Microsoft

PRODUTOS DE APRENDIZADO MICROSOFT OFICIAL

10221B

Configuração e solução de problemas de uma infraestrutura de rede do Windows Server® 2008

Número do produto: 10221B

Peça número: X17-97174

Lançamento: 12/2011

TERMOS DE LICENÇA DA MICROSOFT

OFFICIAL MICROSOFT LEARNING PRODUCTS – EDIÇÃO DO ALUNO – Versões de pré-lançamento e final

Estes termos de licença são um acordo entre a Microsoft Corporation e você. Por favor, leia-os. Eles se aplicam ao conteúdo licenciado supracitado, que inclui a mídia na qual ele está contido, caso haja uma. Os termos também se aplicam aos seguintes itens da Microsoft:

- atualizações,
- suplementos,
- serviços via Internet e
- serviços de suporte

referentes a este conteúdo licenciado, a menos que outros termos acompanhem esses itens. Nesse caso, tais termos se aplicam.

Ao usar o conteúdo licenciado, você estará aceitando estes termos. Se você não os aceitar, não use o conteúdo licenciado.

Se cumprir estes termos de licença, você terá os direitos a seguir.

1. **VISÃO GERAL.**

   Conteúdo Licenciado. O conteúdo licenciado inclui software, materiais impressos, materiais acadêmicos (online e eletrônicos) e qualquer mídia associada.

   Modelo de Licença. O conteúdo licenciado é licenciado por cópia por dispositivo.

2. **DIREITOS DE INSTALAÇÃO E USO.**

   a. **Dispositivo Licenciado.** O dispositivo licenciado é o dispositivo no qual você usa o conteúdo licenciado. Você poderá instalar e usar uma única cópia do conteúdo licenciado no dispositivo licenciado.

   b. **Dispositivo Portátil.** Você poderá instalar uma outra cópia em um dispositivo portátil para uso pelo único usuário principal do dispositivo licenciado.

   c. **Separação de Componentes.** Os componentes do conteúdo licenciado são licenciados como uma única unidade. Você não poderá separar os componentes e instalá-los em dispositivos diferentes.

   d. **Programas de Terceiros**. O conteúdo licenciado poderá conter programas de terceiros. Estes termos de licença se aplicarão ao uso que você fizer desses programas de terceiros, a menos que outros termos acompanhem esses programas.

3. **VERSÕES DE PRÉ-LANÇAMENTO.** Se o conteúdo licenciado for uma versão de pré-lançamento ("beta"), as seguintes cláusulas serão aplicáveis além de outros termos neste contrato:

   a. **Conteúdo Licenciado de Pré-Lançamento.** Este conteúdo licenciado é uma versão de pré-lançamento. Ele não pode conter as mesmas informações e/ou funcionar da mesma maneira que uma versão definitiva do conteúdo licenciado. Podemos alterá-lo na versão comercial definitiva. Além disso, não podemos lançar uma versão comercial. Você deverá informar o disposto acima de maneira clara e visível a todos os Alunos participantes de uma Sessão de Treinamento Autorizado e a todos os Instrutores que ministrarem treinamento nessas Sessões de Treinamento Autorizado. Além disso, informe que você ou a Microsoft não tem qualquer obrigação de fornecer nenhum outro conteúdo, incluindo, mas sem limitação, a versão lançada em caráter definitivo do Conteúdo Licenciado do Curso.

   b. **Comentários.** Se você concordar em enviar à Microsoft comentários sobre o conteúdo licenciado, estará dando à Microsoft, a título gratuito, o direito de usar, compartilhar e comercializar seus comentários de qualquer maneira e para qualquer finalidade. Além disso, você concede a terceiros, sem custos, todos os direitos de patente necessários para que seus produtos, suas tecnologias e seus serviços usem, ou estabeleçam conexão com, qualquer parte específica de um software, Conteúdo Licenciado ou serviço da Microsoft que inclua os comentários. Você não deverá enviar comentários sujeitos a uma licença que exija da Microsoft o licenciamento do seu software ou da sua documentação a terceiros em virtude da inclusão dos seus comentários nesses elementos. Esses direitos permanecerão em vigor após o término deste contrato.

c. **Informações Confidenciais.** O conteúdo licenciado, incluindo qualquer visualizador, interface de usuário, recursos e documentação que porventura estejam presentes no conteúdo licenciado, é confidencial e de propriedade da Microsoft e de seus fornecedores.

   i. **Uso.** Durante cinco anos após a instalação do conteúdo licenciado ou do seu lançamento comercial, o que ocorrer primeiro, você não poderá divulgar informações confidenciais a terceiros. Você poderá divulgar informações confidenciais apenas aos seus funcionários e consultores que tenham a necessidade de conhecer essas informações. Você deverá firmar contratos por escrito com eles para proteger essas informações confidenciais, pelo menos, de maneira idêntica a este contrato.

   ii. **Continuidade da obrigação.** Seu dever de proteger as informações confidenciais permanecerá após o término deste contrato.

   iii. **Exclusões**. Você poderá divulgar informações confidenciais para atender ordens judiciais ou do Poder Público. Você deverá enviar à Microsoft uma notificação prévia por escrito permitindo que ela busque uma medida cautelar ou de outra forma proteja as informações. Entre as informações confidenciais não estão informações que

   - passem a ser de conhecimento público através de atos lícitos;
   - você tenha recebido de terceiros que não violaram obrigações de sigilo para com a Microsoft ou seus fornecedores; ou
   - você tenha desenvolvido de forma independente.

d. **Prazo.** O prazo deste contrato de versões de pré-lançamento é (i) a data que a Microsoft informar a você como data final de uso da versão beta, ou (ii) o lançamento comercial da versão definitiva do conteúdo licenciado, o que for anterior ("prazo do beta").

e. **Uso.** Você deverá deixar de usar todas as cópias da versão beta na rescisão ou no término dessa versão, bem como destruir todas as cópias dela em seu poder ou sob seu controle.

f. **Cópias.** A Microsoft informará os Centros de Treinamento Autorizados se eles podem produzir cópias da versão beta (seja na versão impressa e/ou em CD) e distribuirá essas cópias aos Alunos e/ou Instrutores. Caso a Microsoft permita essa distribuição, você deverá cumprir todos os termos adicionais que a Microsoft apresentar em relação a essas cópias e à distribuição.

4. **DIREITOS DE USO E/OU REQUISITOS DE LICENCIAMENTO ADICIONAIS.**

a. **Elementos de Mídia e Modelos.** Você poderá usar imagens, clip-arts, animações, sons, músicas, formas, videoclipes e modelos fornecidos com o conteúdo licenciado somente para seu uso em treinamento pessoal. Caso deseje usar esses elementos de mídia ou modelos para qualquer outra finalidade, vá para www.microsoft.com/permission para saber se é permitido.

b. **Materiais Acadêmicos.** Caso o conteúdo licenciado inclua materiais acadêmicos (como White papers, laboratórios, testes, folhas de dados e perguntas freqüentes), você poderá copiar e usar esses materiais. Não é permitido fazer modificações nos materiais acadêmicos nem imprimir livros (eletrônicos ou em versão impressa) integralmente. No caso da reprodução de materiais acadêmicos, você concorda que:

- o uso dos materiais acadêmicos será exclusivamente para sua referência ou treinamento pessoal;
- você não republicará nem postará os materiais acadêmicos em nenhum computador de rede, nem os transmitirá em nenhuma mídia;
- você incluirá o aviso de direitos autorais original dos materiais acadêmicos, ou um aviso de direitos autorais em benefício da Microsoft no formato indicado abaixo:

Formato do Aviso:

c. **Código Distribuível.** O conteúdo licenciado poderá conter código que você tem permissão de distribuir nos programas que desenvolver, respeitados os termos abaixo.

i. **Direito de Uso e Distribuição.** O código e os arquivos de texto listados abaixo constituem "Código Distribuível".

- Arquivos REDIST.TXT. Você poderá copiar e distribuir a forma de código objeto do código listado nos arquivos REDIST.TXT.
- Código de Exemplo. Você poderá modificar, copiar e distribuir a forma de código objeto e código-fonte do código identificado como "exemplo" ("sample").
- Distribuição por Terceiros. Você poderá permitir que os distribuidores de seus programas copiem e distribuam o Código Distribuível como parte desses programas.

ii. **Requisitos de Distribuição.** Para qualquer Código Distribuível que distribua, você deverá:

- adicionar ao Código Distribuível, em seus programas, funcionalidades primárias significativas;
- exigir que os distribuidores e usuários finais externos aceitem termos que protejam o código, pelo menos tanto quanto este contrato;
- exibir o seu aviso de direitos autorais válido em seus programas; e
- indenizar, isentar de responsabilidades e defender a Microsoft de quaisquer reivindicações, incluindo honorários advocatícios, decorrentes da utilização ou distribuição de seus programas.

iii. **Restrições à Distribuição.** É vedado:

- alterar quaisquer avisos de direitos autorais, marcas registradas ou patentes que apareçam no Código Distribuível;
- usar marcas registradas da Microsoft nos nomes de seus programas ou de forma a sugerir que seus programas derivam da Microsoft ou são endossados por ela;
- distribuir Código Distribuível para execução em uma plataforma que não seja Windows;
- incluir Código Distribuível em programas mal-intencionados, enganosos ou ilícitos; ou
- modificar ou distribuir o código-fonte de qualquer Código Distribuível de modo que qualquer parte do mesmo fique sujeita a uma Licença Excluída. Uma Licença Excluída significa qualquer licença que requeira, como condição de uso, modificação ou distribuição, que:
  - o código seja divulgado ou distribuído na forma de código-fonte; ou
  - outras pessoas tenham o direito de modificá-lo.

5. **SERVIÇOS VIA INTERNET.** A Microsoft poderá fornecer serviços via Internet com o conteúdo licenciado. Ela poderá alterá-los ou cancelá-los a qualquer momento. Você não poderá usar esses serviços de maneira que possa danificá-los ou prejudicar seu uso por outros. Em nenhuma hipótese você poderá usar os serviços para tentar obter acesso não autorizado a qualquer serviço, dado, conta ou rede.

6. **ESCOPO DA LICENÇA.** O conteúdo licenciado é licenciado, não vendido. Este contrato apenas outorga a você alguns direitos de uso do conteúdo licenciado. A Microsoft se reserva todos os outros direitos. Salvo quando a legislação aplicável lhe conceder mais direitos do que esta limitação, você só poderá usar o conteúdo licenciado conforme expressamente permitido neste contrato. Ao fazer isso, você deverá cumprir quaisquer limitações técnicas no conteúdo licenciado que permitam o seu uso apenas de determinadas maneiras. É vedado(a):

- a divulgação dos resultados de qualquer teste de desempenho do conteúdo licenciado a terceiros sem o prévio consentimento, por escrito, da Microsoft;
- a resolução de limitações técnicas no conteúdo licenciado;
- a realização de engenharia reversa, descompilação ou desmontagem do conteúdo licenciado, exceto e somente na medida em que esta atividade seja expressamente permitida pela legislação aplicável, não obstante esta limitação;
- a produção de mais cópias do conteúdo licenciado do que aquelas especificadas neste contrato ou permitidas pela legislação aplicável, não obstante esta limitação;
- a publicação do conteúdo licenciado para a cópia por outras pessoas;
- transferir o conteúdo licenciado marcado como "beta" ou "pré-lançamento" a terceiros;
- permitir que outros acessem ou usem o conteúdo licenciado;

- o aluguel, arrendamento ou empréstimo do conteúdo licenciado; ou
- o uso do conteúdo licenciado em serviços de hospedagem comercial de conteúdo licenciado.
- Os direitos de acesso ao software para servidor que possa estar incluído com o conteúdo licenciado, inclusive os Discos Rígidos Virtuais, não concedem a você nenhum direito para implementar patentes da Microsoft ou outras propriedades intelectuais da Microsoft em softwares ou dispositivos que acessem o servidor.

7. **CÓPIA DE BACKUP.** Você poderá fazer uma cópia de backup do conteúdo licenciado. Você poderá usá-la apenas para reinstalar o conteúdo licenciado.
8. **TRANSFERÊNCIA PARA OUTRO DISPOSITIVO.** Você poderá desinstalar o conteúdo licenciado e instalá-lo em outro dispositivo para seu uso pessoal em treinamento. Você não poderá fazer isso para compartilhar esta licença com vários dispositivos.
9. **TRANSFERÊNCIA PARA TERCEIROS.** Você não poderá transferir a terceiros essas versões marcadas como "beta" ou "pré-lançamento". Para as versões definitivas, esses termos serão aplicáveis: O primeiro usuário do conteúdo licenciado poderá transferi-lo junto com este contrato diretamente a um terceiro. Antes da transferência, tal terceiro deverá concordar que este contrato se aplica à transferência e ao uso do conteúdo licenciado. O primeiro usuário deverá desinstalar o conteúdo licenciado antes de transferi-lo separadamente do dispositivo. O primeiro usuário não poderá reter cópias.
10. **RESTRIÇÕES À EXPORTAÇÃO.** O conteúdo licenciado está sujeito às leis e normas de exportação dos Estados Unidos. Você deverá cumprir todas as leis e normas nacionais e internacionais de exportação que se aplicam ao conteúdo licenciado. Essas leis incluem restrições a destinos, usuários finais e uso final. Para obter informações adicionais, visite a página www.microsoft.com/exporting.
11. **SOFTWARE/CONTEÚDO LICENCIADO NÃO COMERCIALIZÁVEL ("NFR" ou "Not For Resale").** É vedada a venda de software ou conteúdo licenciado identificado como "NFR" ou "Not for Resale" ("Não Comercializável").
12. **EDIÇÃO ACADÊMICA.** Você deverá ser um "Usuário Educacional Qualificado" para usar conteúdo licenciado identificado como "Academic Edition" ou "AE". Caso você não saiba se é ou não um Usuário Educacional Qualificado, visite a página www.microsoft.com/education ou contate a afiliada da Microsoft em seu país.
13. **CONTRATO INTEGRAL.** Este contrato, e os termos dos suplementos, das atualizações, dos serviços via Internet e dos serviços de suporte usados por você, constituem o contrato integral para o conteúdo licenciado e os serviços de suporte.
14. **LEGISLAÇÃO APLICÁVEL.**
    a. **Nos Estados Unidos.** Se você tiver adquirido o conteúdo licenciado nos Estados Unidos, as leis do Estado de Washington regerão a interpretação deste contrato e serão aplicáveis às reclamações de violação do mesmo, independentemente dos princípios de conflito de leis. As leis do Estado onde você vive regerão todas as outras reclamações, incluindo leis de defesa do consumidor, concorrência desleal e obrigações extracontratuais.
    b. **Fora dos Estados Unidos.** Se você tiver adquirido o conteúdo licenciado em qualquer outro país, as leis desse país serão aplicáveis.
15. **EFEITO LEGAL.** Este contrato descreve alguns direitos legais. Você poderá ter outros direitos de acordo com as leis do seu país. Você também poderá ter direitos em relação ao terceiro de quem o conteúdo licenciado foi adquirido. Este contrato não alterará os seus direitos de acordo com as leis do seu país, caso as leis do seu país não o permitam.
16. **ISENÇÃO DE RESPONSABILIDADE. O CONTEÚDO LICENCIADO É LICENCIADO "NO ESTADO EM QUE SE ENCONTRA". O RISCO DE USÁ-LO É RESPONSABILIDADE SUA. A MICROSOFT NÃO OFERECE GARANTIAS OU CONDIÇÕES EXPRESSAS. VOCÊ PODERÁ TER DIREITOS DE CONSUMIDOR ADICIONAIS DE ACORDO COM SUAS LEIS LOCAIS, OS QUAIS ESTE CONTRATO NÃO PODERÁ ALTERAR. NA EXTENSÃO PERMITIDA PELAS LEIS LOCAIS, A MICROSOFT EXCLUI AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E NÃO-VIOLAÇÃO.**
17. **LIMITAÇÃO E EXCLUSÃO DE RECURSOS E DANOS. VOCÊ PODE RECUPERAR DA MICROSOFT E DE SEUS FORNECEDORES APENAS DANOS DIRETOS LIMITADOS A US$ 5,00 (CINCO DÓLARES AMERICANOS). NÃO É POSSÍVEL RECUPERAR OUTROS DANOS, INCLUINDO CONSEQÜENCIAIS, LUCROS CESSANTES, ESPECIAIS, INDIRETOS OU INCIDENTAIS.**

    Esta limitação aplica-se a:

    - qualquer assunto relacionado ao conteúdo licenciado, ao software, aos serviços, ao conteúdo (incluindo código) em sites de Internet de terceiros ou a programas de terceiros; e
    - reclamações por violação contratual, quebra de garantia ou condição, responsabilidade objetiva, negligência ou outra responsabilidade extracontratual, na extensão permitida pela legislação aplicável.

    Também será aplicada ainda que a Microsoft saiba ou tivesse que saber sobre a possibilidade dos danos. A limitação ou exclusão acima poderá não se aplicar a você pelo fato de o seu país não permitir a exclusão ou limitação de danos incidentais, conseqüenciais ou outros.

Módulo 1

Planejamento e configuração do IPv4

Conteúdo:

Lição 1

Planejamento de uma infraestrutura de rede IPv4

Conteúdo:

Perguntas e respostas

Planejar um esquema de endereçamento IPv4

Pergunta: qual é o endereço de sub-rede para o seguinte host: 192.168.16.17/28?

Resposta: 192.168.16.16. O número 28 significa que apenas 4 bits de host estão disponíveis. Com quatro bits no octeto significativo para a máscara de sub-rede, a máscara seria 255.255.255.240. 240 rende até a primeira sub-rede de 16, com a próxima sub-rede de 32, 48 e 64. O primeiro host na sub-rede 16 é 17. Assim, 192.168.16.17 é o primeiro host. O último host nessa sub-rede é 30, pois 192.168.16.31 é o endereço de difusão da sub-rede 16.

Discussão: Seleção de um esquema de endereçamento adequado

Pergunta: a Contoso.com implementou o IPv4 em toda a organização. No momento, ela está implementando uma nova matriz. O escritório terá 5.000 computadores que serão distribuídos igualmente entre os 10 andares do escritório. Qual classe de endereço seria adequada nesse cenário?

Resposta: qualquer classe seria adequada com o CIDR; no entanto, uma rede de classe B com uma divisão em sub-redes é a opção mais lógica.

Pergunta: a análise do tráfego da rede na matriz existente mostra que o número máximo de hosts de cada sub-rede deve estar em torno de 100. Quantas sub-redes são necessárias e, supondo um endereço de rede 172.16.0.0/16 para todo o local, qual máscara você deve usar para garantir suporte suficiente às sub-redes necessárias?

Resposta: são necessárias pelo menos 50 sub-redes. Para expressar 50 sub-redes, você precisará de 6 bits na máscara. 2^6 rende 64, enquanto 2^5 provê apenas 32 sub-redes.

Pergunta: supondo que o endereço de rede para a matriz seja 172.16.0.0/19, qual máscara você atribuiria a cada sub-rede?

Resposta: a máscara seria de 25 bits e expressa em decimais como 255.255.255.128.

Pergunta: quantos hosts você pode ter em cada sub-rede com base na máscara selecionada?

Resposta: há 7 bits restantes para os hosts, permitidos para 2^7-2 hosts, o que significa 126. Se a máscara de sub-rede era de 26 bits, apenas 62 hosts eram providos e o requisito é para um máximo de 100. No entanto, uma máscara de 26 bits ofereceria suporte a 128 sub-redes e poderia ser considerada como uma configuração válida.

Pergunta: supondo que você implemente a máscara que definiu para cada sub-rede, qual seria o primeiro endereço de sub-rede?

Resposta: com uma máscara de sub-rede de 6 bits, a máscara decimal real seria 255.255.255.128. A primeira sub-rede seria 172.16.0.0/26. Se você optou por uma máscara de 7 bits então, novamente, a primeira sub-rede seria 172.16.0.0/27, mas a máscara decimal seria 255.255.255.192.

Pergunta: quais são o primeiro e o último endereço de host para a primeira sub-rede?

Resposta. com uma máscara de sub-rede de 6 bits, o primeiro host na primeira sub-rede seria 172.16.0.1/26 e o último host seria 172.16.0.126/26. Usando uma máscara de 7 bits, o primeiro host seria 172.16.0.1/27, enquanto o último host seria 172.16.0.62/27.

Lição 2

Visão geral de serviços de resolução de nomes em uma infraestrutura de rede IPv4

Conteúdo:

Leitura adicional

Resolução de nomes com WINS

- Documentação da Microsoft para a implantação da zona GlobalNames do servidor DNS

Lição 3

Configuração e solução de problemas do IPv4

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como capturar e analisar o tráfego de rede usando o Monitor de Rede

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. Inicie o controlador de domínio e a máquina virtual cliente, mas não inicie o servidor até que seja solicitado.

▶ Capturar tráfego com o Monitor de Rede

1. Alterne para NYC-CL1.
2. Na Área de Trabalho, clique duas vezes em **Monitor de Rede 3.4 da Microsoft**.
3. Na caixa de diálogo **Aceitação do Microsoft Update**, clique em **Não**.
4. No Monitor de Rede 3.4 da Microsoft, no painel **Capturas Recentes**, clique na guia **Nova captura** .
5. Na guia **Captura 1**, na barra de menus, clique em **Iniciar**.
6. Inicie o computador NYC-SVR1
7. No computador host, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciador do Hyper-V**.
8. No Gerenciador do Hyper-V™, clique em **10221B-NYC-SVR1** e, no painel Ações, clique em **Iniciar**.
9. No painel **Ações**, clique em **Conectar**. Espere até que a máquina virtual seja iniciada.
10. Faça logon usando as seguintes credenciais:Nome de usuário: **Administrador**
    - Senha: **Pa$$w0rd**
    - Domínio: **Contoso**
11. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
12. No prompt de comando, digite ping **NYC-DC1** e pressione ENTER.

▶ Analisar o tráfego capturado

1. Alterne para NYC-CL1.
2. No menu do Monitor de Rede 3.4 da Microsoft, clique em **Parar**.
3. Clique no terceiro quadro (ou em qualquer quadro que seja o primeiro quadro ARP) no painel Resumo do Quadro.
4. Clique no painel Detalhes do Quadro e expanda **Ethernet**.
5. Discuta com os alunos o conteúdo do quadro. Mencione os campos **DestinationAddress** e **SourceAddress**.
6. Expanda **Arp**.

7. Identifique o endereço IP solicitado. Que endereço é esse? (Esse é o endereço IP local, ou seja, o endereço IP de NYC-SVR1).

▶ Filtrar o tráfego

1. No painel Filtro de Exibição, clique em **Carregar Filtro**.
2. Clique em **Filtros Padrão**, aponte para **NetBios** e clique em **NetBiosNameQuery**.
3. Na caixa de texto **Filtro de Exibição**, localize a linha de texto **NbtNs.NbtNsQuestionSectionData.QuestionName.Name.contains ("www.server.com")**.
4. Altere **("www.server.com")** para que se leia **("contoso")** e clique em **Aplicar**.
5. Vários quadros devem ser retornados. Examine cada um deles e descreva o conteúdo.

▶ Salvar os dados capturados

1. No menu, clique em **Salvar como**.
2. Clique em **Área de Trabalho** e, na caixa **Nome do arquivo**, digite **Inicialização do NYC-SVR1** e clique em **Salvar**.

Observação Reverta todas as máquinas virtuais a seu estado original para os módulos subsequentes.

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: sua organização pretende usar o IPv4 para suas filiais. É exigido um grande número de hosts e sub-redes. Qual endereço de rede privada você recomendaria?

Resposta: 10.0.0.0/8 ou 172.16.0.0/12.

Pergunta: sua organização tem uma linha de aplicativos de negócios que usa nomes NetBIOS. Um número relativamente baixo de pessoas usa esses aplicativos e você está relutando para implementar o WINS. Que alternativa o Windows Server 2008 fornece?

Resposta: implemente a zona GlobalNames no DNS.

Pergunta: seu cliente Windows 7 não pode ser conectado corretamente a um Windows Server. Você suspeita que seja um problema de resolução de nomes. Quais são os dois utilitários que permitem solucionar problemas de resolução de nomes de um computador cliente?

Resposta: ipconfig.exe e nslookup.exe.

Perguntas e respostas de revisão do laboratório

Pergunta: no laboratório, você usou a interface gráfica para configurar o endereço IPv4 em NYC-CL2. O que mais você poderia ter usado?

Resposta: Netsh

Pergunta: qual sintaxe você teria usado para realizar essa tarefa?

Resposta: Netsh interface ipv4 set address name="Conexão Local" source=static addr=172.16.16.3 mask=255.255.255.0 gateway=172.16.16.1 gwmetric=1.

Módulo 2

Configuração e solução de problemas de DHCP

Conteúdo:

Lição 1

Visão geral da função Servidor DHCP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como adicionar a função Servidor DHCP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Instalar e autorizar a função Servidor DHCP

1. Alterne para o computador NYC-SVR1.
2. Na **Barra de Tarefas**, clique em **Gerenciador de Servidores**.
3. No Gerenciador de Servidores, no painel de navegação, clique em **Funções** e, no painel direito, clique em **Adicionar Funções**.
4. No **Assistente para Adicionar Funções**, clique em **Próximo**.
5. Na página **Selecionar Funções do Servidor**, marque a caixa de seleção **Servidor DHCP** e clique em **Próximo**.
6. Na página **Introdução ao Servidor DHCP**, clique em **Próximo**.
7. Na página **Selecionar Ligações de Conexão de Rede**, clique em **Próximo**.
8. Na página **Especificar Configurações de Servidor DNS IPv4**, clique em **Próximo**.
9. Na página **Especificar Configurações de Servidor WINS IPv4**, clique em **Próximo**.
10. Na página **Adicionar ou Editar Escopos DHCP**, clique em **Próximo**.
11. Na página **Configurar o Modo Sem Monitoração de Estado do DHCPv6**, clique em **Desabilitar o modo sem monitoração de estado do DHCPv6 para este servidor** e, em seguida, clique em **Próximo**.
12. Na página **Autorizar Servidor DHCP**, clique em **Próximo**.
13. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
14. Na página **Resultados da Instalação**, clique em **Fechar** e feche o Gerenciador de Servidores.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

Como o DHCP aloca endereços IP

- Microsoft TechNet: Recursos do DHCP

Como funciona o processo de geração de concessão DHCP

- Microsoft TechNet: Como a tecnologia DHCP funciona

Como funciona o processo de renovação da concessão DHCP

- Microsoft TechNet: Como a tecnologia DHCP funciona

Autorização de Servidor DHCP

- Microsoft TechNet: Recursos do DHCP
- Microsoft TechNet: Coleção de rede

Lição 2

Configuração de escopos DHCP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar escopos DHCP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Criar um escopo IPv4

1. Alterne para o computador NYC-SVR1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DHCP**.
3. Em DHCP, no painel de navegação, expanda **nyc-svr1.contoso.com**, expanda **IPv4**, clique com o botão direito do mouse em **IPv4** e clique em **Novo Escopo**.
4. No **Assistente para Novos Escopos**, clique em **Avançar**.
5. Na página **Nome do Escopo**, na caixa **Nome**, digite **Escopo da matriz 1** e clique em **Avançar**.
6. Na página **Intervalo de Endereços IP**, preencha a página usando as informações a seguir e clique em **Avançar:**
   - Endereço IP inicial: **10.10.0.50**
   - Endereço IP final: **10.10.0.100**
   - Comprimento: **16**
   - Máscara de sub-rede: **255.255.0.0**
7. Na página **Adicionar Exclusões e Atraso**, clique em **Avançar**.
8. Na página **Duração da Concessão**, clique em **Avançar**.
9. Na página **Configurar Opções de DHCP**, clique em **Não, configurarei essas opções mais tarde** e clique em **Avançar**.
10. Na página **Concluindo o Assistente para Novos Escopos**, clique em **Concluir**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

O que são escopos DHCP?

- Microsoft TechNet: Configuração de escopos

O que são superescopos e escopos do multicast?

- Microsoft TechNet: Configuração de escopos

O que é uma reserva DHCP

- Microsoft TechNet: Recursos do DHCP

Dimensionamento e disponibilidade do DHCP

- Technet: Configuração de escopos
- Technet: Práticas recomendadas para o DHCP

Lição 3

Configurando opções DHCP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar opções DHCP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Configurar opções de escopo

1. No console do DHCP, no painel de navegação, expanda **Escopo [10.10.0.0] Escopo da Matriz 1**.
2. Clique em **Opções de Escopo**.
3. Clique com o botão direito do mouse em **Opções de Escopo** e clique em **Configurar Opções**.
4. Na caixa de diálogo **Opções de Escopo**, na lista **Opções Disponíveis**, marque a caixa de seleção **003 Roteador**.
5. Em **Entrada de dados**, na caixa **Endereço IP**, digite **10.10.0.1**, clique em **Adicionar** e em **OK**.

▶ Configurar opções de servidor

1. No painel de navegação, clique em **Opções de Servidor**.
2. Clique com o botão direito do mouse em **Opções de Servidor** e clique em **Configurar Opções**.
3. Na caixa de diálogo **Opções de Servidor**, na lista **Opções Disponíveis**, role para baixo na lista para mostrar as duas opções configuradas e clique na guia **Avançadas**.
4. Na lista **Classe de fornecedor**, clique em **Opções Padrão DHCP** para mostrar as opções disponíveis.
5. Na lista **Classe de usuário**, clique em **Classe de Usuário Padrão** para exibir as opções disponíveis.
6. Clique em **OK**.

▶ Criar uma classe de usuário para opções

1. No painel de navegação, clique com o botão direito do mouse em **IPv4** e clique em **Definir Classes de Usuário**.
2. Na caixa de diálogo **Classes de Usuário DHCP**, clique em **Adicionar**.
3. Na caixa de diálogo **Nova Classe**, na caixa **Nome para exibição**, digite **Laptop**.
4. Na caixa **ID**, digite **ABCD** e clique em **OK**.
5. Na caixa de diálogo **Classes de Usuário DHCP**, clique em **Fechar**.
6. No painel de navegação, clique em **Opções de Servidor**.
7. Clique com o botão direito do mouse em **Opções de Servidor** e clique em **Configurar Opções**.
8. Na caixa de diálogo **Opções de Servidor**, clique na guia **Avançadas**.
9. Na lista **Classe de usuário**, clique em **Laptop**.

10. Na caixa de diálogo **Opções de Servidor**, na lista **Opções Disponíveis**, marque a caixa de seleção **044 Servidores WINS/NBNS**.
11. Em **Entrada de dados**, na caixa **Endereço IP**, digite **10.10.0.10**, clique em **Adicionar** e em **OK**.

▶ Habilitar o escopo e configurar a classe de usuário do computador cliente

1. No painel de navegação, clique com o botão direito do mouse em **Escopo [10.10.0.0] Escopo da Matriz 1** e clique em **Ativar**.
2. Alterne para o computador NYC-CL1.
3. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
4. No prompt de comando, digite **ipconfig /setclassid "Conexão Local" laptop** e pressione ENTER.

Observação A conexão de rede local pode ser chamada de Conexão Local 2 ou até mesmo 3.

5. No prompt de comando, digite **ipconfig /renew** e pressione ENTER.
6. No prompt de comando, digite **ipconfig /all** e pressione ENTER

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

O que são opções DHCP?

- Request for Comments 2132
- Microsoft TechNet: Recursos do DHCP

O que são opções DHCP no nível de classe?

- Microsoft TechNet: Recursos do DHCP
- Microsoft TechNet: Uso de classes de opções

Como são aplicadas as opções DHCP

- Microsoft TechNet: Recursos do DHCP

Lição 4

Gerenciamento de um banco de dados DHCP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como gerenciar um banco de dados DHCP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Examinar o intervalo de backup

1. Alterne para NYC-SVR1.
2. Clique em **Iniciar**, na caixa **Pesquisar**, digite **Regedit.exe** e pressione ENTER.
3. No Editor do Registro, navegue para **HKLM\System\CurrentControlSet\Services\DHCPServer\Parameters**.
4. No painel direito, clique duas vezes em **BackupInterval**.
5. Na caixa de diálogo **Editar Valor DWORD (32 bits)**, clique em **Decimal** e em **Cancelar**.
6. Feche o Editor do Registro.

▶ Fazer backup do banco de dados DHCP

1. Alterne para DHCP.
2. No painel de navegação, clique com o botão direito do mouse em **nyc-svr1.contoso.com** e clique em **Backup**.
3. Na caixa de diálogo **Procurar Pasta**, clique em **OK**.

▶ Reconciliar os dados do escopo

1. Clique com o botão direito do mouse em **Escopo [10.10.0.0] Escopo da Matriz 1** e clique em **Reconciliar**.
2. Na caixa de diálogo **Reconciliar**, clique em **Verificar**.
3. Na caixa de diálogo **DHCP**, clique em **OK**.
4. Na caixa de diálogo **Reconciliar**, clique em **Cancelar.**

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

O que é um banco de dados DHCP

- Microsoft TechNet: Recursos do DHCP

Como são feitos o backup e a restauração de um banco de dados DHCP

- Microsoft TechNet: Backup do banco de dados DHCP

Lição 5

Monitoramento e solução de problemas de DHCP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como monitorar o DHCP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Exibir estatísticas do servidor

1. Em DHCP, no painel de navegação, clique com o botão direito do mouse em **IPv4** e clique em **Exibir Estatísticas**.
2. Na caixa de diálogo **Estatísticas do servidor nyc-svr1.contoso.com**, exiba os dados e clique em **Fechar**.

▶ Exibir os arquivos de log

1. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **c:\windows\system32\dhcp** e pressione ENTER.
2. No Explorer, clique duas vezes no arquivo **DhcpSrvLog-DAY.log**, onde DAY é uma abreviação para o nome do dia de hoje.
3. Examine o log e feche o Bloco de Notas e o Explorer.

▶ Usar o Monitor de Rede para monitorar o DHCP

1. Alterne para NYC-CL1.
2. Na Área de Trabalho, clique duas vezes em **Monitor de Rede 3.4 da Microsoft**.
3. Na caixa de diálogo **Aceitação do Microsoft Update**, clique em **Não**.
4. No Monitor de Rede 3.4 da Microsoft, no painel **Capturas Recentes**, clique na guia **Nova captura** .
5. Na guia **Captura 1**, na barra de menus, clique em **Iniciar.**
6. Clique em **Iniciar**, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
7. No prompt de comando, digite **ipconfig /release** e pressione ENTER.
8. No prompt de comando, digite **ipconfig /renew** e pressione ENTER.
9. No menu do Monitor de Rede 3.4 da Microsoft, clique em **Parar**.
10. Na janela Resumo do Quadro, examine os quadros capturados relacionados ao DHCP.
11. Clique em **Carregar Filtro**, aponte para **Filtros Padrão**, aponte para **Exemplos Básicos** e clique em **Filtro de Protocolo – DNS**.
12. Na caixa de texto **Filtro de Exibição**, localize o texto **DNS** e altere-o para **DHCP**. Clique em **Aplicar**.
13. Agora examine os quadros capturados.
14. Clique duas vezes em cada quadro, expanda e discuta o conteúdo.

Observação Reverta todas as máquinas virtuais.

Leitura adicional

O que é o arquivo de log de auditoria de DHCP?

- Microsoft TechNet: Log de auditoria

Monitoramento do desempenho do servidor DHCP

- Microsoft TechNet: Referência de monitoramento do desempenho do DHCP

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Você tem duas sub-redes em sua organização e deseja usar o DHCP para alocar endereços a computadores cliente em ambas as sub-redes. Você não deseja implantar dois Servidores DHCP. Quais fatores devem ser considerados?

Resposta: o roteador que interconecta as duas sub-redes deve oferecer suporte à retransmissão DHCP ou então você deve colocar um relé na sub-rede que não hospeda o servidor DHCP. Além disso, você deve levar em consideração o impacto na disponibilidade do serviço no caso de falha do seu único servidor DHCP.

Pergunta: Sua organização cresceu e seu escopo IPv4 chegou perto de esgotar os endereços. O que pode ser feito nesse caso?

Resposta: implemente um superescopo combinando o escopo existente com um novo.

Pergunta: Quais informações são necessárias para configurar uma reserva DHCP?

Resposta: o endereço MAC do cliente que fará a concessão da reserva.

Pergunta: É aconselhável configurar a opção 003 - Roteador como uma opção de escopo DHCP no nível de servidor?

Resposta: não. Em um ambiente de vários escopos, todos os clientes obteriam a mesma configuração de gateway. Isso é adequado somente onde todos os clientes estiverem na mesma sub-rede.

Perguntas e respostas de revisão do laboratório

Pergunta: no laboratório, você configurou o roteador com o agente de retransmissão DHCP. O que o agente faz?

Resposta: a retransmissão envia mensagens de difusão DHCP a um servidor DHCP configurado no outro lado do roteador.

Pergunta: no laboratório, você configurou um escopo para os computadores da filial em cada um dos dois servidores DHCP para fornecer tolerância a falhas. O que acontece com os clientes que fazem a renovação quando ambos os servidores DHCP estão indisponíveis?

Resposta: se os clientes não fizerem a renovação, mas a concessão da respectiva configuração IP não tiver expirado, eles poderão continuar usando o respectivo endereço. No entanto, se a concessão tiver expirado, os clientes recorrerão ao uso da configuração APIPA ou IP alternativa (se tiver configurada).

Módulo 3

Configuração e solução de problemas de DNS

Conteúdo:

Lição 1

Instalação da função Servidor DNS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como instalar a função Servidor DNS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**.

▶ Instalar a função Servidor DNS

1. Alterne para NYC-SVR1 e, na **Barra de Tarefas**, clique em **Gerenciador de Servidores**.
2. No Gerenciador de Servidores, no painel de navegação, clique em **Funções** e, no painel direito, clique em **Adicionar Funções.**
3. No **Assistente para Adicionar Funções**, na página **Antes de Começar**, clique em **Próximo**.
4. Na página **Selecionar Funções do Servidor**, na lista **Funções**, marque a caixa de seleção **Servidor DNS** e clique em **Próximo**.
5. Na página **Servidor DNS**, clique em **Próximo**.
6. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
7. Quando a função estiver instalada, clique em **Fechar**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

Visão geral da função Sistema de Nomes de Domínio

- Visão geral de DNS
- Noções básicas de zonas e transferência de zona
- Tópico da Ajuda: Noções básicas sobre a integração dos Serviços de Domínio Active Directory

Melhorias do DNS no Windows Server 2008

- O que há de novo no DNS no Windows Server 2008

Melhorias do DNS no Windows Server 2008 R2

- Novidades do DNS no Windows Server 2008 R2

Considerações para implantar a função Servidor DNS

- Tópico da Ajuda: Planejando Servidores DNS

Lição 2

Configuração da função Servidor DNS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar a função Servidor DNS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Configurar as propriedades do servidor DNS

1. Alterne para NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DNS**.
3. No Gerenciador DNS, expanda **NYC-DC1**, selecione e clique com o botão direito do mouse em **NYC-DC1** e clique em **Propriedades**.
4. Na caixa de diálogo **Propriedades de NYC-DC1**, clique na guia **Encaminhadores**.
5. Na guia **Encaminhadores**, clique em **Editar**. Aqui é possível configurar o encaminhamento. Clique em **Cancelar**.
6. Clique na guia **Avançadas**. Você pode configurar opções, incluindo a proteção do cache contra poluição.
7. Clique na guia **Dicas de Raiz**. Aqui, você pode ver a configuração para os servidores de dicas de raiz.
8. Clique na guia **Log de Depuração** e marque a caixa de seleção **Registrar no log os pacotes para depuração**. Aqui, você pode configurar as opções de registro de depuração.
9. Desmarque a caixa de seleção **Registrar no log os pacotes para depuração** e clique na guia **Log de Eventos**.
10. Clique em **Erros e Avisos** e na guia **Âncoras de Confiança**. Aqui é possível configurar a DNSSEC.
11. Clique na guia **Monitoramento**. Você pode executar testes simples e recursivos no servidor usando a guia **Monitoramento**. Marque a caixa de seleção **Uma consulta simples a este servidor DNS** e clique em **Testar Agora**.
12. Clique na guia **Segurança**. Aqui é possível definir permissões para a infraestrutura DNS. Clique em **OK**.

▶ Configurar encaminhamento condicional

1. No painel de navegação, expanda **Encaminhadores Condicionais**.
2. Clique com o botão direito do mouse em **Encaminhadores Condicionais** e clique em **Novo Encaminhador Condicional**.
3. Na caixa de diálogo **Novo Encaminhador Condicional**, na caixa **Domínio DNS**, digite **nwtraders.msft**.
4. Clique na caixa **<Clique aqui para adicionar um endereço IP ou nome DNS>**. Digite **131.107.1.2** e pressione ENTER. A validação falhará.

5. Clique em **OK**.

▶ Limpar o cache DNS

1. No painel de navegação, clique com o botão direito do mouse em **NYC-DC1** e clique em **Limpar Cache.**

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

Quais são os componentes de uma solução DNS?

- Microsoft TechNet: Definição de DNS
- Microsoft TechNet: Recursos de servidor
- Microsoft TechNet: Recursos de cliente

Registros de recursos DNS

- Tópico da Ajuda: Adicionando registros de recursos

O que é o encaminhamento?

- Microsoft TechNet: Noções básicas sobre encaminhadores
- Tópico da Ajuda: Noções básicas sobre Encaminhadores
- Tópico da Ajuda: Usando encaminhadores

Como funciona o cache do servidor DNS

- Tópico da Ajuda: Instalar um Servidor DNS somente de cache

Lição 3

Configuração de zonas DNS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criar zonas

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Criar uma zona de pesquisa inversa

1. Em NYC-DC1, no painel de navegação do Gerenciador DNS, clique em **Zonas de Pesquisa Inversa**.
2. Clique com o botão direito do mouse em **Zonas de Pesquisa Inversa** e clique em **Nova Zona**.
3. No **Assistente de Nova Zona**, clique em **Avançar**.
4. Na página **Tipo de Zona**, clique em **Zona primária** e em **Avançar**.
5. Na página **Escopo de Replicação de Zona do Active Directory**, clique em **Avançar**.
6. Na página **Nome da Zona de Pesquisa Inversa**, clique em **Zona de Pesquisa Inversa IPv4** e em **Avançar**.
7. Na segunda página **Nome da Zona de Pesquisa Inversa**, na caixa **ID de Rede:** , digite **10.10.0** e clique em **Avançar**.
8. Na página **Atualização Dinâmica**, clique em **Avançar**.
9. Na página **Concluindo o Assistente de Nova Zona**, clique em **Concluir**.

▶ Criar uma zona de pesquisa direta

1. Alterne para NYC-SVR1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DNS**.
3. No painel de navegação do Gerenciador DNS, expanda **NYC-SVR1** e clique em **Zonas de Pesquisa Direta**.
4. Clique com o botão direito do mouse em **Zonas de Pesquisa Direta** e clique em **Nova Zona**.
5. No **Assistente de Nova Zona**, clique em **Avançar**.
6. Na página **Tipo de Zona**, clique em **Zona secundária** e em **Avançar**.
7. Na página **Nome da Zona**, na caixa **Nome da zona:** , digite **Contoso.com** e clique em **Avançar**.
8. Na lista **Servidores Mestres** da página **Servidores DNS Principais**, digite **10.10.0.10** e pressione ENTER.
9. Clique em **Avançar** e, na página **Concluindo o Assistente de Nova Zona**, clique em **Concluir**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

O que é uma zona DNS?

- Tópico da Ajuda: Planejando zonas DNS
- Microsoft TechNet: Noções básicas de zonas e transferência de zona

Quais são os tipos de zona DNS?

- Tópico da Ajuda: Noções básicas sobre tipos de zona

O que são zonas de pesquisa direta e inversa?

- Tópico da Ajuda: Noções básicas sobre tipos de zona

O que são zonas de stub?

- Tópico da Ajuda: Noções básicas sobre tipos de zona

Delegação de zonas DNS

- Microsoft TechNet: Delegação de zonas

Lição 4

Configuração de transferências de zona DNS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar transferências de zona DNS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Habilitar transferências de zona DNS

1. Alterne para NYC-DC1.
2. No painel de navegação do Gerenciador DNS, expanda **Zonas de Pesquisa Direta**.
3. Clique com o botão direito do mouse em **Contoso.com** e clique em **Propriedades**.
4. Na caixa de diálogo **Propriedades de Contoso.com**, clique na guia **Transferências de Zona**.
5. Marque a caixa de seleção **Permitir transferências de zona** e clique em **Apenas para servidores listados** na guia **Servidores de Nomes**.
6. Clique em **Notificar** e, na caixa de diálogo **Notificar**, clique em **Servidores listados na guia Servidores de Nomes**. Clique em **OK**.
7. Clique na guia **Servidores de Nomes** e em **Adicionar**.
8. Na caixa de diálogo **Novo Registro de Nome do Servidor**, na caixa **FQDN (nome de domínio totalmente qualificado) do Servidor**, digite **NYC-SVR1.Contoso.com** e clique em **Resolver**. Clique em **OK**.
9. Na caixa de diálogo **Propriedades de Contoso.com**, clique em **OK**.

▶ Atualizar a zona secundária do servidor mestre

1. Alterne para NYC-SVR1.
2. No painel de navegação do Gerenciador DNS, expanda **Zonas de Pesquisa Direta**.
3. Pressione F5 para atualizar a exibição; clique com o botão direito do mouse em **Contoso.com** e clique em **Transferir do Principal**.

Observação Talvez seja preciso repetir a etapa 3 várias vezes antes das transferências de zona. Observe também que a transferência pode ocorrer automaticamente antes que essas etapas sejam executadas manualmente.

▶ Atualizar a zona primária e verificar a alteração na zona secundária

1. Alterne para NYC-DC1.
2. No Gerenciador DNS, clique com o botão direito do mouse em Contoso.com e clique em Novo Alias (CNAME).
3. Na caixa **Nome do alias (usa o domínio pai se deixado em branco)** da caixa de diálogo **Novo Registro de Recursos**, digite **intranet**.

4. Na caixa **Nome de domínio totalmente qualificado (FQDN) para o host de destino**, digite **nyc-dc1.contoso.com** e clique em **OK**.
5. Alterne para NYC-SVR1.
6. No Gerenciador DNS, clique com o botão direito do mouse em **Contoso.com** e clique em **Transferir do Principal**.

Observação O registro pode demorar um pouco para aparecer. Talvez seja preciso pressionar F5 para atualizar a exibição.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

O que é uma transferência de zona DNS?

- Microsoft TechNet: Noções básicas de zonas e transferência de zona

Lição 5

Gerenciamento e solução de problemas de DNS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como gerenciar registros DNS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Configurar o TTL

1. Alterne para NYC-DC1.
2. No Gerenciador DNS, clique com o botão direito do mouse em **Contoso.com** e clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades de Contoso.com**, clique na guia **Início de Autoridade (SOA)**.
4. Na caixa **Tempo de Vida Mínimo (padrão)**, digite **2** e clique em **OK**.

▶ Habilitar e configurar a eliminação

1. Clique com o botão direito do mouse em **NYC-DC1** e clique em **Definir Duração/Eliminação para Todas as Zonas**.
2. Na caixa de diálogo **Definir Propriedades de Duração/Eliminação**, marque a caixa de seleção **Eliminar registros de recursos obsoletos** e clique em **OK**.
3. Na caixa de diálogo **Confirmação de Eliminação/Duração de Servidor**, marque a caixa de seleção **Aplicar configurações às zonas existentes integradas ao Active Directory** e clique em **OK**.

Observação Deixe todas as máquinas virtuais em seu estado atual para a demonstração subsequente.

Demonstração: Como testar a configuração do servidor DNS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Capturar o tráfego de rede do DNS

1. Alterne para NYC-CL1.
2. Na Área de Trabalho, clique duas vezes em **Monitor de Rede 3.4 da Microsoft**.
3. Na caixa de diálogo **Aceitação do Microsoft Update**, clique em **Não**.

4. No Monitor de Rede 3.4 da Microsoft, no painel **Capturas Recentes**, clique na guia **Nova captura**.
5. Na guia **Captura 1**, na barra de menus, clique em **Iniciar.**
6. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
7. No prompt de comando, digite **ipconfig /flushdns** e pressione ENTER.
8. No prompt de comando, digite **ping intranet** e pressione ENTER.
9. No prompt de comando, digite **ipconfig /displaydns** e pressione ENTER.
10. No menu do Monitor de Rede 3.4 da Microsoft, clique em **Parar**.

▶ Filtrar e analisar o tráfego capturado

1. Na janela **Resumo do Quadro**, examine os quadros capturados relacionados ao DNS.
2. Clique em **Carregar Filtro**, aponte para **Filtros Padrão**, para **DNS** e clique em **DnsAllNameQuery**.
3. Clique em **Aplicar**.
4. Agora examine os quadros capturados.
5. Clique duas vezes em cada quadro, expanda e discuta o conteúdo.

▶ Usar o NSLookup.exe para testar o DNS

1. No prompt de comando, digite **nslookup –d2 nyc-svr1.contoso.com. > file.txt** e pressione ENTER.
2. No prompt de comando, digite **notepad file.txt** e pressione ENTER.

Observação Reverta todas as máquinas virtuais.

Leitura adicional

O que é Vida Útil, Duração e Eliminação?

- Microsoft TechNet: Usar Duração e Eliminação

Ferramentas que identificam problemas no DNS

- Centro de ajuda e suporte da Microsoft: Descrição do utilitário DNSLint
- Tópico da Ajuda: Solucionando problemas de servidores DNS
- Microsoft TechNet: Solução de problemas de DNS

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Você está apresentando a um cliente potencial as vantagens de usar o Windows Server 2008 R2. Quais são os novos recursos que você destacaria ao discutir a função Servidor DNS do Windows Server 2008 R2?

Resposta: Carregamento de Zona em Segundo Plano, Suporte para IPv6, Suporte para Controladores de Domínio Somente Leitura e Nomes globais únicos.

Pergunta: você está implantando servidores DNS em um domínio Active Directory e seu cliente exige que a infraestrutura seja resistente a pontos isolados de falha. O que você deve considerar ao planejar a configuração do DNS?

Resposta: você deve garantir a implantação de mais de um controlador de domínio DNS na rede.

Pergunta: qual é a diferença entre consultas recursivas e iterativas?

Resposta: um cliente emite uma consulta recursiva para um servidor DNS. Só há duas respostas possíveis: 1) o endereço IP do domínio solicitado ou 2) host não encontrado. Uma consulta iterativa resolve os endereços IP através do namespace hierárquico DNS. Uma consulta iterativa retorna uma resposta autoritativa ou o endereço IP de um servidor no próximo nível abaixo na hierarquia do DNS.

Pergunta: o que deve ser configurado para que uma zona DNS seja transferida para um servidor DNS secundário?

Resposta: você deve configurar as transferências de zona DNS de modo a permitir que o servidor da zona secundária faça a transferência da zona primária.

Pergunta: você é o administrador de um ambiente DNS do Windows Server 2008 R2. Sua empresa adquiriu outra empresa recentemente. Você quer replicar as respectivas zonas primárias DNS. A empresa adquirida está usando o Bind 4.9.4 para hospedar suas zonas primárias DNS. Você observa um volume considerável de tráfego entre o servidor DNS do Windows Server 2008 R2 e o servidor Bind. Cite um motivo possível para essa ocorrência.

Resposta: o Bind 4.9.4 não oferece suporte ao IXFR. Sempre que ocorre uma mudança na zona Bind, ele precisa replicar a zona inteira em um computador que executa o Windows Server 2008 R2 para manter a atualização.

Pergunta: você deve automatizar o processo de configuração de um servidor DNS para automatizar a implantação do Windows Server 2008 R2. Qual ferramenta do DNS pode ser usada para realizar essa tarefa?

Resposta: você pode utilizar o dnscmd.exe.

Perguntas e respostas de revisão do laboratório

Pergunta: no laboratório, você teve que implantar uma zona secundária, pois nenhum controlador de domínio adicional deveria ser implantado. Se essa condição mudasse, isto é, NYC-SVR1 fosse um controlador de domínio, como isso alteraria seu plano de implementação?

Resposta: Você poderia instalar o AD DS e as funções DNS e não seria preciso configurar nenhuma zona nem transferências de zona.

Módulo 4

Configuração e solução de problemas de TCP/IP IPv6

Conteúdo:

Lição 2

Endereçamento IPv6

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar as definições do cliente IPv6

Etapas da demonstração

Observação: você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como Contoso\Administrator usando a senha Pa$$w0rd.

▶ Configurar um escopo DHCP para clientes IPv6

1. Alterne para NYC-DC1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **central de rede e compartilhamento** e pressione ENTER.
3. Na Central de Rede e Compartilhamento, clique em **Alterar as configurações do adaptador**.
4. Em Conexões de Rede, clique com o botão direito do mouse em **Conexão Local 3** e clique em **Propriedades**.
5. Na caixa de diálogo **Propriedades de Conexão Local 3**, clique duas vezes em **Protocolo TCP/IPv6.**
6. Na caixa de diálogo **Propriedades de Protocolo TCP/IPv6**, clique em **Usar o seguinte endereço IPv6**.
7. Na caixa **Endereço IPv6**, digite **2001:db8:0:1:1a81:f438:3222:e1a2**.
8. Na caixa **Comprimento do prefixo da sub-rede**, digite **64**.
9. Na caixa **Servidor DNS Preferencial**, digite **::1** e clique em **OK**.
10. Na caixa de diálogo **Propriedades de Conexão Local 3**, clique em **OK**.
11. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DHCP**.
12. No painel de navegação do DHCP, expanda **NYC-DC1.Contoso.com** e clique em **IPv6**.
13. Clique com o botão direito do mouse em **IPv6** e clique em **Novo Escopo**.
14. No **Assistente para Novos Escopos**, clique em **Avançar**.
15. Na caixa **Nome** da página **Nome do Escopo**, digite **Escopo IPv6 da Contoso** e clique em **Avançar**.
16. Na caixa **Prefixo** da página **Prefixo do Escopo**, digite **2001:db8:0:1::** e clique em **Avançar**.
17. Na página **Adicionar Exclusões**, clique em **Avançar**.
18. Na página **Concessão de Escopo**, clique em **Avançar**.
19. Na página **Concluindo o Assistente para Novos Escopos**, clique em **Concluir**.
20. No painel de navegação, clique em **Opções de Servidor** e clique duas vezes em **00023 Lista de Endereços IPv6 do Servidor de Nomes DNS Recursivo**.
21. Na caixa de diálogo **Opções de Servidor**, clique duas vezes em **Remover**.
22. Na caixa **Novo endereço IPv6**, digite **2001:db8:0:1:1a81:f438:3222:e1a2**, clique em **Adicionar** e em **OK**.

▶ Configurar o computador cliente

1. Alterne para NYC-CL1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **central de rede e compartilhamento** e pressione ENTER.
3. Na Central de Rede e Compartilhamento, clique em **Alterar as configurações do adaptador**.
4. Em Conexões de Rede, clique com o botão direito do mouse em **Conexão Local 4** e clique em **Propriedades**.
5. Na caixa de diálogo **Propriedades de Conexão Local 4**, desmarque a caixa de seleção **Protocolo TCP/IPv4** e clique em **OK**.
6. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
7. No prompt de comando, digite **ipconfig.exe** e pressione ENTER.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

Configuração automática de endereço para o IPv6

- Introdução ao IP Versão 6

Lição 3

Coexistência com o IPv6

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar o DNS para oferecer suporte ao IPv6

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. Esses dois computadores já estão em execução.

▶ Configurar as associações para o serviço DNS

1. Alterne para NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DNS**.
3. No Gerenciador DNS, clique com o botão direito do mouse em **NYC-DC1** e clique em **Propriedades**.
4. Na guia **Interfaces**, verifique se a caixa de seleção **2001:db8:0:1:1a81:f438:3222:e1a2** está marcada e clique em **OK**.

▶ Verificar a presença de registros AAAA em Contoso.com

1. No painel de navegação do Gerenciador DNS, expanda **NYC-DC1**, expanda **Zonas de Pesquisa Direta** e clique em **Contoso.com**.
2. Observe que há vários registros de host AAAA. Feche o Gerenciador DNS.

Observação Reverta todas as máquinas virtuais.

Leitura adicional

Quais são os tipos de nó?

- Introdução ao IP Versão 6

Coexistência entre o IPv4 e o IPv6

- Tecnologias de transição do IPv6

Lição 4

Tecnologias de transição do IPv6

Conteúdo:

Leitura adicional

O que é Teredo?

- Tecnologias de transição do IPv6

O que é proxy de porta?

- Tecnologias de transição do IPv6

Lição 5

Transição do IPv4 para o IPv6

Conteúdo:

Leitura adicional

Discussão: Considerações sobre a migração do IPv4 para o IPv6

- Tecnologias de transição do IPv6

Processo de transição somente para o IPv6

- Tecnologias de transição do IPv6

Solução de problemas do IPv6

- The Cable Guy - março de 2005

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Quais são os diferentes tipos de endereços unicast IPv6?

Resposta: os diferentes tipos são de link-local, de site-local, exclusivamente local e global.

Pergunta: quais são os principais motivos pelos quais o IPv6 é necessário?

Resposta: ele é necessário devido ao esgotamento do espaço de endereços IPv4 e porque oferece endereçamento de roteadores mais gerenciável e integração de segurança mais eficiente.

Pergunta: qual é o processo chamado quando um cliente configura a si próprio com um endereço IPv6?

Resposta: configuração automática.

Pergunta: que tipo de endereço IP todo cliente IPv6 atribui automaticamente a si próprio?

Resposta: um endereço IP de link-local.

Pergunta: de que modo o escopo de um endereço afeta sua capacidade de se comunicar em uma sub-rede conectada localmente?

Resposta: o escopo limita as redes através das quais um pacote pode ser roteado. Um pacote de dados enviado sob o escopo de link-local não pode ser encaminhado além da sub-rede de link-local por um roteador IPv4. Da mesma forma, um pacote de site-local não será encaminhado além das sub-redes de site-local definidas para um site específico. Somente os endereços globais IPv6 podem ser usados para transmitir na Internet pública. As tecnologias de túnel são ISATAP, 6to4 e Teredo.

Pergunta: qual é a principal finalidade de um túnel Teredo?

Resposta: um túnel Teredo permite que o IPv6 se comunique através de NATs IPv4.

Perguntas e respostas de revisão do laboratório

Pergunta: O que um roteador ISATAP permite que um nó híbrido IPv6/IPv4 faça?

Resposta: ele permite que o nó híbrido se comunique com outras interfaces IPv6. Ele também permite que os hosts IPv6 se comuniquem com outras redes IPv6 através de uma sub-rede IPv4.

Pergunta: o que você precisa definir no servidor DNS para que um roteador ISATAP funcione corretamente?

Resposta: você precisa definir um registro A DNS ou um registro do host, chamado ISATAP, e depois apontá-lo para o endereço IPv4 do roteador ISATAP. Isso permite que os hosts detectem o roteador ISATAP na rede IPv4.

Pergunta: O que faz um anúncio de prefixo quando você está definindo um prefixo no roteador IPv6?

Resposta: permite que os clientes reconheçam os prefixos entre os quais o roteador transitará. Ele também permite que os clientes configurem a si próprios com o prefixo adequado.

Pergunta: por que é necessário desabilitar o roteador ISATAP ao fazer a transição para o IPv6?

Resposta: o roteador ISATAP só é necessário para a comunicação através de sub-redes IPv4.

Módulo 5

Configuração e solução de problemas de Roteamento e Acesso Remoto

Conteúdo:

Lição 2

Configuração do acesso à VPN

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar o acesso à VPN

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-EDGE1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon em 10221B-NYC-DC1 e 10221B-NYC-EDGE1 como **Contoso\Administrator** com a senha **Pa$$w0rd**. Não faça logon em 10221B-NYC-DC1 até ser direcionado.

▶ Configurar as definições de discagem do usuário

1. Alterne para a máquina virtual NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas**, clique em **Usuários do Active Directory** e em **Computadores**.
3. No painel de navegação, expanda **Contoso.com** e clique em **Marketing**.
4. No painel de resultados, clique duas vezes em **Adam Carter**.
5. Na caixa de diálogo **Propriedades de Adam Carter**, clique na guia **Discagem**.
6. Observe que a Permissão de Acesso à Rede é padronizada para Controlar acesso por meio da Diretiva de Rede do NPS. Clique em **OK**.
7. Clique duas vezes em **Marketing** e clique na guia **Membros**.
8. Observe que Adam Carter é um membro do grupo. Clique em **OK**.
9. Feche Usuários e Computadores do Active Directory.

▶ Configurar o Roteamento e Acesso Remoto como um servidor VPN

1. Em NYC-EDGE1, clique em **Iniciar** e em **Ferramentas Administrativas**.
2. No menu **Ferramentas Administrativas**, clique em **Gerenciador de Servidores**. O Gerenciador de Servidores será aberto.
3. No painel da lista **Gerenciador de Servidores (NYC-EDGE1)**, clique com o botão direito do mouse em **Funções** e clique em **Adicionar Funções** no menu de contexto. O Assistente para Adicionar Funções será exibido. Clique em **Próximo**.
4. Na página **Selecionar Funções do Servidor**, selecione **Serviços de Acesso e Diretiva de Rede** e clique em **Próximo**.
5. Na página de introdução dos **Serviços de Acesso e Diretiva de Rede**, clique em **Próximo**.
6. Na página **Selecionar Serviços de Função**, marque as caixas de seleção **Servidor de Diretiva de Rede** e **Serviços de Roteamento e Acesso Remoto** e clique em **Próximo**.
7. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
8. Na página **Resultados da Instalação**, verifique se **Instalação bem-sucedida** aparece no painel de detalhes e clique em **Fechar**.
9. Feche o Gerenciador de Servidores. As funções Serviços de Roteamento e Acesso Remoto e Diretiva de Rede são instaladas em 10221B-NYC-EDGE1.

10. Em NYC-EDGE1, clique em **Iniciar** e em **Ferramentas Administrativas**.
11. No menu **Ferramentas Administrativas**, clique em **Roteamento e Acesso Remoto**. Será exibida a ferramenta administrativa Roteamento e Acesso Remoto.
12. No painel de lista, selecione e clique com o botão direito do mouse em **NYC-EDGE1 (local)** e clique em **Configurar e Habilitar Roteamento e Acesso Remoto**.
13. Clique em **Avançar** na página **Bem-vindo** do assistente.
14. Na página **Configuração**, deixe o padrão **Acesso Remoto (Dial-up ou Rede Virtual Privada)** selecionado e clique em **Avançar**.
15. Na página **Acesso Remoto**, marque a caixa de seleção **VPN** e clique em **Avançar**.
16. Na página **Conexão VPN**, selecione a interface **Pública** e clique em **Avançar**.
17. Na página **Atribuição de Endereço IP**, selecione **De um intervalo de endereços especificado** e clique em **Avançar**.
18. Na página **Atribuição de Intervalo de Endereços**, clique em **Novo** e, na caixa **Endereço IP inicial**, digite o valor **10.10.0.60**. Na caixa **Número de endereços**, digite o valor **25** e clique em **OK**. Clique em **Avançar**.
19. Na página **Gerenciando Múltiplos Servidores de Acesso Remoto**, deixe a seleção padrão **Não, usar o Roteamento e Acesso Remoto para autenticar solicitações de conexão** e clique em **Avançar**. Clique em **Concluir**.
20. Na caixa de diálogo **Roteamento e Acesso Remoto**, clique em **OK**.
21. Na caixa de diálogo Roteamento e Acesso Remoto relativa ao agente de retransmissão DHCP, clique em **OK**. Será iniciado o Serviço Roteamento e Acesso Remoto. Feche o console de Roteamento e Acesso Remoto.
22. Em NYC-EDGE1, clique em **Iniciar** e em **Ferramentas Administrativas**.
23. No menu Ferramentas Administrativas, clique em **Servidor de Diretivas de Rede**. A ferramenta administrativa Servidor de Diretiva de Rede é exibida.
24. No painel de lista, expanda **Diretivas** e clique em **Diretivas de Rede**.
25. Clique com o botão direito do mouse na diretiva **Conexões com o servidor de Roteamento e Acesso Remoto da Microsoft** e clique em **Desabilitar**.
26. Repita para todas as diretivas restantes.

▶ Configurar um cliente VPN

1. Alterne para o computador NYC-CL1 e faça logon como **Contoso\Adam** com a senha **Pa$$w0rd**.
2. Clique em **Iniciar** e em **Painel de Controle**.
3. Na janela Painel de Controle, em Rede e Internet, clique em **Exibir o status e as tarefas da rede**.
4. Na janela **Central de Rede e Compartilhamento**, clique em **Alterar as configurações do adaptador**.
5. Clique com o botão direito do mouse em **Conexão Local 4** e clique em **Propriedades**. Na caixa de diálogo Controle de Conta de Usuário, digite Administrator com a senha **Pa$$w0rd**.
6. Selecione **Protocolo TCP/IP Versão 4 (TCP/IPv4)** e clique em **Propriedades**.

7. Configure as definições de endereço IP a seguir e clique em **OK**:
   - Endereço IP: **131.107.0.20**
   - Máscara de sub-rede: **255.255.255.0**
   - Gateway padrão: **131.107.0.1**
8. Clique em Fechar e no botão **Voltar** para retornar à Central de Rede e Compartilhamento.
9. Na janela Central de Rede e Compartilhamento, em **Alterar as configurações de rede**, clique em **Configurar uma nova conexão ou rede**. Na caixa de diálogo **Escolher uma opção de conexão**, clique em **Conectar-se a um local de trabalho** e em **Avançar**.
10. Na caixa de diálogo **Conectar a um local de trabalho**, selecione a opção **Usar minha conexão com a Internet (VPN)**. Quando solicitado, selecione **Configurarei minha conexão com a Internet mais tarde**.
11. Na caixa de diálogo Digite o **endereço da Internet com o qual se conectar**, especifique o endereço da Internet **131.107.0.2** e o Nome de Destino **SC** e clique em **Avançar**.
12. Na página **Digite o seu nome de usuário e a senha**, deixe o número de usuário e a senha em branco e clique em Criar.
13. Clique em **Fechar** na caixa de diálogo **Conectar a um Local de Trabalho**.
14. Na janela **Central de Rede e Compartilhamento**, clique em **Alterar as configurações do adaptador**.
15. Na página **Conexões de Rede**, clique com o botão direito do mouse em **SC** e clique em **Conectar**.
16. Use as informações a seguir nas caixas de texto **Conectar SC** e clique em **Conectar**:
    - Nome de usuário: **Adam**
    - Senha: **Pa$$w0rd**
    - Domínio: **Contoso**

    A VPN não conecta porque não existe nenhuma política correspondente.
17. Clique em **Fechar**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 3

Visão geral das diretivas de rede

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criar uma diretiva de rede

Etapas da demonstração

Observação Você deve ter concluído a demonstração anterior e todas as máquinas virtuais ainda devem estar em execução e no estado exato em que estavam no fim da demonstração anterior.

▶ Criar uma política de VPN com base na condição dos Grupos do Windows

1. Em NYC-EDGE1, alterne para o console do Servidor de Diretivas de Rede.
2. No painel de lista, expanda **Diretivas**, clique com o botão direito do mouse em **Diretivas de Rede** e clique em **Novo**.
3. Na página **Nova Diretiva de Rede – Especificar Nome da Diretiva de Rede e Tipo de Conexão,** digite **VPN** na caixa de texto **Nome da Diretiva** e, na lista suspensa **Tipo de servidor de acesso à rede**, clique em **Servidor de Acesso Remoto (VPN-Dial up)** e clique em **Avançar**.
4. Na página **Especificar Condições**, clique em **Adicionar**. Na caixa de diálogo **Selecionar Condição**, role para baixo e clique duas vezes em **Grupos do Windows**.
5. Clique em **Adicionar Grupos** e, na caixa **Digite o nome do objeto a ser selecionado**, digite **Marketing**, clique em **Verificar Nomes**, em **OK** duas vezes e em **Avançar**.
6. Na página **Especificar Permissão de Acesso**, mantenha o padrão de **Acesso concedido** e clique em **Avançar**.
7. Na página **Configurar Métodos de Autenticação**, clique em **Avançar**.
8. Na página **Configurar Restrições**, no painel direito de **Restrições**, marque a caixa de seleção **Desconectar após tempo ocioso máximo** e clique em **Avançar**.
9. Na caixa de diálogo **Definir Configurações**, clique em **Avançar** e em **Concluir**.
10. No painel de lista da ferramenta Servidor de Diretivas de Rede, clique no nó **Diretivas de Rede**.
11. Feche a ferramenta Servidor de Diretivas de Rede.

▶ Testar a VPN

1. Em NYC-CL1, clique com o botão direito do mouse em SC e clique em Conectar.
2. Use as informações a seguir nas caixas de texto **Conectar SC** e clique em **Conectar**:
   - Nome de usuário: **Adam**
   - Senha: **Pa$$w0rd**
   - Domínio: **Contoso**

   A VPN conecta.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 4

Visão geral do Kit de Administração do Gerenciador de Conexões

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Etapas de demonstração de como criar um perfil de conexão

Observação Você deve ter concluído a demonstração anterior e todas as máquinas virtuais ainda devem estar em execução e no estado exato em que estavam no fim da demonstração anterior.

▶ Instalar o recurso CMAK

1. Alterne para o computador NYC-DC1.
2. Na **Barra de Tarefas**, clique em **Gerenciador de Servidores**.
3. No painel de navegação do Gerenciador de Servidores, clique em **Recursos**.
4. No painel direito, clique em **Adicionar Recursos**.
5. No **Assistente para Adicionar Recursos**, na página **Selecionar Recursos**, marque a caixa de seleção **Kit de Administração do Gerenciador de Conexões** e clique em **Avançar**.
6. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
7. Na página **Resultados da Instalação**, clique em **Fechar**.
8. Feche o Gerenciador de Servidores.

▶ Criar um perfil de conexão

1. Em NYC-DC1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Kit de Administração do Gerenciador de Conexões**.
2. No Assistente do Kit de Administração do Gerenciador de Conexões, clique em **Avançar**.
3. Na página **Selecionar o Sistema Operacional de Destino**, clique em **Windows 7 ou Windows Vista** e clique em **Avançar**.
4. Na página **Criar ou Modificar um perfil do Gerenciador de Conexões**, clique em **Novo Perfil** e clique em **Avançar**.
5. Na página **Especificar o Nome do Serviço e o Nome do Arquivo**, na caixa **Nome do serviço**, digite **SC da Contoso**, na caixa **Nome do arquivo**, digite **Contoso** e clique em **Avançar**.
6. Na página **Especificar um Nome de Realm**, clique em **Não adicionar um nome de realm ao nome de usuário** e clique em **Avançar**.
7. Na página **Mesclar Informações de Outros Perfis**, clique em **Avançar**.
8. Na página **Adicionar Suporte a Conexões VPN**, marque a caixa de seleção **Catálogo telefônico deste perfil**.
9. Na caixa **Nome ou endereço IP do servidor VPN**, digite **131.107.0.2** e clique em **Avançar**.
10. Na página **Criar ou Modificar uma Entrada VPN**, clique em **Avançar**.
11. Na página **Adicionar um Catálogo Telefônico Personalizado**, desmarque a caixa de seleção **Download automático de atualizações do catálogo telefônico** e clique em **Avançar**.

12. Na página **Configurar Entradas de Sistema de Rede Dial-up**, clique em **Avançar**.
13. Na página **Especificar as Atualizações das Tabelas de Roteamento**, clique em **Avançar**.
14. Na página **Configurar Definições de Proxy do Internet Explorer**, clique em **Avançar**.
15. Na página **Adicionar Ações Personalizadas**, clique em **Avançar**.
16. Na página **Exibir um Bitmap de Logon Personalizado**, clique em **Avançar**.
17. Na página **Exibir um Bitmap de Catálogo Telefônico Personalizado**, clique em **Avançar**.
18. Na página **Exibir Ícones Personalizados**, clique em **Avançar**.
19. Na página **Incluir um Arquivo de Ajuda Personalizado**, clique em **Avançar**.
20. Na página **Exibir Informações de Suporte Personalizadas**, clique em **Avançar**.
21. Na página **Exibir um Contrato de Licença Personalizado**, clique em **Avançar**.
22. Na página **Instalar Arquivos Adicionais com o Perfil do Gerenciador de Conexões**, clique em **Avançar**.
23. Na página **Criar o Perfil e o Programa de Instalação do Gerenciador de Conexões**, clique em **Avançar**.
24. Na página **O Perfil do Gerenciador de Conexões foi Concluído e Está Pronto para ser Distribuído**, clique em **Concluir**.

▶ Examinar o perfil

1. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **C:\Arquivos de Programas\CMAK\Profiles\Windows 7 and Windows Vista\Contoso** e pressione ENTER.
2. Verifique se você pode ver o arquivo executável que foi criado para o perfil.

Observação O perfil que você criou é para edições de 64 bits do Windows 7. A máquina virtual do cliente é de 32 bits.

Observação Reverta todas as máquinas virtuais.

Lição 6

Configuração do DirectAccess

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como instalar e configurar o DirectAccess

Etapas da demonstração

Esta demonstração mostra como:

- Configurar o DNS e o controlador de domínio do AD DS
- Configurar o ambiente da PKI
- Configurar os clientes DirectAccess e testar o acesso à intranet e Internet
- Configurar o servidor DirectAccess
- Verificar a funcionalidade do DirectAccess

Observação Para observar como executar essas tarefas, baixe e extraia o arquivo de conteúdo complementar 10221B-ENU-Companion.zip no site http://www.microsoft.com/learning /en/us/training/companionmoc.aspx e exiba os seguintes arquivos de mídia:
10221B_DirectAccessDemo_Task1.WMV
10221B_DirectAccessDemo_Task2.WMV
10221B_DirectAccessDemo_Task3.WMV
10221B_DirectAccessDemo_Task4.WMV
10221B_DirectAccessDemo_Task5.WMV

Para exibir a transcrição para a demonstração, consulte 10221B_DirectAccessDemo_Transcript_and_Steps.PDF.

Revisões e informações complementares do módulo

Perguntas de revisão

1. Sua organização deseja implementar uma solução econômica que interconecte duas filiais com suas matrizes. De que maneira as VPNs teriam uma função nesse cenário?

Resposta: você poderia implementar VPNs em uma configuração site a site pela Internet para fornecer os recursos de roteamento necessários.

2. O gerente de TI na sua organização está preocupado em abrir muitas portas de firewall para facilitar o acesso remoto de usuários que estão trabalhando de casa por uma VPN. Como você pode atender às expectativas dos usuários remotos enquanto tranquiliza as preocupações do gerente?

Resposta: implemente o SSTP como o protocolo de túnel. Assim, uma conexão é implementada usando o HTTPS; esse protocolo depende da porta TCP 443, uma porta que geralmente já está aberta em firewalls corporativos para facilitar conexões com outros aplicativos e serviços; por exemplo, Outlook Web App e serviços Web.

3. Você tem um servidor VPN com duas políticas de rede configuradas. A primeira tem uma condição que permite acesso aos membros do grupo Contoso, ao qual todos da organização pertencem, mas possui uma restrição de Dia e horário que limita o acesso apenas ao horário de funcionamento do escritório. A segunda política tinha uma condição de associação do grupo Adminis. do Domínio e nenhuma restrição. Por que as conexões por administradores estão sendo negadas fora do horário do escritório e o que pode ser feito em relação a isso?

Resposta: os administradores também são os membros do grupo Contoso e, portanto, a primeira condição da política é atendida. A segunda política não é processada. A solução é remover os administradores do grupo Contoso ou alterar a ordem da política para que a política do administrador seja a primeira da lista.

Perguntas e respostas de revisão do laboratório

Pergunta: no laboratório, você configurou o servidor VPN para alocar uma configuração de endereço IP usando um pool de endereços estáticos. Que alternativa havia?

Resposta: Você poderia usar um servidor DHCP na rede interna para alocar endereços.

Pergunta: se você usasse a alternativa, quantos endereços seriam alocados para o servidor VPN ao mesmo tempo?

Resposta: o servidor DHCP aloca os blocos do servidor VPN de dez endereços por vez para alocar a clientes remotos.

Pergunta: no laboratório, você configurou uma condição de política do tipo de túnel e uma restrição de dia e horário. Se havia duas políticas — a que você criou mais uma adicional que tinha uma condição de associação ao grupo Adminis. do Domínio e uma restrição do tipo de túnel (PPTP ou L2TP) — por que seus administradores não puderam se conectar fora do horário do escritório?

Resposta: os administradores são afetados pela primeira política porque estão usando o tipo de túnel PPTP ou L2TP. Altere a ordem da política.

Pergunta: Por que você criou o grupo DA_Clients?

Resposta: para habilitar o aplicativo das configurações de segurança do DirectAccess para computadores do DirectAccess que são membros desse grupo de segurança.

Pergunta: qual é a finalidade do registro do host DNS nls.contoso.com que você associou a um endereço IP interno?

Resposta: permitir que os clientes do DirectAccess baseados na intranet localizem o Servidor do Local da Rede na intranet.

Pergunta: qual é a finalidade da lista de certificados revogados?

Resposta: permitir que clientes e servidores DirectAccess determinem se os certificados emitidos (usados para autenticação) foram revogados.

Pergunta: por que você disponibiliza a CRL no servidor DirectAccess na rede de perímetro?

Resposta: para que os clientes do DirectAccess na Internet possam acessar a CRL.

Pergunta: por que você usaria o GPO para configurar a implantação de certificado?

Resposta: para implantar de maneira mais rápida e fácil os certificados exigidos para computadores cliente do DirectAccess.

Pergunta: por que você instalou um certificado no computador cliente?

Resposta: sem um certificado, o cliente não pode identificar e autenticar a si próprio no servidor DirectAccess.

Módulo 6

Instalação, configuração e solução de problemas do serviço de função Servidor de Diretivas de Rede

Conteúdo:

Lição 1

Instalação e configuração de um Servidor de Diretivas de Rede

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como instalar o Servidor de Políticas de Rede

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Instalar a função NPS

1. Alterne para NYC-DC1.
2. Na **Barra de Tarefas**, clique em **Gerenciador de Servidores**.
3. No painel de navegação do **Gerenciador de Servidores**, clique em **Funções**.
4. No painel direito, clique em **Adicionar Funções**
5. No Assistente para Adicionar Funções, clique em **Próximo**.
6. Na página **Selecionar Funções do Servidor**, marque a caixa de seleção **Serviços de Acesso e Diretiva de Rede** e clique em **Próximo**.
7. Na página de boas-vindas dos **Serviços de Acesso e Diretiva de Rede**, clique em **Próximo**.
8. Na página **Selecionar Serviços de Função**, marque a caixa de seleção **Servidor de Diretivas de Rede** e clique em **Próximo**.
9. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
10. Na página **Resultados da Instalação**, clique em **Fechar**.
11. Feche o Gerenciador de Servidores.

▶ Registrar o NPS no AD DS

1. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Servidor de Diretivas de Rede**.
2. No painel de navegação, clique com o botão direito do mouse em **NPS (Local)** e clique em **Registrar servidor no Active Directory**.
3. Na caixa de mensagem **Servidor de Diretivas de Rede**, clique em **OK**.
4. Clique novamente em **OK** na caixa de mensagem subsequente **Servidor de Diretivas de Rede**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Demonstração: Como definir configurações gerais do NPS

Etapas da demonstração

Observação Você deve ter concluído a demonstração anterior e todas as máquinas virtuais ainda devem estar em execução e no estado exato em que estavam no fim da

demonstração anterior.

▶ Configurar um servidor RADIUS para conexões VPN

1. Na ferramenta de gerenciamento **Servidor de Diretivas de Rede**, no painel de detalhes **Introdução**, abra a lista suspensa em **Configuração Padrão** e clique em **Servidor RADIUS para Conexões Dial-Up ou VPN**.
2. Em **Servidor RADIUS para Conexões Dial-Up ou VPN**, clique em **Configurar VPN ou Dial-Up**.
3. No assistente **Configurar VPN ou Dial-Up**, clique em **Conexões VPN (Rede Virtual Privada)**, aceite o nome padrão e clique em **Avançar**.
4. Na página **Clientes RADIUS**, clique em **Adicionar**.
5. Na caixa **Nome Amigável** da caixa de diálogo **Novo Cliente RADIUS**, digite **NYC-SVR1** e clique em **Verificar**.
6. Na caixa de endereço da caixa de diálogo **Verificar Endereço**, digite **NYC-SVR1**, clique em **Resolver** e em **OK**.
7. Na caixa de diálogo **Novo Cliente RADIUS**, nas caixas **Segredo compartilhado** e **Confirmar segredo compartilhado**, digite **Pa$$w0rd** e clique em **OK**.
8. Na página **Especificar Servidor Dial-Up ou VPN**, clique em **Avançar**.
9. Na página **Configurar Métodos de Autenticação**, marque a caixa de seleção **Autenticação Criptografada da Microsoft versão 2 (MS-CHAPv2)** e clique em **Avançar**.
10. Na página **Especificar Grupos de Usuários**, clique em **Avançar**.
11. Na página **Especificar Filtros IP**, clique em **Avançar**.
12. Na página **Especificar Configurações de Criptografia**, clique em **Avançar**.
13. Na página **Especificar um Nome de Realm**, clique em **Avançar**.
14. Na página **Concluindo Novas Conexões Privadas Virtuais e Dial-Up e clientes RADIUS**, clique em **Concluir**.
15. Feche a ferramenta administrativa **Servidor de Diretivas de Rede**.

▶ Salvar a configuração

1. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
2. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
netsh nps show config > file.txt
```

3. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Notepad file.txt
```

4. Role pelo arquivo e discuta o conteúdo.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 2

Configuração de clientes e servidores RADIUS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar um cliente RADIUS

Etapas da demonstração

Observação Você deve ter concluído a demonstração anterior e todas as máquinas virtuais ainda devem estar em execução e no estado exato em que estavam no fim da demonstração anterior.

▶ Configurar um cliente RADIUS

1. Alterne para NYC-SVR1.
2. Na **Barra de Tarefas**, clique em **Gerenciador de Servidores**.
3. No painel de navegação do Gerenciador de Servidores, clique em **Funções** e, no painel direito, clique em **Adicionar Funções**.
4. Na página **Antes de Começar**, clique em **Próximo**.
5. Na página **Selecionar Funções do Servidor**, marque a caixa de seleção **Serviços de Acesso e Diretiva de Rede** e clique em **Próximo**.
6. Na página **Serviços de Acesso e Diretiva de Rede**, clique em **Próximo**.
7. Na página **Selecionar Serviços de Função**, marque a caixa de seleção **Serviços de Roteamento e Acesso Remoto** e clique em **Próximo**.
8. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
9. Na página **Resultados da Instalação**, clique em **Fechar**.
10. Feche a janela Gerenciador de Servidores.
11. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Roteamento e Acesso Remoto**.
12. No painel de navegação, selecione **NYC-SVR1 (local).**
13. Clique com o botão direito do mouse em **NYC-SVR1 (Local)** e clique em **Configurar e Habilitar Roteamento e Acesso Remoto**.
14. Na página **Bem-vindo** do **Assistente para Configuração do Servidor de Roteamento e Acesso Remoto**, clique em **Avançar**.
15. Na página **Configuração**, clique em **Configuração personalizada** e clique em **Avançar**.
16. Na página **Configuração Personalizada**, marque a caixa de seleção **Acesso VPN** e clique em **Avançar**.
17. Na página **Concluindo o Assistente para Configuração do Servidor de Roteamento e Acesso Remoto**, clique em **Concluir**.
18. Na caixa de diálogo **Roteamento e Acesso Remoto**, clique em **Iniciar serviço**.
19. Clique com o botão direito do mouse em **NYC-SVR1 (Local)** e clique em **Propriedades**.
20. Na caixa de diálogo **Propriedades de NYC-SVR1 (local)**, clique na guia **IPv4**.
21. Clique em **Pool de endereços estáticos** e clique em **Adicionar**.

22. Na caixa de diálogo **Novo Intervalo de Endereços IPv4**, na caixa **Endereço IP Inicial**, digite **10.10.0.60**. Na caixa **Número de endereços**, digite o valor **25** e clique em **OK**.
23. Na caixa de diálogo Propriedades de NYC-SVR1 (local), clique na guia Segurança.
24. Na lista Provedor de autenticação, clique em Autenticação RADIUS e em Configurar.
25. Na caixa de diálogo Autenticação RADIUS, clique em Adicionar.
26. Na caixa **Nome do servidor** da caixa de diálogo Adicionar Servidor RADIUS, digite **NYC-DC1.**
27. Clique em Alterar e, nas caixas de seleção, Novo segredo e Confirmar novo segredo, digite **Pa$$w0rd** e clique em **OK**.
28. Clique em **OK** três vezes.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Demonstração: Como criar uma nova Diretiva de Solicitação de Conexão

Etapas da demonstração

Observação Você deve ter concluído a demonstração anterior e todas as máquinas virtuais ainda devem estar em execução e no estado exato em que estavam no fim da demonstração anterior.

1. Alterne para o computador NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Servidor de Diretivas de Rede**.
3. No Servidor de Diretivas de Rede, expanda **Diretivas** e clique em **Diretivas de Solicitação de Conexão**. Observe a presença da diretiva Conexões VPN (Rede Virtual Privada); ela foi criada automaticamente pelo assistente quando você especificou a função NPS desse servidor.
4. Clique com o botão direito do mouse em **Diretivas de Solicitação de Conexão** e clique em **Novo**.
5. Na caixa **Nome da diretiva** do assistente **Nova Diretiva de Solicitação de Conexão**, digite **VPN da Contoso**.
6. Na lista **Tipo de servidor de acesso à rede**, clique em **Servidor de Acesso Remoto (VPN-Dial up)** e clique em **Avançar**.
7. Na página **Especificar Condições**, clique em **Adicionar**.
8. Na caixa de diálogo **Selecionar condição**, selecione **Tipo de Porta do NAS** e clique em **Adicionar**.
9. Na caixa de diálogo **Tipo de Porta do NAS**, marque a caixa de seleção **Virtual (VPN)** e clique em **OK**. Clique em **Avançar**.
10. Na página **Especificar Encaminhamento de Solicitações de Conexão**, clique em **Avançar**.
11. Na página **Especificar Métodos de Autenticação**, clique em **Avançar**.
12. Na página **Definir Configurações**, clique em **Avançar**.
13. Na página **Concluindo o Assistente de Diretiva de Solicitação de Conexão**, clique em **Concluir**.
14. Na lista **Diretivas de Solicitação de Conexão**, clique com o botão direito do mouse em **VPN da Contoso** e clique em **Mover para Cima**.

Observação Reverta todas as máquinas virtuais.

Revisões e informações complementares do módulo

Perguntas de revisão

1. Por que é necessário registrar o servidor NPS no Active Directory?

Resposta: quando o NPS pertence ao domínio Active Directory, o NPS executa a autenticação comparando as credenciais de usuário recebidas dos servidores de acesso à rede com as credenciais que o Active Directory armazena para a conta do usuário. O NPS autoriza as solicitações de conexão usando as políticas de rede e verificando as propriedades de discagem da conta do usuário no Active Directory. O servidor NPS deve estar registrado no Active Directory para ter permissão de acessar as credenciais da conta do usuário e as propriedades de discagem.

2. Como é possível usar os recursos de log do NPS mais eficazmente?

Resposta: Você pode usar os recursos de log do NPS mais eficazmente executando as seguintes tarefas:

Ative o log (inicialmente) para registros de autenticação e contabilização. Faça essas seleções após determinar o que é apropriado para seu ambiente.

Certifique-se de configurar o log de eventos com capacidade suficiente para manter os logs.

Faça backup de todos os arquivos de log regularmente, pois eles não poderão ser recriados se forem danificados ou excluídos.

Use o atributo RADIUS Class para controlar o uso e para simplificar a identificação do departamento ou usuário a ser cobrado pelo uso. Embora o atributo Class, que é gerado automaticamente, seja exclusivo para cada solicitação, pode haver registros duplicados nos casos em que a resposta ao servidor de acesso é perdida e a solicitação é enviada novamente. Pode ser necessário excluir as solicitações duplicadas dos seus logs para controlar o uso mais precisamente.

Para fornecer failover e redundância com o log do SQL Server, coloque dois computadores com SQL Server em sub-redes diferentes. Use o Assistente para Criação de Publicação do SQL Server para configurar a replicação do banco de dados entre os dois servidores.

3. O que mais deve ser considerado se você optar por usar uma atribuição de porta não padrão para o tráfego RADIUS?

Resposta: Se você não usar os números de porta RADIUS padrão, será necessário configurar as exceções no firewall do computador local para permitir o tráfego RADIUS nas novas portas.

Perguntas e respostas de revisão do laboratório

Pergunta: O que um proxy RADIUS oferece?

Resposta: quando você usa o NPS como um proxy RADIUS, o NPS encaminha as solicitações de conexão para o NPS ou para outros servidores RADIUS para processamento. Por isso, a associação ao domínio do proxy NPS é irrelevante. O proxy não precisa estar registrado no Active Directory porque ele não precisa acessar as propriedades de discagem das contas do usuário. Além disso, não é necessário configurar políticas de rede em um proxy NPS, pois o proxy não autoriza solicitações de conexão. O proxy NPS pode ser um membro do domínio ou um servidor autônomo sem associação ao domínio.

Pergunta: o que é um cliente RADIUS e quais são alguns exemplos?

Resposta: um NAS (servidor de acesso à rede) é um dispositivo que fornece níveis de acesso a uma rede maior. Um NAS que usa uma infraestrutura RADIUS também é um cliente RADIUS, que envia solicitações de conexão e mensagens de contabilização para um servidor RADIUS para autenticação, autorização e contabilização.

Exemplos de servidores de acesso à rede:

- Servidores de acesso à rede que fornecem conectividade de acesso remoto para uma rede da organização ou para a Internet. Um exemplo é um computador com Windows Server 2008 e serviço de Roteamento e Acesso Remoto que fornece serviços de acesso remoto de rede de conexão discada tradicional ou VPN (rede virtual privada) para a intranet de uma organização.
- Pontos de acesso sem fio que fornecem acesso à camada física da rede de uma organização que usa tecnologias de transmissão e de recepção sem fio.
- Switches que fornecem acesso à camada física da rede de uma organização que usa tecnologias de rede local tradicionais, como a Ethernet.
- Proxies RADIUS que encaminham solicitações de conexão para servidores RADIUS que pertencem a um grupo de servidores remotos RADIUS configurado no proxy RADIUS.

Módulo 7

Implementação da Proteção de Acesso à Rede

Conteúdo:

Lição 3

Configuração da NAP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar a Proteção de Acesso à Rede

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Instalar a função Servidor NPS

1. Em NYC-DC1, clique em **Iniciar**, em **Ferramentas Administrativas** e em **Gerenciador de Servidores**.
2. Clique em **Funções** e, em **Resumo de Funções**, clique em **Adicionar Funções** e em **Próximo**.
3. Marque a caixa de seleção **Serviços de Acesso e Diretiva de Rede** e clique duas vezes em **Próximo**.
4. Marque a caixa de seleção **Servidor de Diretivas de Rede**, clique em **Próximo** e em **Instalar**.
5. Verifique se a instalação foi bem-sucedida e clique em **Fechar**.
6. Feche a janela Gerenciador de Servidores.

▶ Configurar o NPS como um servidor de política de integridade de NAP

1. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Servidor de Diretivas de Rede**.
2. Expanda **Proteção de Acesso à Rede**, expanda **Validadores da Integridade do Sistema**, expanda **Validador de Integridade de Segurança do Windows** e clique em **Configurações**.
3. No painel direito, em **Nome**, clique duas vezes em **Configuração Padrão**.
4. Na seleção **Windows 7/Windows Vista**, desmarque todas as caixas de seleção, exceto **Firewall habilitado para todas as conexões de rede**.
5. Clique em **OK** para fechar a caixa de diálogo **Validador de Integridade de Segurança do Windows**.

▶ Configurar as políticas de integridade

1. Expanda **Diretivas**.
2. Clique com o botão direito do mouse em **Diretivas de Integridade** e clique em **Novo**.
3. Na caixa de diálogo **Criar Nova Diretiva de Integridade**, em **Nome da Diretiva**, digite **Compatível**.
4. Em **Verificações de SHV de cliente**, verifique se a opção **Cliente aprovado em todas as verificações de SHV** está selecionada.
5. Em **SHVs usados nesta diretiva de integridade**, marque a caixa de seleção **Validador da Integridade da Segurança do Windows**.
6. Clique em **OK**.
7. Clique com o botão direito do mouse em **Diretivas de Integridade** e clique em **Novo**.

8. Na caixa de diálogo **Criar Nova Diretiva de Integridade**, em **Nome da Diretiva**, digite **Incompatível**.
9. Em **Verificações de SHV de cliente**, selecione **Cliente reprovado em uma ou mais verificações de SHV**.
10. Em **SHVs usados nesta diretiva de integridade**, marque a caixa de seleção **Validador da Integridade da Segurança do Windows**.
11. Clique em **OK**.

▶ Configurar políticas de rede para computadores compatíveis

1. Garanta que as **Diretivas** sejam expandidas.
2. Clique em **Diretivas de Rede**.
3. Desabilite as duas diretivas padrão localizadas em **Nome da Diretiva** clicando com o botão direito do mouse nas diretivas e clicando em **Desabilitar**.
4. Clique com o botão direito do mouse em **Diretivas de Rede** e clique em **Novo**.
5. Na janela **Especificar Nome de Diretiva de Rede e Tipo de Conexão**, em **Nome da diretiva**, digite **Compatível com Acesso Total** e clique em **Avançar**.
6. Na janela **Especificar Condições**, clique em **Adicionar**.
7. Na caixa de diálogo **Selecionar condição**, clique duas vezes em **Diretivas de Integridade**.
8. Na caixa de diálogo **Diretivas de Integridade**, em **Diretivas de integridade**, selecione **Compatível** e clique em **OK**.
9. Na janela **Especificar Condições**, verifique se **Diretiva de Integridade** está especificada em **Condições** com o valor **Compatível** e clique em **Avançar**.
10. Na janela **Especificar Permissão de Acesso**, verifique se **Acesso concedido** está selecionado e clique em **Avançar**.
11. Na página **Configurar Métodos de Autenticação**, desmarque todas as caixas de seleção, marque a caixa de seleção **Executar somente verificação de integridade de máquina** e clique em **Avançar**.
12. Clique em **Avançar** novamente.
13. Na janela **Definir Configurações**, clique em **Imposição de NAP**. Verifique se a opção **Permitir acesso total à rede** está marcada e clique em **Avançar**.
14. Na janela **Concluindo Nova Diretiva de Rede**, clique em **Concluir**.

▶ Configurar políticas de rede para computadores incompatíveis

1. Clique com o botão direito do mouse em **Diretivas de Rede** e clique em **Novo**.
2. Na janela **Especificar Nome de Diretiva de Rede e Tipo de Conexão**, em **Nome da diretiva**, digite **Incompatível Restrito** e clique em **Avançar**.
3. Na janela **Especificar Condições**, clique em **Adicionar**.
4. Na caixa de diálogo **Selecionar condição**, clique duas vezes em **Diretivas de Integridade**.
5. Na caixa de diálogo **Diretivas de Integridade**, em **Diretivas de integridade**, selecione **Incompatível** e clique em **OK**.

6. Na janela **Especificar Condições**, verifique se **Diretiva de Integridade** está especificada em **Condições** com o valor **Incompatível** e clique em **Avançar**.
7. Na janela **Especificar Permissão de Acesso**, verifique se **Acesso concedido** está selecionado e clique em **Avançar**.
8. Na página **Configurar Métodos de Autenticação**, desmarque todas as caixas de seleção, marque a caixa de seleção **Executar somente verificação de integridade de máquina** e clique em **Avançar**.
9. Clique em **Avançar** novamente.
10. Na janela **Definir Configurações**, clique em **Imposição de NAP**. Selecione **Permitir acesso limitado** e remova a caixa de seleção próxima a **Habilitar correção automática de computadores cliente**.
11. Clique em **Avançar** e em **Concluir**.

▶ Configurar a função Servidor DHCP para NAP

1. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **DHCP**.
2. Em **DHCP**, expanda **NYC-**DC1.contoso.com, expanda **IPv4**, clique com o botão direito do mouse em **Escopo [10.10.0.0] NYCScope** e clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades do Escopo [10.10.0.0] NYCScope**, clique na guia **Proteção de Acesso à Rede**, clique em **Habilitar para este escopo** e clique em **OK**.
4. No painel de navegação, clique em **Opções de Escopo**.
5. Clique com o botão direito do mouse em **Opções de Escopo** e clique em **Configurar Opções**.
6. Na caixa de diálogo **Opções de Servidor**, clique na guia **Avançadas**.
7. Na lista **Classe de usuário**, clique em **Classe Padrão de Proteção de Acesso à Rede**.
8. Na lista **Opções Disponíveis**, marque a caixa de seleção **006 Servidores DNS**.
9. Na caixa **Endereço IP**, digite **10.10.0.10** e clique em **Adicionar**.
10. Na lista **Opções Disponíveis**, marque a caixa de seleção **015 Nome do Domínio DNS**.
11. Na caixa **Valor da cadeia de caracteres**, digite **restricted.contoso.com** e clique em **OK**.
12. Feche o **DHCP**.

▶ Definir as configurações de NAP do cliente

1. Alterne para o computador NYC-CL1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **napclcfg.msc** e pressione ENTER.
3. Em **napclcfg – [Configuração de Cliente NAP (Computador Local)]**, no painel de navegação, clique em **Clientes de Imposição**.
4. No painel **Resultados**, clique com o botão direito do mouse em **Cliente de Imposição de Quarentena DHCP** e clique em **Habilitar**.
5. Feche **napclcfg – [Configuração de Cliente NAP (Computador Local)]**.
6. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **Services.msc** e pressione ENTER.
7. No painel **Resultados** em **Serviços**, clique duas vezes em **Agente de Proteção de Acesso à Rede**.

8. Na caixa de diálogo **Propriedades de Agente de Proteção de Acesso à Rede (Computador Local)**, na lista **Tipo de inicialização**, clique em **Automático**.
9. Clique em **Iniciar** e em **OK**.
10. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **gpedit.msc** e pressione ENTER.
11. Na árvore de console, expanda **Diretiva de Computador Local**, expanda **Configuração do Computador**, expanda **Modelos Administrativos**, expanda **Componentes do Windows** e, por fim, expanda **Central de Segurança**.
12. Clique duas vezes em **Ativar a Central de Segurança (somente PCs no domínio)**, clique em **Habilitado** e em **OK**.
13. Feche a janela do console. Quando for solicitado o salvamento das configurações, clique em **Não**.
14. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **Rede**, e na lista **Painel de Controle (28)**, clique em **Central de Rede e Compartilhamento**.
15. No painel esquerdo da **Central de Rede e Compartilhamento**, clique em **Alterar as configurações do adaptador**.
16. Clique com o botão direito do mouse em **Conexão Local 2** e clique em **Propriedades**.
17. Na caixa de diálogo **Propriedades de Conexão Local 2**, clique duas vezes em **Protocolo TCP/IP Versão 4 (TCP/IPv4)**.
18. Na caixa de diálogo **Propriedades do TCP/IP Versão 4 (TCP/IPv4)**, clique em **Obter um endereço IP automaticamente**.
19. Clique em **Obter o endereço dos servidores DNS automaticamente** e em **OK**.
20. Na caixa de diálogo **Propriedades de Conexão Local 2**, clique em **OK**.

▶ Testar a NAP

1. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
2. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Ipconfig
```

3. Alterne para serviços.
4. No painel Resultados de **Serviços**, clique duas vezes em **Firewall do Windows**.
5. Na caixa de diálogo **Propriedades do Firewall do Windows (Computador Local)**, na caixa **Tipo de inicialização**, clique em **Desabilitado**.
6. Clique em **Parar** e em **OK**.
7. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Ipconfig /release
```

8. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Ipconfig /renew
```

9. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Ipconfig /all
```

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 4

Monitoramento e solução de problemas da NAP

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar o rastreamento de NAP

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Configurar o rastreamento na GUI

1. Alterne para NYC-CL1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **napclcfg.msc** e pressione ENTER.
3. Em **napclcfg – [Configuração de Cliente NAP (Computador Local)]**, no painel de navegação, clique com o botão direito do mouse em **Configuração de Cliente NAP (Computador Local)** na árvore de console e clique em **Propriedades**.
4. Na guia **Geral**, clique em **Habilitado**, na lista **Básico**, clique em **Avançado** e clique em **OK**.

▶ Configurar o rastreamento na linha de comando

1. Alterne para o prompt de comando.
2. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
netsh nap client set tracing state = enable.
```

Observação Reverta todas as máquinas virtuais.

Revisões e informações complementares do módulo

Perguntas de revisão

1. Quais são as três principais configurações de cliente que você precisa definir para a maioria das implantações de NAP?

Resposta: algumas implantações de NAP que usam o Validador da Integridade da Segurança do Windows exigem a habilitação da Central de Segurança. O serviço de Proteção de Acesso à Rede é necessário quando você implanta a NAP em computadores cliente compatíveis com NAP. Além disso, é necessário configurar os clientes de imposição de NAP nos computadores compatíveis com NAP.

2. Você deseja avaliar a integridade e a segurança gerais dos computadores com imposição de NAP. O que você precisa fazer para começar a registrar eventos de NAP?

Resposta: o log de rastreamento de NAP fica desabilitado por padrão e deverá ser habilitado se você desejar solucionar problemas relacionados à NAP ou avaliar a integridade e a segurança gerais dos computadores da organização. Você pode usar o console de Gerenciamento de Cliente NAP ou a ferramenta de linha de comando netsh para habilitar o recurso de log.

3. Em um computador cliente, quais etapas você deve executar para garantir que ele seja avaliado quanto à integridade?

Resposta: habilite o cliente de imposição NAP. Habilite a Central de Segurança. Inicie o serviço do agente NAP.

Perguntas e respostas de revisão do laboratório

Pergunta: O método de imposição de NAP para DHCP é o método de imposição mais fraco do Microsoft Windows Server 2008. O que o torna menos preferível em relação aos outros métodos?

Resposta: ele é menos preferível porque um endereço IP atribuído manualmente ao computador cliente ignora a imposição de NAP para DHCP por completo.

Pergunta: você poderia usar a solução NAP de acesso remoto juntamente com a solução NAP para IPsec? Que vantagem seria obtida com um cenário como esse?

Resposta: sim. É possível usar uma ou todas as soluções NAP em um ambiente. A vantagem é que a comunicação na intranet também seria protegida com IPsec, não somente o túnel entre o host da Internet e o servidor de Roteamento de Acesso Remoto.

Pergunta: você poderia usar a imposição de NAP para DHCP no cliente? Por que sim ou por que não?

Resposta: não. Isso não funcionaria, já que os endereços IP atribuídos ao cliente de Roteamento e Acesso Remoto se originam de um pool estático do próprio servidor de Roteamento e Acesso Remoto.

Módulo 8

Aumento da segurança dos Windows Servers

Conteúdo:

Lição 1

Visão geral da segurança do Windows

Conteúdo:

Perguntas e respostas

Discussão: Identificação de riscos à segurança e de seus custos

Pergunta: quais são alguns dos riscos e custos associados às redes baseadas no Windows?

Resposta: Alguns dos riscos e custos associados às redes baseadas no Windows são:

- O malware é um dos maiores riscos às redes baseadas no Windows. Como um sistema operacional popular, frequentemente, o Windows é alvo dos criadores de malware. O malware pode ser usado para roubar senhas e outras informações úteis de sua organização. O malware também pode começar a usar seu computador para enviar spam. O malware mais sofisticado pode ser escrito especificamente para atingir sua organização.
- Dados roubados são um risco para um sistema de computador. Os dados que são roubados podem ser usados por um concorrente ou usados para complicar sua organização.
- Dados excluídos, sejam excluídos por um usuário com permissões inadequadas ou por malware, podem gerar custos de recuperação de dados.
- Problemas legais passam a ser uma preocupação se dados confidenciais ou privados forem roubados. Isso é especificamente verdadeiro em relação a dados de clientes.

Lição 2

Configuração do Firewall do Windows com Segurança Avançada

Conteúdo:

Perguntas e respostas

Discussão: Por que é importante um firewall baseado no host?

Pergunta: Por que é importante usar um firewall baseado no host, como o Firewall do Windows com Segurança Avançada?

Resposta: O Firewall do Windows com Segurança Avançada é importante pelos seguintes motivos:

- Os computadores são protegidos contra ataques na rede interna. Isso pode impedir malwares de se moverem pela rede interna, bloqueando o tráfego de entrada não solicitado.
- As regras de entrada impedem a verificação para identificar hosts na rede. Os scanners de rede mais simples fazem ping nos hosts em uma rede na tentativa de identificá-los. O Firewall do Windows com Segurança Avançada impede que os servidores membro respondam às solicitações de ping. Os controladores de domínio respondem às solicitações de ping.
- Quando as regras de saída são habilitadas, elas podem impedir que os malwares se espalhem, evitando que eles se comuniquem na rede. No caso de uma epidemia de vírus, você pode configurar os computadores com uma regra de saída específica que impede os vírus de se comunicarem pela rede.
- As regras de segurança de conexão permitem criar regras de firewall sofisticadas que usam informações de autenticação de computador e usuário para limitar a comunicação com computadores de segurança alta.

Etapas detalhadas da demonstração

Demonstração: Como configurar Perfis de Firewall

Etapas da demonstração

Observação será necessária a máquina virtual 10221B-NYC-DC1 para a conclusão desta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Configurar perfis de firewall

Em NYC-DC1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Firewall do Windows com Segurança Avançada** .

1. Em NYC-DC1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Firewall do Windows com Segurança Avançada**.
2. No Firewall do Windows com Segurança Avançada, aponte qual perfil está ativo (Domínio)
3. No painel esquerdo, clique com o botão direito do mouse no nó **Firewall do Windows com Segurança Avançada em Computador Local** e clique em **Propriedades**.
4. Mencione que as conexões de entrada são bloqueadas por padrão.
5. Mencione que as conexões de saída são permitidas por padrão.
6. Na área **Configurações**, clique no botão **Personalizar**.
7. Mencione que a seção de mesclagem de regas será relevante apenas quando as regras estiverem sendo aplicados por meio da Diretiva de Grupo.
8. Clique em **Cancelar**.
9. Na área **Log**, clique no botão **Personalizar**.
10. Mencione que nenhum log é habilitado por padrão.
11. Clique em **Cancelar**.
12. Clique em cada guia de perfil para mostrar que todos eles contêm as mesmas configurações.
13. Clique em **Cancelar**.
14. Clique no nó **Regras de Entrada**.
15. Mostre a coluna que identifica em quais perfis uma regra é aplicada. A maioria das regras no topo da lista é habilitada para todos os perfis.
16. Role para baixo na lista e identifique uma regra que não é aplicada apenas no perfil do domínio.
17. Feche o Firewall do Windows com Segurança Avançada.

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: o modelo de proteção em camadas prescreve tecnologias específicas que devem ser usadas para proteger servidores Windows?

Resposta: não, o modelo de proteção em camadas é usado para organizar seu raciocínio sobre proteção, e não para indicar tecnologias específicas.

Pergunta: sua empresa está preocupada com a segurança e implementou o Firewall do Windows para bloquear a comunicação de saída por padrão nos computadores cliente. Você está implementando um novo programa que seleciona aleatoriamente um número de porta para comunicação na rede. Como você pode permitir que esse programa funcione sem abrir portas que são desnecessárias?

Resposta: a regra de firewall para o novo aplicativo deve ser baseada em um programa, e não em uma porta. Assim, o programa pode acessar a rede, independentemente da porta que está sendo usada.

Pergunta: você está criando um GPO com regras de firewall padronizadas para os servidores em sua organização. Você testou as regras em um servidor autônomo no laboratório de teste. As regras aparecem nos servidores depois que o GPO é aplicado, mas elas não estão sendo aplicadas. Qual é a causa mais provável desse problema?

Resposta: é provável que as regras de firewall não estejam sendo aplicadas ao perfil de firewall correto. É possível que você não as tenha aplicado no perfil de domínio conforme exigido para servidores membro. Para testar regras em um servidor autônomo, elas teriam que ser aplicadas nos perfis de firewall público ou privado.

Pergunta: um colega argumentou que todas as atualizações do Windows devem ser aplicadas automaticamente quando forem liberadas. Você possui um processo alternativo que recomendaria?

Resposta: todas as atualizações devem ser testadas antes de serem aplicadas em um ambiente de produção. É simples implantar atualizações em um conjunto de computadores de teste usando o WSUS.

Perguntas e respostas de revisão do laboratório

Pergunta: Por que foi apropriado implantar a regra de firewall usando a Política de Grupo?

Resposta: neste cenário, muitos computadores precisavam da aplicação da regra. A Política de Grupo é a melhor maneira de aplicar alterações em muitos computadores de forma rápida e fácil.

Pergunta: normalmente, é exigido o uso de wuauclt.exe na implementação do WSUS?

Resposta: não. Neste laboratório, ele foi usado para que as atualizações automáticas consultassem o servidor WSUS e registrassem o computador. Isso acontecerá automaticamente na próxima vez que as atualizações automáticas forem programadas para baixar as atualizações.

Módulo 9

Aumento da segurança para comunicação de rede

Conteúdo:

Lição 1

Visão geral do IPsec

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar as definições do IPsec (opcional)

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Exibir políticas IPsec existentes na Política de Grupo

1. Alterne para NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciamento de Diretiva de Grupo**.
3. Em Gerenciamento de Diretiva de Grupo, expanda **Floresta: Contoso.com**, expanda **Domínios**, expanda **Contoso.com** e clique em **Default Domain Policy**. Na caixa de diálogo **Console do Gerenciamento de Diretiva de Grupo**, clique em **OK**.
4. Clique com o botão direito do mouse em **Diretiva Padrão de Domínio** e clique em **Editar**.
5. No Editor de Gerenciamento de Diretiva de Grupo, em **Configuração do Computador**, expanda **Diretivas**, expanda **Configurações do Windows**, expanda **Configurações de Segurança** e clique em **Diretivas de Segurança IP no Active Directory (CONTOSO.COM).**
6. No painel direito, exiba as três diretivas existentes.

▶ Criar uma política IPsec personalizada

1. Clique com o botão direito do mouse em **Diretivas de Segurança IP no Active Directory (CONTOSO.COM)** e clique em **Criar Diretiva de Segurança IP**.
2. No **Assistente de Diretiva de Segurança IP**, clique em **Avançar**.
3. Na página **Nome da Diretiva de Segurança IP**, na caixa **Nome**, digite **Diretiva de Transferência de Zona do DNS** e clique em **Avançar**.
4. Na página **Solicitações de Comunicação Segura**, clique em **Avançar**.
5. Na página **Concluindo o Assistente de Diretiva de Segurança IP**, clique em **Concluir**. A caixa de diálogo Propriedades da Diretiva de Transferência de Zona do DNS é aberta.

▶ Criar uma regra de segurança

1. Na caixa de diálogo **Propriedades da Diretiva de Transferência de Zona do DNS**, clique em **Adicionar**.
2. No **Assistente de Regra de Segurança**, clique em **Avançar**.
3. Na página **Ponto de Extremidade do Túnel**, clique em **Avançar**.
4. Na página **Tipo de Rede**, clique em **Avançar**.

▶ Criar um novo filtro IP

1. Na página **Lista de Filtros IP**, clique em **Adicionar**.

2. Na caixa de diálogo **Lista de Filtros IP**, na caixa **Nome**, digite **Tráfego da zona do DNS** e clique em **Adicionar**.
3. No **Assistente de Filtro IP**, clique em **Avançar**.
4. Na página **Descrição do Filtro IP e da Propriedade Mirrored**, clique em **Avançar**.
5. Na página **Origem do Tráfego IP**, na lista **Endereço de Origem**, clique em **Um nome DNS específico**.
6. Na caixa **Nome do host**, digite **NYC-DC1.Contoso.com** e clique em **Avançar**.
7. Na caixa de diálogo **Aviso de Segurança**, clique em **Sim**.
8. Na página **Destino do Tráfego IP**, na lista **Endereço de destino**, clique em **Um nome DNS específico**.
9. Na caixa **Nome do host**, digite **NYC-SVR1.Contoso.com** e clique em **Avançar**.
10. Na caixa de diálogo **Aviso de Segurança**, clique em **Sim**.
11. Na lista **Selecionar um tipo de protocolo** da página **Tipo de Protocolo IP**, clique em **TCP** e em **Avançar**.
12. Na página **Porta do Protocolo IP**, em **Definir a porta do protocolo IP**, clique em **Desta porta** e, na caixa, digite **53**. Clique em **Para esta porta** e, na caixa, digite **53**. Clique em **Avançar**.
13. Na página **Concluindo o Assistente de Filtro IP**, clique em **Concluir**.
14. Na caixa de diálogo **Lista de Filtros IP**, clique em **OK**.

▶ Conclusão do Assistente de Regra de Segurança

1. Na página **Lista de Filtros IP** do **Assistente de Regra de Segurança**, clique em **Tráfego de zona do DNS** e em **Avançar**.
2. Na página **Ação de Filtro**, clique em **Requer Segurança** e em **Avançar**.
3. Na página **Método de Autenticação**, clique em **Avançar**.
4. Na página **Concluindo o Assistente de Regra de Segurança**, clique em **Concluir**.

▶ Conclusão do Assistente de Regra de Segurança IP

1. Na caixa de diálogo **Propriedades da Política de Transferência de Zona do DNS**, clique em **OK**
2. No painel direito do **Editor de Gerenciamento da Diretiva de Grupo**, clique com o botão direito do mouse em **Diretiva de Transferência de Zona do DNS**

Importante Não atribua a política. Mostre aos alunos que essa etapa é necessária apenas para ativar a regra que você criou.

3. Feche todas as janelas

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Leitura adicional

Maneiras de usar o IPsec

- Determinando suas necessidades de IPsec

Ferramentas usadas para configurar o IPsec

- Tópico da Ajuda: Firewall do Windows com Segurança Avançada

Lição 2

Configuração de regras de segurança de conexão

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar uma regras de Segurança de Conexão

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Habilitar o tráfego ICMP no NYC-SVR1

1. Alterne para NYC-SVR1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **Firewall do Windows com Segurança Avançada** e pressione ENTER.
3. Clique com o botão direito do mouse em **Regras de Entrada** e clique em **Nova Regra**.
4. Na caixa de diálogo **Assistente para Nova Regra de Entrada**, clique em **Personalizado** e em **Avançar**.
5. Na página **Programas**, clique em **Avançar**.
6. Na página **Protocolo e Portas**, na lista **Tipo de protocolo**, clique em **ICMPv4** e em **Avançar**.
7. Na página **Escopo**, clique em **Avançar**.
8. Na página **Ação**, clique em **Permitir a conexão, se for segura** e clique em **Avançar**.
9. Na página **Usuários**, clique em **Avançar**.
10. Na página **Computadores**, clique em **Avançar**.
11. Na página **Perfil**, clique em **Avançar**.
12. Na página **Nome**, na caixa **Nome**, digite **ICMPv4 permitido** e clique em **Concluir**.

▶ Criar uma regra entre servidores no NYC-SVR1

1. Clique com o botão direito do mouse em **Regras de Segurança de Conexão** e clique em **Nova Regra**.
2. No **Assistente para Nova Regra de Segurança de Conexão**, clique em **Servidor para servidor** e clique em **Avançar**.
3. Na página **Pontos de Extremidade**, clique em **Avançar**.
4. Na página **Requisitos**, clique em **Exigir autenticação para conexões de entrada e saída** e clique em **Avançar**.
5. Na página **Método de Autenticação**, clique em **Avançado** e em **Personalizar**.
6. Na caixa de diálogo **Personalizar Métodos de Autenticação Avançados**, em **Primeira autenticação**, clique em **Adicionar**.
7. Na caixa de diálogo **Adicionar Primeiro Método de Autenticação**, clique em **Chave Pré-compartilhada**, digite **secreto** e clique em **OK**.

8. Na caixa de diálogo **Personalizar Métodos de Autenticação Avançados**, clique em **OK**.
9. Na página **Método de Autenticação**, clique em **Avançar**.
10. Na página **Perfil**, clique em **Avançar**.
11. Na caixa **Nome** da página **Nome**, digite **Servidor para Servidor da Contoso** e clique em **Concluir**.

▶ Criar uma regra entre servidores no NYC-CL1

1. Alterne para NYC-CL1.
2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **Firewall do Windows com Segurança Avançada** e pressione ENTER.
3. Clique com o botão direito do mouse em **Regras de Segurança de Conexão** e clique em **Nova Regra**.
4. No **Assistente para Nova Regra de Segurança de Conexão**, clique em **Servidor para servidor** e clique em **Avançar**.
5. Na página **Pontos de Extremidade**, clique em **Avançar**.
6. Na página **Requisitos**, clique em **Exigir autenticação para conexões de entrada e saída** e clique em **Avançar**.
7. Na página **Método de Autenticação**, clique em **Avançado** e em **Personalizar**.
8. Na caixa de diálogo **Personalizar Métodos de Autenticação Avançados**, em **Primeira autenticação**, clique em **Adicionar**.
9. Na caixa de diálogo **Adicionar Primeiro Método de Autenticação**, clique em **Chave Pré-compartilhada**, digite **secreto** e clique em **OK**.
10. Na caixa de diálogo **Personalizar Métodos de Autenticação Avançados**, clique em **OK**.
11. Na página **Método de Autenticação**, clique em **Avançar**.
12. Na página **Perfil**, clique em **Avançar**.
13. Na caixa **Nome** da página **Nome**, digite **Servidor para Servidor da Contoso** e clique em **Concluir**.

▶ Testar a regra

1. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
2. No prompt de comando, digite **ping 10.10.0.24** e pressione ENTER.
3. Alterne para o Firewall do Windows com Segurança Avançada.
4. Expanda **Monitoramento**, expanda **Associações de Segurança** e clique em **Modo Principal**.
5. No painel direito, clique duas vezes no item listado.
6. Exiba as informações no **Modo Principal** e clique em **OK**.
7. Expanda **Modo Rápido**.
8. No painel direito, clique duas vezes no item listado.
9. Exiba as informações no **Modo Rápido** e clique em **OK**.

Observação Reverta todas as máquinas virtuais.

Leitura adicional

O que são regras de Segurança de Conexão?

- Tópico da Ajuda: Regras de Segurança de Conexão

O que são os modos de túnel e de transporte?

- Tópico da Ajuda: Especificar pontos de extremidade de túnel
- Tópico da Ajuda: Túnel de IPsec

Escolha de requisitos de autenticação

- Tópico da Ajuda: Requisitos de autenticação

Escolha de um método de autenticação

- Tópico da Ajuda: Métodos de autenticação
- Firewall do Windows com Segurança Avançada

Lição 3

Configuração da imposição de NAP para IPsec

Conteúdo:

Leitura adicional

Imposição IPsec para redes lógicas

- Arquitetura da plataforma NAP

Funcionamento da imposição de NAP para IPsec

- Introdução à Proteção de Acesso à Rede
- Guia passo a passo: Demonstre a imposição IPsec da NAP em um laboratório de teste

Lição 4

Monitoramento e solução de problemas do IPsec

Conteúdo:

Leitura adicional

Monitoramento do IPsec usando o Firewall do Windows com Segurança Avançada

- Tópico da Ajuda: Monitoramento do Firewall do Windows com Segurança Avançada

Monitoramento do IPsec usando o Monitor de Segurança IP

- Tópico da Ajuda: Monitorando o IPsec
- Tópico da Ajuda: Monitorando o Modo principal
- Tópico da Ajuda: Monitorando o Modo rápido

Revisões e informações complementares do módulo

Perguntas de revisão

1. Você precisa garantir que o tráfego que passa entre um computador na rede de perímetro e um implantado na rede interna seja criptografado e autenticado. O computador no perímetro não faz parte da sua floresta AD DS. Quais métodos de autenticação você poderia usar se tentasse estabelecer uma regra de Segurança de Conexão entre esses dois computadores?

Resposta: você NÃO poderia usar o Kerberos, pois o computador do perímetro não está na floresta. Portanto, você poderia usar: certificados ou uma chave pré-compartilhada.

2. Para habilitar a NAP com imposição IPsec, quais políticas devem ser configuradas no servidor NPS?

Resposta: uma política de solicitação de conexão, uma política de rede e uma política de integridade de NAP.

3. Você é responsável por monitorar computadores que participam de uma rede protegida por IPsec. Você deseja fazer isso remotamente, mas está tendo dificuldades para se conectar com computadores remotos do console do Monitor de Segurança IP. O que é preciso fazer?

Resposta: você pode monitorar os computadores remotamente em um único console, mas precisa modificar uma chave do Registro para que o sistema remoto aceite uma conexão do console. Configurar a chave do Registro, EnableRemoteMgmt, como 1 evita o erro "O serviço IPsec não está sendo executado", quando você gerenciar um computador remotamente. Você pode desabilitar esse recurso definindo a chave a seguir como zero (0): HKLM\system\currentcontrolset\services\policyagent.

Perguntas e respostas de revisão do laboratório

Pergunta: no laboratório, você criou uma política específica de unidade organizacional para um aplicativo específico. Se a Contoso desejasse criar uma regra de isolamento de domínio, o que você faria?

Resposta:

1. Criaria um novo GPO vinculado ao domínio (ou modificaria a política padrão do domínio).
2. Criaria uma regra de segurança de conexão para isolamento de domínio dentro desse GPO

Pergunta: que método de autenticação você selecionaria?

Resposta: o Kerberos seria mais fácil, pois todos os computadores fazem parte da mesma floresta.

Módulo 10

Configuração e solução de problemas de serviços de arquivo e impressão de rede

Conteúdo:

Lição 1

Configuração e solução de problemas de compartilhamentos de arquivos

Conteúdo:

Perguntas e respostas

Solução de problemas de permissões de acesso de arquivos de rede

Pergunta: Se a permissão de compartilhamento Controle Total e a permissão NTFS Leitura forem atribuídas a um usuário, que permissão ele terá para acessar dados no compartilhamento?

Resposta: O usuário terá acesso de Leitura aos arquivos do compartilhamento.

Etapas detalhadas da demonstração

Demonstração: Como criar um compartilhamento de arquivos

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Crie um compartilhamento de arquivos usando a interface simplificada

1. Em NYC-DC1, clique em **Iniciar** e em **Computador**.
2. No Windows Explorer, no painel esquerdo, clique em **Disco Local (C:)**.
3. Na barra de menus, clique em **Nova pasta**.
4. Para definir o nome da pasta, digite **Share1** e pressione ENTER.
5. Clique com o botão direito do mouse em **Share1** e clique em **Propriedades**.
6. Na janela **Propriedades de Share1,** na guia **Compartilhamento,** clique em **Compartilhar**.
7. Na janela **Compartilhamento de Arquivos,** na caixa **Adicionar,** digite **Marketing** e pressione ENTER. Observe que o grupo Marketing é adicionado com permissão Leitura.
8. Clique em **Marketing** para mostrar as opções disponíveis para níveis de permissão. Observe que proprietário não está disponível. Somente Leitura e Leitura/Gravação podem ser atribuídas. Mencione aos alunos que isto está configurando permissões NTFS em lugar de permissões de compartilhamento. A permissão de compartilhamento define que esse compartilhamento será Controle Total para o Grupo Todos.
9. Clique em **Compartilhar**.
10. Anote o caminho UNC para o compartilhamento e mostre-o para os alunos. Clique em **Pronto**.
11. Na janela **Propriedades de Share1,** clique em **Fechar**.

▶ Crie um compartilhamento de arquivos usando o compartilhamento avançado

1. No Windows Explorer, na barra de menus, clique em **Nova pasta**.
2. Para definir o nome da pasta, digite **Share2** e pressione ENTER.
3. Clique com o botão direito do mouse em **Share2** e clique em **Propriedades**.
4. Na janela **Propriedades de Share2,** na guia **Compartilhamento,** clique em **Compartilhamento Avançado**.
5. Na janela **Compartilhamento Avançado,** marque a caixa de seleção **Compartilhar esta pasta** e clique em **Permissões**.
6. Na janela **Permissões para Share2,** leia as permissões padrão atribuídas.
7. Com o grupo Todos selecionado, marque a caixa de seleção **Permitir Controle Total** e clique em **OK**.
8. Na janela **Compartilhamento Avançado,** clique em **Aplicar**.

▶ Tarefa 3: Configurar o compartilhamento avançado para um compartilhamento de arquivos

1. Na janela **Compartilhamento Avançado**, clique no botão **Adicionar**.
2. Na janela **Novo Compartilhamento,** na caixa **Nome do compartilhamento,** digite **Contabilidade** e clique em **OK**. Agora esta pasta é compartilhada com dois nomes de compartilhamentos e configuração independente para permissões de compartilhamento.
3. Na janela **Compartilhamento Avançado,** clique em **Cache**. Observe as opções disponíveis para os alunos.

Observação O BranchCache será abordado no Módulo 9: Otimização do acesso aos dados para filiais.

4. Na janela **Configurações Offline,** clique em **Cancelar**.
5. Na janela **Compartilhamento Avançado,** clique em **OK**.
6. Na janela **Propriedades de Share2**, clique em **Fechar**.
7. Feche o Windows Explorer.

Demonstração: Como configurar permissões NTFS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como Contoso\Administrator usando a senha Pa$$w0rd.

▶ Configurar permissões NTFS

1. Em NYC-DC1, clique em **Iniciar** e em **Computador**.
2. No Windows Explorer, no painel esquerdo, clique em **Disco Local (C:)**.
3. Clique com o botão direito do mouse em **Share1** e clique em **Propriedades**.
4. Na janela **Propriedades de Share1,** na guia **Segurança,** examine os grupos e usuários listados. Estas são as permissões NTFS criadas pelo compartilhamento de arquivos simplificado da demonstração anterior.
5. Na caixa **Nomes de grupo ou de usuário,** clique em **Marketing** e leia as permissões listadas.
6. Clique em **Editar**.
7. Na janela **Permissões para Share1,** clique em **Marketing**.
8. Na área **Permissões para Marketing,** marque a caixa de seleção **Permitir Modificar permissão** e clique em **OK**.

▶ Exibir permissões NTFS avançadas

1. Na janela **Propriedades de Share1,** clique em **Avançadas**.
2. Na página **Configurações de Segurança Avançadas de Share1**, clique em **Alterar Permissões**.

3. Na janela **Configurações de Segurança Avançadas de Share1,** clique em **Marketing** e então clique em **Editar**.
4. Na janela **Entrada de Permissão para Share1,** examine as opções disponíveis e clique em **Cancelar**.
5. Na página **Configurações de Segurança Avançadas de Share1,** clique em **Cancelar**.
6. Na página **Configurações de Segurança Avançadas de Share1,** clique na guia **Auditoria**. A Auditoria pode ser usada para acompanhar quais usuários estão acessando e modificando arquivos.
7. Clique na guia **Proprietário**. Esta guia lhe permite alterar o proprietário de um arquivo ou pasta.
8. Clique na guia **Permissões Efetivas**. Esta guia permite a você consultar as permissões NTFS efetivas para um usuário ou grupo quando todas as associações de grupo forem consideradas.
9. Clique em **Cancelar**.
10. Na janela **Propriedades de Share1,** clique em **Cancelar.**

▶ Exibir permissões herdadas

1. No Windows Explorer, clique duas vezes em **Share1**.
2. Na barra de menus, clique em **Nova pasta**.
3. Para definir o nome da pasta, digite **Subfolder** e pressione ENTER.
4. Clique com o botão direito do mouse em **Subpasta** e clique em **Propriedades**.
5. Na guia **Segurança,** clique em **Marketing** e examine as permissões. Observe que as marcas de seleção que indicam as permissões estão acinzentadas porque são herdadas.

Lição 2

Criptografia de arquivos de rede com EFS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criptografar um arquivo usando EFS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha Pa$$w0rd exceto se houver observação em contrário.

▶ Verificar se uma conta de computador oferece suporte a EFS em um compartilhamento de rede

1. Em NYC-DC1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Usuários e Computadores do Active Directory**.
2. Se necessário, expanda **Contoso.com** and click **Domain Controllers**.
3. Clique com o botão direito do mouse em **NYC-DC1** e clique em **Propriedades**.
4. Na guia **Delegação,** verifique se **Confiar nocomputador para delegação a qualquer serviço (apenas Kerberos)** está selecionado e clique em **Cancelar**. Essas configurações estão ativadas por padrão em controladores de domínio, mas precisam ser habilitadas para a maioria dos servidores de arquivos para que ofereçam suporte ao EFS.
5. Feche Usuários e Computadores do Active Directory.

▶ Usar EFS para criptografar um arquivo em um compartilhamento de rede

1. Em NYC-CL1, faça logon como **Contoso\Adam** com a senha **Pa$$w0rd**.
2. Clique em **Iniciar**, digite **\\NYC-DC1\Share1** e pressione ENTER.
3. No Windows Explorer, clique com o botão direito do mouse em uma área aberta, aponte para **Novo** e clique em **Documento do Microsoft Office Word**.
4. Digite **MyEncryptedFile** e pressione ENTER para nomear o arquivo.
5. Clique duas vezes em **MyEncryptedFile** para abri-lo.
6. Se necessário, clique em **OK** para fechar a mensagem de erro.
7. Se necessário, clique em **OK** para definir o nome de usuário.
8. No documento, digite **Meus dados secretos** e clique no botão **Salvar**.
9. Feche o Word.
10. Clique com o botão direito do mouse em **MyEncryptedFile** e clique em **Propriedades**.
11. Na janela **Propriedades de MyEncryptedFile,** na guia **Geral,** clique em **Avançado**.
12. Na janela **Atributos Avançados,** marque a caixa de seleção **Criptografar o conteúdo para proteger os dados** e clique em **OK**.
13. Na janela **Propriedades de MyEncryptedFile,** clique em **OK**.

▶ Exibir o certificado usado para criptografia

1. Em NYC-DC1, clique em **Iniciar** e em **Computador**.
2. Navegue até C:\Users\. Observe que Adam tem um perfil no computador. Este é o local onde o certificado é autoassinado. Ele não poderá ser exibido no snap-in Certificados do MMC, a menos que Adam faça logon localmente no servidor.
3. Navegue até C:\Users\Adam\AppData\roaming\Microsoft\SystemCertificates\My\Certificates. Essa é a pasta que armazena o certificado autoassinado para Adam.

▶ Testar o acesso a um arquivo criptografado

1. Em NYC-CL1, faça logon como **Contoso\Don** com a senha **Pa$$w0rd**.
2. Clique em **Iniciar**, digite **\\NYC-DC1\Share1** e pressione ENTER.
3. Clique duas vezes em **MyEncryptedFile**.
4. Se necessário, clique em **OK** para definir o nome de usuário.
5. Clique em **OK** para apagar a mensagem de acesso negado.
6. Feche o Word.

Lição 3

Criptografia de partições com o BitLocker

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criptografar uma partição usando o BitLocker

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Preparação da demonstração

1. No host virtual, abra o Gerenciador do Hyper-V, se necessário.
2. Clique com o botão direito do mouse em **10221B-NYC-DC1** e clique em **Configurações**.
3. Na lista de hardware, verifique se BitLocker.vfd está listado. Este é o disquete virtual que será usado como uma alternativa a um TPM.
4. Se o BitLocker.vfd não estiver listado, clique em **Unidade de Disquete**, clique no arquivo do **Disquete virtual (.vfd)**, clique em **Navegar**, selecione **C:\Arquivos de Programas\Microsoft Learning\10221\Drives\10221B-NYC-DC1\Virtual Hard Disks\BitLocker.vfd** e clique em **OK**.

▶ Instalar o recurso BitLocker

1. Em NYC-DC1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciador de Servidores**.
2. No Gerenciador de Servidores, clique em **Recursos** e clique em **Adicionar Recursos**.
3. Na lista de recursos, marque a caixa de seleção **Criptografia de Unidade de Disco BitLocker** e clique em **Avançar**.
4. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
5. Na página **Resultados,** clique em **Fechar**.
6. Na janela popup, clique em **Sim** para reiniciar.
7. Quando o reinício for concluído, faça logon como **Administrator** com a senha **Pa$$w0rd**.
8. Aguarde até a conclusão da instalação e clique em **Fechar** para fechar o Gerenciador de Servidores.

▶ Configurar o Bitlocker para não exigir um TPM

1. Em NYC-DC1, clique em **Iniciar**, digite **gpedit.msc** e pressione ENTER.
2. Na janela Editor de Diretiva de Grupo Local, navegue até **Configuração do Computador\Modelos Administrativos\Componentes do Windows\Criptografia de Unidade de Disco BitLocker\Unidades de Sistema Operacional**.
3. Clique duas vezes em **Exigir autenticação adicional na inicialização**.
4. Na janela Exigir autenticação adicional na inicialização, clique em **Habilitado**.
5. Verifique se a caixa de seleção **Permitir BitLocker sem um TPM compatível** está marcada e clique em **OK**.
6. Feche a janela **Editor de Diretiva de Grupo Local**.

▶ Habilitar o BitLocker quando um TPM não estiver disponível

1. Em NYC-DC1, clique em **Iniciar** e clique em **Painel de Controle**.
2. No Painel de Controle, clique em **Sistema e Segurança** e clique em **Criptografia de Unidade de Disco BitLocker**.
3. Na janela **Criptografia de Unidade de Disco BitLocker,** ao lado de C:, clique em **Ligar BitLocker**. Essa janela é a que normalmente você usaria para ligar o BitLocker.

> **Observação** No ambiente do Hyper-V usado para os laboratórios, não há um modo de usar uma unidade flash USB virtual. Portanto, o BitLocker deve estar habilitado em um prompt de comando.

4. Feche a janela **Criptografia de Unidade de Disco BitLocker.**
5. Clique em **Iniciar**, aponte para **Todos os Programas**, clique em **Acessórios** e clique em **Prompt de Comando**.
6. No prompt de comando, digite **manage-bde.exe -on C: -rp -sk A:** e pressione ENTER. É necessário fazer isso na linha de comando porque a interface gráfica do BitLocker não permite que você selecione um disquete para armazenar a chave.
7. Reinicie NYC-DC1 para concluir o processo de criptografia para C:.

▶ Acessar a senha de recuperação

1. Faça logon como **Administrator** com a senha **pa$$w0rd**.
2. Clique em **Iniciar** e clique em **Painel de Controle**.
3. No Painel de Controle, clique em **Sistema e Segurança** e clique em **Criptografia de Unidade de Disco BitLocker**.
4. Leia o status da unidade C:.
5. Clique em **Gerenciar BitLocker**.
6. Clique em **Salvar ou imprimir chave de recuperação novamente**.
7. Clique em **Salvar a chave de recuperação em um arquivo**, navegue até D:\Labfiles e clique em **Salvar**.
8. Clique em **Sim** para salvar o arquivo nesse local.
9. Feche todas as janelas abertas.
10. Clique em **Iniciar** e em **Computador**.
11. Navegue até **D:\Labfiles** e clique duas vezes no arquivo de texto **Chave de Recuperação do Bitlocker.**
12. Examine a chave de recuperação de 48 dígitos.
13. Feche todas as janelas abertas.

Lição 4

Configuração e solução de problemas de impressão de rede

Conteúdo:

Perguntas e respostas

Discussão: Solução de problemas de impressão via rede

Pergunta: Quais são alguns dos problemas comuns de impressão de rede e como eles são solucionados?

Resposta: Alguns problemas comuns de impressão de rede são:

- **Trabalhos de impressão que não são exibidos corretamente:** Normalmente, isso é causado por drivers incorretos. Tente atualizar o driver no servidor com a versão mais recente do fabricante. Quando você atualiza o driver para a impressora compartilhada no servidor, ele é enviado por push ao cliente.
- **Trabalho de impressão corrompido bloqueando a fila:** Em algumas ocasiões, os trabalhos de impressão são corrompidos e impedem a impressão de outros trabalhos de impressão. Para resolver esse problema, você deverá excluir o trabalho de impressão corrompido. Se não for possível excluir o trabalho de impressão corrompido na interface gráfica, talvez seja necessário parar o serviço de spooler e excluir o trabalho manualmente de C:\Windows\System32\spool\PRINTERS.
- **Usuário incapaz de instalar drivers:** Você pode evitar esse problema instalando drivers de impressora para todos os sistemas operacionais no servidor de impressão. Quando uma impressora de rede é instalada, o usuário não precisa de permissão para instalar os drivers. Se for necessário instalar impressoras locais, os drivers poderão ser pré-testados usando pnputil para carregá-los no cache de driver.

Etapas detalhadas da demonstração

Demonstração: Como criar várias configurações para um dispositivo de impressão

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Tarefa 1: Criar uma impressora compartilhada

1. Em NYC-DC1, clique em **Iniciar** e clique em **Dispositivos e Impressoras**.
2. Na janela **Dispositivos e Impressoras,** clique em **Adicionar uma impressora**.
3. Na janela **Adicionar Impressora,** clique em **Adicionar uma impressora local**.
4. Na página **Escolher uma porta de impressora,** clique em **Avançar**. Em um cenário da vida real, você selecionaria uma porta TCP/IP Padrão para se comunicar com uma impressora de rede.
5. Na página **Instalar o driver da impressora,** clique em **Avançar** para aceitar a seleção padrão. Em um cenário da vida real, você selecionaria o driver da sua impressora.
6. Na página **Digite o nome de uma impressora,** na caixa **Nome da impressora,** digite **AllUsers** e clique em **Avançar**.
7. Na página **Compartilhamento de Impressora,** clique em **Avançar** para compartilhar a impressora com as configurações padrão.
8. Na página **Você adicionou com êxito a AllUsers,** clique em **Concluir**.

▶ Tarefa 2: Criar uma segunda impressora usando a mesma porta

1. Na janela **Dispositivos e Impressoras,** clique em **Adicionar uma impressora**.
2. Na janela **Adicionar Impressora,** clique em **Adicionar uma impressora local**.
3. Na página **Escolher uma porta de impressora,** clique em **Avançar**. Essa será a mesma porta que foi selecionada para a impressora criada na tarefa anterior.
4. Na página **Instalar o driver da impressora,** clique em **Avançar** para aceitar a seleção padrão, que é o mesmo driver da impressora usado para a impressora criada na tarefa anterior.
5. Na página **Que versão do driver você deseja usar,** clique em **Avançar** para reutilizar o mesmo driver da impressora.
6. Na página **Digite o nome de uma impressora,** na caixa **Nome da impressora,** digite **Executives** e clique em **Avançar**.
7. Na página **Compartilhamento de Impressora,** clique em **Avançar** para compartilhar a impressora com as configurações padrão.
8. Na página **Você adicionou com êxito,** clique em **Concluir**.
9. Na janela **Dispositivos e Impressoras,** examine a lista de dispositivos. Observe que só a impressora Executives está listada.

▶ Tarefa 3: Aumentar a prioridade da segunda impressora

1. Na janela Dispositivos e Impressoras, clique com o botão direito do mouse em **Executives**, aponte para **Propriedades da impressora** e clique em **Executives**.
2. Na guia **Avançado,** na caixa **Prioridade,** digite **10** e clique em **OK**. Agora, os trabalhos enviados à impressora Executives têm prioridade mais alta do que os enviados à impressora AllUsers e serão impressos primeiro.

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Você está planejando a configuração de permissões NTFS e de compartilhamento em novo servidor de arquivos. Um de seus colegas sugere que as permissões de compartilhamento deveriam ser limitadas ao mínimo possível em vez de atribuir Controle Total ao grupo Todos. Por que essa não é uma preocupação quando são usadas permissões NTFS?

Resposta: Quando as permissões NTFS são usadas para proteger os dados em um compartilhamento de arquivos, não podem ser substituídas por permissões de compartilhamento mais permissivas. Contanto que as permissões NTFS sejam configuradas corretamente, as permissões de compartilhamento poderão ser configuradas como controle total. Se as permissões de compartilhamento forem limitadas, isso aumentará a complexidade do gerenciamento de permissões de compartilhamento.

Pergunta: Sua organização tem uma mistura de usuários móveis com laptops com Windows XP e Windows 7. Os usuários móveis usam uma VPN para acessar arquivos remotamente. Um usuário que foi atualizado recentemente para o Windows 7 observou que o acesso a arquivos pela VPN está muito mais rápido agora. Por que isso está acontecendo?

Resposta: O Windows 7 e Windows Server 2008 R2 incluem SMB 2.1 para compartilhamento de arquivos. Ele é um protocolo muito mais rápido do que o SMB 1 no Windows XP.

Pergunta: Você está planejando habilitar o BitLocker nos servidores localizados em escritórios remotos para aumentar a segurança. Um de seus colegas está preocupado pois acha que isso aumentará a complexidade do acesso dos usuários a compartilhamentos de arquivos nesses servidores. Por que essa não é uma preocupação válida?

Resposta: O BitLocker é completamente transparente ao usuário e aplicativos quando está habilitado. Ele não aumentará a complexidade para os usuários.

Pergunta: Alguns usuários têm começado a criptografar arquivos armazenados em compartilhamentos de rede para protegê-los de usuários de outros departamentos com permissões NTFS para esses arquivos. Esse é um modo efetivo de impedir que os usuários exibam e modifiquem esses arquivos?

Resposta: Sim. Um arquivo com criptografia EFS não pode ser aberto ou modificado por usuários não autorizados. Por padrão, somente o usuário que criptografou um arquivo e o agente de recuperação podem descriptografar o arquivo.

Pergunta: Um departamento em sua organização tem adicionado impressoras manualmente em computadores que executam impressão IP direta para a impressora física. Eles estão fazendo isso de forma que todos os usuários obtenham acesso automático à impressora depois de instalada. Você pode configurar um servidor de impressão e ainda disponibilizar as impressoras para todos os usuários?

Resposta: Sim. Se você usar as preferências de Diretiva de Grupo ou se tiver configurado um GPO no Gerenciamento de Impressão, uma impressora distribuída para o computador estará disponível para todos os usuários desse computador.

Perguntas e respostas de revisão do laboratório

Pergunta: No Exercício 1, por que Adam só consultou a pasta Marketing?

Resposta: A enumeração baseada em acesso limitou a exibição da pasta para Adam para somente aquilo que ele tinha permissão para acessar. Adam não tinha permissão para acessar a pasta Production e, portanto, ela estava oculta.

Pergunta: No Exercício 2, por que a conta Administrator foi capaz de abrir o arquivo criptografado?

Resposta: O certificado que foi adicionado como o agente de recuperação foi gerado pela CA e foi adicionado à conta Administrator ao mesmo tempo que foi adicionada ao GPO.

Pergunta: Quando duas portas são habilitadas para uma impressora, como você sabe para onde um trabalho de impressão será direcionado?

Resposta: Não é possível prever que porta será usada. É por isso que ambas as impressoras físicas devem estar no mesmo local físico.

Módulo 11

Otimização do acesso aos dados para filiais

Conteúdo:

Lição 1

Acesso aos dados de filial

Conteúdo:

Perguntas e respostas

Discussão: Desafios do acesso aos dados de filial

Pergunta: Por que as conexões de rede entre filiais e a matriz são relativamente lentas e não confiáveis?

Resposta: Os links de rede que oferecem conectividade de WAN são caros. Uma forma de minimizar custos usada pela maioria das organizações é a compra da menor velocidade de conectividade aceitável. Além disso, a distância da conectividade de WAN aumenta a latência. Por fim, nem toda a conectividade de WAN é não confiável, mas normalmente ela é menos confiável do que a rede interna da matriz.

Pergunta: Como a conectividade de rede lenta e não confiável afeta os usuários das filiais?

Resposta: Se os serviços de logon de dados são fornecidos pela matriz, a conectividade de rede lenta e não confiável impedirá que os usuários das filiais trabalhem. Se a conectividade com a matriz não estiver disponível, isso impedirá os usuários de acessar dados ou de fazer logon na rede. A conectividade lenta impede que os usuários executem seus trabalhos com a rapidez que gostariam e resulta em uma produtividade inferior.

Pergunta: Como o gerenciamento de sistemas de computadores em filiais se compara ao gerenciamento de sistemas de computador na matriz?

Resposta: Normalmente, os escritórios remotos possuem menos gerenciamento de sistemas de computadores do que a matriz. Nos escritórios menores, pode não haver uma equipe local para auxiliar os usuários e executar as tarefas de gerenciamento.

Pergunta: Como a segurança do sistema nas filias se compara à segurança do sistema na matriz?

Resposta: Com frequência, as filiais possuem uma segurança fraca para sistemas de computador, filiais têm segurança pobre para sistemas de computadores. Em alguns casos, os servidores não ficam em uma sala trancada.

Lição 2

Visão geral do DFS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como instalar a função DFS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**.

▶ Instalar a função DFS

1. Alterne para NYC-DC1.
2. Na barra de tarefas, clique em **Gerenciador de Servidores**.
3. No painel do console, clique em **Funções**.
4. No painel de detalhes, clique em **Adicionar Funções**.
5. No Assistente para Adicionar Funções, clique em **Próximo**.
6. Na página **Selecionar Funções do Servidor**, marque a caixa de seleção **Serviços de Arquivo** e clique em **Próximo**.
7. Na página **Serviços de Arquivo**, clique em **Próximo**.
8. Na página **Selecionar Serviço de Função**, marque a caixa de seleção ao lado de **Sistema de Arquivos Distribuído**. Clique em **Avançar**.
9. Na página **Criar um Namespace DFS**, selecione a opção **Criar um namespace mais tarde usando o snap-in Gerenciamento DFS no Gerenciador de Servidores** e clique em **Avançar**.
10. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
11. Na página **Resultados da instalação,** clique em **Fechar**.
12. Feche o **Gerenciador de Servidores**.
13. Alterne para NYC-SVR1.
14. Na barra de tarefas, clique em **Gerenciador de Servidores**.
15. No painel do console, clique em **Funções**.
16. No painel de detalhes, em **Serviços de Arquivo**, clique em **Adicionar Serviços de Função**.
17. Na página **Selecionar Serviço de Função**, marque a caixa de seleção ao lado de **Sistema de Arquivos Distribuído**. Clique em **Avançar**.
18. Na página **Criar um Namespace DFS**, selecione a opção **Criar um namespace mais tarde usando o snap-in Gerenciamento DFS no Gerenciador de Servidores** e clique em **Avançar**.
19. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
20. Na página **Resultados da instalação,** clique em **Fechar**.
21. Feche o **Gerenciador de Servidores**.

    Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 3

Configuração de namespaces DFS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criar namespaces

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Criar um novo namespace

1. Alterne para NYC-SVR1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciamento DFS**.
3. No console **Gerenciamento DFS**, no painel do console, clique em **Namespaces**.
4. Clique com o botão direito do mouse em **Namespaces** e clique em **Novo Namespace**. O **Assistente de Novo Namespace** será iniciado.
5. Na página **Servidor de Namespaces,** em **Servidor**, digite **NYC-SVR1**. Clique em **Avançar**.
6. Na página **Nomes e Configurações do Namespace**, em **Nome**, digite **Pesquisar**. Clique em **Avançar**.
7. Na página **Tipo de Namespace**, verifique se **Namespace baseado em domínio** está selecionado. Verifique também se **Habilitar o modo Windows Server 2008** está selecionado e clique em **Avançar**.
8. Na página **Examinar Configurações e Criar Namespace**, clique em **Criar**.
9. Na página **Confirmação**, verifique se a criação da tarefa de namespace foi bem-sucedida e clique em **Fechar**.
10. No painel do console, expanda o nó **Namespace** e clique em **\\Contoso.com\Research**. Descreva as quatro guias do painel de detalhes.
11. No painel do console, clique com o botão direito do mouse em **\\Contoso.com\Research**, e clique em **Propriedades**. Descreva as opções das guias Geral, Indicações e Avançado.
12. Clique em **OK** para fechar **\\Contoso.com\Research** caixa de diálogo **Propriedades**.

▶ Criar uma nova pasta e um destino de pasta

1. No painel do console Gerenciamento DFS, clique com o botão direito do mouse em **\\Contoso.com\Research** e clique em **Nova Pasta**.
2. Na caixa de diálogo **Nova Pasta**, em **Nome**, digite **Propostas**.
3. Na caixa de diálogo **Nova Pasta**, em **Destinos de pasta**, clique em **Adicionar**.
4. Na caixa de diálogo **Adicionar Destino de Pasta**, digite **\\NYC-SVR1\Proposal_docs** e clique em **OK**.
5. Na caixa de diálogo **Aviso**, clique em **Sim** para criar a pasta compartilhada.
6. Na caixa de diálogo **Criar Compartilhamento**, configure o seguinte e clique em **OK**.

7. Caminho local da pasta compartilhada: **C:\Proposal_docs**
8. Permissões da pasta compartilhada: **Administradores têm acesso total; outros usuários têm permissões de leitura e gravação**
9. Na caixa de diálogo **Aviso**, clique em **Sim** para criar a pasta.
10. Clique em **OK** para fechar a caixa de diálogo Nova Pasta.
11. Na painel do console, expanda **\\Contoso.com\Research**, e clique em **Propostas**. Explique que atualmente só existe um Destino de Pasta. Para oferecer redundância, um segundo destino de pasta pode ser adicionado com a Replicação DFS configurada. Explique também que este processo seria repetido para cada pasta a ser hospedada no namespace.
12. Para testar o namespace, clique em **Iniciar** e, na caixa **Pesquisar programas e arquivos**, digite **\\Contoso.com\Research**. Pressione ENTER. A pasta **Propostas** será exibida.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 4

Configuração e solução de problemas de Replicação DFS

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar a replicação DFS

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Criar um novo destino de pasta para replicação

1. Alterne para NYC-SVR1.
2. Em **Gerenciamento DFS**, clique com o botão do mouse na pasta **Propostas** e clique em **Adicionar Destino de Pasta**.
3. Na caixa de diálogo **Novo Destino de Pasta**, digite **\\NYC-DC1\Proposal_docs** e clique em **OK**.
4. Na caixa de diálogo **Aviso**, clique em **Sim** para criar a pasta compartilhada.
5. Na caixa de diálogo **Criar Compartilhamento**, configure o seguinte e clique em **OK**.
   - Caminho local da pasta compartilhada: **C:\Proposal_docs**
   - Permissões da pasta compartilhada: **Administradores têm acesso total; outros usuários têm permissões de leitura e gravação**
6. Na caixa de diálogo **Aviso**, clique em **Sim** para criar a pasta.
7. Na caixa de diálogo **Replicação**, clique em **Sim** para criar um grupo de replicação. O **Assistente para Replicação de Pasta** será iniciado.

▶ Criar um novo grupo de replicação

1. No **Assistente para Replicação de Pasta**, na página **Nome do Grupo de Replicação e da Pasta Replicada**, aceite as entradas padrão para **Nome do grupo de replicação** e **Nome da pasta replicada**. Clique em **Avançar**.
2. Na página **Qualificação da Replicação**, observe que NYC-DC1 e NYC-SVR1 estão qualificadas como membros de replicação DFS. Clique em **Avançar**.
3. Na página **Membro Primário**, selecione **NYC-SVR1** como membro primário. Clique em **Avançar**.
4. Na página **Seleção de Topologia**, deixe a seleção padrão **Malha completa**, que replicará todos os dados entre todos os membros do grupo de replicação. Se você teve três ou mais membros dentro do grupo de replicação, você também poderá escolher **Hub e spoke**, que lhe permite configurar um cenário de publicação onde dados são replicados de um hub comum para o resto dos membros. Você também pode escolher **Sem topologia**, que permite configurar a topologia mais tarde. Clique em **Avançar**.
5. Na página **Agendamento e Largura de Banda do Grupo de Replicação**, deixe a seleção padrão Replicar continuamente. Em seguida, defina a configuração para usar Largura de banda completa. Observe que você também pode escolher uma agenda específica para replicar durante dias e horas específicos. Clique em **Avançar**.

6. Na página **Revisar Configurações e Criar Grupo de Replicação**, clique em **Criar**.
7. Na página **Confirmação**, verifique se todas as tarefas foram bem-sucedidas e clique em **Fechar**. Observe o aviso **Atraso na Replicação** e clique em **OK**.
8. No painel do console, expanda **Replicação**.
9. Em **Replicação**, clique em **contoso.com\research\proposals**. Clique e discuta cada uma das guias do painel de detalhes.

 **Observação** Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Lição 5

Configuração de BranchCache

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar o modo BranchCache

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1, 10221B-NYC-SVR1 e 10221B-NYC-CL1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Habilitar o BranchCache em um servidor de arquivos.

1. Alterne para NYC-DC1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciador de Servidores**.
3. No painel esquerdo, expanda **Funções** e clique em **Serviços de Arquivo**.
4. Se necessário, role até **Serviços de Função** e clique em **Adicionar Serviços de Função**.
5. Na página **Selecionar Serviços de Função**, marque a caixa de seleção **BranchCache para arquivos de rede** e clique em **Próximo**.
6. Na página **Confirmar Seleções de Instalação,** clique em **Instalar**.
7. Na página **Resultados da instalação,** clique em **Fechar**.
8. Feche o Gerenciador de Servidores.
9. Clique em **Iniciar**, digite **gpedit.msc** e pressione ENTER.
10. Navegue até **Configuração do Computador\Modelos Administrativos\Rede\Servidor Lanman** e clique duas vezes em **Publicação de Hash para BranchCache**.
11. Na janela **Publicação de Hash para BranchCache**, clique em **Habilitado**.
12. Na caixa **Opções**, selecione **Permitir publicação de hash somente para pasta compartilhada na qual o BranchCache estiver habilitada** e clique em **OK**.
13. Feche o Editor de Diretiva de Grupo Local.
14. Abra o Windows Explorer da barra de tarefas e navegue até C:\.
15. Clique em **Nova Pasta**, digite **Compartilhar** e pressione ENTER.
16. Clique com o botão direito do mouse em **Compartilhar** e clique em **Propriedades**.
17. Na janela **Propriedades de Compartilhamento**, clique na guia **Compartilhamento** e clique em **Compartilhamento Avançado**.
18. Na janela **Compartilhamento Avançado**, clique em **Cache**.
19. Na janela **Configurações Offline**, marque a caixa de seleção **Habilitar BranchCache** e clique em **OK**.
20. Feche todas as janelas abertas.

Observação Reverta todas as máquinas virtuais.

Revisões e informações complementares do módulo

Perguntas de revisão

1. Como o DFS pode ser usado na sua implantação de Serviços de Arquivos?

Resposta: Você pode usar o DFS para fornecer namespaces DFS e replicação de arquivos. Os namespaces de DFS oferecem uma exibição virtual de pastas compartilhadas em diferentes servidores. A replicação de DFS oferece alta disponibilidade e tolerância a falhas, arquivos e pastas.

2. O que a configuração do Membro Primário faz quando a replicação é definida?

Resposta: O Membro Primário é usado como o servidor autoritativo durante a replicação inicial. Após a conclusão da replicação inicial, a indicação do membro primário é removida.

3. Que tipo de tecnologia de compactação é usado pelo DFS do Windows Server 2008?

Resposta: O Windows Server 2008 usa a Compactação Diferencial Remota para ajudar a otimizar as transferências de dados nas redes com largura de banda limitada.

4. Qual é a diferença entre o BranchCache e o DFS?

Resposta: O BranchCache só armazena em cache os arquivos acessados por usuários em um local remoto. O DFS replica arquivos entre matriz e um local remoto de forma que todos os arquivos existam em ambos os locais.

5. Por que você desejaria implementar o BranchCache em modo de cache hospedado em vez de no modo cache distribuído?

Resposta: Quando modo de cache distribuído é usado, o cache é distribuído entre todos os computadores Windows 7. Entretanto, é provável que os computadores Windows 7 sejam desligados ou computadores laptop sejam removidos do escritório. Isso significa que um arquivo armazenado em cache pode não estar disponível, forçando-o a ser baixado por um link WAN novamente. O modo de cache hospedado mantém os arquivos armazenados em cache em um servidor de arquivos que sempre estará disponível.

Perguntas e respostas de revisão do laboratório

Pergunta: Quais são os requisitos para implantar um namespace no modo Windows Server 2008?

Resposta: O domínio deve usar o nível funcional de domínio Windows Server 2008 e todos os servidores de namespaces devem executar o Windows Server 2008.

Pergunta: Quais são as vantagens de hospedar um namespace em vários servidores de namespaces?

Resposta:A hospedagem de um namespace em vários servidores de namespaces aumenta a disponibilidade, se um desses servidores vier a falhar. Os usuários ainda poderão acessar o namespace por meio de um dos servidores de namespaces restantes.

Pergunta: No laboratório, você moveu NYC-SVR1 para sua própria OU. Por quê?

Resposta: As definições de configuração de cliente foram feitas na Diretiva de Domínio Padrão vinculada à raiz do domínio. Esses configurações de Diretiva de Grupo impedem que o modo hospedado seja configurado em NYC-SVR1. Ao mover NYC-SVR1 para sua própria UO habilitada, você bloqueia a herança de Diretiva de Grupo para essa UO e impede que essas configurações sejam aplicadas a NYC-SVR1.

Módulo 12

Controle e monitoramento do armazenamento de rede

Conteúdo:

Lição 1

Monitoramento de armazenamento de rede

Conteúdo:

Perguntas e respostas

Discussão: Desafios do gerenciamento de armazenamento

Pergunta: Quais são alguns dos desafios de gerenciamento de armazenamento enfrentados pela sua organização?

Resposta: Estes são alguns dos desafios de gerenciamento:

- Determinando usos de armazenamento existentes. Muitas organizações não têm um método automatizado para identificar a quantidade de armazenamento em uso, e tão importante quanto, a quantidade de armazenamento livre.
- Estabelecimento e imposição de políticas de uso de armazenamento. Muitas organizações não têm um modo de controlar a quantidade de armazenamento utilizado por usuários individuais ou departamentos diferente do tamanho do disco.
- Previsão de requisitos futuros Se uma organização não acompanhar o uso de armazenamento com o passar do tempo, não poderão identificar tendências de uso e planejar a expansão do armazenamento de um modo oportuno.

Etapas detalhadas da demonstração

Demonstração: Como instalar e configurar o FSRM

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

Instalar o FSRM

1. Em NYC-SVR1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciador de Servidores**.
2. No Gerenciador de Servidores, no painel esquerdo, expanda **Funções**, clique em **Serviços de Arquivo** e clique em **Adicionar Serviços de Função**.
3. Na janela **Adicionar Serviços de Função,** marque a caixa de seleção **Gerenciador de Recursos de Servidor de Arquivos** e clique em **Próximo**.
4. Na página **Configurar o Monitoramento de Utilização de Armazenamento,** clique em **Próximo**.
5. Na página **Confirmar Seleções de Instalação,** clique em **Instalar**.
6. Na página **Resultados da instalação,** clique em **Fechar**.

Exibir opções de configuração do FSRM

1. Clique em **Iniciar**, clique em **Ferramentas Administrativas** e clique em **Gerenciador de Recursos de Servidor de Arquivos**.
2. No painel esquerdo da janela **Gerenciador de Recursos de Servidor de Arquivos**, clique com o botão direito do mouse em **Gerenciador de Recursos de Servidor de Arquivos (Local)** e clique em **Configurar Opções**.
3. Clique em cada uma das guias da janela **Opções do Gerenciador de Recursos de Servidor de Arquivos**, observando as opções disponíveis em cada guia. Feche a janela **Opções do Gerenciador de Recursos de Servidor de Arquivos**.
4. No painel esquerdo, em **Gerenciador de Recursos de Servidor de Arquivos**, expanda cada um dos componentes e exiba os detalhes de cada subnó.

Lição 2

Controle da utilização do armazenamento de rede

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criar e configurar uma cota

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Para se preparar para a demonstração

1. Em NYC-SVR1, clique em **Iniciar**, digite **cmd** e pressione ENTER.
2. No prompt de comando, digite **md C:\Projects** e pressione ENTER.
3. No prompt de comando, digite **net share Projects=C:\Projects** e pressione ENTER.
4. Feche o prompt de comando.

▶ Criar um novo modelo de cota

1. Em NYC-SVR1, clique em **Iniciar**, clique em **Ferramentas Administrativas** e clique em **Gerenciador de Recursos de Servidor de Arquivos**.
2. Na árvore do console **Gerenciador de Recursos de Servidor de Arquivos**, expanda **Gerenciamento de Cota** e clique em **Modelos de Cota**.
3. Clique com o botão direito do mouse em **Modelos de Cota** e selecione **Criar Modelo de Cota**.
4. No campo **Nome do modelo**, digite **Pastas de Projeto 1 GB.**
5. No campo **Limite**, digite **1**.
6. Na caixa suspensa à direita do campo **Limite**, selecione **GB**.
7. Selecione **Cota flexível. Permitir que usuarios excedam limite(usar para monitoracao)**.
8. Na área **Limites de notificação,** clique em **Adicionar.**
9. Na guia **Mensagem de email**, marque as caixas de seleção e clique em **Log de Eventos**. Clique em **Sim** no aviso do Gerenciador de Recursos de Servidor de Arquivos.
10. Marque a caixa de seleção **Enviar aviso para log de eventos** e clique em **OK**. Novamente, clique em **Sim** para ignorar o aviso sobre a configuração do servidor SMTP. Se forem interessados os alunos, mostre para eles como configure o servidor SMTP que é usado para enviar notificações depois desta demonstração definindo Opções do Gerenciador de Recursos de Servidor de Arquivos.
11. Clique em **OK** para fechar a caixa de diálogo **Criar Modelo de Cota**.

▶ Criar uma nova cota baseada em um modelo de cota

1. No painel de detalhes, clique com o botão direito do mouse em **Pastas de Projeto 1 GB** e clique em **Criar Cota do Modelo**.
2. No campo **Caminho da cota**, digite **C:\Projects** e clique em **Aplicar modelo e criar cotas em subpastas novas e existentes automaticamente.**
3. Clique em **Criar**.

▶ Gerar uma notificação de cota

1. Clique em **Iniciar**, digite **cmd** e pressione ENTER.
2. Digite **md C:\Projects\Project1** e pressione ENTER.
3. Digite **cd C:\Projects\Project1** e pressione ENTER.
4. Digite **fsutil file createnew largefile.txt 1300000000** e pressione ENTER.
5. Clique em **Iniciar**, clique em **Ferramentas Administrativas** e clique em **Visualizar Eventos**.
6. Em **Visualizar Eventos**, expanda **Logs do Windows** e clique em **Aplicativo**.
7. Observe o evento com ID de Evento 12325.
8. Feche todas as janelas abertas em NYC-SVR1.

Lição 3

Gerenciamento de tipos de arquivo no armazenamento de rede

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como implementar a triagem de arquivo

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Criar um grupo de arquivos

1. Em NYC-SVR1, clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Gerenciador de Recursos de Servidor de Arquivos**.
2. Na árvore do console **Gerenciador de Recursos de Servidor de Arquivos**, expanda **Gerenciamento de Triagem de Arquivo** e clique em **Grupos de Arquivos.**
3. Clique com o botão direito do mouse em **Grupos de Arquivos** e clique em **Criar Grupo de Arquivos**.
4. Na janela **Criar Propriedades do Grupo de Arquivos,** digite **Arquivos de Mídia MPx** no campo **Nome do grupo de arquivos**.
5. No campo **Arquivos a serem incluídos,** digite ***.mp*** e clique em **Adicionar.** Normalmente, são arquivos de mídia como mp3.
6. No campo **Arquivos a serem excluídos,** digite ***.mpp** e clique em **Adicionar**. São arquivos do Microsoft Project.
7. Clique em **OK**.

▶ Criar um modelo de triagem de arquivo

1. Na árvore do console **Gerenciador de Recursos de Servidor de Arquivos**, clique em **Modelos de Triagem de Arquivo.**
2. Clique com o botão direito do mouse em **Modelos de Triagem de Arquivo** e clique em **Criar Modelo de Triagem de Arquivo**.
3. Na janela **Criar Modelo de Triagem de Arquivo**, digite **Bloquear arquivos de Mídia MPx** no campo **Nome do modelo**.
4. Em **Tipo de triagem**, verifique se **Triagem ativa. Não permita os usuários para salvar arquivos sem autorização** está selecionado.
5. Na seção **Grupos de arquivos**, clique na caixa de seleção para marcar o grupo de arquivos **Arquivos de Mídia MPx**.
6. Clique na guia **Log de Eventos**.
7. Clique na caixa de seleção para marcar **Enviar aviso para log de eventos** e clique em **OK**.

▶ Criar uma triagem de arquivo.

1. No **Gerenciador de Recursos de Servidor de Arquivos**, selecione e clique com o botão direito do mouse em **Triagens de Arquivos** e clique em **Criar Triagem de Arquivo.**

2. Na janela **Criar Triagem de Arquivo**, digite **C:\Projects** no campo **Caminho da triagem de arquivo**.
3. Na janela **Criar Tiragem de Arquivo**, clique na caixa suspensa em **Derivar propriedades desse modelo de triagem de arquivo (recomendável)** e clique em **Bloquear Arquivos de Mídia MPx**.
4. Clique em **Criar**.
5. Feche o Gerenciador de Recursos de Servidor de Arquivos.

▶ Testar a triagem de arquivo

1. Clique em **Iniciar** e em **Computador**.
2. Navegue até a biblioteca de Documentos.
3. No painel direito, clique com o botão direito do mouse no espaço vazio, aponte para **Novo** e clique em **Documento de Texto**.
4. Renomeie **Novo Documento de Texto.txt** para **musicfile.mp3**.
5. Clique com o botão direito do mouse em musicfile.mp3 e clique em **Copiar**.
6. Navegue até **C:\Projects**.
7. No painel direito, clique com o botão direito do mouse no espaço vazio e clique em **Colar**.
8. Aparece um aviso mostrando que o acesso à pasta de destino está negado. Clique em **Cancelar** e feche a janela do gerenciador.

Demonstração: Como configurar a classificação de arquivos

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**.

▶ Criar uma propriedade de classificação

1. Em NYC-SVR1, clique em **Iniciar**, clique em **Ferramentas Administrativas** e clique em **Gerenciador de Recursos de Servidor de Arquivos**.
2. Expanda o nó **Gerenciamento de Classificação** e clique em **Propriedades de Classificação**.
3. Clique com o botão direito do mouse em **Propriedades de Classificação** e clique em **Criar Propriedade**.
4. Na janela **Criar Definição de Propriedade de Classificação**, digite **Confidencial** no campo **Nome da propriedade** e digite **Atribui um valor Sim ou Não à confidencialidade** no campo **Descrição**.
5. Em **Tipo de propriedade**, clique na caixa suspensa e selecione **Sim/Não**.
6. Clique em **OK**.

▶ Criar uma regra de classificação

1. Clique no nó **Regras de Classificação**.

2. Clique com o botão direito do mouse no nó **Regras de Classificação** e clique em **Criar uma Nova Regra**.
3. No campo **Nome da regra**, digite **Documentos de Folha de Pagamento Confidencial**.
4. No campo **Descrição**, digite **Classificar documentos contendo a palavra "folha de pagamento" como confidencial**.
5. Na área **Escopo**, clique no botão **Adicionar**.
6. Na janela **Procurar Pasta**, expanda **Disco Local (C:)**, clique **Projetos** e clique em **OK**.
7. Na janela **Definições de Regra de Classificação**, clique na guia **Classificação**.
8. Na área **Mecanismo de classificação**, clique na caixa suspensa e clique em **Classificador de Conteúdo**.
9. Na seção **Nome da propriedade**, escolha como nome da Propriedade **Confidencial** e **o valor de Propriedade Sim** e clique no botão **Avançado**.
10. Na janela **Parâmetros de Regra Adicionais**, clique na guia **Parâmetros de Classificação Adicionais**.
11. Na guia **Parâmetros de Classificação Adicionais,** clique duas vezes na célula em branco abaixo da coluna **Nome** e digite **Cadeia de Caracteres**.
12. Clique duas vezes na coluna **Valor** e digite **folha de pagamento**.
13. Clique em **OK**.
14. Na janela **Definições de Regra de Classificação,** clique em **OK**.

▶ Criar um arquivo contendo a palavra folha de pagamento

1. Clique em **Iniciar** e em **Computador**.
2. Navegue até **C:\Projects**.
3. Clique com o botão direito do mouse em uma área aberta, aponte para **Novo** e clique em **Documento de Texto**.
4. Digite **January** e pressione ENTER para renomear o arquivo January.txt.
5. Clique duas vezes em **January.txt** para abri-lo.
6. No Bloco de Notas, digite **Informações da folha de pagamento para janeiro**.
7. Feche o Bloco de Notas e salve as alterações.
8. Feche o Windows Explorer.

▶ Modificar a agenda de classificação

1. No Gerenciador de Recursos de Servidor de Arquivos, clique com o botão direito do mouse no nó **Regras de Classificação** e clique em **Configurar Agendamento de Classificação**.
2. Na janela **Opções do Gerenciador de Recursos de Servidor de Arquivos**, verifique se a guia **Classificação Automática** está selecionada e clique no botão **Criar**.
3. Na janela **Agendamento**, clique no botão **Novo**.
4. No campo **Hora de início**, digite **8:30** e clique em **OK**.
5. Na janela **Opções do Gerenciador de Recursos de Servidor de Arquivos**, clique em **OK**.

6. Clique com o botão direito do mouse no nó **Regras de Classificação** e clique em **Executar a Classificação com Todas as Regras Agora**.
7. Na janela **Executar Classificação**, selecione **Esperar a classificacao para concluir a exe** e clique em **OK**.
8. Exiba o relatório e verifique se **January.txt** está listado na parte inferior do relatório.
9. Feche todas as janelas abertas em NYC-SVR1.

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Você deseja usar a classificação de arquivo e o gerenciamento de arquivos para expirar determinados documentos em todos os servidores de arquivos de sua organização. Há alguma limitação de onde é possível executar classificações de arquivo e o gerenciamento de arquivos?

Resposta: Sim, a classificação de arquivo e o gerenciamento de arquivos só estão disponíveis no Windows Server 2008 R2. Não podem ser usados em servidores de arquivos do Windows Server 2008.

Pergunta: Você deseja usar o gerenciamento de arquivos para expirar documentos antigos em compartilhamentos de arquivos departamentais. Um colega está preocupado pois a exclusão de arquivos sem autorização irá gerar reclamações dos departamentos.

Resposta: Seu colega está correto. Os departamentos devem ser consultados antes que uma política assim seja departamentos antes de uma política assim seja colocada em prática. Os departamentos devem tomar parte da definição de como os arquivos serão selecionados para remoção e de qualquer requisito para arquivamento.

Pergunta: Você implementou a triagem de arquivo para impedir que os usuários de armazenassem arquivos de vídeo no volume de dados compartilhado que contém pastas departamentais. Entretanto, o departamento de Marketing precisa armazenar arquivos de vídeo na pasta departamental. Como você pode permitir isso?

Resposta: Crie uma exceção de triagem de arquivo para a pasta de d*a* pasta do departamento de Marketing que permite arquivos de vídeo. Uma exceção de triagem de arquivo substitui a triagem de arquivo.

Pergunta: Você propôs que cotas do FSRM fossem usadas para controlar o tamanho de compartilhamentos de arquivos departamentais. Um colega tem experiência com cotas NTFS e não acham que elas são práticas de usar, uma vez que se baseiam em propriedade de arquivo. O que pode dizer a seu colega sobre as cotas do FSRM para superar essa objeção?

Resposta: As cotas do FSRM não se baseiam em propriedade de arquivo. As cotas do FRSM podem ser aplicadas diretamente a uma pasta para limitar o tamanho dessa pasta, a despeito de que usuários forem proprietários dos arquivos.

Pergunta: Os dados em um compartilhamento de arquivos departamental aumentaram em 10 GB em um único dia. Normalmente, o crescimento é menor do que 1 GB. Você desconfia que um usuário tenha colocado vários arquivos grandes no compartilhamento de arquivos departamental. Como é possível confirmar isso?

Resposta: Você pode usar o relatório de armazenamento Arquivos Grandes para identificar arquivos grandes no compartilhamento. Também pode usar o relatório de armazenamento Arquivos Mais Acessados Recentemente para identificar arquivos criados recentemente.

Perguntas e respostas da revisão do laboratório

Pergunta: Quando você criou a cota no compartilhamento Home, por que selecionou a opção Aplicar modelo e criar cotas em subpastas novas e existentes automaticamente?

Resposta: Essa opção configura a cota para a ser aplicada a subpastas. Ao selecionar essa opção, a cota é se aplicada à pasta base de cada usuário.

Pergunta: Qual é a diferença entre triagem ativa e triagem passiva?

Resposta: A triagem ativa impede que os usuários salvem arquivos que coincidam com a triagem de arquivo. A triagem passiva permite que o arquivo seja salvo e só envia uma notificação.

Pergunta: Por que é importante agendar tarefas de gerenciamento de arquivos?

Resposta: Se uma tarefa de gerenciamento de arquivos não for agendada, então é provável que a tarefa nunca seja executada ou seja executada de maneira irregular. A automatização do processo garante que o gerenciamento de arquivos seja executado de modo oportuno.

Módulo 13

Recuperação de servidores e dados de rede

Conteúdo:

Lição 1

Recuperação de dados de rede com cópias de sombra

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como configurar cópias de sombra

Etapas da demonstração

Observação Será necessária a máquina virtual 10221B-NYC-DC1 para a conclusão desta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**.

▶ Habilitar cópias de sombra em C:

1. Em NYC-DC1, clique em **Iniciar** e em **Computador**.
2. No Windows Explorer, clique com o botão direito do mouse em **Disco Local (C:)** e clique em **Configurar Cópias de Sombra**.
3. Na janela **Cópias de Sombra,** clique em **C:** e clique em **Ativada**.
4. Na janela **Habilitar Cópias de Sombra,** clique em **Sim**.

▶ Exibir configurações para cópias de sombra

1. Na janela Cópias de Sombra, clique em **Configurações**.
2. Mostre que o tamanho máximo alocado é de 10% do espaço em disco.
3. Clique em **Agendar** e clique na lista suspensa para mostrar que as cópias de sombra serão criadas às 7 horas e ao meio-dia.
4. Feche todas as janelas abertas.

Demonstração: Como restaurar dados de um cópia de sombra

Etapas da demonstração

Observação Será necessária a máquina virtual 10221B-NYC-DC1 para a conclusão desta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**.

▶ Criar um novo arquivo

1. Em NYC-DC1, clique em **Iniciar** e em **Computador**.
2. Navegue até **C:** e clique em **Nova pasta**.
3. Digite **Data** e pressione ENTER para renomear a nova pasta.
4. Navegue até **C:\Data**.
5. Clique com o botão direito do mouse em uma área aberta, aponte para **Novo** e clique em **Documento de Texto**.
6. Digite **TestFile** e pressione ENTER para renomear o arquivo.
7. Clique duas vezes em **TestFile.txt** para abrir o documento.
8. No Bloco de Notas, digite **Versão 1**.
9. Feche o Bloco de Notas e clique em **Salvar** para salvar as alterações.

▶ Criar uma cópia de sombra

1. No Windows Explorer, clique com o botão direito do mouse em **Disco Local (C:)** e clique em **Configurar Cópias de Sombra**.
2. Na janela **Cópias de Sombra,** clique em **Criar Agora**.
3. Quando a cópia de sombra for concluída, clique em **OK**.

▶ Modificar o arquivo

1. No Windows Explorer, clique duas vezes em **TestFile.txt** para abrir o documento.
2. No Bloco de Notas, digite **Versão 2**.
3. Feche o Bloco de Notas e clique em **Salvar** para salvar as alterações.

▶ Restaurar uma versão anterior

1. No Windows Explorer, clique com o botão direito do mouse em **TestFile.txt** e clique em **Restaurar versões anteriores**.
2. Na janela Propriedades de TestFile.txt, na guia **Versões Anteriores**, clique na versão mais recente do arquivo e clique em **Restaurar**.
3. Na janela de aviso e clique em **Restaurar**.
4. Clique em **OK** para fechar a mensagem de êxito.
5. Clique em **OK** para fechar a janela Propriedades de TestFile.txt.
6. Clique duas vezes em **TestFile.txt** para abrir o documento e verificar se a versão anterior foi restaurada.
7. Feche todas as janelas abertas.

Revisões e informações complementares do módulo

Perguntas de revisão

Pergunta: Todos os servidores de arquivos em sua organização estão usando a configuração padrão para cópia de sombra. Um usuário excluiu acidentalmente conteúdo de um arquivo e então salvou o arquivo às 11:00. Você pode restaurar a versão correta de uma cópia de sombra?

Resposta: A configuração padrão para cópias de sombra tira um instantâneo às 07:00 e ao meio-dia. Você pode restaurar uma versão do arquivo das 07:00. Qualquer alteração feita a partir das 07:00 foi perdida.

Pergunta: Todos os servidores de arquivos em sua organização estão usando a configuração padrão para cópia de sombra. Um usuário excluiu acidentalmente um arquivo há várias semanas, mas não tinha percebido isso até hoje. É possível recuperar este arquivo de uma cópia de sombra?

Resposta: Possivelmente. Uma quantidade específica de espaço em disco é alocada para as cópias de sombra. Se as alterações desde o momento em que esses arquivos foram excluídos forem menores do que a quantidade de espaço em disco alocado, os arquivos poderão ser recuperados de uma cópia de sombra. Não há um período específico pelo qual uma cópia de sombra é válida.

Pergunta: Sua organização determinou que serão usadas quatro horas por semana para a restauração de arquivos de usuário do backup ou de cópia de sombra. Um colega sugeriu que os usuários fossem treinados para executar restaurações de cópias de sombra para reduzir a carga de trabalho do suporte técnico. Essa é uma boa ideia?

Resposta: É possível que o usuário execute restaurações de uma cópia de sombra. Entretanto, os usuários devem estar cientes das ramificações da restauração de arquivos de uma cópia de sombra, incluindo a potencial perda de dados atualizados em um arquivo. Muitas organizações preferem deixar o suporte técnico ou os administradores executarem essa tarefa.

Pergunta: Sua organização abriu uma nova filial com um único servidor. O servidor tem um banco de dados SQL usado por um aplicativo local. O Backup do Windows Server pode ser usado para fazer backup e restauração do banco de dados?

Resposta: Sim, o Backup do Windows Server tem capacidade para executar backups de aplicativos, incluindo o SQL Server. Ele usa o gravador VSS do SQL Server para garantir que os backups estejam consistentes e para truncar logs de transações.

Pergunta: Você configurou um novo servidor para executar um backup diário em um compartilhamento de rede em outro servidor. Essa é uma solução temporária até que seu software de backup padrão esteja funcionando. Depois de vários dias, você precisa restaurar um arquivo, mas só existe o backup mais recente para seleção e não de vários dias, como esperado. Por que isso ocorreu?

Resposta: Ao fazer backup em um compartilhamento de rede, o Backup do Windows Server não pode usar o recurso de cópia de sombra para manter várias versões de backup; isso só pode ser executado em um disco local ou disco rígido externo.

Perguntas e respostas de revisão do laboratório

Pergunta: Por que você precisou entrar nas propriedades do compartilhamento para restaurar um arquivo excluído de uma cópia de sombra?

Resposta: A restauração de um arquivo excluído é feita a partir das propriedades da pasta que continha o arquivo. Neste caso, o arquivo era a pasta raiz de do compartilhamento. Portanto, o arquivo excluído é restaurado das propriedades do compartilhamento.

Pergunta: Quando você executou o segundo backup, por que o espaço em disco em uso não aumentou na unidade de destino?

Resposta: O Backup do Windows Server é capaz de controlar quais dados foram alterados e somente os dados alterados são adicionados à unidade de destino. Neste caso, dados mínimos foram alterados no disco entre os dois backups.

Módulo 14

Monitoramento dos servidores da infraestrutura de rede do Windows Server 2008

Conteúdo:

Lição 2

Usando o Performance Monitor

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como capturar dados de contador com um Conjunto de Coletores de Dados

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon em ambas as máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**.

▶ criar um conjunto de coletores de dados

1. Alterne para o computador NYC-SVR1.
2. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Monitor de Sistema**.
3. No **Monitor de Desempenho**, no painel de navegação, expanda **Conjuntos de Coletores de Dados** e clique em **Definido pelo Usuário**.
4. Clique com o botão direito do mouse em **Definido pelo Usuário**, aponte para **Novo** e clique em **Conjunto de Coletores de Dados**.
5. No assistente **Criar Novo Conjunto de Coletores de Dados**, na caixa **Nome**, digite **Desempenho de NYC-SVR1**.
6. Clique em **Criar manualmente (avançado)** e clique em **Avançar**.
7. Na página **Que tipo de dados você deseja incluir?**, marque a caixa de seleção **Contador de desempenho** e clique em **Avançar**.
8. Na página **Que contadores de desempenho gostaria para registrar em log?**, clique em **Adicionar**.
9. Na lista **Contadores disponíveis,** expanda **Processador**, clique em **% tempo de processador** e clique em **Adicionar >>**.
10. Na lista **Contadores disponíveis**, expanda **Memória**, clique em **Páginas/s** e clique em **Adicionar >>.**
11. Na lista **Contadores disponíveis,** expanda **PhysicalDisk**, clique em **% tempo de disco** e clique em **Adicionar >>**.
12. Clique em **Comprimento Médio da Fila de Disco** e clique em **Adicionar >>**.
13. Na lista **Contadores disponíveis,** expanda **Sistema**, clique em **Comprimento da fila de processador** e clique em **Adicionar >>**.
14. Na lista **Contadores disponíveis**, expanda **Interface de Rede**, clique em **Bytes Total/seg**, clique em **Adicionar >>** e clique em **OK**.
15. Na página **Que contadores de desempenho deseja registrar em log?**, na caixa **Intervalo de amostra**, digite **1** e clique em **Avançar**.
16. Na página **Onde deseja salvar os dados?**, clique em **Avançar**.
17. Na página **Criar conjunto de coletores de dado?**, clique em **Salvar e fechar** e clique em **Concluir**.

18. No Monitor de Desempenho, no painel Resultados, clique com o botão direito do mouse em **Desempenho de NYC-SVR1** e clique em **Iniciar**.

▶ Criar uma carga de disco no servidor

1. Na Barra de Tarefas do Windows, clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
2. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Fsutil file createnew bigfile 104857600
```

3. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Copy bigfile \\nyc-dc1\c$
```

4. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Copy \\nyc-dc1\c$\bigfile bigfile2
```

5. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Del bigfile*.*
```

6. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
Del \\nyc-dc1\c$\bigfile*.*
```

7. Feche o prompt de comando.

▶ Analisar os dados resultantes em um relatório

1. Alterne para o Monitor de Desempenho.
2. No painel de navegação, clique com o botão direito do mouse em **Desempenho de NYC-SVR1** e clique em **Parar**.
3. No Monitor de Desempenho, no painel de navegação, clique em **Monitor de Sistema**.
4. Na barra de ferramentas, clique em **Exibir dados de logs**.
5. Na caixa de diálogo **Propriedades do Monitor de Desempenho**, na guia **Origem**, clique em **Arquivos de log** e clique em **Adicionar**.
6. Na caixa de diálogo **Selecionar Arquivo de Log**, clique duas vezes em **Admin**.
7. Clique duas vezes em **Desempenho de NYC-SVR1**, clique duas vezes na pasta **NYC-SVR1_date-00001** e então clique duas vezes em **DataCollector01.blg**.
8. Clique na guia **Dados** e em **Adicionar**.
9. Na lista **Adicionar Contadores,** na lista **Contadores disponíveis,** expanda **Memória**, clique em **Páginas/s** e então clique em **Adicionar >>**.
10. Expanda **Interface de Rede**, clique em **Total de Bytes/seg** e então clique em **Adicionar >>**.
11. Expanda **PhysicalDisk**, clique em **% tempo dedisco** e então clique em **Adicionar >>**.
12. Clique em **Comprimento Médio da Fila de Disco** e clique em **Adicionar >>**.
13. Expanda **Processador**, clique em **% tempo de processador** e então clique em **Adicionar >>**.

14. Expanda **Sistema**, clique em **Comprimento da fila de processador**, clique em **Adicionar >>** e então clique em **OK**.
15. Na caixa de diálogo **Propriedades do Monitor de Desempenho**, clique em **OK**.
16. Na barra de ferramentas, clique na seta para baixo e clique em **Relatório**.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Demonstração: Como configurar um alerta

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Criar um conjunto de coletores de dados com um contador de alertas

1. Alterne para o computador NYC-SVR1.
2. No Monitor de Desempenho, no painel de navegação, expanda **Conjuntos de Coletores de Dados** e clique em **Definido pelo Usuário**.
3. Clique com o botão direito do mouse em **Definido pelo Usuário**, aponte para **Novo** e clique em **Conjunto de Coletores de Dados**.
4. No assistente **Criar novo Conjunto de Coletores de Dados**, na **caixa Nome**, digite **Alerta de NYC-SVR1**.
5. Clique em **Criar manualmente (avançado)** e clique em **Avançar**.
6. Na página **Que tipo de dados você deseja incluir?**, clique em **Alerta do Contador de Desempenho** e clique em **Avançar**.
7. Na página **Que contadores de desempenho deseja monitorar?**, clique em **Adicionar**.
8. Na lista **Contadores disponíveis**, expanda **Processador**, clique em **% tempo de processador**, clique em **Adicionar >>** e então clique em **OK**.
9. Na página **Que contadores de desempenho deseja monitorar?**, na lista **Alertar quando**, clique em **Acima**.
10. Na caixa **Limite**, digite **10** e então clique em **Avançar**.
11. Na página **Criar conjunto de coletores de dados?**, clique em **Concluir**.
12. No painel de navegação, expanda o nó **Definido pelo Usuário** e clique em **Alerta de NYC-SVR1**.
13. No painel Resultados, clique com o botão direito em **DataCollector01** e clique em **Propriedades**.
14. Na caixa de diálogo **Propriedades de DataCollector01**, na caixa **Intervalo de amostragem**, digite **1** e clique na guia **Ação de Alerta**.
15. Marque a caixa de seleção **Registrar uma entrada no log de eventos do aplicativo** e clique em **OK**.

16. No painel de navegação, clique com o botão direito em **Alerta de NYC-SVR1** e clique em **Iniciar**.

▶ Gerar uma carga no servidor para exceder o limite configurado

1. Clique em **Iniciar**, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
2. No prompt de comando, digite os comandos a seguir e pressione ENTER:

```
C:

Cd\Labfiles
```

3. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
StressTool 95
```

4. Aguarde um minuto para permitir que alertas sejam gerados.
5. Pressione CTRL+C.
6. Feche o prompt de comando.

▶ Examinar o log de eventos para obter o evento resultante

1. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Visualizador de Eventos**.
2. No Visualizador de Eventos, no painel de navegação, expanda **Logs de Windows** e clique em **Aplicativo**.
3. Examine o log para mensagens relacionadas a desempenho.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Demonstração: Como exibir relatórios do Monitor de Desempenho

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** com a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Exibir um relatório de desempenho

1. No painel de navegação, expanda o nó **Relatórios**, expanda **Definido pelo Usuário** e clique em **Desempenho de NYC-SVR1**.
2. Expanda a pasta abaixo de Desempenho de NYC-SVR1. Esse era o relatório gerado pelo processo de coleta do Conjunto de coletores de dados anterior. Você pode alterar da exibição de gráfico para qualquer outra exibição com suporte.
3. Feche todas as janelas abertas.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a

próxima demonstração.

Lição 3

Monitorando logs de eventos

Conteúdo:

Etapas detalhadas da demonstração

Demonstração: Como criar uma exibição personalizada

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Exibir exibições personalizadas de Funções de Servidor

1. Alterne para o Visualizador de Eventos.
2. No painel de navegação, expanda **Modos de Exibição Personalizados**, expanda **Funções de Servidor** e clique em **Servidor de arquivos**. Esse é a exibição personalizada específica da função Servidor de Arquivos.

▶ Crie uma exibição personalizada

1. No painel de navegação, clique com o botão direito em **Modos de Exibição Personalizados** e clique em **Criar Modo de Exibição Personalizado**.
2. Na caixa de diálogo **Criar Modo de Exibição Personalizado**, marque as caixas de diálogo **Crítico**, **Aviso** e **Erro**.
3. Na lista **Logs de eventos**, expanda **Logs do Windows** e marque as caixas de seleção **Sistema** e **Aplicativo**. Clique com o mouse novamente na caixa de diálogo **Criar Modo de Exibição Personalizado** e clique em **OK**.
4. Na caixa de diálogo **Salvar Filtro para Modo de Exibição Personalizado**, na caixa **Nome**, digite **Erros e avisos** e clique em **OK**.
5. No Visualizador de Eventos, no painel direito, exiba os eventos que são visíveis em seu Modo de Exibição Personalizado.

Observação Deixe todas as máquinas virtuais no estado em que se encontram para a próxima demonstração.

Demonstração: Como configurar uma inscrição de evento

Etapas da demonstração

Observação Você precisa das máquinas virtuais 10221B-NYC-DC1 e 10221B-NYC-SVR1 para concluir esta demonstração. Faça logon nas máquinas virtuais como **Contoso\Administrator** usando a senha **Pa$$w0rd**. As máquinas virtuais devem estar em execução desde a demonstração anterior.

▶ Configurar o computador de origem

1. Alterne para NYC-DC1.

2. Clique em **Iniciar** e, na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
3. No prompt de comando, digite o comando a seguir e pressione ENTER:

```
winrm quickconfig
```

4. Quando solicitado, digite **Y** e pressione ENTER.
5. Clique em **Iniciar**, aponte para **Ferramentas Administrativas** e clique em **Usuários e Computadores do Active Directory**.
6. Nos Usuários e Computadores do Active Directory, no painel de navegação, clique em **Builtin**.
7. No painel de resultados, clique duas vezes em **Administradores**.
8. Na caixa de diálogo **Propriedades de Administradores**, clique na guia **Membros**.
9. Clique em **Adicionar** e, na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, clique em **Tipos de Objeto**.
10. Na caixa de diálogo **Tipos de Objeto**, marque a caixa de seleção **Computadores** e clique em **OK**.
11. Na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, na caixa **Digite os nomes de objeto a serem selecionados**, digite **nyc-svr1** e clique em **OK**.
12. Na caixa de diálogo **Propriedades de Administrador**, clique em **OK**.

▶ Configurar o computador coletor

1. Alterne para NYC-SVR1.
2. Clique em **Iniciar** e na caixa **Pesquisar**, digite **cmd.exe** e pressione ENTER.
3. No prompt de comando, digite o comando a seguir e pressione ENTER.

```
Wecutil qc
```

4. Quando solicitado, digite **Y** e pressione ENTER.

▶ Criar e exibir o log assinado

1. No Visualizador de Eventos, no painel de navegação, clique em **Assinaturas**.
2. Clique com o botão direito do mouse em **Assinaturas** e clique em **Criar Assinatura**.
3. Na caixa de diálogo **Propriedades da Assinatura**, na caixa **Nome da Assinatura**, digite **Eventos de NYC-DC1**.
4. Clique em **Coletor Iniciado** e então clique em **Selecionar Computadores**.
5. Na caixa de diálogo **Computadores**, clique em **Adicionar Computadores de Domínio**.
6. Na caixa de diálogo **Selecionar Computador**, na caixa **Digite o nome do objeto a ser selecionado**, digite **NYC-DC1** e clique em **OK**.
7. Na caixa de diálogo **Computadores**, clique em **OK**.
8. Na caixa de diálogo **Propriedades da Assinatura - Eventos de NYC-DC1**, clique em **Selecionar Eventos**.

9. Na caixa de diálogo **Filtro de Consulta**, marque as caixas de diálogo **Nivel Crítico**, **Aviso**, **Informação**, **Modo Detalhado** e **Erro**.
10. Na lista **Registrado**, clique em **Últimos 30 dias**.
11. Na lista **Logs de Eventos**, selecione **Logs do Windows**. Clique com o mouse novamente na caixa de diálogo **Filtro de Consulta** e clique em **OK**.
12. Na caixa de diálogo **Propriedades da Assinatura - Eventos de NYC-DC1**, clique em **OK**.
13. No Visualizador de Eventos, no painel de navegação, expanda **Logs do Windows**.
14. Clique em **Eventos Encaminhados**.

Observação Reverta todas as máquinas virtuais.

Revisões e informações complementares do módulo

Perguntas de revisão

1. Que contadores significativos você deve monitorar no Desempenho do Sistema do Windows Server?

Resposta: Processador >% tempo de processador

Sistema > Comprimento da fila de processador

Memória > Páginas/s

Disco Físico > % tempo de disco

Disco Físico > Comprimento Médio da Fila de Disco

2. Por que é importante monitorar o desempenho do servidor periodicamente?

Resposta: Isso ajuda você a executar o planejamento de capacidade, a identificar e a remover gargalos de desempenho e auxilia a solução de problemas.

3. Por que usar os alertas de Desempenho?

Resposta: O uso de alertas permite que você reaja com mais rapidez ao surgimento de problemas relacionados ao desempenho, talvez antes que eles tenham a oportunidade de afetar a produtividade dos usuários.

Perguntas e respostas de revisão do laboratório

Pergunta: Durante o laboratório, você coletou dados em um conjunto de coletores de dados. Qual é a vantagem de coletar dados desse modo?

Resposta: Ao coletar dados em conjuntos de coletores de dados, você pode analisar e comparar os dados aos dados históricos e pode tirar conclusões sobre a capacidade de servidor.

Envie-nos seus comentários

Para obter informações sobre problemas conhecidos, você pode pesquisar a Base de Dados de Conhecimento Microsoft em Ajuda e Suporte da Microsoft, antes de enviar comentários. Pesquise pelo número e pela revisão do curso ou por seu título.

Observação Nem todos os produtos de treinamento possuem um artigo da Base de Dados de Conhecimento. Se for esse o caso, pergunte ao instrutor se existem entradas de log de erros.

Comentários sobre o curso

Envie todos os comentários sobre o curso para msupport@mscourseware.com. Somos gratos por seu interesse e sua contribuição. Analisamos todos os emails recebidos e encaminhamos as informações para a equipe apropriada. Infelizmente, por conta do volume, não podemos fornecer uma resposta, mas podemos usar seus comentários para melhorar sua experiência futura em relação a produtos do Microsoft Learning.

Relatando erros

Ao enviar comentários, inclua o nome e o número do produto de treinamento na linha de assunto do email. Ao enviar comentários ou relatar bugs, inclua os seguintes dados:

1. Número da peça do documento ou CD
2. Número da página ou local
3. Descrição completa do erro ou alteração sugerida

Forneça todos os detalhes necessários para nos ajudar a verificar o problema.

Importante Todos os erros e sugestões são avaliados, mas apenas os que são validados são adicionados ao artigo da Base de Dados de Conhecimento do produto.