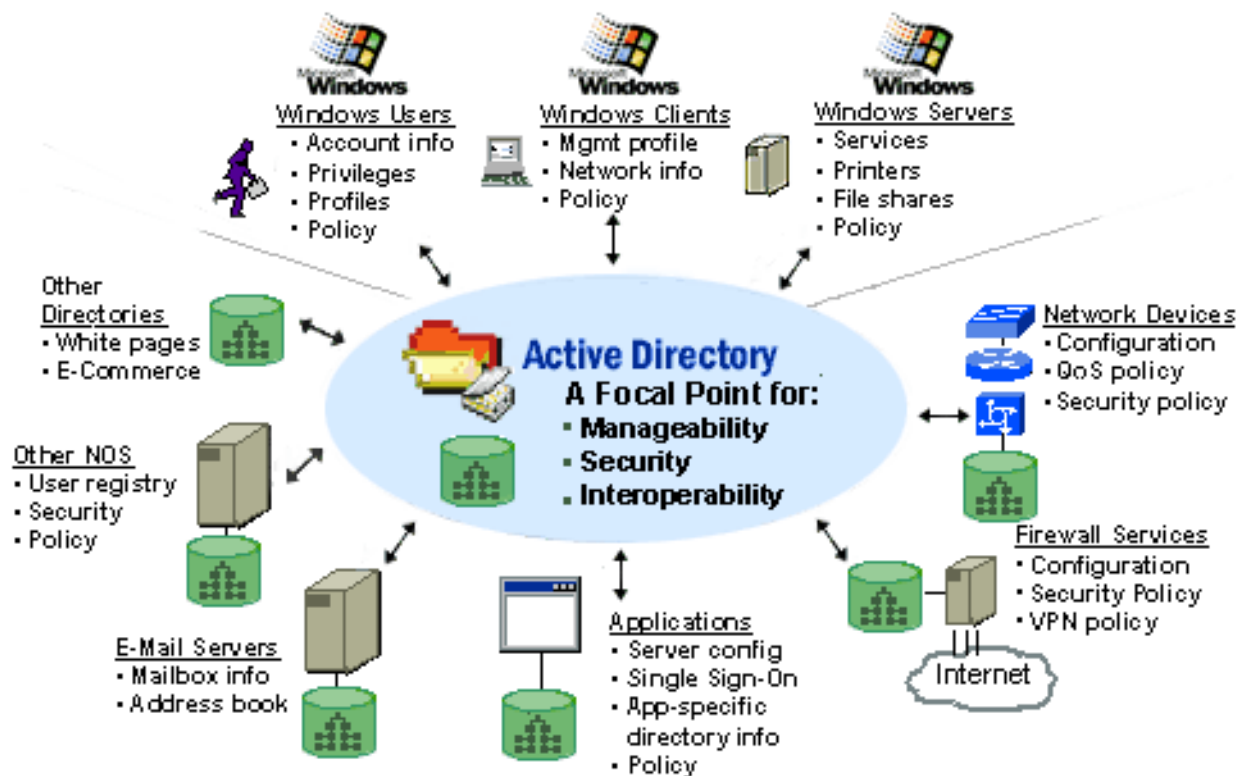


# Active Directory



# Evolution of the Microsoft NOS

- ***Network operating system, or “NOS,”*** is the term used to describe a networked environment in which various types of resources, such as **user, group, and computer accounts, are stored in a central repository that is controlled by administrators** and accessible to end users. Typically, a NOS environment is comprised of **one or more servers** that provide **NOS services**, such as authentication, authorization, and account manipulation, and multiple end users that access those services.
- Microsoft’s first integrated NOS environment became available in 1990 with the release of Windows NT 3.0, which combined many features of the LAN Manager protocols and of the OS/2 operating system. The NT NOS slowly evolved over the next eight years until **Active Directory was first released in beta form in 1997.**

# Evolution of the Microsoft NOS

- Under Windows NT, the **“domain” concept was introduced, providing a way to group resources** based on administrative and security boundaries. NT domains were flat structures limited to about **40,000 objects (users, groups, and computers)**. For large organizations, this limitation imposed superficial boundaries on the design of the domain structure. Often, domains were geographically limited as well because the **replication** of data between domain controllers (i.e., servers providing the NOS services to end users) performed poorly over high-latency or low-bandwidth links. **Another significant problem with the NT NOS was delegation of administration**, which typically tended to be an all-or-nothing matter at the domain level.
- Microsoft was well aware of these limitations and the need to rearchitect its NOS model into something that would be much more scalable and flexible. It looked to **LDAP-based directory services as a possible solution**.

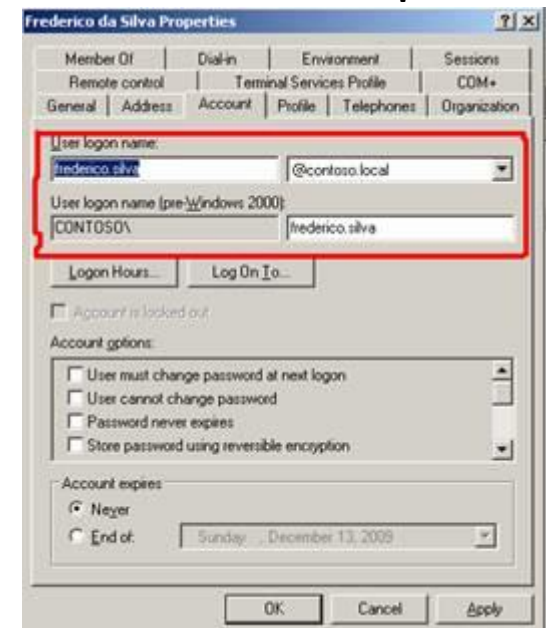
# O que é um serviço de diretório?

- Em nossa agenda podemos organizar, dias, semanas, meses e até anos, passando por pessoas, nomes, sobrenomes, datas de aniversário, dados importantes dentre outros.
- O **serviço de diretório** tem exatamente o mesmo sentido, o sentido de **organizar** e **principalmente ter um local centralizado para a busca de informações necessárias no dia a dia, para nossos trabalhos.**



# O que é um serviço de diretório?

- Quando criamos um novo usuário, estamos utilizando o **serviço de diretório**, nesta base de dados (agenda), estamos guardando, nomes, sobrenomes, endereços, logins, senhas, grupos, ao qual o usuário pertence dentre outras tantas opções que podemos cadastrar, tudo isto ficará disponível dentro de uma base de dados, que poderá ser utilizada pelos nossos servidores.



# Soluções de serviço de diretório



Novell  
eDirectory

The logo for Novell eDirectory features the word "Novell" in a large, bold, orange sans-serif font. Below it, the word "eDirectory" is written in a smaller, orange sans-serif font. The text is positioned to the left of a large, solid blue triangle that points downwards.

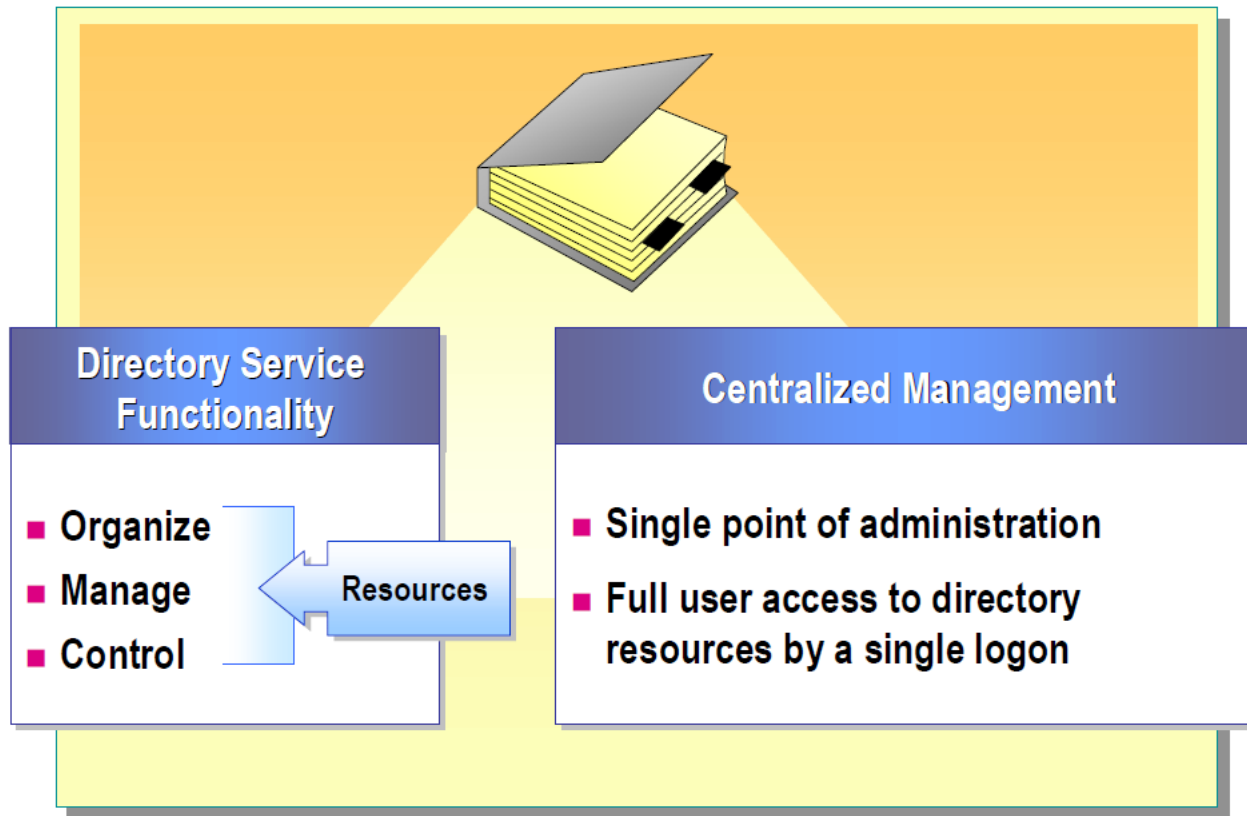
Active Directory



# Por que usar o Active Directory?

- O Active Directory assumiu o mercado de serviços de diretório pelo seu **desempenho, segurança e principalmente disponibilidade**, o Active Directory esta no mercado desde o lançamento do **Windows 2000 Server**, após o seu nascimento assumiu a liderança dos serviços de diretório, utilizando como base o LDAP e a comunicação através de replicação lançou vários atributos e principalmente ferramentas para facilitar o gerenciamento de informações nas empresas.
- **Hoje quando usamos um usuário para logar no domínio de nossa empresa, estamos utilizando um serviço de diretório** e por consequência usando o Active Directory.

# Active Directory

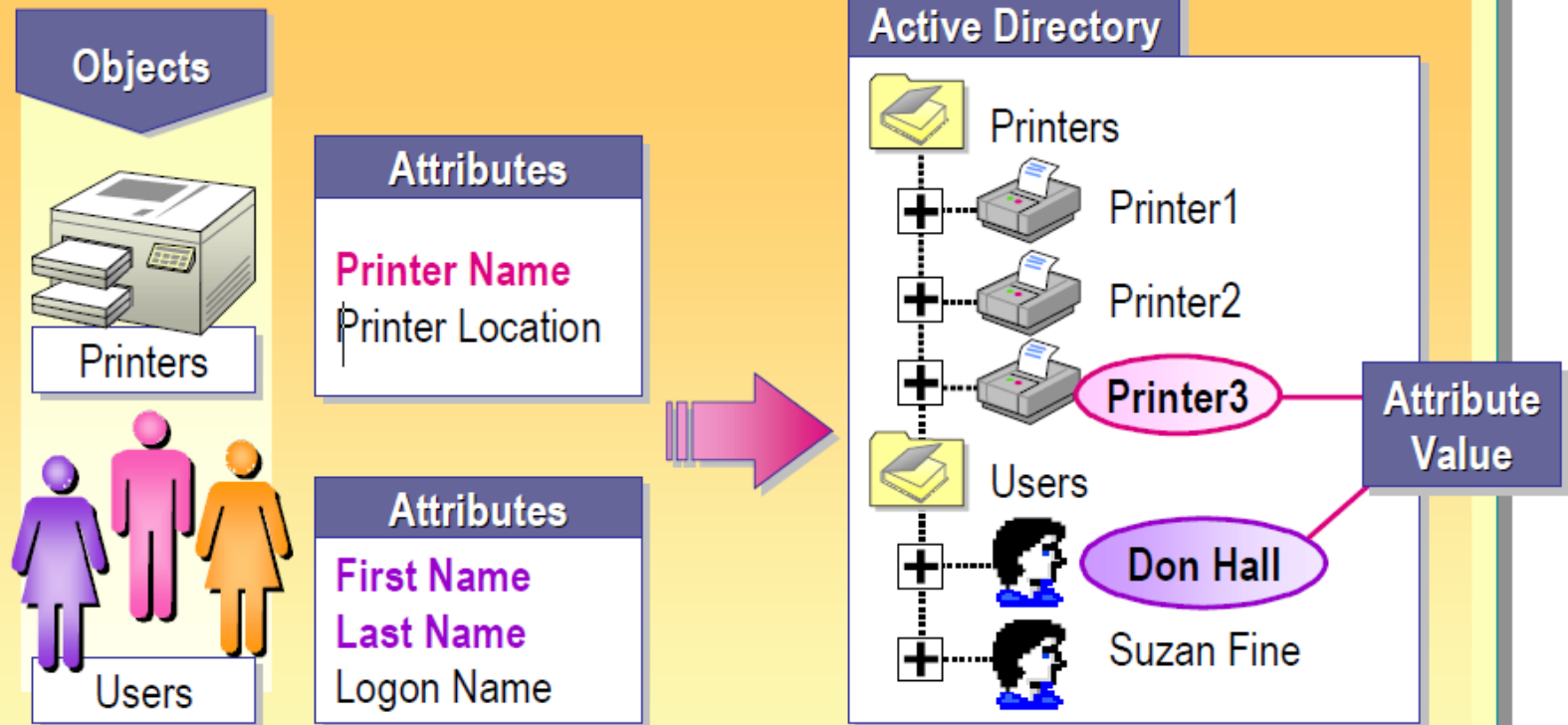




# Active Directory

- O Active Directory é uma **implementação de serviço de diretório** no protocolo LDAP que **armazena informações sobre objetos em rede de computadores** e disponibiliza essas informações a usuários e administradores.
- Usando a função de servidor dos Serviços de Domínio Active Directory® (AD DS), você pode criar uma infraestrutura **escalável, segura e gerenciável para gerenciamento de usuário e recursos** e pode fornecer suporte para aplicativos habilitados por diretório, como o Microsoft® Exchange Server.
- O AD DS fornece um **banco de dados distribuído** que armazena e gerencia informações sobre recursos da rede e dados específicos de aplicativos habilitados por diretório.

# Objetos no Active Directory



- Objects Represent Network Resources
- Attributes Store Information About an Object

# Componentes do AD

AD DS is composed of both logical and physical components

Logical components	Physical components
<ul style="list-style-type: none"><li>• Partitions</li><li>• Schema</li><li>• Domains</li><li>• Domain trees</li><li>• Forests</li><li>• Sites</li><li>• OUs</li><li>• Containers</li></ul>	<ul style="list-style-type: none"><li>• Domain controllers</li><li>• Data stores</li><li>• Global catalog servers</li><li>• RODCs</li></ul>

# Domain



- O Domínio é a unidade básica da estrutura lógica do AD.

- Um domínio pode armazenar milhões de objetos.
- É uma unidade de segurança, que define os direitos administrativos sobre um grupo de recursos.

# The AD DS Domain Contains User, Computers, Groups

- An AD DS domain is a logical container used to manage user, computer, group, and other objects.
- All of the domain objects are stored in the AD DS database, a copy of which is stored on each domain controller.
- **There are many types of objects in the AD DS database**, including user accounts, computer accounts, and groups. The following list briefly describes these three object types:
  - **User accounts.** User accounts contain the information required to authenticate a user during the sign-in process and build the user's access token.
  - **Computer accounts.** Each domain-joined computer has an account in AD DS. Computer accounts are used for domain-joined computers in the same ways that user accounts are used for users.
  - **Groups.** Groups are used to organize users or computers to make it easier to manage permissions and group policy in the domain.

# The AD DS Domain Provides Authentication

- Whenever a domain-joined computer starts, or a user signs in to a domain-joined computer, AD DS authenticates them.
- Authentication verifies that the computer or user has the proper credentials for an AD DS account.

# **The AD DS Domain Provides Authorization**

- Windows operating systems use authorization and access control technologies to allow authenticated users to access resources.

# Active Directory Concepts

- [Active Directory Concepts.mp4](#)
- <https://www.youtube.com/watch?v=3sFzqCr85Ks>



# Banco de Dados do AD

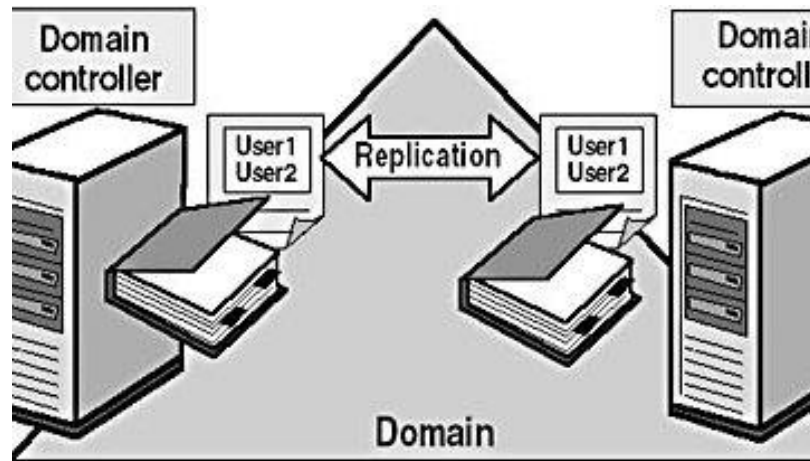
- **O AD fisicamente tem um banco de dados**, este banco é conhecido com **NTDS.dit** e está localizado na pasta %SystemRoot%\NTDS\ntds.dit em uma instalação default do AD.
- **Este diretório chamado de NTDS apenas existirá nos servidores que tenham a função de Domain Controllers (DC's).**
- Neste diretório existirão os arquivos relacionados abaixo:
  - **Ntds.dit** - Arquivo de banco de dados do AD
  - **Edb.log** - Arquivo onde são armazenados todas as transações feitas no AD.
  - **Edb.chk** - Arquivo de checkpoint controla transações no arquivo Edb.log já foram comitadas no arquivo Ntds.dit.
  - **Res1.log** - Arquivo de reserva assegura que alterações sejam gravadas na base(Ntds.dit) no caso de falta de espaço em disco.
  - **Res2.log** - Arquivo de reserva assegura que alterações sejam gravadas na base(Ntds.dit) no caso de falta de espaço em disco.

# Domain Controller



- O AD DS (Serviços de Domínio do Active Directory) armazena dados do diretório e gerencia a comunicação entre usuários e domínios, incluindo os processos de logon do usuário, a autenticação e as pesquisas em diretório.
- **Um controlador de domínio Active Directory é um servidor executando o AD DS.**

- Estrutura lógica do AD é gravada em uma base de dados física chamada de Ntds.dit.



- Cada servidor quando recebe a função de **Domain Controller**, herda a criação do diretório %SystemRoot%\NTDS\ e toda a sua estrutura.
- Todos os dados criados originalmente são replicados para o novo DC criado.

# What is a Windows Domain Controller?

- [What is a Windows Domain Controller.mp4](#)
- [https://www.youtube.com/watch?v=cTe5GsyhKUK](#)



# Requisitos para executar os Serviços de Domínio Active Directory

Requisito	Descrição
TCP/IP	Configure os endereços de servidor TCP/IP e DNS adequados.
NTFS	As unidades que armazenam o banco de dados, os arquivos de log e a pasta SYSVOL para Serviços de Domínio Active Directory (AD DS) devem ser colocadas em um volume fixo local. SYSVOL deve ser colocado em um volume formatado com o sistema de arquivos NTFS. Para fins de segurança, o banco de dados e os arquivos de log do Active Directory devem ser colocados em um volume que seja formatado com o NTFS.
Credenciais	Para instalar uma nova floresta do AD DS, é necessário ser Administrador local no servidor. Para instalar um controlador de domínio adicional em um domínio existente, você precisa ser um membro do grupo Administradores de Domínio.
Infraestrutura do DNS (Sistema de Nomes de Domínio)	<p>Verifique se uma infraestrutura do DNS está correta. Ao instalar o AD DS, você pode incluir a instalação do servidor DNS, caso seja necessária.</p> <p>Quando você cria um novo domínio, uma delegação do DNS é criada automaticamente durante o processo de instalação. A criação de uma delegação do DNS exige credenciais que tenham permissões para atualizar as zonas DNS pai.</p>

# INSTALANDO O ACTIVE DIRECTORY NO WINDOWS SERVER 2016

- [Instalação AD Windows 2012-2016c.pdf](#)

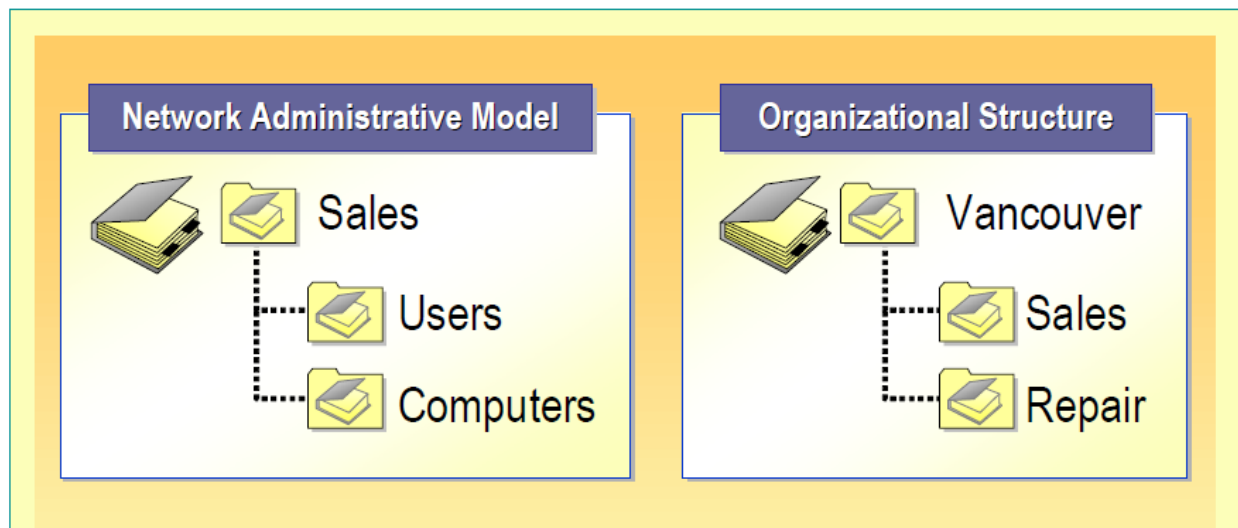
# Windows Server 2016 How to install an Active Directory Domain Controller

- [Windows Server 2016 How to install an Active Directory Domain Controller.mp4](#)
- <https://www.youtube.com/watch?v=VkcoX8v4IQ>



# Organizational Units

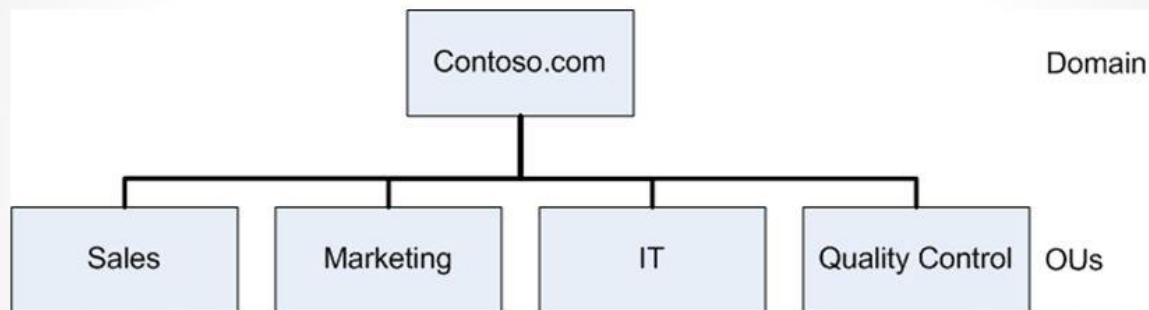
- Os domínios podem ser divididos em OU(Unidades Organizacionais).
- Estas são utilizadas como containers, para organizar objetos dentro de um domínio em grupos administrativos lógicos que refletem de alguma forma a estrutura organizacional ou estrutura de negócio da organização.





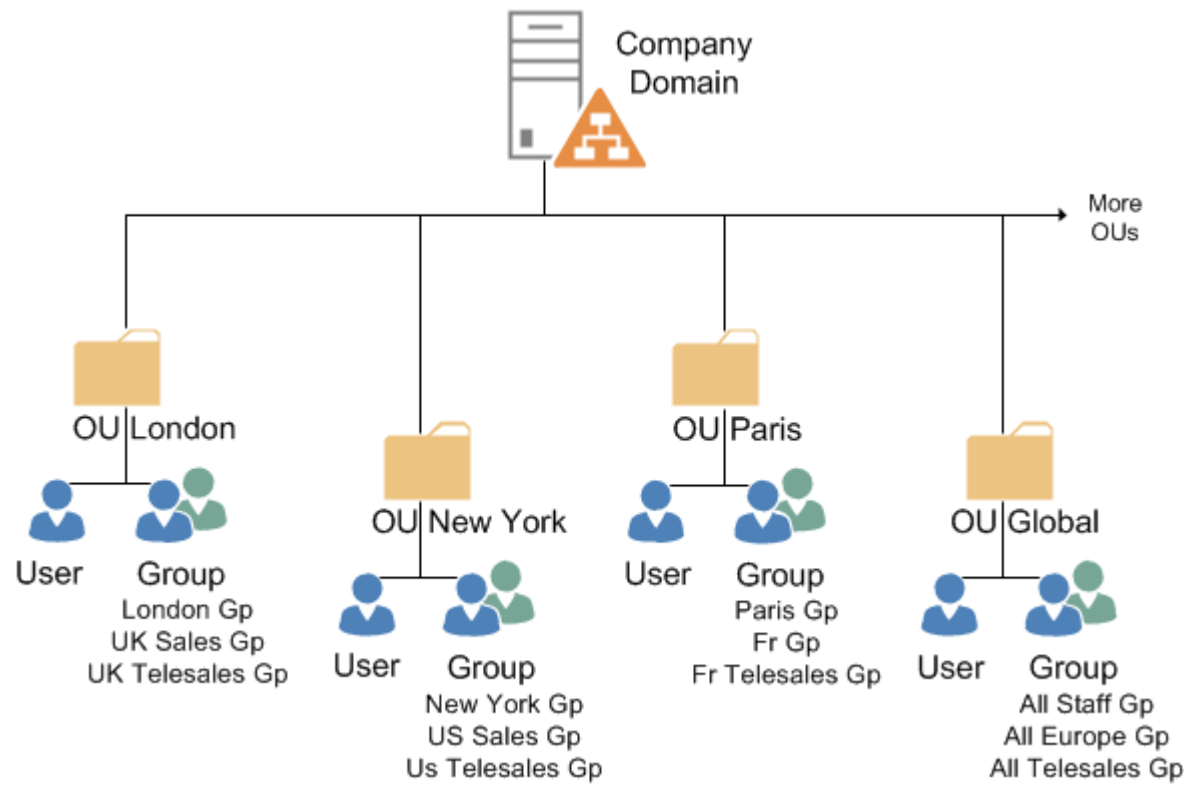
# Exemplo 1

## Organizational Units



Organizational units subordinate to a domain

# Exemplo 2



# Atividade

**Nome:**

**Turma:**

**Data:**   /   /