Capítulo 1

Criação de um domínio do Active Directory

O Active Directory Domain Services (AD DS, Serviços de Domínio Active Directory) e seus serviços relacionados formam a base das redes corporativas em execução no Microsoft Windows. Em conjunto, eles funcionam como ferramentas que armazenam informações sobre as identidades de usuários, computadores e serviços; autenticam um usuário ou computador; e fornecem um mecanismo com o qual o usuário ou o computador pode acessar os recursos na empresa. Neste capítulo, você começará a explorar o Active Directory do Windows Server 2008 R2 instalando a função Active Directory Domain Services e criando um controlador de domínio em uma nova floresta do Active Directory. Você descobrirá que o Windows Server 2008 R2 apresenta melhorias em muitos dos conceitos e recursos do Active Directory que você já conhece.

Este capítulo enfoca a criação de uma nova floresta do Active Directory com um único domínio em um único controlador de domínio. Nos exercícios deste capítulo, você criará um domínio chamado contoso.com, o qual será utilizado em todos os outros exercícios deste kit de treinamento. Nos capítulos subsequentes, você adquirirá experiência em outros cenários e na implementação de outros componentes-chave do Active Directory integrados ao AD DS.

Objetivo do exame neste capítulo:

- Configurar uma floresta ou um domínio.

Lições neste capítulo:

Antes de começar

Para concluir as lições deste capítulo, você deve:

- Ter dois computadores em que instalará o Windows Server 2008 R2. Os computadores podem ser sistemas físicos que preenchem os requisitos mínimos de hardware do Windows Server 2008 encontrados em *http://www.microsoft.com/windowsserver2008/en/us/system-requirements.aspx* ou *http://technet.microsoft.com/en-us/library/dd379511(WS.10).aspx*. Você precisará de pelo menos 512 MB de RAM, 32 GB de espaço livre no disco rígido e um processador x64 com uma velocidade de clock mínima de 1,4 GHz. Alternativamente, você pode utilizar máquinas virtuais que preenchem os mesmos requisitos.
- Ter uma versão de avaliação do Windows Server 2008 R2. Uma versão de avaliação de 180 dias do Windows Server 2008 R2 com SP1 está disponível para download em *http://www.microsoft.com/windowsserver2008/en/us/trial-software.aspx*.

Mundo real

Jason Kellington

O Windows Server 2008 R2 dá suporte somente a processadores x64 ou Itanium 2; não oferece mais suporte à arquitetura de processadores x86. Se os requisitos desse sistema não forem atendidos, não será possível instalar o Windows Server 2008 R2. Isso é muito importante ao fazer a atualização de servidores preexistentes para o Windows Server 2008 R2. Servidores preexistentes baseados na arquitetura de processadores x86 devem ser substituídos por hardware baseado na arquitetura de processador x64 ou Itanium 2.

No cenário de instalação mais comum do AD DS, o servidor funciona como controlador de domínio, o qual mantém uma cópia do banco de dados do AD DS e replica esse banco de dados em outros controladores de domínio. Os controladores de domínio são os componentes mais críticos em uma infraestrutura de Active Directory e devem funcionar com o menor número possível de componentes não relacionados adicionais instalados. Essa configuração oferece controladores de domínio mais estáveis e confiáveis porque limita a possibilidade de outros aplicativos ou serviços interferirem nos componentes do AD DS em execução no controlador de domínio.

Nas versões do Windows Server anteriores ao Windows Server 2008, os administradores do servidor tinham que selecionar e configurar os componentes individuais em um servidor para assegurar que componentes não essenciais do Windows fossem desabilitados ou desinstalados. No Windows Server 2008, os componentes-chave do Windows são divididos em grupos relacionados por funcionalidade chamados de funções. A administração baseada em funções permite ao administrador simplesmente selecionar a função ou as funções que o servidor deve preencher. Em seguida, o Windows Server 2008 instala os componentes apropriados do Windows necessários para realizar essa função. Você entenderá a administração baseada em funções à medida que avançar nos exercícios deste livro.

Lição 1: Instalação do Active Directory Domain Services

O Active Directory Domain Services (AD DS) fornece a funcionalidade de uma solução Identity and Access (IDA, Identidade e Acesso) para redes corporativas. Nesta lição, você aprenderá sobre o AD DS e outras funções do Active Directory suportadas pelo Windows Server 2008. Também explorará o Server Manager (Gerenciador do Servidor), ferramenta com a qual é possível configurar funções de servidor, e o Active Directory Domain Services Installation Wizard (Assistente de Instalação dos Serviços de Domínio Active Directory) aprimorado. Esta lição também revisa os conceitos-chave da solução IDA e do Active Directory.

Depois de ler esta lição, você será capaz de:

- Explicar a função IDA em uma rede corporativa.
- Entender o relacionamento entre os serviços do Active Directory.
- Instalar a função do Active Directory Domain Services (AD DS) e configurar um controlador de domínio do Windows Server 2008 R2 utilizando a interface do Windows.

Tempo estimado da lição: 60 minutos

Active Directory, Identity and Access

A infraestrutura IDA se refere às ferramentas e tecnologias de base usadas para integrar pessoas, processos e tecnologia em uma organização. Uma infraestrutura IDA efetiva assegura que as pessoas certas tenham acesso aos recursos corretos no momento oportuno.

Como mencionado previamente, o Active Directory oferece a solução IDA para redes corporativas em execução no Windows. O AD DS é o componente básico de uma infraestrutura IDA do Active Directory. O AD DS coleta e armazena informações IDA da empresa em um banco de dados chamado *repositório de dados do Active Directory*. O repositório de dados contém todas as informações pertinentes sobre todos os objetos existentes dentro da infraestrutura Active Directory. Além disso, o AD DS age como um hub de comunicação e de informações para serviços adicionais do Active Directory que juntos formam uma infraestrutura IDA completa.

O Active Directory armazena informações sobre usuários, grupos, computadores e outras identidades. Uma identidade é, no sentido mais amplo, uma representação de um objeto que realizará ações na rede corporativa. Por exemplo, um usuário abrirá documentos a partir de uma pasta compartilhada em um servidor. O documento será mantido seguro com permissões em uma lista de controle de acesso (ACL, access control list). O acesso ao documento é gerenciado pelo subsistema de segurança do servidor, que compara a identidade do usuário às identidades na ACL para determinar se a solicitação de acesso pelo usuário será concedida ou negada.

Computadores, grupos, serviços e outros objetos também realizam ações na rede e devem ser representados por identidades. Entre as informações armazenadas sobre uma identidade estão as propriedades que identificam unicamente o objeto, como um nome de usuário ou um identificador de segurança (SID, security identifier) e a senha para a identidade. O repositório de identidades é, portanto, um componente da infraestrutura IDA. O repositório de dados do Active Directory, também conhecido como *diretório*, é um repositório de identidades. O próprio diretório é hospedado em um banco de dados ar-

mazenado e gerenciado por um controlador de domínio – um servidor que desempenha a função AD DS. Se houver controladores de domínio múltiplos na infraestrutura do Active Directory, eles trabalham juntos para manter uma cópia do armazenamento de dados em cada controlador de domínio. As informações desse armazenamento permitem que o Active Directory realize as três principais funções de uma infraestrutura IDA: autenticação, controle de acesso e auditoria.

- **Autenticação** Um usuário, computador ou outro objeto deve primeiro confirmar sua identidade para a infraestrutura do Active Directory antes de poder funcionar como parte do domínio do Active Directory. Esse processo de verificação geralmente ocorre pela troca de informações protegidas ou sigilosas, como uma senha ou um certificado digital. Depois que as informações de autenticação tiverem sido submetidas ao Active Directory e confirmadas como sendo válidas, o usuário pode prosseguir como membro do domínio e realizar ações como solicitar acesso a arquivos compartilhados, enviar trabalho de impressão a uma impressora, acessar e ler emails ou quaisquer outras ações dentro do domínio.

Autenticação Kerberos em um domínio do Active Directory

Em um domínio do Active Directory, o protocolo Kerberos é utilizado para autenticar as identidades. Quando um usuário ou computador efetua logon no domínio, o Kerberos autentica suas credenciais e emite um pacote de informações chamado *tíquete de concessão de tíquete* (TGT, Ticket Granting Ticket). Antes de o usuário realizar uma tarefa como conectar-se ao servidor para solicitar um documento, uma solicitação Kerberos é enviada a um controlador de domínio junto com o TGT que identifica o usuário autenticado. O controlador de domínio emite ao usuário outro pacote de informações chamado *tíquete de serviço*, que identifica o usuário autenticado para o servidor. O usuário apresenta o tíquete de serviço ao servidor, que o aceita como prova de que o usuário foi autenticado.

Essas transações Kerberos resultam em um único logon de rede. Depois que o usuário ou computador se conectou inicialmente e recebeu um TGT, o usuário é autenticado dentro de todo o domínio e pode receber tíquetes de serviço que o identificam para qualquer serviço. Toda essa atividade de tíquetes é gerenciada pelos clientes e serviços Kerberos incorporados ao Windows e é transparente para o usuário.

- **Controle de acesso** A infraestrutura IDA é responsável por proteger informações e recursos, assegurando que o acesso aos recursos somente seja concedido às identidades que devem ter esse acesso. O acesso a recursos e informações confidenciais importantes deve ser gerenciado de acordo com as diretivas da empresa. Cada objeto individual (como computadores, pastas, arquivos e impressoras) dentro do Active Directory tem uma lista de controle de acesso discricionário (DACL, discretionary access control list) associada, a qual contém informações referentes às identidades que receberam direito de acesso ao objeto e ao nível de acesso concedido.

  Quando um usuário cuja identidade já foi autenticada no domínio tenta acessar um recurso, a DACL do recurso é verificada para determinar se a identidade do usuário consta da lista. Se a identidade estiver na lista, o usuário pode acessar o recurso de acordo com as especificações das permissões de acesso da DACL listadas para esse usuário.

- **Auditoria** O controle das atividades que ocorrem dentro da infraestrutura IDA é chamado de auditoria. A auditoria permite que as organizações monitorem os eventos que ocorrem na infraestrutura IDA, incluindo acesso a arquivos e pastas, onde

e quando os usuários estiverem efetuando logon, alterações na infraestrutura IDA e funcionalidade geral do Active Directory. O comportamento da auditoria é controlado por listas de controle de acesso do sistema (SACLs, system access control lists). Da mesma forma que a DACL mencionada anteriormente, cada objeto da infraestrutura IDA possui uma SACL associada. A SACL contém uma lista de identidades cuja atividade naquele recurso será auditada, assim como o nível de auditoria que ocorrerá para cada identidade.

O AD DS não é o único componente da solução IDA que é suportado pelo Windows Server 2008. Com a versão do Windows Server 2008, a Microsoft consolidou vários componentes anteriormente separados em uma plataforma IDA integrada. O próprio Active Directory agora inclui cinco tecnologias, cada uma das quais identificada com uma palavra-chave que indica o propósito da tecnologia, como mostrado na Figura 1-1.

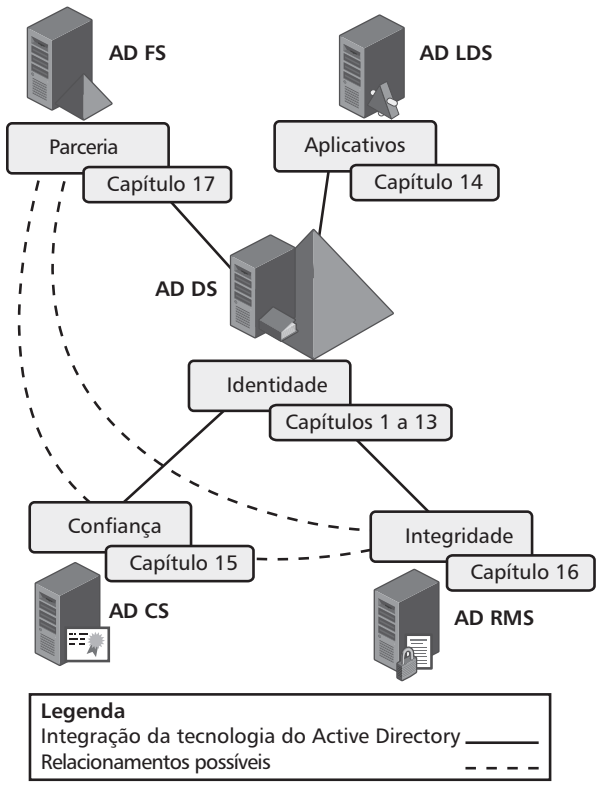

Figura 1-1 Integração das cinco tecnologias do Active Directory.

Essas cinco tecnologias compreendem uma solução IDA completa:

- **Active Directory Domain Services (Identidade)** O AD DS, como descrito antes, é projetado para fornecer um repositório central ao gerenciamento de identidades dentro de uma organização. O AD DS fornece serviços de autenticação, autorização e auditoria em uma rede e suporta o gerenciamento de objetos por meio de Group Policy (diretivas de grupo). O AD DS também fornece o gerenciamento de informações e serviços de compartilhamento, permitindo aos usuários localizar qualquer

componente – servidores de arquivos, impressoras, grupos e outros usuários – pesquisando o diretório. Por causa disso, o AD DS muitas vezes é tratado como um serviço de diretório de sistema operacional de rede. O AD DS é a principal tecnologia do Active Directory e deve ser implantado em todas as redes que executam sistemas operacionais Windows Server 2008. Os Capítulos 1 a 13 tratam do AD DS.

> ***MAIS INFORMAÇÕES*** **PROJETO DO AD DS**
>
> Para mais detalhes sobre o planejamento da implementação do AD DS e sobre informações referentes ao projeto do AD DS, consulte o Guia de Projeto do AD DS em *http://technet.microsoft.com/en-us/library/cc754678(WS.10).aspx*.

- **Active Directory Lightweight Directory Services (Aplicativos)** Essencialmente, uma versão autônoma do Active Directory, a função Active Directory Lightweight Directory Services (AD LDS, Serviços de Diretórios Leves do Active Directory), antes conhecida como Active Directory Application Mode (ADAM, Modo de Aplicativo do Active Directory), fornece suporte a aplicativos compatíveis com diretório. O AD LDS é, na verdade, um subconjunto do AD DS porque ambos estão baseados no mesmo código básico. O diretório AD LDS só armazena e replica informações relacionadas a aplicativos e é comumente utilizado por aplicativos que exigem um armazenamento de diretório, mas não exigem que as informações sejam replicadas de uma maneira tão ampla como, por exemplo, todos os controladores de domínio. O AD LDS também permite implantar um esquema personalizado para suportar um aplicativo sem modificar o esquema AD DS. A função AD LDS é realmente leve e suporta múltiplos armazenamentos de dados em um único sistema, portanto, cada aplicativo pode ser implantado com seu próprio diretório, esquema, atribuições de Lightweight Directory Access Protocol (LDAP) e portas SSL, e seu log de eventos de aplicativo. Como o AD LDS não se baseia no AD DS, ele pode ser utilizado em um ambiente autônomo ou de grupo de trabalho. Contudo, em ambientes de domínio, o AD LDS pode utilizar o AD DS para a autenticação de entidades de segurança Windows (usuários, grupos e computadores). O AD LDS também pode ser usado para fornecer serviços de autenticação em redes expostas, como extranets. Empregar o AD LDS nessa situação fornece menos risco do que utilizar o AD DS. O Capítulo 14, "Active Directory Lightweight Directory Services", trata do AD LDS.
- **Active Directory Certificate Services (Confiança)** Organizações podem utilizar o Active Directory Certificate Services (AD CS, Serviços de Certificados do Active Directory) a fim de configurar uma autoridade certificadora para emitir certificados digitais como parte de uma infraestrutura de chave pública (PKI, public key infrastructure) que vincula a identidade de uma pessoa, dispositivo ou serviço a uma chave privada correspondente. Os certificados podem ser utilizados para autenticar usuários e computadores, fornecer autenticação baseada na Web, suportar autenticação de cartão inteligente e suportar aplicativos, incluindo redes sem fio seguras, redes virtuais privadas (VPNs, virtual private networks), Internet Protocol Security (IPSec), Encrypting File System (EFS), assinaturas digitais, etc. O AD CS fornece um modo eficiente e seguro de emitir e gerenciar certificados. Você pode utilizar o AD CS para fornecer esses serviços a comunidades externas. Se fizer isso, o AD CS deve estar vinculado a uma autoridade de certificação externa conhecida que provará a outros que você é quem diz ser. O AD CS é projetado para criar confiança em um

mundo não confiável; como tal, ele deve confiar em processos comprovados que certificam que cada pessoa ou computador que obtém um certificado foi criteriosamente verificado e aprovado. Em redes internas, o AD CS pode ser integrado ao AD DS para fornecer automaticamente certificados aos usuários e computadores. O Capítulo 15, "Serviços de certificado e infraestrutura de chave pública do Active Directory", trata do AD CS.

- **Active Directory Rights Management Services (Integridade)** Embora um servidor em execução no Windows possa negar ou permitir acesso a um documento baseado na DACL do documento, há poucas maneiras de controlar o que acontece ao documento e seu conteúdo depois que um usuário o abre. O Active Directory Rights Management Services (AD RMS, Serviços de Gerenciamento de Direitos do Active Directory) é uma tecnologia de proteção das informações que permite implementar modelos persistentes de diretiva de uso que definem a utilização autorizada e não autorizada, seja online, seja offline, dentro ou fora do firewall. Por exemplo, você pode configurar um modelo que permite aos usuários ler um documento, mas não imprimir ou copiar seu conteúdo. Assim, você pode assegurar a integridade dos dados gerados, proteger a propriedade intelectual e controlar quem pode fazer o que com os documentos produzidos pela sua organização. O AD RMS exige um domínio do Active Directory com controladores de domínio em execução no Windows 2000 Server com o Service Pack 3 (SP3) ou superior; o IIS; um servidor de banco de dados como o Microsoft SQL Server 2008; o cliente AD RMS, que pode ser baixado do Microsoft Download Center e é incluído por padrão no Windows Vista, no Windows 7 e no Windows Server 2008; e um navegador compatível com RMS ou um aplicativo como Microsoft Internet Explorer, Microsoft Office, Microsoft Word, Microsoft Outlook ou Microsoft PowerPoint. O AD RMS pode basear-se no AD CS para incorporar certificados a documentos, bem como no AD DS para gerenciar direitos de acesso. O Capítulo 16, "Active Directory Rights Management Services", trata do AD RMS.
- **Active Directory Federation Services (Parceria)** O Active Directory Federation Services (AD FS, Serviços de Federação do Active Directory) permite que uma organização estenda a solução IDA para múltiplas plataformas, incluindo ambientes Windows e não Windows, e projete identidades e direitos de acesso cruzando limites de segurança para parceiros confiáveis. Em um ambiente federado, cada organização mantém e gerencia suas próprias identidades, mas cada empresa também pode projetar com segurança e aceitar identidades de outras organizações. Os usuários são autenticados em uma rede, porém, podem acessar recursos em outra – um processo conhecido como *logon único* (SSO, Single Sign-On). O AD FS suporta parcerias porque permite que diferentes organizações compartilhem o acesso a aplicativos de extranet baseando-se em suas próprias estruturas AD DS internas para fornecer o processo de autenticação real. Para tanto, o AD FS estende a estrutura interna do AD DS ao mundo externo por meio das portas Transmission Control Protocol/Internet Protocol (TCP/IP) comuns como 80 (HTTP) e 443 (Secure HTTP, ou HTTPS). Ele normalmente reside na rede de perímetro. O AD FS pode basear-se no AD CS para criar servidores confiáveis e no AD RMS para fornecer proteção externa à propriedade intelectual. O Capítulo 17, "Active Directory Federation Services", trata do AD FS.

Em conjunto, as funções do Active Directory fornecem uma solução IDA integrada. O AD DS ou o AD LDS fornece serviços de diretório fundamentais tanto nas implementações de domínio como nas implementações autônomas. O AD CS fornece credenciais confiáveis na forma de certificados digitais PKI. O AD RMS protege a integridade das informa-

ções contidas nos documentos. E o AD FS suporta parcerias eliminando a necessidade de ambientes federados para criar identidades múltiplas e separadas para uma única entidade de segurança.

Além da solução IDA

Contudo, o Active Directory oferece mais do que uma simples solução IDA. Ele também fornece os mecanismos para suportar, gerenciar e configurar recursos nos ambientes de rede distribuída.

Um conjunto de regras, o *esquema*, define classes de objetos e atributos que podem estar contidos no diretório. O fato de o Active Directory ter objetos de usuário que incluem um nome de usuário e uma senha, por exemplo, ocorre porque o esquema define a classe de objetos *user*, os dois atributos e a associação entre a classe de objeto e os atributos.

A administração baseada em diretivas reduz a carga de gerenciamento até mesmo das maiores e mais complexas redes, fornecendo um ponto único em que especificar as configurações que são depois implantadas em múltiplos sistemas. Você aprenderá sobre essas diretivas, incluindo Group Policy, diretivas de auditoria e diretivas de senha refinada, no Capítulo 6, "Implementação de infraestrutura de Group Policy", no Capítulo 7, "Gerenciamento de segurança corporativa e configurações de Group Policy", e no Capítulo 8, "Aprimoramento da segurança de autenticação em um domínio AD DS".

Os serviços de replicação distribuem os dados de diretório por uma rede, o que inclui o próprio armazenamento dos dados, bem como os dados necessários para implementar as diretivas e a configuração, incluindo scripts de logon. No Capítulo 8, no Capítulo 11, "Gerenciamento de sites e replicação do Active Directory", e no Capítulo 10, "Administração de controladores de domínio", você aprenderá sobre a replicação do Active Directory. Há até mesmo uma partição separada do armazenamento de dados denominada *configuration* que mantém informações sobre configuração, topologia e serviços de rede.

Vários componentes e tecnologias permitem pesquisar o Active Directory e localizar objetos no armazenamento de dados. Uma partição do armazenamento de dados chamada *catálogo global* (global catalog, também conhecida como *conjunto de atributos parcial*) contém informações sobre cada objeto no diretório. Ela é um tipo de índice que pode ser utilizado para localizar objetos no diretório. Interfaces programáticas como a Active Directory Services Interface (ADSI) e protocolos como o LDAP podem ser utilizados para ler e manipular o armazenamento de dados.

O armazenamento de dados do Active Directory também pode ser utilizado para suportar aplicativos e serviços não diretamente relacionados ao AD DS. Dentro do banco de dados, as partições de aplicativo podem armazenar dados para suportar aplicativos que exigem dados replicados. O serviço Domain Name System (DNS, Sistema de Nomes de Domínio) em um servidor que executa no Windows Server 2008 pode armazenar suas informações em um banco de dados chamado *zona integrada do Active Directory*, que é mantida como uma partição de aplicativo no AD DS e replicada usando-se serviços de replicação do Active Directory.

Componentes de uma infraestrutura do Active Directory

Os 13 primeiros capítulos deste kit de treinamento se concentram na instalação, configuração e gerenciamento do AD DS. O AD DS fornece a base da solução IDA e o ge-

renciamento de uma rede corporativa. Vale a pena investir algum tempo revisando os componentes de uma infraestrutura do Active Directory.

> ***OBSERVAÇÃO*** **ONDE ENCONTRAR DETALHES DO ACTIVE DIRECTORY**
>
> Para mais detalhes sobre o Active Directory, consulte o Help do produto instalado com o Windows Server 2008 e a home page do Windows Server 2008 R2, localizada em *http://technet.microsoft.com/en-us/windowsserver/bb310558.aspx*.

- **Armazenamento de dados do Active Directory** Como mencionado na seção anterior, o AD DS armazena suas identidades no diretório – um armazenamento de dados hospedado nos controladores de domínio. O diretório é um banco de dados de arquivo único chamado Ntds.dit e localizado por padrão na pasta %SystemRoot%\Ntds em um controlador de domínio. O banco de dados é dividido em várias partições, incluindo esquema, configuração e contexto de nomenclatura de domínios que contém os dados sobre objetos dentro de um domínio – usuários, grupos e computadores, por exemplo. Dependendo do ambiente, também pode haver partições de aplicativo e um conjunto de atributos parcial (PAS, partial attribute set), também chamado de *catálogo global*.
- **Controladores de domínio** Os controladores de domínio (DCs, domain controllers) são servidores que realizam a função AD DS e mantêm uma cópia do armazenamento de dados do Active Directory com outros dados importantes para o domínio. Como parte dessa função, eles também executam o serviço Kerberos Key Distribution Center (KDC), que realiza a autenticação e outros serviços do Active Directory. O Capítulo 10 detalha as funções executadas pelos DCs.
- **Domínio** São necessários um ou mais controladores de domínio para criar um domínio no Active Directory. Um domínio é uma unidade administrativa dentro da qual certas capacidades e características são compartilhadas. Primeiro, todos os controladores de domínio replicam a partição do armazenamento de dados do domínio, a qual contém, entre outras coisas, os dados da identidade de usuários do domínio, grupos e computadores. Como todos os DCs mantêm o mesmo repositório de identidades, qualquer DC pode autenticar qualquer identidade em um domínio. Além disso, um domínio define os limites das diretivas administrativas, como as diretivas de complexidade de senha e de bloqueio de conta. Essas diretivas configuradas em um domínio afetam todas as contas no domínio e não afetam contas em outros domínios. As modificações podem ser feitas nos objetos no banco de dados do Active Directory por qualquer controlador de domínio e serão replicadas a todos os outros controladores de domínio. Portanto, nas redes em que a replicação de todos os dados entre os controladores de domínio não pode ser suportada, talvez seja necessário implementar mais de um domínio para gerenciar a replicação dos subconjuntos de identidades. Você aprenderá mais sobre domínios no Capítulo 12, "Gerenciamento de múltiplos domínios e florestas".
- **Floresta** Uma *floresta* é uma coleção de um ou mais domínios do Active Directory. O primeiro domínio instalado em uma floresta é chamado *domínio raiz da floresta*. Uma floresta contém uma única definição de configuração de rede e uma única instância do esquema de diretório.

  Uma floresta é uma instância única do diretório – nenhum dado é replicado pelo Active Directory fora dos limites da floresta. Consequentemente, a floresta define um limite de segurança. O Capítulo 12 explora o conceito de floresta em mais detalhes.

- **Árvore** O namespace de DNS dos domínios em uma floresta cria árvores dentro da floresta. Se um domínio for um subdomínio de outro domínio, os dois domínios serão considerados uma árvore. Por exemplo, se a floresta *treyresearch.net* contiver dois domínios – *treyresearch.net* e *antarctica.treyresearch.net* –, esses domínios constituirão uma parte contígua do namespace de DNS, formando assim uma árvore única. Se, inversamente, os dois domínios forem *treyresearch.net* e *proseware.com*, os quais não são contíguos no namespace de DNS, a floresta será considerada como tendo duas árvores. As árvores são o resultado direto dos nomes de DNS escolhidos para os domínios na floresta.

A Figura 1-2 ilustra uma floresta do Active Directory para a Trey Research, que mantém uma pequena operação em uma estação de campo na Antártida. Como o link entre a Antártida e a sede é caro, lento e inseguro, a Antártida é configurada como um domínio separado. O nome de DNS da floresta é *treyresearch.net*. O domínio Antártida é um domínio filho no namespace de DNS, *antarctica.treyresearch.net*; portanto, é considerado um domínio filho na árvore de domínio.

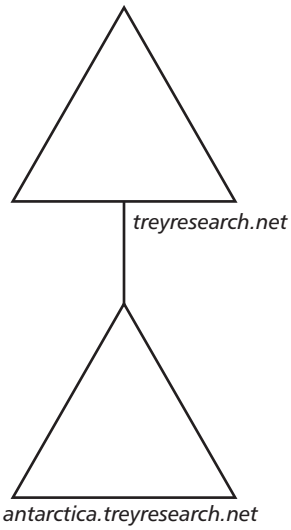

Figura 1-2 Uma floresta do Active Directory com dois domínios.

- **Nível funcional** A funcionalidade disponível em um domínio ou floresta do Active Directory depende do seu *nível funcional*. O nível funcional é uma configuração do AD DS que habilita recursos avançados do AD DS por todo o domínio ou por toda a floresta. Há seis níveis funcionais de domínio (nativo do Windows 2000, misto do Windows 2000, Windows Server 2003, provisório do Windows Server 2003, Windows Server 2008 e Windows Server 2008 R2); e cinco níveis funcionais de floresta (Windows Server 2000, Windows Server 2003, provisório do Windows Server 2003, Windows Server 2008 e Windows Server 2008 R2). À medida que você eleva o nível funcional de um domínio ou floresta, os recursos fornecidos pela versão do Windows envolvida tornam-se disponíveis para o AD DS. Por exemplo, quando o nível funcional de floresta é elevado para o Windows Server 2008 R2, a capacidade de habilitar a Lixeira do Active Directory torna-se disponível. Com a Lixeira do Active Directory, os objetos excluídos do Active Directory são mantidos no estado em que

estavam antes da exclusão. Isso permite fácil restauração de objetos previamente excluídos, se necessário. O importante a saber sobre os níveis funcionais é que eles determinam as versões do Windows autorizadas nos controladores de domínio. Antes de elevar o nível funcional de domínio para o Windows Server 2008, todos os controladores de domínio devem estar rodando o Windows Server 2008. O Capítulo 12 discute os níveis funcionais de domínio e floresta.

- **Unidades organizacionais** O Active Directory é um banco de dados hierárquico. Os objetos no armazenamento de dados podem ser agrupados em contêineres. Um tipo de contêiner é a classe de objeto chamada *container*. Podem-se ver os contêineres padrão, incluindo Users, Computers e Builtin, quando se abre o snap-in do Active Directory Users and Computers (Usuários e Computadores do Active Directory). Outro tipo de contêiner é a *unidade organizacional* (OU, organizational unit). As OUs, além de fornecerem um contêiner para objetos, também fornecem um escopo com o qual gerenciá-los. Isso ocorre porque as OUs podem ter objetos chamados *Group Policy Objects* (GPOs, objetos de Group Policy) vinculados a elas. As GPOs podem conter definições de configuração que serão então aplicadas automaticamente pelos usuários ou computadores em uma OU. No Capítulo 2, "Administração do Active Directory Domain Services", você aprenderá mais sobre OUs, e, no Capítulo 6, você explorará as GPOs.
- **Sites** Quando você considera a topologia de rede de uma empresa distribuída, certamente discutirá os sites ou localizações da rede física. Contudo, os sites do Active Directory têm um significado bem específico. Um site do Active Directory é um objeto que representa uma parte da empresa dentro da qual se espera uma conectividade de rede de largura de banda alta consistente. Um site define um limite de uso de replicação e serviços. Os controladores de domínio dentro de um site replicam as modificações em questão de segundos. Contudo, as modificações são replicadas entre sites de maneira controlada sob a suposição de que as conexões entre os sites são lentas, caras ou inseguras se comparadas às conexões dentro de um site. Além disso, os clientes preferem utilizar serviços distribuídos fornecidos pelos servidores nos seus sites ou no site mais próximo. Por exemplo, quando um usuário efetua logon no domínio, o cliente do Windows primeiro tenta se autenticar com um controlador de domínio no site. O cliente fará uma tentativa de se autenticar com um DC em outro site somente se nenhum controlador de domínio estiver disponível no site. O Capítulo 11 detalha a configuração e a funcionalidade dos sites do Active Directory.

Cada um desses componentes é discutido detalhadamente mais adiante neste kit de treinamento. Neste ponto, se você tiver pouco conhecimento do Active Directory, é importante que tenha uma noção básica da terminologia, dos componentes e de seus relacionamentos.

Preparação da criação de uma nova floresta do Windows Server 2008

Antes de instalar a função AD DS em um servidor e promovê-la para atuar como um controlador de domínio, planeje a infraestrutura do Active Directory. Algumas informações necessárias para criar um controlador de domínio são:

- O nome do domínio e o nome de DNS. Um domínio deve ter um nome de DNS único, por exemplo, contoso.com, bem como um nome curto, por exemplo, CONTOSO, chamado de *nome NetBIOS*. O NetBIOS é um protocolo de rede utilizado desde as

primeiras versões do Microsoft Windows NT e ainda é especificado e utilizado para compatibilidade com versões anteriores.

- Se o domínio precisa suportar controladores de domínio que rodam versões anteriores do Windows. Ao criar uma nova floresta do Active Directory, você configura o nível funcional. Se o domínio incluir apenas controladores de domínio do Windows Server 2008 R2, você poderá configurar o nível funcional apropriadamente para tirar proveito dos recursos avançados introduzidos por essa versão do Windows.
- Detalhes de como o DNS será implementado para suportar o Active Directory. É uma prática recomendada implementar o DNS para suas zonas de domínio Windows utilizando o Windows DNS Service, como você aprenderá no Capítulo 9, "Integração do Domain Name System ao AD DS"; mas é possível suportar um domínio do Windows em um serviço de DNS de terceiros.
- Configuração de IP para o controlador de domínio. Os controladores de domínio exigem valores para endereços IP estáticos e máscara de sub-rede. Além disso, o controlador de domínio deve ser configurado com um endereço de servidor de DNS para realizar a resolução de nomes. Se você criar uma nova floresta e executar o Windows DNS Service no controlador de domínio, poderá configurar o endereço DNS para que ele aponte para o endereço IP do próprio servidor. Depois que o DNS é instalado, o próprio servidor pode resolver os nomes DNS.
- O nome de usuário e a senha de uma conta no grupo Administrators (Administradores) do servidor. A conta deve ter uma senha – e a senha não pode ser o campo vazio.
- A localização em que o armazenamento de dados (incluindo *Ntds.dit*) e o volume do sistema (SYSVOL) devem ser instalados. Por padrão, esses armazenamentos são criados em %SystemRoot%; por exemplo, C:\Windows, nas pastas NTDS e SYSVOL, respectivamente. Ao criar um controlador de domínio, você pode redirecionar esses armazenamentos para outras unidades.

> ***MAIS INFORMAÇÕES*** **IMPLANTAÇÃO DO AD DS**
>
> Essa lista compreende as configurações que você será solicitado a definir ao criar um controlador de domínio. Há várias considerações adicionais com relação à implantação do AD DS em um ambiente corporativo que devem ser examinadas. Consulte o Guia de Implantação do AD DS em *http://technet.microsoft.com/en-us/library/cc753963(WS.10).aspx* para mais informações.

Adição da função AD DS utilizando a interface do Windows

Depois de coletar as informações dos pré-requisitos listados anteriormente, você está pronto para adicionar a função AD DS. Há várias maneiras de realizar esse procedimento. Nesta lição, você aprenderá a criar um controlador de domínio utilizando a interface do Windows. Na próxima lição, você aprenderá a fazer o mesmo utilizando a linha de comando.

O Windows Server 2008 fornece uma configuração baseada em função, instalando apenas os componentes e serviços necessários para as funções que um servidor executa. Esse gerenciamento de servidor baseado em função é refletido no novo console admi-

nistrativo, Server Manager, mostrado na Figura 1-3. O Server Manager consolida as informações, as ferramentas e os recursos necessários para suportar as funções de um servidor.

Você pode adicionar funções a um servidor utilizando o link Add Roles na home page do Server Manager ou clicando com o botão direito do mouse no nó Roles na árvore de console e escolhendo Add Roles.

O Add Roles Wizard apresenta uma lista das funções disponíveis para a instalação e o orienta na instalação das funções selecionadas.

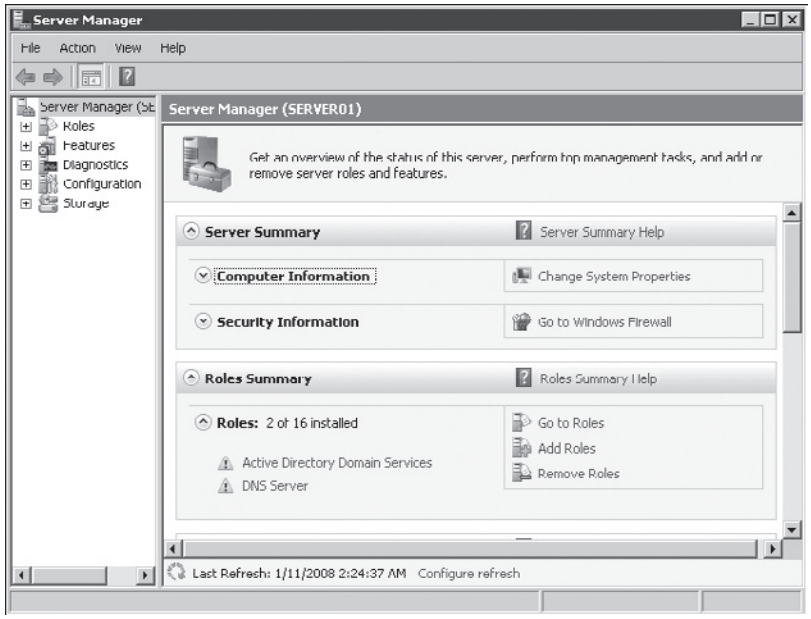

Figura 1-3 Server Manager.

Criação de um controlador de domínio

Depois de adicionar a função AD DS, os arquivos exigidos para executar a função são instalados no servidor; porém, o servidor ainda não funciona como um controlador de domínio. Posteriormente, você precisa executar o Active Directory Domain Services Installation Wizard, que pode ser iniciado utilizando-se o comando *Dcpromo.exe* para configurar e inicializar o Active Directory.

> ***PRÁTICA***
>
> O Exercício 4, "Instale uma nova floresta do Windows Server 2008 R2", no final desta lição, discute como configurar o AD DS utilizando o Active Directory Domain Services Installation Wizard.

Teste rápido

- Você quer utilizar um novo servidor rodando Windows Server 2008 R2 como um controlador de domínio no seu domínio do Active Directory. Que comando você usa para iniciar a configuração do controlador de domínio?

Resposta

- *Dcpromo.exe*

Prática: Criação de uma floresta do Windows Server 2008 R2

Nesta prática, você criará a floresta do AD DS para a Contoso, Ltd. Essa floresta será utilizada em todos os exercícios deste kit de treinamento. Você começará instalando o Windows Server 2008 R2 e realizando as tarefas de configuração da pós-instalação. Depois, adicionará a função AD DS e promoverá o servidor a um controlador de domínio na floresta contoso.com utilizando o Active Directory Domain Services Installation Wizard.

Exercício 1: Instale o Windows Server 2008 R2

Neste exercício, você instalará o Windows Server 2008 R2 em um computador ou máquina virtual.

1. Ligue o computador e insira o DVD de instalação do Windows Server 2008 R2.

   Se estiver utilizando uma máquina virtual (VM, virtual machine), poderá ter a opção de montar uma imagem ISO do DVD de instalação. Consulte a documentação da seção Help da VM para orientação.

   Se o disco rígido do sistema estiver vazio, o sistema deverá inicializar a partir do DVD. Se houver dados no disco, talvez seja solicitado que você pressione uma tecla para inicializar a partir do DVD.

   Se o sistema não inicializar a partir do DVD ou oferecer um menu de inicialização, acesse as configurações da BIOS do computador e configure a ordem de inicialização para que o sistema seja inicializado a partir do DVD.

   O Install Windows Wizard aparece conforme a Figura 1-4.

2. Selecione idioma, configuração regional e layout do teclado apropriados ao seu sistema e clique em Next.

3. Clique em Install Now.

   A configuração é iniciada, e uma lista de versões a serem instaladas é mostrada conforme a Figura 1-5.

4. Selecione Windows Server 2008 R2 Standard (Full Installation) e clique em Next.

5. Marque a caixa de seleção I Accept The License Terms e clique em Next.

6. Clique em Custom (Advanced).

7. Na página Where Do You Want To Install Windows, selecione a partição na qual você quer instalar o Windows Server 2008.

   Se precisar criar, excluir, estender ou formatar as partições, ou se precisar carregar um driver personalizado de armazenamento em massa para acessar o subsistema de disco, clique em Driver Options (Advanced).

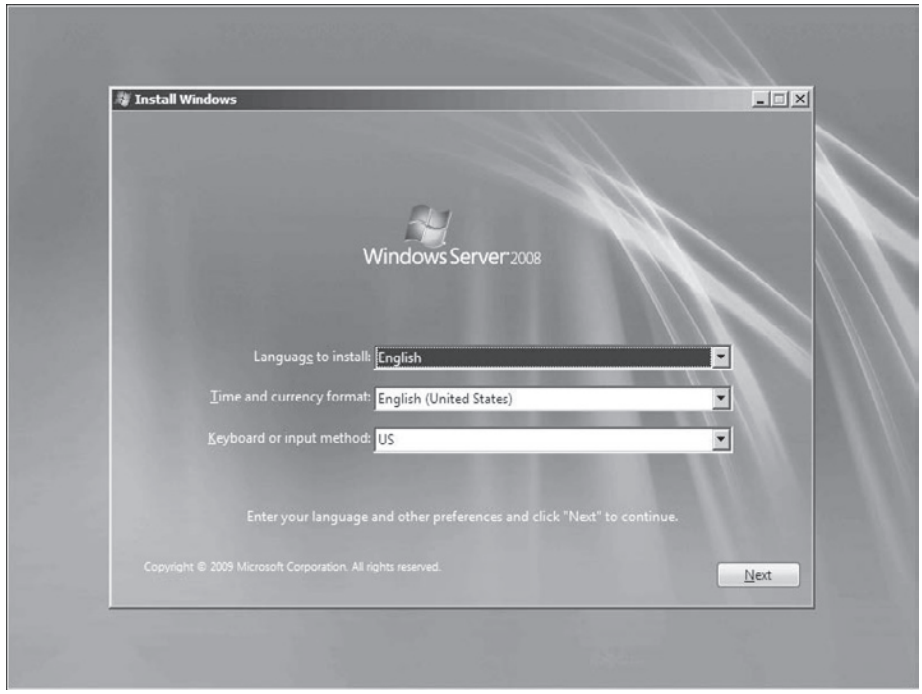

Figura 1-4 Install Windows Wizard.

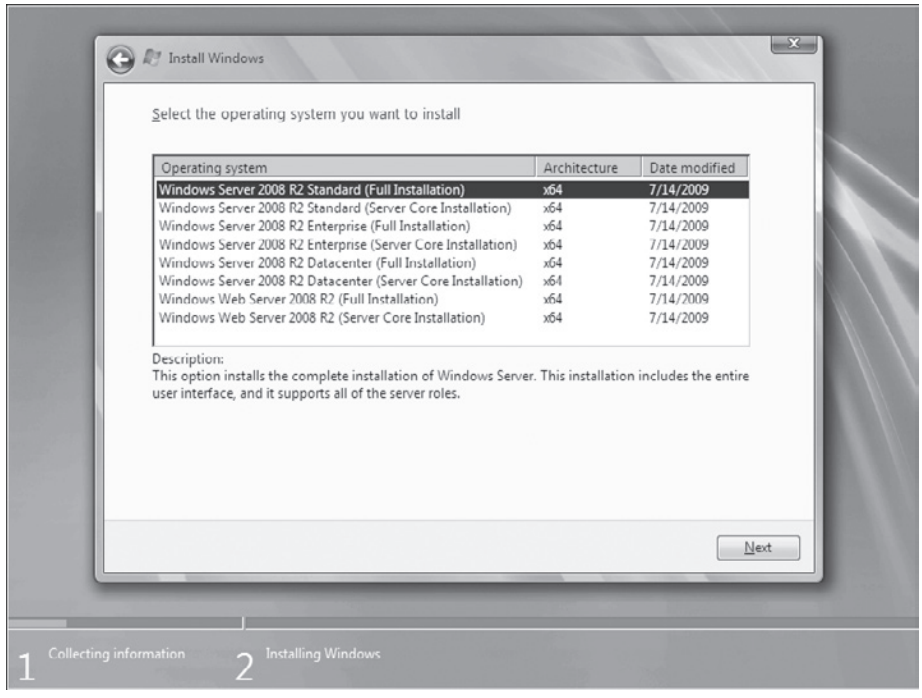

Figura 1-5 Página Select the operating system you want to install.

8. Clique em Next.

   A página Installing Windows aparece conforme a Figura 1-6. A janela informa o progresso da instalação do Windows.

   Nota: Se você estiver instalando sobre uma versão existente do Windows, o instalador emite um aviso neste ponto e solicita que você continue.

   A instalação do Windows Server 2008 R2 é baseada em imagens. Portanto, a instalação é significativamente mais rápida do que as versões anteriores do Windows, embora os sistemas operacionais sejam bem maiores do que as versões anteriores. O computador reiniciará uma ou mais vezes durante a instalação.

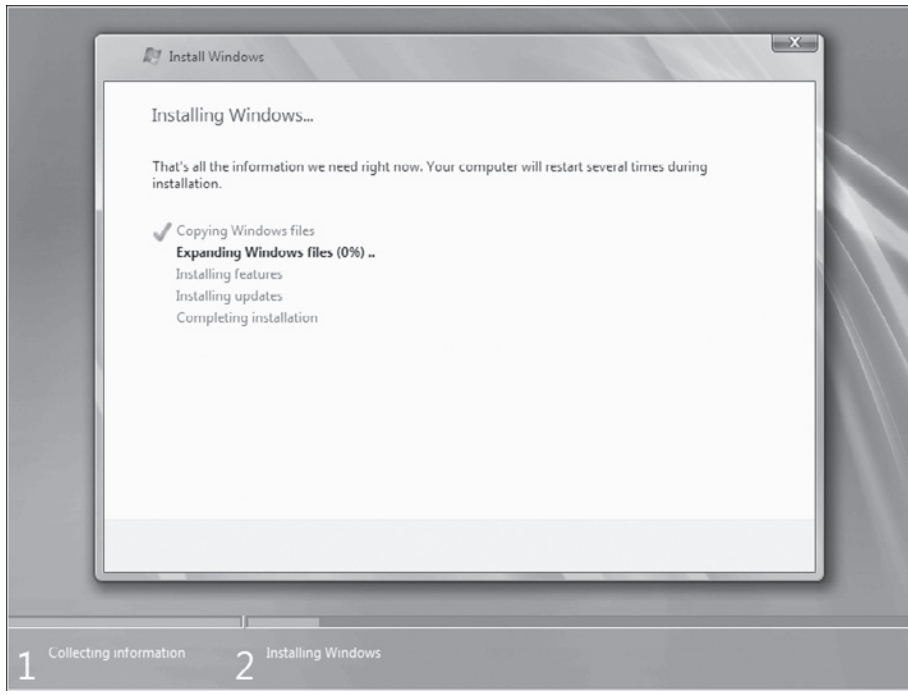

Figura 1-6 Página Installing Windows.

   Quando a instalação terminar, você será informado de que a senha do usuário precisa ser alterada antes de efetuar logon pela primeira vez.

9. Clique em OK.

10. Digite uma senha para a conta Administrator nas duas caixas New Password e Confirm Password e pressione Enter.

    A senha deve ter pelo menos sete caracteres e deve ter no mínimo três dos quatro seguintes tipos de caractere:

    - Maiúsculas: A-Z
    - Minúsculas: a-z

- Numéricos: 0-9
- Não alfanuméricos: símbolos como $, #, @ e !

> ***OBSERVAÇÃO*** **NÃO ESQUEÇA ESSA SENHA**
>
> Sem ela, você não será capaz de efetuar logon no servidor para realizar os outros exercícios neste kit de treinamento. Alternativamente, você pode selecionar a opção Create A Password Reset Disk para iniciar o assistente que cria um disco que pode ser usado para recuperar a senha caso ela seja extraviada ou esquecida.

11. Clique em OK.

    O desktop da conta Administrator aparece.

Exercício 2: Realize a configuração de pós-instalação

Neste exercício, você realizará a configuração da pós-instalação do servidor para preparar o servidor com o nome e as configurações de TCP/IP exigidos para os exercícios neste kit de treinamento.

1. Espere até o desktop da conta Administrator aparecer.

   A janela Initial Configuration Tasks (Tarefas de Configuração Inicial) aparece, conforme a Figura 1-7. Essa ferramenta é projetada para facilitar a realização das tarefas de melhor prática da configuração da pós-instalação.

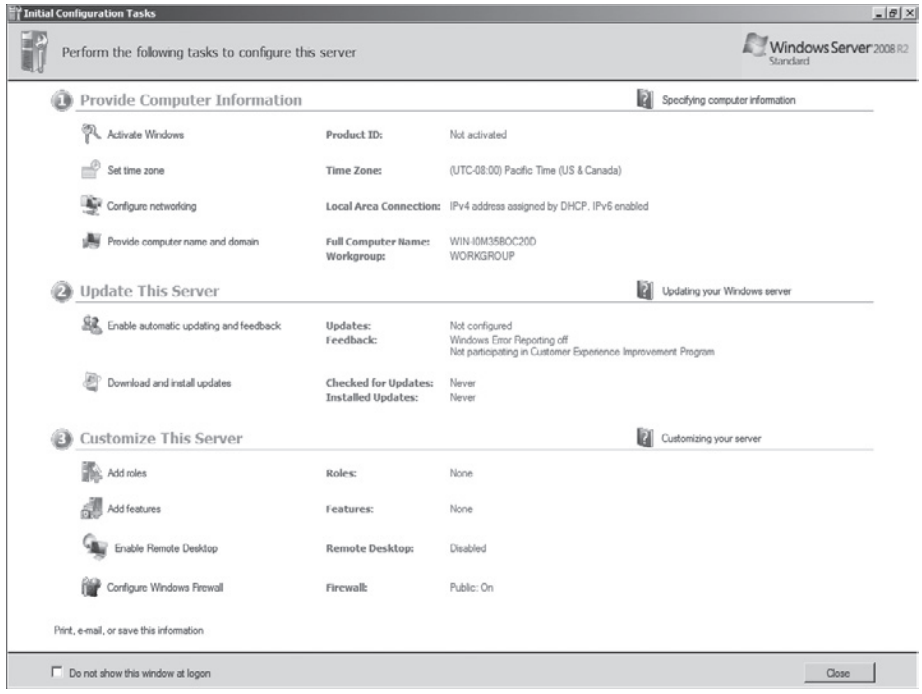

Figura 1-7 Janela Initial Configuration Tasks.

2. Na janela Initial Configuration Tasks, clique em Provide Computer Name And Domain.
3. Na janela System Properties na guia Computer Name, clique em Change.
4. Altere o texto na caixa Computer Name para SERVER01 e clique em OK.
5. Na caixa de diálogo Computer Name/Domain Changes, clique em OK.
6. Na caixa de diálogo System Properties, clique em Close.

   Você é solicitado a reiniciar o computador para aplicar essas alterações. Não reinicie o computador até que seja instruído a fazê-lo mais adiante neste exercício.
7. Clique em Restart Later.
8. Clique em Configure Networking na janela Initial Configuration Tasks.

   Os demais exercícios desta lição criam um domínio utilizando os endereços de IP no intervalo 10.0.0.11–10.0.0.20, com uma máscara de sub-rede de 255.255.255.0. Se esses endereços forem utilizados no seu ambiente de produção e o servidor estiver conectado ao seu ambiente de produção, você também deverá alterar os endereços IP usados neste livro para que o domínio contoso.com que você criará nestes exercícios não entre em conflito com sua rede de produção.
9. Clique com o botão direito do mouse e depois clique em Properties.
10. Clique em Internet Protocol Version 4 (TCP/IPv4) e, depois, em Properties.

    O Windows Server 2008 R2 também fornece suporte nativo ao Internet Protocol Version 6 (TCP/IPv6).
11. Clique em Use The Following IP Address. Insira a configuração a seguir:
    - IP address: **10.0.0.11**
    - Subnet mask: **255.255.255.0**
    - Default gateway: **10.0.0.1**
    - Preferred DNS server: **10.0.0.11**
12. Clique em OK e, então, em Close.
13. Feche a janela Network Connections.
14. Clique em Set Time Zone e configure o fuso horário conforme o seu ambiente.
15. Se o servidor tiver uma conexão à Internet, é altamente recomendável clicar em Download And Install Updates para que você possa atualizar o servidor com as atualizações de segurança mais recentes da Microsoft.

    Observe os links Add Roles e Add Features na janela Initial Configuration Tasks. No próximo exercício, você utilizará o Server Manager para adicionar funções e recursos ao SERVER01.

    Esses links são outra maneira de realizar as mesmas tarefas.

    O comportamento padrão da janela Initial Configuration Tasks é aparecer a cada vez que você efetuar logon no servidor.
16. Marque a caixa de seleção Do Not Show This Window At Logon para que a janela Initial Configuration Tasks não apareça da próxima vez que você efetuar logon.

Se você precisar abrir a janela Initial Configuration Tasks no futuro, execute o comando *Oobe.exe*.

17. Clique em Close.
18. Quando for solicitado a reiniciar, clique em Yes.

> ***OBSERVAÇÃO*** **CRIE UM SNAPSHOT DA SUA MÁQUINA VIRTUAL APÓS REINICIAR**
>
> Se você estiver utilizando uma máquina virtual para fazer este exercício e a máquina virtual permitir criar snapshots de um ponto no tempo do estado da máquina, crie um snapshot nesse momento. Essa instalação de linha de base do Windows Server 2008 R2 pode ser utilizada para fazer os exercícios neste capítulo, o que lhe permite testar vários métodos para adicionar a função AD DS.

Exercício 3: Instale uma nova floresta do Windows Server 2008 R2 com a Interface do Windows

Neste exercício, você adicionará a função AD DS ao servidor que instalou e configurou no Exercício 1, "Instale o Windows Server 2008 R2", e no Exercício 2, "Realize a configuração de pós-instalação."

1. Efetue logon no servidor com a conta Administrator e a senha usada no Exercício 1.

   Se o Server Manager não abrir automaticamente, abra-o a partir do grupo de programa Administrative Tools.
2. Na seção Roles Summary da home page, clique em Add Roles. Você pode precisar rolar para ver a porção Roles Summary da janela.
3. Na primeira página do Add Roles Wizard, clique em Next.
4. Na página Select Server Roles, marque a caixa de seleção ao lado do Active Directory Domain Services.
5. Quando for solicitado a adicionar os recursos exigidos para o Active Directory Domain Services, clique em Add Required Features para prosseguir.
6. Na página Select Server Roles, clique em Next.
7. Na página Active Directory Domain Services, clique em Next.
8. Na página Confirm Installation Selections, clique em Install.

   A página Installation Progress informa o status das tarefas da instalação.
9. Na página Installation Results, confirme se a instalação foi bem-sucedida e clique em Close.

   Na seção Roles Summary da home page do Server Manager, você perceberá uma mensagem de erro indicada por um círculo vermelho com um x branco. Você também verá uma mensagem na seção Active Directory Domain Services da página. Esses dois links o levarão à página de funções Active Directory Domain Services do Server Manager, mostrada na Figura 1-8. A mensagem exibida lembra que é necessário executar o *Dcpromo.exe*, o que você fará no próximo exercício.

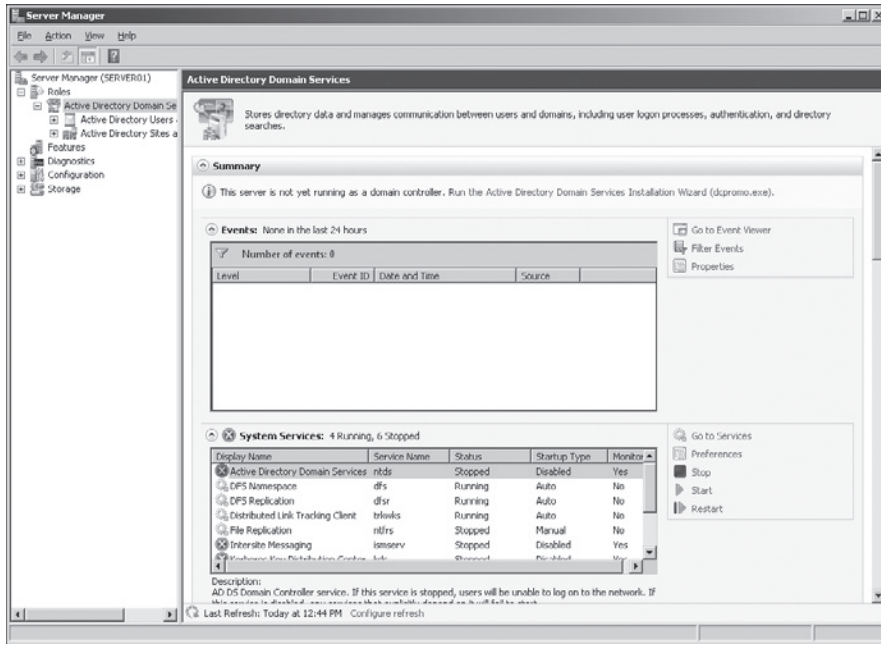

Figura 1-8 Página de funções Active Directory Domain Services no Server Manager.

Exercício 4: Instale uma nova floresta do Windows Server 2008 R2

Neste exercício, você utilizará o Active Directory Domain Services Installation Wizard (*Dcpromo.exe*) para criar uma nova floresta do Windows Server 2008.

1. Clique em Start e em Run, digite **Dcpromo.exe** e, então, clique em OK.

> ***OBSERVAÇÃO*** **O DCPROMO ADICIONARÁ A FUNÇÃO AD DS SE NECESSÁRIO**
>
> No exercício anterior, você adicionou a função AD DS utilizando o Server Manager. Mas, se você executar o *Dcpromo.exe* em um servidor em que a função AD DS ainda não foi instalada, o *Dcpromo.exe* instalará a função automaticamente.

   O Active Directory Domain Services Installation Wizard aparece. No Capítulo 10, você aprenderá sobre os modos avançados desse assistente.

2. Clique em Next.
3. Na página Operating System Compatibility, revise o aviso sobre as configurações de segurança padrão para os controladores de domínio do Windows Server 2008 R2 e clique em Next.
4. Na página Choose a Deployment Configuration, escolha Create A New Domain In A New Forest e clique em Next.
5. Na página Name The Forest Root Domain, digite **contoso.com** e clique em Next.

O sistema realiza uma verificação para assegurar que o nome de DNS e o nome NetBIOS para a floresta ainda não estão em uso na rede.

6. Na página Set Forest Functional Level, escolha nível funcional de floresta do Windows Server 2008 R2 e clique em Next.

   Cada um dos níveis funcionais é descrito na caixa Details na página. Escolher o nível funcional de floresta do Windows Server 2008 R2 assegura que todos os domínios na floresta operem no nível funcional do domínio do Windows Server 2008 R2, o que habilita vários novos recursos fornecidos pelo Windows Server 2008 R2. Você aprenderá mais sobre os níveis funcionais no Capítulo 12.

   A página Additional Domain Controller Options aparece. O DNS Server é selecionado por padrão. O Active Directory Domain Services Installation Wizard cria uma infraestrutura de DNS durante a instalação do AD DS. O primeiro controlador de domínio em uma floresta deve ser um servidor de catálogo global (GC) e não pode ser um controlador de domínio somente leitura (RODC, Read-only Domain Controller).

7. Clique em Next.

   Um aviso aparece informando que uma delegação do servidor de DNS não pode ser criada. No contexto deste exercício, você pode ignorar esse erro. As delegações dos domínios de DNS serão discutidas no Capítulo 9. Clique em Yes para ignorar a mensagem.

8. Na página Location For Database, Log Files, And SYSVOL, aceite as localizações padrão para o arquivo de banco de dados, os arquivos de log de serviço de diretório e os arquivos SYSVOL e clique em Next.

   A melhor prática em um ambiente de produção é armazenar esses arquivos em três volumes separados que não contêm aplicativos ou outros arquivos não relacionados ao AD DS. Esse design de melhores práticas aprimora o desempenho e aumenta a eficiência do backup e da restauração.

9. Na página Directory Services Restore Mode Administrator Password, digite uma senha forte nas caixas Password and Confirmed Password. Clique em Next.

   Não se esqueça da senha que você atribuiu ao Directory Services Restore Mode Administrator.

10. Na página Summary, revise suas seleções.

    Se alguma configuração estiver incorreta, clique em Back para fazer as modificações.

11. Clique em Next e, em seguida, clique em Finish.

    A configuração do AD DS inicia. O servidor precisará ser reinicializado quando o processo estiver concluído.

Resumo da lição

- Os serviços do Active Directory compreendem uma solução integrada para identidade e acesso nas redes corporativas.
- O Active Directory Domain Services (AD DS) fornece o serviço de diretório e os componentes da autenticação da solução IDA. Além disso, o AD DS facilita o gerenciamento até de redes distribuídas grandes e complexas.

- Os sistemas do Windows Server 2008 são configurados com base nas funções que eles executam. Você pode adicionar a função AD DS utilizando o Server Manager.
- Utilize o *Dcpromo.exe* para configurar o AD DS e criar um controlador de domínio.

Revisão da lição

Responda às questões a seguir para testar seu conhecimento sobre a Lição 1, "Instalação do Active Directory Domain Services". As perguntas também estão disponíveis no CD do livro (em inglês) se você preferir revisá-las na forma eletrônica.

> ***OBSERVAÇÃO*** **RESPOSTAS**
>
> As respostas a estas perguntas e as explicações das respostas estão na seção "Respostas" no final do livro.

1. O que é exigido para criar um controlador de domínio com sucesso? (Cada resposta correta apresenta parte da solução. Escolha todas as que se aplicam.)
   - **A.** Um nome de domínio de DNS válido
   - **B.** Um nome NetBIOS válido
   - **C.** Um servidor DHCP para atribuir um endereço IP ao controlador de domínio
   - **D.** Um servidor de DNS
2. A Trey Research adquiriu recentemente a Litware, Inc. Por causa de questões regulamentadoras relacionadas à replicação de dados, ela decidiu configurar um domínio filho na floresta de usuários e computadores da Litware. A floresta da Trey Research atualmente contém apenas controladores de domínio do Windows Server 2008 R2. O novo domínio será criado promovendo-se um controlador de domínio do Windows Server 2008 R2, mas talvez você precise utilizar os sistemas existentes do Windows Server 2003 como controladores de domínio no domínio Litware. Que configuração dos níveis funcionais será apropriada?
   - **A.** Nível funcional da floresta do Windows Server 2008 R2 e nível funcional do domínio do Windows Server 2008 R2 para o domínio Litware
   - **B.** Nível funcional da floresta do Windows Server 2008 R2 e nível funcional do domínio do Windows Server 2003 para o domínio Litware
   - **C.** Nível funcional da floresta do Windows Server 2003 e nível funcional do domínio do Windows Server 2008 R2 para o domínio Litware
   - **D.** Nível funcional da floresta do Windows Server 2003 e nível funcional do domínio do Windows Server 2003 para o domínio Litware

Lição 2: Active Directory Domain Services no Server Core

A segurança é um fator importante a ser considerado ao implantar servidores com a função Active Directory Domain Services (AD DS) instalada. Muitas organizações armazenam dados sensíveis no diretório, como informações pessoais e senhas de usuários, que devem ser protegidos adequadamente. Embora a configuração baseada em função do Windows Server 2008 R2 reduza a superfície de ataque de um servidor, instalando apenas os componentes e serviços exigidos pelas suas funções, é possível reduzir a superfície de ataque do servidor ainda mais instalando o Windows Server 2008 R2 com a opção de instalação do Server Core. Trata-se de uma instalação mínima do Windows Server que instala apenas os componentes mais críticos do sistema operacional básico exigidos para executar o Windows Server 2008 R2. A maioria dos elementos da interface gráfica do usuário (GUI, graphical user interface) Windows não é instalada como parte da instalação do Server Core, limitando a capacidade de usuários mal-intencionados de obter acesso ao servidor usando a interface familiar do Windows Explorer.

Uma instalação do Server Core pode ser administrada de outro servidor usando ferramentas remotas da GUI, como o Server Manager, para as tarefas mais comuns. Contudo, para gerenciar uma instalação do Server Core localmente, deve-se conhecer as ferramentas de linha de comando necessárias para administrar um servidor Windows Server 2008 R2 e suas funções instaladas. Nesta lição, você aprenderá mais sobre a opção de instalação do Server Core. Você também aprenderá a configurar um controlador de domínio a partir da linha de comando em uma instalação do Server Core e a remover os controladores de domínio a partir de um domínio.

Depois de ler esta lição, você será capaz de:

- Identificar as vantagens e a funcionalidade da instalação do Server Core.
- Instalar e configurar o Server Core.
- Adicionar e remover o AD DS utilizando as ferramentas de linha de comando.

Tempo estimado da lição: 60 minutos

Introdução ao Server Core

A instalação do Server Core do Windows Server 2008 R2 é uma instalação mínima do Windows que consome aproximadamente 3 GB de espaço de disco e menos de 256 MB de memória e limita as funções e os recursos de servidor que podem ser adicionados, mas pode aprimorar a segurança e a gerenciabilidade do servidor reduzindo a superfície de ataque. O número de serviços e componentes em execução em um dado momento qualquer é limitado, assim há menos oportunidades para que um usuário mal-intencionado comprometa a segurança do servidor. Devido ao número reduzido de funções e recursos instalados, a instalação do Server Core também reduz a carga do gerenciamento do servidor, o que exige menos atualizações e menos manutenção.

O Server Core suporta as seguintes funções de servidor:

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- BranchCache Hosted Cache
- DNS Server
- Dynamic Host Configuration Protocol (DHCP) Server
- File Services
- Hyper-V
- Print and Media Services
- Streaming Media Services
- Web Server (IIS) (incluindo um subconjunto de ASP.NET)

O Server Core também suporta estes recursos opcionais:

- Failover Clustering
- Multipath I/O
- Network Load Balancing
- Quality of Service (QoS)
- Removable Storage Management
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet client
- Windows Bitlocker Drive Encryption
- Windows Internet Naming Service (WINS)
- Windows-on-Windows 64-bit (WoW64)
- Windows PowerShell
- Windows Server Backup

Instalação do Server Core

Você pode instalar o Server Core utilizando os mesmos passos apresentados no Exercício 1 da Lição 1.

Os seguintes pontos descrevem as principais diferenças entre uma instalação completa do Windows Server 2008 R2 e a instalação do Server Core:

- Você deve selecionar a opção Server Core Installation ao executar o assistente de instalação do Windows Server 2008 R2, conforme a Figura 1-9.

- No final do processo de instalação, aparecerá uma janela do prompt de comando em vez da janela de GUI do Windows Server 2008 R2.

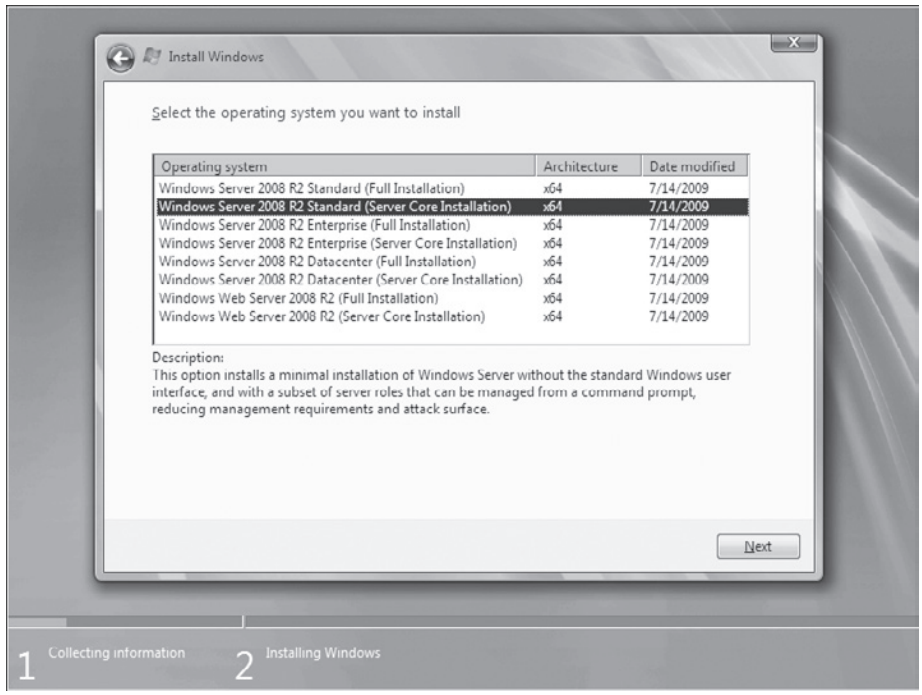

Figura 1-9 Página de seleção de sistemas operacionais do Install Windows Wizard.

Realização das tarefas de configuração iniciais

Em um servidor executando uma instalação completa do Windows Server 2008 R2, a janela Initial Configuration Tasks aparece para orientá-lo na configuração da pós-instalação do servidor. A instalação do Server Core não fornece qualquer GUI, portanto, você precisa concluir as tarefas utilizando as ferramentas de linha de comando. A Tabela 1-1 lista as tarefas de configuração comuns e os comandos que você pode utilizar. Para aprender mais sobre qualquer comando, abra um prompt de comando e digite o nome do comando seguido por **/?**.

Tabela 1-1 Comandos da configuração do Server Core

Tarefa	Comando
Alterar a senha de administrador	*Net user administrator **
Especificar uma configuração de IPv4 estático	*Netsh interface ipv4*
Ativar Windows Server	*Cscript c:windowssystem32slmgr.vbs -ato*
Ingressar em um domínio	*Netdom*

(Continua)

Tabela 1-1 Comandos da configuração do Server Core *(Continuação)*

Tarefa	Comando
Instalar componentes opcionais (funções, serviços de função ou recursos)	Pacote ou recurso *Ocsetup.exe* Observe que os nomes de pacote ou recurso diferenciam maiúsculas de minúsculas. Listar os pacotes e recursos válidos digitando o comando **Ocsetup /?**.
Exibir funções, componentes e recursos instalados	*Oclist.exe*
Ativar Remote Desktop (Área de Trabalho Remota)	*Cscript c:\windows\system32\scregedit.wsf /AR 0*
Promover um controlador de domínio	*Dcpromo.exe*
Configurar o DNS	*Dnscmd.exe*
Configurar o DFS	*Dfscmd.exe*

O comando *Ocsetup.exe* adiciona funções e recursos do Server Core suportados ao servidor. A exceção a esse regra é o AD DS. Não utilize o *Ocsetup.exe* para adicionar ou remover o AD DS. Utilize, em vez disso, o *Dcpromo.exe*.

Configuração do Servidor

O Windows Server 2008 R2 inclui uma ferramenta de linha de comando baseada em menu chamada *Configuração do Servidor* (Server Configuration) para tarefas administrativas básicas (ver Figura 1-10). A Configuração do Servidor oferece um conjunto simples de comandos administrativos que podem ser executados digitando-se números de menu baseados em contexto mapeados para executáveis de linha de comando, em vez de digitar a sintaxe dos executáveis de linha de comando manualmente. Embora a Configuração do Servidor possa economizar tempo nas tarefas administrativas simples, tarefas mais complicadas, como configurar o Active Directory Domain Services, ainda precisam ser realizadas a partir da linha de comando.

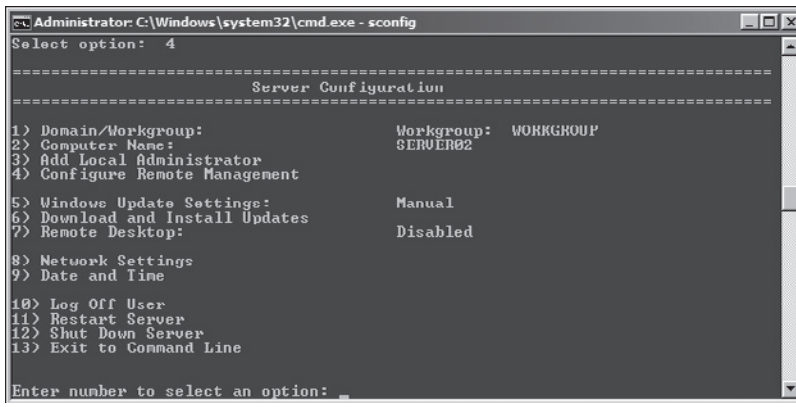

Figura 1-10 Janela Server Configuration.

> ***OBSERVAÇÃO*** **EXECUÇÃO DA CONFIGURAÇÃO DO SERVIDOR**
>
> Para executar a Configuração do Servidor na instalação do Server Core do Windows Server 2008 R2, digite **sconfig.exe** no prompt de comando e depois pressione Enter.

Adição do AD DS a uma instalação do Server Core

Como não há um Active Directory Domain Services Installation Wizard no Server Core, você deve utilizar a linha de comando para executar o *Dcpromo.exe* com os parâmetros que configuram o AD DS. Para aprender sobre os parâmetros do *Dcpromo.exe*, abra uma linha de comando e digite **dcpromo.exe /?**. Cada cenário de configuração tem informações adicionais sobre uso. Por exemplo, digite **dcpromo.exe /?:Promotion** para obter instruções de uso detalhadas para promover um controlador de domínio.

> ***MAIS INFORMAÇÕES*** **PARÂMETROS DA INSTALAÇÃO AUTÔNOMA**
>
> Uma listagem dos parâmetros da instalação autônoma para AD DS está disponível em *http://technet.microsoft.com/en-us/library/cc732086(WS.10).aspx*.

Remoção de controladores de domínio

Ocasionalmente, talvez haja alguma razão para colocar um controlador de domínio offline a fim de fazer uma manutenção extensa ou removê-lo de forma permanente. É importante que você remova um controlador de domínio de maneira correta para que as informações sobre ele sejam removidas do Active Directory.

Para remover um controlador de domínio, utilize o comando *Dcpromo.exe*. Se você executar o comando em um controlador de domínio utilizando a interface do Windows, o Active Directory Domain Services Installation Wizard guiará você ao longo do processo. Se quiser utilizar a linha de comando ou estiver removendo o AD DS de uma instalação do Server Core, digite **dcpromo.exe /?:Demotion** para obter informações de uso com relação aos parâmetros da operação de rebaixamento.

Ao rebaixar um controlador de domínio, você deve fornecer uma senha que será atribuída à conta Administrator local do servidor depois do rebaixamento.

Prática: Instalação de um controlador de domínio do Server Core

Nesta prática, você adicionará um controlador de domínio à floresta contoso.com criada na prática da Lição 1. Para aumentar a segurança e reduzir a sobrecarga do gerenciamento do novo DC, você promoverá um servidor que executa o Server Core a controlador de domínio. Antes de fazer os exercícios desta prática, você precisa completar a prática da Lição 1.

Exercício 1: Instale o Server Core

Neste exercício, você instalará o Server Core em um computador ou em uma máquina virtual.

1. Insira o DVD de instalação do Windows Server 2008 R2.

   Se estiver utilizando uma VM, talvez você tenha a opção de montar uma imagem ISO do DVD de instalação. Consulte a documentação da seção Help da VM para orientação.

2. Ligue o computador.

   Se o disco rígido do sistema estiver vazio, o sistema deverá inicializar a partir do DVD. Se houver dados no disco, talvez seja solicitado que você pressione uma tecla para inicializar a partir do DVD.

   Se o sistema não inicializar a partir do DVD ou oferecer um menu de inicialização, acesse as configurações da BIOS do computador e configure a ordem de inicialização para que o sistema seja inicializado a partir do DVD.

3. Selecione idioma, configuração regional e layout do teclado apropriados ao seu sistema e clique em Next.
4. Clique em Install Now.
5. Selecione Windows Server 2008 R2 Standard (Server Core Installation) e clique em Next.
6. Marque a caixa de seleção I Accept The License Terms e clique em Next.
7. Clique em Custom (Advanced).
8. Na página Where Do You Want To Install Windows, selecione o disco no qual você quer instalar o Windows Server 2008 R2.

   Se precisar criar, excluir, estender ou formatar as partições, ou se precisar carregar um driver personalizado de armazenamento em massa para acessar o subsistema de disco, clique em Driver Options (Advanced).

9. Clique em Next.
10. Quando a instalação terminar, você será informado de que a senha do Administrador precisa ser alterada. Clique em OK.
11. Digite uma senha para a conta Administrator nas duas caixas New Password e Confirm Password e pressione Enter.

    A senha deve ter pelo menos sete caracteres e deve ter no mínimo três dos quatro tipos de caractere seguintes:

    A. Maiúsculas: A–Z

    B. Minúsculas: a–z

    C. Numéricos: 0–9

    D. Não alfanuméricos: símbolos como $, #, @ e !

> ***OBSERVAÇÃO*** **NÃO ESQUEÇA ESSA SENHA**
>
> Sem ela, você não conseguirá efetuar logon no servidor para realizar os outros exercícios deste kit de treinamento.

12. Clique em OK.

    O prompt de comando para a conta Administrator aparece.

Exercício 2: Realize a configuração de pós-instalação no Server Core

Neste exercício, você realizará a configuração da pós-instalação do servidor para prepará-lo com o nome e as configurações de TCP/IP exigidas para os exercícios restantes nesta lição.

Nota: Assegure-se de que SERVER01 está sendo executado ao realizar estes exercícios. SERVER02 acessa o banco de dados AD DS de SERVER01 ao longo do exercício.

1. Renomeie o servidor digitando **netdom renamecomputer %computername%/ newname: SERVER02**. Você será solicitado a pressionar Y para confirmar a operação. Alternativamente, você pode configurar o nome do computador digitando **sconfig** na linha de comando e usando a ferramenta de configuração do servidor baseada em menu. De qualquer forma, você será solicitado a reiniciar o seu computador após mudar o nome dele. Não reinicie o computador até ser instruído a fazê-lo mais adiante nesta prática.

   A ferramenta de configuração do servidor também pode ser usada para realizar os passos 2 e 6 do exercício.

2. Configure o endereço IPv4 do servidor digitando cada um dos comandos netsh a seguir:

   ```
   netsh interface ipv4 set address name="Local Area Connection"
      source=static address=10.0.0.12 mask=255.255.255.0 gateway=10.0.0.1 1

   netsh interface ipv4 set dnsserver name="Local Area Connection"
      source=static address=10.0.0.11 primary
   ```

   Se você receber um erro, verifique se sua interface de rede se chama "Local Area Connection" digitando netsh interface Show interface. Substitua a "Local Area Connection" mostrada nos comandos acima pelo nome correto da sua conexão de rede.

3. Confirme a configuração IP que você digitou anteriormente com o comando **ipconfig /all**.

4. Reinicie digitando **shutdown /r /t 0**.

5. Efetue logon como Administrator.

6. Adicione o domínio digitando o comando **netdom join %computername% /domain: contoso.com**.

7. Reinicie digitando **shutdown /r /t 0** e então efetue logon novamente como Administrator.

8. Exiba as funções de servidor instaladas digitando **oclist | more**.

   Observe o identificador de pacote para a função do servidor de DNS: DNS-Server--Core-Role.

9. Digite **ocsetup** e pressione Enter.

   Surpresa! Há uma pequena quantidade de GUI no Server Core.

10. Clique em OK para fechar a janela.

11. Digite **ocsetup DNS-Server-Core-Role**.

    Os identificadores de pacote diferenciam maiúsculas de minúsculas.

12. Digite **oclist** e confirme que a função do servidor de DNS está instalada.

Exercício 3: Crie um controlador de domínio com o Server Core

Neste exercício, você adicionará a função AD DS à instalação do Server Core utilizando o comando *Dcpromo.exe*.

1. Digite **dcpromo.exe /?** e pressione Enter.

   Revise as informações sobre o uso.

2. Digite **dcpromo.exe /?:Promotion** e pressione Enter.

   Revise as informações sobre o uso.

3. Digite o comando a seguir para adicionar e configurar a função AD DS:

   ```
   dcpromo /unattend /replicaornewdomain:replica
   /replicaDomainDNSName:contoso.com /ConfirmGC:Yes
   /UserName:Administrator UserDomain:Contoso /Password:*
   /safeModeAdminPassword:P@ssword
   ```

   onde * é a senha que você usou no Exercício 1.

4. Quando solicitado a inserir as credenciais de rede, digite a senha da conta Administrator no domínio contoso.com e clique em OK.

   A função AD DS será instalada e configurada, e, então, o servidor reiniciará.

Exercício 4: Remova um controlador de domínio

Neste exercício, você removerá o AD DS da instalação do Server Core.

1. Efetue logon na instalação do Server Core como Administrator.
2. Digite **dcpromo /unattend /AdministratorPassword:*senha*** onde *senha* é uma senha forte que se tornará a senha de administrador local do servidor depois que o AD DS for removido. Pressione Enter.

Resumo da lição

- O Windows Server 2008 R2 Server Core Installation, mais conhecido como Server Core, é uma instalação mínima do Windows que suporta um subconjunto de funções e recursos de servidor.
- O Server Core pode aprimorar a segurança e a gerenciabilidade dos servidores Windows.
- O comando *Ocsetup.exe* é utilizado para adição e remoção de funções do Server Core, exceto o AD DS, que é adicionado utilizando-se o *Dcpromo.exe*.
- Você pode configurar completamente uma operação de promoção ou rebaixamento utilizando o comando *Dcpromo.exe /unattend* com os parâmetros apropriados para a operação.

Revisão da lição

Responda às perguntas a seguir para testar seu conhecimento sobre as informações da Lição 2, "Active Directory Domain Services no Server Core". As perguntas também estão disponíveis no CD do livro (em inglês) se você preferir revisá-las na forma eletrônica.

> ***OBSERVAÇÃO*** **RESPOSTAS**
>
> As respostas a estas perguntas e as explicações das respostas estão na seção "Respostas" no final do livro.

1. Você está conectado como Administrator em SERVER02, um dos quatro controladores de domínio no domínio contoso.com que executam o Server Core. Você quer rebaixar o controlador de domínio. Qual dos itens a seguir é exigido?
   - **A.** A senha de Administrator local
   - **B.** As credenciais para um usuário no grupo Domain Admins
   - **C.** As credenciais para um usuário no grupo Domain Controllers
   - **D.** O endereço de um servidor de DNS
2. SERVER02 está executando o Server Core. Ele já está configurado com a função AD DS. Você quer adicionar o Active Directory Federated Services (AD FS) ao servidor. O que você deve fazer?
   - **A.** Instalar a função Active Directory Certificate Services.
   - **B.** Instalar a função Active Directory Federated Services.
   - **C.** Instalar a função AD Rights Management Services.
   - **D.** Reinstalar o servidor como Windows Server 2008 R2 (Full Installation).

Revisão do capítulo

Para reforçar as habilidades aprendidas neste capítulo, você pode:

- Ler o resumo do capítulo.
- Ler a lista de termos-chave introduzidos neste capítulo.
- Completar o cenário. Esse cenário especifica uma situação do mundo real que envolve os tópicos deste capítulo e solicita que você crie uma solução.
- Fazer um teste.

Resumo do capítulo

- Os serviços do Active Directory executam as funções de acesso de identidade e as funções de gerenciamento para suportar a rede de uma organização.
- Um controlador de domínio hospeda o armazenamento de dados e serviços correlacionados do Active Directory. Os controladores de domínio são criados adicionando-se a função AD DS e então configurando o AD DS utilizando o *Dcpromo.exe*.
- O Server Core ajuda a reduzir os custos do gerenciamento e aumentar a segurança dos controladores de domínio.

Termos-chave

Os seguintes termos foram introduzidos neste capítulo. Você sabe o que eles significam?

- autenticação
- catálogo global (ou conjunto de atributos parcial)
- domínio
- domínio raiz da floresta
- esquema
- floresta
- Kerberos
- nível funcional
- repositório de identidades
- site

Cenário

No cenário a seguir, você aplicará o que aprendeu sobre a instalação do Server Core e os serviços de domínio do Active Directory relacionados. As respostas a estas perguntas estão na seção "Respostas" no final deste livro.

Cenário: Criação de uma floresta do Active Directory

Você foi solicitado a criar uma nova floresta do Active Directory para um novo projeto de pesquisa na Trey Research. Por causa da natureza sigilosa do projeto, você precisa assegurar que o diretório seja o mais seguro possível. Você está pensando em utilizar uma instalação do Server Core nos dois servidores que funcionarão como controladores de domínio.

- Você pode criar uma floresta do Active Directory utilizando apenas os servidores do Server Core?
- Que comando você utilizará para configurar os endereços IP estáticos nos servidores?
- Que comando você utilizará para adicionar a função de servidor de DNS?
- Que comando você utilizará para adicionar o Active Directory Domain Services?

Faça um teste

Os testes no CD deste livro (em inglês) oferecem muitas opções. Você pode fazer um teste sobre apenas um objetivo de exame ou sobre todo o conteúdo do exame de certificação 70-640. É possível configurar o teste para que ele simule a experiência de fazer um exame de certificação ou configurá-lo no modo de estudo (study mode) para examinar as respostas corretas e explicações depois de cada questão.

> ***MAIS INFORMAÇÕES*** **TESTES**
>
> Para mais detalhes sobre todas as opções de testes disponíveis, consulte a seção "Como utilizar os testes", na Introdução deste livro.