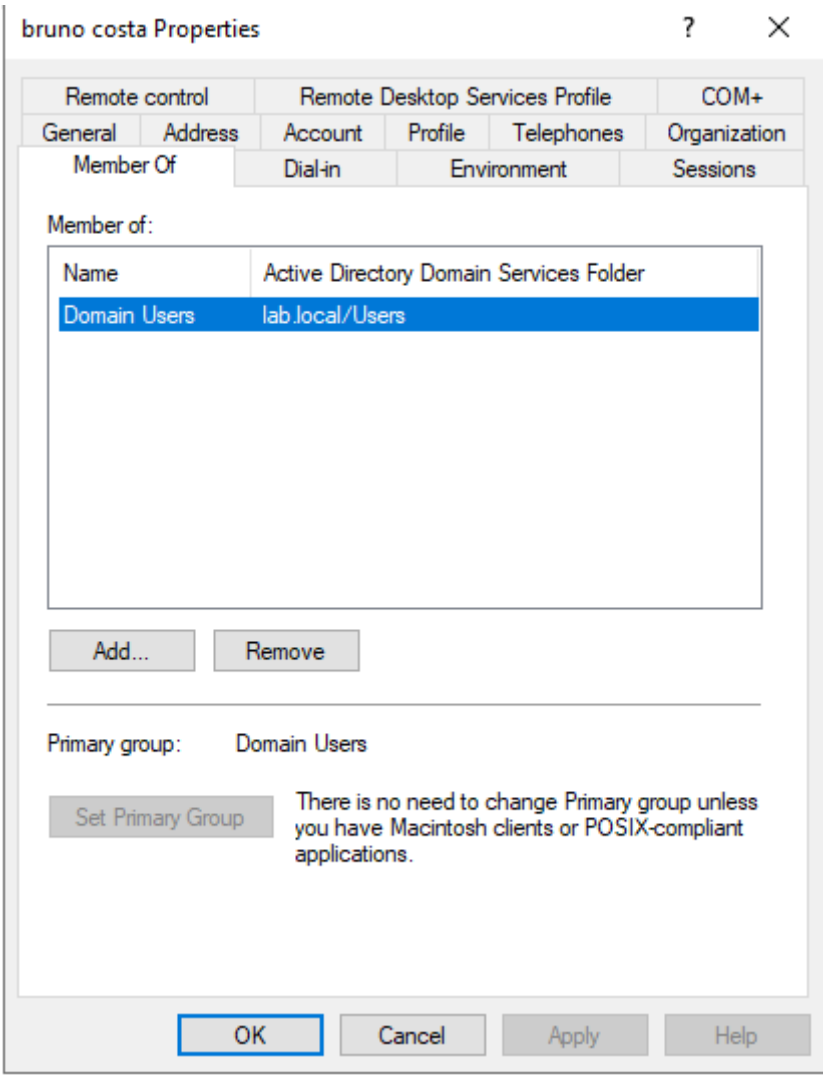


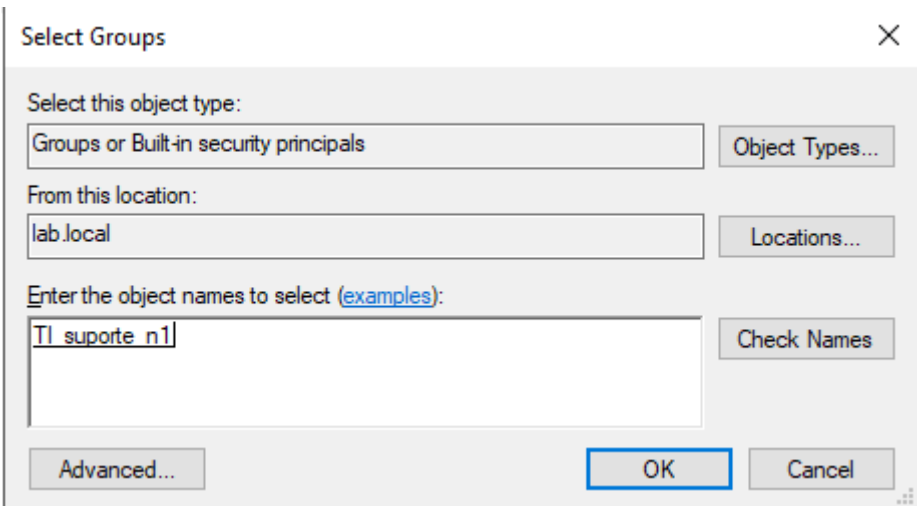

New Object - User
Create in: lab.local/TI
First name:
Bruno
Initials:
Last name:
Costa
Full name:
Bruno Costa
User logon name:
bruno.costa
@lab.local
User logon name (pre-Windows 2000):
LAB\
bruno.costa
< Back
Next >
Cancel


New Object - User
Create in: lab.local/TI
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel


New Object - User
Create in: lab.local/TI
When you click Finish, the following object will be created:
Full name: bruno costa
User logon name: bruno.costa@lab.local
The user must change the password at next logon.
< Back
Finish
Cancel


bruno costa Properties
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
bruno costa
First name:
bruno
Initials:
Last name:
costa
Display name:
bruno costa
Description:
Office:
Telephone number:
Other...
E-mail:
Web page:
Other...
OK
Cancel
Apply
Help


bruno costa Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
lab.local/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

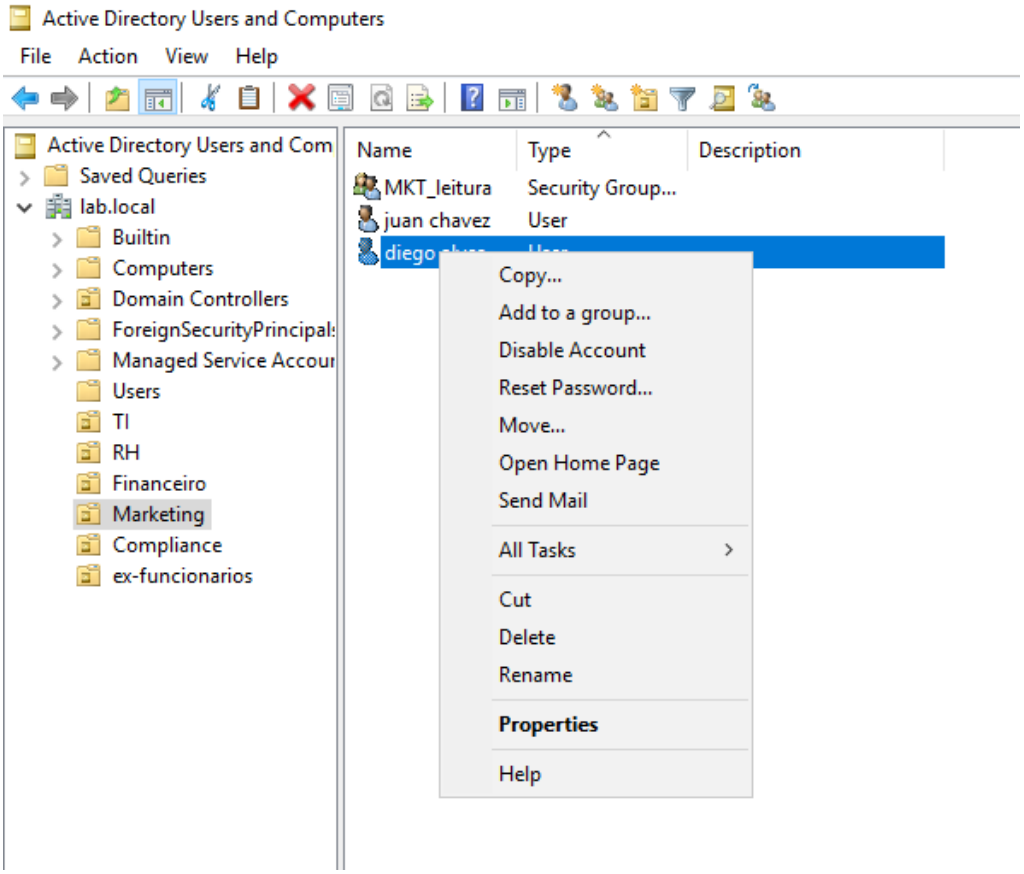

Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
lab.local
Locations...
Enter the object names to select (examples):
TI_suporte_n1
Check Names
Advanced...
OK
Cancel

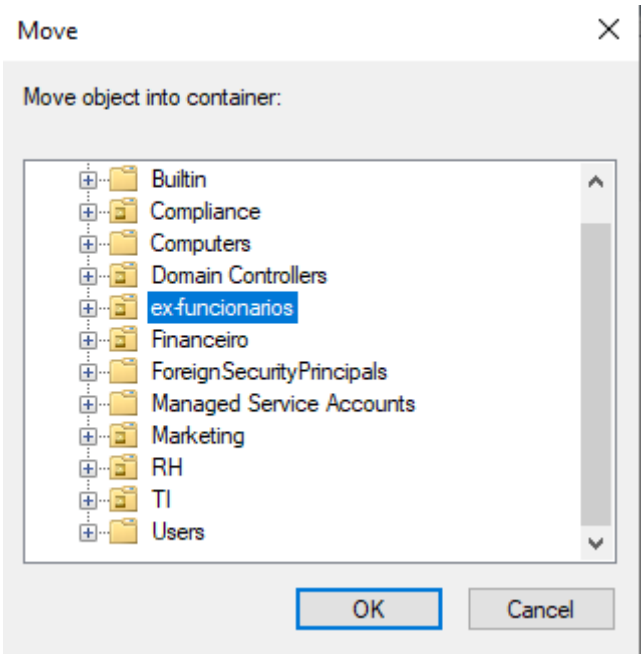
Offboarding dos usuários

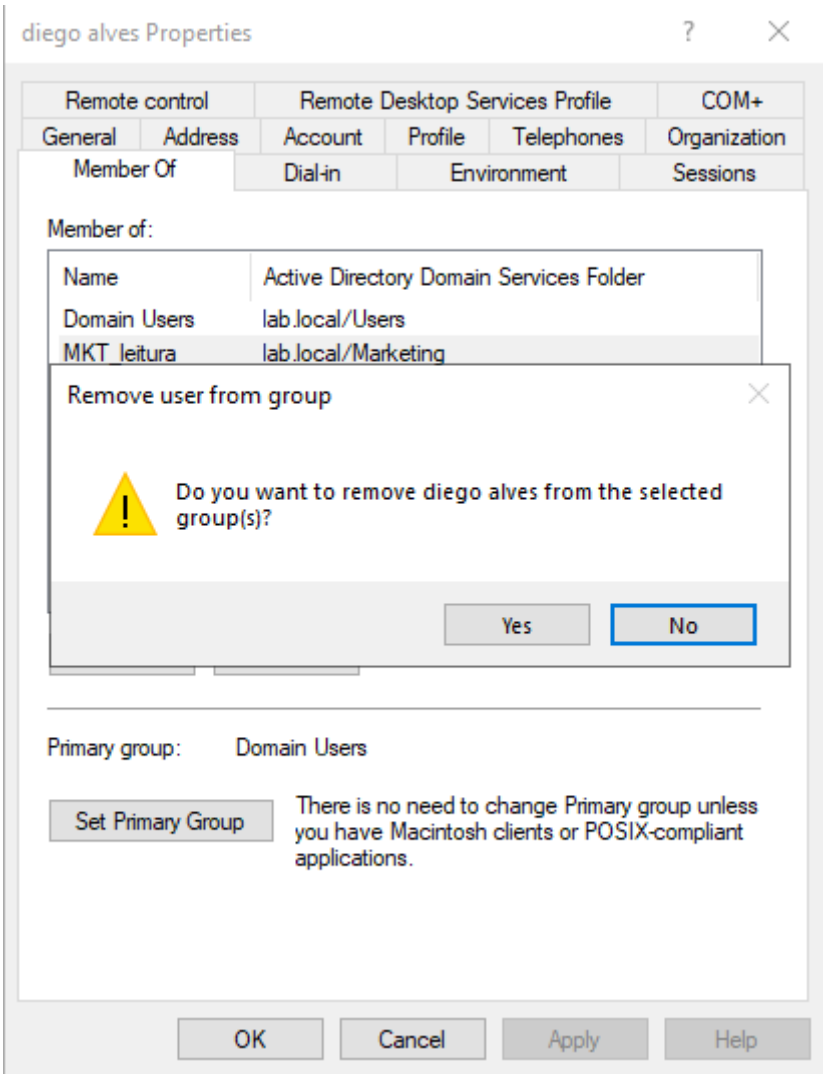
Quando um usuário é desligado é necessário que ele tenha o bloqueio dos acessos e sua conta seja desativada no ato do desligamento do usuário. Nossa equipe de RH enviou a planilha com os desligamentos a serem efetivados e iremos seguir de acordo apresentado abaixo:

Nome	Cargo	Departamento	Sistemas Acessados	Data Admissão	Data Desligamento
Diego Alves	Analista de Marketing	Marketing	CRM, Pastas_MKT	10/11/2025	21/01/2026

Para realizar o desligamento, iremos primeiro desativar a conta do usuário clicando com o botão direito do mouse e selecionando **“Disable Account”** e iremos receber a notificação que a conta dele foi desativada. Agora devemos movimentar o usuário para a OU “**ex-funcionarios”** clicando com o botão direito e selecionando a opção **“move”** e selecionando a unidade organizacional. Após movimentar o usuário para a unidade organizacional **“ex-funcionarios”** para manter o registro de no mínimo 30 dias conforme a LGPD iremos remover o usuário do grupo que ele pertencia (**MKT_leitura)** para finalizar o processo de offboarding, para isso iremos abrir as propriedades do usuário, selecionar a aba **“Member of”** e em seguida selecionar o grupo e clicar em **“remove”** e clicar em **“Yes”**, finalize clicando em **“apply” e “ok”**.




Move
Move object into container:
Builtin
Compliance
Computers
Domain Controllers
ex-funcionarios
Financeiro
ForeignSecurityPrincipals
Managed Service Accounts
Marketing
RH
TI
Users
OK
Cancel


diego alves Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
lab.local/Users
MKT_leitura
lab.local/Marketing
Remove user from group
Do you want to remove diego alves from the selected group(s)?
Yes
No
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help