Unidade V

5 DOMÍNIO *VERSUS* GRUPO DE TRABALHO

Battisti e Popovici (2015) afirmam que o Windows Server 2012 R2 pode ser utilizado de duas formas distintas. Segundo eles, pode-se trabalhar com essa versão do servidor em Workgroup e Domínio.

> Uma rede baseada no Windows Server 2012 R2 pode ser criada utilizando-se dois conceitos diferentes, dependendo da maneira com que os Servidores Windows Server 2012 R2 são configurados. Os servidores podem ser configurados para fazerem parte de um Domínio ou de um Grupo de Trabalho, mais comumente chamado de Workgroup (BATTISTI; POPOVICI, 2015, p. 47).

A diferença básica entre os dois modelos está na forma de gerenciamento e armazenamento. Em um ambiente Workgroup, as contas de usuários e todos os recursos administrativos estão distribuídos nos servidores que compõem a rede. Dessa forma, a administração se torna distribuída, aumentando o esforço administrativo para o gestor de TI e reduzindo a segurança do ambiente.

Já em um ambiente de Domínio, toda a estrutura administrativa (contas de usuários, grupos, políticas etc.) é armazenada em um ponto central (servidores com funções específicas), facilitando a administração e reduzindo o esforço administrativo do gestor de TI e da equipe técnica, além de aumentar a segurança de todo o ambiente.

Em um domínio, será necessário ter pelo menos um servidor para manter o banco de dados que armazenará todos os objetos necessários ao funcionamento do ambiente. Esse banco é baseado em um padrão conhecido como LDAP (Lightweight Directory Access Protocol) e é chamado de **NTDS.DIT**. Por padrão, fica armazenado em uma pasta dentro da pasta do Sistema Operacional (c:\windows\ntds).

Desde o Windows 2000, para gerenciar toda essa estrutura de uma maneira mais organizada (hierárquica), a Microsoft agregou ao ambiente de domínio o serviço do Active Directory, também baseado no protocolo LDAP, que tem como principal característica possibilitar a estruturação do ambiente de forma hierárquica, permitindo ao administrador organizar sua estrutura dividindo o ambiente por localidade, funções etc.

Observação

O servidor que armazena o banco de dados é conhecido como controlador de domínio e **não pode** ser configurado em uma versão cliente do Windows.

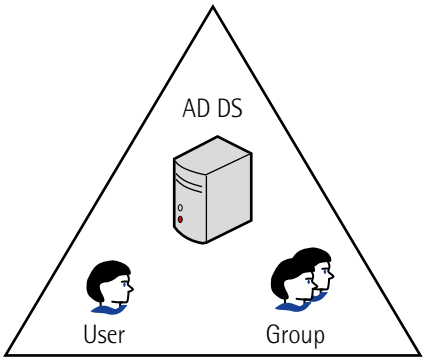

Figura 100 – Domínio do Active Directory

Conforme exibido na figura anterior, um domínio sempre será representado pela imagem de um triângulo, que simboliza o grupo ou conjunto de recursos. O Controlador de Domínio (DC) é o servidor em que o banco de dados com os objetos será armazenado, e os objetos representarão os recursos disponíveis no domínio em questão.

Ao ser configurado o primeiro domínio de uma infraestrutura, junto com ele serão configurados alguns outros recursos importantes para o funcionamento do domínio, conhecidos como floresta e árvore de domínio.

Ainda segundo Battisti e Popovici (2015), uma floresta é uma coleção de domínios com Schema e configuração compartilhados, representado por um único e lógico Global Catalog (GCs) e conectado por uma árvore dispersa de relações de confiança transitivas. Uma floresta é representada por um domínio-raiz de floresta.

Essa estrutura será responsável pela organização e pelo controle administrativo de todo o ambiente.

5.1 Instalando um domínio do Active Directory

Nos passos a seguir, será demonstrada a instalação de um domínio do Active Directory. Nessa etapa, o servidor já se encontra configurado com um IP fixo. O nome do servidor já foi definido, portanto o procedimento será iniciado a partir do processo de instalação da função do **Serviço de Domínio do Active Directory** (AD DS, sigla em inglês do serviço).

Para iniciar a sequência de procedimentos, deve-se estar logado com um usuário administrador local do servidor e iniciar a ferramenta Gerenciador do Servidor. A partir daí, deverão ser seguidos os passos apresentados neste subtópico. Eles serão divididos em duas etapas: instalação da função AD DS e, posteriormente, configuração do domínio.

5.1.1 Instalando a função AD DS

- **Passo 1:** no Gerenciador do Servidor, selecione o menu **Gerenciar** e a opção **Adicionar Funções e Recursos**, conforme exibido na figura seguinte.

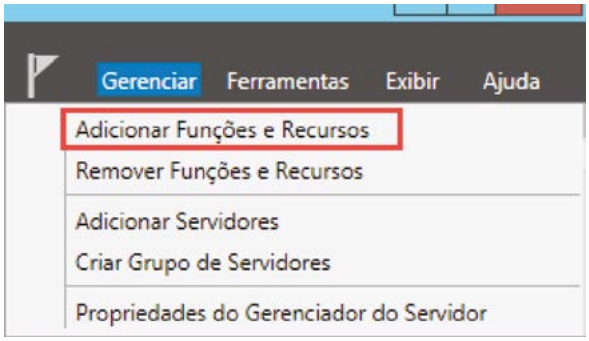

Figura 101 – Adicionando funções

- **Passo 2:** após clicar três vezes no botão **Próximo**, selecione na lista a função **Serviço de Domínio do Active Directory**, conforme exibido na figura a seguir.

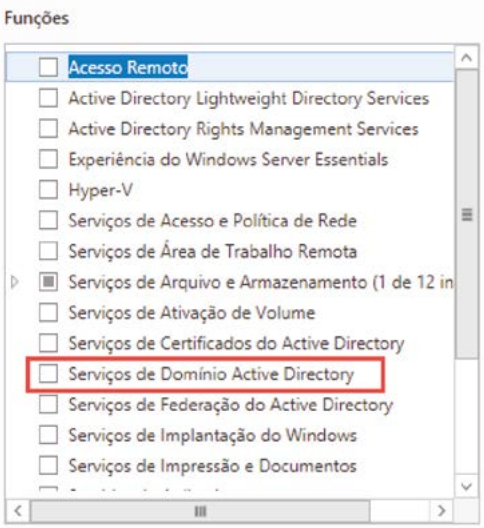

Figura 102 – Lista de funções

- **Passo 3:** confirme a adição das ferramentas administrativas do Active Directory clicando no botão **Adicionar Recursos** e, em seguida, clique três vezes no botão **Próximo**. Para concluir, clique no botão **Instalar**.

Essa sequência de procedimentos irá instalar a função do Serviço de Diretório do Active Directory. Feito isso, deve-se iniciar a segunda etapa de procedimentos, em que o servidor será promovido para um controlador de domínio.

Para executar essa tarefa, seguir estes passos:

- **Passo 1:** na tela que conclui a instalação da função, clique no *link* **Promover este servidor a um controlador de domínio**, conforme exibido na próxima figura.

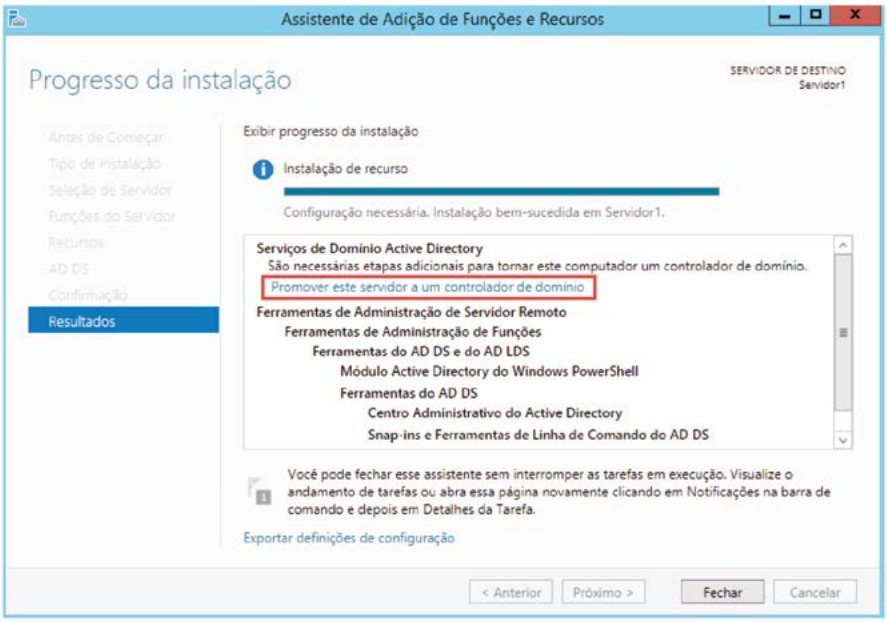

Figura 103 – Promovendo controladores de domínio

- **Passo 2:** para dar início à criação do primeiro domínio da floresta, selecione a opção **Adicionar uma nova floresta** e informe o nome do domínio que será criado. Feito isso, clique em **Próximo** para continuar o procedimento, conforme exibido na figura a seguir.

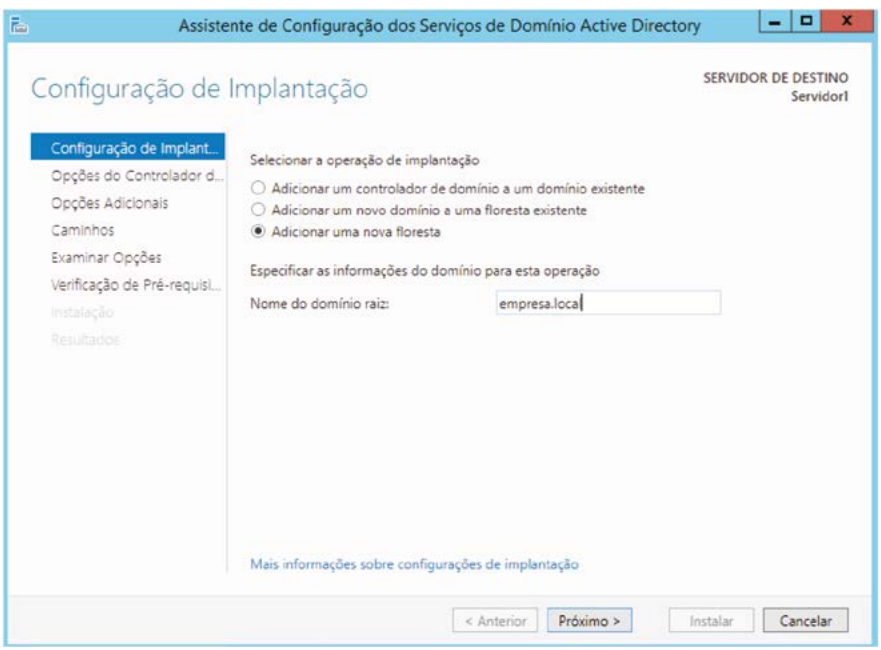

Figura 104 – Nova floresta

- **Passo 3:** mantenha a configuração-padrão e informe uma senha para o modo de restauração do serviço de diretório (essa senha deverá ser usada em caso de solução de problemas do AD, quando o servidor deverá ser reiniciado no modo de segurança).

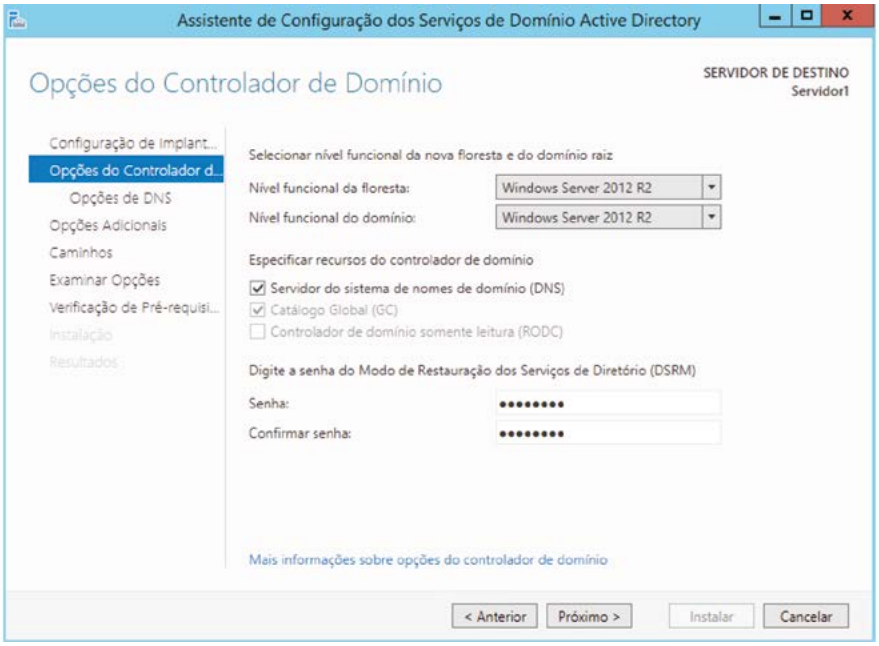

Figura 105 – Opções do controlador de domínio

- **Passo 4:** clique cinco vezes em **Próximo** e, então, clique no botão **Instalar** para dar início à promoção do servidor para controlador de domínio, conforme exibido na figura seguinte.

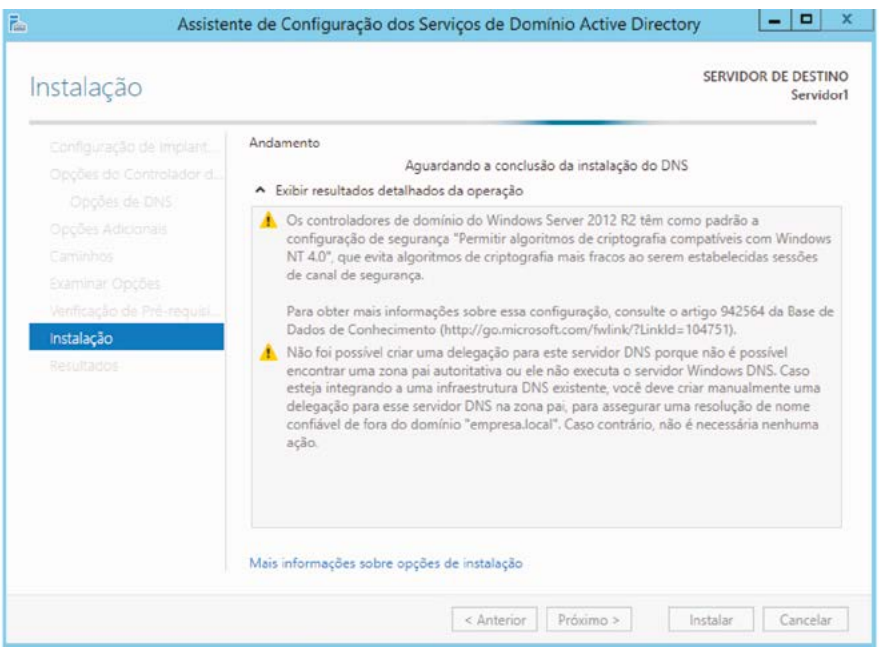

Figura 106 – Instalação do controlador de domínio

Após esse processo, o servidor irá reiniciar automaticamente para concluir a promoção do domínio e, então, essa tarefa estará concluída.

A partir desse momento, o servidor configurado para controlador de domínio deixará de possuir contas locais e passará a ter todas as suas contas de usuários armazenadas no banco de dados do Active Directory (NTDS.DIT). Assim, deve-se logar usando a conta de domínio, e não mais a conta local do administrador, conforme exibido na figura seguinte.

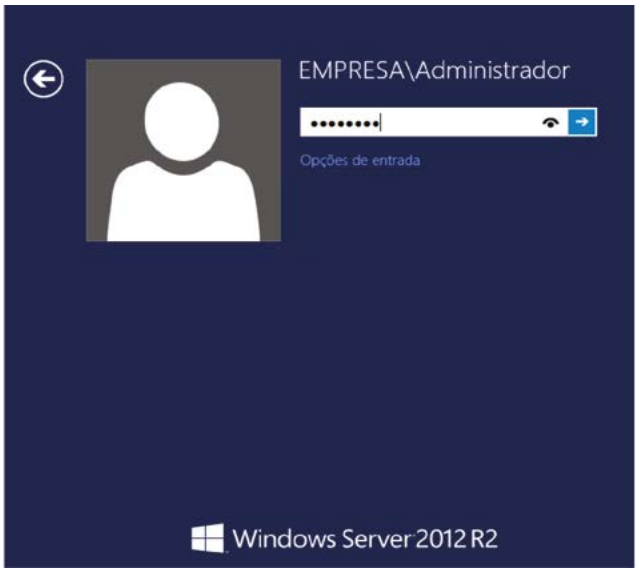

Figura 107 – Logando no controlador de domínio

A partir do Gerenciador do Servidor, pode-se observar que a instalação do Active Directory foi efetuada com sucesso e que o serviço está instalado, conforme exibido na figura seguinte.

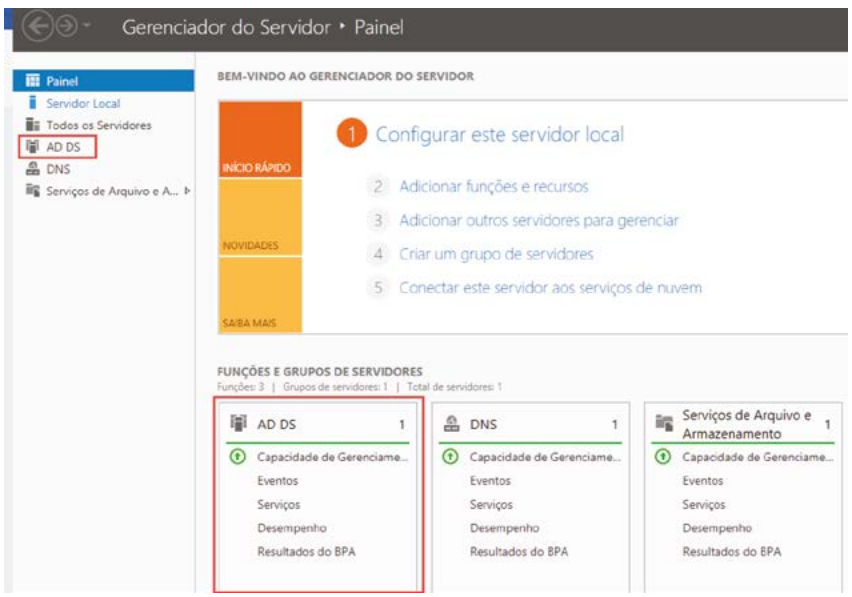

Figura 108 – Gerenciador do Servidor: ADDS

Lembrete

Todas as contas de usuários do domínio são armazenadas no banco de dados do Active Directory (NTDS.DIT)

O servidor de DNS também será configurado automaticamente para manter todo o ambiente configurado. Ferramentas para gestão do serviço estarão disponíveis para a gestão no Menu Ferramentas, no Gerenciador do Servidor do Windows 2012 R2, conforme exibido na figura a seguir.

Figura 109 – Ferramentas do Active Directory

5.1.2 Instalando um servidor-réplica do Active Directory

Uma réplica do controlador de domínio é também conhecida como um controlador de domínio adicional. Garantirá a disponibilidade do serviço na eventual falha de um dos servidores.

De acordo com Tanenbaum (2011, p. 48), em um ambiente de redes, é necessário manter a redundância dos serviços críticos para garantir a sua eficiência.

Pensando dessa forma, recomenda-se que, para todos os servidores da rede, ou pelo menos para os mais críticos, sejam criadas réplicas – uma cópia ativa, garantindo que, na falha de um dos servidores, sua cópia mantenha os serviços funcionando e disponíveis para os usuários.

Apesar de ser possível criar réplicas do controlador de domínio do Active Directory entre servidores com versões diferentes do Windows, é bastante recomendado que essas réplicas sejam feitas sempre com servidores de mesma versão e arquitetura, para assegurar a uniformidade dos recursos oferecidos na rede.

Para criar uma réplica, deve-se atentar para algumas preocupações especiais. Dentre elas, as mais importantes são:

- a réplica deve comunicar-se com o outro controlador de domínio;
- no servidor-réplica, o DNS preferencial na placa de rede deve apontar para o servidor DNS onde estão os registros de domínio;
- deve-se garantir que nenhum *firewall* ou serviço de segurança impeça a comunicação entre os servidores.

Para executar a configuração da réplica, executar as tarefas a seguir:

- **Passo 1:** no servidor-réplica, no Gerenciador do Servidor, instale a função **Serviços de Domínio do Active Directory** a partir do menu Gerenciar, conforme exibido na figura a seguir.

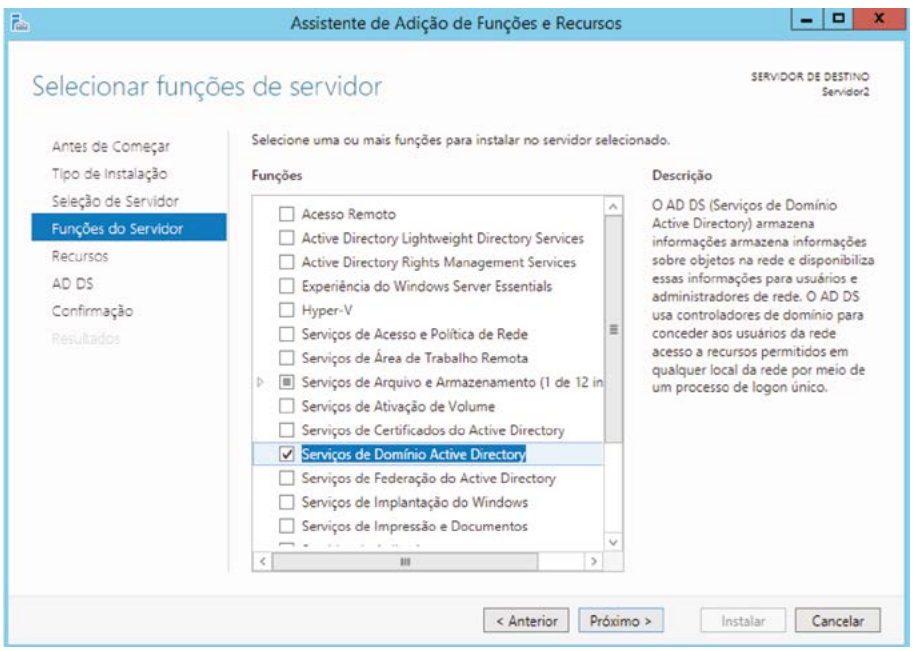

Figura 110 – Assistente de adição de funções

- **Passo 2:** clique três vezes no botão **Próximo** e, em seguida, no botão **Instalar** para concluir a instalação da função no servidor que será configurado como réplica.
- **Passo 3:** perceba que, até este momento, o procedimento é o mesmo executado no primeiro servidor, ou seja, após a instalação da função, você deverá clicar no *link* **Promover este servidor a um controlador de domínio** para iniciar o processo de promoção, conforme exibido na figura seguinte.

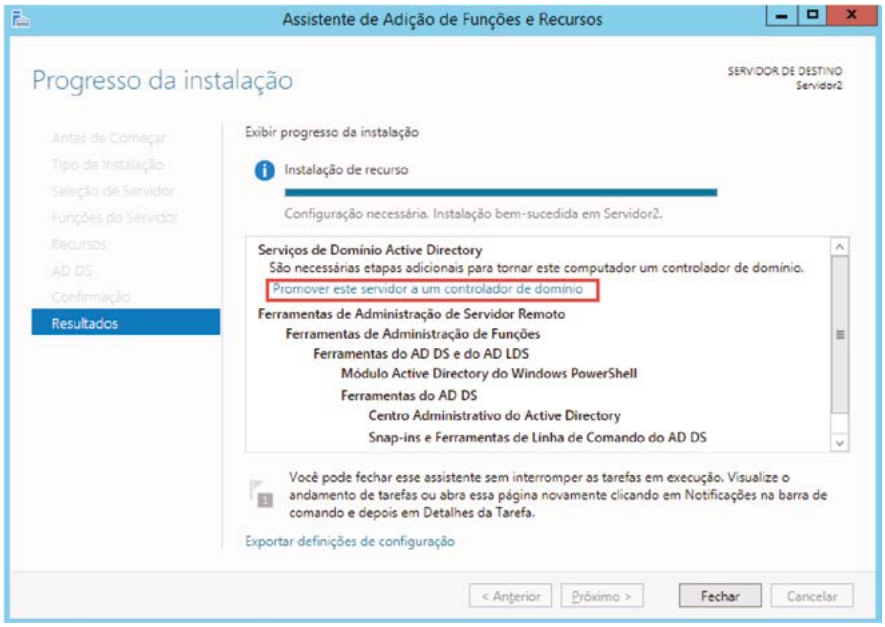

Figura 111 – Promovendo um controlador de domínio-réplica

A partir de agora, será notada a diferença de configuração entre a etapa passada, em que foi configurado um novo controlador de domínio, e este momento, em que será configurado um servidor-réplica para esse mesmo domínio.

- **Passo 1:** após clicar no *link* **Promover este servidor a um controlador de domínio**, conforme exibido na figura seguinte, selecione a opção **Adicionar um controlador de domínio a um domínio existente**. Informe o nome do domínio ao qual o servidor será associado e o nome de usuário administrador e a senha do domínio em questão.

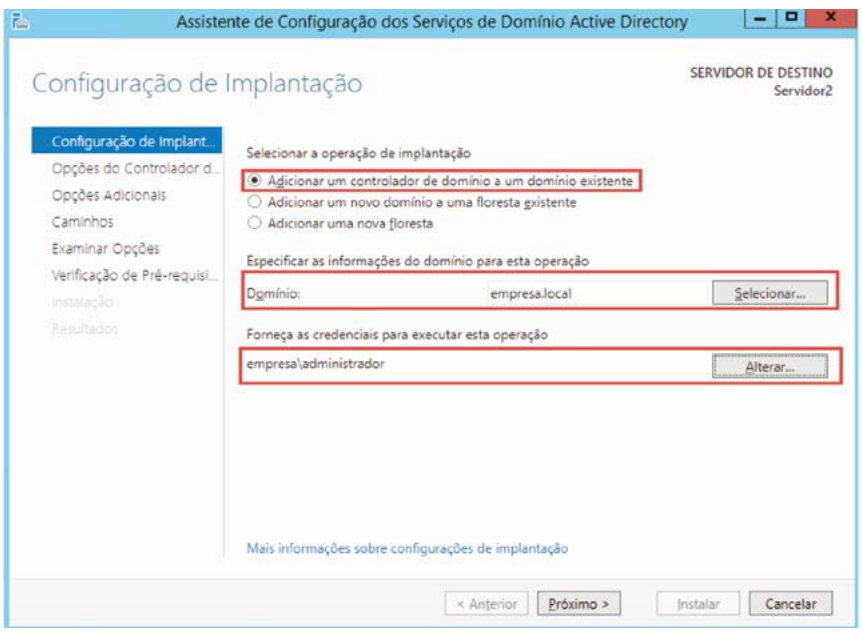

Figura 112 – Configuração da réplica

- **Passo 2:** após clicar em **Próximo**, conforme exibido na figura seguinte, mantenha as informações-padrão da tela seguinte e informe apenas a senha para o administrador do modo DSRM, que preferencialmente não deveria ser a mesma senha do administrador do domínio.

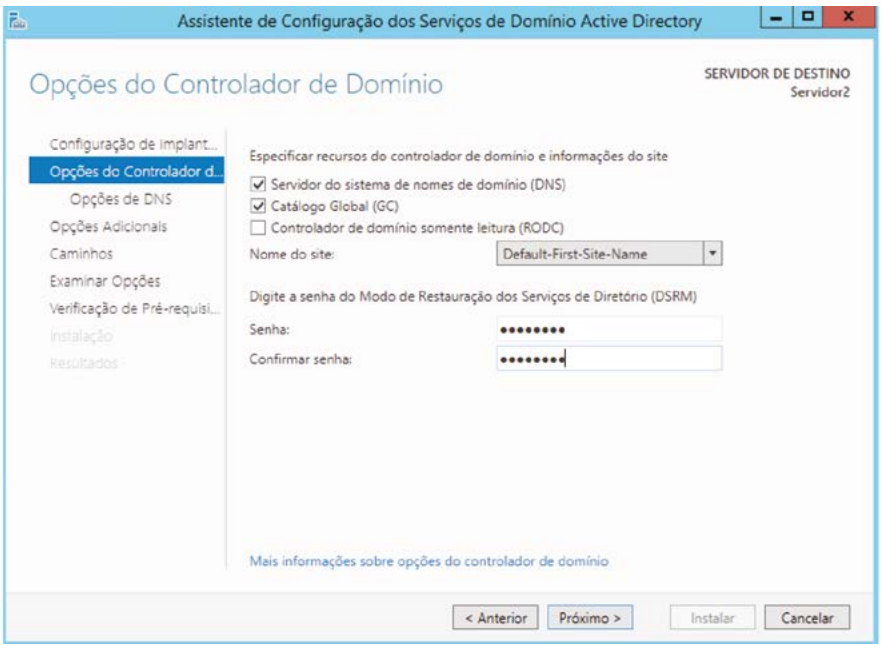

Figura 113 – Definindo funções da réplica

- **Passo 3:** após preencher as informações importantes mostradas na tela da figura anterior, clique cinco vezes no botão **Próximo** e, em seguida, clique no botão **Instalar** para concluir a promoção do servidor-réplica, conforme exibido na figura a seguir.

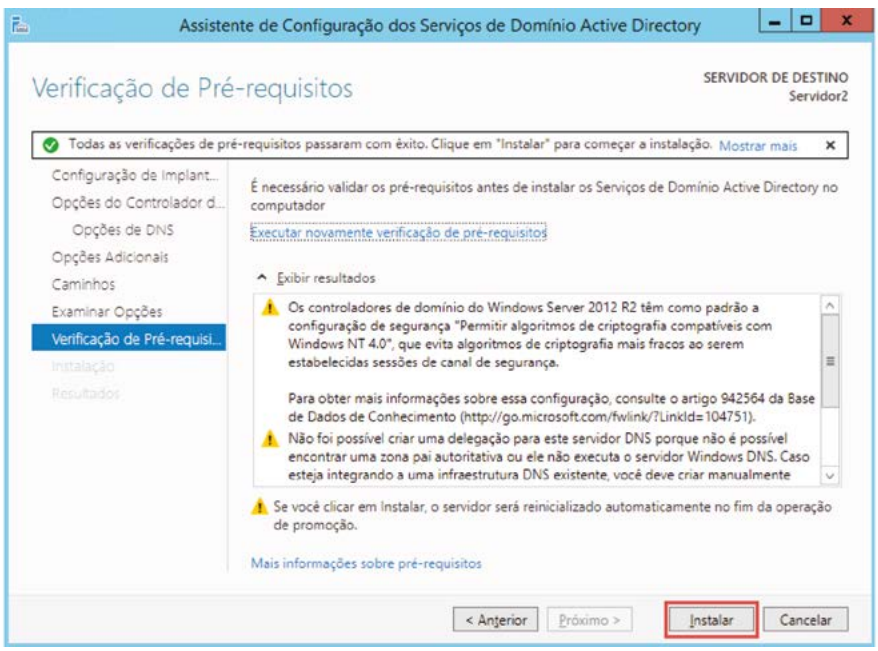

Figura 114 – Verificação de pré-requisitos

Observação

Vale destacar que durante esse processo ambos os servidores devem estar ligados, conectados à rede e se comunicando. Não é possível executar esse procedimento de forma *off-line*.

Após a conclusão do processo, o servidor irá reiniciar automaticamente e, nesse momento, da mesma forma que no servidor anterior, deve-se efetuar o *login* com um usuário do domínio.

Concluída a instalação da réplica, os dois servidores possuem uma cópia do banco de dados NTDS.DIT e estão sincronizados. Na ausência de um dos servidores, o outro será capaz de manter o ambiente funcionando e garantirá a autenticação dos usuários da rede.

Uma maneira simples de efetuar um teste de saúde da replicação entre os controladores de domínio é usar o comando **repadmin /replsum**. Esse comando deve ser executado a partir de um Prompt de Comando do MS-DOS, conforme exibido na figura seguinte.

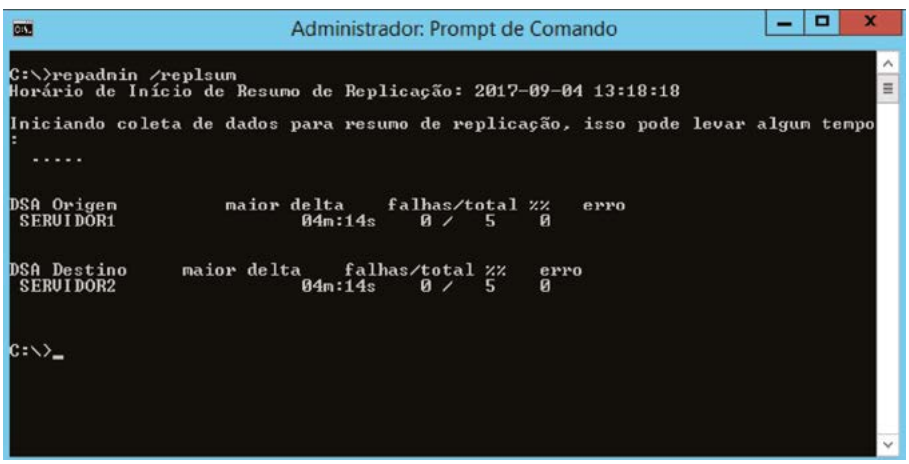

Figura 115 – Validando a replicação

Conforme pode ser observado na figura anterior, o comando executa uma espécie de **ping** entre os servidores e apresenta um resultado de saúde dessa comunicação entre eles. A coluna falha com o resultado 0 (zero) demonstra que não ocorreram falhas na replicação entre os controladores de domínio e que a configuração da réplica ocorreu com sucesso.

Saiba mais

Para saber mais sobre servidor-réplica do Active Directory, leia os capítulos 22 e 23 do livro:

BATTISTI, J.; POPOVICI, E. *Windows Server 2012 R2 e Active Directory*. São Paulo: Instituto Alpha, 2015.

5.1.3 Ingressando um computador no domínio

Após a configuração de um domínio do Active Directory, os computadores clientes da rede e demais servidores devem ser ingressados nesse domínio para que o processo de gerenciamento centralizado possa ocorrer.

O procedimento de inclusão de um dispositivo no domínio é bastante simples e requer apenas alguns ajustes nas configurações dos equipamentos que irão ingressar no novo ambiente.

Para começar, recomenda-se que os nomes dos dispositivos sejam definidos e, sempre que possível, seja estabelecida uma convenção de nomes para facilitar a identificação desses dispositivos.

É importante também que a configuração IP seja estabelecida para todos os dispositivos. Esta pode ser feita manualmente ou via DHCP (o mais recomendado). Mas o importante é que esses dispositivos se comuniquem com o domínio ao qual serão adicionados e, principalmente, que façam isso resolvendo nomes via DNS.

Na figura a seguir, é apresentado um exemplo de configuração de IP do computador cliente que será ingressado no domínio. Pode-se observar que, nesse caso, o IP foi definido manualmente, e que, na configuração de DNS preferencial e alternativo, foram definidos os IPs dos dois controladores de domínio instalados anteriormente.

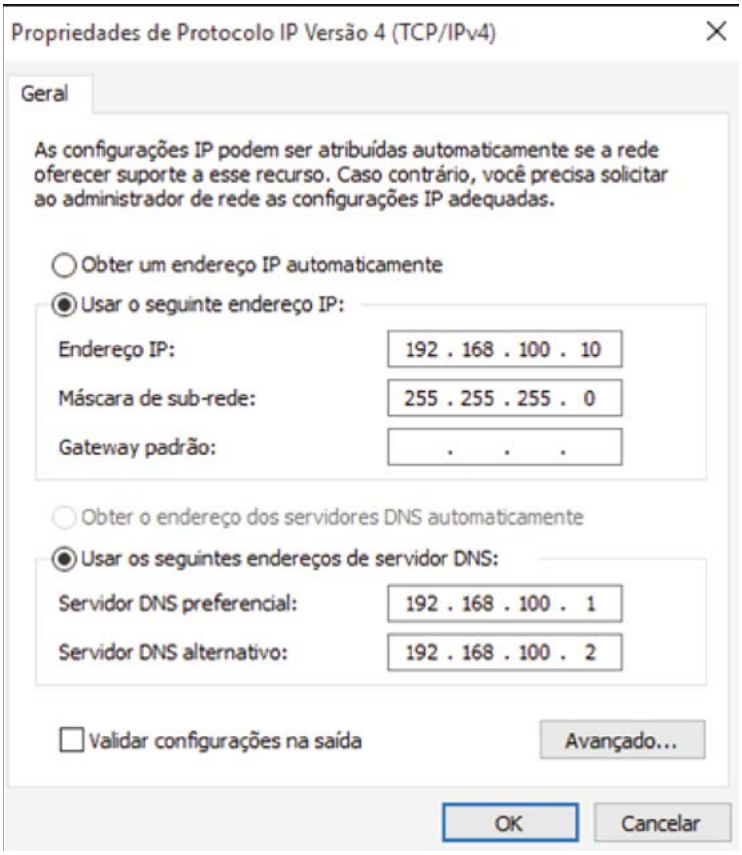

Figura 116 – Configuração de IP do cliente

Pode-se ainda efetuar um simples teste com o comando **ping** no cliente para validar que ele está conseguindo se comunicar e resolver os nomes de domínio no qual será ingressado, conforme exibido na figura a seguir.

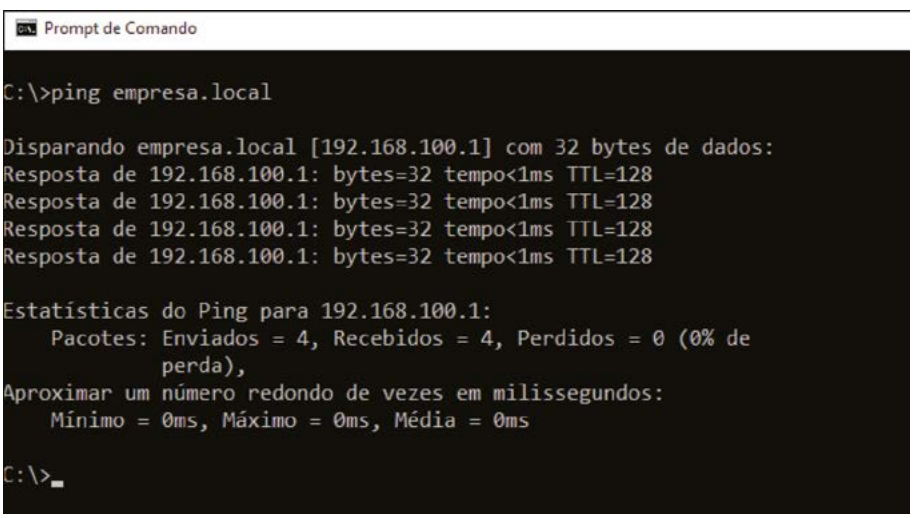

Figura 117 – Comando **ping**

Após efetuar o teste de conectividade, pode-se adicionar o computador cliente ao domínio; para isso, executar os passos a seguir.

- **Passo 1:** logado com um usuário administrador local da máquina, no Menu Iniciar, procure pelo ícone **Meu computador** e clique sobre ele com o botão direito do *mouse*, selecionando em seguida a opção **Propriedades**, conforme exibido na figura a seguir.

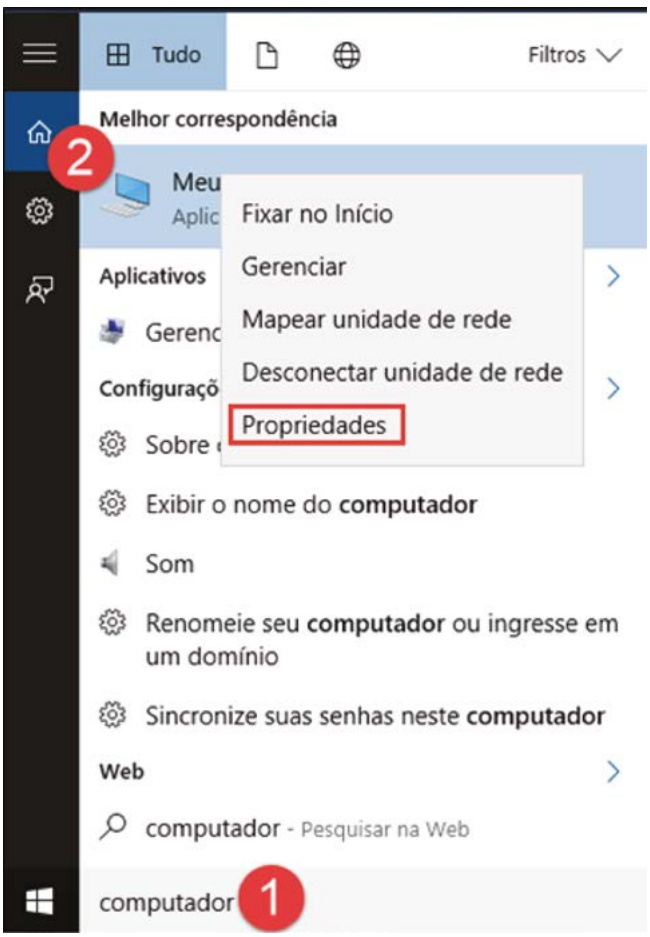

Figura 118 – Propriedades do Windows 10

- **Passo 2:** nas propriedades do computador, selecione, no nó **Nome do computador, domínio e configurações de grupo de trabalho**, a opção **Alterar configurações**, conforme exibido na figura seguinte.

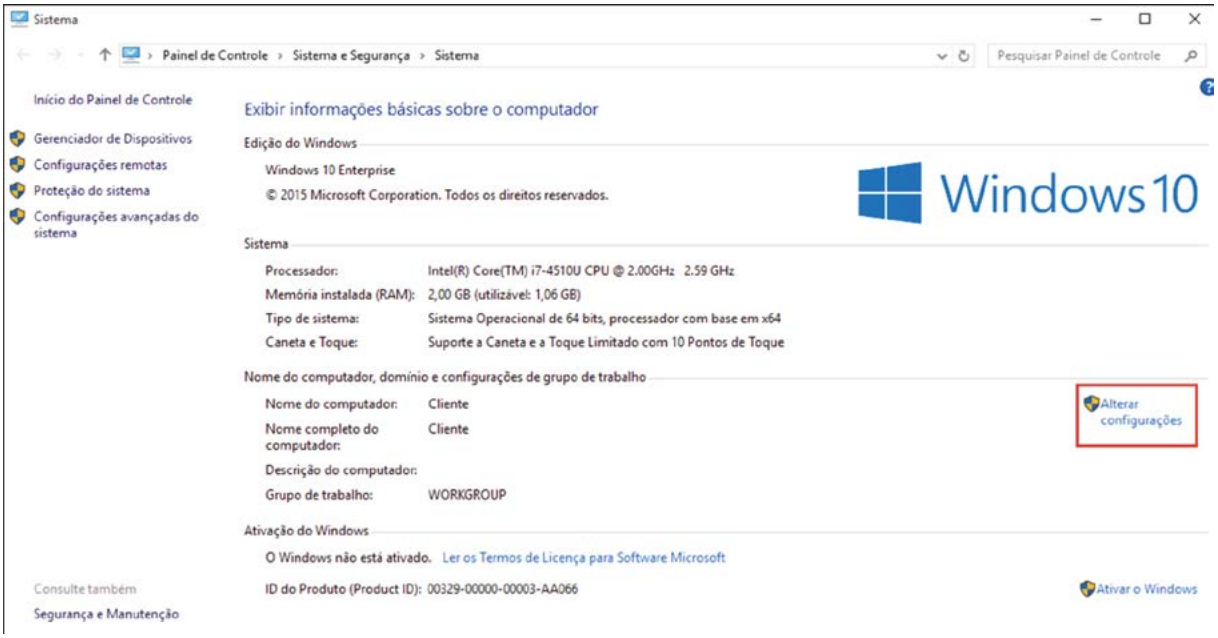

Figura 119 – Propriedades do Sistema

- **Passo 3:** na tela **Propriedades do Sistema**, clique no botão **Alterar** para ter acesso à configuração de domínio do computador, conforme exibido na próxima figura.

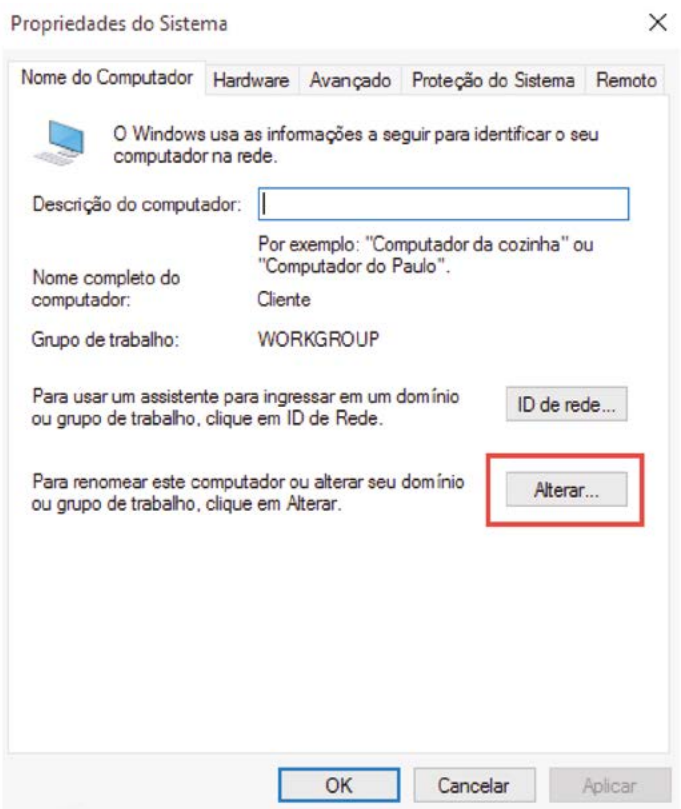

Figura 120 – Alterar propriedades do sistema

- **Passo 4:** na tela **Alteração de Nome/Domínio do Computador**, selecione no conjunto **Membro de** a opção **Domínio** e informe o nome do domínio em que o computador cliente será inserido, conforme exibido na figura seguinte.

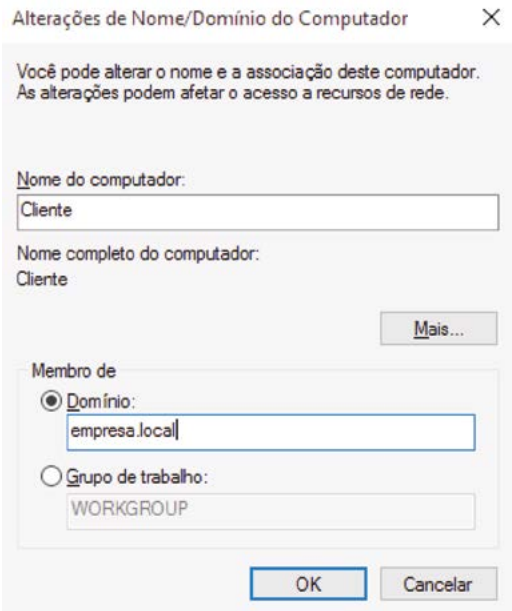

Figura 121 – Alterações de Nome/Domínio

Executado esse procedimento, será solicitado ao técnico que informe um nome de usuário e senha válida (não precisa ser administrador) no domínio, para que o sistema valide o acesso e conclua o processo de associação do dispositivo ao domínio.

Lembrete

É importante ressaltar que só poderão ingressar, no domínio, computadores com sistemas operacionais Professional. Máquinas com Sistema Operacional Home não possibilitam esse tipo de operação.

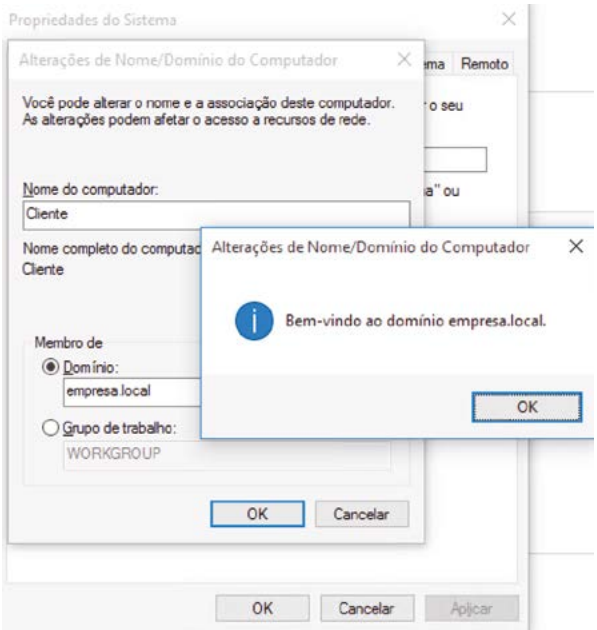

Figura 122 – Bem-vindo ao domínio

A figura anterior apresenta a confirmação do processo de ingresso do computador no domínio.

Ao ingressar um computador no domínio, uma conta será criada para a máquina no Active Directory. Essa conta será utilizada para permitir que os administradores gerenciem o dispositivo, aplique políticas de grupo e até mesmo monitorem o seu funcionamento. Desde o Windows 2000, as contas de computadores no Active Directory representam objetos ativos. Assim, se um administrador desabilitar essa conta do domínio, o computador perderá a capacidade de logon nele.

Para logar com um usuário do domínio, basta informar o nome do domínio e o usuário, conforme demonstrado na figura a seguir.

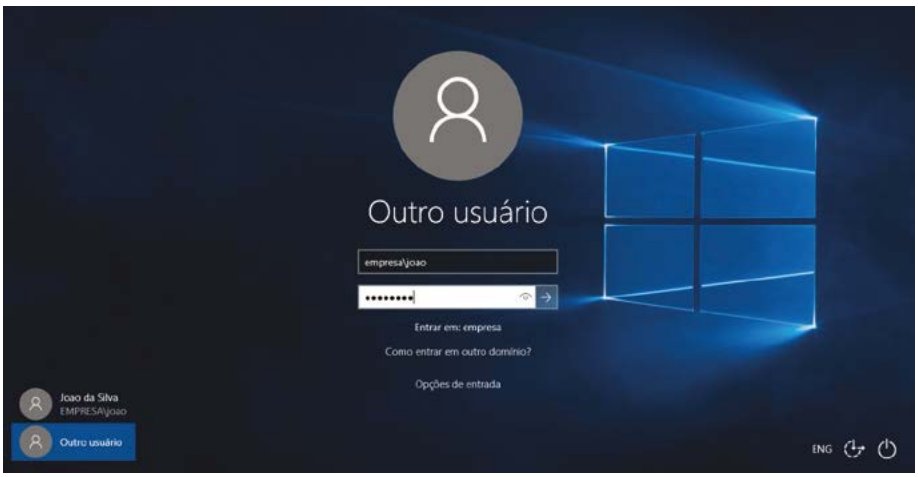

Figura 123 – Logando no domínio

5.2 Criando e gerenciando objetos no Active Directory

Durante a administração de uma rede com um domínio Microsoft, uma das tarefas importantes é exatamente a gestão de objetos do Active Directory. Para facilitar a organização de toda a estrutura, o ambiente permite que objetos chamados de **Unidade Organizacional** (OU) sejam criados dentro da estrutura do domínio. Esses objetos podem ser utilizados para agrupar usuários, grupos e computadores por localidade, função ou tipo.

Figura 124 – Estrutura do Active Directory

Normalmente essas OUs são criadas para configurar e atribuir Políticas de Grupo e delegar permissões administrativas.

Como pode ser observado na figura anterior, dentro da estrutura do Active Directory, existem dois tipos de objetos para organizar o ambiente: a **Unidade Organizacional**, representada com o desenho de um pequeno livro no meio da pasta, e os **Containers**, representados apenas por uma pasta amarela.

Os *containers* são objetos normalmente criados pelo sistema e para uso do próprio sistema, como o *container* **Managed Services Accounts**, no qual poderão ser armazenadas contas gerenciadas para autenticação de recursos do sistema. Esses objetos não dão suporte à criação de subobjetos, ou seja, não são estruturas hierárquicas.

No caso das Unidades Organizacionais, são objetos que podem ser criados tanto pelo sistema quanto pelos próprios administradores para estruturar o ambiente e facilitar sua administração. Esses objetos possibilitam a criação de subobjetos, permitindo que outras OUs sejam criadas dentro da OU-pai, ou seja, como se pode observar na imagem anterior, são estruturas hierárquicas.

Podem-se criar OUs diretamente na raiz de um domínio ou dentro de outra Unidade Organizacional. Para isso, é possível utilizar ferramentas gráficas ou até mesmo comandos via PowerShell.

5.2.1 Ferramentas de gerenciamento do Active Directory

Para gerenciar o Active Directory, o Windows oferece algumas ferramentas que irão permitir ao administrador, de forma simples, gerenciar os principais objetos de um domínio. Dentre elas, destacam-se a ferramenta **Usuários e Computadores do Active Directory** (DSA.MSC) e a **Central Administrativa do Active Directory**.

Usuários e Computadores do Active Directory é uma ferramenta mais conhecida pelos administradores, pois está disponível no Windows Server desde a versão 2000 do Sistema Operacional. Permite gerenciar os principais objetos do ambiente, por exemplo, Unidades Organizacionais, usuários, computadores, Grupos, entre outros.

O processo é bastante simples. Conforme exibido na próxima figura, podem-se criar objetos clicando sobre o domínio ou a OU desejada com o botão direito do *mouse* e selecionando a opção **Novo**. A partir desse ponto, pode-se escolher o objeto que será criado e seguir preenchendo o formulário com as informações necessárias para a criação do objeto.

Vale destacar que para cada tipo de objeto criado dentro do ambiente um tipo de informação diferente será solicitada ao administrador. Durante a leitura deste livro-texto, serão abordadas informações sobre os principais atributos e sobre a criação dos principais tipos de objetos do Active Directory, que são necessários para garantir a correta administração e o devido controle de um domínio do Windows Server.

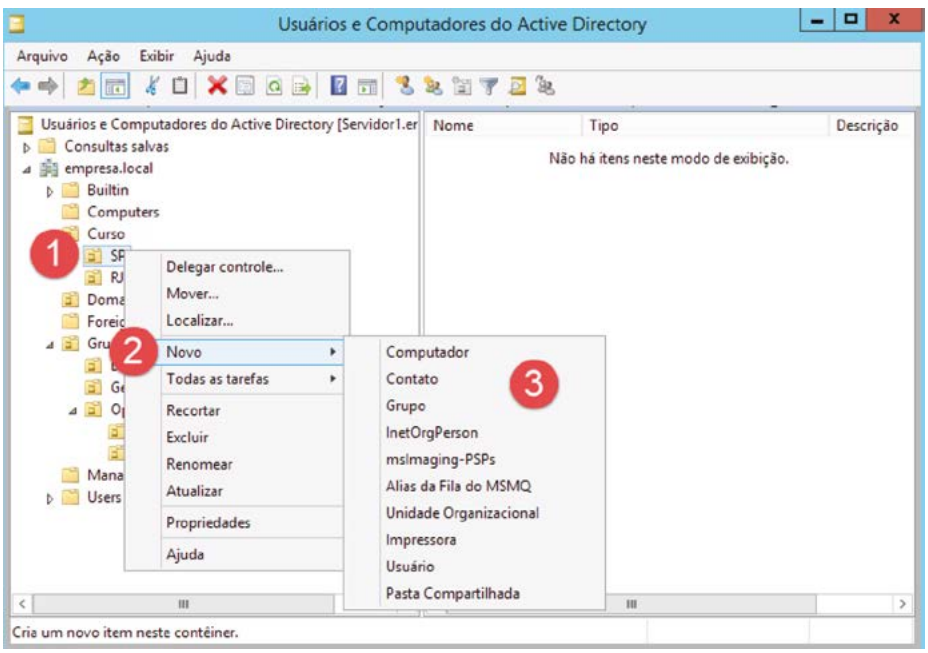

Figura 125 – Criando objetos no Active Directory

Outra ferramenta que pode ser utilizada para gerenciar objetos do Active Directory é a **Central Administrativa do Active Directory**. Exibida na figura a seguir, essa ferramenta é mais recente.

Incluída na versão final do Windows 2008 R2 e oficializada a partir da primeira versão do Windows 2012, apresenta uma aparência mais moderna e possui como diferencial apresentar os comandos PowerShell que podem ser usados na criação dos objetos, característica comum nas ferramentas atuais da Microsoft, como Exchange Server.

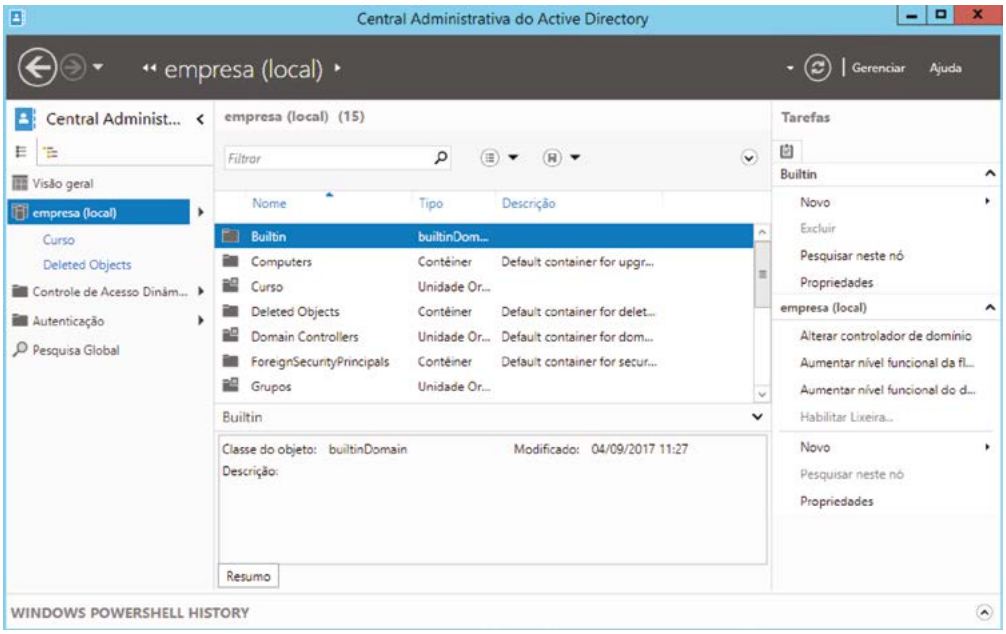

Figura 126 – Central Administrativa do Active Directory

No caso da central administrativa, os controles para criação de administração dos objetos irão aparecer no lado direito da tela, na Barra de Tarefas, conforme exibido na figura a seguir.

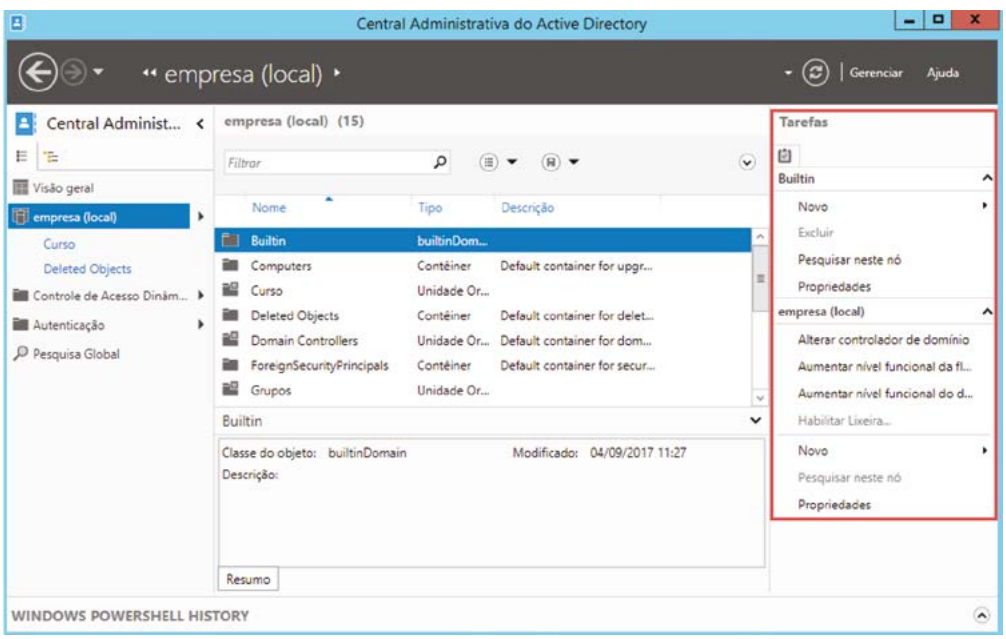

Figura 127 – Gestão de objetos na central administrativa

A partir dessa ferramenta, pode-se também habilitar a lixeira do Active Directory. Uma vez habilitada, ela não poderá mais ser desabilitada e irá permitir que os objetos excluídos sejam recuperados, caso necessário, conforme exibido na figura seguinte.

Para habilitar a Lixeira do Active Directory, basta selecionar o domínio e, na Barra de Tarefas, clicar na opção **Habilitar Lixeira**. A partir desse momento, será exibido no domínio um novo *container* chamado **Deleted Objects**. Clicando nele, poderão ser observados objetos que foram excluídos, e clicando sobre esses objetos com o botão direito do *mouse*, pode-se recuperá-los.

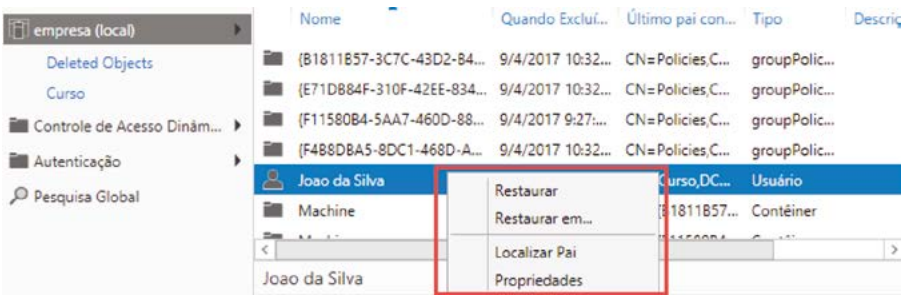

Figura 128 – Restaurando objetos do Active Directory

Os objetos excluídos no serviço de diretório do Windows Server 2012 R2 ficarão na lixeira por até 180 dias. Depois disso, serão automaticamente removidos do ambiente.

Para criar um objeto usando a Central Administrativa do Active Directory, basta selecionar o domínio ou a Unidade Organizacional em que se pretende criá-lo e então selecionar, na Barra de Tarefas, a função **Novo**, conforme exibido na figura a seguir.

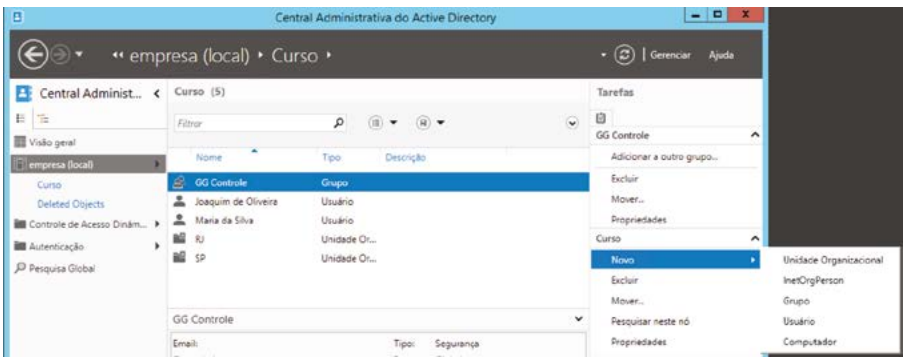

Figura 129 – Novo objeto

5.2.2 Tipos de objetos do Active Directory

No Active Directory, dentre os diversos tipos de objetos que podem ser criados, podem-se destacar os seguintes:

- **Usuário:** é o principal objeto que deve ser criado para a administração do ambiente e para garantir o acesso dos usuários. Representará os usuários do domínio, e recomenda-se que cada

usuário da rede tenha o seu objeto criado dentro do Active Directory. Dentre seus principais atributos, podem-se destacar os apresentados na figura a seguir.

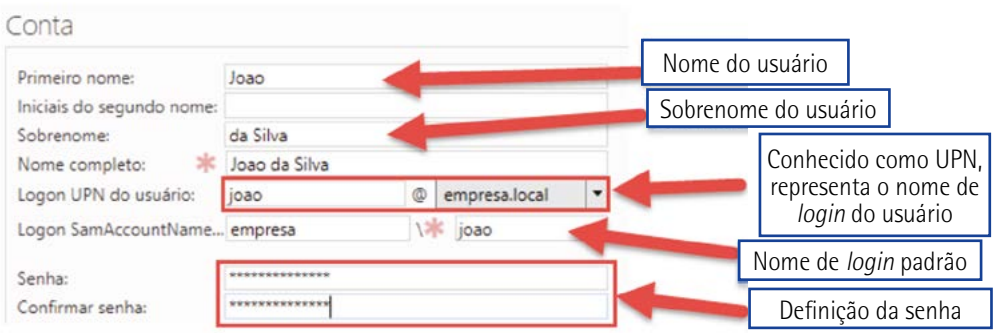

Figura 130 – Criando um objeto usuário

Deve-se destacar que, ao criar o objeto usuário, este possui dois campos para definição de nome de *login:* o campo UPN (User Principal Name) e o campo SamAccountName. Desses dois campos, o último é obrigatório; já o campo UPN é opcional e normalmente usado para *logon* em alguns tipos de aplicações que exigem o formato **User@domínio**.

- **Grupo:** objeto utilizado como recurso administrativo para delegar permissões, controle de acesso a objetos e até mesmo em listas de distribuição de *e-mails*. É a principal maneira de reduzir os esforços administrativos do usuário durante a gestão de um ambiente. Ao criar um grupo, podem-se definir o tipo e o escopo deste, conforme apresentado na figura seguinte.

Figura 131 – Criando grupos

Quanto ao tipo, os grupos podem ser criados como Distribuição ou Segurança:

- **Distribuição:** grupos utilizados para distribuição de *e-mails*; muito comuns quando a rede possui um Servidor Exchange instalado no ambiente. Esses grupos não podem ser utilizados para atribuição de permissões em listas de controle de acesso.

- **Segurança:** grupos utilizados para atribuir permissões em objetos dentro do ambiente; podem também ser utilizados como listas de distribuição.

Quanto ao escopo, um grupo pode ser configurado como **Domínio Local**, **Global** ou **Universal**. Basicamente o escopo define o alcance do grupo dentro da floresta. Por exemplo, um grupo de domínio

local só pode ganhar permissão de acesso em recursos que estejam no mesmo domínio em que ele foi criado, e um grupo de escopo global pode receber permissões em recursos que estejam fora do domínio em que ele foi criado.

Saiba mais

Para saber mais sobre as ferramentas de gerenciamento do AD e demais tipos de objetos, leia os capítulos 38 e 39 do livro:

BATTISTI, J.; POPOVICI, E. *Windows Server 2012 R2 e Active Directory*. São Paulo: Instituto Alpha, 2015.

Todo objeto do grupo pode ser associado a outros grupos e também pode ter uma lista de membros, que herdarão as permissões obtidas pelo grupo, conforme exibido na figura seguinte.

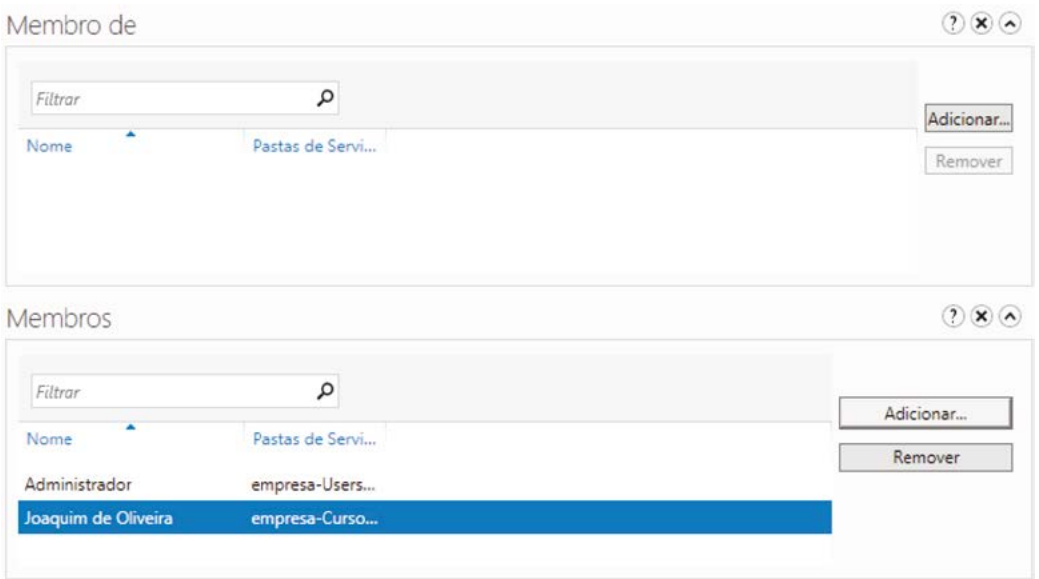

Figura 132 – Propriedades de grupo

Resumo

Nesta unidade aprendemos sobre domínio e grupo de trabalho.

Foi possível ver a confirmação de Battisti e Popovici (2015), quando afirmam que uma rede baseada em Windows Server 2012 R2 pode ser configurada para domínio ou grupo de trabalho (*workgroup*). Aprendemos que em um ambiente de grupo de trabalho a administração é mais distribuída, requerendo maior esforço da gestão

de TI e reduzindo a segurança, ao contrário do ambiente de domínio, que centraliza as informações, facilitando a gestão e proporcionando mais segurança às informações.

Aprendemos a realizar a instalação de um domínio do Acitive Directory e suas funções, assim como a instalar e configurar um servidor-réplica para garantir a redundância das informações.

Por fim, aprendemos sobre os tipos de objeto e como criá-los e gerenciá-los no Active Directory.

Exercícios

Questão 1. (Cespe 2017, adaptada) A respeito de Active Directory e LDAP, assinale a opção correta.

A) *Bind* é uma operação do LDAP cujo objetivo é testar se uma entrada tem determinado valor como atributo.

B) Existem dois tipos de servidores nos domínios baseados em *Active Directory*: *domain controller* e *member server*.

C) No Linux e no Windows, o *Active Directory* armazena apenas as informações do usuário que está logado no sistema, sendo descartadas informações dos demais usuários.

D) O LDAP é utilizado para fornecer um par de senhas para o usuário: uma senha para ambientes gráficos (Windows, Linux etc.) e outra para *mainframes*.

E) Nos domínios baseados no AD, podemos ter um tipo de servidor: Controlador de Domínio (DC – *Domain Controller*).

Resposta correta: alternativa B.

Análise da resposta

Para que os usuários possam acessar os recursos disponíveis na rede, deverão efetuar o *logon*. Quando o usuário efetua *logon*, o AD verifica se as informações fornecidas são válidas e, em caso positivo, faz a autenticação. O AD é organizado de forma hierárquica, com o uso de domínios. Caso uma rede utilize o AD, poderá conter vários domínios. Um domínio é nada mais do que um limite administrativo e de segurança, ou seja, o administrador do domínio possui permissões somente nesse domínio, e não em outros. As políticas de segurança também se aplicam somente a esse domínio, e não a outros. Resumindo: diferentes domínios podem ter diferentes administradores e diferentes políticas de segurança.

Nos domínios baseados no AD, podemos ter dois tipos de servidores: Controlador de Domínio (DC – *Domain Controller*) e Servidor Membro (*Member Server*).

Questão 2. (Inaz do Pará 2017) O sistema operacional Windows Server 2012 possui uma tecnologia que criptografa o disco rígido do computador, para que em caso de roubo ou de extravio, as informações contidas, neste dispositivo, fiquem protegidas de um acesso indevido. Qual o nome dado a essa tecnologia de segurança do sistema operacional?

A) BranchCache.

B) Clustering de Failover.

C) Kerberos.

D) BitLocker.

E) Smartcards.

Resolução desta questão na plataforma.