CAPÍTULO 1

Visão geral da administração do Windows Server 2012

O Microsoft Windows Server 2012 é um sistema operacional de servidor poderoso, versátil e completo, elaborado a partir dos aperfeiçoamentos disponibilizados no Windows Server 2008 R2 pela Microsoft. O Windows Server 2012 e o Windows 8 compartilham alguns recursos porque fizeram parte de um mesmo projeto de desenvolvimento. Esses recursos têm uma base de códigos em comum e estão presentes em muitas áreas do sistema operacional, incluindo gerenciamento, segurança, rede e armazenamento. Por isso, é possível aplicar grande parte do conhecimento sobre o Windows 8 ao utilizar o Windows Server 2012.

Este capítulo faz uma introdução ao Windows Server 2012 e explora o modo como as modificações na arquitetura afetam a maneira de gerenciar e trabalhar com o Windows Server 2012. No decorrer deste capítulo e dos capítulos seguintes, você encontrará discussões sobre os diversos aprimoramentos e recursos de segurança. Essas discussões exploram todos os aspectos de segurança do computador, incluindo a segurança física, a segurança de informações e a segurança de rede. Embora o foco deste livro seja a administração do Windows Server 2012, as dicas e técnicas apresentadas podem auxiliar qualquer pessoa que preste suporte, desenvolva ou trabalhe com o sistema operacional Windows Server 2012.

Windows Server 2012 e Windows 8

Antes de implantar o Windows Server 2012, você deve planejar atentamente a arquitetura do servidor. Como parte do planejamento de implementação, é preciso considerar a configuração de software que será utilizada e modificar a configuração de hardware em cada servidor para adequá-la aos requisitos relacionados. Para mais flexibilidade nas implantações de servidores, é possível implantar servidores utilizando um destes três tipos de instalação:

- **Instalação com interface gráfica do usuário (GUI, graphical user interface)** Opção de instalação que fornece todas as funcionalidades; também cha-

mada de *instalação de servidor completo*. É possível configurar um servidor de forma a obter qualquer combinação permitida de funções, serviços de funções e recursos, além de uma interface de usuário completa ser fornecida para o gerenciamento do servidor. Essa opção de instalação oferece uma solução mais dinâmica e é recomendada para implantações do Windows Server 2012 em que a função de servidor possa mudar no decorrer do tempo.

- **Instalação Server Core** Opção de instalação mínima que fornece um subconjunto fixo de funções mas não inclui o Server Graphical Shell (Shell Gráfico de Servidor), o Microsoft Management Console (MMC, Console de Gerenciamento Microsoft) e o Desktop Experience. É possível configurar uma instalação Server Core com um conjunto limitado de funções. Uma interface de usuário limitada é fornecida para o gerenciamento do servidor, e grande parte do gerenciamento é realizada localmente em um prompt de comando ou remotamente por meio de ferramentas de gerenciamento. Essa opção de instalação é ideal para as situações nas quais deseja-se dedicar servidores a uma função de servidor específica ou a uma combinação de funções. Pelo fato de não haver funcionalidades adicionais instaladas, a sobrecarga causada por outros serviços é reduzida, por isso há mais recursos para a função ou funções dedicadas.
- **Instalação com interface mínima do servidor** Opção intermediária de instalação na qual é realizada uma instalação completa e, em seguida, o Server Graphical Shell é removido. Resta uma interface de usuário mínima, o Microsoft Management Console, o Server Manager (Gerenciador de Servidores) e um subconjunto do Control Panel (Painel de Controle) para gerenciamento local. Essa opção de instalação é ideal para situações nas quais você deseja controlar minuciosamente as tarefas que podem ser realizadas em um servidor, assim como as funções e os recursos instalados, mas nas quais ainda deseja a conveniência da interface gráfica.

Escolhe-se o tipo de instalação durante a instalação do sistema operacional. Diferentemente das versões anteriores do Windows Server, é possível alterar o tipo de instalação após a instalação de um servidor. Uma diferença-chave entre os tipos de instalação refere-se à presença das ferramentas gráficas de gerenciamento e do shell gráfico. Uma instalação Server Core não possui esses recursos; uma instalação de servidor completo possui os dois; e uma instalação com interface mínima possui apenas as ferramentas gráficas de gerenciamento.

MAIS INFORMAÇÕES **Diversas funções e recursos de servidor requerem o shell gráfico, como a função Fax Server (Servidor de Fax), o Remote Desktop Session Host (Host de Sessão da Área de Trabalho Remota), o Windows Deployment Services (Serviços de Implantação do Windows) e a interface de usuário para Internet Printing (Impressão via Internet). Além desses casos, no Event Viewer (Visualizador de Eventos), o modo de exibição Details requer o shell gráfico, assim como a interface gráfica para o Windows Firewall.**

Assim como o Windows 8, o Windows Server 2012 possui os seguintes recursos:

- **Modularização para independência de idiomas e geração de imagens de disco com independência de hardware** Cada componente do sistema operacional é projetado como um módulo independente que pode ser adicionado ou removido facilmente. Essa funcionalidade fornece a base para a configuração da arquitetura do Windows Server 2012. A Microsoft distribui o Windows Server

2012 através de imagens de disco no formato de arquivo de imagem do Windows (WIM), que utiliza compactação e armazenamento em instância única para reduzir significativamente o tamanho dos arquivos de imagem.

- **Ambientes de pré-instalação e de pré-inicialização** O Windows Preinstallation Environment 4.0 (Windows PE 4.0) substitui o MS-DOS como o ambiente de pré-instalação e fornece um ambiente de pré-inicialização para instalação, implantação, recuperação e solução de problemas. O ambiente de pré-instalação do Windows (Windows PE) fornece um ambiente de inicialização com um gerenciador que permite escolher o aplicativo a ser utilizado para carregar o sistema operacional. Em sistemas com múltiplos sistemas operacionais, o acesso aos sistemas operacionais anteriores ao Windows 7 ocorre no ambiente de inicialização, por meio da entrada para sistemas operacionais anteriores.
- **Controle de conta de usuário e elevação de privilégio** O User Account Control (UAC, Controle de Conta de Usuário) aumenta a segurança do computador através da separação entre contas de administrador e contas de usuário padrão. Com o UAC, todos os aplicativos são executados utilizando os privilégios de administrador ou de usuário padrão, e, por padrão, um prompt de segurança é mostrado toda vez que um aplicativo que requer privilégios de administrador for executado. A forma como o prompt de segurança trabalha depende das configurações da Group Policy (política de grupo). Se o logon for realizado utilizando a conta de Administrador interno, normalmente não serão mostrados prompts de elevação.

No Windows 8 e no Windows Server 2012, recursos com bases de código comuns possuem interfaces de gerenciamento idênticas. Na verdade, praticamente todos os utilitários do Control Panel disponíveis no Windows Server 2012 são idênticos ou muito parecidos com suas funções correspondentes no Windows 8. É claro, existem exceções em alguns casos devido a configurações padrão. Pelo fato de o Windows Server 2012 não utilizar índices de desempenho, os servidores do Windows não possuem avaliações do Windows Experience Index (Índice de Experiência do Windows). Pelo fato de o Windows Server 2012 não utilizar o modo Sleep ou modos relacionados, os servidores do Windows não possuem as funcionalidades suspender, hibernar e despertar. Pelo fato de não ser comum querer estender as opções de gerenciamento de energia no Windows Server, o Windows Server 2012 possui um conjunto limitado de opções de energia.

O Windows Server 2012 não inclui os aprimoramentos do Windows Aero, Windows Sidebar, gadgets do Windows ou qualquer outro aprimoramento de interface de usuário, pois o Windows Server 2012 foi projetado para fornecer desempenho ótimo das tarefas relacionadas ao servidor, não para possibilitar a personalização ampla da aparência da área de trabalho. Dito isso, quando estiver trabalhando com a instalação de servidor completo, é possível adicionar o recurso Desktop Experience e habilitar alguns recursos do Windows 8 no servidor.

O recurso Desktop Experience fornece a funcionalidade da área de trabalho do Windows ao servidor. Os recursos adicionados ao Windows incluem o Windows Media Player, temas de desktop, Vídeo para Windows (suporte AVI), Windows Defender, Limpeza de disco, Central de sincronização, Gravador de som, Mapa de caracteres e Ferramenta de captura. Embora esses recursos permitam que um servidor seja utilizado como um computador desktop, eles podem reduzir o desempenho geral do servidor.

Pelo fato de os recursos em comum entre o Windows 8 e o Windows Server 2012 terem tantas semelhanças, não abordarei as modificações de interface em relação às

versões anteriores de sistemas operacionais, nem discutirei como o UAC funciona, entre outras coisas. Uma cobertura abrangente desses recursos pode ser encontrada no *Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012), o qual sugiro que você utilize em conjunto com este livro. Além dessa ampla cobertura de tarefas administrativas, o *Windows 8 Administration Pocket Consultant* aborda como personalizar o sistema operacional e o ambiente do Windows, como configurar dispositivos de hardware e de rede, como gerenciar o acesso dos usuários e as configurações gerais, como configurar computadores móveis, como utilizar gerenciamento remoto e assistência remota, como solucionar problemas do sistema e muito mais. Este livro, por outro lado, é totalmente voltado à administração de serviços de diretório, dados e rede.

Introdução ao Windows Server 2012

O sistema operacional Windows Server 2012 inclui várias edições diferentes. Todas as edições do Windows Server 2012 dão suporte a múltiplos núcleos em um processador. É importante destacar que, embora um edição possa dar suporte a apenas um processador de soquetes independentes (também chamado de *processador físico*), esse processador único pode ter até oito núcleos (também chamados de *processadores lógicos*).

O Windows Server 2012 é um sistema operacional disponível apenas em 64 bits. Neste livro, refiro-me aos sistemas de 64 bits projetados para a arquitetura x64 como sistemas de *64 bits*. Como as diversas edições do servidor suportam os mesmos recursos e ferramentas de administração, você pode usar as técnicas discutidas neste livro independente da edição do Windows Server 2012 que estiver utilizando.

Quando instala o sistema Windows Server 2012, você configura o sistema de acordo com a função pretendida na rede, seguindo estas orientações:

- Os servidores geralmente são designados como parte de um grupo de trabalho ou de um domínio.
- Grupos de trabalho são associações de computadores nas quais cada computador é gerenciado separadamente.
- Domínios são conjuntos de computadores que podem ser gerenciados coletivamente através de controladores de domínio, que são funções do Windows Server 2012 que gerenciam o acesso à rede, ao banco de dados de diretório e a recursos compartilhados.

OBSERVAÇÃO **Neste livro, *Windows Server 2012* e *família Windows Server 2012* referem-se a todas as edições do Windows Server 2012. As diversas edições do servidor suportam os mesmos recursos e ferramentas de administração.**

Diferente do Windows Server 2008, o Windows Server 2012 utiliza uma tela inicial. Start (Iniciar) é uma janela, não um menu. Os programas podem ter seus blocos na tela Start (Tela Inicial). Ao clicar no bloco, o programa será executado. Geralmente, ao pressionar e manter pressionado ou clicar com o botão direito em um programa, um painel de opções será exibido. A barra Charms é um painel com as opções Start, Desktop e PC Settings. Com uma interface tátil, é possível exibir a barra Charms deslizando o toque a partir do canto direito da tela. Com um mouse e um teclado, é possível exibir a barra Charms movendo o ponteiro do mouse sobre o botão oculto no canto inferior direito ou no canto superior direito das telas Start, Desktop ou PC Settings; ou pressionando a tecla Windows+C.

Toque em ou clique em Search para exibir o painel Search. Qualquer texto digitado enquanto a tela Start estiver aberta será inserido na caixa Search no painel Search. A caixa Search pode focar em Apps, Settings ou Files. Quando focada em Apps, é possível utilizar Search para encontrar rapidamente programas instalados. Quando focada em Settings, é possível utilizar Search para encontrar rapidamente configurações e opções no Control Panel. Quando focada em Files, é possível utilizar Search para encontrar arquivos rapidamente.

Uma maneira de abrir um programa rapidamente é pressionar a tecla Windows, digitar o nome do programa e pressionar a tecla Enter. Esse atalho funcionará enquanto a caixa Search estiver focada em Apps (que é o padrão).

Ao pressionar a tecla Windows, você irá alternar entre a tela Start e a área de trabalho (ou, se estiver trabalhando com PC Settings, irá alternar entre Start e PC Settings). Em Start, há um bloco para o Desktop no qual você pode tocar ou clicar para exibir a área de trabalho. Também é possível exibir a área de trabalho pressionando a tecla Windows+D ou, para apenas olhar rapidamente a área de trabalho, pressione e mantenha pressionadas as teclas Windows+Vírgula. Em Start, o acesso ao Control Panel se dá tocando ou clicando no bloco do Control Panel. Na área de trabalho, o acesso ao Control Panel se dá pela barra Charms, tocando ou clicando em Settings, depois em Control Panel. Além dessa forma, já que o File Explorer está fixado à barra de tarefas da área de trabalho, por padrão é possível acessar o Control Panel a partir da área de trabalho seguindo estas etapas:

1. Abra o File Explorer tocando ou clicando no ícone da barra de tarefas.
2. Toque ou clique no botão de opção na extrema direita (seta para baixo) na lista de endereços.
3. Toque ou clique em Control Panel.

As telas Start e Desktop possuem um menu que pode ser exibido pressionando e mantendo pressionado ou clicando com o botão direito do mouse no canto inferior esquerdo da tela Start ou da área de trabalho. As opções do menu incluem Prompt de comando, Prompt de comando (Admin), Device Manager (Gerenciador de Dispositivos), Event Viewer (Visualizador de Eventos), System (Sistema) e Task Manager (Gerenciador de Tarefas). Em Start, o botão oculto no canto esquerdo da tela mostra uma miniatura da área de trabalho; ao tocar ou clicar nessa miniatura, a área de trabalho é aberta. Na área de trabalho, o botão oculto no canto esquerdo da tela mostra uma miniatura de Start; ao tocar ou clicar nessa miniatura, a tela Start é aberta. Ao pressionar e manter pressionada ou ao clicar com o botão direito do mouse na miniatura, um menu de atalho será exibido.

Agora, Shutdown e Restart são opções das configurações de Energia. Isso significa que, para desligar ou reiniciar um servidor, deve-se seguir estas etapas:

1. Exiba as opções de Start deslizando da extremidade direita da tela para a esquerda ou movendo o ponteiro do mouse para o canto superior direito ou inferior direito da tela.
2. Toque ou clique em Settings e depois em Power.
3. Toque ou clique em Shut Down ou Restart conforme o desejado.

Como alternativa, pressione o botão de energia físico do servidor para iniciar um desligamento ordenado que irá realizar o logoff e em seguida o desligamento efetivo. Se estiver utilizando o sistema em computador desktop e o computador tiver um bo-

tão para dormir, o botão dormir será desabilitado por padrão, assim como as opções de fechamento de tampa para computadores portáteis. Além disso, os servidores são configurados para desligar o vídeo após 10 minutos de inatividade.

O Windows 8 e o Windows Server 2012 suportam a especificação Advanced Configuration and Power Interface (ACPI, Interface de Energia e Configuração Avançada) 5.0. O Windows utiliza a ACPI para controlar as transições de estado de energia do sistema e dos dispositivos, alternando o estado dos dispositivos entre ativo com energia plena, com pouca energia e desligado, para reduzir o consumo de energia.

As configurações de energia para um computador dependem do plano de energia ativo. É possível acessar os planos de energia no Control Panel tocando ou clicando em System And Security (Sistema e Segurança) e depois em Power Options. O Windows Server 2012 inclui o utilitário Power Configuration (Powercfg.exe) para o gerenciamento das opções de energia via linha de comando. Em um prompt de comando, é possível visualizar os planos de energia selecionados digitando **powercfg /l**. O plano de energia ativo estará marcado com um asterisco.

O plano de energia ativo padrão do Windows Server 2012 é chamado de Balanced (Equilibrado). O plano Balanced é configurado para fazer o seguinte:

- Nunca desligar os discos rígidos (em oposição a desligar os discos rígidos após um período de tempo ocioso especificado)
- Desabilitar eventos cronometrados para acordar o computador (em oposição a habilitar eventos cronometrados para acordar o computador)
- Habilitar suspensão seletiva USB (em oposição a desabilitar suspensão seletiva)
- Utilizar economia de energia média para links PCI Express ociosos (em oposição à economia de energia máxima estar ligada ou desligada)
- Utilizar resfriamento ativo do sistema, no qual aumenta-se a velocidade do ventilador antes de reduzir a velocidade dos processadores (em oposição a utilizar resfriamento passivo do sistema, no qual reduz-se a velocidade dos processadores antes de aumentar a velocidade do ventilador)
- Utilizar estados mínimo e máximo de processadores se essa opção for possível (em oposição a utilizar um estado fixo)

OBSERVAÇÃO **O consumo de energia é uma questão importante, especialmente à medida que organizações tentam tornar-se mais sustentáveis. Economizar energia também pode resultar numa economia de dinheiro para a empresa e, em alguns casos, pode permitir a instalação de mais servidores em seu centro de dados. Se, por exemplo, você instalar o Windows Server 2012 em um laptop (para teste ou para uso pessoal), suas configurações de energia serão um pouco diferentes e também haverá configurações para quando o laptop estiver se alimentando apenas da bateria.**

Opções de gerenciamento de energia

Quando se está trabalhando com gerenciamento de energia, aspectos importantes incluem os seguintes:

- Modos de resfriamento
- Estados dos dispositivos
- Estados dos processadores

A ACPI define modos de resfriamento ativo e passivo. Esses modos de resfriamento são inversamente relacionados entre si:

- O resfriamento passivo reduz o desempenho do sistema, mas é mais silencioso porque há menos ruído do ventilador. Com o resfriamento passivo, o Windows diminui o consumo de energia para reduzir a temperatura de funcionamento do computador à custa do desempenho do sistema. Nesse modo, o Windows reduz a velocidade do processador a fim de resfriar o computador antes de aumentar a velocidade do ventilador, o que aumentaria o consumo de energia.
- O resfriamento ativo permite o desempenho máximo do sistema. Com o resfriamento ativo, o Windows aumenta o consumo de energia para reduzir a temperatura da máquina. Nesse modo, o Windows aumenta a velocidade do ventilador para resfriar o computador antes de tentar reduzir a velocidade do processador.

As políticas de energia incluem um limite máximo e mínimo para o estado do processador, chamados de *estado máximo do processador* e *estado mínimo do processador*, respectivamente. Esses estados são implementados através do uso de um recurso da ACPI 3.0 ou versões mais recentes, chamado de limitação do processador, que determina os estados de desempenho do processador atualmente disponíveis para serem utilizados pelo Windows. Ao configurar os valores máximo e mínimo, você define os limites para os estados de desempenho permitidos; também é possível utilizar o mesmo valor mínimo e máximo para forçar o sistema a permanecer em um estado de desempenho específico. O Windows reduz o consumo de energia limitando a velocidade do processador. Por exemplo, se o limite superior for 100% e o limite inferior for 5%, o Windows pode diminuir a potência do processador dentro desse intervalo conforme a carga de trabalho para reduzir o consumo de energia. Em um computador com um processador de 3GHz, o Windows ajustaria a frequência de funcionamento do processador entre 0,15GHz e 3,0GHz.

O recurso de limitação do processador e outros estados de desempenho relacionados foram introduzidos no Windows XP e não são novidade, mas essas implementações iniciais foram projetadas para computadores com processadores com soquetes independentes e não para computadores com processadores com núcleos. Como resultado, não são eficientes na redução do consumo de energia em computadores com processadores lógicos. O Windows 7 e versões posteriores de Windows reduzem o consumo de energia em computadores com processadores com núcleos múltiplos utilizando um recurso da ACPI 4.0 chamado de *suspensão de processador lógico* e atualizando os recursos de limitação do processador para trabalhar com núcleos do processador.

O recurso *suspensão de processador lógico* foi projetado para garantir que o Windows utilize o menor número possível de núcleos do processador em uma determinada carga de trabalho. O Windows alcança isso ao consolidar a carga de trabalho no menor número de núcleos possível e, ao mesmo tempo, suspendendo o uso dos núcleos inativos do processador. Conforme mais poder de processamento for necessário, o Windows ativa os núcleos inativos do processador. A funcionalidade para deixar o processador ocioso funciona juntamente com o gerenciamento dos estados de desempenho ao nível de núcleo.

A ACPI define os estados de desempenho do processador, também chamados de *p-states*, e estados de suspensão por ociosidade, também chamados de *c-states*. Estados de desempenho do processador incluem P0 (o processador/núcleo usa sua

capacidade máxima de desempenho e pode consumir o máximo de energia), P1 (o processador/núcleo é limitado abaixo do seu nível máximo e consome menos do que o máximo de energia) e P*n* (em que o estado *n* é um número máximo dependente do processador, e em que o processador/núcleo está em seu nível mínimo e consome o mínimo de energia ao mesmo tempo que permanece em estado ativo).

Estados de suspensão por ociosidade incluem C0 (o processador/núcleo consegue executar instruções), C1 (o processador/núcleo tem a menor latência e permanece em um estado de energia sem realizar execuções), C2 (o processador/núcleo tem mais latência para aumentar a economia de energia em comparação ao estado C1) e C3 (o processador/núcleo tem a maior latência para aumentar a economia de energia em comparação aos estados C1 e C2).

MAIS INFORMAÇÕES **A ACPI 4.0 foi finalizada em junho de 2009 e a ACPI 5.0 em dezembro de 2011. Computadores fabricados antes dessa época provavelmente não terão um firmware totalmente compatível, e você provavelmente terá que atualizar o firmware quando uma versão revisada compatível for disponibilizada. Em alguns casos, e especialmente com hardwares mais antigos, talvez não seja possível atualizar o firmware de um computador para torná-lo totalmente compatível com a ACPI 4.0 ou ACPI 5.0. Por exemplo, se estiver configurando as opções de energia e não houver as opções de estado mínimo e máximo do processador, o firmware do computador não é totalmente compatível com a ACPI 3.0 e provavelmente também não suportará por completo a ACPI 4.0 ou a ACPI 5.0. Ainda assim, verifique se há atualizações no site do fabricante do hardware.**

Quanto aos processadores/núcleos, o Windows alterna entre qualquer p-state e a partir do estado C1 para o estado C0 quase instantaneamente (frações de milissegundos) e tende a não utilizar os estados de suspensão profundos, por isso não há necessidade de preocupar-se quanto ao impacto no desempenho ao diminuir a potência ou ativar processadores/núcleos. Os processadores/núcleos são disponibilizados quando tornam-se necessários. Dito isso, a forma mais fácil de limitar o gerenciamento de energia do processador é modificando o plano de energia ativo e definindo como 100% tanto o estado mínimo quanto o estado máximo do processador.

O recurso *suspensão de processador lógico* é utilizado para reduzir o consumo de energia por meio da remoção de um processador lógico da lista de processos sem afinidade com o processador do sistema operacional. No entanto, como processos com afinidade com o processador reduzem a eficácia desse recurso, é desejável um planejamento cuidadoso antes de estabelecer as configurações de afinidade com processador para aplicativos. O Windows System Resource Manager (Gerenciador de Recursos de Sistema do Windows) possibilita o gerenciamento dos recursos do processador através de metas de porcentagem de uso do processador e através de regras de afinidade com o processador. Ambas as técnicas reduzem a eficácia da suspensão de processadores lógicos.

O Windows economiza energia ao colocar ou retirar núcleos do processador dos p-states e c-states apropriados. Em um computador com quatro processadores lógicos, o Windows pode utilizar p-states de 0 a 5, em que P0 permite 100% de uso, P1 permite 90% de uso, P2 permite 80% de uso, P3 permite 70% de uso, P4 permite 60% de uso e P5 permite 50% de uso. Quando um computador está ativo, o processador lógico 0 provavelmente está ativo com um p-state entre 0 e 5 e os outros processadores provavelmente estão em um p-state adequado ou em um estado de suspensão. A Figura 1-1 mostra um exemplo. Aqui, o processador lógico 1 está rodando a 90%, o processador lógico 2 está rodando a 80%, o processador lógico 3 está rodando a 50% e o processador lógico 4 está em estado de suspensão.

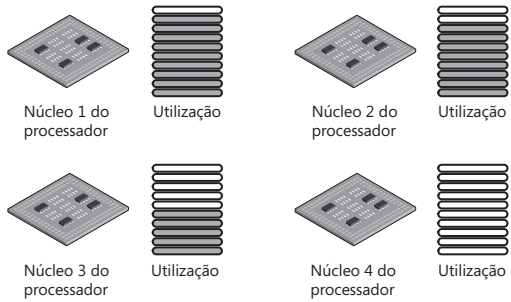

FIGURA 1-1 Para entender os estados de processador.

MUNDO REAL **A ACPI 4.0 e a ACPI 5.0 definem quatro estados de energia globais. No G0, estado de funcionamento no qual o software é executado, o consumo de energia é o mais alto e a latência é a mais baixa. No G1, estado de suspensão, no qual o software não é executado, a latência varia com o estado de suspensão, e o consumo de energia é menor do que no estado G0. No G2 (também chamado de estado de suspensão S5), estado ocioso no qual o sistema operacional não é executado, a latência é longa e o consumo de energia é bem próximo de zero. No G3, estado ocioso mecânico, no qual o sistema operacional não é executado, a latência é longa e o consumo de energia é zero. Também há um estado global especial, conhecido como estado de suspensão não volátil S4, no qual o sistema operacional escreve todo o contexto do sistema em um arquivo de armazenamento não volátil, permitindo que o contexto do sistema seja salvo e restaurado.**

Dentro do estado de suspensão global, o G1, há variações. O S1 é um estado de suspensão em que todo o contexto do sistema é mantido. O S2 é um estado de suspensão parecido com o S1, exceto que os contextos da CPU e do cache do sistema se perdem e o controle se dá após reiniciar o computador. O S3 é um estado de suspensão no qual todos os contextos da CPU, do cache e do chipset se perdem e o hardware mantém o contexto da memória e restaura alguns contextos das configurações da CPU e do cache L2. O S4 é um estado de suspensão no qual assume-se que o hardware tenha desligado todos os dispositivos a fim de reduzir ao máximo o consumo e que apenas o contexto da plataforma continua sendo mantido. O S5 é um estado de suspensão no qual assume-se que o hardware está em um estado ocioso, no qual nenhum contexto é mantido e uma inicialização completa é necessária quando o sistema é despertado.

Dispositivos também têm estados de energia. D0, o estado totalmente ligado, consome o maior nível de energia. O D1 e o D2 são estados intermediários que muitos dispositivos não utilizam. O D3hot é um estado de economia de energia, no qual o dispositivo é enumerado por software e pode, por opção, preservar o contexto do dispositivo. D3 é o estado desligado, no qual o contexto do dispositivo é perdido e o sistema operacional deve reinicializar o dispositivo para ligá-lo novamente.

Ferramentas e protocolos de rede

O Windows Server 2012 possui um pacote de ferramentas de rede que inclui o Network Explorer (Explorador de Rede), a Network And Sharing Center (Central de Rede e Compartilhamento) e o Network Diagnostics (Diagnóstico de Rede). A Figura 1-2 mostra a Network And Sharing Center.

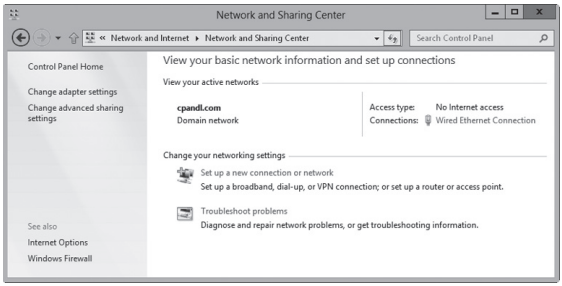

FIGURA 1-2 Network And Sharing Center fornece acesso rápido a opções de compartilhamento, descoberta e rede.

Para entender as opções de rede

As configurações de compartilhamento e descoberta na Network And Sharing Center controlam as configurações básicas de rede. Quando as configurações de descoberta estão ativadas e um servidor está conectado a uma rede, o servidor consegue ver os outros computadores e dispositivos da rede que estejam visíveis na rede. Quando as configurações de compartilhamento são ativadas ou desativadas, as várias opções de compartilhamento tornam-se permitidas ou restritas. Como será discutido no Capítulo 12, "Compartilhamento de dados, segurança e auditoria", as opções de compartilhamento incluem compartilhamento de arquivos, compartilhamento de pasta pública, compartilhamento de impressora e compartilhamento protegido por senha.

No Windows 8 e no Windows Server 2012, as redes são identificadas como um dos seguintes tipos:

- **Domain (Domínio)** Uma rede na qual os computadores são conectados ao domínio corporativo do qual fazem parte.
- **Work (Trabalho)** Uma rede privada na qual os computadores são configurados como membros de um grupo de trabalho e não são conectados diretamente à Internet pública.
- **Home (Doméstica)** Uma rede privada na qual os computadores são configurados como membros de um grupo de doméstico e não são conectados diretamente à Internet pública.
- **Public (Pública)** Uma rede pública na qual os computadores são conectados à uma rede em um local público, como restaurantes ou aeroportos, e não à uma rede interna.

Esses tipos de rede estão organizados em três categorias: doméstica ou de trabalho, domínio e pública. Cada categoria de rede tem configurações de rede específicas. Como o computador salva configurações de compartilhamento e firewall separadamente para cada categoria de rede, é possível utilizar diferentes configurações de bloqueio e permissão para cada categoria de rede. Quando você se conecta a uma rede, vê uma caixa de diálogo que permite a especificação da categoria da rede. Se você selecionar Private e o computador determinar que está conectado ao domínio corporativo do qual faz parte, a categoria de rede é definida como rede de domínio.

Baseado na categoria de rede, o Windows Server define as configurações que ligam e desligam a opção da descoberta. O estado ligado (On, habilitado) significa que o computador pode descobrir outros computadores e dispositivos na rede e que outros computadores na rede podem descobrir o computador. O estado desligado (Off, desabilitado) significa que o computador não pode descobrir outros computadores e dispositivos na rede e que outros computadores na rede também não podem descobrir o computador.

É possível habilitar a opção da descoberta e o compartilhamento de arquivos utilizando tanto a janela Network quanto Advanced Sharing Settings na Network And Sharing Center. No entanto, a opção da descoberta e o compartilhamento de arquivos estão bloqueados por padrão na rede pública, o que aumenta a segurança ao impedir que computadores da rede pública descubram outros computadores e dispositivos naquela rede. Quando a opção da descoberta e o compartilhamento de arquivos estão desabilitados, os arquivos e impressoras que você compartilhou no computador não podem ser acessados a partir da rede. Além disso, alguns programas talvez não consigam acessar a rede.

Como trabalhar com protocolos de rede

Para permitir que um servidor acesse uma rede, você deve instalar uma rede TCP/IP e um adaptador de rede. O Windows Server utiliza TCP/IP como o protocolo padrão de rede de longa distância (WAN). Normalmente, a rede é instalada durante a instalação do sistema operacional. Você também pode instalar a rede TCP/IP a partir das propriedades da conexão de rede local.

Os protocolos TCP e IP possibilitam que os computadores comuniquem-se através de várias redes e através da Internet utilizando adaptadores de rede. O Windows 7 e as versões mais recentes do Windows possuem uma arquitetura com uma camada dupla de IP, no qual tanto o protocolo IP versão 4 (IPv4) quanto o protocolo IP versão 6 (IPv6) estão implementados e compartilham camadas de rede e transporte em comum. O IPv4 possui endereços de 32 bits e é a primeira versão de IP utilizada na maioria das redes, incluindo a Internet. O IPv6, por outro lado, possui endereços de 128 bits e é a versão mais atual de IP.

OBSERVAÇÃO **Clientes do DirectAccess só enviam tráfego IPv6 através da conexão do DirectAccess para o servidor do DirectAccess. Graças ao apoio do NAT64 e do DNS64 em um servidor do DirectAccess no Windows Server 2012, clientes do DirectAccess agora podem iniciar comunicações com hosts que possuem só IPv4 na intranet corporativa. O NAT64 e o DNS64 operam em conjunto para converter o tráfego de conexão de entrada de um nó de IPv6 em um tráfego de IPv4. O NAT64 converte o tráfego de IPv6 de entrada em um tráfego de IPv4 e realiza uma conversão inversa para o tráfego de resposta. O DNS64 resolve o nome de um host somente IPv4 como um endereço IPv6 convertido.**

MUNDO REAL **O recurso TCP Chimney Offload foi introduzido com o Windows Vista e o Windows Server 2008. Esse recurso permite que o subsistema de rede descarregue o funcionamento de uma conexão TCP/IP do processador do computador para seu adaptador de rede, contanto que o adaptador de rede suporte o funcionamento de descarregamento TCP/IP. Tanto conexões TCP/IPv4 quanto conexões TCP/IPv6 podem ser descarregadas. Para o Windows 7 e versões mais recentes do Windows, conexões TCP são descarregadas, por padrão, em adaptadores de rede de 10 gigabits por segundo (Gbps), mas não são descarregadas, por padrão, em adaptadores de rede de 1 Gbps. Para descarregar conexões TCP em um adaptador de rede de 1 ou 10 Gbps, é preciso habilitar o descarregamento de TCP inserindo o comando seguinte em**

um prompt de comandos com privilégios elevados: netsh int tcp set global chimney=enabled. É possível verificar o status do descarregamento de TCP digitando netsh int tcp show global. Embora o descarregamento de TCP opere com o Firewall do Windows, o descarregamento de TCP não será usado com o IPsec, o Hyper V (solução de virtualização da Microsoft), nem com o balanceamento da carga de rede ou com o serviço NAT (conversão de endereços de rede). Para verificar se o descarregamento de TCP está funcionando, digite netstat-t e confira o estado de descarregamento. O estado de descarregamento é listado como *offloaded* ou *inhost*.

O Windows também utiliza o receive-side scaling (RSS) e o NetDMA (acesso direto à memória de rede). É possível habilitar ou desabilitar o RSS digitando netsh int tcp set global rss=enabled ou netsh int tcp set global rss=disabled, respectivamente. Para verificar o status do RSS, digite netsh int tcp show global. É possível habilitar ou desabilitar o NetDMA definindo um valor DWord de 1 ou 0, respectivamente, abaixo da entrada de registro EnableTCPA. Essa entrada de registro encontra-se em HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

Endereços IPv4 de 32 bits costumam ser expressos por quatro valores decimais separados, como 127.0.0.1 ou 192.168.10.52. Os quatro valores decimais são chamados de *octetos* porque cada um deles representa 8 bits do total de 32 bits. Com endereços IPv4 unicast padrão, uma parte variável do endereço IP representa o ID da rede e uma parte variável do endereço IP representa o ID do host. O endereço IPv4 de um host e o endereço MAC da máquina utilizado pelo adaptador de rede do host não têm correlação.

Endereços IPv6 de 128 bits são divididos em seis blocos de 16 bits delimitados por dois-pontos. Cada bloco de 16 bits é expresso de forma hexadecimal, como FEC0:0:0:02BC:FF:BECB:FE4F:961D. Com endereços IPv6 unicast padrão, os primeiros 64 bits representam o ID de rede e os últimos 64 bits representam a interface de rede. Como muitos blocos de endereço IPv6 são definidos por 0, um conjunto contíguo de blocos de 0 pode ser expresso por "::", uma notação chamada de *notação de dois-pontos*. Se utilizarmos a notação de dois-pontos, os dois blocos 0 no endereço anterior podem ser compactados como FEC0::02BC:FF:BECB:FE4F:961D. Três ou mais blocos de 0 seriam compactados da mesma forma. Por exemplo, FFE8:0:0:0:0:0:0:1 torna-se FFE8::1.

Quando o hardware da rede é detectado durante a instalação do sistema operacional, o IPv4 e o IPv6 são habilitados por padrão; não é necessário instalar um componente em separado para habilitar o suporte ao IPv6. A arquitetura modificada de IP no Windows 7 e em versões mais recentes do Windows é chamada de *Next Generation TCP/IP stack*, e inclui muitos aprimoramentos que aperfeiçoam a forma como o IPv4 e o IPv6 são utilizados.

Controladores de domínio, servidores membros e serviços de domínio

Quando você instala o Windows Server 2012 em um novo sistema, pode configurar o servidor como servidor membro, controlador de domínio ou servidor autônomo. As diferenças entre esses tipos de servidores é de extrema importância. Servidores membros fazem parte de um domínio, mas não armazenam informações de diretório. Controladores de domínio diferenciam-se dos servidores membros porque armazenam informações de diretório e fornecem serviços de autenticação e de diretório ao domínio. Servidores autônomos não fazem parte de um domínio. Como os servidores autônomos possuem seu próprio banco de dados de usuário, autenticam solicitações de logon de forma independente.

Como trabalhar com o Active Directory

O Windows Server 2012 dá suporte a um modelo de replicação multimestre. Nesse modelo, qualquer controlador de domínio pode receber alterações de diretório e replicar essas alterações para outros controladores de domínio automaticamente. O Windows Server distribui um diretório de informações inteiro, chamado de um *repositório de dados*. Dentro de um repositório de dados há conjuntos de objetos que representam contas de computador, usuários e grupos, além de recursos compartilhados como servidores, arquivos e impressoras.

Domínios que utilizam Active Directory são chamados de *domínios do Active Directory*. Embora domínios do Active Directory funcionem com apenas um controlador de domínio, você pode e deve configurar múltiplos controladores de domínio no domínio. Dessa forma, se um controlador de domínio falhar, você pode contar que os outros controladores de domínio lidem com autenticação e outras tarefas críticas.

A Microsoft fez várias alterações no Active Directory na versão original do Windows Server 2008. Como resultado, a Microsoft realinhou a funcionalidade de diretório e criou uma família de serviços relacionados, incluindo os seguintes:

- **Active Directory Certificate Services (AD CS, Serviços de Certificados do Active Directory)** O AD CS fornece as funções necessárias para emitir e revogar certificados digitais para usuários, computadores clientes e servidores. O AD CS utiliza CAs (*certificate authorities*, autoridades de certificação), que são responsáveis por confirmar a identidade dos usuários e computadores e por emitir e validar certificados que confirmem essas identidades. Domínios podem ter CAs raiz corporativas, que são servidores de certificação da raiz da hierarquia de certificação para esses domínios e são os servidores de certificação mais confiáveis da empresa, e CAs subordinadas, que são membros de uma hierarquia de certificação corporativa específica. Grupos de trabalho somente podem possuir CAs raiz autônomas, que são servidores de certificação da raiz da hierarquia de certificação não corporativa, e CAs subordinadas autônomas, que são membros de uma hierarquia de certificação não corporativa específica.
- **Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory)** O AD DS fornece os serviços de diretório necessários para estabelecer um domínio, incluindo o repositório de dados que armazena informações sobre objetos na rede e as disponibiliza para os usuários. O AD DS utiliza controladores de domínio para gerenciar o acesso aos recursos de rede. Uma vez que os usuários fazem sua autenticação ao efetuar logon em um domínio, suas credenciais armazenadas podem ser utilizadas para acessar recursos da rede. Como o AD DS é a parte mais importante do Active Directory e é um requisito para aplicativos e tecnologias compatíveis com diretório, eu o chamo simplesmente de Active Directory em vez de Active Directory Domain Services ou AD DS.
- **Active Directory Federation Services (AD FS, Serviços de Federação do Active Directory)** O AD FS complementa os recursos de autenticação e gerenciamento de acesso do AD DS, estendendo-os para a World Wide Web. O AD FS utiliza agentes da Web para fornecer aos usuários acesso a aplicativos da web hospedados internamente e proxies para gerenciar o acesso para cliente. Uma vez que o AD FS estiver configurado, os usuários podem utilizar suas identidades digitais para autenticar-se na Web e acessar aplicativos da web hospedados internamente com um navegador da Web como o Internet Explorer.

- **Active Directory Lightweight Directory Services (AD LDS)** O AD LDS fornece um repositório de dados para aplicativos compatíveis com diretórios que não requeiram AD DS e que não necessitam ser implantados em controladores de domínio. O AD LDS não funciona como um serviço do sistema operacional e pode ser utilizado tanto nos ambientes de domínios como nos de grupos de trabalho. Cada aplicativo que é executado em um servidor pode ter seu próprio repositório de dados implementado através do AD LDS.
- **Active Directory Rights Management Services (AD RMS)** O AD RMS fornece uma camada de proteção para as informações de uma empresa que podem ser estendidas além do ambiente da empresa, fazendo com que mensagens de email, documentos, páginas da Web e outros sejam protegidos de acessos não autorizados. O AD RMS utiliza um serviço de certificação para emitir certificados de direitos de conta que identificam os usuários, grupos e serviços confiáveis; um serviço de licenciamento que fornece acesso a informações protegidas a usuários, grupos e serviços autorizados; e um serviço de registro em log para monitorar e manter o serviço de gerenciamento de direitos. Uma vez que a confiança tenha sido estabelecida, os usuários com certificados de direitos da conta podem atribuir direitos a informações. Esses direitos controlam quais usuários podem acessar a informação e o que podem fazer com ela. Usuários com certificados de direitos da conta também podem acessar conteúdo protegido se o acesso tiver sido concedido a eles. A criptografia garante que o acesso a informações protegidas seja controlado tanto dentro como fora das empresas.

A Microsoft introduziu alterações adicionais com o Windows Server 2012. Essas alterações incluem um novo nível funcional de domínio, chamado de *nível funcional de domínio do Windows Server 2012*, e um novo nível funcional de floresta, chamado de *nível funcional de floresta do Windows Server 2012*. As diversas outras alterações são discutidas no Capítulo 6, "Como utilizar o Active Directory".

Como utilizar controladores de domínio somente leitura

O Windows Server 2008 e as versões mais recentes dão suporte a controladores de domínio somente leitura (RODC, Read-Only Domain Controllers) e a Restartable Active Directory Domain Services. Um RODC é um controlador de domínio adicional que hospeda uma réplica somente leitura do repositório de dados de um domínio do Active Directory. Os RODCs são ideais para as necessidades de filiais, onde a segurança física de um controlador de domínio não é garantida. Com exceção de senhas, os RODCs armazenam os mesmos objetos e atributos que os controladores de domínio graváveis armazenam. Esses objetos e atributos são replicados para RODCs através de replicação unidirecional a partir de um controlador de domínio gravável que age como um parceiro de replicação.

Como por padrão os RODCs não armazenam senhas nem credenciais além das utilizadas por sua própria conta de computador e na conta Krbtgt (Kerberos Target), os RODCs extraem as credenciais de usuário e de computador de um controlador de domínio gravável com o Windows Server 2008 ou versão mais recente. Se permitir através de uma política de replicação de senha aplicada a um controlador de domínio gravável, um RODC extrairá e armazenará em cache as credenciais conforme necessário até que essas credenciais mudem. Como apenas um subconjunto de credenciais fica armazenado em um RODC, isso limita o número de credenciais que podem ser comprometidas.

DICA **Qualquer usuário de domínio pode ser definido como um administrador local de um RODC sem precisar conceder nenhum outro direito no domínio. Um RODC pode agir como um catálogo global mas não como um mestre de operações. Embora os RODCs possam extrair informações de controladores de domínio com o Windows Server 2003, podem extrair atualizações da partição do domínio somente de um controlador de domínio gravável com Windows Server 2008 ou versão mais recente no mesmo domínio.**

Como utilizar o Restartable Active Directory Domain Services

O Restartable Active Directory Domain Services (Serviços de Domínio do Active Directory Reinicializáveis) é um recurso que permite a um administrador iniciar e parar o AD DS. No console Services, o serviço Active Directory Domain Services está disponível em controladores de domínio, permitindo que você pare e reinicie o AD DS com facilidade da mesma forma que faz com qualquer outro serviço que estiver sendo executado localmente no servidor. Enquanto o AD DS estiver pausado, é possível realizar tarefas de manutenção que, caso contrário, iriam requerer reiniciar o servidor, como desempenhar a desfragmentação offline do banco de dados do Active Directory, aplicar atualizações ao sistema operacional ou iniciar uma restauração autoritativa. Enquanto o AD DS estiver pausado em um servidor, outros controladores de domínio podem controlar as tarefas de autenticação e logon. Métodos de logon biométrico, credenciais armazenadas em cache e cartões inteligentes continuam tendo suporte. Se nenhum outro controlador de domínio estiver disponível e nenhum desses métodos de logon for aplicável, você ainda pode fazer o logon no servidor utilizando a conta e a senha do Directory Services Restore Mode.

Todos os controladores de domínio com Windows Server 2008 ou versões mais recentes suportam o Restartable Active Directory Domain Services, até mesmo RODCs. Se for administrador, você pode iniciar ou parar o AD DS usando a entrada Domain Controller no utilitário Services. Devido ao Restartable Active Directory Domain Services, controladores de domínio com Windows Server 2008 ou versões mais recentes têm três estados possíveis:

- **Active Directory Started** O Active Directory está iniciado e o controlador de domínio tem o mesmo estado de execução que um controlador de domínio com o Windows 2000 Server ou Windows Server 2003. Isso permite que o controlador de domínio forneça serviços de autenticação e logon para um domínio.
- **Active Directory Stopped** O Active Directory está pausado e o controlador de domínio não pode mais fornecer serviços de autenticação e logon para um domínio. Esse modo compartilha algumas características tanto de um servidor membro como de um controlador de domínio no Directory Services Restore Mode. Como ocorre com um servidor membro, o servidor conecta-se ao domínio. Os usuários podem efetuar logon interativamente utilizando métodos de logon biométrico, credenciais em cache e cartões inteligentes. Os usuários também podem efetuar logon na rede utilizando outro controlador de domínio para logon de domínio. Como ocorre no Directory Services Restore Mode, o banco de dados do Active Directory (Ntds.dit) no controlador de domínio local está offline. Isso significa que é possível realizar operações que necessitam que o AD DS esteja offline, como a desfragmentação do banco de dados e aplicação de atualizações de segurança, sem necessidade de reiniciar o controlador de domínio.
- **Directory Services Restore Mode** O Active Directory encontra-se em modo de restauração. O controlador de domínio possui o mesmo estado de restauração que um controlador de domínio com o Windows Server 2003. Esse modo permite

realizar uma restauração autoritativa ou não autoritativa do banco de dados do Active Directory.

Quando estiver trabalhando com o AD DS no estado Stopped, você deve lembrar que serviços dependentes também estão pausados quando o AD DS estiver pausado. Isso significa que o File Replication Service (FRS, Serviço de Replicação de Arquivos), o Kerberos Key Distribution Center (KDC, Centro de Distribuição de Chaves) e o Intersite Messaging (Mensagens entre Sites) são pausados antes do Active Directory ser pausado, e que mesmo quando estão sendo executados, esses serviços dependentes são reiniciados quando o Active Directory é reiniciado. Além disso, é possível reiniciar um controlador de domínio no Directory Services Restore Mode, mas não é possível iniciar um controlador de domínio com o Active Directory no estado Stopped. Para chegar ao estado Stopped, primeiramente é preciso iniciar o controlador de domínio normalmente para então parar o AD DS.

Serviços de resolução de nomes

Os sistemas operacionais Windows utilizam resolução de nomes para facilitar a comunicação com outros computadores em uma rede. A resolução de nomes associa os nomes dos computadores com os endereços IP numéricos utilizados para comunicações na rede. Assim, em vez de utilizar cadeias longas de dígitos, os usuários podem acessar um computador da rede utilizando um nome fácil.

Os atuais sistemas operacionais Windows suportam três sistemas de resolução de nomes:

- Domain Name System (DNS, Sistema de Nomes de Domínio)
- Windows Internet Name Service (WINS, Serviço de Cadastramento na Internet do Windows)
- Link-Local Multicast Name Resolution (LLMNR)

As seções que seguem analisam esses serviços.

Como utilizar o DNS

O DNS é o serviço de resolução de nomes que resolve nomes de computadores para endereços IP. Ao utilizar o DNS, o nome de host totalmente qualificado computer84.cpandl.com, por exemplo, pode ser resolvido para um endereço IP, permitindo que ele e os outros computadores se encontrem. O DNS opera na pilha de protocolo TCP/IP e pode ser integrado com o WINS, com o Dynamic Host Configuration Protocol (protocolo DHCP) e o AD DS. Como será discutido no Capítulo 15, "Como executar clientes e servidores DHCP", o protocolo DHCP é utilizado para endereçamento de IP dinâmico e configuração TCP/IP.

O DNS organiza grupos de computadores em domínios. Esses domínios são organizados em estrutura hierárquica, que pode ser definida na Internet para redes públicas ou na empresa para redes privadas (também chamadas de *intranets* e *extranets*). Os vários níveis da hierarquia identificam computadores individuais, domínios organizacionais e domínios de primeiro nível (top-level). Para o nome do host totalmente qualificado computer84.cpandl.com, *computer84* representa o nome do host para um computador individual, *cpandl* é o domínio organizacional e *com* é o domínio de primeiro nível.

Domínios de primeiro nível são a raiz da hierarquia DNS; eles também são chamados de *domínios-raiz*. Esses domínios são organizados geograficamente, por tipo de organização e por função. Domínios normais, como cpandl.com, também são chamados de *domínios-pai*. São chamados de domínios-pai porque são os pais de uma estrutura organizacional. Domínios-pai podem ser divididos em subdomínios que podem ser utilizados por grupos ou departamentos dentro de uma empresa.

Subdomínios são geralmente chamados de *domínios-filho*. Por exemplo, o nome de domínio totalmente qualificado (FQDN, fully qualified domain name) para um computador de um grupo de recursos humanos poderia ser jacob.hr.cpandl.com. Aqui, *jacob* é o nome do host, *hr* é o domínio-filho e *cpandl.com* é o domínio-pai.

Domínios do Active Directory utilizam o DNS para implementar sua estrutura de nomeação e hierarquia. O Active Directory e o DNS são quase totalmente integrados, tanto que é preciso instalar o DNS na rede antes de instalar os controladores de domínio utilizando o Active Directory. Durante a instalação do primeiro controlador de domínio em uma rede do Active Directory, você tem a oportunidade de instalar o DNS automaticamente se um servidor DNS não for encontrado na rede. Também pode especificar se deseja que o DNS e o Active Directory sejam totalmente integrados. Na maioria dos casos, é aconselhável responder afirmativamente a ambas as perguntas. Com a integração total, as informações do DNS são armazenadas diretamente no Active Directory. Isso permite que você aproveite as capacidades do Active Directory. A diferença entre integração parcial e total é muito importante:

- **Integração parcial** Com a integração parcial, o domínio utiliza o armazenamento de arquivo padrão. As informações do DNS são armazenadas em arquivos de texto com a extensão .dns, e a localização padrão desses arquivos é %SystemRoot%\System32\Dns. As atualizações para o DNS são controladas por um único servidor DNS autoritativo. Esse servidor é designado como o servidor DNS primário para um domínio específico ou área específicos dentro de um domínio chamado de *zona*. Clientes que utilizam atualizações dinâmicas do DNS através do DHCP devem estar configurados para utilizar o servidor DNS primário da zona. Se não estiverem, suas informações de DNS não serão atualizadas. Da mesma forma, atualizações dinâmicas através do DHCP não podem ocorrer se o servidor DNS primário estiver offline.
- **Integração total** Com a integração total, o domínio utiliza o armazenamento integrado com o diretório. As informações de DNS são armazenadas diretamente no Active Directory e ficam disponíveis através do contêiner para o objeto *dnsZone*. Como as informações fazem parte do Active Directory, qualquer controlador de domínio pode acessar os dados e uma abordagem multimestre pode ser utilizada para atualizações dinâmicas através do DHCP. Isso permite que qualquer controlador de domínio com o serviço DNS Server manipule as atualizações dinâmicas. Além disso, clientes que utilizam atualizações dinâmicas de DNS através do DHCP podem utilizar qualquer servidor DNS que faça parte da zona. Um benefício adicional da integração com o diretório é a habilidade de utilizar a segurança de diretório para controlar o acesso às informações de DNS.

Se observar a forma como as informações de DNS são replicadas pela rede, você verá mais vantagens na integração total com o Active Directory. Com a integração parcial, as informações de DNS são armazenadas e replicadas separadamente do Active Directory. Ter duas estruturas separadas reduz a eficácia tanto do DNS quanto do Active Directory e torna a administração mais complexa. Como o DNS é menos eficiente que

o Active Directory em replicar alterações, esse tipo de abordagem aumenta o tráfego da rede e a quantidade de tempo que leva para replicar as alterações de DNS pela rede.

Para habilitar o DNS na rede, é preciso configurar os clientes e servidores DNS. Quando você configura os clientes DNS, informa aos clientes os endereços IP dos servidores DNS da rede. Utilizando esses endereços, os clientes podem comunicar-se com os servidores DNS de qualquer parte da rede, mesmo que os servidores estejam em sub-redes diferentes.

Quando a rede utiliza o DHCP, é necessário configurar o DHCP para que trabalhe junto com o DNS. Para fazer isso, configure as opções de escopo DHCP 006 DNS Servers e 015 Domain Name como especificado em "Configuração das opções de escopo" no Capítulo 15. Além disso, se os computadores da rede precisarem ficar acessíveis a partir de outros domínios do Active Directory, é preciso criar registros para eles no DNS. Os registros no DNS são organizados em zonas; uma zona é, simplesmente, uma área de um domínio. Para configurar um servidor DNS, leia a explicação em "Configuração de um servidor DNS primário" no Capítulo 16, "Otimização do DNS".

Quando você instala o Servidor DNS em um RODC, o RODC consegue extrair uma réplica somente leitura de todas as partições de diretório de aplicativo utilizadas pelo DNS, incluindo *ForestDNSZones* e *DomainDNSZones*. Então, os clientes podem consultar a resolução de nomes no RODC como consultariam em qualquer outro servidor DNS. No entanto, como no caso de atualizações do diretório, o servidor DNS em um RODC não suporta atualizações diretas. Isso significa que o RODC não registra um registro de recurso de servidor de nomes (NS, name server) em nenhuma zona integrada ao Active Directory que hospeda. Quando um cliente tenta atualizar seus registros de DNS contra um RODC, o servidor retorna uma referência a um servidor DNS que o cliente pode utilizar para atualização. O servidor DNS no RODC deve receber a atualizaçao do registro do servidor DNS que recebeu os detalhes da atualização utilizando uma solicitação replicate-single-object (replicação de objeto único) que é executada em segundo plano.

O Windows 7 e versões mais recentes adicionaram suporte ao DNSSEC (Extensões de segurança DNS). O cliente DNS com esses sistemas operacionais pode enviar consultas que indiquem suporte ao DNSSEC, processar registros relacionados e determinar se um servidor DNS possui registros validados em seu nome. Nos servidores Windows, isso permite que os servidores DNS assinem zonas com segurança e hospedem zonas assinadas com DNSSEC. Também permite que servidores DNS processem registros relacionados e desempenhem validação e autenticação.

Como utilizar o Windows Internet Name Service

O WINS é um serviço que resolve nomes de computadores para endereços IP. Utilizando o WINS, o nome do computador COMPUTER84, por exemplo, pode ser resolvido para um endereço IP que permita a computadores em uma rede Microsoft encontrarem-se e trocarem informações. O WINS é necessário para dar suporte a sistemas anteriores ao Windows 2000 e a aplicativos mais antigos que utilizam NetBiOS sobre TCP/IP, como os utilitários de linha de comando .NET. Se você não tiver aplicativos ou sistemas anteriores ao Windows 2000 na rede, não precisa utilizar o WINS.

O WINS funciona melhor em ambientes de cliente/servidor nos quais os clientes WINS enviam solicitações de resolução de nomes com rótulo único (host) para servidores WINS e os servidores WINS resolvem essas solicitações e respondem com o endereço IP equivalente. Quando todos os seus servidores DNS tiverem o Windows Ser-

ver 2008 ou uma versão mais recente, implantar uma zona de Nomes Globais (Global Names) cria registros globais estáticos, com rótulo único, sem depender do WINS. Isso permite que os usuários tenham acesso a hosts utilizando nomes de rótulo único em vez de FQDNs e remove a dependência ao WINS. Para transmitir informações e consultas WINS, os computadores utilizam o NetBIOS. O NetBIOS fornece uma interface de programação de aplicativo (API, application programming interface) que possibilita a comunicação entre os computadores de uma rede. Os aplicativos do NetBIOS dependem do WINS ou do arquivo LMHOSTS local para resolver nomes de computadores para endereços IP. Nas redes anteriores ao Windows 2000, o WINS era o principal serviço de resolução de nomes disponível. No Windows 2000 e em redes mais recentes, o DNS é o principal serviço de resolução de nomes e o WINS tem uma função diferente. Essa função serve para fazer com que sistemas anteriores ao Windows 2000 possam navegar por listas de recursos da rede e para permitir que o Windows 2000 e sistemas mais recentes localizem os recursos NetBIOS.

Para habilitar a resolução de nomes WINS na rede, é preciso configurar os clientes e servidores WINS. Quando você configura os clientes WINS, informa aos clientes os endereços IP dos servidores WINS da rede. Utilizando esses endereços, os clientes podem comunicar-se com os servidores WINS de qualquer parte da rede, mesmo que os servidores estejam em sub-redes diferentes. Os clientes WINS também podem comunicar-se utilizando um método de transmissão através do qual os clientes transmitem mensagens para outros computadores do mesmo segmento da rede local solicitando seus endereços IP. Pelo fato de essas mensagens serem transmitidas por difusão (broad-cast), o servidor WINS não precisa ser utilizado. Qualquer cliente sem WINS que suporte esse tipo de transmissões de mensagem também poderá utilizar esse método para resolver nomes de computador para endereços IP.

Quando os clientes comunicam-se com servidores WINS, estabelecem sessões que têm estas três partes:

- **Registro de nome** Durante o registro de nome, o cliente dá ao servidor seu nome de computador e seu endereço IP e solicita que seja adicionado no banco de dados WINS. Se o nome de computador e endereço IP não estiverem em uso na rede, o servidor WINS aceita a solicitação e registra o cliente no banco de dados WINS.
- **Renovação de nome** O registro de nome não é permanente. Em vez disso, o cliente pode utilizar o nome por um período específico chamado de *concessão*. O cliente também recebe um prazo para renovar a concessão, esse prazo é chamado de intervalo de renovação. O cliente deve registrar-se novamente no servidor WINS durante o intervalo de renovação.
- **Liberação de nome** Se o cliente não puder renovar a concessão, o registro de nome é liberado, permitindo que outro sistema da rede utilize o nome de computador, endereço IP ou ambos. Os nomes também são liberados quando um cliente WINS é desligado.

Depois que um cliente estabelece um sessão com o servidor WINS, o cliente pode solicitar serviços de resolução de nome. O método utilizado para resolver nomes de computador para endereço IP depende de como a rede está configurada. Estes quatro métodos de resolução de nomes estão disponíveis:

- **B-node (difusão)** Utiliza mensagem de difusão para resolver nomes de computador para endereços IP. Computadores que necessitam resolver um nome

transmitem uma mensagem para cada host da rede local, solicitando o endereço IP para um nome de computador. Em uma rede grande com centenas ou milhares de computadores, essas mensagens de difusão podem usar largura de banda significativa da rede.

- **P-node (ponto a ponto)** Utiliza servidores WINS para resolver nomes de computador para endereços IP. Como explicado anteriormente, sessões de cliente têm três partes: registro de nome, renovação de nome e liberação de nome. Nesse modo, quando um cliente precisa resolver um nome de computador para um endereço IP, o cliente envia uma mensagem de consulta ao servidor e o servidor responde com uma resposta.
- **M-node (misto)** É uma combinação de B-node com P-node. Com o M-node, um cliente WINS primeiramente tenta utilizar o B-node para resolução de nomes. Se a tentativa falhar, o cliente tenta utilizar o P-node. Como o B-node é utilizado antes, esse método tem os mesmos problemas com uso da largura de banda da rede que o B-node.
- **H-node (híbrido)** Também é uma combinação de B-node com P-node. Com o H-node, um cliente WINS primeiramente tenta utilizar o P-node para resolução de nomes ponto a ponto. Se a tentativa falhar, o cliente tenta utilizar mensagem de difusão com o B-node. Como o primeiro método é o ponto a ponto, o H-node oferece o melhor desempenho na maioria das redes. O H-node também é o método padrão para resolução de nomes WINS.

Se servidores WINS estiverem disponíveis na rede, os clientes Windows utilizam o método P-node para resolução de nomes. Se não houver servidores WINS disponíveis na rede, os clientes Windows utilizam o método B-node para resolução de nomes. Computadores com Windows também podem utilizar o DNS e os arquivos locais LMHOSTS e HOSTS para resolver nomes de rede. O Capítulo 16 aborda como trabalhar com o DNS.

Quando você utiliza o DHCP para atribuir endereços IP dinamicamente, deve configurar o método de resolução de nomes para clientes DHCP. Para fazer isso, configure as opções de escopo DHCP para 046 WINS/NBT Node Type como especificado em "Configuração das opções de escopo" no Capítulo 15. O melhor método a utilizar é o H-node. Você obterá o melhor desempenho e terá tráfego de rede reduzido.

Como utilizar o Link-Local Multicast Name Resolution (LLMNR)

O LLMNR atende a uma necessidade por serviços ponto a ponto de resolução de nomes para dispositivos com um endereço IPv4, IPv6 ou ambos, permitindo que dispositivos IPv4 e IPv6 em uma única sub-rede sem um servidor WINS ou DNS resolvam o nome um do outro – um serviço que nem o WINS nem o DNS podem fornecer inteiramente. Embora o WINS possa fornecer serviços de resolução de nomes ponto a ponto e cliente/servidor para IPv4, ele não suporta endereços IPv6. O DNS, por outro lado, suporta endereços IPv4 e Ipv6, mas depende dos servidores designados a fornecer serviços de resolução de nomes.

O Windows 7 e versões mais recentes dão suporte ao LLMNR. O LLMNR é projetado para clientes IPv4 e IPv6 em configurações nas quais outros sistemas de resolução de nomes não estão disponíveis, como em:

- Redes residenciais ou de escritórios pequenos
- Redes ad hoc
- Redes corporativas em que serviços DNS não estão disponíveis

O LLMNR é projetado para complementar o DNS habilitando resolução de nomes em situações nas quais a resolução de nomes DNS convencional não é possível. Embora o LLMNR possa substituir a necessidade pelo WINS nos casos em que o NetBIOS não é necessário, o LLMNR não é um substituto do DNS porque opera somente na sub-rede local. Como impede-se que o tráfego do LLMNR propague-se pelos roteadores, ele não tem como saturar a rede por acidente.

Como o WINS, utiliza-se o LLMNR para resolver um nome de host, como COMPUTER84, para um endereço IP. Por padrão, o LLMNR vem habilitado em todos os computadores com Windows 7 ou versões mais recentes, e esses computadores utilizam o LLMNR somente quando todas as tentativas de procurar por um nome de host através do DNS falham. Como resultado, a resolução de nomes funciona assim para o Windows 7 e versões mais recentes:

1. Um computador host envia uma consulta para seu servidor DNS configurado como primário. Se o computador host não receber uma resposta ou receber um erro, ele tenta cada servidor DNS configurado como alternativo por vez. Se o host não tiver um servidor DNS configurado ou não conseguir conectar-se a um servidor DNS sem erros, a resolução de nomes falha e passa para o LLMNR.
2. O computador host envia uma consulta multicast por meio do protocolo UDP (User Datagram Protocol) solicitando o endereço IP para o nome que está procurando. Essa consulta é restrita à sub-rede local (também chamada de *link local*).
3. Cada computador no link local que dê suporte ao LLMNR e que seja configurado para responder as consultas que chegam recebe a consulta e compara o nome ao seu próprio nome de host. Se o nome de host não for igual, o computador descarta a consulta. Se o nome de host for igual, o computador transmite uma mensagem unicast contendo o seu endereço IP para o host original.

Também é possível utilizar o LLMNR para mapeamento reverso. Com um mapeamento reverso, um computador envia uma consulta unicast para um endereço IP específico, solicitando o nome de host do computador de destino. Um computador com LLMNR habilitado que recebe a solicitação envia uma resposta unicast contendo seu nome de host para o host de origem.

Exige-se que computadores com LLMNR habilitado garantam que seus nomes sejam únicos na sub-rede local. Na maioria dos casos, um computador verifica se há exclusividade quando é iniciado, quando é retomado após um estado de suspensão e quando você altera as configurações da interface de rede. Se um computador ainda não tiver determinado que o nome é exclusivo, deve indicar essa condição quando responder a uma consulta de nome.

MUNDO REAL **Por padrão, o LLMNR vem habilitado automaticamente em computadores com Windows 7 ou versões mais recentes. É possível desabilitar o LLMNR através das configurações de registro. Para desabilitar o LLMNR para todas as interfaces de rede, crie e defina com valor 0 o seguinte item no registro: HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast.**

Para desabilitar o LLMNR para interfaces de rede específicas, crie e defina com valor 0 para o item no registro: HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Adapter-GUID/EnableMulticast.

Aqui, *AdapterGUID* é o identificador global exclusivo (GUID, global unique identifier) do adaptador de interface de rede para o qual você deseja desabilitar o LLMNR. É possível habilitar o LLMNR novamente a qualquer momento configurando para 1 esses valores de registro. Você também pode gerenciar o LLMNR usando Group Policy.

Ferramentas frequentemente utilizadas

Muitos utilitários estão disponíveis para administrar os sistemas Windows Server 2012. As ferramentas mais utilizadas incluem as seguintes:

- **Control Panel** Uma coleção de ferramentas para gerenciar a configuração do sistema. É possível organizar o Control Panel de diferentes formas de acordo com o modo de exibição que estiver utilizando. Um modo de exibição é simplesmente uma forma de organizar e representar opções. Altera-se o modo de exibição utilizando a lista View By. O modo Category é o padrão e fornece acesso a ferramentas por categorias, ferramentas e tarefas-chave. Os modos Large Icons e Small Icons são modos de exibição alternativos que listam cada ferramenta separadamente por nome.
- **Ferramentas administrativas gráficas** Ferramentas-chave para gerenciar os computadores da rede e seus recursos. É possível acessar essas ferramentas selecionando-as individualmente no grupo de programa Administrative Tools.
- **Assistentes administrativos** Ferramentas projetadas para automatizar tarefas administrativas-chave. É possível acessar muitos assistentes administrativos no Server Manager – o console de administração central do Windows Server 2012.
- **Utilitários de linha de comando** É possível iniciar a maioria dos utilitários usando o prompt de comando. Além desses utilitários, o Windows Server 2012 fornece outros que são úteis para trabalhar com os sistemas Windows Server 2012.

Para aprender como utilizar qualquer uma das ferramentas de linha de comando .NET, digite **NET HELP** em um prompt de comando seguido pelo nome do comando, como **NET HELP SHARE**. O Windows Server 2012 fornece, então, uma visão geral de como o comando é utilizado.

Windows PowerShell 3.0

Para mais flexibilidade nos scripts de sua linha de comando, o Windows PowerShell 3.0 é uma alternativa. O Windows PowerShell 3.0 é um comando shell completo que pode utilizar comandos internos (chamados de *cmdlets)*, recursos de programação internos e utilitários de linha de comando padrão. Um console de comando e um ambiente gráfico estão disponíveis.

Embora o console do Windows PowerShell e o ambiente de criação de scripts gráfico estejam instalados por padrão, muitos outros recursos do PowerShell não vêm instalados por padrão. Dentre eles estão o mecanismo Windows PowerShell 2.0, que é fornecido para compatibilidade com versões anteriores de aplicativos host PowerShell, e o Windows PowerShell Access, que permite ao servidor agir como um gateway da web para gerenciar o servidor remotamente utilizando o PowerShell e um cliente web.

MUNDO REAL **É possível instalar todos esses recursos adicionais do Windows PowerShell utilizando o assistente Add Roles And Features (Adicionar Funções e Recursos). Na área de trabalho, toque ou clique no botão Server Manager na barra de tarefas. Essa opção está inclusa por padrão. Em Server Manager, toque ou clique em Manage e depois em Add Roles And Features. Isso faz com que o assistente Add Roles And Features seja executado, com ele é possível adicionar recursos. Observe, no entanto, que com o Windows Server 2012, além de poder desabilitar uma função ou recurso, também é possível remover os binários necessários para tal função ou recurso. Os binários necessários para a instalação de funções e recursos são chamados de *payloads*.**

O console do Windows PowerShell (PowerShell.exe) é um ambiente de 32 bits ou de 64 bits para trabalhar com o Windows PowerShell na linha de comando. Nas versões de 32 bits do Windows, você encontrará o PowerShell executável de 32 bits no diretório %SystemRoot%\System32\ WindowsPowerShell\v1.0. Nas versões de 64 bits do Windows, você encontrará o PowerShell executável de 32 bits no diretório %SystemRoot%\SysWow64\WindowsPowerShell\v1.0 e o de 64 bits no diretório %SystemRoot%\System32\WindowsPowerShell\v1.0.

Na área de trabalho, é possível abrir o console do Windows PowerShell tocando ou clicando no botão PowerShell na barra de tarefas. Essa opção está inclusa por padrão. Em sistemas de 64 bits, a versão de 64 bits do PowerShell é iniciada por padrão. Se deseja utilizar o console do PowerShell de 32 bits em um sistema de 64 bits, é preciso selecionar a opção Windows PowerShell (x86).

Você pode iniciar o Windows PowerShell a partir de um prompt de comando do Windows (Cmd.exe) digitando o seguinte:

```
powershell
```

OBSERVAÇÃO **O caminho do diretório para o Windows PowerShell deverá estar em seu caminho de comando (path) por padrão. Isso garante que você possa iniciar o Windows PowerShell a partir de um prompt de comando sem antes ter que mudar para o diretório relacionado.**

Após iniciar o Windows PowerShell, você pode digitar o nome de um cmdlet no prompt e o cmdlet será executado de forma muito parecida com a de um comando de linha de comando. Também pode-se executar cmdlets em scripts. Cmdlets são nomeados utilizando pares de palavras (um verbo e um substantivo). O verbo indica o que o cmdlet faz no geral. O substantivo indica com o que especificamente o cmdlet trabalha. Por exemplo, o cmdlet Get-Variable recupera todas as variáveis de ambiente do Windows PowerShell e retorna seus valores, ou recupera uma variável de ambiente com nome específico e retorna seu valor. Os verbos comuns associados aos cmdlets são:

- **Get-** Pesquisa um objeto específico ou um subconjunto de um tipo de objeto, como um contador de desempenho específico ou todos os contadores de desempenho
- **Set-** Modifica as configurações específicas de um objeto
- **Enable-** Habilita uma opção ou um recurso
- **Disable-** Desabilita uma opção ou um recurso
- **New-** Cria uma nova instância de um item, como um novo evento ou serviço
- **Remove-** Remove uma instância de um item, como um evento ou log de evento

No prompt do Windows PowerShell, é possível obter uma lista completa de cmdlets digitando **get-help *-***. Para obter documentação de ajuda sobre um cmdlet específico, digite **get-help** seguido pelo nome do cmdlet, como em **get-help get-variable**.

Todos os cmdlets também possuem aliases configuráveis que agem como atalhos para a execução de um cmdlet. Para listar todos os aliases disponíveis, digite **get-item –path alias:** no prompt do Windows PowerShell. Você pode criar um alias que invoque qualquer comando utilizando o seguinte:

```
new-item –path alias:AliasName –value:FullCommandPath
```

Aqui, *AliasName* é o nome do alias a ser criado, e *FullCommandPath* é o caminho completo para o comando a ser executado, como

```
new-item –path alias:sm –value:c:\windows\system32\compmgmtlauncher.exe
```

Esse exemplo cria o alias *sm* para iniciar o Server Manager. Para utilizar esses alias, você deve simplesmente digitar **sm** e pressionar Enter quando estiver trabalhando com o Windows PowerShell.

MUNDO REAL **De modo geral, tudo o que pode ser digitado em um prompt de comando também pode ser digitado no prompt do PowerShell. Isso é possível porque o PowerShell procura utilitários e comandos externos como parte de seu processamento normal. Contanto que o utilitário ou comando externo encontre-se em um diretório especificado pela variável de ambiente PATH, o utilitário ou comando será executado adequadamente. Entretanto, lembre-se de que a ordem de execução do PowerShell pode determinar se um comando é executado como esperado ou não. Para o PowerShell, a ordem de execução é 1) aliases alternativos internos ou definidos por perfil, 2) funções internas ou definidas por perfil, 3) palavras-chave de idiomas ou cmdlets, 4) scripts com a extensão .ps1, e 5) arquivos, utilitários e comandos externos. Assim, se qualquer elemento de 1 a 4 na ordem de execução tiver o mesmo nome que um comando, esse elemento será executado em vez do comando esperado.**

Windows Remote Management

Os recursos de comunicação remota do Windows PowerShell são suportados pelo protocolo WS-Management e pelo serviço WinRM (Windows Remote Management) que implementa o WS-Management no Windows. Computadores com o Windows 7 e versões mais recentes, assim como o Windows Server 2008 R2 e versões mais recentes, incluem o WinRM 2.0 ou versão mais recente. Se quiser gerenciar um servidor do Windows a partir de uma estação de trabalho, é necessário ter certeza de que o WinRM 2.0 e o Windows PowerShell 3.0 estão instalados e de que o servidor possui um listener do WinRM habilitado. Uma extensão do IIS, instalável como um recurso do Windows chamado WinRM IIS Extension, permite que um servidor aja como um gateway da web para gerenciar o servidor remotamente utilizando o WinRM e um cliente web.

Como habilitar e utilizar o WinRM

É possível verificar a disponibilidade do WinRM 2.0 e configurar o Windows PowerShell para comunicação remota seguindo estas etapas:

1. Toque ou clique em Start; aponte para o Windows PowerShell. Inicie o Windows PowerShell como um administrador pressionando e segurando ou clicando com o botão direito do mouse no atalho para o Windows PowerShell e selecionando Run As Administrator.
2. Por padrão, o serviço WinRM vem configurado para inicialização manual. Deve-se alterar o tipo de inicialização para Automatic e iniciar o serviço em cada

computador com o qual deseja trabalhar. No prompt do Windows PowerShell, é possível verificar que o serviço WinRM está sendo executado, basta utilizar o seguinte comando:

```
get-service winrm
```

Como mostrado no exemplo a seguir, o valor da propriedade *Status* na saída deve ser *Running*:

```
Status    Name            DisplayName
-------   -----           -----------
Running   WinRM           Windows Remote Management
```

Se o serviço estiver pausado, digite o seguinte comando para iniciar o serviço e configurá-lo para iniciar automaticamente no futuro:

```
set-service –name winrm –startuptype automatic –status running
```

3. Para configurar o Windows PowerShell para utilização remota, digite o seguinte comando:

```
Enable-PSRemoting –force
```

É possível habilitar a utilização remota somente quando o computador estiver conectado a uma rede corporativa ou privada. Se seu computador estiver conectado a uma rede pública, é necessário desconectá-lo da rede pública e conectá-lo a uma rede corporativa ou privada para então realizar essa etapa. Se uma ou mais conexões do seu computador tiver o tipo de conexão Public Network mas estiver, na verdade, conectado a uma rede corporativa ou privada, é preciso alterar o tipo de conexão em Network And Sharing Center e então realizar essa etapa.

Em muitos casos, é possível trabalhar com computadores remotos em outros domínios. Entretanto, se o computador remoto não for um membro de domínio confiável, talvez o computador remoto não consiga autenticar as suas credenciais. Para habilitar a autenticação, é preciso adicionar o computador remoto à lista de hosts confiáveis para o computador local no WinRM. Para tanto, siga estas etapas:

```
winrm set winrm/config/client '@{TrustedHosts"RemoteComputer"}'
```

Aqui, *RemoteComputer* é o nome do computador remoto, como

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

Quando estiver trabalhando com computadores de um grupo de trabalho ou grupo doméstico, você deve utilizar HTTPS como transporte ou adicionar a máquina remota às configurações de TrustedHosts. Se não conseguir conectar-se a um host remoto, verifique se o serviço está sendo executado no host remoto e se ele está aceitando solicitações, para isso, execute o seguinte comando no host remoto:

```
winrm quickconfig
```

Esse comando analisa e configura o serviço WinRM. Se o serviço WinRM estiver configurado corretamente, você verá saídas parecidas com estas:

```
WinRM already is set up to receive requests on this machine.
WinRM already is set up for remote management on this machine.
```

Se o serviço WinRM não estiver configurado corretamente, você verá erros e precisará responder afirmativamente para diversos prompts que permitem configurar o gerenciamento remoto automaticamente. Quando esse processo estiver concluído, o WinRM estará configurado corretamente.

Sempre que utilizar os recursos remotos do Windows PowerShell, inicie o Windows PowerShell como um administrador pressionando e segurando ou clicando com o botão direito do mouse no atalho do Windows PowerShell e selecionando Run As Administrator. Para iniciar o Windows PowerShell a partir de outro programa, como o prompt de comando, é preciso iniciar tal programa como um administrador.

Como configurar o WinRM

Quando você estiver trabalhando com um prompt de comando elevado como administrador, pode utilizar o utilitário de linha de comando WinRM para visualizar e gerenciar a configuração do gerenciamento remoto. Digite **winrm get winrm/config** para exibir informações detalhadas sobre a configuração do gerenciamento remoto.

Se analisar a listagem de configuração, perceberá que há uma hierarquia de informações. A base dessa hierarquia, o nível Config, é referenciado com o caminho winrm/config. Em seguida há subníveis para cliente, serviço e WinRS, referenciados por winrm/config/client, winrm/config/service e winrm/config/winrs. É possível alterar o valor da maioria dos parâmetros de configuração utilizando o seguinte comando:

```
winrm set ConfigPath @{ParameterName="Value"}
```

Aqui, *ConfigPath* é o caminho da configuração, *ParameterName* é o nome do parâmetro com o qual você deseja trabalhar, e *Value* define o valor para o parâmetro, como

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Aqui, define-se o parâmetro *MaxShellsPerUser* dentro de winrm/config/winrs. Esse parâmetro controla o número máximo de conexões a um computador remoto que podem estar ativas por um usuário. (Por padrão, cada usuário pode ter apenas cinco conexões ativas.) Lembre-se de que alguns dos parâmetros são somente leitura e não podem ser configurados dessa forma.

O WinRM requer pelo menos um ouvinte (listener) para indicar transportes e endereços IP que aceitem solicitações de gerenciamento. O transporte deve ser HTTP, HTTPS ou ambos. Com HTTP, as mensagens podem ser criptografadas utilizando criptografia NTLM ou Kerberos. Com HTTPS, utiliza-se o protocolo SSL (Secure Sockets Layer) na criptografia. É possível analisar os ouvintes configurados digitando **winrm enumerate winrm/config/ listener**. Como mostrado na Listagem 1-1, esse comando exibe os detalhes da configuração dos ouvintes configurados.

LISTAGEM 1-1 Exemplo de configuração para ouvintes

```
Listener
    Address = *
    Transport = HTTP
    Port = 80
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.1.225
```

Por padrão, seu computador está provavelmente configurado para ouvir qualquer endereço IP. Se esse for o caso, você não verá saída. Para limitar o WinRM para endereços IP específicos, o endereço de loopback local do computador (127.0.0.1) e endereços IPv4 e IPv6 atribuídos podem ser configurados explicitamente para ouvir. Você pode configurar um computador para que ouça solicitações de todos os endereços IP configurados através do HTTP digitando o seguinte:

```
winrm create winrm/config/listener?Address=*+Transport=HTTP
```

Você pode ouvir solicitações de todos os endereços IP configurados através do HTTPS digitando isto:

```
winrm create winrm/config/listener?Address=*+Transport=HTTPS
```

Aqui, o asterisco (*) indica todos os endereços IP configurados. Perceba que a propriedade *CertificateThumbprint* deve estar vazia para compartilhar a configuração SSL com outro serviço.

É possível habilitar ou desabilitar um ouvinte para um endereço IP específico digitando

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP
@{Enabled="true"}
```

ou

```
winrm set winrm/config/listener?Address=IP:192.168.1.225+Transport=HTTP
@{Enabled="false"}
```

É possível habilitar ou desabilitar autenticação básica no cliente digitando

```
winrm set winrm/config/client/auth @{Basic="true"}
```

ou

```
winrm set winrm/config/client/auth @{Basic="false"}
```

Você pode habilitar ou desabilitar a autenticação do Windows usando o NTLM ou o Kerberos (conforme adequado) digitando

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

ou

```
winrm set winrm/config/client @{TrustedHosts=""}
```

Além de gerenciar o WinRM na linha de comando, é possível gerenciar o serviço utilizando Group Policy (política de grupo). Como resultado, as configurações via Group Policy podem acabar sobrescrevendo qualquer configuração que você inserir.