Capítulo 1

Planejamento de resolução de nomes e de endereçamento de protocolo de Internet

Como administrador corporativo, você será responsável pelo ambiente e pela arquitetura de TI geral dentro de sua empresa. Administradores corporativos convertem metas de negócios em decisões de tecnologia; projetam estratégias de médio a longo prazo; tomam decisões-chave e fazem recomendações sobre, por exemplo, infraestrutura de rede, serviços de diretório, diretivas de segurança, continuidade de negócios, estrutura administrativa, práticas recomendadas, padrões e service-level agreements (SLAs, contratos de nível de serviço).

O administrador corporativo é responsável pelas alterações no projeto de infraestrutura e na configuração global. Se pretende avançar em sua carreira e se tornar um administrador corporativo, ou se já desempenha tarefas de administrador corporativo e deseja adquirir uma certificação que corresponda à sua experiência, você já é um administrador de rede e de servidores experiente com, normalmente, experiência de dois anos ou mais administrando redes corporativas. O exame 70-647 não se destina a iniciantes, nem este kit de treinamento. Apenas 20% do exame 70-647 estão focados em suas habilidades em realizar tarefas; o exame está principalmente direcionado para o planejamento estratégico e para o projeto de tecnologias do Microsoft Windows Server 2008 R2 para satisfazer as necessidades dos sistemas de informação do negócio.

Como administrador experiente, você certamente conhece a resolução de nomes e o endereçamento de protocolo IP versão 4 (IPv4). Você provavelmente já se deparou com endereços do protocolo IP versão 6 (IPv6), mas talvez não os conheça bem. Este capítulo não tenta percorrer terreno antigo, mas, ao contrário, examina os novos recursos e abordagens implementados no Windows Server 2008 R2.

> ***IMPORTANTE*** **OBJETIVOS DO EXAME**
>
> Os objetivos relacionados com a resolução de nomes e o endereçamento IP no exame 70-647 são similares àqueles no exame 70-646 Windows Server 2008 Server Administration. Se você se preparou anteriormente para o exame 70-646, verá que este capítulo discute tópicos que já estudou. Nesse caso, trate este material como uma revisão.

Objetivos do exame neste capítulo:

- Planejar a resolução de nomes e o endereçamento IP.

Lições neste capítulo:

Antes de começar

Para concluir as lições deste capítulo, você deve ter:

- Instalado o Windows Server 2008 R2 Enterprise em um servidor configurado como um controlador de domínio no domínio *contoso.internal*. O Domain Name System (DNS, Sistema de Nomes de Domínio) integrado ao Active Directory é instalado por padrão no primeiro controlador de domínio de um domínio. O nome do computador é Glasgow. Configure um endereço IPv4 estático de 10.0.0.11 com uma máscara de sub-rede 255.255.255.0. O endereço IPv4 do servidor DNS é 10.0.0.11. Além da configuração IPv4 e do nome do computador, aceite todas as configurações de instalação padrão. Você pode obter uma versão de avaliação do Windows Server 2008 R2 Enterprise a partir do Centro de Download da Microsoft em *http://technet.microsoft.com/en-us/evalcenter/default.aspx*.
- Instalado o Windows Vista ou 7 Business (PRO), Enterprise ou Ultimate em um computador cliente vinculado ao domínio *contoso.internal*. O nome do computador é Melbourne. Inicialmente, esse computador deve ter um endereço IPv4 estático de 10.0.0.21 com uma máscara de sub-rede 255.255.255.0. O endereço IPv4 do servidor DNS é 10.0.0.11. Você pode obter o software de avaliação que permite implementar a edição de avaliação por 30 dias do Windows 7 Enterprise em *http://technet.microsoft.com/en-us/evalcenter/default.aspx*.
- Criado uma conta de usuário com o nome de usuário Kim_Akers e a senha P@ssw0rd. Adicione essa conta aos grupos Domain Admins, Enterprise Admins e Schema Admins.
- É recomendável utilizar uma rede isolada que não faça parte da sua rede de produção para fazer os exercícios práticos deste livro. O acesso à Internet não é exigido para os exercícios e você não precisa configurar um gateway padrão. Para minimizar tempo e despesas de configuração de computadores físicos, é recomendável

utilizar máquinas virtuais. Para executar computadores como máquinas virtuais dentro do Windows, você pode utilizar o Virtual PC 2007, Virtual Server 2005 R2, Hyper-V Server 2008 R2 ou um software de máquina virtual de terceiros. Para baixar o Virtual PC 2007, visite *http://www.microsoft.com/downloads/en/details.aspx?FamilyId=04D26402-3199-48A3-AFA2-2DC0B40A73B6&displaylang=en*.

- Para baixar o Virtual Server 2005 R2 ou o Hyper-V Server 2008 R2, visite *http://www.microsoft.com/windowsserversystem/virtualserver/downloads.aspx*.

Mundo real

David R. Miller

Como consultor há muitos anos, fui abordado por diversas empresas tendo problemas inesperados de rede. Muito frequentemente, uma das principais causas dos problemas era a implementação com falhas ou incompleta dos serviços de resolução de nomes. A variedade de peculiaridades relatada pelos usuários da rede é uma lista de fenômenos aparentemente não relacionados. Desde ícones e aplicativos desaparecidos da área de trabalho do usuário, a falhas na impressão, em logins e mais.

Mesmo que você execute apenas as últimas versões dos sistemas operacionais da Microsoft, é muito provável que haja aplicativos baseados no NetBIOS em execução na rede que falharão periodicamente sem uma implementação adequada do Windows Internet Name Service (WINS).

A função DNS Server no Windows Server 2008 R2 segue todas as Request For Comments (RFCs) que definem e padronizam o protocolo DNS. Embora a implementação da Microsoft do DNS deva ser interoperável com servidores e dispositivos DNS de terceiros, muitas vezes, quando o DNS está causando uma falha na empresa, só essa diferença sutil pode significar percorrer tranquilamente (ou não) os serviços de localização de resolução de nomes e de serviço de rede. Muitas vezes vi que, ao passo que servidores e dispositivos DNS de terceiros são gradualmente abandonados, a variedade de problemas de rede se torna um problema do passado.

Se seu ambiente tiver mais do que uns poucos servidores do Windows, você provavelmente deve estar executando o WINS e deve planejar cuidadosamente a implementação do DNS, com uma preferência por utilizar serviços DNS da Microsoft, que são finamente ajustados para dar suporte ao Active Directory.

Lição 1: Planejamento de resolução de nomes

Como administrador experiente, você já deve ter trabalhado com o DNS e com o DNS dinâmico da Microsoft. Você também deve conhecer os nomes do Network Basic Input Output System (NetBIOS), o NetBIOS Extended User Interface (protocolo NetBEUI) e o WINS. Portanto, o objetivo desta lição não é explicar a operação básica desses recursos, mas sim examinar as melhorias do Windows Server 2008 R2, especialmente para o DNS, e discutir o planejamento de uma infraestrutura de resolução de nomes através de uma rede corporativa.

Uma das primeiras decisões de planejamento que você precisa tomar é usar ou não o WINS para resolver nomes NetBIOS. A Microsoft descreve o WINS como tendendo a se tornar obsoleto e introduziu a zona DNS GlobalNames para fornecer a resolução de nomes de rótulo único para grandes redes corporativas que podem não querer implantar o WINS. Isso foi encarado como uma substituição para o WINS, mas a resolução de nomes do NetBIOS ainda é requerida por muitos aplicativos e sistemas operacionais herdados. Para a maioria dos ambientes, o WINS ainda é um requisito e, felizmente, tem suporte total no Windows Server 2008 R2.

Ao planejar uma infraestrutura DNS, você deve decidir quando utilizar zonas DNS integradas ao Active Directory, primárias padrão, secundárias, stub, de pesquisa inversa e GlobalNames. Você precisa planejar o encaminhamento DNS e quando utilizar o encaminhamento condicional, que é especialmente relevante para o ambiente corporativo em que pode ter múltiplas florestas do Active Directory Domain Services (AD DS, Serviços de Domínio Active Directory) funcionando na mesma intranet. O Windows Server 2008 R2 (e o Windows Vista e o Windows 7) suportam o IPv6 por padrão, e você precisa entender e utilizar os registros IPv6 no DNS. A segurança do sistema DNS foi aprimorada no lançamento do Windows Server 2008 R2, com a inclusão do DNSSEC, DNS Cache Locking e o uso de portas de origem não intuitivas a partir do DNS Socket Pool.

Depois de ler esta lição, você será capaz de:

- Identificar a função do WINS em seu ambiente de TI.
- Considerar os recursos DNS do Windows Server 2008 R2 ao planejar sua infraestrutura de resolução de nomes.
- Identificar as melhorias do Windows Server 2008 R2 para o DNS e utilizá-las em seu processo de planejamento.
- Determinar a necessidade do DNSSEC para fornecer informações de resolução de nomes confiáveis.
- Administrar o DNS utilizando o snap-in do Microsoft Management Console (MMC, Console de Gerenciamento da Microsoft) e ferramentas de linha de comando.

Duração estimada da lição: 45 minutos

Planejamento do sistema de nomes de domínio utilizando o Windows Server 2008 R2

O DNS resolve nomes de hosts para endereços IP e também pode resolver endereços IP para nomes de hosts em zonas DNS de pesquisa inversa. A função de servidor DNS

do Windows Server 2008 R2 conserva os recursos introduzidos pelo DNS do Windows Server 2003 e do Windows Server 2008, inclusive a configuração dinâmica e transferência da zona incremental, e apresenta diversos novos recursos e aprimoramentos de segurança. O Windows Server 2008 R2 dá suporte para o IPv4, bem como para o IPv6, e é praticamente essencial para o suporte do serviço de diretório do Active Directory da Microsoft. Esta lição abrange as melhorias para o DNS introduzidas no Windows Server 2008 R2 e como o DNS lida com endereços IPv6.

A Microsoft recomenda a utilização do serviço DNS Server do Windows Server 2008 R2 para dar suporte ao AD DS, embora outros tipos de servidores DNS possam dar suporte à implantação do AD DS. Um recurso introduzido no DNS do Windows Server 2003 que pode usufruir de Directory Replication Services (DRS, Serviços de replicação do diretório) do AD DS é a partição de diretório de Aplicativo para replicação. Uma partição é um contêiner de dados no AD DS que mantém dados para replicação. Você pode armazenar dados de aplicativos nas partições de diretório de Aplicativo do AD DS e, a seguir, especificar quais controladores de domínio devem receber uma cópia da partição utilizando o DRS.

Configuração do DNS do Windows Server 2008 R2

A integração com outros serviços do Windows, incluindo AD DS, WINS (se habilitado) e Dynamic Host Configuration Protocol (DHCP e DHCPv6) assegura que o DNS dinâmico do Windows Server 2008 R2 exija pouca ou nenhuma configuração manual. Computadores que executam o serviço DNS Client registram seus nomes de host e endereços IPv4 e IPv6 (embora não endereços IPv6 de link local) dinamicamente. Você pode configurar o DNS Server e os serviços DNS Client para realizar atualizações dinâmicas seguras. Isso assegura que somente computadores membros do domínio autenticados com os direitos apropriados possam atualizar registros de recurso no servidor DNS.

> ***MAIS INFORMAÇÕES*** **PROTOCOLO DE ATUALIZAÇÃO DINÂMICA**
>
> Para mais informações sobre o protocolo de atualização dinâmica, consulte *http://www.ietf.org/rfc/rfc2136.txt* e *http://www.ietf.org/rfc/rfc3007*.

> ***NOTA*** **ATUALIZAÇÕES DINÂMICAS SEGURAS**
>
> As atualizações dinâmicas seguras só estão disponíveis para zonas que estejam integradas com o AD DS.

Utilização de zonas stub

Uma *zona stub*, com suporte no DNS do Windows Server 2008 R2, é uma cópia de zona que contém apenas os registros de recursos necessários para identificar os servidores DNS autoritativos dessa zona. Isso inclui os registros SOA e NS para um namespace ou uma zona. Uma zona stub também detém os registros de recursos A para os servidores de nomes, mas não para todos os hosts registrados na zona. As zonas stub asseguram

que servidores DNS hospedando uma zona "parent" (pai) possam determinar servidores DNS autoritativos para zonas filhas, ajudando, assim, a manter uma resolução de nomes DNS eficiente. A Figura 1-1 mostra uma zona stub especificada no New Zone Wizard.

Você pode utilizar zonas stub quando os servidores de nome na zona destino estiverem em transição, como quando parte ou toda a rede da empresa estiver passado por uma transição de endereço IP e a resolução precisa de nomes for problemática. Por exemplo, a Contoso Ltd. recentemente adquiriu a empresa de vendas Litware Inc. A Contoso e a Litware têm domínios do Windows Server 2008 R2. Os servidores DNS da Litware têm uma configuração complexa com muitos registros de recursos dentro de muitas zonas e subzonas. A Litware utiliza controles de segurança apropriados para gerenciar de forma segura seus namespaces do DNS, assim esses sistemas DNS devem permanecer intactos. Além disso, você não quer ter de reproduzir esses numerosos controles e zonas em seus servidores DNS. Você configuraria zonas stub em seus servidores DNS para que eles sempre soubessem como encontrar os servidores DNS da Litware para a resolução exata de nomes e serviços, mesmo se os endereços IP dos servidores DNS da Litware mudarem.

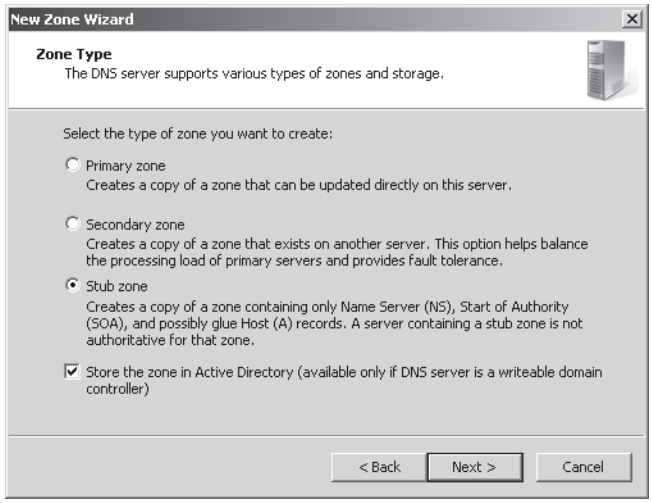

Figura 1-1 Criação de uma zona stub no New Zone Wizard.

Nesse caso, seu plano incluiria uma zona stub nos servidores DNS da Contoso com registros de recursos que identifiquem os servidores DNS autoritativos para o domínio *litware.com*. À medida que os nomes e endereços IP dos servidores DNS do domínio *litware.com* mudarem, a zona stub nos servidores DNS da Contoso será automaticamente atualizada com as alterações por meio de pequenas transferências de zona.

As zonas stub são úteis quando domínios filhos existem (somente do Active Directory ou namespace). Os registros de delegação são criados em uma zona para o domínio filho no servidor DNS do domínio pai. Os registros de delegação (na verdade um registro NS e um registro A para cada servidor DNS do domínio filho de interesse) são muitas

vezes chamados de registros cola (*glue records*), pois associam o namespace filho ao namespace pai para resolução. Por exemplo, o servidor de nomes para a zona *contoso.com* pode delegar autoridade para a zona *sales.contoso.com* a um servidor DNS naquele domínio filho. Então você utiliza zonas stub em domínios filhos para manter os registros de servidores DNS para domínios pais. Você utiliza registros de delegação para obter resolução para nomes e serviços em domínios filhos (delegar para baixo), e pode utilizar zonas stub nos servidores DNS do domínio filho para realizar resoluções e serviços em domínios pais (stub up).

Encaminhamento de DNS

Se um servidor DNS não tiver uma zona em seu banco de dados para o host de destino especificado em uma solicitação de cliente, poderá consultar outro servidor DNS (pré-configurado). Quando um servidor DNS encaminha uma solicitação de resolução de nomes em nome de um cliente, o servidor DNS upstream que puder auxiliar com a resolução é conhecido como *encaminhador*. Esse processo acontece recursivamente até o computador cliente receber o endereço IP ou o servidor DNS e o sistema encaminhador estabelecer que o nome consultado não pode ser resolvido.

O serviço DNS Server do Windows 2008 R2 utiliza *encaminhadores condicionais* para estender a configuração padrão do encaminhador. Um encaminhador condicional é um servidor DNS ao qual são encaminhadas consultas DNS segundo o nome de domínio DNS na consulta. Por exemplo, você pode configurar um servidor DNS para encaminhar todas as consultas que ele receber por nomes com terminação em *adatum.com* ao endereço IP de um ou mais servidores DNS especificados que sejam autoritativos para o domínio *adatum.com*. Esse recurso é especialmente útil em extranets corporativas, nas quais várias empresas e domínios possuem ligação direta entre suas redes privadas. Quando um servidor DNS do Windows Server 2008 R2 recebe uma consulta para um namespace desconhecido, ele primeiro verifica se a consulta corresponde a encaminhadores condicionais. Se não, o servidor DNS consultará recursivamente o encaminhador padrão. Se não houver um encaminhador condicional correspondente e o encaminhador padrão não puder resolver o nome, se configurado, o servidor DNS utilizará suas dicas raiz em uma tentativa de resolver o nome.

Quando o servidor DNS estiver instalado em um controlador de domínio, é geralmente recomendável remover as *dicas raiz* do servidor para que o servidor DNS (que também é um controlador de domínio) não tente realizar a resolução de nomes iterativa na Internet. Esses servidores DNS devem estar configurados com um encaminhador, muitas vezes um servidor DNS somente de cache, para realizar as consultas iterativas com o sistema de servidor raiz público.

> ***NOTA*** **REPLICAÇÃO DE ENCAMINHADORES ADICIONAIS**
>
> No Windows Server 2008 R2, as entradas de encaminhamento condicional podem ser armazenadas no AD DS e configuradas para replicar a todos os servidores DNS da floresta, todos os servidores DNS do domínio ou todos os controladores de domínio do domínio.

A Figura 1-2 mostra a caixa de diálogo utilizada para criar um encaminhador condicional. Você não pode realmente configurar isso em sua rede de testes porque só tem um servidor DNS.

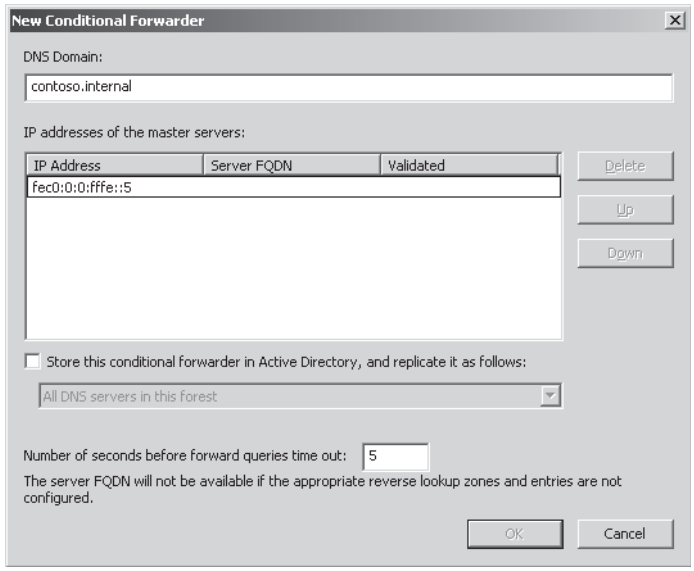

Figura 1-2 Especificação de um encaminhador condicional.

Transferências de zona e replicação

As zonas DNS do Windows Server 2008 R2 podem ser transferidas e replicadas entre servidores DNS para redundância e para aprimorar a eficiência da resolução de nomes do DNS. As zonas são replicadas para servidores DNS quando a zona estiver integrada ao Active Directory e ambos os servidores DNS existirem em controladores de domínio. Caso contrário, a zona é transferida entre um servidor DNS primário (master) e um secundário (ou slave). Se você adicionar um novo servidor DNS à rede e configurá-lo como um servidor DNS secundário para uma zona existente, ele realizará uma *transferência de zona* completa para obter uma cópia somente leitura de todos os registros de recursos na zona. Qualquer alteração adicional na zona autoritativa será transferida para a zona secundária em atualizações subsequentes da zona. O Windows Server 2003 introduziu a transferência de zona incremental que atualiza somente as alterações para a zona autoritativa e o Windows Server 2008 R2 dá suporte a essa funcionalidade. Antes do Windows Server 2003, uma transferência de zona completa era sempre necessária, ela atualizava todos os registros na zona DNS autoritativa para o servidor DNS secundário, mesmo se não tivessem sido alterados.

Você pode configurar transferências de zona para qualquer servidor DNS, apenas para servidores DNS especificados e para servidores DNS listados na guia Name Servers (qualquer servidor que tenha registrado um registro NS). A Figura 1-3 mostra uma zona

DNS configurada para permitir transferências de zona apenas para servidores DNS listados na guia Name Servers.

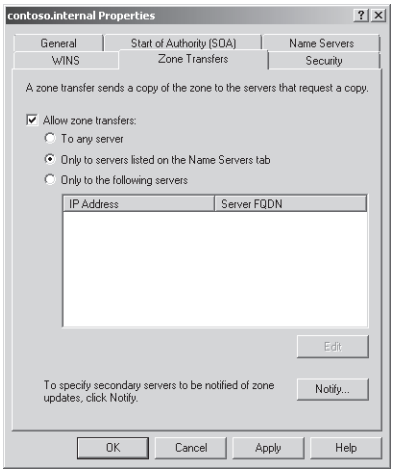

Figura 1-3 Configuração de transferências de zona.

Registros DNS

Como profissional de redes, você deve conhecer os tipos de registro DNS padrão, como host IPv4 (A), Start of Authority (SOA), Pointer (PTR, Resgistro ponteiro), nome canônico ou alias (CNAME), Name Server (NS, servidor de nomes), Mail Exchanger (MX), Service Location (SRV, Serviço de rede) e assim por diante. Você pode utilizar outros tipos de registro DNS, como Andrew File System Database (AFSDB) e endereço Asynchronous Transfer Mode (ATM, modo de transferência assíncrona), se estiver configurando a compatibilidade com sistemas DNS não Windows. Se precisar criar um registro IPv6 para um cliente que não pode se registrar com o AD DS, você precisa criar um registro AAAA manualmente.

Administração do DNS

Você pode utilizar a interface gráfica do snap-in DNS Manager do MMC para gerenciar e configurar o serviço DNS Server. O Windows Server 2008 R2 também fornece assistentes de configuração para realizar tarefas comuns de administração de servidor. A Figura 1-4 mostra a ferramenta DNS Manager bem como registros de host IPv4 e IPv6 registrados dinamicamente no DNS. Observe que, se acessar essa ferramenta neste ponto da lição, os registros IPv6 não serão exibidos, pois você ainda não configurou os endereços IPv6. Você o fará na sessão de prática mais adiante nesta lição e na Lição 2 deste capítulo.

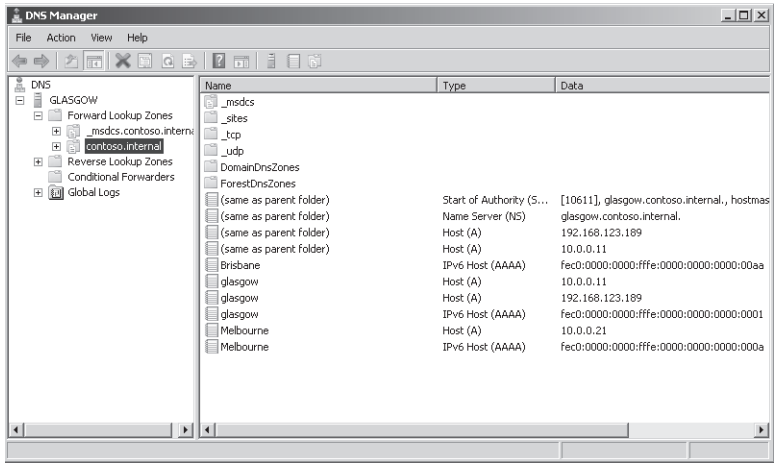

Figura 1-4 DNS Manager.

O Windows Server 2008 R2 fornece ferramentas de linha de comando que auxiliam no melhor gerenciamento de servidores e clientes DNS na rede e suporte a eles. As ferramentas a seguir se mostrarão úteis na configuração e administração de seu ambiente DNS. Lembre-se de visualizar a ajuda em cada um desses comandos para uma lista de seus parâmetros e funções detalhadas:

- ***dnscmd*** Para configurar e administrar o serviço DNS. Você pode gerenciar registros IPv4 e IPv6, criar zonas de pesquisa direta e pesquisa inversa (ou reversa), e gerenciar partições de diretório de aplicativos para replicação.
- ***ipconfig*** Para visualizar configurações IP do adaptador de rede. Você pode liberar e renovar as concessões de IPv4 e IPv6 de DHCP vinculadas a um adaptador de rede. Não esqueça o comando *ipconfig /all* para visualizar a configuração completa de IP.
- ***nslookup*** Para testar o serviço DNS e consultar informações de registro. Esse comando fornece seu próprio prompt de comando e pode ser utilizado para recuperar todos os registros de uma zona com o uso do comando *ls -d <nome do domínio/zona>*.

> ***NOTA NSLOOKUP LS -D <DOMAIN NAME>***
>
> A partir do Shell do comando *nslookup*, use o comando *ls -d <nome do domínio>* a fim de solicitar uma transferência de zona para o domínio especificado. A partir do Shell do prompt de comando (CMD), use o comando *nslookup -d <nome do domínio>* para solicitar a transferência de zona. Por motivos de segurança, por padrão, as transferências de zona estão desabilitadas. Para fazer esse comando funcionar corretamente, você deve permitir transferências de zona para o computador que executa esta solicitação via *nslookup*.

- ***netsh*** Uma ferramenta variada e poderosa para gerenciar interfaces de rede. Esse comando também fornece seu próprio prompt de comando. O comando *netsh interface ipv6 show dnsservers* exibe configurações DNS de IPv6 e indica quais endereços do servidor DNS estão configurados estaticamente.

Teste rápido

1. Qual comando de interface de linha de comando você pode utilizar para criar zonas de pesquisa inversa?
2. Quais comandos de interface de linha de comando liberam e renovam configurações de IPv6 dinâmico?

Respostas

1. *dnscmd*
2. *ipconfig /release6* e *ipconfig /renew6*

Utilização de novos recursos e aprimoramentos do DNS

A função DNS Server no Windows Server 2008 R2 fornece os recursos novos ou aprimorados a seguir:

- A função DNS Server do Windows Server 2008 R2 fornece *zonas somente leitura* primárias em read-only domain controllers (RODCs, controladores de domínio somente leitura). Uma zona DNS em um RODC é autoritativa, mas não é atualizada dinamicamente sempre que uma nova entidade de rede (cliente, servidor, impressora de rede ou projetor de rede) for adicionada ao domínio. Se uma entidade de rede for adicionada no mesmo site que um RODC, ele poderá recuperar os registros DNS correspondentes de um controlador de domínio gravável, desde que o controlador de domínio gravável esteja configurado para permiti-lo. Isso permite que a resolução de nomes seja realizada localmente no site, em vez de através de uma WAN (Wide area network, rede de longa distância).

MAIS INFORMAÇÕES **RODCS**

Para obter informações adicionais sobre os RODCs, visite *http://technet2.microsoft.com/windowsserver2008/en/library/ea8d253e-0646-490c-93d3-b78c5e1d9db71033.mspx?mfr=true*.

- O *DNS Security Extensions* (DNSSEC, extensões de segurança do DNS) utiliza certificados e assinaturas digitais para adicionar um elemento de verificação e relação de confiança ao sistema de resolução de nomes.
- O DNS Cache Locking pode ser utilizado para proteger entradas no cache do servidor DNS de serem substituídas. Os ataques de envenenamento do DNS podem se apoderar de conexões de clientes substituindo entradas no cache DNS com entradas apontando para endereços IP de servidores mal-intencionados.
- O DNS Socket Pool utiliza um pool randômico de portas de origem selecionadas na inicialização do serviço, em vez de utilizar uma porta de origem previsível. Isso reduz ainda mais a superfície de ataque do cache DNS e ajuda a proteger contra envenenamentos do DNS.
- A DNS Devolution proporciona resolução de nomes de host para sistemas que existam em domínios pai ao acrescentar, primeiro, o namespace de domínio para o do-

mínio base ao nome de host e realizar consulta e, a seguir, acrescentar o namespace de domínio para cada domínio pai ao nome de host e realizar consulta.

- O carregamento de dados de zona DNS é uma operação em segundo plano no Windows Server 2008 R2. Se precisar reiniciar um servidor DNS que hospede uma ou mais zonas DNS grandes armazenadas no AD DS, o servidor pode responder a consultas de cliente mais rapidamente porque não precisa esperar até que todos os dados da zona sejam carregados.
- A *zona DNS GlobalNames* fornece a resolução de nomes de rótulo único para grandes redes corporativas que não implantam o WINS. Essa zona é utilizada quando não é prático utilizar sufixos de nome DNS para fornecer a resolução de nomes de rótulo único.
- A função DNS Server do Windows Server 2008 R2 dá suporte completo a endereços IPv6. Ela implementa registros AAAA de IPv6 e dá suporte a zonas IPv6 de pesquisa inversa.

Suporte a RODCs

Um RODC fornece uma cópia de sombra de um controlador de domínio e não pode ser configurado diretamente. Isso o torna menos vulnerável a ataques. A Microsoft aconselha utilizar RODCs em localizações em que não é possível garantir a segurança física de um controlador de domínio. Você pode delegar a configuração do RODC a contas não administrativas e não precisa ter administradores de domínio ou corporativos trabalhando em filiais.

O DNS do Windows Server 2008 R2 dá suporte a zonas autoritativas primárias somente leitura (algumas vezes chamadas de zonas de filiais). Quando um servidor do Windows Server 2008 R2 está configurado como um RODC, ele replica a cópia somente leitura de todas as partições do Active Directory que o DNS utiliza, incluindo a partição de domínio, ForestDNSZones e DomainDNSZones. Um usuário com as permissões apropriadas pode visualizar o conteúdo de uma zona primária somente leitura, mas não pode alterá-lo. O conteúdo de uma zona somente leitura em um RODC se altera apenas quando a zona DNS no controlador de domínio mestre for alterada e o controlador de domínio mestre estiver configurado para permitir que o RODC recupere essas alterações.

Extensões de segurança do DNS

Historicamente, o sistema DNS tem permanecido desprotegido com poucas proteções de segurança, se alguma. Contudo, os riscos ao sistema DNS dentro de uma empresa e na Internet são numerosos. Imagine o que agressores poderiam realizar se conseguissem reconfigurar os servidores DNS na Internet. Eles poderiam se apoderar de todas as sessões Web que desejassem e redirecionar as conexões a sites falsificados ou a sites man-in-the-middle (de interceptação) que furtam dados, enchem de código mal-intencionado, e infectam e comprometem computadores cliente por todo o mundo. O DNSSEC é apontado como uma solução-chave para esse tipo de vulnerabilidade.

Baseado em RFCs, o DNSSEC do Windows Server 2008 R2 utiliza certificados e assinaturas digitais para fornecer origem autoritária, integridade dos dados e negação de existência autenticada. As assinaturas de zona são verificadas com o uso de uma chave pública confiável, chamada de âncora de confiança. Os clientes são configurados para

o DNSSEC utilizando configurações em uma nova Name Resolution Policy Table (NRPT, Tabela de diretiva de resolução de nomes) que pode ser implantada por diretiva de grupo (GPO, Group Policy Object) para membros do domínio, ou por meio das configurações de registro para não membros de domínio. As comunicações entre clientes e servidores DNS são autenticadas e protegidas com o uso do IPsec. O DNSSEC utiliza Next Secure (NSEC ou NSEC3) para proibir "passagem de zona" por agressores que recuperam todos os registros em uma zona.

> ***NOTA*** **INTEROPERABILIDADE DO DNSSEC**
>
> As implementações do DNSSEC no Windows Server 2003 e no Windows Server 2008 não são interoperáveis com a implementação do DNSSEC no Windows Server 2008 R2 devido à depreciação de RFCs mais antigas relacionadas ao DNSSEC.

Bloqueio de cache DNS

O *bloqueio de cache* proporciona segurança aprimorada contra o envenenamento de cache. Um ataque comum e relativamente fácil tem sido o envenenamento de cache DNS, no qual um agressor envia ao servidor DNS uma resposta DNS (normalmente não solicitada) para gravar ou substituir uma entrada no cache DNS de mapeamentos de nome para endereço IP previamente resolvidos do servidor. Esse mapeamento falso é utilizado para redirecionar clientes a sites ou outros serviços Web mal-intencionados. A capacidade de controlar se esses mapeamentos armazenados em cache podem ou não ser substituídos antes que seu Time-to-Live (TTL) termine naturalmente é nova no Windows Server 2008 R2.

DNS Socket Pool

Outro recurso para a proteção contra o envenenamento de cache DNS é o *DNS Socket Pool*. Esse recurso é novo no Windows Server 2008 R2 e permite que você especifique uma porta de origem selecionada de forma aleatória para o servidor DNS utilizar quando emitir consultas DNS. Em vez de sempre utilizar uma porta previsível, única e fácil de ser atacada, você pode configurar seu servidor DNS para selecionar de forma aleatória uma porta de origem para utilizar para suas consultas DNS em um intervalo de 1 a 10 mil portas diferentes. Quanto maior o pool, mais difícil será para o agressor adivinhar corretamente. As exclusões podem ser configuradas para portas e intervalos reservados. Por padrão, o DNS Socket Pool é configurado para utilizar um tamanho de pool de 2.500 com a porta específica selecionada dentro deste intervalo na inicialização do serviço.

Controle de DNS Devolution

DNS Devolution é o processo de acréscimo do sufixo de domínio local a um nome de host consultado e, se não resolvido, remoção de um nome da estrutura (do nome do domínio pai), construindo um fully qualified domain name (FQDN, nome de domínio totalmente qualificado) e, a seguir, nova consulta. Se não houver resolução, repetindo o processo até atingir alguns limites padrão no namespace. O Windows Server 2008 R2 ajusta o comportamento padrão para produzir mais resoluções bem-sucedidas e adiciona a capacidade de ajustar a profundidade do namespace para construir FQDNs. Por exemplo, para fazer as consultas pararem em *corp.contoso.com*, você deve definir um nível 3 de delegação de poderes, pois o namespace de domínio tem três rótulos: corp, contoso e com.

Carregamento de zona em segundo plano

Em uma empresa de grande porte com grandes zonas do Windows Server 2003 (ou versões anteriores) que armazenam dados do DNS em AD DS, reiniciar um servidor DNS pode levar um tempo considerável. O servidor DNS precisa recuperar dados da zona do AD DS e, enquanto isso, fica indisponível para atender a solicitações de clientes.

O DNS do Windows Server 2008 R2 lida com essa situação através do carregamento de zona de segundo plano. Um servidor DNS do Windows Server 2008 R2 carrega dados de zona do AD DS em segundo plano e pode responder quase imediatamente a solicitações de clientes quando reinicia, em vez de aguardar até que suas zonas sejam totalmente carregadas. Além disso, como os dados da zona são armazenados no AD DS e não em um arquivo, esses dados podem ser acessados assíncrona e imediatamente quando uma consulta é recebida. Os dados de zona baseada em arquivo só podem ser acessados por uma leitura de arquivo sequencial e requerem mais tempo para acessar do que dados no AD DS.

Quando o servidor DNS inicia, identifica todas as zonas a serem carregadas, carrega dicas de raiz (root hints) a partir de arquivos ou armazenadas no AD DS, carrega todas as zonas baseadas em arquivo e começa a responder a consultas e remote procedure calls (RPCs, chamadas de procedimento remoto) enquanto utiliza processos em segundo plano (threads de processador adicionais) para carregar zonas que são armazenadas no AD DS. O efeito do carregamento em segundo plano nessa situação é que um servidor DNS reinicializado entra no modo online mais rapidamente para compartilhar a carga de satisfazer a solicitações de clientes.

Teste rápido

- Qual registro DNS permite que um nome de host seja resolvido para um endereço IPv6?

Resposta

- AAAA

Utilização da zona DNS GlobalNames para suporte herdado

O WINS utiliza o NetBT, que a Microsoft descreve como uma abordagem obsoleta. Contudo, ele fornece registros estáticos, globais, com nomes de rótulo único e ainda é muito utilizado. O DNS do Windows Server 2008 R2 introduz a zona GlobalNames para manter nomes de rótulo único e fornecer suporte herdado para redes que antes utilizavam o WINS para resolução de nomes NetBIOS. Normalmente, o escopo de replicação dessa zona é a floresta inteira, assegurando que a zona possa fornecer nomes de rótulo único por toda a floresta. Isso, todavia, requer que o nome NetBios (rótulo único) para um host seja exclusivo em toda a floresta. A zona GlobalNames também dá suporte à resolução de nomes de rótulo único em todas as partes de uma empresa que contenha múltiplas florestas – contanto que você utilize os registros de recurso Service Location (SRV) para publicar a localização da zona GlobalNames. Isso potencialmente permite que empresas desabilitem o WINS e o NetBT. Como você já deve ter ouvido nos últimos dez anos, o WINS e o NetBT provavelmente não terão suporte em futuras versões do Windows Server. Você precisa lembrar-se disso ao planejar alterações em sua estrutura de resolução de nomes e ao decidir se conservará ou não o WINS. Desabilitar o NetBT

reduz a superfície de ataque de seus servidores e os torna menos vulneráveis a usuários mal-intencionados, mas pode introduzir alguns problemas para alguns aplicativos baseados no NetBIOS.

A zona GlobalNames fornece resolução de nomes de rótulo único para um conjunto limitado de nomes de hosts, em geral servidores e sites corporativos centralmente gerenciados, e não é utilizada para a resolução de nomes de ponto a ponto. A resolução de nomes de estação de trabalho de cliente e as atualizações dinâmicas não são suportadas. Em vez disso, a zona GlobalNames detém registros de recursos CNAME para mapear um nome de rótulo único para um FQDN. Em redes utilizando o WINS hoje, a zona GlobalNames em geral contém registros de recursos para nomes gerenciados centralmente que já estão estaticamente configurados no servidor WINS.

A Microsoft recomenda integrar a zona GlobalNames ao AD DS e configurar todos os servidores DNS autoritativos com uma cópia local da zona GlobalNames. Isso fornece desempenho e escalabilidade máximos. A integração AD DS da zona GlobalNames é necessária para dar suporte à implantação da zona GlobalNames em múltiplas florestas.

> ***NOTA*** **HABILITAÇÃO DE UM SERVIDOR DNS PARA DAR SUPORTE A ZONAS GLOBALNAMES**
>
> A opção */config* na ferramenta de linha de comando *dnscmd* habilita um servidor DNS para dar suporte a zonas GlobalNames.

> ***NOTA*** **REGISTRO DE GLOBALNAMES**
>
> Diferente do WINS, a funcionalidade da zona GlobalNames não permite que entradas de nome de host sejam registradas dinamicamente. Todas as entradas de nome de host na zona GlobalNames devem ser criadas manualmente.

Planejamento da replicação do WINS para suporte herdado

Como administrador corporativo, você precisa dar suporte a redes antigas como, por exemplo, os domínios do Windows NT 4.0. Embora tenhamos ouvido que o WINS está quase obsoleto, você precisa saber como lhe dar suporte e o incluir em seu planejamento e projeto. Perguntas sobre o WINS provavelmente aparecerão no exame 70-647. As principais decisões de planejamento e design que você precisa tomar ao planejar os serviços WINS serão sobre qual topologia de replicação do WINS utilizar. Talvez você não lide com o WINS há algum tempo e, por isso, esta seção inclui algumas informações básicas com a finalidade de revisão.

A replicação de banco de dados do WINS acontece sempre que o banco de dados do WINS for alterado em qualquer servidor WINS como, por exemplo, quando um nome do NetBIOS é liberado. A replicação do WINS habilita um servidor WINS para resolver nomes do NetBIOS de hosts registrados em outros servidores WINS. Para replicar entradas de banco de dados, cada servidor WINS deve estar configurado como pull partner (parceiro de recepção) ou como push partner (parceiro de envio) com ao menos um outro servidor WINS.

Um push partner envia uma mensagem para seus pull partners avisando-os quando seu banco de dados do WINS foi alterado. Quando os pull partners do servidor WINS

respondem à mensagem com uma solicitação de replicação, o servidor WINS envia uma cópia de suas novas entradas no banco de dados para seus pull partners.

Um pull partner é um servidor WINS que solicita novas entradas do banco de dados de seus push partners solicitando entradas com um número de versão mais alto do que as entradas recebidas durante a última replicação.

A replicação push ocorre quando um número determinado de atualizações para o banco de dados do WINS aconteceu e funciona melhor quando se tem links rápidos entre os servidores WINS que podem dar suporte a uma largura de banda alta. Você configura a replicação pull para acontecer em intervalos específicos e pode controlar o tráfego de replicação ajustando a largura de banda. A replicação pull é utilizada entre sites conectados por links WAN lentos. Para replicar entradas de banco de dados em ambas as direções, configure cada servidor para ser um push partner e um pull partner. Cada servidor WINS deve ser um push partner e um pull partner (mas não necessariamente um com o outro) para que a replicação seja concluída.

> ***NOTA*** **REPLICAÇÃO DO WINS**
>
> A replicação push ocorre quando um número determinado de entradas atualizadas do banco de dados do WINS é alcançado. A replicação pull é configurada para acontecer em intervalos específicos.

O modo como você planeja sua topologia de replicação do WINS depende principalmente dos requisitos da topologia de rede e da recuperação de desastre de sua empresa. As seguintes topologias de replicação do WINS estão disponíveis:

- **Topologia centralizada do WINS** Essa topologia utiliza um único servidor WINS centralizado de alta disponibilidade ou um cluster de servidores WINS. A topologia centralizada do WINS simplifica a implantação e a manutenção. Não existe sobrecarga de replicação de servidor-para-servidor e todos os clientes são configurados com o mesmo endereço de servidor WINS. A tolerância a falhas pode ser alcançada com o uso de cluster. Se, no entanto, o banco de dados compartilhado do cluster for corrompido, ele precisará ser restaurado a partir do backup. Não ocorre replicação do WINS nessa topologia. A topologia centralizada do WINS não fornece tolerância a falhas ao banco de dados WINS.
- **Topologia full-mesh do WINS** Essa topologia é um design distribuído do WINS com múltiplos servidores ou clusters WINS implantados por toda a empresa. Você precisa planejar a replicação do WINS para assegurar a sincronização do banco de dados do WINS entre todos os servidores WINS. Todos os servidores WINS se replicam com todos os outros servidores WINS. Você pode configurar a replicação manualmente ou utilizando o recurso de descoberta automática do WINS (configuração automática de parceiro). Em uma topologia full-mesh do WINS, alguns clientes podem ser configurados para utilizar um servidor WINS como o primário, e o restante dos clientes podem utilizar outro servidor WINS, o que permite a implementação do balanceamento de carga. A topologia full-mesh do WINS é normalmente utilizada quando a topologia de rede consiste em múltiplos datacenters e escritórios remotos. Cada servidor WINS replica com todos os outros servidores WINS nessa topologia, o que causa um volume significativo de tráfego de rede. Essa topologia

pode introduzir riscos de segurança e requer mais gerenciamento e suporte do que outras tecnologias. A topologia full-mesh do WINS é ilustrada na Figura 1-5.

- **Topologia ring (anel) do WINS** Essa topologia é um design distribuído do WINS em que cada servidor WINS se replica com um parceiro vizinho específico, formando um círculo. Essa topologia precisa ser criada manualmente, pois as relações entre cada par de servidores devem ser determinadas e configuradas por um administrador do WINS. Uma topologia de anel do WINS é mais simples de manter do que uma topologia full-mesh do WINS e você pode provisionar o balanceamento de carga distribuindo seus clientes pelos servidores WINS. No entanto, a solução de problemas é mais difícil em uma topologia de anel do WINS, e o *tempo de convergência*, ou seja, o tempo que uma alteração no banco de dados leva para se replicar para todos os servidores WINS, é maior porque as atualizações são transmitidas em sequência de servidor a servidor. A topologia de anel do WINS é ilustrada na Figura 1-5.
- **Topologia hub-and-spoke do WINS** Esse é um design distribuído do WINS em que um servidor WINS central é designado como o hub e servidores WINS adicionais se replicam somente com o hub no site em que estão localizados. Uma topologia hub-and-spoke do WINS fornece convergência eficiente, gerenciamento simples e provisionamento conveniente para balanceamento de carga. Ela é normalmente utilizada quando a topologia de rede consiste em um datacenter central e múltiplos escritórios remotos ou filiais. O datacenter central geralmente fornece a resolução de nomes para a maioria dos computadores da rede e as filiais fornecem a resolução de nomes para computadores locais. A topologia hub-and-spoke do WINS é ilustrada na Figura 1-5.

Quando tiver planejado sua topologia de replicação do WINS, você pode determinar o número necessário de servidores WINS. Isso depende do número de clientes que precisam de serviços de resolução de nomes do WINS, da largura de banda disponível para consultas e registros de nome de clientes e da replicação de servidor-para-servidor entre sites. Como diretriz, deveria haver um servidor WINS para cada 10 mil clientes, com um mínimo de dois servidores WINS para fornecer redundância em sites que precisam de serviços WINS altamente disponíveis.

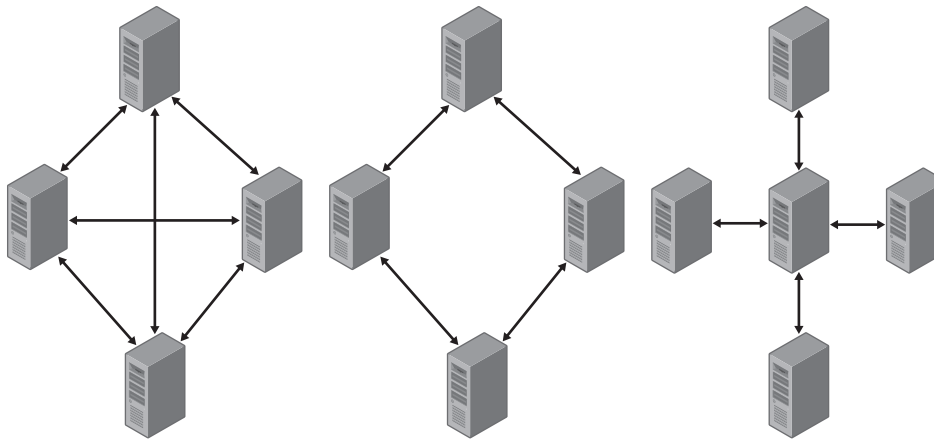

Figura 1-5 Topologias de replicação do WINS.

Suporte de endereços IPv6

O DNS do Windows Server 2008 R2 dá suporte tão completo a endereços IPv6 quanto a endereços IPv4. Os endereços IPv6 registram-se dinamicamente e você pode criar um registro de host AAAA para qualquer computador na rede com um sistema operacional que não dê suporte ao registro dinâmico. Você também pode criar zonas IPv6 de pesquisa inversa. Você configurará um registro AAAA e criará uma zona de pesquisa inversa (reversa) para IPv6 na sessão de prática mais adiante nesta lição.

> ***MAIS INFORMAÇÕES*** **ZONAS IPV6 DE PESQUISA INVERSA (REVERSA)**
>
> Para mais informações sobre zonas IPv6 de pesquisa inversa e informações adicionais sobre diversos tópicos relacionados ao IPv6, consulte *http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx*.

A ferramenta de linha de comando *dnscmd* aceita endereços tanto em formato IPv4 quanto IPv6. Os servidores DNS do Windows Server 2008 R2 podem enviar consultas recursivas para servidores de IPv6 e a lista de servidores de encaminhamento (forwarders servers) de DNS pode conter tanto endereços IPv4 como IPv6. Clientes DHCP podem registrar endereços IPv6 além de (ou em vez de) endereços IPv4. Os servidores DNS do Windows Server 2008 R2 dão suporte ao namespace de domínio *ip6.arpa* para pesquisa inversa.

> **Teste rápido**
>
> - Qual recurso o DNS do Windows Server 2008 R2 introduz que auxiliará empresas a abandonar gradualmente o WINS e o NetBT?
>
> **Resposta**
>
> - A zona GlobalNames

Planejamento de uma infraestrutura de DNS

Como profissional de rede, você deve saber que em um sistema DNS dinâmico a maioria dos hosts e servidores registra seus registros de host (A) automaticamente, e que você pode configurar o DHCP para criar registros DNS quando alocar concessões. Em comparação com o DNS estático anterior, em que os registros precisavam ser adicionados manualmente (a menos que o DNS fosse integrado com o WINS), o DNS dinâmico requer pouquíssima configuração manual.

Ao avançar em sua profissão escolhida, descobrirá que o planejamento toma muito de seu tempo, e o guia do exame menciona o planejamento de tarefas executadas por administradores corporativos e de decisões tomadas por eles; portanto, você precisa considerar o processo de planejamento de uma infraestrutura do DNS.

Planejamento de um namespace DNS

Planejar e definir um namespace DNS é normalmente tarefa para um administrador corporativo. Você precisa conhecer as opções disponíveis para que possa planejar e implementar decisões no nível da empresa de maneira mais eficiente.

Se você utilizar um namespace DNS somente para propósitos internos, o nome não precisa seguir o padrão definido na RFC 1123, "Requirements for Internet Hosts – Application and Support"; na RFC 2181, "Clarifications to the DNS Specification"; e no conjunto de caracteres especificado na RFC 2044, "UTF-8, a Transformation Format of Unicode and ISO 10646". O namespace *contoso.internal* que você configurou na rede de testes é um exemplo desse tipo de namespace.

Todavia, quando você especifica um namespace corporativo para ser utilizado na Internet, ele precisa ser registrado com a autoridade apropriada e seguir os padrões das RFC's relevantes. Exemplos de namespaces corporativos são *treyresearch.net* e *tailspintoys.com*. A maioria das empresas tem uma rede privada e uma rede pública. Você pode implementar a infraestrutura de namespaces do DNS utilizando um dos seguintes esquemas:

- Utilize namespaces diferentes (também chamados de quebrados ou não contíguos) para seus namespaces externos e internos, como *contoso.lan* e *contoso.com*. Isso aprimora a segurança isolando os dois namespaces um do outro e impedindo que recursos internos sejam expostos diretamente à Internet.

  Um projeto de DNS digno de consideração utiliza esse namespace não contíguo para representar a rede interna e o ambiente do Active Directory e os recursos Web voltados para o público. Utilize algo como *contoso.lan* e *contoso.com*, respectivamente. Na LAN (local area network, rede local) corporativa, configure um servidor DNS em um controlador de domínio para dar suporte ao empreendimento privado. Adicione uma *zona integrada ao Active Directory* para *contoso.lan* e configure-a utilizando todos os recursos melhores e mais recentes, como atualizações dinâmicas e replicação seguras para servidores DNS internos apropriados para balanceamento de carga, distribuição geográfica e redundância. Configure seus clientes do Active Directory/DNS para utilizar um servidor DNS próximo que hospede a zona integrada ao Active Directory para *contoso.lan* como seu servidor DNS preferencial e aponte para um servidor DNS diferente, do mesmo site ou de um site próximo que hospede *contoso.lan* como o alternativo.

  Nesse mesmo servidor DNS interno, configure uma zona DNS primária para os recursos que residam no namespace público *contoso.com*. Nessa zona *contoso.com*, você deve desabilitar atualizações dinâmicas e precisará adicionar manualmente registros de recursos para cada host público que quiser que o mundo público encontre.

  Configure um servidor DNS autônomo (não um membro do domínio do Active Directory *contoso.lan*) e baseado em arquivo que seja conectado à rede de perímetro (também conhecida como DMZ ou zona desmilitarizada). Adicione uma zona secundária para *contoso.com*, utilizando a zona interna *contoso.com* e o servidor como seu primário (master). Isso permite que você administre o namespace público em seu servidor DNS interno e torna a cópia da zona, na rede de perímetro, exposta. Como ela é uma cópia da zona somente leitura, fortalece a zona pública contra

ataques. Você obviamente precisará permitir e configurar transferências de zona da primária para a secundária, configurar a função Notificar para atualizações rápidas e fazer uma regra de permissão de ponto a ponto no firewall interno da rede de perímetro para passar as transferências de zona na porta 53.

Agora, o público pode acessar somente seus recursos públicos desejados e seus clientes internos do Active Directory podem acessar todo o namespace do Active Directory, bem como os recursos públicos da corporação.

- Utilize o mesmo namespace corporativo para as porções internas e externas (voltadas ao público) de sua rede. Essa configuração é chamada de DNS *split-horizon* e pode fornecer resolução segura de nomes a recursos nas redes interna e externa. No entanto, você precisa assegurar que os tipos de zona e os registros apropriados estão sendo armazenados nos servidores DNS internos e externos e que a segurança de sua rede interna está protegida.

  Utilize zonas integradas ao Active Directory em servidores DNS internos para dar suporte ao Active Directory. Utilize uma zona Primária (baseada em arquivo) no servidor DNS autônomo externo para dar suporte apenas aos recursos voltados ao público. Desabilite as atualizações dinâmicas na zona DNS pública. Adicione registros de recursos manualmente para os recursos públicos à zona interna integrada ao Active Directory e à zona pública.

  O servidor DNS público somente mantém registros públicos. A zona interna mantém todos os registros do Active Directory mais os registros públicos adicionados manualmente. Esses servidores nunca compartilham dados do DNS.

> ***NOTA*** **USUÁRIOS INTERNOS REQUEREM ACESSO A RECURSOS EXTERNOS**
>
> A utilização de um único namespace corporativo apresenta um desafio quando usuários internos precisam de resolução de nomes para recursos acessíveis publicamente, pois a zona DNS externa não está configurada para resolver recursos internos. Esse desafio pode ser superado pela duplicação manual dos registros de recursos externos em servidores DNS internos para clientes internos resolverem recursos da corporação voltados ao público. Você também pode configurar um DNS split (dividido), descrito mais adiante nesta lição.

- Utilize namespaces delegados para identificar a rede interna de sua empresa. Por exemplo, a Trey Research poderia ter o namespace público *treyresearch.net* e o namespace privado *intranet.treyresearch.net*. Isso se encaixa com a estrutura do Active Directory e é implementado com facilidade se você utilizar o DNS integrado ao Active Directory. Você precisa garantir que clientes internos possam resolver endereços de namespace externos, mas que clientes externos não possam resolver endereços de namespace internos. Todos os dados de domínio interno são isolados na árvore de domínio e requerem uma infraestrutura de servidor DNS própria. Um servidor DNS interno encaminhará as solicitações para um endereço de namespace externo a um servidor DNS externo. A desvantagem da delegação de namespace é que os FQDNs podem se tornar muito longos. A extensão máxima de um FQDN é de 255 bytes. Os FQDNs para controladores de domínio são limitados a 155 bytes.

A zona integrada ao Active Directory proporciona diversas vantagens. Uma das mais importantes é a vantagem que as informações da zona DNS são replicadas automa-

ticamente com outras informações do AD DS através de distributed file system replication (DFSR, replicação do sistema de arquivos distribuído). Você pode implementar RODCs que tenham zonas DNS autoritativas somente leitura e que proporcionem resolução de nomes local segura em filiais em que a segurança física dos servidores não possa ser garantida. Você pode implementar zonas DNS secundárias em *servidores Windows DNS* ou *BIND* que não precisam fazer parte da estrutura do Active Directory. Por exemplo, os servidores DNS nas zonas periféricas frequentemente são servidores autônomos.

O modo como você implementa o Active Directory em sua rede desempenha um papel importante na determinação de como os domínios devem ser criados e aninhados um dentro do outro. A sua estrutura de zona normalmente reflete sua estrutura de domínios do Active Directory, embora isso não seja obrigatório. Você pode criar zonas delegadas com facilidade. Por exemplo, você pode utilizar *engineering.tailspintoys.com* em vez de *tailspintoys.com/engineering*.

Você pode particionar o namespace do DNS por localização geográfica, departamento ou ambos. Por exemplo, se a Tailspin Toys tiver várias localizações, mas um único departamento de Recursos Humanos localizado no escritório da sede, você pode utilizar o namespace *hr.tailspintoys.com*. Se a Contoso Ltd. tiver uma sede em Denver e fábricas em Boston e Dallas, você pode configurar os namespaces *denver.contoso.com*, *boston.contoso.com* e *dallas.contoso.com*.

Planejamento do encaminhamento de DNS

Um encaminhador é um servidor DNS upstream que normalmente tem acesso a namespaces adicionais para resolução. Os clientes DNS, chamados de resolvedores, são configurados com o endereço IP de seu servidor DNS preferencial. Os resolvedores submetem consultas de resolução de nomes a seu servidor DNS preferencial. Se o servidor DNS não puder realizar a resolução e estiver configurado com o endereço IP de um encaminhador, o servidor DNS encaminhará a consulta de resolução ao encaminhador.

O Windows Server 2003 introduziu o encaminhamento condicional, descrito anteriormente nesta lição, e ele também pode ser utilizado no Windows Server 2008 R2. Visto que encaminhadores condicionais são mapeados para namespaces específicos, um namespace consultado é verificado em relação às listagens do encaminhador condicional antes do encaminhador (padrão) ser consultado. Você deve planejar utilizar encaminhadores condicionais quando precisar de resolução de nomes para namespaces para os quais o servidor DNS não seja autoritativo e quando souber o endereço IP de um servidor DNS que seja autoritativo para esse namespace. Isso é comum em florestas grandes, geográfica ou politicamente dispersas com muitos domínios do Active Directory.

DICA DO EXAME

Encaminhar solicitações DNS requer que o servidor DNS possa fazer consultas recursivas. As respostas de exame que sugerem configurar o encaminhamento e desabilitar a recursão podem ser descartadas, pois são incorretas.

Um cenário de encaminhamento DNS típico pode especificar um servidor DNS com permissão para encaminhar consultas a servidores DNS fora do firewall corporativo, como ao servidor DNS público do provedor de acesso à Internet (ISP, Internet Service Provider – provedor de serviços de Internet). Essa implementação possibilita que o firewall seja configurado para permitir tráfego DNS apenas a partir desse servidor DNS específico e para permitir que apenas respostas válidas sejam enviadas para o servidor DNS interno, na rede protegida. Utilizando essa abordagem, o tráfego DNS restante – tanto de entrada como de saída – pode ser descartado no firewall. Isso aprimora a segurança geral da rede e do serviço DNS.

Planejamento do tipo de zona

As redes do Active Directory normalmente utilizam servidores DNS instalados em controladores de domínio e utilizam zonas integradas ao Active Directory para resolução de nomes interna. Nesse caso, as informações de zona DNS são mantidas em controladores de domínio graváveis no domínio (em geral, todos os controladores de domínio são graváveis). Isso proporciona as vantagens de DFSR, failover e redundância de dados se um controlador de domínio parar de funcionar e tem a disponibilidade aumentada para aceitar atualizações por meio de sua disposição em vários mestres. As zonas primárias padrão instaladas em servidores autônomos do Windows podem ser utilizadas quando um servidor DNS gravável for necessário, mas o acesso ao banco de dados do Active Directory é considerado um risco de segurança; por exemplo, em zonas periféricas como a rede de perímetro. Os RODCs podem ser utilizados quando quiser as vantagens de um DNS integrado ao Active Directory, mas não puder garantir a segurança física de seus servidores, como em filiais.

As zonas *primárias* padrão, as integradas ao Active Directory e as *secundárias* padrão podem fornecer informações de zona para zonas DNS secundárias padrão. Em redes do Windows Server 2008 R2, as zonas DNS secundárias podem ser implementadas em controladores de domínio, servidores membro, servidores autônomos e RODCs. Instalar um servidor DNS secundário em uma localização remota pode melhorar significativamente a confiabilidade e a velocidade de resolução de nomes nessa localização. Os servidores de zona secundária aumentam a redundância fornecendo resolução de nomes mesmo se o servidor de zona primária não responder e, quando os resolvedores estão configurados corretamente, reduzem a carga em servidores primários distribuindo solicitações de resolução de nomes entre mais servidores DNS. Um servidor de zona secundária não precisa fazer parte do domínio do Active Directory (exceto no caso de controladores de domínio e RODCs) e você pode instalar zonas secundárias em servidores não Windows. Você também pode configurar servidores de zona secundária em máquinas virtuais.

Teste rápido

- Qual é o nome do registro que conecta um namespace pai a seu namespace filho? (Esse tipo de registro na verdade contém dois registros de recursos, um registro NS e um registro A.)

Resposta

- Um registro cola (glue record)

Como profissional de rede, você provavelmente já configurou a classificação por vencimento (aging) e a limpeza (scavenge) para registros de DNS, configurou atualizações dinâmicas, especificou escopos da replicação de zona e configurou transferências de zona. No entanto, uma coisa é saber como fazer essas configurações. Uma coisa bem diferente é planejar suas zonas e decidir quais são as melhores configurações para sua estrutura de resolução de nomes. Isso é trabalho para um administrador corporativo.

Se um grande número de registros de recurso obsoletos permanecer nas zonas, ocupará espaço em disco no servidor e causará transferências de zona desnecessariamente longas. Os servidores DNS que carregam zonas contendo registros de recurso obsoletos correm o risco de utilizar informações desatualizadas para responder a consultas de clientes, podendo causar problemas de resolução de nomes. Os servidores e as zonas DNS podem ser configurados para limpar registros de recursos obsoletos dentro de um período de tempo. Em ambientes em que registros de recursos podem se tornar obsoletos, você precisa garantir ter habilitado a limpeza desses registros.

O projeto das configurações de classificação por vencimento e limpeza depende do seu tráfego de resolução de nomes e da frequência com que sua rede é alterada. Uma rede que é razoavelmente estável, com algumas estações sendo adicionadas ou removidas, provavelmente pode ser configurada com longas configurações de classificação por vencimento e ciclos de limpeza menos frequentes do que um ambiente mais dinâmico. As limpezas frequentes e períodos curtos de classificação por vencimento podem aumentar seu tráfego de rede.

As zonas DNS também podem ser configuradas para permitir ou negar atualizações dinâmicas, embora seja incomum que atualizações dinâmicas sejam negadas em redes modernas. As zonas integradas ao Active Directory também podem ser configuradas para permitir apenas atualizações dinâmicas seguras. As atualizações dinâmicas seguras, discutidas anteriormente nesta lição, são altamente recomendadas por assegurarem que apenas alterações autorizadas sejam feitas nos dados do DNS.

> ***NOTA*** **ATUALIZAÇÕES DINÂMICAS SEGURAS**
>
> Somente zonas integradas ao Active Directory dão suporte a atualizações dinâmicas seguras.

Ao planejar o escopo da replicação de zonas integradas ao Active Directory, você precisa decidir se a zona deve ser replicada para todos os servidores DNS da floresta, todos os servidores DNS do domínio (o padrão) ou todos os controladores de domínio do domínio. Se precisar ampliar o escopo da replicação, você pode configurar a zona para se replicar para todos os servidores DNS da floresta. A replicação para todos os controladores de domínio é recomendada somente se você tiver controladores de domínio do Windows 2000 Server em seu ambiente.

Você pode configurar o servidor de nomes primário, o intervalo de atualização e os valores TTL mínimos padrão para registros de recursos da zona no registro SOA da zona. O TTL controla a quantidade de tempo mínima com que clientes, inclusive outros servidores DNS, armazenam em cache registros de recursos para a zona. Se seu ambiente for dinâmico, com alterações de endereço IP frequentes, planeje configurar o TTL mínimo com um valor baixo, como um dia.

Ao planejar zonas DNS, você precisa especificar se as transferências de zona são permitidas e, em caso afirmativo, para quais servidores. Você pode configurar transferências de zona para qualquer servidor, para os servidores de nomes listados na guia Name Servers ou na zona, ou para uma lista específica de servidores de nomes.

Planejamento de dicas de raiz

Quando você instala um servidor DNS do Windows Server 2008 R2 que tenha acesso à Internet, o servidor é automaticamente configurado com uma lista de servidores raiz. Se um servidor DNS receber uma consulta para uma zona DNS para a qual não é autoritativo, o servidor enviará uma consulta para um dos servidores raiz que inicia uma série de consultas iterativas até que o nome seja resolvido. Você pode utilizar dicas de raiz para preparar servidores que são autoritativos para zonas "não raiz" para que eles possam descobrir servidores autoritativos que gerenciem domínios em um nível mais alto ou em outras subárvores do namespace de domínio do DNS.

As dicas de raiz são essenciais para servidores que são autoritativos em níveis mais baixos do namespace para localizar e encontrar outros servidores. Por padrão, o serviço DNS Server implementa dicas de raiz usando um arquivo chamado *Cache.dns* que normalmente contém os registros de recursos NS e A para os servidores raiz da Internet. No entanto, se você estiver utilizando o serviço DNS Server em uma rede privada, deve planejar remover esse arquivo para desabilitar seu servidor DNS para consulta a servidores de nomes da Internet, ou editar ou substituir esse arquivo com registros similares que apontem para seus próprios servidores DNS de raiz internos.

Planejamento para integrar o AD DS a uma infraestrutura existente do DNS

Muitas organizações empresariais já utilizam um ou mais servidores Berkeley Internet Name Domain (BIND). O BIND fornece resolução de nomes para sistemas UNIX ou resolução de nomes da Internet para usuários internos. Nesse caso, o DNS integrado ao Active Directory precisa interoperar com a infraestrutura DNS do BIND.

Há duas opções disponíveis na infraestrutura DNS do Windows Server 2008 R2:

- Você pode utilizar a infraestrutura DNS existente para hospedar a zona DNS para o AD DS. Isso pode reduzir os requisitos de hardware e o trabalho administrativo. No entanto, essa opção também pode significar que a infraestrutura DNS tenha suporte por uma equipe diferente da que dá suporte ao AD DS. Como administrador corporativo, uma de suas tarefas é racionalizar sua equipe de suporte, e você ou seu gerente de linha podem achar essa opção inaceitável.
- Você pode implantar o DNS do Windows Server 2008 R2 para usufruir os diversos recursos avançados, como zonas integradas ao Active Directory, replicação de zonas e atualizações dinâmicas seguras. Utilize encaminhadores e zonas stub para integrar ambas as infraestruturas do DNS. Isso pode lhe dar uma maior flexibilidade para o projeto da infraestrutura do DNS, o projeto do namespace DNS e o modelo de administração do DNS. Os servidores DNS do Windows Server 2008 R2 podem encaminhar qualquer consulta DNS por registros hospedados na infraestrutura existente do DNS para os servidores DNS existentes.

A Figura 1-6 ilustra o encaminhamento de consultas DNS entre uma infraestrutura DNS do Windows Server 2008 R2 e uma infraestrutura DNS do BIND.

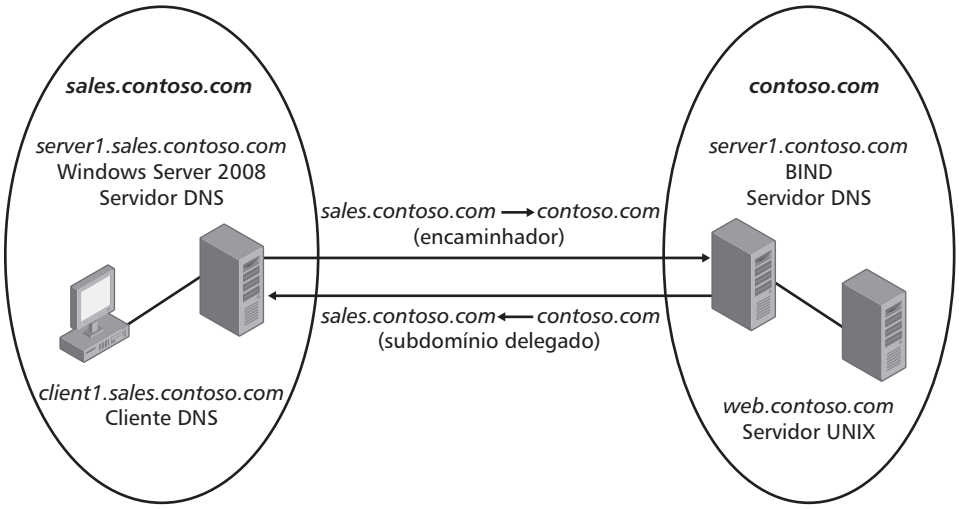

Figura 1-6 Encaminhamento de consultas DNS.

Por exemplo, a Contoso Ltd. tem uma infraestrutura existente do DNS baseada no BIND com o nome de domínio DNS *contoso.com*. A Contoso planeja implantar uma nova infraestrutura de DNS no Windows Server 2008 R2 para o AD DS com o nome de domínio DNS *sales.contoso.com*. Uma entrada de encaminhamento condicional para *contoso.com* foi criada no servidor DNS do Windows Server 2008 R2 no domínio *sales.contoso.com*. Os registros de delegação (ou glue record – registro cola) para *sales.contoso.com* foram criados em um servidor DNS baseado no BIND no domínio *contoso.com*.

Quando um cliente do domínio *sales.contoso.com* precisa acessar um servidor Web UNIX no namespace *contoso.com*, consulta seu servidor DNS preferencial no namespace *sales.contoso.com*. Esse servidor DNS não é autoritativo para a zona *contoso.com*, mas tem uma entrada de encaminhamento condicional para a zona *contoso.com*. Através da entrada de encaminhamento condicional no servidor DNS do namespace *sales.contoso.com*, o servidor DNS do Windows contata o servidor DNS baseado no BIND para o namespace *contoso.com* para recuperar a resolução de nome solicitada para *web.contoso.com* para o resolvedor.

Planejamento da zona GlobalNames

Historicamente, o DNS só resolvia FQDNs. Esses FQDNs precisavam de um nome de host com um componente de domínio, como *webserver1.contoso.com*. A zona GlobalNames permite a resolução de somente um nome de host, como o WINS no mundo NetBIOS, pois, por padrão, os nomes de host e os nomes NetBIOS são o mesmo. Para planejar o projeto de sua zona GlobalNames, você precisa entender os cenários de implantação em que uma zona GlobalNames pode ser configurada. Você pode implantar uma zona GlobalNames em um ambiente de floresta única ou de múltiplas florestas. Uma implantação em floresta única de uma zona GlobalNames permite a resolução de rótulo único ou de nome de host

através do DNS utilizando uma única zona GlobalNames integrada ao Active Directory. Uma implantação em múltiplas florestas de uma zona GlobalNames permite a resolução de nomes de host de rótulo único através do DNS utilizando uma zona GlobalNames integrada ao Active Directory para cada floresta do ambiente de múltiplas florestas.

Você pode adaptar a implantação da zona GlobalNames em floresta única para atender a uma série de requisitos de resolução de nomes de host de rótulo único das seguintes maneiras:

- **Todos os domínios e computadores cliente em uma floresta** A Microsoft recomenda esse cenário para empresas que tenham uma única floresta e um pequeno número de domínios. A resolução de nomes de rótulo único é fornecida para todos os computadores cliente inseridos no domínio da floresta. Nesse cenário, você precisa assegurar que todos os servidores DNS autoritativos da floresta sejam controladores de domínio do Windows Server 2008. Você precisa, então, criar uma zona GlobalNames integrada ao AD DS em um servidor DNS da floresta e replicá-la para todos os controladores de domínio da floresta que sejam servidores DNS. A seguir, adicione registros CNAME para nomes de rótulo único apontando para o FQDN dos servidores de recursos.
- **Uma zona GlobalNames em múltiplas florestas** Esse cenário de implantação é recomendado para empresas que tenham múltiplos domínios e florestas. Você pode personalizar um servidor DNS para múltiplas florestas para atender a diversos requisitos de resolução de nomes de rótulo único para todos os domínios e computadores cliente em todas as florestas assegurando que todos os servidores DNS autoritativos da floresta sejam servidores DNS em controladores de domínio do Windows Server 2008. Você também precisa garantir que a funcionalidade da zona GlobalNames tenha sido habilitada em cada servidor DNS da floresta. Você cria uma zona GlobalNames integrada ao AD DS em um servidor DNS em uma floresta e replica a zona GlobalNames para todos os controladores de domínio da floresta que sejam servidores DNS. A seguir, você adiciona registros CNAME para nomes de rótulo único apontando para o FQDN dos servidores de recursos. Em cada uma das outras florestas, você adiciona *registros de recursos* de serviço apontando para cada servidor DNS controlador de domínio remoto que hospede uma cópia local da zona GlobalNames para a zona *_msdcs* que abrange a floresta.
- **Um conjunto seleto de servidores DNS hospeda a zona GlobalNames** A Microsoft recomenda esse cenário de implantação para empresas que tenham múltiplos domínios e florestas, mas queiram limitar a zona GlobalNames a um conjunto seleto de servidores DNS. Esse cenário de implantação fornece a resolução de nomes de rótulo único para todos os computadores cliente nas florestas.
- **Domínios seletos através de múltiplas florestas** A Microsoft recomenda essa implantação quando você quiser implantar uma zona GlobalNames em um ambiente de múltiplas florestas em um conjunto de domínios seletos como um programa-piloto.

Prática: Configure o DNS

Nesta prática, você fará uma configuração IPv6 estática no controlador de domínio Glasgow. A seguir, você configurará um registro AAAA estático e uma zona IPv6 de pesquisa inversa. Por fim, você criará um registro ponteiro (PTR) na zona de pesquisa inversa para o computador Glasgow.

Exercício 1: Configuração do IPv6 no computador Glasgow

Neste exercício, você configurará o IPv6 no computador Glasgow (o controlador de domínio). Você precisa fazê-lo porque criará uma zona IPv6 de pesquisa inversa e um registro PTR para o computador Glasgow nos próximos exercícios. O exercício pede que você efetue logon interativamente no controlador de domínio. Se você quiser fazê-lo de forma mais realista, pode efetuar logon no cliente Melbourne e se conectar ao controlador de domínio através da Área de Trabalho Remota.

1. Efetue logon no controlador de domínio Glasgow com a conta Kim_Akers.
2. A partir do Painel de Controle, inicie o Network and Sharing Center. Clique em Change Adapter Settings.
3. Clique com o botão secundário do mouse na conexão de rede de sua rede privada e escolha Properties.
4. Se uma caixa de diálogo Universal Access Control (UAC) aparecer, clique em Continue para fechá-la.
5. Selecione Internet Protocol Version 6 (TCP/IPv6) e clique em Properties.
6. Configure o endereço IPv6 estático de site local **fec0:0:0:fffe::1**.
7. Configure o endereço do servidor DNS preferencial **fec0:0:0:fffe::1**. A caixa de diálogo Properties deve ser similar à Figura 1-7.

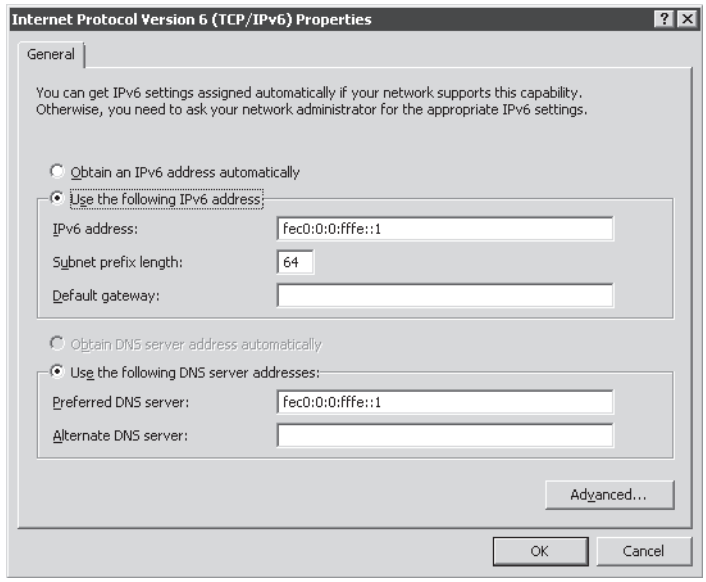

Figura 1-7 Configuração do IPv6 no controlador de domínio.

8. Clique em OK. Feche a caixa de diálogo Local Area Connections Properties.
9. Feche a janela Network Connections.
10. Feche o Network And Sharing Center.

> ***NOTA*** **MÁQUINAS VIRTUAIS**
>
> Se estiver utilizando uma máquina virtual para implementar seu servidor e cliente no mesmo computador, é recomendável fechar sua máquina virtual e reiniciar seu computador após configurar as interfaces.

Exercício 2: Configuração de um registro AAAA

O servidor autônomo Brisbane tem um sistema operacional que não pode se registrar no DNS do Windows Server 2008 R2. Portanto, você precisa criar um registro AAAA manual para esse servidor. Seu endereço IPv6 é fec0:0:0:fffe::aa. Observe que você pode criar um registro AAAA para esse servidor mesmo que ele não exista atualmente em sua rede.

1. Se necessário, efetue logon no controlador de domínio Glasgow com a conta Kim_Akers.
2. Em Administrative Tools, abra o DNS Manager.
3. Se uma caixa de diálogo UAC aparecer, clique em Continue.
4. No DNS Manager, expanda Forward Lookup Zones. Clique com o botão secundário do mouse em *contoso.internal* e escolha New Host (A ou AAAA).
5. Insira o nome do servidor e o endereço IPv6 como mostrado na Figura 1-8. Certifique-se de que a caixa de seleção Create associated pointer (PTR) Record não esteja marcada.

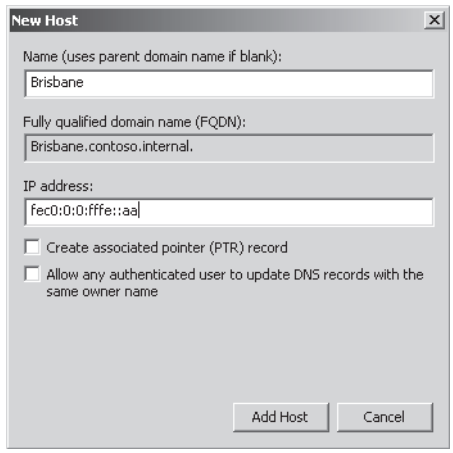

Figura 1-8 Especificação de um registro de New Host DNS.

6. Clique em Add Host. Clique em OK para limpar a caixa de mensagem DNS.
7. Clique em Done. Certifique-se de que o novo registro existe no DNS Manager.
8. Feche o DNS Manager.

Exercício 3: Configuração de uma zona IPv6 de pesquisa inversa

Neste exercício, você criará uma zona IPv6 de pesquisa inversa para todos os endereços IPv6 de site local – isto é, os endereços que começam com fec0. Em seguida, você criará um registro PTR na zona. Observe que, no IPv6, os endereços de zona de pesquisa inversa são inseridos como nibbles de 4 bits em ordem inversa, portanto, fec0 torna-se 0.c.e.f.

1. Se necessário, efetue logon no controlador de domínio com a conta Kim_Akers.
2. Clique em Start, clique com o botão secundário do mouse em Command Prompt e escolha Run As Administrator.
3. Se uma caixa de diálogo UAC aparecer, clique em Continue.
4. Digite **dnscmd glasgow /ZoneAdd 0.c.e.f.ip6.arpa /DsPrimary**. Feche o command Prompt.
5. Em Administrative Tools, abra o DNS Manager. Se uma caixa de diálogo UAC aparecer, clique em Continue.
6. Expanda Forward Lookup Zones. Selecione *contoso.internal*.
7. Clique com o botão secundário do mouse no registro AAAA para Glasgow e escolha Properties.
8. Marque a caixa de seleção Update Associated Pointer (PTR) Record. Clique em OK.
9. Expanda Reverse Lookup Zones e selecione 0.c.e.f.ip6.arpa. Assegure-se de que o registro PTR para Glasgow existe, como mostrado na Figura 1-9.

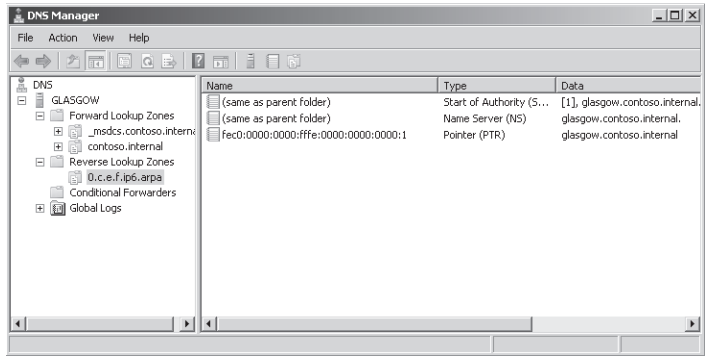

Figura 1-9 O registro PTR para Glasgow no DNS Manager.

10. Efetue logoff do controlador de domínio.

Resumo da lição

- A função DNS Server no Windows Server 2008 R2 atende a todos os padrões atuais e pode funcionar de forma bem-sucedida com a maioria das outras implementações de DNS Server.
- O DNS do Windows Server 2008 R2 é dinâmico e normalmente requer pouquíssima configuração estática. Você pode utilizar a GUI do DNS Manager ou as ferramentas

de linha de comando como *dnscmd*, *nslookup*, *ipconfig* e *netsh* para configurar e gerenciar o DNS.

- As novas funções do DNS do Windows Server 2008 R2 incluem o carregamento de zona em segundo plano, o suporte a RODCs e a zona de DNS GlobalNames. O DNS do Windows Server 2008 R2 dá suporte completo a zonas IPv6 de pesquisa direta e de pesquisa inversa.
- O WINS resolve nomes NetBIOS para endereços IP. O Windows Server 2008 R2 dá suporte ao WINS para fornecer suporte a redes mais antigas. A zona DNS GlobalNames fornece a resolução de nomes de rótulo único para grandes redes corporativas que não utilizam o WINS.

Revisão da lição

As perguntas a seguir têm o objetivo de reforçar as informações-chave apresentadas nesta lição. Elas também estão disponíveis (em inglês) no CD que acompanha o livro, caso você prefira visualizá-las em formato eletrônico.

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

1. Qual topologia do WINS utiliza um projeto distribuído do WINS com múltiplos servidores ou clusters WINS implantados por toda a empresa, com cada servidor ou cluster se replicando com todos os outros servidores ou clusters WINS?
   - **A.** Topologia centralizada do WINS
   - **B.** Topologia full mesh do WINS
   - **C.** Topologia de anel (ring) do WINS
   - **D.** Topologia hub and spoke do WINS
2. Qual registro do DNS permite que você especifique o intervalo de atualização e as configurações de TTL?
   - **A.** SOA
   - **B.** NS
   - **C.** SRV
   - **D.** CNAME
3. Qual comando permite que um servidor DNS dê suporte a zonas GlobalNames?
   - **A.** *dnscmd /createdirectorypartition*
   - **B.** *dnscmd /enlistdirectorypartition*
   - **C.** *dnscmd /config*
   - **D.** *dnscmd /createbuiltindirectorypartitions*