

SERVIDORES E SERVIÇOS DE INTERCONECTIVIDADE WINDOWS

UNIDADE 2 – INSTALANDO O ACTIVE DIRECTORY, CRIANDO USUÁRIOS, GRUPOS E UNIDADES ORGANIZACIONAIS

Autor: Denilson Luís Bonatti

Revisora: Cilene Renata Real

INICIAR

Introdução

Caro estudante, um dos grandes diferenciais que fazem empresas optarem por utilizar o Windows Server como sistema operacional de seus servidores é o Active Directory. Com ele, é possível criar controles lógicos em pequenas e grandes organizações, dando mais segurança às informações, independente da estrutura física da empresa. Esses controles lógicos vão desde um simples controle de logon e senha de usuário, até o compartilhamento de informações e permissões de acesso.

Nesta unidade, aprenderemos como instalar o Active Directory e como provisionar um servidor a controlador de domínio, além de aprender como criar usuários, computadores, grupos de usuários e computadores, unidades organizacionais e delegar funções administrativas a usuários do domínio.

Bons estudos!

2.1 Instalação do AD DS

Ao instalar o Windows Server em um computador, você pode optar por configurar uma função de servidor específica para esse computador, como um servidor de arquivos, um servidor web, servidor DHCP ou outra função. Quando você deseja criar uma nova floresta de domínios ou um controlador de

domínio adicional em um domínio existente, é necessário instalar e configurar o servidor com a função de controlador de domínio, instalando o Active Directory.

O controlador de domínio é o servidor no qual o Active Directory será instalado. Sendo assim, esse servidor armazenará os objetos pertencentes ao domínio, como usuários, computadores, grupo de usuários etc. Ele também será o responsável por definir as políticas de segurança aplicadas aos usuários e computadores do domínio. Desse modo, para a instalação do Active Directory, alguns requisitos devem ser observados.

» a) Definição de um IP fixo para o servidor

Este servidor deverá ser encontrado pelas máquinas-clientes da rede local. Sendo assim, é importante que o servidor possua um endereçamento IP fixo. Endereçamentos IPs entregues por um servidor DHCP ou outro dispositivo que tenha este serviço, como roteadores, podem renovar o endereçamento IP entregue ao servidor, fazendo com que os apontamentos feitos a ele fiquem desatualizados. A configuração de um IP fixo para o servidor pode ser realizada pelo painel **Local Server**, na janela do Server Manager, no item **Ethernet**.

Para estabelecer uma conexão com um hospedeiro remoto (ou mesmo para enviar um datagrama), é necessário saber o seu endereço IP. Visto que gerenciar listas de endereços IP de 32 bits é inconveniente para as pessoas, um esquema chamado DNS (Domain Name System — serviço de nomes de domínio) foi inventado como um banco de dados que mapeia nomes de hospedeiros em ASCII em seus endereços IP (TANENBAUM, 2016, p. 398).

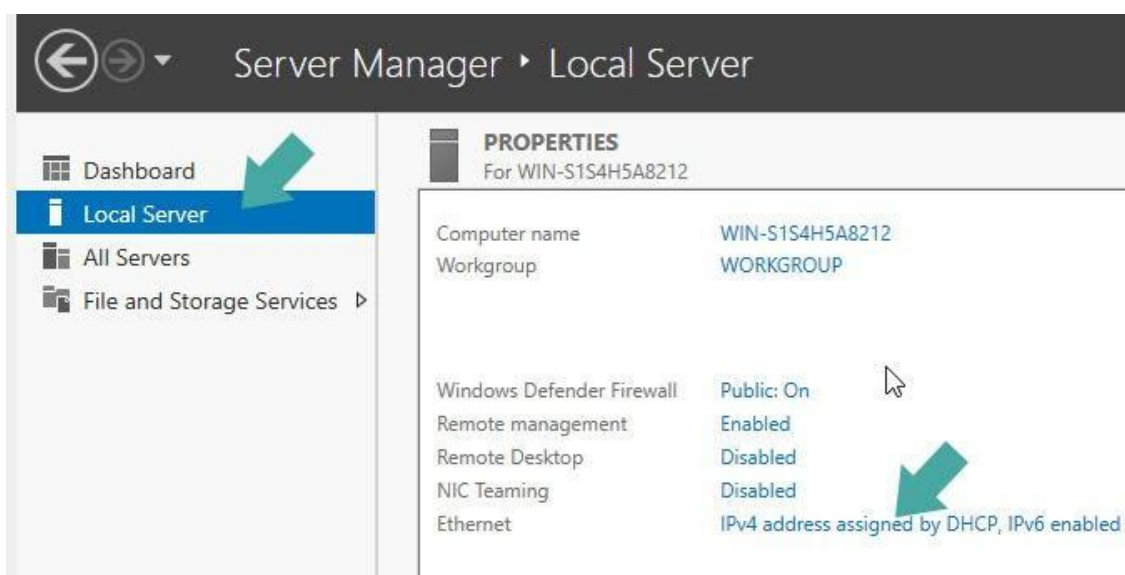


Figura 1 – Captura de tela do Local Server no Server Manager para alterar as configurações de IP.

Um servidor pode conter mais de um dispositivo de rede e o endereçamento IP pode ser realizado utilizando IPv4 ou IPv6. Neste exemplo, o servidor possui apenas um dispositivo de rede e será utilizado IPv4.



VOCÊ SABIA?

O comitê gestor de internet no Brasil (CGI) oferece uma grande quantidade de informações sobre o IPv6. Em seu site, é possível fazer cursos gratuitos e ter acesso a e-books sobre o tema. Veja algumas dessas opções no link: < <https://cursoseventos.nic.br/cursos/> >.

No exemplo mostrado na Figura 2, as máquinas pertencentes ao domínio deverão ter acesso ao endereçamento IP 192.168.100.10. Por padrão, as máquinas-clientes deverão estar endereçadas na rede 191.168.100.0.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 100 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

Figura 2 – Captura de tela de definição do IP 192.168.100.10 para o servidor.

» b) Nomear o servidor

Outra configuração importante a ser observada antes da instalação do Active Directory é o nome do servidor. Ao realizar a instalação do Windows Server 2019, o servidor recebe um nome provisório, que pode ser consultado e alterado no painel **Local Server**, na janela do **Server Manager**.

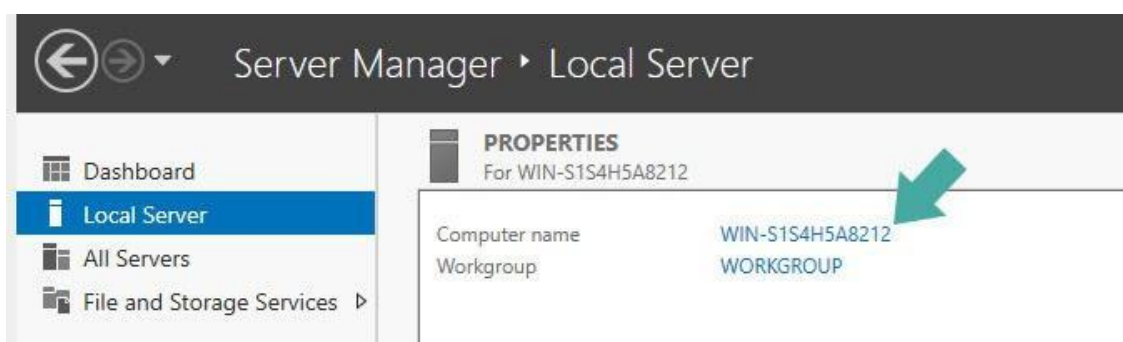


Figura 3 – Captura de tela da definição de nome provisório do servidor.

O ideal é que este servidor tenha um nome que o identifique, ou seja, um nome que possa fazer referência a sua função na rede. Neste exemplo, foi definido o nome **ServerAD-DS**, fazendo referência a sua futura função de controlador de domínio: Active Directory Domain Services.

Após a definição do nome, o servidor precisará ser reiniciado. O próximo passo é a instalação do Active

Directory. A instalação do Active Directory também pode ser realizada diretamente pelo Server Manager no painel **Dashboard** , clicando em **Add Roles and Features** .

Como é padrão em qualquer procedimento de instalação, será aberta uma janela com a descrição da função do assistente em execução. A partir da versão 2012, os assistentes de instalação e provisionamento do Active Directory se tornaram mais dinâmicos e mais fáceis de acompanhar. Conforme aconselha Thompson (2014, p. 30): “Quem está iniciando em administração de rede de servidores não deve desprezar os assistentes e as orientações do sistema operacional”.

Clicando no botão **Next** , a próxima etapa é definir o tipo de instalação. É possível instalar uma função ou recurso em um servidor ou instalar um recurso específico para um ambiente de infraestrutura virtual (Virtual Desktop Infrastructure). O Active Directory é uma função que deve ser instalada em um servidor, desta forma, a opção **Role-based or feature-based installation** deve ser selecionada. Clicando no botão **Next** , o próximo item a ser selecionado é em qual servidor esta instalação será realizada. Em um ambiente com vários servidores, é possível escolher o servidor no qual o recurso será instalado. Alguns recursos também podem ser instalados em discos virtuais pré-configurados. Neste exemplo, como temos apenas um servidor, somente ele poderá ser selecionado. Clicando em Next, o próximo passo é definir quais recursos serão instalados. Instalaremos o Active Directory, desta forma, o item **Active Directory Domain Certificate Services** deve ser selecionado.

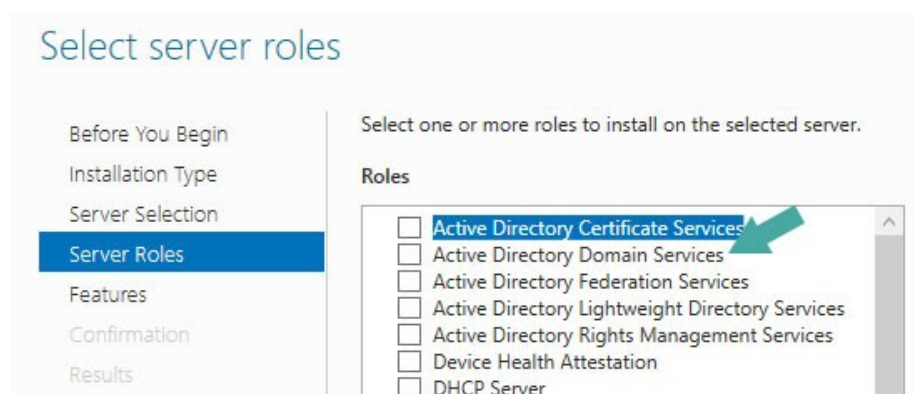


Figura 4 – Captura de tela da seleção dos recursos do Active Directory Domain Services.

Ao selecionar a função **Active Directory Domain Services** , uma nova janela será exibida, indicando os recursos adicionais que deverão ser instalados. Esses recursos, em sua maioria, são ferramentas administrativas necessárias para o gerenciamento das funções do Active Directory. Clicando em **Add Feature** , confirmamos a instalação destes recursos.

Avançando nas definições da instalação, é possível instalar um recurso adicional juntamente com o Active Directory. Alguns destes recursos já foram pré-selecionados, pois são recursos necessários para o funcionamento do Active Directory. Outros recursos poderiam ser selecionados nesta etapa, como ferramentas de backup e outras funções. Neste exemplo, somente os recursos pré-selecionados serão instalados.

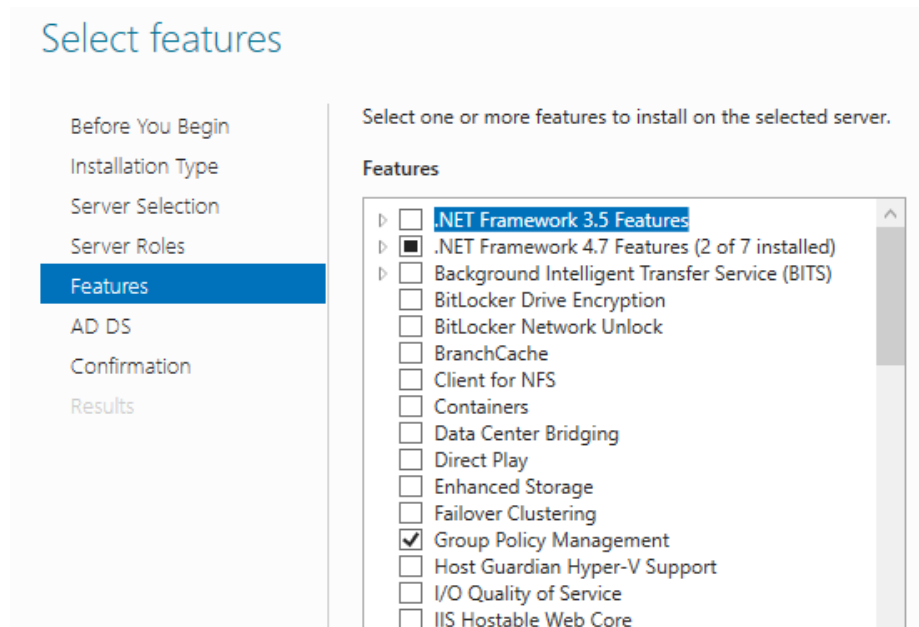


Figura 5 – Captura de tela da janela de seleção de recursos adicionais.

Clicando em **Next** para avançar a instalação, temos uma explicação do principal recurso que estamos instalando, o Active Directory. Links de outras informações relevantes são exibidos para possíveis consultas. Avançando a instalação, é apresentado um resumo de todos os recursos que serão instalados no servidor.

Clicando em **Install**, a instalação dos arquivos será iniciada.

A instalação Active Directory não implica o provisionamento deste servidor a controlador de domínio. Após a instalação do software, é necessário realizar as configurações de provisionamento. Isso pode ser feito clicando no link **Promote this server to a domain controller**.

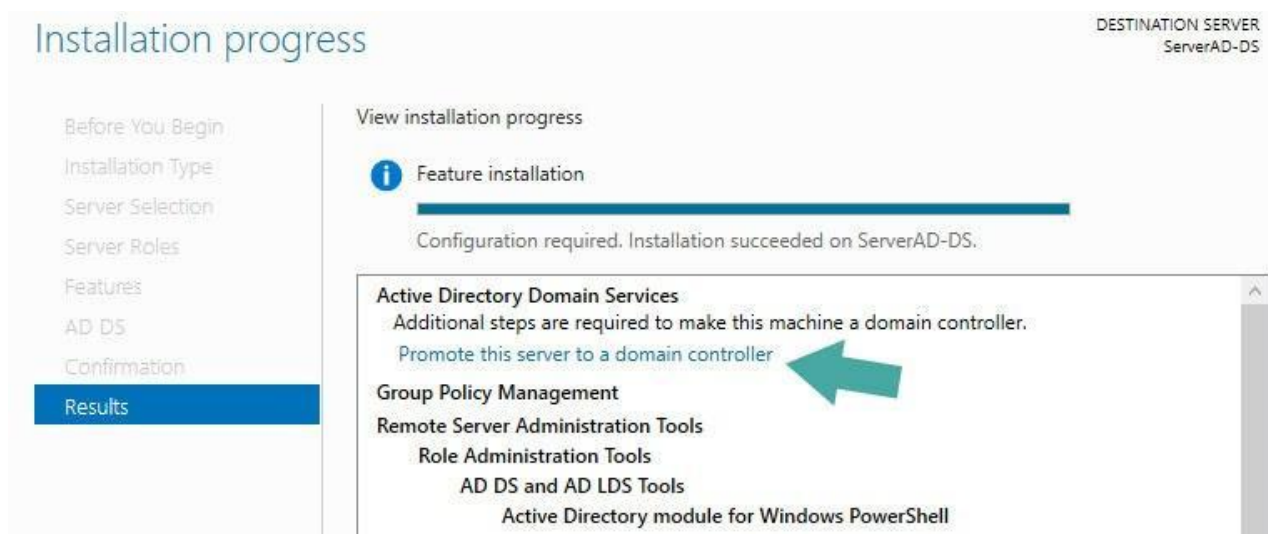


Figura 6 – Link para o provisionamento do servidor a controlador de domínio.

Feito isso, um novo assistente será exibido. Neste assistente, inicialmente devemos indicar o tipo de

implementação que será realizada. Algumas perguntas podem ser feitas para a seleção correta:

Já existe uma floresta criada, ou é necessário criar uma nova floresta de domínios?

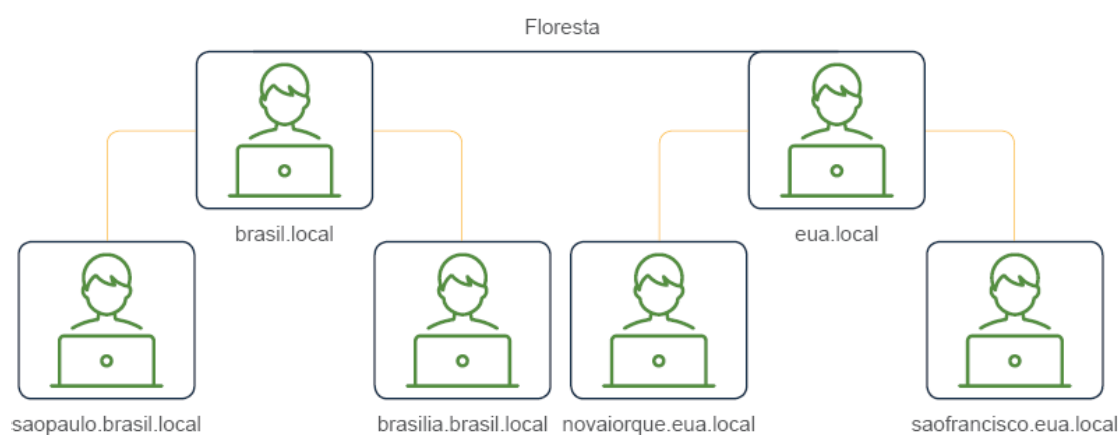
Se já existe uma floresta, será criado um novo domínio ou esse servidor será um controlador de domínio adicional?

Para que haja um domínio, é necessário que uma floresta exista. Para uma implementação inicial em ambientes em que não existam um controlador de domínio, é necessário criar uma nova floresta.

2.1.1 Definição de floresta

Uma floresta no Active Directory é uma coleção de uma ou mais de árvores de domínio. Os domínios (árvores) presentes em uma floresta podem compartilhar o mesmo nome de domínio, mas não é necessariamente obrigatório.

Infográfico 1 – Representação gráfico de uma floresta e de árvores de domínio



Fonte: Elaborado pelo autor, 2020

A principal vantagem da criação de uma floresta no Active Directory é que ela atua como um mecanismo centralizado para gerenciar e controlar a autenticação de toda a organização. Os administradores podem criar contas de usuário e senha para os funcionários da organização, o que significa que o Active Directory pode autenticar os logins.

As florestas, que são os limites de segurança da estrutura lógica, podem ser estruturadas para fornecer autonomia e isolamento de dados e serviços em uma organização. Em infraestruturas mais enxutas como, por exemplo, um supermercado que possui uma matriz e uma filial com dois servidores, um para cada unidade, e dez máquinas-clientes em cada unidade, não há a necessidade da criação de dois domínios para cada unidade. Essa divisão pode ser feita por unidades organizacionais.

As unidades organizacionais oferecerão a organização necessária aos computadores e usuários, sem a

necessidade de criar vários domínios em uma floresta. O exemplo que será desenvolvido nesta unidade terá apenas uma floresta, cujo domínio será **empresa.local**. Esse domínio não terá nenhum domínio filho, como **matriz.empresa.local** ou **filial1.empresa.local**. Toda a organização lógica será feita por unidades organizacionais. A Figura 7 apresenta um exemplo de como a estrutura lógica pode ser organizada em apenas um domínio, utilizando unidades organizacionais.

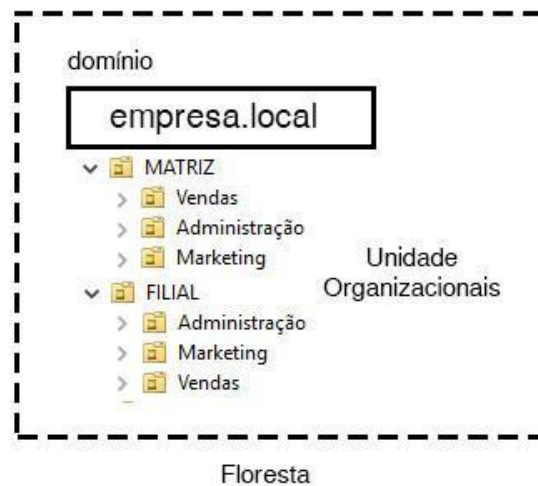


Figura 7 – Representação gráfica de uma floresta com apenas um domínio. A organização pode ser feita por unidades organizacionais.

Fonte: Elaborado pelo autor.

2.1.2 Domínios

Os domínios são estruturados em uma floresta para fornecer autonomia de dados e otimizar a replicação em uma determinada região. Essa separação de estruturas lógicas aprimora a capacidade de gerenciamento e reduz os custos administrativos porque a estrutura lógica não é afetada por alterações na estrutura física. A estrutura lógica também permite controlar o acesso aos dados. Isso significa que ela pode ser utilizada para compartilhar dados e, ao mesmo tempo, definir como serão as permissões de acesso a estes dados. Explicando de forma prática, podemos configurar para que usuários do domínio **saopaulo.brasil.local** não tenham acesso a computadores e informações dos usuários do domínio **brasil.brasil.local**. Dessa forma, apenas pela estrutura lógica do domínio é possível organizar a segurança de dados da empresa.

Como exemplo, teremos apenas na nossa floresta um domínio chamado **empresa.local**. Sabendo disso, é necessário inicialmente criar uma nova floresta para a criação desse domínio. Na criação do novo domínio, devemos selecionar a opção **Add a New Forest** (adicionar uma nova floresta) e definir o nome do domínio raiz. Em **Root domain name** foi definido o nome **empresa.local**.





Figura 8 – Captura de tela para criação de uma nova floresta.

Avançando no provisionamento do servidor, devemos definir o controle funcional da floresta e do domínio. Suponhamos que haverá vários domínios raiz nesta floresta, com vários servidores que serão controladores de domínio. As versões do software Active Directory, instaladas em diferentes servidores, devem ser compatíveis entre si.

Se um desses servidores da floresta for controlador de domínio e possuir a versão 2012 R2 do Windows Server, os demais servidores devem ter o nível funcional compatível com esta versão. Neste caso, o nível funcional desta floresta deverá ser Windows Server 2012 R2. Da mesma forma, é possível indicar o nível funcional do domínio, caso se tenha, neste domínio específico, um servidor que seja controlador de domínio com uma versão mais antiga do Windows Server, os demais servidores com Active Directory nos domínios filhos deverão ter versões compatíveis. Resumidamente, o nível funcional da floresta deve ser a versão do Windows Server mais antiga da floresta, sabendo que o Windows Server 2019 é compatível com o nível funcional até o Windows Server 2008.

Observe, na Figura 9, que, apesar de estarmos utilizando o Windows Server 2019, o nível funcional da floresta mais atual é a do Windows Server 2016. Sabemos, então, que não houve atualizações significativas no Active Directory entre as versões 2016 e 2019.

Neste exemplo, com uma infraestrutura mais enxuta, como apenas um domínio e servidor, iremos somente utilizar a versão 2019 do Windows Server. Sendo assim, o nível funcional da floresta e do domínio serão da versão 2016.

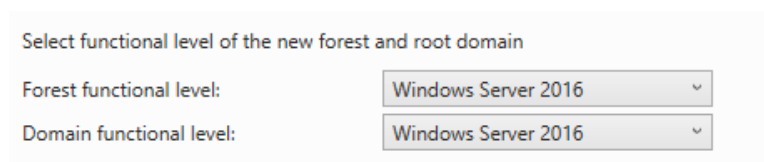


Figura 9 – Captura de tela da definição do nível funcional.

Nesta próxima etapa do provisionamento, observe, pela Figura 10, que a opção **Domain Name System** (DNS) é selecionada por padrão quando estamos criando uma nova floresta. Como o Active Directory terá o catálogo de nomes dos computadores da floresta e como este catálogo pode ser atualizado

constantemente, é importante que o servidor de DNS esteja presente no mesmo servidor.

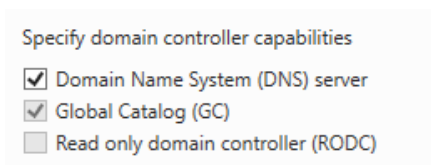


Figura 10 – Captura de tela da definição do nível funcional.

É possível que outro servidor seja o servidor DNS, mas em um ambiente com Active Directory é aconselhável que o mesmo servidor possua este serviço, desta forma, a opção **Domain Name Server** está selecionada para a instalação e provisionamento neste servidor. O catálogo global (Global Catalog - GC) deve ser instalado neste servidor, pois estamos criando uma nova floresta. É neste catálogo que os objetos pertencentes ao Active Directory serão armazenados.

Por último, temos a opção **Read only domain controller**, que pode ser definida somente para servidores que serão controlador de domínio somente leitura, ou seja, sem a permissão de escrita e edição de objetos no Active Directory. Este tipo de servidor somente é possível como controlador de domínio adicional em um domínio que já possua um controlador de domínio principal. Como este é o primeiro domínio da floresta, e, conseqüentemente, é o primeiro servidor como controlador de domínio, esta opção não pode ser utilizada, pois este servidor deverá ter permissão para criar, editar e excluir objetos no Active Directory.

Ainda nesta etapa de provisionamento do servidor, é necessário definir uma senha de restauração do Active Directory para o caso de haver algum problema com este servidor e o catálogo de objetos do Active Directory precisar ser restaurado em outro servidor, por exemplo.

Avançando na instalação, será exibido um alerta com a indicação de que não é possível criar uma delegação DNS, pois não foi encontrada nenhuma zona DNS, já que não temos nenhum serviço de DNS ativo. No entanto, o serviço de DNS será criado automaticamente assim que o controlador de domínio for provisionado, desta forma, basta avançar com o provisionamento do servidor.

O próximo passo é definirmos o nome NetBIOS. O NetBIOS é um protocolo que fornece serviços de comunicação em redes locais. Ele usa um protocolo de software chamado NetBIOS Frames, que permite que aplicativos e computadores em uma rede local se comuniquem com o hardware da rede e transmitam dados pela rede. Por padrão, o nome de domínio é definido para o nome NetBIOS, como apresentado no assistente de provisionamento.

A próxima etapa é definir onde será salvo o banco de dados do Active Directory, o local onde serão salvos os logs do sistema e a pasta SYSVOL, que é utilizada para armazenamento de scripts.

O ideal é que todas essas pastas sejam salvas em outro disco, em um local diferente do sistema operacional para melhorar a performance e para que os arquivos salvos nas pastas sejam facilmente recuperados caso o servidor se perca por problemas de hardware. Neste exemplo, serão indicados os locais padrão. Avançando no provisionamento, temos um resumo de todas as opções definidas para a confirmação. A seguir, serão verificados os pré-requisitos necessários para o provisionamento deste servidor para controlador de domínio. Caso algo não seja atendido, uma mensagem será exibida com o pré-requisito não atendido. Caso todos os pré-requisitos sejam atendidos, o provisionamento do servidor será liberado.

O próximo passo é clicar no botão **Install** e aguardar o fim da instalação e do provisionamento. O servidor precisará ser reiniciado ao final da instalação.

No próximo log on, o administrador não estará mais logando como administrador local, mas sim como administrador do domínio **empresa.local**. Assim, finalizamos a instalação do Active Directory e o provisionamento do servidor como controlador de domínio do domínio **empresa.local**.

2.2 Gerenciamento de contas

Após a instalação do Active Directory e de promover o servidor como controlador de domínio, novas ferramentas para o gerenciamento de computadores, contas de usuários e nomes de domínio e outras atividades serão instaladas. Essas ferramentas estão disponíveis no menu **Tools**, presente na janela do **Server Manager**.

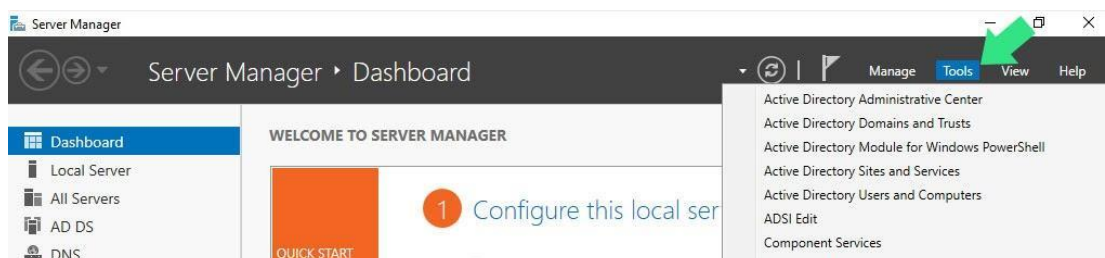


Figura 11 - Novas ferramentas para o gerenciamento de objetos do AD.

As principais ferramentas para o gerenciamento de objetos do Active Directory são:

» Clique nas abas para saber mais sobre o assunto

**Active Directory
Administrative Center**

**Active Directory
Users and Computers**

**Group
Policy Management**

Os dois principais objetos pertencentes a um domínio são o usuário e o computador, em que usuário corresponde ao elemento humano, ou seja, o funcionário de uma determinada corporação, e o computador ao objeto de uso do usuário.

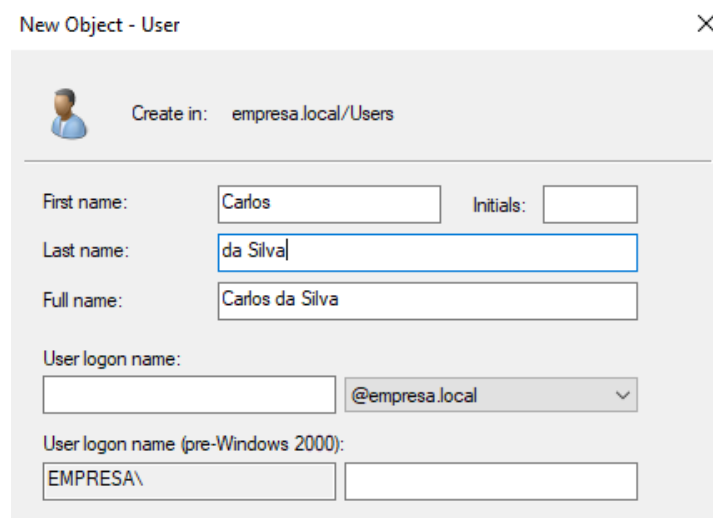
Vamos pensar no cenário de uma empresa de contabilidade. A empresa como um todo é representada pelo domínio **empresa.local**. Os funcionários desta empresa são os usuários. Todos os computadores da empresa também pertencem ao domínio **empresa.local**. Desta forma, todos os usuários e computadores do domínio **empresa.local** estarão regidos pelas regras aplicadas a este domínio.

2.2.1 Criação de usuários

Para que um funcionário possa logar em um dos computadores do domínio, ele precisa de uma conta de usuário. Esta conta guarda basicamente informações como nome, endereço, função na empresa, e-mail e, principalmente, um nome de usuário para login e a senha de acesso.

Vamos aprender a criar um usuário por meio da ferramenta **Active Directory Users and Computers**. Por padrão, o Active Directory apresenta uma série de contêineres e unidades organizacionais. Mais à frente, entenderemos melhor quais são as funções das unidades organizacionais. É apresentado um contêiner com o nome de **Users**, em que estão contidos os usuários padrão do domínio, entre eles, o usuário administrador (administrator). Inicialmente, vamos acompanhar a criação de um usuário diretamente no contêiner **Users**. Pelo botão **Add New User**, presente na janela do **Active Directory Users and Computer**, é possível dar início à criação de um novo usuário.

Inicialmente, é necessário indicar o nome e o sobrenome deste novo usuário.



New Object - User

Create in: empresa.local/Users

First name: Carlos Initials:

Last name: da Silva

Full name: Carlos da Silva

User logon name: @empresa.local

User logon name (pre-Windows 2000): EMPRESA\

Figura 12 – Captura de tela para janela de criação de um novo usuário.

O próximo passo é definir o nome de log on do usuário (**User logon name**). O funcionário da empresa utilizará este nome de log on para ter acesso ao computador do domínio. O nome de log on deve ser único dentro do mesmo domínio e, para que fique mais fácil para o usuário memorizá-lo, deve ter de relação com seu nome. Neste exemplo, o nome do usuário é Carlos da Silva, desta forma, podemos criar o nome de logon das seguintes formas:

» Clique nas abas para saber mais sobre o assunto

Sobrenome e nome
separados por pontoNome e sobrenome
separados por pontoSobrenome e nome
separados por underscoreNome e sobrenome
separados
por underscoreSobrenome e
nome sem
separaçãoNome e
sobrenome
sem separaçãoNome com
caractere
numérico

O ideal é que se crie um padrão de criação de nomes de log on de usuários que seja respeitado para a criação de todos os usuários do domínio. Como exemplo, o padrão aplicado será nome e sobrenome separados por ponto, desta forma, teremos o nome de log on **carlos.dasilva**.

Avançando no assistente de criação de usuário, o próximo passo é definir uma senha de acesso para o usuário. Por padrão, podemos definir uma senha provisória para esse usuário com a opção **User must change password at next logon** (O usuário deve alterar a senha no próximo log on) selecionada. Desse modo, o usuário será obrigado a trocar a senha assim que logar pela primeira vez em um computador do domínio **empresa.local**.

Outra forma é definir a senha do usuário e com a opção **User cannot change password** (O usuário não pode alterar a senha). Se esta opção for selecionada, a senha não poderá ser alterada pelo usuário. Essa opção pode ser útil para usuários provisórios, como visitantes da empresa que terão acesso aos computadores do domínio.

Por padrão, a senha do usuário deve ser alterada a cada 42 dias. Caso não deseje que esse padrão seja respeitado, selecione a opção **Password never expires** (A senha nunca expira). Também existe a possibilidade de criar um usuário e deixá-lo desabilitado, desta forma, esse usuário existirá no domínio mas estará impossibilitado de realizar o log on. Essa opção pode ser utilizada para usuários visitantes da empresa e, na data da visita, o usuário é habilitado a realizar o log on. Como exemplo, serão definidas as opções padrão de criação de usuário, indicando uma senha provisória que deverá ser alterada no próximo log on.

Vale saber que esta senha também deve respeitar uma complexidade mínima, a mesma de criação de senha aplicada ao administrador do domínio. Segundo Thompson:

Na próxima etapa você deve informar uma senha qualquer, tendo o cuidado de marcar a opção O usuário deve alterar a senha no próximo logon. Uma sugestão é

usar uma senha inicial padrão para todos, assim quando você informar o nome do usuário, basta informar a senha padrão, que será alterada no primeiro login. Existe algum risco nessa sugestão de senha padrão, porque outra pessoa pode acessar a conta usando a senha padrão e modificá-la. (2014, p. 254)

Avançando no assistente de criação de usuários, um resumo das opções selecionadas será exibido. Clicando em **Finish**, o usuário será criado e, por padrão, poderá logar em qualquer computador pertencente ao domínio **empresa.local**.

Após criar um usuário para o domínio, o próximo passo é criar um computador para o domínio **empresa.local**. Sem a definição dos computadores pertencentes ao domínio, um usuário não poderá realizar o log on. O usuário somente poderá realizar o log on em computadores pertencentes ao domínio.

2.2.2 Criação de computadores

Uma das primeiras coisas a fazer após a criação de um domínio e a instalação do Active Directory é ingressar um computador ao domínio, pois se o computador não estiver ingressado ao domínio, o usuário não poderá realizar o log on no computador do cliente. Inicialmente, o único computador já ingressado ao domínio é o servidor. É possível visualizar este computador clicando em **Domain Controllers**.

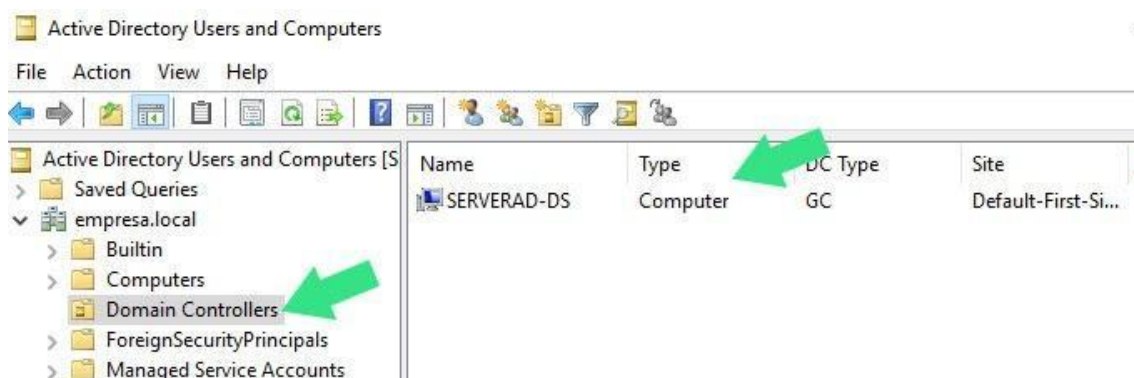


Figura 13 – Captura de tela de exibição do servidor ingressado ao domínio.

Existem duas formas de criar um computador no Active Directory:

1. Criar o seu nome antes que o computador seja ingressado ao domínio. Desta forma, o nome do computador ficará inativo até que seja ingressado.
2. Ingressar o computador ao domínio diretamente. Desta forma, a criação do nome do computador no Active Directory será feita automaticamente.

Por padrão, todos os novos computadores ingressados no domínio serão armazenados em **Computers**.

Vamos ingressar um computador ao domínio **empresa.local**. Neste exemplo, será utilizado um computador com o sistema operacional Windows 10. Ingressaremos o computador ao domínio sem referenciá-lo anteriormente no Active Directory. Dessa forma, sua criação será feita assim que ele for ingressado ao domínio. Duas configurações são importantes para um computador-cliente seja ingressado ao domínio:

» a) Endereçamento IP

A máquina-cliente deve possuir um endereçamento IP com acesso ao servidor na mesma rede do servidor ou acessível via roteamento entre redes. Neste exemplo, indicaremos para a máquina-cliente o endereçamento IP 192.168.100.50, ou seja, na mesma rede do servidor, a rede 192.168.100.0. Vale saber que estamos utilizando um endereçamento IP fixo, mas para a máquina-cliente este procedimento não é necessário, ela poderia receber um endereçamento IP via servidor DHCP ou por outro dispositivo com este serviço de entrega de IPs, como um roteador.

» b) Endereçamento IP do servidor DNS

É importante também que esse computador-cliente saiba quem é o controlador de domínio da rede. Para isso, ele precisa saber resolver os nomes dos computadores da rede em números IPs, ou seja, ele precisa saber que o servidor com o nome ServerAD-DS possui o endereçamento IP 192.168.100.10. Sendo assim, é necessário indicar quem é o servidor de nome primário da rede (Servidor DNS). Por padrão, quando instalamos o Active Directory em um servidor, ele também recebe o serviço de resolução de nomes, ou seja, o nosso controlador de domínio também é o nosso servidor de DNS. Dessa forma, é preciso indicar que o controlador de domínio com o IP 192.168.100.10 é o servidor de DNS primário da rede.

As configurações de IP e Servidor DNS preferencial podem ser feitas por meio das Configurações de rede e internet do Painel de controle do Windows 10.



VOCÊ QUER VER?

Caso você tenha dúvidas sobre o serviço de DNS, o vídeo *A importância do DNS nas redes, explicada pelo NIC.br*, acessível pelo link: < <https://www.youtube.com/watch?v=epWv0-eqRMw> > demonstra, de uma maneira bem didática, a função de um servidor DNS na internet e para redes locais.

O próximo passo é adicionar o computador-cliente ao domínio. É possível realizar este procedimento pelo Explorador de arquivos do Windows, acessando o atalho **Este Computador** e, posteriormente, clicando no botão **Propriedades**, indicado na Figura 14.



Figura 14 – Captura de tela de atalho para o acesso às propriedades do computador.

Observe que o computador possui um nome provisório e ele ainda pertence ao grupo de trabalho padrão do Windows, chamado de Workgroup.

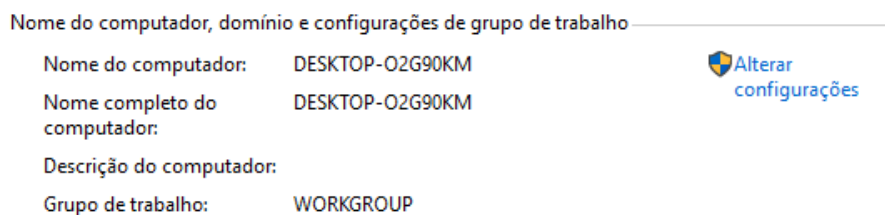


Figura 15 – Captura de tela da exibição do nome e grupo de trabalho no Windows 10.

Esta janela apresenta a opção **Alterar configurações**, na qual é possível alterar as configurações de nome e domínio do computador-cliente. Suponhamos que esse computador pertença ao departamento administrativo da empresa. O ideal é que consigamos identificar um computador pelo seu nome para facilitar sua localização na empresa e também sua setorização dentro do Active Directory. Neste exemplo, chamaremos este computador de ADM1 e suponhamos que ele seja o primeiro computador do departamento administrativo da empresa. Para isso, foi digitado, em **Nome do computador**, o nome ADM1. Em **Membro de**, foi selecionado **Domínio**, pois esse computador não pertence mais a um grupo de trabalho, mas sim ao domínio **empresa.local**. Observe que o nome de domínio **empresa.local** foi indicado.

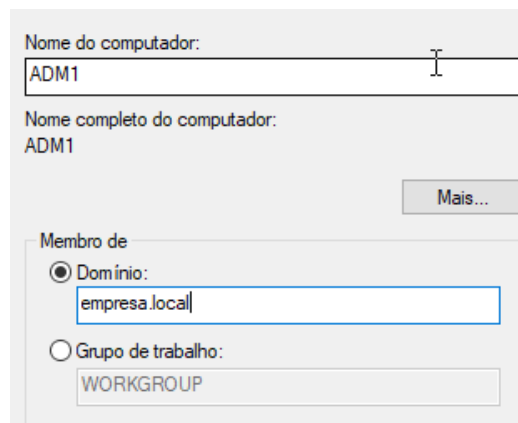


Figura 16 – Captura de tela da definição do nome e domínio da máquina-cliente.

Para que uma máquina seja adicionada a um domínio, é necessário que um usuário com permissão para isso realize o procedimento. Por padrão, qualquer usuário do domínio pode adicionar até dez computadores ao domínio (salvo o administrador, que pode adicionar um número ilimitado de computadores).

Observe que o usuário administrador (administrator) foi utilizado juntamente com a senha. Após a confirmação do usuário administrador, a máquina ingressará ao domínio após ser reiniciada. Por padrão, o computador é automaticamente adicionado a **Computer**.

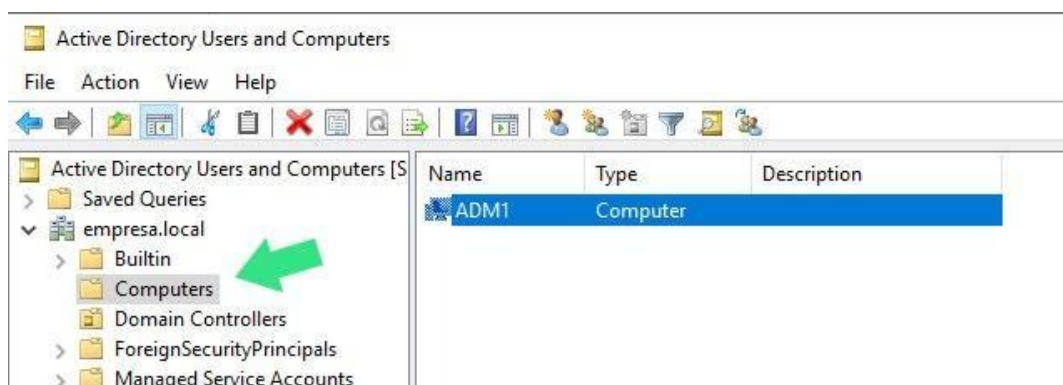


Figura 17 – Computador ADM1 adicionado ao contêiner Computers.

Este computador agora estará vinculado às políticas de segurança definidas pelo Active Directory e somente poderá ser logado ao domínio por usuários previamente autorizados.

2.3 Gerenciamento de grupos

Para facilitar a gerência e edição de regras que serão aplicadas a diversos usuários e computadores, é possível criar grupos no Active Directory. Vamos supor que, em determinado setor da empresa, alguns usuários poderão ter acesso a um compartilhamento de pasta e somente estes usuários poderão realizar alterações nos arquivos pertencentes a esta pasta. Para que não seja necessário aplicar as permissões para cada usuário individualmente, é possível criar um grupo de usuários, adicionar os usuários ao grupo e aplicar as permissões ao grupo em vez de aplicar as permissões individualmente usuário por usuário.

Para criar um grupo no Active Directory, basta clicar no botão **Create a new group in the current container** (Criar um novo grupo no container atual).

A primeira coisa a ser definida na criação de um grupo é o seu nome, que normalmente deve estar relacionado a sua função ou aos usuários que serão adicionados ao grupo. A criação de grupos de usuários pode facilitar os aspectos de segurança em uma rede, pois é possível simplificar a atribuição de direitos e permissões de um usuário. Outras características importantes dos grupos de usuários:

- Os usuários de um domínio podem ser membros de vários grupos, tendo permissões compartilhadas com os grupos ao qual ele pertence;
- Contas de computadores podem ser membros de grupos, recebendo automaticamente atribuições de segurança aplicadas ao grupo.

2.3.1 Grupos universais, globais e locais

Outro fator importante na definição de um grupo, além do seu nome, é a escolha do escopo de atuação do grupo e o seu tipo. A definição do escopo limitará a atuação de um grupo de usuários dentro de uma floresta do Active Directory. Os escopos são:

- **Domain Group** (Grupos de domínio local): os membros podem receber permissões somente em um único domínio, em nosso exemplo, somente no domínio empresa.local.
- **Global** (Grupos globais): os membros podem receber permissões em qualquer domínio na floresta. Se nesta floresta existissem dois domínios como empresa.local e empresa2.local os usuários poderiam receber permissões nos dois domínios.
- **Universal** (Grupos universais): os membros desses grupos podem receber permissões em qualquer domínio na árvore de domínio ou floresta, ou seja, se dentro de um domínio houver subdomínios atribuídos, os usuários também poderão receber permissões de qualquer domínio atrelados à árvore.

Por padrão, ao criar um grupo, é atribuído o escopo Global, limitando as atribuições de segurança dentro dos domínios da floresta. O próximo passo é definir o tipo. Existem dois tipos de grupo que podem ser criados no Active Directory.

Security (Grupos de segurança): usados para atribuir permissões aos recursos compartilhados.

Distribution (Grupos de distribuição): cria listas de distribuição por e-mail. Por padrão, na criação de um grupo, o tipo definido é Security.

Neste exemplo, será atribuído o nome GRP_Vendas, levando em consideração que os usuários pertencentes a este grupo são do departamento de vendas. Este grupo será enquadrado no escopo Global e será do tipo Security.

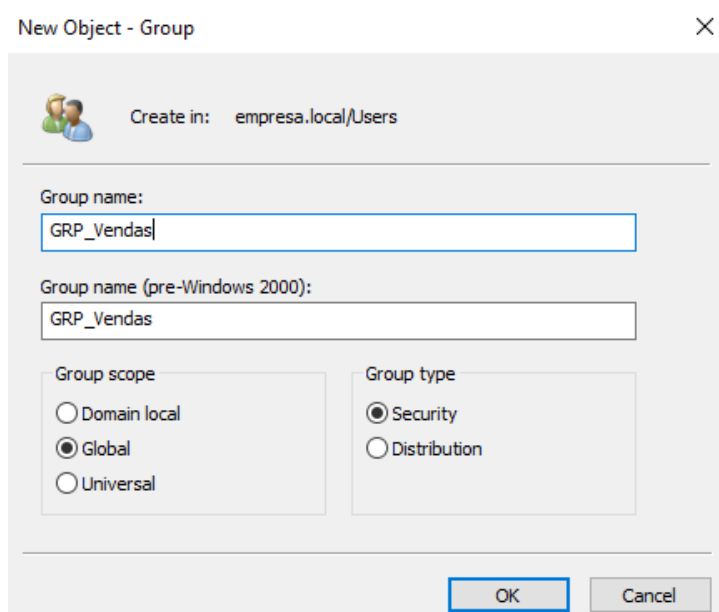


Figura 18 – Definições para a criação de um novo grupo no AD.

Após a criação de um grupo, os usuários ou computadores podem ser adicionados a este grupo, consultando as propriedades do grupo criado. Desta forma, é possível adicionar e remover usuários e computadores ao grupo e também é possível adicionar outros grupos a este grupo.

2.3.2 Unidades organizacionais

Outra forma de organizar os objetos do Active Directory, como usuários, computadores e grupos, é a criação de unidades organizacionais. As unidades organizacionais funcionam como pastas para armazenamento de objetos, facilitando a sua organização a atribuições de políticas de grupo. Por exemplo, em vez de armazenar todos os usuários no contêiner **Users**, é possível organizar os usuários por setores como administração, vendas, marketing etc.

As Unidades Organizacionais, às quais vamos nos referir usando a abreviatura UO, representam uma forma interessante de gerenciar objetos no AD. Elas podem

ser usadas para organizar vários objetos, como contas de usuário, contas de grupos, máquinas etc. A UO é um contêiner e as configurações aplicadas a ele se refletem nos objetos do contêiner. Na prática, a administradora cria as contas de grupos e usuários e depois cria contêineres, as UOs, estrategicamente pensadas para organizar as permissões de acesso à rede. Use UO para: organizar objetos no domínio, delegar controle administrativo e simplificar o gerenciamento de recursos agrupados (THOMPSON, 2014; p. 320).

É possível também criar um contêiner específico dentro das unidades organizacionais para armazenar os computadores e impressoras daquele setor. Por exemplo, na Figura 19, temos uma empresa com três departamentos: administração, vendas e marketing. Para cada unidade organizacional criada, foi criado um contêiner de nome **Computadores**, com o objetivo de armazenar os computadores do setor, e outro contêiner chamado **Usuários**, para armazenar os usuários e grupos de usuários do setor.

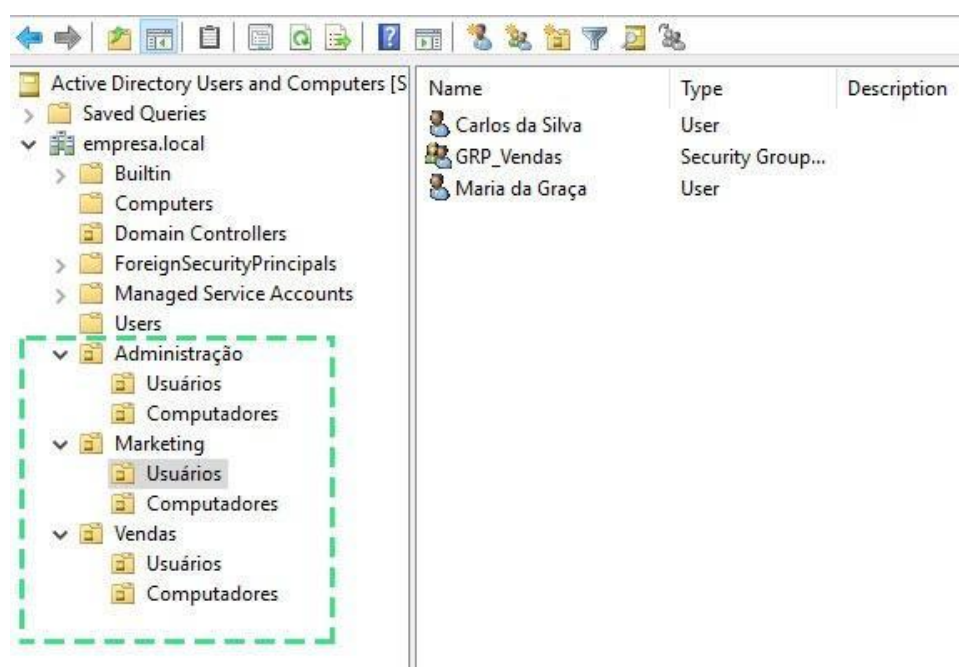


Figura 19 – Captura de tela das organizações dos objetos do AD em contêineres.

A criação de unidades organizacionais é feita pelo botão **Create a new organizational unit in the current container** (criar uma nova unidade organizacional no container atual), conforme indicado na Figura 20.



Figura 20 – Botão utilizado para a criação de unidades organizacionais.

A organização em unidades facilita muito a localização de usuários e computadores específicos, pelo administrador, sem que seja necessário utilizar ferramentas de busca. Outra vantagem importante na criação de unidades organizacionais é que, caso seja necessário criar uma política de segurança, por exemplo um papel de parede padrão para os computadores do departamento de marketing, basta que a política seja criada dentro da unidade organizacional Marketing para que seja atribuída somente aos computadores pertencentes ao setor.

2.4 Administração

Em grandes empresas com grande infraestrutura e muitos funcionários, é extremamente trabalhoso para o administrador do domínio gerenciar todos os usuários do Active Directory. Tomemos como exemplo uma situação na qual, no departamento de vendas, serão contratados dez novos funcionários que terão acesso aos computadores do departamento. Caso a administração do Active Directory esteja centralizada no administrador do domínio, o responsável pelo departamento deve contatá-lo e pedir a criação desses dez novos usuários. As unidades organizacionais também permitem delegar tarefas administrativas a usuários ou grupos, sem precisar torná-los um administrador do domínio. Caso o administrador da rede atribua funções de administrador de domínio para um determinado usuário, este passa a ter permissões totais dentro de todas as unidades organizacionais do domínio. Permissões que darão poderes ao usuário para excluir e editar objetos dentro de todo o domínio.

2.4.1 Direitos administrativos

Este tipo de atribuição de poderes ou direitos não é aconselhável por questões de segurança. Poderes totais de administração devem estar atribuídos somente ao usuário administrativo do domínio e usuários específicos. No Active Directory, é possível dar poderes limitados aos usuários dentro de uma unidade organizacional, como por exemplo:

- Gerenciar usuários (criar, excluir e editar usuários dentro da unidade organizacional);
- Gerenciar grupos;
- Modificar a associação ao grupo;
- Gerenciar links de diretiva de grupo;
- Redefinir senhas em contas de usuário.

Desta forma, somente direitos específicos poderão ser realizados pelos usuários com esses direitos administrativos.

2.4.2 Delegando administração

É possível delegar a um funcionário responsável por um determinado departamento permissões para criar, excluir e editar usuários **apenas** na unidade organizacional marketing, por exemplo.

Vamos acompanhar um exemplo. Clicando com o botão da direita do mouse sobre a unidade organizacional marketing, é possível selecionar a opção **Delegate Control** (delegar controle). Um assistente será aberto e o próximo passo é selecionar os usuários que receberão as delegações.

É possível adicionar mais de um usuário. Avançando pelo assistente, a próxima etapa é selecionar quais serão as permissões delegadas aos usuários. Neste exemplo, foram selecionadas as permissões de criar, excluir e editar usuários, resetar senhas e criar e gerenciar grupos de usuários.

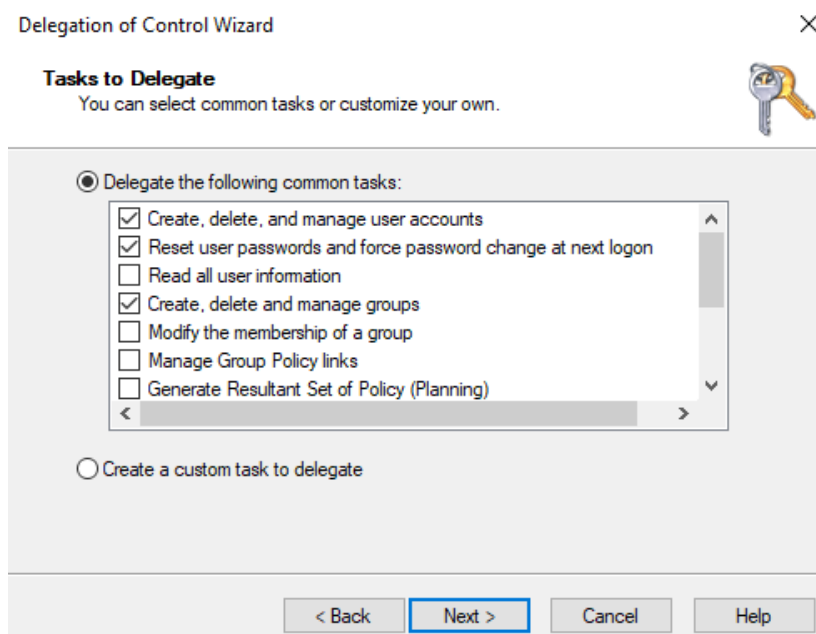


Figura 21 – Captura de tela das delegações que serão aplicadas aos usuários.

Finalizando, o assistente o usuário e/ou usuários selecionados terão as permissões atribuídas para a unidade organizacional a qual pertence.

Síntese

Caros alunos, vimos, nesta unidade, que, ao utilizarmos a interface gráfica do Windows Server a partir dos assistentes de instalação e provisionamento, é possível instalar o Active Directory e provisionar o servidor a controlador de domínio de uma maneira simplificada. Estudamos também que, por meio das ferramentas do Active Directory, operações inerentes aos usuários e computadores do domínio podem ser feitas de maneira simplificada. Antes de finalizar, pudemos conhecer a importância da criação de grupos de usuários e computadores, a definição das unidades organizacionais e como elas podem ser utilizadas para delegar funções administrativas a usuários pertencentes a ela.

Referências bibliográficas

TANENBAUM, A. S. **Sistemas operacionais modernos** . 4. ed. São Paulo: Pearson, 2016.

THOMPSON, M. A. **Microsoft Windows Server 2012** : instalação, configuração e administração de redes. 2. ed. São Paulo: Érica, 2014.
