

SERVIÇOS DE INTERCONNECTIVIDADE WINDOWS

UNIDADE 3 – CONHECENDO O SERVIÇO DE SITE DO ACTIVE DIRECTORY E APLICANDO AS POLÍTICAS DE GRUPOS

Autor: Denilson Bonati

Revisora: Cilene Renata Real

INÍCIO

Introdução

Nesta unidade, conheceremos métodos de organização dos objetos do Active Directory, por meio de sites. Esse tipo de organização pode ser muito importante em ambientes que possuem apenas um domínio, mas que possuem outras organizações físicas ou geográficas, como matrizes e filiais em outras cidades ou localizações. Aqui, conheceremos as políticas de grupo e sua função dentro do ambiente do Active Directory. Será demonstrada a função de um servidor de arquivos e quais ferramentas o Windows Server fornece para classificação, compartilhamento e segurança dos arquivos em um servidor. Por último, conheceremos o gerenciamento do DNS em um ambiente com o Active Directory.

3.1 Serviços e sites do AD

O que torna o Active Directory uma ferramenta muito poderosa e o principal diferencial na escolha de utilização do Windows Server como software para administrar grandes e pequenas redes são as suas características de estruturação lógica e física. A estrutura lógica consiste no sistema de florestas e domínios; a estrutura física são os servidores controladores de domínios e o servidor em geral, como servidores de arquivos, máquinas clientes (hosts), sub-redes físicas etc.

O serviço de sites do Active Directory consiste em um meio lógico para representar aspectos físicos de uma rede dentro do Active Directory. O conceito de “sites” no Active Directory representa uma divisão física. Por exemplo, suponhamos que temos um domínio com o nome de empresa local. Nele, queremos dividir fisicamente três localidades distintas dentro da mesma empresa, como a matriz na cidade de São Paulo, uma filial na cidade do Rio de Janeiro e outra filial na cidade de Manaus. Essa divisão pode ser realizada sem a necessidade de criação de outros domínios filhos, como **riodejaneiro.empresa.local** ou **manaus.empresa.local**.

3.1.1 Visão geral

Os sites do Active Directory são a melhor solução para gerenciar organizações que possuem filiais em diferentes localizações geográficas, mas que se enquadram no mesmo domínio. Sites são agrupamentos físicos de sub-redes IP, usadas para replicar informações, com eficiência, entre controladores de domínio.

Os sites podem ser utilizados e pensados como um mapeamento que irá descrever as melhores rotas para se executar uma replicação dentro do Active Directory, fazendo com que esta atividade seja feita o mais rápido possível, dentro das limitações físicas da rede – como, por exemplo, problemas de banda de rede e de conexão com a internet. A criação de um site permite que se exerça melhor controle sobre o tráfego de replicação e o processo de autenticação. Quando houver mais de um controlador de domínio dentro de um mesmo site associado, ele será capaz de lidar com mais velocidade com as requisições de login e com as diretivas de grupos aplicadas.

Os sites podem ser explicados como locais físicos, que contêm vários objetos. Eles

devem poder ser descritos usando seus limites. Como exemplo, usuários, computadores e dispositivos de rede localizados em um escritório em Londres podem ser tratados como um site e podem ser identificados exclusivamente a partir de objetos semelhantes localizados no escritório de Seattle. (FRANCIS, 2017, p. 318)

O gerenciamento de sites no Active Directory pode ser feito na ferramenta Active Directory Sites and Services (Sites e serviços do Active Directory). Esta ferramenta pode ser acessada pelo menu **Tool**, na janela do Server Manager.

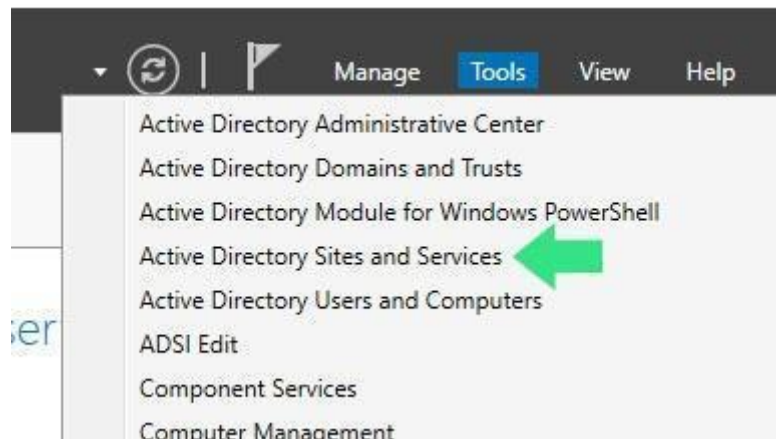


Figura 1 – Captura de tela de acesso ao gerenciamento de sites.

Fonte: Elaborada pelo autor, 2020.

Por padrão, o contêiner Default-First-Site-Name (Nome do primeiro site padrão) é criado para a floresta. Isso pode ser observado na Figura 2, observando a ferramenta **Active Directory Sites and Services**.

Até que outro site seja criado, todos os controladores de domínio serão atribuídos automaticamente a esse site.

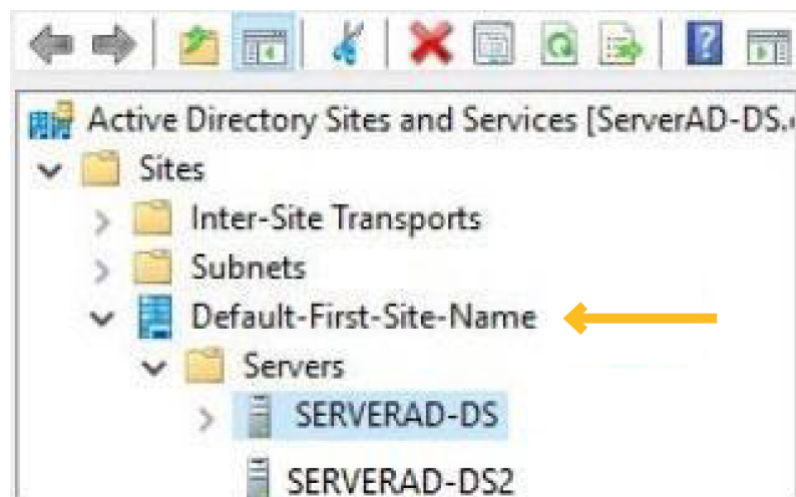


Figura 2 – Captura de tela do site padrão.

Fonte: Elaborada pelo autor, 2020.

Observe que, no mesmo site Default, a empresa possui, além do controlador de domínio principal, um novo controlador de domínio chamado SERVERAD-DS2. Neste exemplo, o nome Default-First-Site-Name foi alterado para o nome Matriz. Desta forma, será mais fácil a identificação dos objetos do diretório da empresa matriz dentro do Active Directory. Para simplificar o exemplo, teremos apenas mais um site chamado de Filial que será utilizado para gerenciar objetos como computadores e usuários da filial desta empresa.

3.1.2 Site links

Outra configuração importante, antes da criação de um novo site, é a definição do link do site, ou site link. Os links do site permitem definir quais sites estão conectados entre si, além do custo relativo da conexão.

Imagine o seguinte cenário: uma empresa possui uma filial na cidade de São Paulo e outra na cidade de Ribeirão Preto. As duas filiais possuem infraestruturas próprias com controladores de domínios próprios. As filiais são pertencentes a um mesmo domínio do Active Directory. Diariamente alterações são realizadas na filial de São Paulo e na Filial de Ribeirão Preto: novos computadores, novos usuários, novas permissões, etc. Em algum momento, deve existir a atualização dos dados entre as filiais pelo Active Directory, ou seja, o controlador de domínio da cidade de São Paulo deve estar ciente das alterações realizadas na cidade de Ribeirão Preto e vice-versa. Para isso, é criado um link de site para definir como serão essas atualizações.

Crie um design de link de site para conectar seus sites com links de site. Os links de site refletem a conectividade entre sites e o método usado para transferir o tráfego de replicação. Você deve conectar sites com links de site para que os controladores de domínio em cada site possam replicar Active Directory alterações (MICROSOFT, 2020).

Ao criar um link de site, são especificados quais sites estarão conectados por esse link e qual será o custo ou métrica da conexão. Em uma infraestrutura com apenas dois sites, pode-se ter apenas um link de site ligando duas cidades, por exemplo. Já em

infraestruturas maiores, com três sites, como três grandes andares de um prédio ou ainda três departamentos, é necessário criar mais de um link. Imagine uma empresa presente em três cidades: Rio de Janeiro, Manaus e São Paulo. Como é possível considerar o tráfego das informações? Todo o tráfego deve ser roteado pela cidade do Rio de Janeiro, cidade onde fica a matriz? Se a resposta for sim, pode-se criar dois links de site: Rio de Janeiro e Manaus, que será responsável pela replicação entre Rio de Janeiro e Manaus, e outro com o nome de Rio de Janeiro e São Paulo. Nesse padrão, a infraestrutura da cidade do Rio de Janeiro deve estar apta a receber um grande volume de dados das replicações de Manaus e São Paulo.

Em um link de site, é possível definir um custo de replicação, o que, por padrão, possui o valor 100. Caso se opte para o custo de 100, para o link Rio de Janeiro e Manaus, e o de 200 para o link Rio de Janeiro e São Paulo, a prioridade de replicação será dada ao link com o custo maior.

Neste exemplo, foi apenas renomeado o link padrão, com o nome de DEFAULTSITE LINK, para o nome Matriz-Filial. Os links de sites podem ser criados e consultados na pasta IP do container Inter-Site transports.

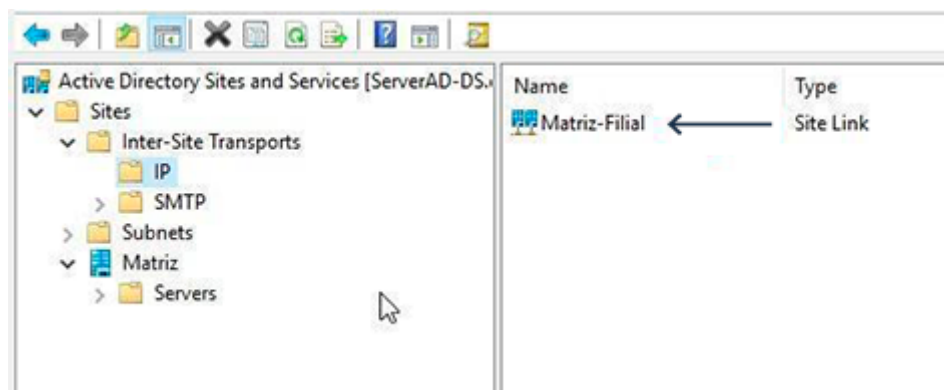


Figura 3 – Captura de tela: Definição de um único link de site.

Fonte: Elaborada pelo autor, 2020.

Não existe a obrigatoriedade de trocar o nome padrão do link. Esta operação foi realizada apenas para a melhor identificação.

» Criando um novo site

Quando já possuímos o site Matriz, o próximo passo é criar o novo site chamado de Filial. É possível criar um novo selecionando a opção New Site (novo site) e criar um novo site. Neste exemplo, foi indicado o nome Filial, como apresentado na Figura 4.

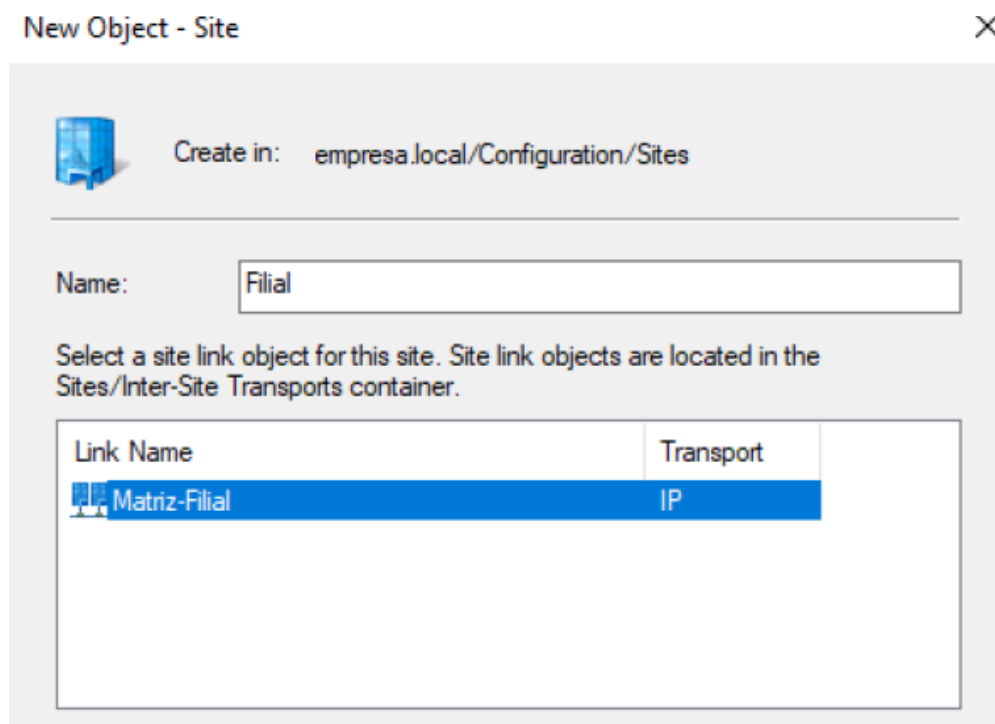


Figura 4 – Captura de tela: criação de um novo site.

Fonte: Elaborada pelo autor, 2020.

Observe que, antes de confirmar a criação de um site, é necessário definir quais serão os links do site. Neste exemplo, foi selecionado o link Matriz-Filial. Após a criação do site, é possível indicar qual será o servidor responsável pelas requisições de login e outras operações do Active Directory, dentro deste site. Neste exemplo, o servidor responsável em atender às requisições deste site será o servidor SERVERADDS-2. Dessa forma, é possível mover o servidor para o container Servers do site Filial, como apresentado na Figura 5.



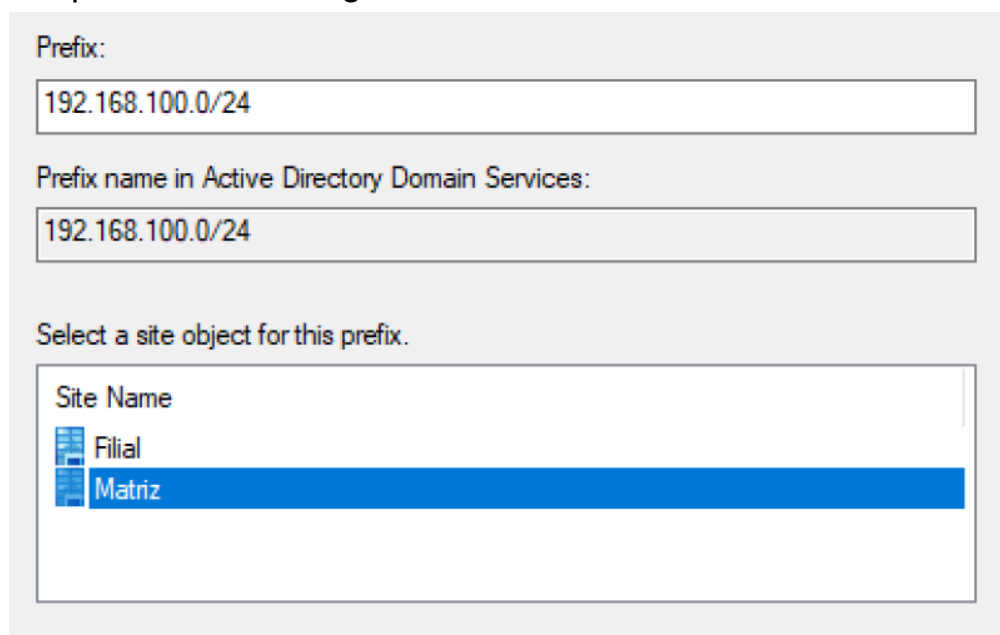
Figura 5 – Captura de tela: o servidor SERVERAD-DS2 atenderá as requisições de login e outras atividades inerentes ao AD no site Filial.

Fonte: Elaborada pelo autor, 2020.

3.1.3 Sub-redes

Outro item a ser configurado, caso seja necessário, são as definições de sub-rede. Uma sub-rede é uma parte do espaço IP de uma rede. As sub-redes são descritas pelo endereço de rede IP, combinado a uma máscara de sub-rede medida em bits. Por exemplo, a máscara de sub-rede 255.255.255.0 é uma máscara de sub-rede de 24 bits. Se você tiver uma máscara de 24 bits para a rede 192.168.100.0, seu objeto de sub-rede será descrito como 192.168.100.0/24. Os objetos de sub-rede no Active Directory são uma representação lógica das sub-redes em seu ambiente. Eles podem, mas não necessariamente precisam, refletir suas definições reais de sub-rede física.

Neste exemplo, teremos a sub-rede matriz descrita com a faixa de IP 192.168.100.0/24, enquanto a sub-rede Filial terá outra faixa de IP 192.168.101.0/24. Clicando com o botão da direita sobre o contêiner Subnets e selecionando a opção **New**, a janela apresentada na Figura 6 será exibida.



Prefix:

192.168.100.0/24

Prefix name in Active Directory Domain Services:

192.168.100.0/24

Select a site object for this prefix.

Site Name
Filial
Matriz

Figura 6 – Captura de tela: definição de uma nova sub-rede.

Fonte: Elaborada pelo autor, 2020.

Observe que, na definição da sub-rede, é preciso indicar a que site ela será vinculada. Utilizando este mesmo procedimento é possível criar outra sub-rede para o site Filial.

3.1.4 Replicação

Em qualquer infraestrutura é aconselhável o uso de mais de um controlador de domínio. Imagine uma empresa com apenas um servidor como controlador de domínio. Caso haja algum problema com este servidor, todos os funcionários (usuários do

domínio) não terão como realizar suas tarefas, pois uma das funções do Active Directory é promover o login desses usuários no domínio.

Dessa forma, é importante a utilização de mais de um controlador de domínio para suprir problemas técnicos com o controlador de domínio principal e também para dividir a carga de funções em sites diferentes, como os criados anteriormente: matriz e filial. Cada controlador de domínio deve armazenar o mesmo banco de dados. Para que o banco de dados do Active Directory permaneça constante, a replicação deve ocorrer.

Todo controlador de domínio na rede deve estar ciente de todas as alterações feitas. Quando o controlador de domínio aciona uma sincronização, ele passa os dados pela rede física para o destino. No ambiente do Active Directory, existem principalmente dois tipos de replicação:

Tipos de replicação

» Clique nas abas para saber mais sobre o assunto

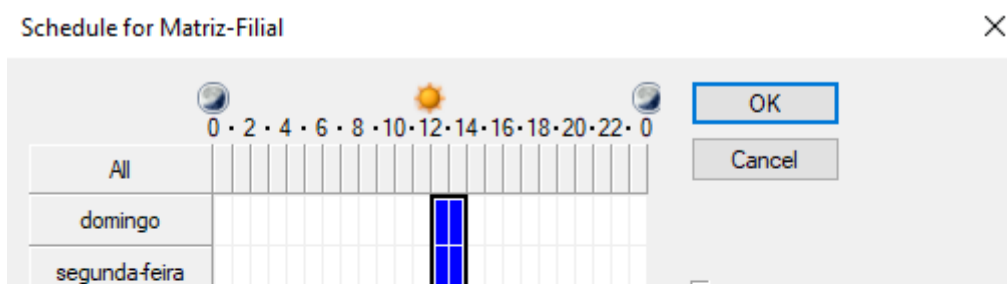
REPLICAÇÃO INTRA-SITE

REPLICAÇÃO ENTRE SITES

A replicação entre os sites é feita pelo link de site configurado anteriormente e é por ele que podemos definir as configurações de replicação.

Clicando com o botão da direita sobre o link, podemos seleccionar a opção **Properties** (propriedades). Nesta janela de propriedades, encontra-se um botão com o nome **Change Schedule** (Mudar horário).

Na janela que é apresentada na Figura 7, é possível definir os dias e horário em que a replicação entre sites ocorrerá, sendo possível, por exemplo, definir a replicação para todos os dias, das 12 às 14 horas, como o indicado na próxima imagem.



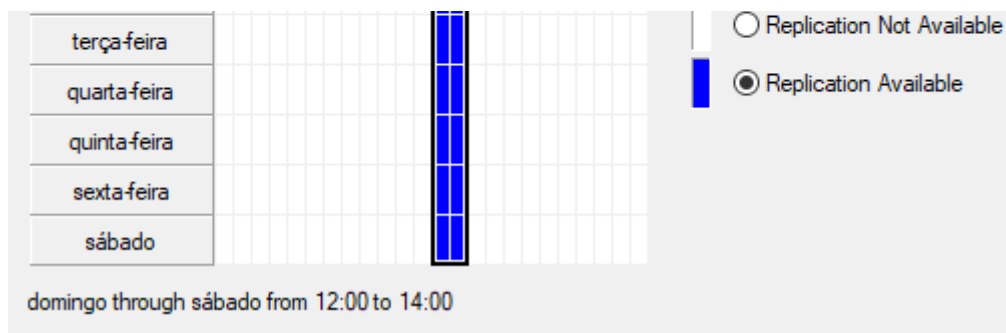


Figura 7 – Captura de tela: definição de dia e horário para a replicação.

Fonte: Elaborada pelo autor, 2020.

É importante que uma replicação seja feita o mais rápido possível. Os usuários e computadores criados em um determinado site, ou qualquer alteração de segurança, deve ser replicada o mais rápido possível para todos os controladores de domínio da empresa, a fim de que todos estejam sempre atualizados, com as referências de usuários atualizadas. Imagine um novo usuário criado no site B que, prontamente, precisará fazer um acesso remoto aos computadores do site A. Caso a replicação ainda não tenha sido realizada, esse usuário pode não ter o acesso ao site A. Portanto, data e horários específicos devem ser definidos em grandes infraestruturas com problemas de conexão, para evitar congestionamentos na rede.

3.2 GPO

As políticas de grupo, também chamadas simplesmente por GPO, são um conjunto de regras de segurança que pode ser aplicado a usuários e computadores de um domínio ou que pode também ser aplicado, localmente, no sistema operacional, como o Windows 10, por exemplo.

GPO significa Group Policy Object, ou objeto de política de grupo. É uma infraestrutura hierárquica que permite realizar alterações nos objetos de uma rede, como usuários, grupos, computadores e pastas. Com a implementação do GPO, conseguimos inibir muitos riscos de segurança em uma rede. Podemos, por exemplo, bloquear o acesso ao painel de controle por um usuário da rede.

Essas configurações são feitas sem acessar o computador do usuário, bastando configurar uma política na conta de acesso que

ele utiliza para acessar a rede (SERAGGI, 2019. p. 88).

Tendo um domínio, a aplicação dessas regras de segurança pode ser feita de maneira simplificada e centralizada utilizando as ferramentas do Windows Server. As políticas de grupo são usadas geralmente para restringir ações do usuário que podem pôr em risco a segurança de uma rede, como a instalação de programas e acesso a ferramentas de configuração do sistema operacional. As políticas de grupo também podem ser utilizadas para padronização de papel de parede, instalação automatizada de softwares, restrição e mapeamento de compartilhamento de pastas.

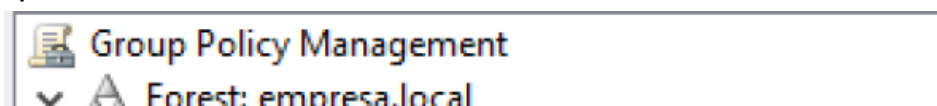
3.2.1 Definições Gerais

Com a prévia criação de unidades organizacionais no Active Directory, é possível restringir uma política de grupo para determinado setor de uma empresa. Imagine que se tenha uma unidade organizacional com o nome de Vendas e que os usuários tenham uma pasta compartilhada com arquivos de uso comum entre os vendedores. Para facilitar, o administrador da rede pode criar um compartilhamento somente para os usuários dessa unidade organizacional, impedindo que usuários de outros departamentos, como Secretaria e Administração tenham acesso a esta pasta. Outra forma de aplicar as políticas de grupo é aplicá-las a sites previamente criados. Imagine dois sites, um para a cidade de São Paulo e outro para a cidade do Rio de Janeiro. Os usuários da cidade do Rio de Janeiro possuem uma impressora disponível para impressão de documentos no setor administrativo. Por outro lado, os usuários do site São Paulo não deverão ter acesso a esta impressora, já que ele está geograficamente em outra cidade. Dessa forma, o administrador da rede pode criar uma política de grupo de compartilhamento da impressora somente para os usuários do site Rio de Janeiro.

3.2.2 Criação e gerenciamento

A criação e edição das políticas de grupo podem realizadas clicando no menu **Tool** da janela do Server Manager, selecionando a opção **Group Policy Management**.

Observe, pela Figura 8, que as unidades organizacionais do domínio são exibidas junto aos sites previamente criados:



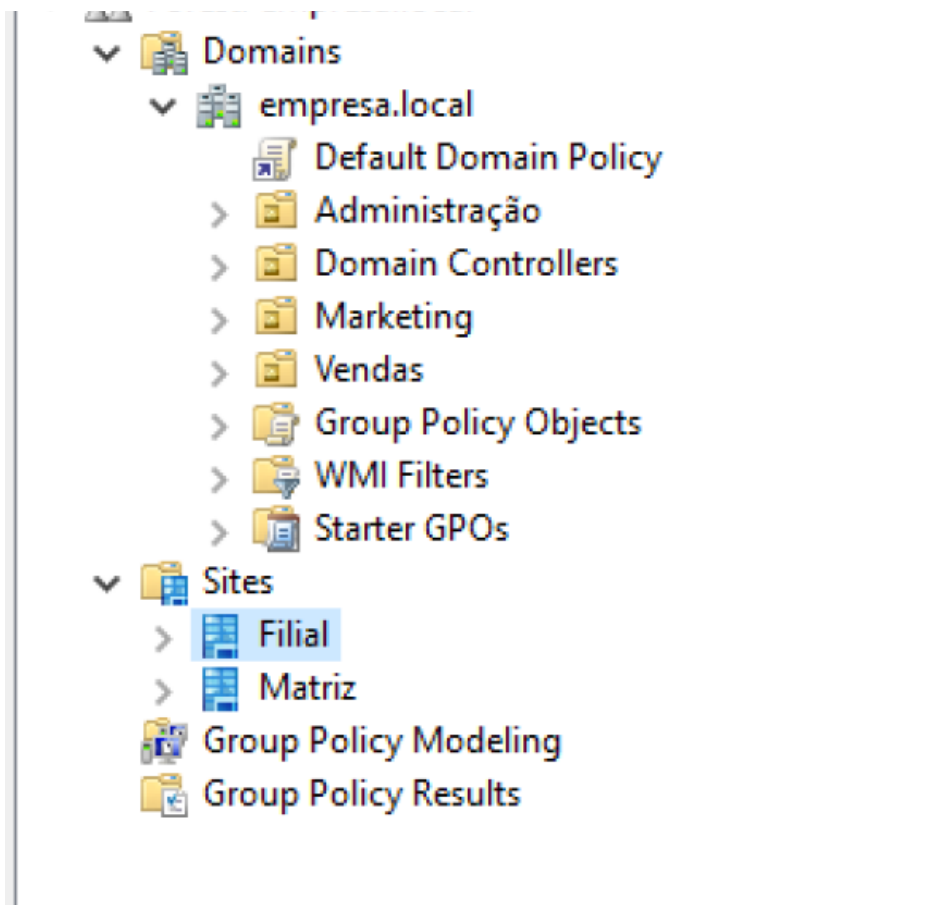


Figura 8 – Captura de tela: exibição das UOs e dos sites presentes no domínio.

Fonte: Elaborada pelo autor, 2020.

Como exemplo, iremos criar uma GPO para proibir o acesso ao painel de controle para todos os usuários do domínio.

Clicando com o botão da direita sobre o nome do domínio, é possível selecionar a opção **Create a GPO in this domain and link it here** (Crie um GPO neste domínio e vincule-o aqui).

Um nome para a nova GPO será solicitado. É aconselhável sempre a indicação de um nome que especifique a função da GPO, como “Proibir acesso ao painel de controle”. O próximo passo é editar a GPO recém-criada. Clicando no botão da direita sobre o nome da GPO, é possível selecionar a opção **Edit** (Editar). É possível criar políticas de grupo que serão aplicadas aos computadores (computer configuration). Neste caso, nos computadores do domínio ou para os usuários do domínio, como apresentado na Figura 9.





Figura 9 – Captura de tela: forma de aplicações de GPO, usuários ou computadores.

Fonte: Elaborada pelo autor, 2020.

Neste caso, as configurações serão aplicadas aos usuários do domínio, mas também é possível indicar uma unidade organizacional. Dessa forma, a política de grupo somente será aplicada à UO definida. Clicando na pasta Policies (Políticas) de User Configuration, será exibida uma série de outras subpastas, como apresentado na Figura 10:

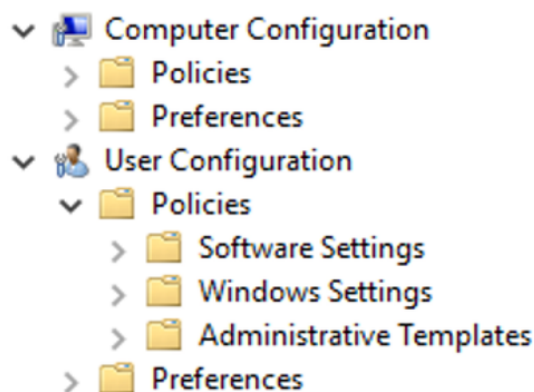


Figura 10 – Captura de tela: organização das GPOs.

Fonte: Elaborada pelo autor, 2020.

As configurações de acesso ao painel de controle estão na pasta Administrative Templates (Modelos administrativos).

Dentro de Administrative Templates é possível encontrar uma pasta com o nome de Control Panel (Painel de controle). Uma das políticas encontradas dentro de Controle Panel é Prohibit access to the control panel and PC settings (Proibir o acesso ao painel de controle e às configurações do PC). Dando um clique duplo em Prohibit access to the control panel and PC settings, é possível editar esta configuração. Selecionando a opção **Enable** (Ativo), a proibição ao acesso do painel de controle será ativada.

Confirmando com o botão **Ok**, a política de grupo será criada e aplicada aos usuários da UO Marketing.



VOCÊ QUER LER?

O universo das políticas de grupo é muito extenso. Como elas, podemos definir de uma simples padronização de papel de parede até o bloqueio de hardware em máquinas. Por ser um campo muito extenso, existem livros e cursos específicos somente para este tema. Uma dica é sempre buscar informação na documentação oficial da Microsoft, disponível no link: < <https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/planning-the-gpos> >.

3.3 FSRM

O Gerenciador de Recursos do Servidor de Arquivos (FSRM) é uma ferramenta em que é possível administrar, no Windows Server, recursos específicos para um servidor de arquivos. Normalmente, em uma empresa, arquivos de uso comum ou arquivos são necessários nos locais onde maiores controles de uso e compartilhamento não são salvos localmente em cada máquina cliente da rede, mas sim em discos específicos controlados pelo servidor de arquivos.

Utilizando os recursos FSRM, é possível definir cotas de uso para cada usuário ou grupo de usuário, classificar e proteger arquivos, para que esses tenham acesso permitido somente para usuários qualificados.

O Gerenciador de Recursos do Servidor de Arquivos fornece um conjunto de funcionalidades que permitem gerenciar e classificar os dados que são armazenados em servidores de arquivos. Entre as novidades, estão a capacidade de limpar os valores de propriedade, que já não se aplicam a um arquivo atualizado durante a reavaliação dos valores de propriedade de classificação existentes e a definição dos valores máximos de relatório de armazenamento. (THOMPSON, 2014, p. 43)

Os principais recursos do FSRM são:

Principais recursos do FSRM

» Clique nas setas ou arraste para visualizar o conteúdo

específico ou em uma pasta. A gerência de cota pode ser aplicada a um usuário específico ou a um grupo de usuários. O gerenciamento permite utilizar modelos pré-definidos para sua utilização;

INFRAESTRUTURA DE CLASSIFICAÇÃO

Permite ao administrador criar políticas de acesso a arquivos com base em processos de classificação. As políticas incluem, além da restrição de acesso, criptografia e monitoramento de alteração de arquivos;

TAREFAS DE GERENCIAMENTO

Permite ao administrador gerenciar a criação e a alteração de arquivos. É possível criar relatórios por data, por exemplo, indicando a alteração e qual usuário realizou a alteração em pastas ou arquivos específicos;

GERENCIAMENTO DE TRIAGENS

Com este recurso é possível controlar quais tipos de arquivos o usuário poderá salvar em determinadas pastas. Por exemplo, o administrador pode criar uma triagem em que arquivos com extensão MP3 não sejam armazenados em pastas pessoais.

É possível, também, criar relatórios de armazenamentos, indicando quanto da cota disponível cada usuário está utilizando.

3.3.1 Instalando o gerenciamento de FSRM

Para que as ferramentas de aplicação de cotas e demais funções do FSRM estejam disponíveis, é necessário instalá-las.

A instalação pode ser realizada no servidor desejado na janela do Server Manager, clicando **Add Role and Feature** . No assistente que será exibido, avançando até Select Server Role, é possível selecionar o item **File Server Resource Manager** , como indicado na Figura 11.

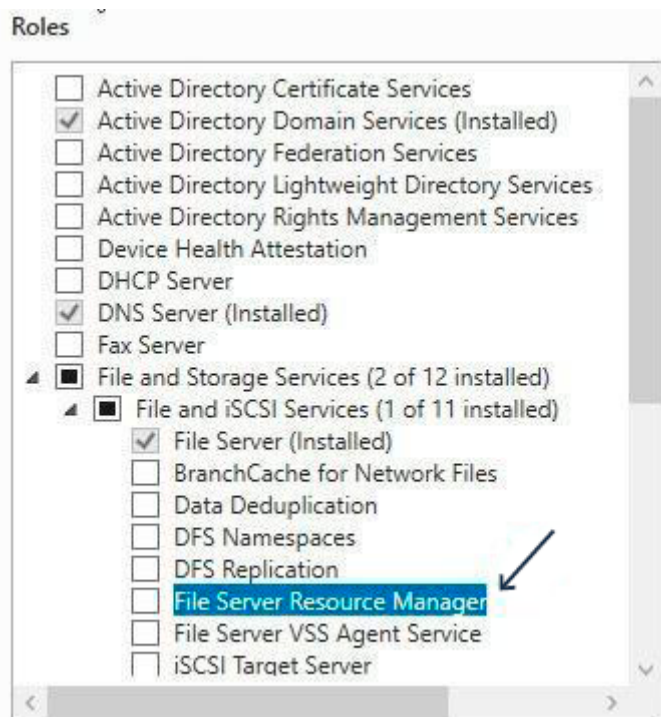


Figura 11 – Captura de tela: recursos para serem instalados para o gerenciamento do servidor de arquivos.

Fonte: Elaborada pelo autor, 2020.

Com o recurso selecionado, basta avançar o assistente até o botão *Install* (instalar) ser exibido. Clicando no botão *Install* , basta aguardar a instalação.

3.3.2 Criando cotas

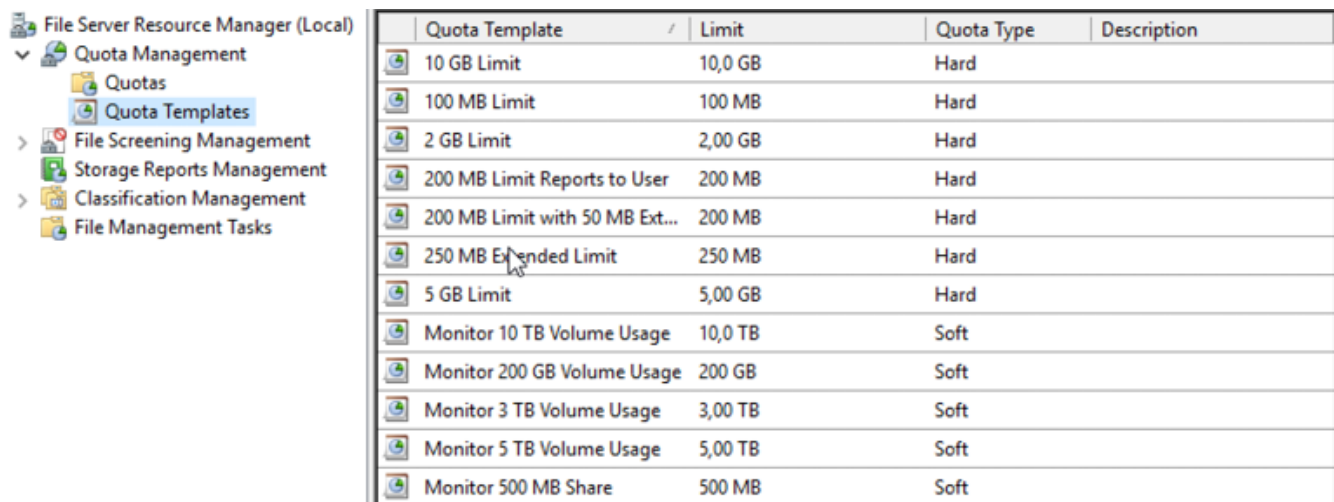
Como exemplo, aplicaremos uma cota de 150 MB para uma pasta compartilhada com o nome de Pública. Esta pasta será compartilhada com todos os usuários do domínio. Todos eles poderão armazenar, no máximo, 150 MB. Esta pasta foi criada e compartilhada na unidade C do servidor SERVERAD-DS. O próximo passo é aplicar a cota de 150 MB.

A configuração deve ser feita acessando o File Server Resource Manager. Isso pode ser feito pela janela do Server Manager, clicando em **Tools** e selecionando **File Server**

Resource Manager .

O próximo passo é abrir o gerenciamento de cotas, clicando em **Quota Management** (Administração de cota).

Antes de aplicar a cota, é necessário criar um “Template” de cota, que será aplicado à pasta Pública. Isso pode ser feito clicando em **Quota Templates** . Observe, pela próxima Figura 12, que já existem alguns templates de cotas pré-definidos.



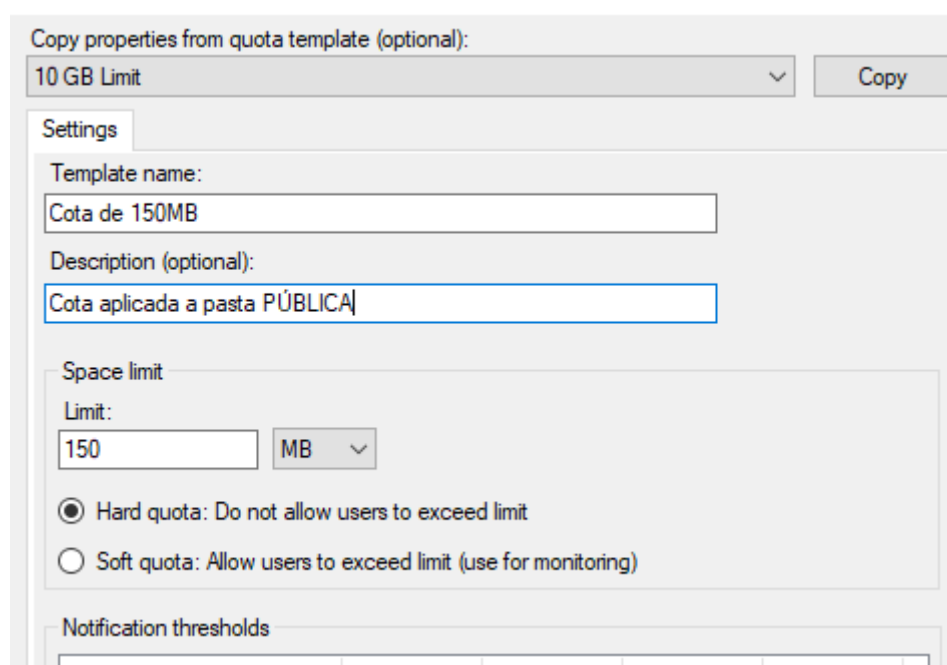
The screenshot shows the File Server Resource Manager (Local) console. On the left, the 'Quota Templates' folder is selected under 'Quota Management'. On the right, a table lists the existing templates.

Quota Template	Limit	Quota Type	Description
10 GB Limit	10,0 GB	Hard	
100 MB Limit	100 MB	Hard	
2 GB Limit	2,00 GB	Hard	
200 MB Limit Reports to User	200 MB	Hard	
200 MB Limit with 50 MB Ext...	200 MB	Hard	
250 MB Extended Limit	250 MB	Hard	
5 GB Limit	5,00 GB	Hard	
Monitor 10 TB Volume Usage	10,0 TB	Soft	
Monitor 200 GB Volume Usage	200 GB	Soft	
Monitor 3 TB Volume Usage	3,00 TB	Soft	
Monitor 5 TB Volume Usage	5,00 TB	Soft	
Monitor 500 MB Share	500 MB	Soft	

Figura 12 – Captura de tela: cotas previamente definidas.

Fonte: Elaborada pelo autor, 2020.

Neste exemplo, apresentado na Figura 13, criaremos nosso próprio template, clicando em Create quota template. Uma nova janela de configuração será exibida, na qual, inicialmente, deve ser especificado o nome do template, uma breve descrição e o valor da cota.



The screenshot shows the 'Create quota template' dialog box. It has a 'Settings' tab. The 'Template name' field contains 'Cota de 150MB'. The 'Description (optional)' field contains 'Cota aplicada a pasta PÚBLICA'. The 'Space limit' section shows a 'Limit' of '150' and a unit of 'MB'. The 'Hard quota' radio button is selected.

Copy properties from quota template (optional):
10 GB Limit [v] [Copy]

Settings

Template name:
Cota de 150MB

Description (optional):
Cota aplicada a pasta PÚBLICA

Space limit

Limit:
150 MB [v]

☒ Hard quota: Do not allow users to exceed limit
☐ Soft quota: Allow users to exceed limit (use for monitoring)

Notification thresholds



Figura 13 – Captura de tela: definição de um novo template.

Fonte: Elaborada pelo autor, 2020.

As cotas podem receber o parâmetro “Hard” ou “Soft”. Selecionando “Hard”, os usuários não poderão armazenar mais de 150MB e serão proibidos de armazenar mais arquivos, caso a cota esteja excedida.

Selecionando “Soft”, o administrador da rede receberá um aviso de cota excedida (um log será criado), mas o usuário não será proibido de armazenar novos arquivos. Clicando em **Ok**, o template será criado. O próximo passo é aplicar a cota à pasta Pública. Clicando em **Quotas** e, posteriormente, selecionando **Create Quota**, um novo assistente será exibido.

Em “Quota Path”, referenciado na Figura 14, indica-se o caminho da pasta C:\PÚBLICA e selecione-se o template Cota de 150Mb.

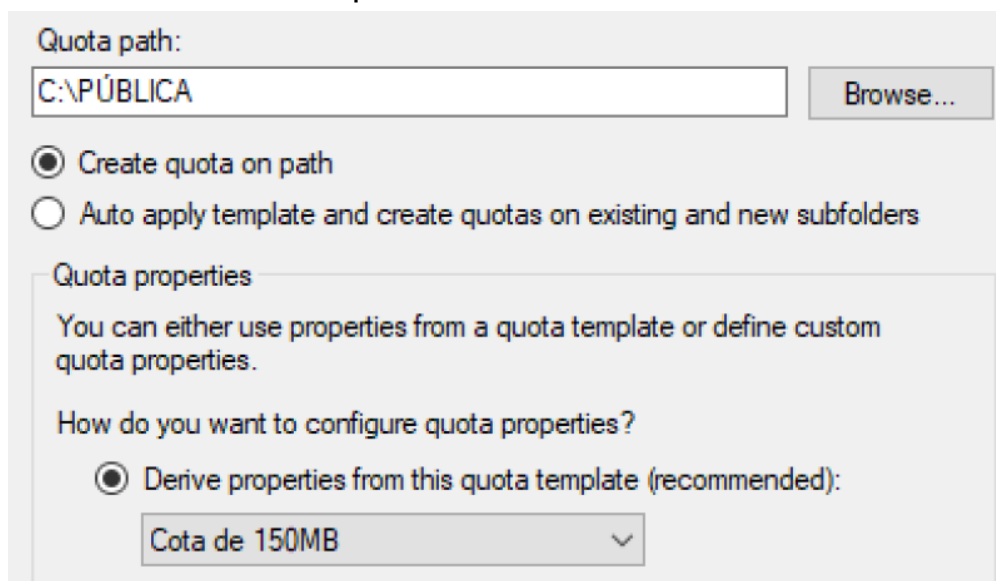


Figura 14 – Captura de tela: definição da pasta e template.

Fonte: Elaborada pelo autor, 2020.

Clicando em **Ok**, a cota será aplicada à pasta selecionada. Nos mapeamentos feitos aos usuários com acesso à pasta pública, todos os usuários terão uma cota máxima de 150MB para armazenar arquivos.

3.4 DNS

Todo computador em uma rede, seja ela uma rede interna (intranet) ou uma rede externa, como a internet, possui um endereço, uma identificação conhecida por IP (Internet Protocol). Normalmente, um computador não é referenciado por sua numeração IP, mas pelo seu nome. Com o Active Directory instalado, o serviço de DNS é automatizado, ou seja, toda vez que um novo computador ingressa no domínio, ele automaticamente é ingressado com um novo registro DNS.

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).

Exemplo: caso uma máquina possua o nome MKT1, possua o IP 192.168.100.50 e seja ingressada no domínio **empresa.local**, automaticamente o registro **MKT1.empresa.local** é criado, apontando para o IP 192.168.100.50.

Da mesma forma, os servidores da rede com os nomes SERVERAD-DS e SERVERAD-DS2 são referenciados apontando para os seus respectivos IPs. Para visualizar este cenário com o uso do Active Directory, no Server Manager, clique em **Tools** e selecione **DNS**.

Observe, na Figura 15, que temos a indicação do nome do servidor DNS, SERVERAD-DS e, na pasta Forward Lookup Zone, temos o domínio **empresa.local**. Clicando sobre o domínio, temos todas as ponteiros criados automaticamente.

(same as parent folder)	Start of Authority (SOA)	[132], serverad-ds.empres...	static
(same as parent folder)	Name Server (NS)	serverad-ds.empresa.local.	static
(same as parent folder)	Host (A)	10.0.0.60	12/06/2020 14:00:00
(same as parent folder)	Host (A)	192.168.100.10	12/06/2020 14:00:00
(same as parent folder)	Host (A)	192.168.100.11	27/05/2020 00:00:00
(same as parent folder)	IPv6 Host (AAAA)	2804:4800:1150:007f:bc6b:...	12/06/2020 14:00:00
MKT1	Host (A)	192.168.100.50	12/06/2020 14:00:00
serverad-ds	Host (A)	192.168.100.10	static
serverad-ds	Host (A)	10.0.0.60	static
serverad-ds	IPv6 Host (AAAA)	2804:4800:1150:007f:bc6b:...	static
SERVERAD-DS2	Host (A)	192.168.100.11	27/05/2020 00:00:00



Figura 15 – Captura de tela: registros automaticamente criados pelo AD.

Fonte: Elaborada pelo autor, 2020.

Observe, pela Figura 15, que os registros dos endereçamentos IP para os computadores e servidores do domínio são referenciados pelo nome dado aos computadores na instalação, ou quando adicionados a um domínio. Este nome de computador é chamado de FQDN (Nome de domínio totalmente qualificado). Por exemplo, se um computador com o nome MKT1 ingressar no domínio **empresa.local**, o FQDN do computador será **MKT1.empresa.local**.

3.4.1 Zonas de DNS

As zonas são áreas que armazenam informações de nome sobre um ou mais domínios DNS. Todas as informações adicionadas a uma zona DNS são incrementadas na forma de registros. Para cada nome de DNS presente, as zonas serão as responsáveis em responder às requisições inerentes ao domínio. Por exemplo, uma requisição para o nome **MKT1.empresa.local** foi feita a um servidor DNS. O ponteiro MKT1 pertence à zona **empresa.local**, que terá a responsabilidade de retornar o número IP do ponteiro MKT1.

O serviço de DNS, incorporado ao Active Directory, possui dois tipos de zonas DNS.

Tipos de zonas DNS

» Clique nas setas ou arraste para visualizar o conteúdo

ponteiros. As zonas primárias são criadas automaticamente quando promovemos um servidor a controlador de domínio. Todo serviço de DNS precisa, ao menos, possuir uma zona primária para a edição de novos ponteiros;

ZONA SECUNDÁRIA

as informações referentes ao DNS neste servidor estarão vinculadas às diretivas do servidor primário.

ZONA STUB

As zonas de stub são como uma zona secundária, mas apenas armazenam dados de zona parciais. Essas zonas são úteis para ajudar a reduzir as transferências, passando as solicitações para servidores autoritativos. Essas zonas contêm apenas os registros SOA, NS e A.



VOCÊ QUER VER?

Para entender melhor como é o funcionamento do DNS, com mais detalhes sobre zonas de pesquisa e registros, assista ao vídeo *A importância do DNS nas redes explicada pelo NIC.br*:

» Zona de pesquisa direta (Forward Lookup Zone)

As zonas de pesquisa direta (Forward Lookup Zone) são as zonas responsáveis por resolver nomes de computadores em números Ips. Por exemplo, uma requisição é feita ao servidor DNS pelo nome Serverad-ds pertencente ao domínio **empresa.local** . O servidor DNS irá retornar o seu endereçamento IP, por exemplo, 192.168.100.10.

» Zona de pesquisa inversa

As zonas de pesquisa inversa resolvem os endereços IP em nomes de host. Por exemplo, quando é consultado o IP 192.168.100.10, o servidor irá resolver para **serverad-ds.empresa.local** . Um registro DNS reverso teve que ser criado para que a requisição pelo número IP fosse resolvida em nome do host.

3.4.2 Criando uma zona de pesquisa direta primária

O servidor DNS, demonstrado na Figura 15, é o responsável por responder as requisições feitas para o domínio **empresa.local** . Suponhamos que este mesmo servidor também seja o responsável por responder às requisições para o domínio empresa.com.br. Neste caso, será necessário criar uma nova zona de pesquisa primária.

Clicando com o botão da direita sobre a pasta Forward lookup zone, é possível selecionar a opção *New zone* (Nova Zona).

Um novo assistente será exibido. Clicando em **Next** , a primeira coisa a ser definida será o tipo de zona a ser criada. Neste caso, criaremos uma zona de pesquisa primária (Primary zone), pois todas as atualizações de registros DNS serão feitas neste servidor.

Zone Type

The DNS server supports various types of zones and storage.



Select the type of zone you want to create:

☒ Primary zone

Creates a copy of a zone that can be updated directly on this server.

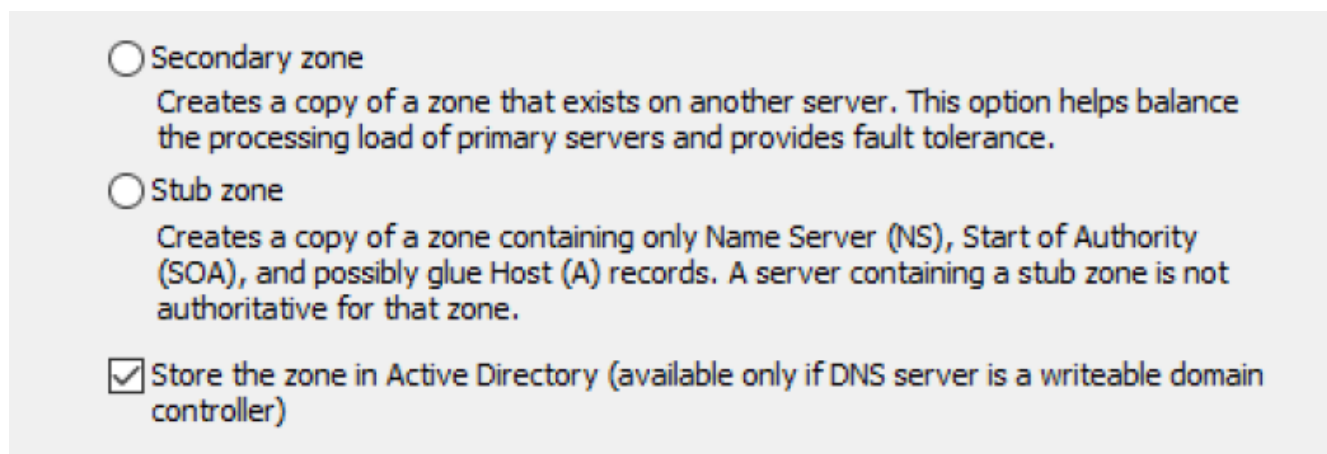


Figura 16 – Captura de tela: definição do tipo de zona DNS.

Fonte: Elaborada pelo autor, 2020.

O próximo passo é selecionar quais servidores replicarão as informações desta nova zona DNS. Como estamos utilizando o Active Directory, neste exemplo será selecionada a opção *To All DNS Servers running on domain controllers in the domain : **empresa.local*** (Para todos os servidores executando como controladores de domínio no domínio empresa.local). Isto fará com que a replicação destas novas informações seja feita em todos os servidores controladores de domínio do domínio **empresa.local**.

O próximo passo é indicar o nome da zona. Neste exemplo, foi indicado o nome empresa.com.br. A seguir é definido como serão as atualizações dos registros para esta nova zona DNS. Vamos deixar uma atualização dinâmica, utilizando o Active Directory. Deixe a opção padrão selecionada: selecione *Allow only secure dynamics updates (Recommended for Active Directory)* – em português, “Permitir apenas atualizações dinâmicas (Recomendado para Active Directory)”.

Clicando em **Next**, temos o botão **Finish**, para finalizar a criação da nova zona DNS.

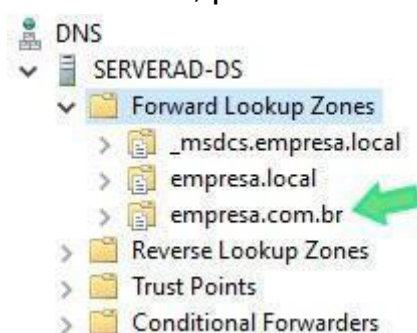


Figura 17 – Captura de tela: nova zona de DNS criada.

Fonte: Elaborada pelo autor, 2020.

Temos a nova zona DNS, mas o próximo passo é criar os registros. Inicialmente vamos conhecer quais são os tipos de registros.

3.4.3 Tipos de registros

Os registros são as informações armazenadas dentro de uma zona DNS, que terão as referências para a resolução dos nomes. Os principais tipos de registros que podem ser armazenados em uma zona DNS são:

A: Os registros do tipo A, também chamados de ponteiros ou hosts, são os principais tipos de registro dentro de uma zona primária em um servidor DNS. Esse tipo de registro amarra um endereço IP a um nome de domínio.

AAAA: Este tipo de registro tem a mesma função do registro do tipo A, porém faz a vinculação de um nome DNS para um endereço IPv6.

AFSDB: Este tipo de registro em um servidor DNS é utilizado para vincular um nome de domínio a um servidor de banco de dados.

CNAME: Usado para indicar um outro nome para um ponteiro um registro do tipo A ou AAAA. É uma forma de redirecionamento. Por exemplo, `www.empresa.local` pode direcionar para `example.local`.

MX : Este tipo de registro em um servidor DNS é utilizado para vincular-se ao servidor de e-mails.

PTR: Registro utilizado para fornecer o DNS reverso. Os registros PTR atribuem endereços IP a um nome.

SOA: É o registro mais importante do DNS. A sigla significa Start of Authority. Indica o responsável por respostas autoritárias a um domínio, ou seja, o responsável pelo domínio. Indica o endereçamento IP do servidor DNS principal.

3.4.4 Criando um novo registro

Anteriormente, criamos uma nova zona de pesquisa direta para o domínio empresa.com.br. Suponhamos que, nesta infraestrutura, haja um servidor web hospedando um website, com o endereçamento IP 192.168.100.13.

Como visto, o registro de um host pode ser realizado com o registro AA. Poderíamos dar o nome deste registro de www. Dessa forma, teríamos o nome FQDN www.empresa.com.br.

Serão apresentadas, sobre a zona empresa.com.br, as opções tipo de registro que poderão ser criadas, como apresentado na Figura 18.

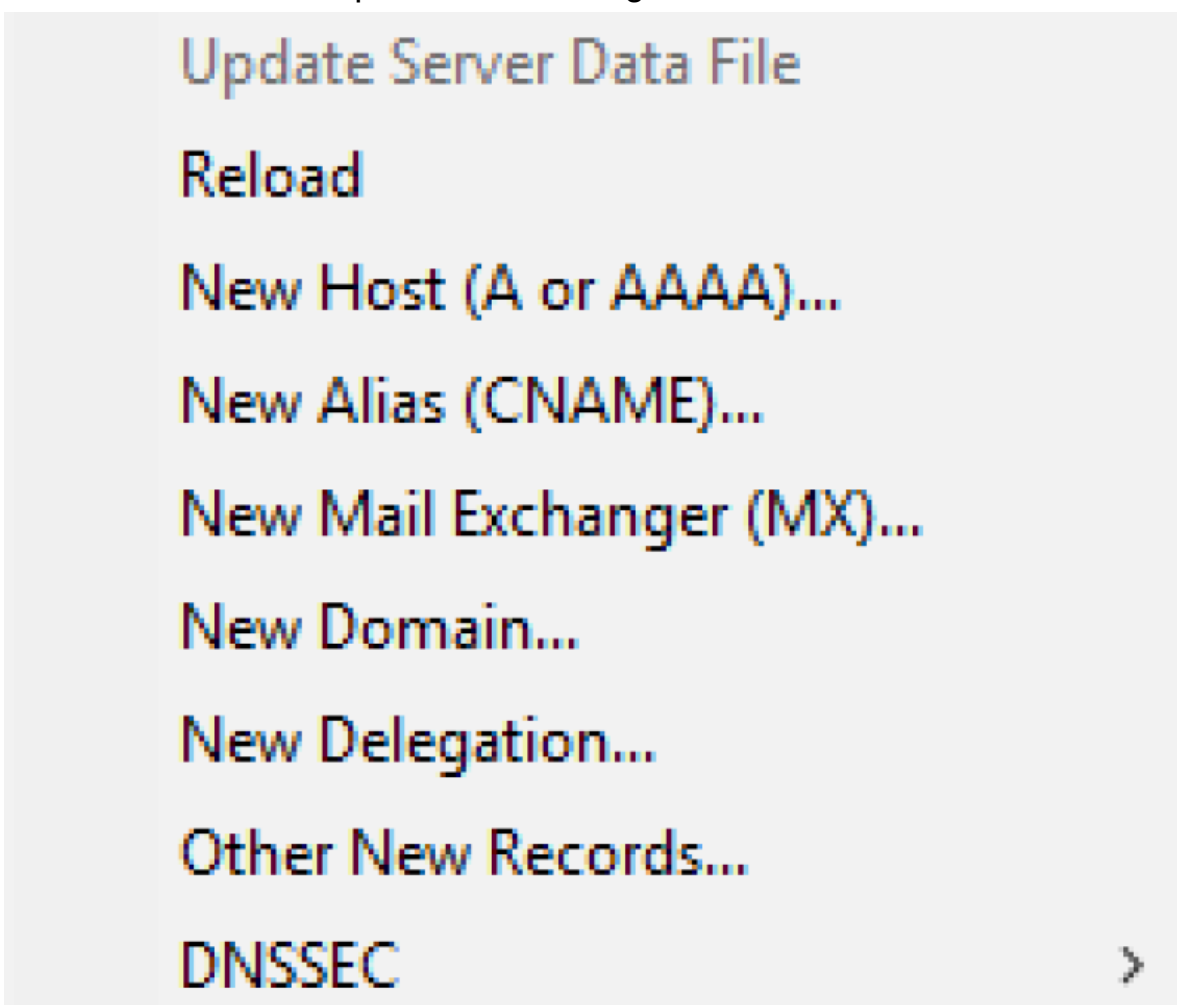


Figura 18 – Captura de tela: definição do tipo de registro.

Fonte: Elaborada pelo autor, 2020.

Neste exemplo, é selecionado New Host (A or AAAA).

O nome do host deve ser indicado em Name. Neste exemplo, foi indicado o nome www e o seu endereçamento IP deve ser indicado em IP address, como indicado na Figura

19:

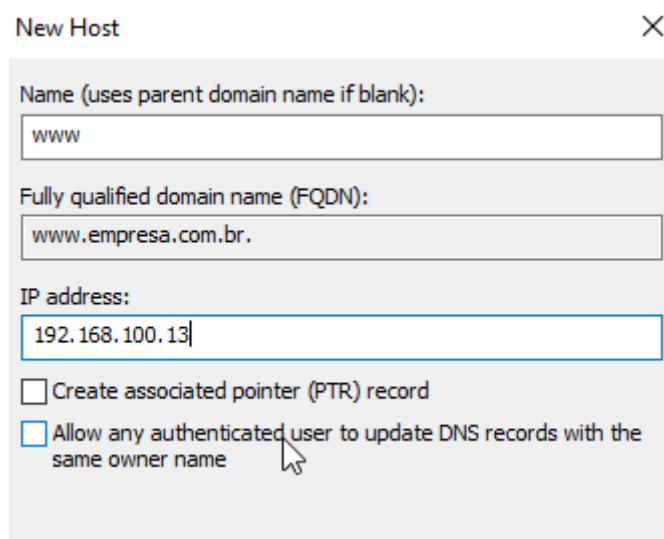
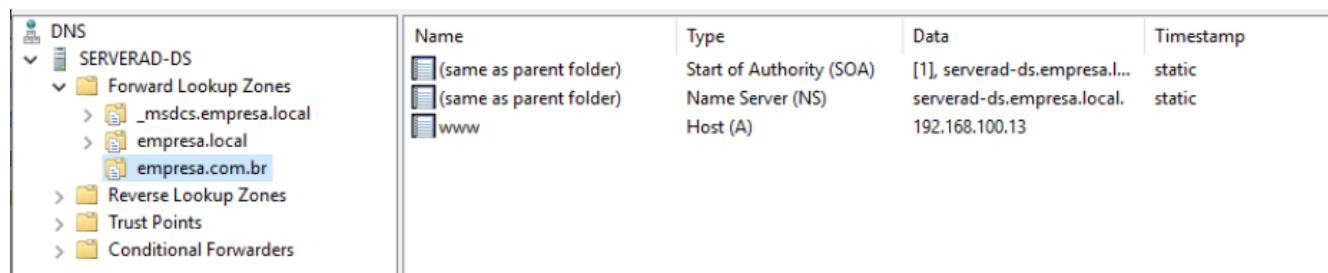


Figura 19 – Captura de tela: configurações do novo registro.

Fonte: Elaborada pelo autor, 2020.

Clicando em **Ok** , temos o novo host DNS para a zona primária empresa.com.br. Qualquer requisição feita pelo nome www ao domínio empresa.com.br será retornado o seu endereçamento IP.



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], serverad-ds.empresacombr.local	static
(same as parent folder)	Name Server (NS)	serverad-ds.empresacombr.local	static
www	Host (A)	192.168.100.13	

Figura 20 – Captura de tela: exibição do novo registro.

Fonte: Elaborada pelo autor, 2020.

Um teste de funcionamento pode ser feito pelo comando ping e indicando o nome do host. O servidor DNS deve retornar o endereçamento IP correto.

```
C:\Users\administrator>ping www.empresacombr  
Disparando www.empresacombr [192.168.100.13] com 32 bytes de dados:
```

Figura 21 – Captura de tela: utilização do comando ping.

Fonte: Elaborada pelo autor, 2020.

Observe que, após a consulta ao servidor DNS do endereço www.empresacombr, houve o retorno do IP correto definido na configuração do novo registro.

Síntese

Vimos, nesta unidade, que o administrador deve estar ciente da infraestrutura que ele administrará. O Windows Server apresenta ferramentas para organizar logicamente essa infraestrutura. Com os sites, é possível realizar essa tarefa, mas caberá sempre ao administrador definir a melhor forma de organização e replicação das informações. Também vimos que o Active Directory irá solucionar a grande maioria das atividades relacionadas ao DNS de uma empresa, mas novamente caberá ao administrador adicionar novas zonas de DNS e novos registros, caso seja necessário.

Para finalizar, entendemos que, em uma empresa, políticas de segurança são necessárias para o bom funcionamento de todos os recursos. As políticas de grupos do Windows Server são ferramentas essenciais para essas atividades.

Referências bibliográficas

A IMPORTÂNCIA do DNS nas redes, explicada pelo NIC.br Postado por NIC.br. 8 min 59 s. son. color. port. Disponível em: < <https://www.youtube.com/watch?v=epWv0-egRMw> >. Acesso em: 27 jul. 2020.

FRANCIS, D. **Mastering Active Directory** . 2. ed. Birmingham: Packt Publishing Ltd, 2017.

MICROSOFT. **Criar um design de link de site** . 2020. Disponível em: < <https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/plan/creating-a-site-link-design> >. Acesso em 25 jun. 2020.

SERAGGI, M. R. **Windows server 2016** . 1. ed. São Paulo: Editora Senac, 2019.

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. 2ª ed. São Paulo: Érica, 2014.
