

OFFICIAL MICROSOFT LEARNING PRODUCT

24412B

**Configuração de serviços avançados
do Windows Server® 2012**

Conteúdo Complementar

As informações incluídas neste documento, incluindo URL e outras referências a sites da Internet, estão sujeitas a alterações sem aviso prévio. Salvo indicação em contrário, os nomes de empresas, organizações, produtos, nomes de domínios, endereços de email, logotipos, pessoas, lugares e acontecimentos aqui mencionados são fictícios e de nenhuma forma pretendem representar empresas, organizações, produtos, nomes de domínios, endereços de email, logotipos, pessoas, lugares ou acontecimentos. O cumprimento de todas as leis de direitos autorais é de exclusiva responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa, por escrito, da Microsoft Corporation.

A Microsoft pode ter patentes, aplicativos de patente, marcas registradas, direitos autorais ou outros direitos de propriedade intelectual abordando o assunto em questão neste documento. Exceto se expressamente previsto em um acordo de licença por escrito da Microsoft, o fornecimento deste documento não lhe concede licença para essas patentes, marcas registradas, direitos autorais ou outra propriedade intelectual.

Os nomes dos fabricantes, produtos ou URLs fornecidos servem apenas para fins informativos e a Microsoft não faz promessas nem oferece garantias, expressas, implícitas ou legais referentes a esses fabricantes ou ao uso dos produtos com qualquer tecnologia Microsoft. A inclusão de um fabricante ou produto não implica endosso da Microsoft do fabricante ou produto. Podem ser fornecidos links para sites de terceiros. Esses sites não são controlados pela Microsoft e a Microsoft não se responsabiliza pelo conteúdo de qualquer site vinculado ou qualquer link existente em um site vinculado, ou qualquer mudança ou atualização em tais sites. A Microsoft não se responsabiliza pela divulgação por webcast ou qualquer outra forma de transmissão recebida de qualquer site vinculado. A Microsoft está fornecendo esses links somente para sua conveniência, e a inclusão de tais links não implica endosso da Microsoft em relação ao site ou aos produtos nele contidos.

© 2013 Microsoft Corporation. Todos os direitos reservados.

Microsoft e as marcas comerciais listadas em <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> são marcas comerciais do grupo de empresas Microsoft. Todas as outras marcas comerciais pertencem aos respectivos proprietários

Número do produto: 24412B

Peça número: X18-86908

Lançamento: 3/2013

TERMOS DE LICENÇA MICROSOFT CURSO CONDUZIDO PELO INSTRUTOR DA MICROSOFT

Os presentes termos de licença constituem um acordo entre a Microsoft Corporation (ou, dependendo do local no qual você esteja domiciliado, uma de suas afiliadas) e você. Leia-os atentamente. Eles se aplicam ao uso que você faz do conteúdo que acompanha este contrato, que inclui, se houver, a mídia na qual você o recebeu. Esses termos de licença também se aplicam ao Conteúdo do Instrutor e a quaisquer atualizações e suplementos para o Conteúdo Licenciado, a menos que outros termos acompanhem esses itens. Nesse caso, estes últimos serão aplicados.

O ACESSO, DOWNLOAD OU USO DO CONTEÚDO LICENCIADO REPRESENTA SUA ACEITAÇÃO DESTES TERMOS. SE VOCÊ NÃO ACEITAR OS TERMOS, NÃO ACESSE, BAIXE NEM USE O CONTEÚDO LICENCIADO.

Ao cumprir estes termos de licença, você terá os direitos abaixo para cada licença de software adquirida.

1. DEFINIÇÕES.

- a. "Centro de Treinamento Autorizado" significa um Membro do Programa Microsoft IT Academy, Membro de Competência de Treinamento da Microsoft ou uma outra entidade que a Microsoft pode designar de tempo em tempo.
- b. "Sessão de Treinamento Autorizado" significa a aula de treinamento conduzida pelo instrutor usando o Curso Conduzido pelo Instrutor da Microsoft conduzido por um Instrutor em ou por meio de um Centro de Treinamento Autorizado.
- c. "Dispositivo em Sala de Aula" significa 1 (um) computador dedicado e protegido que um Centro de Treinamento Autorizado possui ou controla, localizado nas instalações de treinamento do Centro de Treinamento Autorizado que atende ou excede o nível de hardware especificado para o referido Curso Conduzido pelo Instrutor da Microsoft.
- d. "Usuário Final" significa um indivíduo que está (i) devidamente inscrito em e participando de uma Sessão de Treinamento Autorizado ou Sessão de Treinamento Privado, (ii) um funcionário de um Membro MPN ou (iii) um funcionário em tempo integral da Microsoft.
- e. "Conteúdo Licenciado" significa o conteúdo que acompanha este contrato, que pode incluir o Curso Conduzido pelo Instrutor da Microsoft ou o Conteúdo do Instrutor.
- f. "Instrutor Certificado pela Microsoft" ou "MCT" significa um indivíduo que é (i) contratado para ministrar uma sessão de treinamento para Usuários Finais em nome de um Centro de Treinamento Autorizado ou Membro do MPN e (ii) atualmente certificado como um Instrutor Certificado pela Microsoft pelo Programa do Programa de Certificação da Microsoft.

- g. "Curso Conduzido pelo Instrutor da Microsoft" significa o curso de treinamento conduzido pelo instrutor com a marca da Microsoft que instrui profissionais de TI e desenvolvedores nas tecnologias da Microsoft. Um título de Curso Conduzido pelo Instrutor da Microsoft pode ser um curso com a marca MOC, Microsoft Dynamics ou Microsoft Business Group.
- h. "Membro do Programa Microsoft IT Academy" significa um membro ativo do Programa Microsoft IT Academy.
- i. "Membro de Competência de Treinamento da Microsoft" significa um membro ativo do programa Microsoft Partner Network de boa reputação que no momento retém o status de Competência de Treinamento.
- j. "MOC" significa o curso conduzido pelo instrutor de "Official Microsoft Learning Product", conhecido como Microsoft Official Course, que instrui profissionais de TI e desenvolvedores nas tecnologias da Microsoft.
- k. "Membro MPN" significa um membro ativo do programa Microsoft Partner Network com nível silver ou gold de boa reputação.
- l. "Dispositivo Pessoal" significa 1 (um) computador pessoal, dispositivo, estação de trabalho ou dispositivo eletrônico digital que você pessoalmente possui ou controla que atende ou excede o nível de hardware especificado para o referido Curso Conduzido pelo Instrutor da Microsoft.
- m. "Sessão de Treinamento Privado" significa as aulas de treinamento conduzidas pelo instrutor fornecidas pelos Membros MPN para clientes corporativos para ensinar um objetivo de aprendizagem predefinido usando o Curso Conduzido pelo Instrutor da Microsoft. Essas aulas não são anunciadas nem promovidas para o público em geral, e a participação na aula é restrita aos indivíduos empregados por ou contratados por um cliente corporativo.
- n. "Instrutor" significa (i) um instrutor academicamente certificado contratado por um Membro do Programa Microsoft IT Academy para ministrar uma Sessão de Treinamento Autorizado e/ou (ii) um MCT.
- o. "Conteúdo do Instrutor" significa a versão do instrutor do Curso Conduzido pelo Instrutor da Microsoft e conteúdo suplementar adicional projetado exclusivamente para o uso dos Instrutores para ministrar uma sessão de treinamento usando o Curso Conduzido pelo Instrutor da Microsoft. O Conteúdo do Instrutor pode incluir apresentações do Conteúdo do Instrutor, guia de preparação do instrutor, treinamento sobre os materiais do instrutor, pacotes do Microsoft One Note, guia de configuração da sala de aula e formulário de comentários do curso de pré-lançamento. Para fins de esclarecimento, o Conteúdo do Instrutor não inclui nenhum software, disco rígido virtual ou máquinas virtuais.

2. DIREITOS DE USO. O Conteúdo Licenciado é licenciado, não vendido. O Conteúdo Licenciado é licenciado em uma *base de uma cópia por usuário*, de forma que você pode adquirir uma licença para cada indivíduo que acessa ou usa o Conteúdo Licenciado.

2.1 A seguir, há cinco conjuntos separados de direitos de uso. Apenas um conjunto de direitos se aplica a você.

a. Se você for um Membro do Programa Microsoft IT Academy:

- i. Cada licença adquirida em seu próprio nome só pode ser usada para revisar 1 (uma) cópia do Curso Conduzido pelo Instrutor da Microsoft no formato fornecido a você. Se o Curso Conduzido pelo Instrutor da Microsoft estiver no formato digital, você poderá instalar 1 (uma) cópia em até 3 (três) Dispositivos Pessoais. Você não poderá instalar o Curso Conduzido pelo Instrutor da Microsoft em um dispositivo que não lhe pertença ou sobre o qual não tenha controle.
- ii. Para cada licença adquirida em nome de um Usuário Final ou Instrutor, você poderá:
 1. distribuir uma (1) versão de cópia impressa do Curso Conduzido pelo Instrutor da Microsoft para 1 (um) Usuário Final que esteja inscrito na Sessão de Treinamento Autorizado e apenas imediatamente antes do início da Sessão de Treinamento Autorizado, ou seja, o assunto do Curso Conduzido pelo Instrutor da Microsoft que está sendo fornecido **ou**
 2. fornecer 1 (um) Usuário Final com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (uma) versão digital do Curso Conduzido pelo Instrutor da Microsoft **ou**
 3. fornecer 1 (um) Instrutor com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (um) Conteúdo do Instrutor,

desde que você cumpra com os termos abaixo:
- iii. você só fornecerá acesso ao Conteúdo Licenciado aos indivíduos que tenham adquirido uma licença válida para o Conteúdo Licenciado,
- iv. você garantirá que cada Usuário Final que esteja participando de uma Sessão de Treinamento Autorizado tenha sua própria cópia licenciada válida do Curso Conduzido pelo Instrutor da Microsoft sujeito à Sessão de Treinamento Autorizado,
- v. você garantirá que cada Usuário Final fornecido com a versão da cópia impressa do Curso Conduzido pelo Instrutor da Microsoft será apresentado com uma cópia deste contrato e cada Usuário Final concordará que seu uso do Curso Conduzido pelo Instrutor da Microsoft estará sujeito aos termos neste contrato antes de fornecer a eles o Curso Conduzido pelo Instrutor da Microsoft. Cada indivíduo terá que denotar sua aceitação deste contrato de forma exigível pelas leis locais antes de acessar o Curso Conduzido pelo Instrutor da Microsoft,
- vi. você garantirá que cada Instrutor que esteja ministrando uma Sessão de Treinamento Autorizado tenha sua própria cópia licenciada válida do Conteúdo do Instrutor sujeito à Sessão de Treinamento Autorizado,
- vii. você só usará Instrutores qualificados que tenham conhecimento profundo de e experiência na tecnologia da Microsoft sujeita ao Curso Conduzido pelo Instrutor da Microsoft que está sendo ensinado para todas as Sessões de Treinamento Autorizado,
- viii. você só fornecerá no máximo 10 horas de treinamento por semana para cada Sessão de Treinamento Autorizado que usa um título MOC e
- ix. você reconhece que os Instrutores que não são MCTs não terão acesso a todos os recursos do instrutor para o Curso Conduzido pelo Instrutor da Microsoft.

b. Se você for um Membro de Competência de Treinamento da Microsoft:

- i. Cada licença adquirida em seu próprio nome só pode ser usada para revisar 1 (uma) cópia do Curso Conduzido pelo Instrutor da Microsoft no formato fornecido a você. Se o Curso Conduzido pelo Instrutor da Microsoft estiver no formato digital, você poderá instalar 1 (uma) cópia em até 3 (três) Dispositivos Pessoais. Você não poderá instalar o Curso Conduzido pelo Instrutor da Microsoft em um dispositivo que não lhe pertença ou sobre o qual não tenha controle.
- ii. Para cada licença adquirida em nome de um Usuário Final ou Instrutor, você poderá:
 1. distribuir uma (1) versão de cópia impressa do Curso Conduzido pelo Instrutor da Microsoft para 1 (um) Usuário Final que esteja participando da Sessão de Treinamento Autorizado e apenas imediatamente antes do início da Sessão de Treinamento Autorizado, ou seja, o assunto do Curso Conduzido pelo Instrutor da Microsoft que está sendo fornecido **ou**
 2. fornecer 1 (um) Usuário Final que esteja participando da Sessão de Treinamento Autorizado com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (uma) versão digital do Curso Conduzido pelo Instrutor da Microsoft **ou**
 3. você fornecerá 1 (um) Instrutor com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (um) Conteúdo do Instrutor,

desde que você cumpra com os termos abaixo:
- iii. você só fornecerá acesso ao Conteúdo Licenciado aos indivíduos que tenham adquirido uma licença válida para o Conteúdo Licenciado,
- iv. você garantirá que cada Usuário Final que esteja participando de uma Sessão de Treinamento Autorizado tenha sua própria cópia licenciada válida do Curso Conduzido pelo Instrutor da Microsoft sujeito à Sessão de Treinamento Autorizado,
- v. você garantirá que cada Usuário Final fornecido com a versão da cópia impressa do Curso Conduzido pelo Instrutor da Microsoft será apresentado com uma cópia deste contrato e cada Usuário Final concordará que seu uso do Curso Conduzido pelo Instrutor da Microsoft estará sujeito aos termos neste contrato antes de fornecer a eles o Curso Conduzido pelo Instrutor da Microsoft. Cada indivíduo terá que denotar sua aceitação deste contrato de forma exigível pelas leis locais antes de acessar o Curso Conduzido pelo Instrutor da Microsoft,
- vi. você garantirá que cada Instrutor que esteja ministrando uma Sessão de Treinamento Autorizado tenha sua própria cópia licenciada válida do Conteúdo do Instrutor sujeito à Sessão de Treinamento Autorizado,
- vii. você só usará Instrutores qualificados com credenciais de Certificação da Microsoft aplicáveis sujeitas ao Curso Conduzido pelo Instrutor da Microsoft que está sendo ensinado para todas as Sessões de Treinamento Autorizado,
- viii. você só usará MCTs qualificados que também tenham credenciais de Certificação da Microsoft aplicáveis sujeitas ao título MOC que está sendo ensinado para todas as Sessões de Treinamento Autorizado usando o MOC,
- ix. você só fornecerá acesso ao Curso Conduzido pelo Instrutor da Microsoft para Usuários Finais e
- x. você só fornecerá acesso ao Conteúdo do Instrutor aos Instrutores.

c. Se você for um Membro MPN:

- i. Cada licença adquirida em seu próprio nome só pode ser usada para revisar 1 (uma) cópia do Curso Conduzido pelo Instrutor da Microsoft no formato fornecido a você. Se o Curso Conduzido pelo Instrutor da Microsoft estiver no formato digital, você poderá instalar 1 (uma) cópia em até 3 (três) Dispositivos Pessoais. Você não poderá instalar o Curso Conduzido pelo Instrutor da Microsoft em um dispositivo que não lhe pertença ou sobre o qual não tenha controle.
- ii. Para cada licença adquirida em nome de um Usuário Final ou Instrutor, você poderá:
 1. distribuir uma (1) versão de cópia impressa do Curso Conduzido pelo Instrutor da Microsoft para 1 (um) Usuário Final que esteja participando da Sessão de Treinamento Privado e apenas imediatamente antes do início da Sessão de Treinamento Privado, ou seja, o assunto do Curso Conduzido pelo Instrutor da Microsoft que está sendo fornecido **ou**
 2. fornecer 1 (um) Usuário Final que esteja participando da Sessão de Treinamento Privado com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (uma) versão digital do Curso Conduzido pelo Instrutor da Microsoft **ou**
 3. você fornecerá 1 (um) Instrutor que está ministrando a Sessão de Treinamento Privado com o código de resgate exclusivo e instruções sobre como eles podem ser acessar 1 (um) Conteúdo do Instrutor,

desde que você cumpra com os termos abaixo:
- iii. você só fornecerá acesso ao Conteúdo Licenciado aos indivíduos que tenham adquirido uma licença válida para o Conteúdo Licenciado,
- iv. você garantirá que cada Usuário Final que esteja participando de uma Sessão de Treinamento Privado tenha sua própria cópia licenciada válida do Curso Conduzido pelo Instrutor da Microsoft sujeito à Sessão de Treinamento Privado,
- v. você garantirá que cada Usuário Final fornecido com a versão da cópia impressa do Curso Conduzido pelo Instrutor da Microsoft será apresentado com uma cópia deste contrato e cada Usuário Final concordará que seu uso do Curso Conduzido pelo Instrutor da Microsoft estará sujeito aos termos neste contrato antes de fornecer a eles o Curso Conduzido pelo Instrutor da Microsoft. Cada indivíduo terá que denotar sua aceitação deste contrato de forma exigível pelas leis locais antes de acessar o Curso Conduzido pelo Instrutor da Microsoft,
- vi. você garantirá que cada Instrutor que esteja ministrando uma Sessão de Treinamento Privado tenha sua própria cópia licenciada válida do Conteúdo do Instrutor sujeito à Sessão de Treinamento Privado,
- vii. você só usará Instrutores qualificados com credenciais de Certificação da Microsoft aplicáveis sujeitas ao Curso Conduzido pelo Instrutor da Microsoft que está sendo ensinado para todas as Sessões de Treinamento Privado,
- viii. você só usará MCTs qualificados que tenham credenciais de Certificação da Microsoft aplicáveis sujeitas ao título MOC que está sendo ensinado para todas as Sessões de Treinamento Privado usando o MOC,
- ix. você só fornecerá acesso ao Curso Conduzido pelo Instrutor da Microsoft para Usuários Finais e
- x. você só fornecerá acesso ao Conteúdo do Instrutor aos Instrutores.

d. **Se você for um Usuário Final:**

Para cada licença adquirida, você poderá usar o Curso Conduzido pelo Instrutor da Microsoft unicamente para seu uso de treinamento pessoal. Se o Curso Conduzido pelo Instrutor da Microsoft estiver no formato digital, você poderá acessar o referido curso online usando o código de resgate exclusivo fornecido a você pelo provedor de treinamento e instalar e usar 1 (uma) cópia do Curso Conduzido pelo Instrutor da Microsoft em até 3 (três) Dispositivos Pessoais. Você também poderá imprimir 1 (uma) cópia do Curso Conduzido pelo Instrutor da Microsoft. Você não poderá instalar o Curso Conduzido pelo Instrutor da Microsoft em um dispositivo que não lhe pertença ou sobre o qual não tenha controle.

e. **Se você for um Instrutor.**

- i. Para cada licença adquirida, você poderá instalar e usar 1 (uma) cópia do Conteúdo do Instrutor no formato fornecido a você em 1 (um) Dispositivo Pessoal unicamente para preparar e fornecer uma Sessão de Treinamento Autorizado ou Sessão de Treinamento Privado e instalar 1 (uma) cópia adicional em outro Dispositivo Pessoal como uma cópia de backup que pode ser usada unicamente para reinstalar o Conteúdo do Instrutor. Você não poderá instalar nem usar uma cópia do Conteúdo do Instrutor em um dispositivo que não lhe pertença ou sobre o qual não tenha controle.
- ii. Você poderá personalizar as partes escritas do Conteúdo do Instrutor que estão logicamente associadas à instrução de uma sessão de treinamento de acordo com a versão mais recente do contrato do MCT. Se você optar por exercer os direitos acima, você concorda em cumprir com os seguintes termos: (i) personalizações só poderão ser usadas para ministrar as Sessões de Treinamento Autorizado e as Sessões de Treinamento Privado e (ii) todas as personalizações cumprirão com este contrato. Para fins de esclarecimento, qualquer uso de "*personaliza*" se refere apenas à alteração da ordem de slides e conteúdo e/ou ao não uso de todos os slides ou conteúdo, não significa alterar nem modificar nenhum slide ou conteúdo.

2.2 **Separação de Componentes.** O Conteúdo Licenciado é licenciado como uma única unidade, e você não poderá separar seus componentes e instalá-los em dispositivos diferentes.

2.3 **Redistribuição de Conteúdo Licenciado.** Exceto como expressamente fornecido nos direitos de uso acima, você não poderá distribuir nenhum Conteúdo Licenciado ou qualquer parte dele (incluindo qualquer modificação permitida) para outras pessoas, sem a permissão expressa por escrito da Microsoft.

2.4 **Serviços e Programas de Terceiros.** O Conteúdo Licenciado poderá conter programas ou serviços de terceiros. Esses termos de licenças se aplicarão ao uso que você faz de programas ou serviços de terceiros, a menos que outros termos acompanhem esses programas e serviços.

2.5 **Termos Adicionais.** Algum Conteúdo Licenciado pode conter componentes com termos, condições e licenças adicionais com relação a seu uso. Quaisquer termos não conflitantes nessas condições e licenças também se aplicarão ao uso que você faz desse respectivo componente e complementa os termos descritos neste contrato.

3. CONTEÚDO LICENCIADO BASEADO EM TECNOLOGIA DE PRÉ-LANÇAMENTO. Se o assunto do Conteúdo Licenciado se basear em uma versão de pré-lançamento da tecnologia da Microsoft ("**Pré-lançamento**"), as seguintes cláusulas serão aplicáveis além de outros termos neste contrato:

- a. **Conteúdo Licenciado de Pré-Lançamento.** O assunto do Conteúdo Licenciado está na versão de Pré-lançamento da tecnologia da Microsoft. A tecnologia talvez não funcione da forma que uma versão final da tecnologia, e nós poderemos mudar a tecnologia para a versão final. Além disso, é possível que uma versão final não seja lançada. O Conteúdo Licenciado baseado na versão final da tecnologia não pode conter as mesmas informações do Conteúdo Licenciado baseado na versão de Pré-lançamento. A Microsoft não tem nenhuma obrigação de fornecer a você nenhum conteúdo adicional, inclusive nenhum Conteúdo Licenciado baseado na versão final da tecnologia.
- b. **Comentários.** Se você concordar em enviar à Microsoft comentários sobre o Conteúdo Licenciado, quer diretamente ou por meio de seu designado terceirizado, você dará 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, produto ou serviço da Microsoft que inclua os comentários. Você não deverá enviar feedback que esteja sujeito a uma licença que requeira da Microsoft o licenciamento do software, de tecnologias ou produtos a terceiros em virtude da inclusão do seu feedback nesses elementos. Esses direitos permanecerão em vigor após o término deste contrato.
- c. **Prazo de Pré-lançamento.** Se você for Membro do Programa Microsoft IT Academy, Membro de Competência de Treinamento da Microsoft, Membro MPN ou Instrutor, você parará de usar todas as cópias do Conteúdo Licenciado na tecnologia de Pré-lançamento na (i) data na qual a Microsoft te informar que é a data de término para usar o Conteúdo Licenciado na tecnologia de Pré-lançamento ou (ii) 60 (sessenta) dias depois do lançamento comercial da tecnologia sujeita ao Conteúdo Licenciado, o que quer que ocorra primeiro ("**Prazo de Pré-lançamento**"). Mediante a expiração ou o término do prazo de Pré-lançamento, você excluirá de uma maneira irreparável e destruirá todas as cópias do Conteúdo Licenciado em seu poder ou sob seu controle.

4. ESCOPO DA LICENÇA. O Conteúdo Licenciado é licenciado, não vendido. Este contrato simplesmente confere a você alguns direitos de uso do Conteúdo Licenciado. A Microsoft se reserva todos os outros direitos. Salvo quando a lei aplicável conferir outros direitos, não obstante a presente limitação, o Conteúdo Licenciado deverá ser usado conforme expressamente permitido neste contrato. Ao fazer isso, você deverá respeitar todas as limitações técnicas do Conteúdo Licenciado que permitam seu uso apenas de determinadas formas. Exceto se expressamente permitido neste contrato, você não poderá:

- acessar nem permitir a nenhum indivíduo acesso ao Conteúdo Licenciado se eles não tiverem adquirido uma licença válida para o Conteúdo Licenciado,
- alterar, remover ou ocultar nenhum aviso de direito autoral ou outros avisos de proteção (inclusive marcas d'água), marcas ou identificações contidas no Conteúdo Licenciado,
- modificar ou criar um trabalho derivado de qualquer Conteúdo Licenciado,
- exibir publicamente ou tornar o Conteúdo Licenciado disponível para outros acessarem ou usarem,
- copiar, imprimir, instalar, vender, publicar, transmitir, emprestar, adaptar, reutilizar, vincular a ou publicar, tornar disponível ou distribuir o Conteúdo Licenciado a qualquer terceiro,
- contornar quaisquer limitações técnicas do Conteúdo Licenciado ou
- aplicar engenharia reversa, descompilar, remover ou, de outra maneira, impedir proteções ou desmontar o Conteúdo Licenciado, salvo e somente na medida em que essa atividade seja expressamente permitida pela lei aplicável, não obstante a presente limitação.

- 5. RESERVA DE DIREITOS E PROPRIEDADE.** A Microsoft se reserva todos os outros direitos que não foram expressamente concedidos a você neste contrato. O Conteúdo Licenciado é protegido por direitos autorais e outros tratados e leis de propriedade intelectual. A Microsoft ou seus fornecedores detêm o título, os direitos autorais e outros direitos de propriedade intelectual do Conteúdo Licenciado.
- 6. RESTRIÇÕES À EXPORTAÇÃO.** O Conteúdo Licenciado está sujeito às leis e aos regulamentos de exportação dos Estados Unidos. Você deverá cumprir todas as leis e os regulamentos internacionais e nacionais de exportação que se aplicam ao Conteúdo Licenciado. Essas leis incluem restrições relacionadas a destinos, usuários finais e uso final. Para obter informações adicionais, consulte o site www.microsoft.com/exporting.
- 7. SERVIÇOS DE SUPORTE.** Como o Conteúdo Licenciado é fornecido “no estado em que se encontra”, a Microsoft poderá não prestar serviços de suporte para ele.
- 8. RESCISÃO.** Sem prejuízo de quaisquer outros direitos, a Microsoft poderá rescindir este contrato caso você não cumpra qualquer de seus termos e condições. Mediante o término deste contrato por qualquer motivo, você interromperá imediatamente todo o uso de e excluirá e destruirá todas as cópias do Conteúdo Licenciado em seu poder ou sob seu controle.
- 9. LINKS PARA SITES DE TERCEIROS.** Você pode criar links para sites de terceiros por meio do uso do Conteúdo Licenciado. Os sites dos outros fabricantes não estão sob controle da Microsoft, e nem a Microsoft se responsabiliza pelo conteúdo de qualquer site de terceiros, por nenhum link presente nos sites de terceiros, ou por qualquer mudança ou atualização nos sites de terceiros. Nem a Microsoft é responsável pela transmissão pela Web nem por qualquer outra forma de transmissão recebida de qualquer site de terceiros. A Microsoft está fornecendo esses links a sites de terceiros para você somente como uma conveniência, e a inclusão de qualquer link não implica o aval da Microsoft ao respectivo site.
- 10. ACORDO INTEGRAL.** Este contrato e quaisquer termos adicionais do Conteúdo do Instrutor, atualizações e suplementos constituem o acordo integral do Conteúdo Licenciado, das atualizações e dos suplementos.
- 11. LEI APLICÁVEL.**
- a. Nos Estados Unidos. Se você tiver adquirido o Conteúdo Licenciado nos Estados Unidos, este contrato será regido e interpretado de acordo com as leis do Estado de Washington, que serão aplicadas às reclamações de violação de contrato, independentemente dos princípios de conflito de leis. As leis do estado no qual você reside regerão todas as outras reclamações, incluindo leis de defesa do consumidor, concorrência desleal e atos ilícitos extracontratuais.
 - b. Fora dos Estados Unidos. Caso você tenha adquirido este Conteúdo Licenciado em qualquer outro país, as leis desse país serão aplicáveis.
- 12. EFEITO LEGAL.** Este contrato descreve determinados direitos previstos em lei. Outros direitos podem ser conferidos a você de acordo com as leis do seu país. Você também poderá ter direitos em relação à parte de quem o Conteúdo Licenciado foi adquirido. Este contrato não altera seus direitos previstos nas leis do seu país, caso essas leis não o permitam.

13. ISENÇÃO DE GARANTIA. O CONTEÚDO LICENCIADO É LICENCIADO “NO ESTADO EM QUE SE ENCONTRA” E “CONFORME A DISPONIBILIDADE”. VOCÊ ASSUME O RISCO DE USÁ-LA. A MICROSOFT E SUAS RESPECTIVAS AFILIADAS NÃO OFERECEM OUTRAS GARANTIAS NEM CONDIÇÕES CONTRATUAIS. VOCÊ PODERÁ TER DIREITOS DE CONSUMIDOR ADICIONAIS DE ACORDO COM SUAS LEIS LOCAIS, OS QUAIS ESTE CONTRATO NÃO PODE ALTERAR. ATÉ O LIMITE PERMITIDO PELAS LEIS LOCAIS, A MICROSOFT E SUAS RESPECTIVAS AFILIADAS EXCLUEM TODAS E QUAISQUER GARANTIAS LEGAIS DE PADRÕES DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E NÃO VIOLAÇÃO.

14. LIMITAÇÕES E EXCLUSÕES DE RECURSOS E DANOS. A INDENIZAÇÃO DE DANOS DIRETOS PELA MICROSOFT, SUAS RESPECTIVAS AFILIADAS E SEUS FORNECEDORES RESTRINGE-SE AO VALOR DE US\$ 5,00. NÃO SERÁ POSSÍVEL RECUPERAR QUAISQUER OUTROS DANOS, INCLUSIVE DANOS CONSEQUENCIAIS, ESPECIAIS, INDIRETOS, INCIDENTAIS OU POR LUCROS CESSANTES.

Esta limitação se aplica a:

- toda e qualquer questão relacionada ao Conteúdo Licenciado, aos serviços ou ao conteúdo (inclusive código) em sites ou programas de terceiros e
- reclamações por violação de contrato, violação de garantia ou condição, responsabilidade objetiva, negligência ou outro ato ilícito extracontratual, de acordo com os termos da lei aplicável.

A limitação também se aplicará mesmo que a Microsoft saiba ou tenha sido avisada da possibilidade de danos. A limitação ou exclusão acima poderá não se aplicar a você se a legislação do seu país proibir, entre outros, a exclusão ou a limitação de danos incidentais ou consequenciais.

Nota: como este Conteúdo Licenciado é distribuído em Quebec, Canadá, algumas das cláusulas são fornecidas abaixo em francês.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection des consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 \$ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Revisado em junho de 2012

Módulo 1

Implementação de serviços de rede avançados

Conteúdo:

Lição 1: Configuração de recursos avançados de DHCP	14
Lição 2: Definição das configurações avançadas de DNS	16
Lição 3: Implementação de IPAM	19
Revisão e informações complementares do módulo	22
Perguntas e respostas da revisão do laboratório	24

Lição 1

Configuração de recursos avançados de DHCP

Conteúdo:

Demonstração

15

Demonstração

Demonstração: Configuração de failover de DHCP

Etapas da demonstração

Configure uma relação de failover de DHCP

1. Entre em LON-SVR1 como **Adatum\Administrador** com uma senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, clique em **Ferramentas** e, na lista suspensa, clique em **DHCP**. Observe que o servidor é autorizado, mas que nenhum escopo é configurado.
3. Alterne para LON-DC1. No Gerenciador do Servidor, clique em **Ferramentas** e, na lista suspensa, clique em **DHCP**.
4. No console DHCP, expanda **lon-dc1.adatum.com**, selecione e clique com o botão direito em **IPv4** e clique em **Configurar Failover**.
5. No Assistente de Configuração de Failover, clique em **Avançar**.
6. Na página **Especificar o servidor parceiro a ser usado para failover**, no campo **Servidor Parceiro**, insira **172.16.0.21** e clique em **Avançar**.
7. Na página **Criar uma nova relação de failover**, no campo **Nome da relação**, insira **Adatum**.
8. No campo **Prazo de Entrega Máximo do Cliente**, defina as horas como **zero** e defina os minutos como **15**.
9. Verifique se o campo **Modo** está definido como **Balancear carga**.
10. Verifique se o **Percentual de Balanceamento de Carga** está definido como **50%**.
11. Marque a caixa de seleção **Intervalo de Alternância de Estado**. Deixe o valor padrão de 60 minutos.
12. No campo **Habilitar Segredo Compartilhado de Autenticação de Mensagem**, digite **Pa\$\$w0rd** e clique em **Avançar**.
13. Clique em **Concluir** e clique em **Fechar**.
14. Alterne para LON-SVR1. Observe que o nó IPv4 é ativo.
15. Atualize o nó **IPv4**, expanda o nó **IPv4** e **Escopo**.
16. Clique em **Pool de Endereços** e observe que o pool de endereços está configurado.
17. Clique em **Opções de Escopo** e observe que as opções de escopo estão configuradas.
18. Feche o console DHCP em LON-DC1 e LON-SVR1.
19. Reverta LON-SVR1.

Lição 2

Definição das configurações avançadas de DNS

Conteúdo:

Demonstração

17

Demonstração

Demonstração: Configuração de DNSSEC

Etapas da demonstração

Configurar o DNSSEC

1. Entre em **LON-DC1** como **Adatum\Administrador** com uma senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, clique em **Ferramentas** e, na lista suspensa, clique em **DNS**.
3. No DNS, expanda **LON-DC1**, expanda **Zonas de Pesquisa Direta** e selecione e clique com o botão direito em **Adatum.com**.
4. No menu, clique em **DNSSEC > Assinar a Zona**.
5. No Assistente de Assinatura de Zona, clique em **Avançar**.
6. Clique em **Personalize os parâmetros de assinatura da zona** e clique em **Avançar**.
7. Na página **Mestre de Chave**, clique em **O servidor DNS LON-DC1 é o Mestre de Chave**. Clique em **Avançar**.
8. Na página **Chave KSK**, clique em **Avançar**.
9. Na página **Chave KSK**, clique em **Adicionar**.
10. Na página **Nova Chave KSK**, clique em **OK**.
11. Na página **Chave KSK**, clique em **Avançar**.
12. Na página **ZSK (Chave de Assinatura da Área)**, clique em **Avançar**.
13. Na página **ZSK (Chave de Assinatura da Área)**, clique em **Adicionar**.
14. Na página **Nova ZSK (Chave de Assinatura da Área)**, clique em **OK**.
15. Na página **ZSK (Chave de Assinatura da Área)**, clique em **Avançar**.
16. Na página **NSEC (Next Secure)**, clique em **Avançar**.
17. Na página **Âncoras de Confiança (TAs)**, marque a caixa de seleção **Habilitar a distribuição de âncoras de confiança nesta zona** e então clique em **Avançar**.
18. Na página **Parâmetros de Assinatura e Sondagem**, clique em **Avançar**.
19. Na página **Extensões de Segurança DNS (DNSSEC)**, clique em **Avançar** e clique em **Concluir**.
20. Em Gerenciador DNS, expanda **Pontos de Confiança**, expanda **com** e clique em **Adatum**. Verifique se os registros de recurso DNSKEY existem e se seu status é válido.
21. No Gerenciador do Servidor, clique em **Ferramentas** e, na lista suspensa, clique em **Gerenciamento de Política de Grupo**.
22. No GPMC (Console de Gerenciamento de Política de Grupo), expanda **Floresta: Adatum.com, Domínios e Adatum.com**, clique com o botão direito do mouse em **Default Domain Policy** e clique em **Editar**.

23. No Editor de Gerenciamento de Política de Grupo, em **Configuração do Computador**, expanda **Políticas e Configurações do Windows** e clique na pasta **Política de Resolução de Nome**.
24. Na seção Criar Regras, no campo **Sufixo**, digite **Adatum.com** para aplicar a regra ao sufixo do namespace.
25. Marque a caixa de seleção **Habilitar DNSSEC nesta regra**.
26. Marque a caixa de seleção **Exigir que clientes DNS verifiquem se os dados de nome e endereço foram validados pelo servidor DNS** e clique em **Criar**.
27. Feche todas as janelas abertas.

Lição 3

Implementação de IPAM

Conteúdo:

Demonstração

20

Demonstração

Demonstração: Instalação e configuração do IPAM

Etapas da demonstração

Instalar o IPAM

1. Entre em **LON-SVR2** como **Adatum\Administrador** com uma senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, clique em **Adicionar funções e recursos**.
3. No Assistente de Adição de Funções e Recursos, clique em **Avançar**.
4. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
5. Na página **Selecionar servidor de destino**, clique em **Próximo**.
6. Na página **Selecionar funções do servidor**, clique em **Próximo**.
7. Na página **Selecionar recursos**, marque a caixa de seleção **Servidor de Gerenciamento de Endereços IP (IPAM)**.
8. No menu pop-up **Adicionar recursos que são necessários para Servidor de Gerenciamento de Endereços IP (IPAM)**, clique em **Adicionar recursos** e clique em **Próximo**.
9. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
10. Quando o Assistente de Adição de Funções e Recursos for concluído, feche o assistente.

Configurar o IPAM

1. No painel de navegação do Gerenciador do Servidor, clique em **IPAM**.
2. No painel Visão Geral de IPAM, clique em **Conectar a servidor IPAM**. Clique em **LON-SVR2.Adatum.com** e clique em **OK**.
3. Clique em **Provisionar o servidor IPAM**.
4. No Assistente para Provisionar IPAM, clique em **Próximo**.
5. Na página **Selecione o método de provisionamento**, verifique se **Com base na Política de Grupo** está selecionado, na caixa **Prefixo do nome de GPO**, digite **IPAM** e clique em **Próximo**.
6. Na página **Confirmar as Configurações**, clique em **Aplicar**. O provisionamento levará alguns minutos para terminar.
7. Quando o provisionamento terminar, clique em **Fechar**.
8. No painel Visão Geral de IPAM, clique em **Configurar descoberta de servidor**.
9. Na caixa de diálogo **Configurar Descoberta de Servidor**, clique em **Adicionar** para adicionar o domínio Adatum.com e clique em **OK**.
10. No painel Visão Geral de IPAM, clique em **Iniciar descoberta de servidor**. A descoberta pode levar de 5 a 10 minutos para ser executada. A barra amarela indica quando a descoberta é concluída.

11. No painel Visão Geral de IPAM, clique em **Selecionar ou adicionar servidores para gerenciar e verificar o acesso ao IPAM**. Observe se o Status de Acesso do IPAM está bloqueado. Role até a exibição Detalhes e observe o relatório de status. O servidor IPAM ainda não recebeu nenhuma permissão para gerenciar LON-DC1 por Política de Grupo.
12. Na barra de tarefas, clique com o botão direito do mouse no ícone do Windows PowerShell e clique em **Executar como Administrador**.
13. No prompt do Windows PowerShell®, digite o comando a seguir e pressione Enter:

```
Invoke-IPAMGpoProvisioning -Domain Adatum.com -GpoPrefixName IPAM -IPAMServerFqdn LON-SVR2.adatum.com -DelegatedGpoUser Administrador
```

14. Quando você precisar confirmar a ação, digite **S** e pressione Enter. O comando levará alguns minutos para terminar.
15. Feche o Windows PowerShell.
16. Alterne para Gerenciador do Servidor. No painel de detalhes IPv4, clique com o botão direito do mouse em **LON-DC1** e clique em **Editar Servidor**.
17. Na caixa de diálogo **Adicionar ou Editar Servidor**, defina o campo **Status da capacidade de gerenciamento** como **Gerenciado** e clique em **OK**.
18. Alterne para **LON-DC1**.
19. Na barra de tarefas, clique no ícone Windows PowerShell.
20. No prompt do Windows PowerShell, digite **Gpupdate /force** e pressione Enter.
21. Feche o Windows PowerShell.
22. Volte a LON-SVR2 e, em Gerenciador do Servidor, clique com o botão direito do mouse em LON-DC1 e clique em **Atualizar Status de Acesso do Servidor**. A descoberta pode levar de 5 a 10 minutos para ser executada. A barra amarela indica quando a descoberta é concluída. Depois que descoberta for concluída, atualize IPv4 clicando no ícone **Atualizar**. Pode levar até 5 minutos para o status mudar.
23. No painel Visão Geral de IPAM, clique em **Recuperar dados de servidores gerenciados**. Essa ação levará alguns minutos para terminar.

Revisão e informações complementares do módulo

Prática recomendada

- Implemente o failover de DHCP para garantir que os computadores cliente possam continuar recebendo informações de configuração de IP no caso de uma falha de servidor.
- Verifique se há pelo menos dois servidores DNS hospedando cada zona.
- Use o IPAM para controlar a distribuição de endereços IP e atribuições de endereço estático.

Perguntas de revisão

Pergunta: Qual é uma das desvantagens de usar o IPAM?

Resposta: Se você usar o IPAM, não poderá gerenciar dispositivos de rede habilitados para DHCP (como gateways e WAPs) no console de gerenciamento do IPAM.

Problemas e cenários reais

Alguns clientes de rede estão recebendo a configuração de DHCP incorreta. Qual ferramenta você deve usar para começar o processo de solução de problemas?

Resposta: Alguns clientes de rede estão recebendo a configuração de DHCP incorreta. Qual ferramenta você deve usar para começar o processo de solução de problemas?

Quais são algumas possíveis causas das configurações incorretas?

Resposta: Pode haver um servidor DHCP antigo na rede. Coisas comuns a serem procuradas serão dispositivos de gateway, como modems a cabo ou PBX (central privada de comutação telefônica), que têm um componente de DHCP habilitado. Outra possibilidade é que alguém tenha configurado o endereço IP manualmente no cliente.

Ferramentas

Ferramenta	Uso	Local
Dnscmd	Configure todos os aspectos do gerenciamento de DNS	%systemroot%\System32\dnscmd.exe
Console DHCP	Controle todos os aspectos do gerenciamento de DHCP de uma interface do usuário	%systemroot%\System32\dhcpcmgmt.msc
Console de DNS	Controle todos os aspectos do gerenciamento de DNS de uma interface do usuário	%systemroot%\System32\dnsmgmt.msc
Console de gerenciamento do IPAM	Controle todos os aspectos do gerenciamento de IPAM	Gerenciador do Servidor

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
Os usuários não podem mais acessar o site de um fornecedor que podiam acessar historicamente.	O endereço IP do site pode ter sido alterado, mas o bloqueio de cache de DNS não está atualizando o endereço IP armazenado em cache para FQDN porque o TTL do registro ainda não expirou. Você deve limpar o cache manualmente no servidor DNS.
Os servidores gerenciados não podem se conectar ao servidor IPAM.	Verifique se o serviço Banco de Dados Interno do Windows e o serviço Ativação de Processos do Windows estão em execução no servidor IPAM.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação de serviços de rede avançados

Pergunta: Os computadores cliente deixarão de se comunicar imediatamente na rede se não houver nenhum servidor DHCP funcionando?

Resposta: Não, os computadores cliente continuarão funcionando normalmente na rede até a concessão no endereço IP expirar.

Pergunta: Qual é o tamanho padrão do pool de soquetes DNS?

Resposta: O tamanho padrão do pool de soquetes DNS é 2.500.

Pergunta: Qual valor o bloqueio de cache de DNS usa para determinar quando atualizar um endereço IP no cache de DNS?

Resposta: A determinação é feita baseada no valor TTL (Vida útil) do registro de endereço desde o registro de recurso SOA (início de autoridade).

Módulo 2

Implementação de serviços de arquivo avançados

Conteúdo:

Lição 1: Configuração do armazenamento iSCSI	26
Lição 2: Configuração de BranchCache	30
Lição 3: Otimização do uso de armazenamento	33
Revisão e informações complementares do módulo	37
Perguntas e respostas da revisão do laboratório	40

Lição 1

Configuração do armazenamento iSCSI

Conteúdo:

Perguntas e respostas	27
Leitura adicional	27
Demonstração	27

Perguntas e respostas

O que é iSCSI?

Pergunta: Você pode usar a rede TCP/IP interna de sua organização para fornecer iSCSI?

Resposta: Sim, é possível. Porém, como prática recomendada, você deve ter uma rede TCP/IP dedicada para iSCSI de forma que outro tráfego de rede não interfira na comunicação iSCSI e, assim, a comunicação iSCSI não interfira no tráfego de rede.

Servidor de destino iSCSI e iniciador iSCSI

Pergunta: Quando você pensa em implementar a inicialização sem disco a partir de destinos iSCSI?

Resposta: As respostas variarão com base na experiência, mas você poderia considerar isso principalmente se desejar implementar tecnologias de virtualização como uma VDI (Infraestrutura de Área de Trabalho Virtual) em sua organização.

Leitura adicional

Servidor de destino iSCSI e iniciador iSCSI

 **Leitura adicional:** Para obter mais informações sobre a introdução de destinos iSCSI no Windows Server 2012, consulte: <http://go.microsoft.com/fwlink/?LinkId=270038>
(*Alguns dos sites abordados neste curso pode ser em Inglês*)

Demonstração

Demonstração: Configuração de um destino iSCSI

Etapas da demonstração

Adicionar o serviço de função de servidor de destino iSCSI

1. Em LON-DC1, em Gerenciador do Servidor, clique em **Gerenciar** e clique em **Adicionar funções e recursos**.
2. No Assistente de Adição de Funções e Recursos, na página **Antes de começar**, clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
4. Na página **Selecionar servidor de destino**, verifique se **Selecionar um servidor no pool de servidor** está selecionado e clique em **Próximo**.
5. Na página **Selecionar funções do servidor**, expanda **Serviços de Arquivo e Armazenamento (Instalado)**, expanda **Serviços de Arquivo e iSCSI**, marque a caixa de seleção **Servidor de Destino iSCSI** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
8. Quando a instalação for concluída, clique em **Fechar**.

Criar dois discos virtuais iSCSI e um destino iSCSI

1. Em LON-DC1, no Gerenciador do Servidor, no painel de navegação, clique em **Serviços de Arquivo e Armazenamento**.
2. No painel Serviços de Arquivo e Armazenamento, clique em **iSCSI**.
3. No painel DISCOS VIRTUAIS iSCSI, clique em **TAREFAS** e, na caixa de listagem suspensa **TAREFAS**, clique em **Novo Disco Virtual iSCSI**.
4. No Assistente de Novo Disco Virtual iSCSI, na página **Selecionar localização do disco virtual iSCSI**, em **Localização do armazenamento**, clique em na unidade **C** e clique em **Próximo**.
5. Na página **Especificar nome do disco virtual iSCSI**, digite **iSCSIDisk1** e clique em **Próximo**.
6. Na página **Especificar tamanho do disco virtual iSCSI**, na caixa **Tamanho**, digite **5**, na caixa de listagem suspensa, verifique se **GB** está selecionado e clique em **Próximo**.
7. Na página **Atribuir destino iSCSI**, clique em **Novo destino iSCSI** e clique em **Próximo**.
8. Na página **Especificar nome de destino**, na caixa **Nome**, digite **LON-SVR2** e clique em **Próximo**.
9. Na página **Especificar servidores de acesso**, clique em **Adicionar**.
10. Na caixa de diálogo **Selecionar um método para identificar o iniciador**, clique em **Inserir um valor para o tipo selecionado**, na caixa de listagem suspensa **Tipo**, clique em **Endereço IP**, no campo **Valor**, digite **172.16.0.22** e clique em **OK**.
11. Na página **Especificar servidores de acesso**, clique em **Próximo**.
12. Na página **Habilitar Autenticação**, clique em **Próximo**.
13. Na página **Confirmar seleções**, clique em **Criar**.
14. Na página **Exibir resultados**, espere até a criação terminar e clique em **Fechar**.
15. No painel DISCOS VIRTUAIS iSCSI, clique em **TAREFAS** e, na caixa de listagem suspensa **TAREFAS**, clique em **Novo Disco Virtual iSCSI**.
16. No Assistente de Novo Disco Virtual iSCSI, na página **Selecionar localização do disco virtual iSCSI**, em **Localização do armazenamento**, clique em na unidade **C** e clique em **Próximo**.
17. Na página **Especificar nome do disco virtual iSCSI**, digite **iSCSIDisk2** e clique em **Próximo**.
18. Na página **Especificar tamanho do disco virtual iSCSI**, na caixa **Tamanho**, digite **5**, na caixa de listagem suspensa, verifique se **GB** está selecionado e clique em **Próximo**.
19. Na página **Atribuir destino iSCSI**, clique em **lon-svr2** e clique em **Próximo**.
20. Na página **Confirmar seleções**, clique em **Criar**.
21. Na página **Exibir resultados**, espere até a criação terminar e clique em **Fechar**.

Demonstração: Conexão ao armazenamento iSCSI

Etapas da demonstração

Etapas de preparação

Antes de iniciar esta demonstração, execute as etapas a seguir:

1. No computador host, clique no ícone **Gerenciador Hyper-V** na barra de tarefas.
2. No console Gerenciador Hyper-V, clique com o botão direito em **24412B-LON-SVR2**, e clique em **Configurações**.
3. Na janela **Configurações de 24412B-LON-SVR2**, no painel esquerdo, verifique se ambos os adaptadores de rede herdados estão conectados a **Rede Privada**.
4. Se um adaptador de rede herdado tiver um status **Não conectado**, clique em **Adaptador de Rede Herdado** e, no painel direito, na lista suspensa **Rede**, selecione **Rede Privada** e clique em **OK**.

Conectar ao destino iSCSI

1. Em LON-SVR2, no Gerenciador do Servidor, clique no menu **Ferramentas** e clique em **Iniciador iSCSI**.
2. Na caixa de mensagem **Microsoft iSCSI**, clique em **Sim**.
3. Na caixa de diálogo **Propriedades do Iniciador iSCSI**, na guia **Destinos**, digite **LON-DC1** e clique em **Conectar Rápido**.
4. Na janela Conexão Rápida, na seção **Destinos descobertos**, clique em **iqn.1991-05.com.microsoft:lon-dc1-lon-svr2-target** e clique em **Concluído**.
5. Na caixa de diálogo **Propriedades do Iniciador iSCSI**, clique em **OK** para fechar a caixa de diálogo.

Verificar a presença da unidade iSCSI

1. Em LON-SVR2, em Gerenciador do Servidor, no menu **Ferramentas**, clique em **Gerenciamento do Computador**.
2. No console Gerenciamento do Computador, no **nó Armazenamento**, clique em **Gerenciamento de Disco**. Note que os novos discos são adicionados. Porém, todos eles estão atualmente offline e não formatados.
3. Feche o console Gerenciamento do Computador.



Observação: Deixe os computadores funcionando, pois você precisará deles para a próxima demonstração.

Lição 2

Configuração de BranchCache

Conteúdo:

Demonstração

31

Demonstração

Demonstração: Configuração de BranchCache

Etapas da demonstração

Adicionar o BranchCache para o serviço de função Arquivos de Rede

1. No LON-DC1, no Gerenciador do Servidor, clique em **Adicionar funções e recursos**.
2. No Assistente de Adição de Funções e Recursos, na página **Antes de começar**, clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
4. Na página **Selecionar servidor de destino**, verifique se **Selecionar um servidor no pool de servidor** está selecionado e clique em **Próximo**.
5. Na página **Selecionar funções do servidor**, expanda **Serviços de Arquivo e Armazenamento (Instalado)**, expanda **Serviços de Arquivo e iSCSI**, marque a caixa de seleção **BranchCache para arquivos de rede** e clique em **Avançar**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
8. Quando a instalação for concluída, clique em **Fechar**.

Habilitar o BranchCache para o servidor

1. Em LON-DC1, clique na tela inicial.
2. Na tela inicial, digite **gpedit.msc** e pressione ENTER.
3. Expanda **Configuração do Computador**, expanda **Modelos Administrativos**, expanda **Rede**, clique em **Lanman Server** e clique duas vezes em **Publicação de Hash para BranchCache**.
4. Na caixa de diálogo **Publicação de Hash para BranchCache**, clique em **Habilitado**.
5. Na caixa **Opções**, em **Ações da publicação de hash**: selecione **Permitir publicação de hash somente para a pasta compartilhada na qual o BranchCache está habilitado** e clique em **OK**.
6. Feche o Editor de Política de Grupo Local.

Habilitar o BranchCache para um compartilhamento de arquivos

1. Na barra de tarefas, clique no ícone do Explorador de Arquivos.
2. Na janela do Explorador de Arquivos, clique em **Disco Local (C:)**.
3. Na barra de acesso rápida localizada no lado superior esquerdo da janela, clique em **Nova Pasta**, digite **Share** e pressione Enter.
4. Clique com o botão direito do mouse do mouse em **Share** e clique em **Propriedades**.
5. Na caixa de diálogo **Propriedades de Share**, clique na guia **Compartilhamento** e clique em **Compartilhamento Avançado**.

6. Na caixa de diálogo **Compartilhamento Avançado**, clique em **Compartilhar esta pasta** e clique em **Cache**.
7. Na caixa de diálogo **Configurações Offline**, marque a caixa de seleção **Habilitar BranchCache** e clique em **OK**.
8. Na caixa de diálogo **Compartilhamento Avançado**, clique em **OK** e clique em **Fechar**.
9. Feche todas as janelas abertas.

Lição 3

Otimização do uso de armazenamento

Conteúdo:

Perguntas e respostas	34
Leitura adicional	34
Demonstração	34

Perguntas e respostas

O que é o Gerenciador de Recursos de Servidor de Arquivos?

Pergunta: Você está usando o FSRM atualmente no Windows Server 2008 R2? Em caso afirmativo, para que áreas você o utiliza?

Resposta: As respostas variarão com base nas experiências dos alunos com o FSRM no Windows Server 2008 R2. O FSRM é usado nas seguintes áreas:

- Infraestrutura de classificação de arquivos
- Tarefas de gerenciamento de arquivos
- Gerenciamento de cota
- Gerenciamento de triagem de arquivo

Leitura adicional

O que é o Gerenciador de Recursos de Servidor de Arquivos?



Leitura adicional: Para obter mais informações sobre FSRM, consulte Novidades em Gerenciador de Recursos de Servidor de Arquivos em <http://go.microsoft.com/fwlink/?LinkId=270039>.

Demonstração

Demonstração: Configuração da classificação de arquivos

Etapas da demonstração

1. Em LON-SVR1, o console Gerenciador do Servidor deve abrir automaticamente. No console Gerenciador do Servidor, no canto superior direito, clique em **Ferramentas** e clique em **Gerenciador de Recursos de Servidor de Arquivos**.
2. Em Gerenciador de Recursos de Servidor de Arquivos, expanda **Gerenciamento de Classificação**, clique e clique com o botão direito em **Propriedades de Classificação** e clique em **Criar Propriedade Local**.
3. Na janela Criar Propriedade de Classificação Local, no campo **Nome**, digite **Corporate Documentation**, na caixa de listagem suspensa **Tipo de Propriedade**, verifique se **Sim/Não** está selecionado e clique em **OK**.
4. Em Gerenciador de Recursos de Servidor de Arquivos, expanda **Gerenciamento de Classificação**, clique em **Regras de Classificação** e, no painel Ação, clique em **Criar Regra de Classificação**.
5. Na janela Criar Regra de Classificação, na guia **Geral**, no campo **Nome da regra**, digite **Regra de Documentos Corporativos** e verifique se a caixa de seleção **Habilitar** está marcada.

6. Na janela Criar Regra de Classificação, na guia **Escopo**, clique em **Adicionar**.
7. Na janela Procurar Pasta, expanda **Allfiles (E:\)**, **Labfiles**, clique na pasta **Corporate Documentation** e clique em **OK**.
8. Na janela Criar Regra de Classificação, na guia **Classificação**, na caixa de listagem suspensa **Método de classificação**, clique em **Classificador de Pasta**. Na caixa de listagem suspensa **Propriedade - Escolher uma propriedade a ser atribuída a arquivos**, clique em **Corporate Documentation** e, na caixa de listagem suspensa **Propriedade - Especifique um valor**, clique em **Sim**.
9. Na janela Criar Regra de Classificação, na guia **Tipo de Avaliação**, clique em **Reavaliar os valores de propriedade existentes**, verifique se o botão de opção **Agregar os valores** está selecionado e clique em **OK**.
10. Em Gerenciador de Recursos de Servidor de Arquivos, no painel Ação, clique em **Executar Classificação Agora com Todas as Regras**.
11. Na janela Executar classificação, selecione o botão de opção **Esperar a conclusão da classificação** e clique em **OK**.
12. Revise o **Relatório de classificação automática** que é exibido no Windows Internet Explorer® e verifique se o relatório lista o mesmo número de arquivos classificados como na pasta **Documentação Corporativa**.
13. Feche o Internet Explorer.

Demonstração: Configuração da eliminação da duplicação de dados

Etapas da demonstração

Adicionar o serviço de função de eliminação de duplicação de dados

1. Em LON-SVR1, em Gerenciador do Servidor, clique no menu **Gerenciar** e clique em **Adicionar funções e recursos**.
2. No Assistente de Adição de Funções e Recursos, na página **Antes de começar**, clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
4. Na página **Selecionar um servidor de destino**, verifique se **Selecionar servidor no pool de servidor** está selecionado e clique em **Próximo**.
5. Na página **Selecionar funções do servidor**, expanda **Serviços de Arquivo e Armazenamento (Instalado)**, expanda **Serviços de Arquivo e iSCSI**, marque a caixa de seleção **Desduplicação de Dados** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Confirmar seleções de instalação**, clique em **Próximo**.
8. Quando a instalação for concluída, clique em **Fechar**.

Habilitar a eliminação de duplicação de dados

1. No Gerenciador do Servidor, no painel de navegação, clique em **Serviços de Arquivo e Armazenamento**.
2. No painel Serviços de Arquivo e Armazenamento, clique em **Volumes**.
3. No painel Volumes, clique com o botão direito na unidade **E:** e, na caixa de listagem suspensa, clique em **Configurar Eliminação da Duplicação de Dados**.
4. Na caixa de diálogo **Configurações de Eliminação de Duplicação de Allfiles (E:\)**, marque a caixa de seleção **Habilitar a eliminação de duplicação de dados**, na caixa **Eliminar duplicações de arquivos com mais de (em dias)**, digite **3** e clique em **Definir Agenda de Eliminação de Duplicação**.
5. Na caixa de diálogo **Agenda de Eliminação de Duplicação de LON-SVR1**, clique em **Habilitar otimização de processamento**, na caixa de listagem suspensa **Hora inicial**, clique na hora atual e clique em **OK**.
6. Na caixa de diálogo **Configurações de Eliminação de Duplicação de Allfiles (E:\)**, clique em **OK**.

Testar a eliminação de duplicação de dados

1. Em LON-SVR1, abra uma janela Explorador de Arquivos, navegue até a unidade E:, clique com o botão direito no arquivo **OBSInstaller.exe** e clique em **Copiar**.
2. Cole o arquivo **OBSInstaller.exe** nas pastas **LabFiles**.
3. Em LON-SVR1, abra a pasta E:\LabFiles, clique com o botão direito do mouse em **OBSInstaller.exe** e clique em **Propriedades**.
4. Na caixa de diálogo **Propriedades**, observe os valores para **Tamanho** e **Tamanho em Disco**.
5. Repita as etapas 5 a 7 para **OBSInstaller.exe** na pasta raiz da unidade **E:** unidade.
6. Em LON-SVR1, abra a janela do Windows PowerShell.
7. No prompt do Windows PowerShell, digite o seguinte cmdlet e pressione Enter:

```
Start-DedupJob -Type Optimization -Volume E:
```

8. Digite **Get-DedupJob** e pressione Enter. Verifique se o processo está em execução.
9. Espere um ou dois minutos e repita o comando **Get-Dedupjob**.
10. Se você não obtiver nenhum resultado, isso significará que o trabalho de eliminação de duplicação foi concluído.
11. Na pasta raiz da unidade **E:**, clique com o botão direito em **OBSInstaller.exe** e clique em **Propriedades**.
12. Na caixa de diálogo **Propriedades**, observe os valores para **Tamanho** e **Tamanho em Disco**. O tamanho no disco deve ser muito menor do que era anteriormente.

Revisão e informações complementares do módulo

Prática recomendada

- Ao considerar uma solução de armazenamento iSCSI para sua organização, gaste a maioria do tempo no processo de design. O processo de design é crucial porque permite otimizar a solução para todas as tecnologias que usarão o armazenamento iSCSI, como serviços de arquivo, Exchange Server e SQL Server. O design também deve acomodar o crescimento futuro dos dados comerciais de suas organizações. Bons processos de design garantem uma implantação com êxito da solução que satisfará os requisitos comerciais de sua organização.
- Ao planejar a implantação do BranchCache, trabalhe de perto com seus administradores de rede para otimizar o tráfego de rede pela WAN.
- Ao planejar classificações de arquivo, comece com os requisitos comerciais de sua organização. Identifique as classificações que você aplicará aos documentos e defina um método que você usará para identificar documentos para classificação. Antes de você implantar a infraestrutura de classificação de arquivo, crie um ambiente de teste e teste os cenários para garantir que sua solução resultará em uma implantação com êxito, e que os requisitos comerciais de suas organizações serão satisfeitos.

Perguntas de revisão

Pergunta: Como o BranchCache difere do Sistema de Arquivos Distribuídos?

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.

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

Resposta: Quando você usa o modo de cache distribuído, o cache é distribuído a todos os computadores que executam o Windows 8. Porém, é provável que computadores ou laptops que estão executando o Windows 8 sejam desligados ou removidos do escritório. Isso significa que um arquivo armazenado em cache pode não estar disponível, o que o forçará a ser baixado por um link WAN novamente. Porém, o modo de cache hospedado será usado provavelmente quando um computador que está executando o sistema operacional Windows Server 2012 estiver disponível na filial.

Pergunta: Você pode configurar Eliminação de duplicação de dados em um volume de inicialização?

Resposta: Não, você não pode configurar Eliminação de duplicação de dados em um volume de inicialização. Você só pode configurar a Eliminação de duplicação de dados em volumes que não são volumes de sistema ou inicialização. A Eliminação de duplicação de dados também não é suportada no ReFS (Sistema de Arquivos Resiliente).

Pergunta: Por que você implementaria uma infraestrutura de classificação de arquivo?

Resposta: A infraestrutura de classificação de arquivo permite gerenciar grupos de arquivos com base em vários atributos de arquivo e pasta. Usando essa tecnologia, você pode automatizar tarefas de manutenção de arquivos e pastas, como limpar dados obsoletos ou proteger informações confidenciais.

Problemas e cenários reais

Sua organização está pensando em implantar uma solução iSCSI. Você é um administrador do Windows Server 2012 é responsável por criar e implantar a nova solução. Essa nova solução será usada por um tipo diferente de tecnologias, como o servidor de arquivos Windows Server 2012, o Exchange Server e o SQL Server. Você está enfrentando um desafio de criar uma solução iSCSI ideal, mas, ao mesmo tempo, você não sabe ao certo se a solução que vai propor para sua organização satisfará os requisitos de todas as tecnologias que acessarão o armazenamento iSCSI. O que fazer?

Resposta: Você deve incluir na equipe que criará e implantará a solução iSCSI especialistas de áreas diferentes de especialização. Membros da equipe que serão envolvidos no projeto devem incluir administradores do Windows Server 2012, administradores de rede, administradores de armazenamento e administradores de segurança. Isso é necessário de forma que a solução de armazenamento iSCSI tenha um ótimo desempenho e segurança e tenha procedimentos consistentes de gerenciamento e de operações.

Sua organização está pensando em implantar uma solução BranchCache. Você é um administrador do Windows Server 2012 em sua organização responsável por criar e implantar a nova solução. Os gerenciadores comerciais da organização estão preocupados com a segurança dos dados que serão armazenados nas filiais. Eles também estão preocupados sobre como a organização eliminará riscos de segurança como falsificação de dados, revelação de informações e ataques de negação de serviço. O que fazer?

Resposta: Você deve incluir um especialista de segurança em sua equipe de design. Você também deve considerar o modelo de proteção em camadas de análise de riscos de segurança. O BranchCache elimina os riscos de segurança do seguinte modo:

- Violação de dados. A tecnologia BranchCache usa hashes para confirmar se, durante a comunicação, o computador cliente e o servidor não alteraram os dados.
- Divulgação de informações. O BranchCache envia conteúdo criptografado a clientes, mas eles devem ter a chave de criptografia para descriptografar o conteúdo. Como o usuário mal-intencionado em potencial não teria a chave de criptografia, se um invasor tentar monitorar o tráfego de rede para acessar os dados enquanto estiverem em trânsito entre clientes, a tentativa não terá nenhum êxito.
- Negação de serviço. Se um invasor tentar sobrecarregar o cliente com solicitações para obter dados, a tecnologia BranchCache incluirá contadores e temporizadores de gerenciamento de fila para impedir que os clientes sejam sobrecarregados.

Sua organização está usando grandes quantidades de espaço em disco para armazenamento de dados e está enfrentando um desafio de organizar e gerenciar os dados. Além disso, sua organização deve satisfazer requisitos de segurança, conformidade e prevenção de vazamento de dados das informações confidenciais da empresa. O que fazer?

Resposta: Você deve implantar a infraestrutura de classificação de arquivo. Com base na classificação do arquivo, você pode configurar tarefas de gerenciamento de arquivo que permitirão gerenciar grupos de arquivos baseado em vários atributos de arquivo e pasta. Você também pode automatizar tarefas de manutenção de arquivos e pastas, como limpar dados obsoletos ou proteger informações confidenciais.

Ferramentas

Ferramenta	Uso	Onde encontrar
Servidor de destino iSCSI	Configurar destinos iSCSI	Em Gerenciador do Servidor, em Servidores de Arquivo e Armazenamento
Iniciador iSCSI	Configure um cliente para conectar a um disco virtual de destino iSCSI	Em Gerenciador do Servidor, na caixa de listagem suspensa Ferramentas
Ferramenta Avaliação de Eliminação de Duplicação (DDPEval.exe)	Analise um volume para descobrir as economias em potencial ao habilitar Eliminação de duplicação de dados	C:\windows\system32
Gerenciador de Recursos de Servidor de Arquivos	Um conjunto de recursos que permitem gerenciar e classificar dados que são armazenados em servidores de arquivos	Gerenciador do Servidor

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do BranchCache

Pergunta: Neste laboratório, você moveu LON-SVR1 para sua própria OU (unidade organizacional). Por quê?

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

Pergunta: Quando você pensaria em implementar o BranchCache em sua própria organização?

Resposta: As respostas variarão, mas o BranchCache só será importante se você tiver uma filial ou um local que esteja conectado à sede de sua organização com um link de pouca largura de banda.

Módulo 3

Implementação do Controle de Acesso Dinâmico

Conteúdo:

Revisão e informações complementares do módulo	42
Perguntas e respostas da revisão do laboratório	44

Revisão e informações complementares do módulo

Prática recomendada

- Use políticas de acesso central em vez de configurar expressões condicionais em recursos.
- Habilite as configurações de Assistência para Acesso Negado.
- Sempre teste as alterações feitas a regras e políticas de acesso central antes de implementá-las.
- Use classificações de arquivos para atribuir propriedades a arquivos.

Perguntas de revisão

Pergunta: O que é uma declaração?

Resposta: Uma declaração consiste em informações que o AD DS informa sobre um objeto, que em geral é um usuário ou um computador.

Pergunta: Qual é a finalidade das políticas de acesso central?

Resposta: As políticas de acesso central permitem que os administradores criem políticas que serão aplicadas a um ou mais servidores de arquivos em uma organização. As políticas de acesso central contêm uma ou mais regras. Cada regra contém configurações que determinam sua aplicabilidade e suas permissões.

Pergunta: O que é a Assistência para acesso negado?

Resposta: A Assistência para Acesso Negado é um novo recurso do Windows Server 2012 que ajuda os usuários a responder a problemas de acesso negado antes de ligar para o suporte técnico. A Assistência para Acesso Negado fornece informações sobre o problema e direciona os usuários para o lugar apropriado para obter assistência.

Ferramentas

Ferramenta	Uso	Local
Centro Administrativo do Active Directory	Administração e criação de declarações, propriedades de recursos, regras e políticas	Ferramentas administrativas
Console de Gerenciamento de Política de Grupo (GPMC)	Gerenciamento da política de grupo	Ferramentas administrativas
Editor de Gerenciamento de Política de Grupo	Edição de GPOs (Objetos de Política de Grupo)	GPMC

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
As declarações não são preenchidas com os valores apropriados.	Verifique se o atributo correto está selecionado para a declaração. Além disso, verifique se o valor do atributo para um objeto específico está preenchido.
Uma expressão condicional não permite o acesso.	Verifique se a expressão está definida corretamente. Além disso, tente usar a guia Acesso Efetivo para solucionar o problema.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do Controle de Acesso Dinâmico

Pergunta: Existem declarações padrão definidas para os usuários?

Resposta: Não, você deve definir as declarações para os usuários.

Pergunta: Como as classificações de arquivos aprimoram o Controle de Acesso Dinâmico?

Resposta: Usando as classificações de arquivos, você pode definir atributos em arquivos automaticamente e então usar esses atributos em expressões condicionais ao implementar o Controle de Acesso Dinâmico.

Pergunta: É possível implementar o Controle de Acesso Dinâmico sem usar uma política de acesso central?

Resposta: Sim, você pode definir expressões condicionais diretamente nos recursos.

Módulo 4

Implementação de implantações distribuídas dos Serviços de Domínio do Active Directory

Conteúdo:

Lição 1: Visão geral de implantações distribuídas do AD DS	46
Lição 2: Implantação de um ambiente distribuído do AD DS	48
Lição 3: Configuração de relações de confiança do AD DS	51
Revisão e informações complementares do módulo	54
Perguntas e respostas da revisão do laboratório	55

Lição 1

Visão geral de implantações distribuídas do AD DS

Conteúdo:

Perguntas e respostas

47

Perguntas e respostas

Discussão: Visão geral dos componentes do AD DS

Pergunta: O que é um domínio AD DS?

Resposta: Um domínio do AD DS é um agrupamento lógico de objetos de usuário, computador e grupo para fins de gerenciamento e segurança. Todos esses objetos são armazenados no banco de dados do AD DS, e uma cópia desses dados é armazenada em cada controlador de domínio no domínio do AD DS. Por isso, o banco de dados do AD DS é tolerante a falhas e os clientes podem acessar as informações de domínio AD DS em qualquer controlador de domínio do AD DS no domínio AD DS. O AD DS oferece um diretório hierárquico pesquisável, além de uma estrutura de aplicação de parâmetros de configuração e segurança para objetos da empresa. Você pode usar o AD DS e os GPOs (Objetos de Política de Grupo) para aplicar definições de configuração e segurança a contas de usuário e computador.

Pergunta: O que é uma árvore do AD DS?

Resposta: Uma árvore de domínio do AD DS é uma coleção de um ou mais domínios AD DS que formam um namespace contíguo. Por exemplo, se o primeiro domínio na floresta for adatum.com, você poderá criar um domínio adicional como um domínio filho nesse namespace. Um exemplo é atl.adatum.com.

Às vezes, é bom ter mais de um domínio na floresta. Quando você adiciona um domínio a uma floresta existente, pode adicioná-lo como um domínio filho a um domínio existente. Isso adiciona o domínio à árvore de domínio. Você também pode criar o domínio como uma nova árvore de domínio na floresta. Um exemplo disso seria se a A. Datum Corporation, uma empresa estabelecida com uma floresta do AD DS denominada adatum.com, adquirisse uma empresa chamada Fabrikam, Inc. Uma árvore adicional chamada fabrikam.com poderia ser criada na floresta adatum.com. Embora o novo domínio seja uma nova árvore de domínio, ainda está integrado com a floresta existente.

Pergunta: O que é uma floresta do AD DS?

Resposta: Uma floresta do AD DS consiste em uma coleção de uma ou mais árvores do AD DS. Cada árvore do AD DS conterá um ou mais domínios AD DS. A floresta do AD DS é o limite definitivo para a segurança e a administração do AD DS.

Pergunta: O que são relações de confiança?

Resposta: Relações de confiança (confianças) são pipelines de autenticação entre domínios diferentes. Há confianças que são geradas automaticamente como parte do processo de instalação de domínio e há confianças que você cria manualmente por outras razões. As relações de confiança formam a estrutura que permite o compartilhamento de recursos entre domínios e também fornecem a estrutura que oferece suporte à autenticação entre domínios.

Pergunta: O que é o catálogo global?

Resposta: O catálogo global fornece um diretório central de todo objeto na floresta e é exclusivo em cada floresta do AD DS. Diferentemente das partições de domínio individual que armazenam um conjunto de atributos graváveis completo para todos os objetos no domínio, o catálogo global é uma lista somente leitura de alguns atributos para cada objeto na floresta. O catálogo global facilita a localização de objetos de domínios diferentes em uma floresta de vários domínios. Por exemplo, o Microsoft® Exchange Server 2000 e as versões mais novas usam o catálogo global para localizar todos os destinatários de email em uma floresta.

Lição 2

Implantação de um ambiente distribuído do AD DS

Conteúdo:

Leitura adicional	49
Demonstração	49

Leitura adicional

Níveis funcionais de domínio AD DS

 **Leitura adicional:** Para saber mais sobre os níveis funcionais de domínio do AD DS, consulte *Noções básicas sobre níveis funcionais do AD DS* em <http://go.microsoft.com/fwlink/?LinkId=270028>.

Migração para o Windows Server 2012 AD DS de uma versão anterior

 **Leitura adicional:**

- Você pode baixar a Ferramenta de Migração do Active Directory versão 3.2 de <http://go.microsoft.com/fwlink/?LinkId=270029>.
- Você pode baixar o Guia da Ferramenta de Migração do Active Directory de <http://go.microsoft.com/fwlink/?LinkId=270045>.

Demonstração

Demonstração: Instalação de um controlador de domínio em um novo domínio em uma floresta

Etapas da demonstração

Configure LON-SVR1 como um controlador de domínio do AD DS em atl.adatum.com

1. Entre em **LON-DC1** como **Adatum\Administrador** com a senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, na coluna esquerda, clique em **Todos os Servidores**.
3. Clique com o botão direito do mouse do mouse em **Todos os Servidores** e clique em **Adicionar Servidores**.
4. Na janela nome (CN); digite **LON-SVR1** e clique em **Localizar Agora**.
5. Selecione **LON-SVR1**, clique na seta de adição e clique em **OK**.
6. No Gerenciador do Servidor, na janela Servidores, clique com o botão direito do mouse em **LON-SVR1** e clique em **Adicionar Funções e Recursos**.
7. No Assistente de Adição de Funções e Recursos, clique em **Próximo**.
8. Na página **Selecionar tipo de instalação**, verifique se a **Instalação baseada em função ou recurso** selecionada e clique em **Próximo**.
9. Na página **Selecionar servidor de destino**, verifique se a opção **Selecionar um servidor no pool de servidor** está selecionada. Na página **Pool de Servidores**, verifique se **LON-SVR1.Adatum.com** está realçado e clique em **Próximo**.
10. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Serviços de Domínio Active Directory**, clique em **Adicionar Recursos** e clique em **Próximo**.

11. Na página **Selecionar recursos**, clique em **Próximo**.
12. Na página **Serviços de Domínio Active Directory**, examine a mensagem e clique em **Próximo**.
13. Na página **Confirmar seleções de instalação**, examine a mensagem e clique em **Instalar**.
A instalação levará vários minutos.
14. Na página **Resultados**, clique em **Promover este servidor a um controlador de domínio**.
O assistente continua.

Acesse LON-SVR1 como Adatum\Administrador

1. Na página **Configuração de Implantação**, selecione a opção **Adicionar um novo domínio a uma floresta existente** e, ao lado de **Selecionar tipo de domínio**, confirme se o item **Domínio Filho** está selecionado.
2. No campo **Nome de domínio pai**, verifique se **Adatum.com** está listado.
3. Na caixa **Novo nome de domínio**, digite **atl**, e clique em **Alterar**.
4. Quando você for solicitado a fornecer as credenciais para executar essa operação, utilize o nome de usuário **Adatum\Administrador** e a senha **Pa\$\$w0rd** e clique em **OK**.
5. Na janela Configuração de Implantação, clique em **Próximo**.
6. Na página **Opções do Controlador de Domínio**, verifique se a opção **Windows Server 2012** está selecionada como o **Nível funcional do domínio**, se **Servidor do sistema de nomes de domínio (DNS)** está selecionado e se **Catálogo Global (GC)** está selecionado.
7. Nas caixas de texto **Digite a senha do Modo de Restauração dos Serviços de Diretório (DSRM)**, digite **Pa\$\$w0rd** em ambas e clique em **Próximo**.
8. Na página **Opções de DNS**, clique em **Próximo**.
9. Nas três janelas seguintes (Opções Adicionais, Caminhos e Examinar Opções), clique em **Próximo**.
Na janela Verificação de Pré-requisitos, clique em **Instalar**.
10. Examine as informações e permita a reinicialização de LON-SVR1 como um controlador de domínio do AD DS no novo domínio AD DS que você criou na floresta d AD DS.
11. No Assistente de Configuração dos Serviços de Domínio do Active Directory, clique em **Fechar**.
12. No Assistente de Adição de Funções e Recursos, clique em **Fechar**.
13. Entre em LON-SVR1 como **Adatum\Administrador** com a senha **Pa\$\$w0rd** e examine algumas das ferramentas do AD DS para confirmar a instalação do novo domínio.

Lição 3

Configuração de relações de confiança do AD DS

Conteúdo:

Leitura adicional	52
Demonstração	52

Leitura adicional

Definição das configurações de confiança avançadas do AD DS



Leitura adicional:

- Para obter mais informações sobre como configurar a quarentena de filtro de SID em relações de confiança externas, acesse <http://go.microsoft.com/fwlink/?LinkId=270030>.
- Para obter mais informações sobre como habilitar a autenticação seletiva em uma relação de confiança de floresta, acesse <http://go.microsoft.com/fwlink/?LinkId=270046>.
- Para obter mais informações sobre roteamento de sufixo de nome, acesse <http://go.microsoft.com/fwlink/?LinkId=270047>.

Demonstração

Demonstração: Configuração de uma relação de confiança de floresta

Etapas da demonstração

Configurar a resolução de nomes DNS usando um encaminhador condicional

1. Em LON-DC1, no Gerenciador do Servidor, clique no menu **Ferramentas** e, na lista suspensa, clique em **DNS**. O Gerenciador DNS é aberto.
2. No Gerenciador DNS, expanda **LON-DC1**, clique e clique com o botão direito do mouse em **Encaminhadores Condicionais** e clique em **Novo Encaminhador Condicional**.
3. Na janela Novo Encaminhador Condicional, na caixa **Domínio DNS**, digite **treyresearch.net**.
4. Na caixa de texto **Endereços IP dos servidores mestres**: digite **172.16.10.10**. Clique no espaço aberto e clique em **OK**. (Se um erro for exibido, ignore-o).
5. Feche o **Gerenciador DNS**.
6. Alterne para **MUN-DC1** e repita as etapas 1 a 5. Use to nome de domínio de **Adatum.com** com o endereço IP de **172.16.0.10**.

Configurar uma relação de confiança de floresta seletiva bidirecional

1. Em LON-DC1, no menu **Ferramentas**, clique em **Domínios e Relações de Confiança do Active Directory**.
2. Quando a janela Domínios e Relações de Confiança do Active Directory for aberta, clique com o botão direito do mouse em **Adatum.com** e clique em **Propriedades**.

3. Na caixa de diálogo **Propriedades de Adatum.com**, na guia **Relações de Confiança**, clique em **Nova Relação de Confiança**.
4. No Assistente de Nova Relação de Confiança, clique em **Avançar**.
5. Na página **Nome de relação de confiança**, na caixa de texto **Nome**, digite **treyresearch.net**, e clique em **Avançar**.
6. No Assistente de Nova Relação de Confiança, clique em **Relação de confiança entre florestas** e clique em **Avançar**.
7. Na página **Direção da relação de Confiança**, clique em **Bidirecional** e clique em **Avançar**.
8. Na página **Lados da Relação de Confiança**, clique em **Este domínio e o domínio especificado** e clique em **Avançar**.
9. Na caixa de texto **Nome de Usuário**: digite **Administrador**. Na caixa de texto **Senha**, digite **Pa\$\$w0rd** e clique em **Avançar**.
10. Na página **Nível de Autenticação de relação de confiança de saída - floresta local**, clique em **Autenticação seletiva** e clique em **Avançar**,
11. Na página **Floresta de relação de confiança de saída especificada pelo nível de autenticação**, clique em **Autenticação seletiva** e clique em **Avançar**,
12. Na página **Seleções de Relação de Confiança Concluídas**, clique em **Avançar**.
13. Na página **Criação de Relação de Confiança Concluída**, clique em **Avançar**.
14. Na página **Confirmar Relação de Confiança de Saída**, clique em **Sim, confirmar a relação de confiança de saída** e clique em **Avançar**.
15. Na página **Confirmar relação de confiança de entrada**, clique em **Sim**, confirmar a relação de confiança de entrada e clique em **Avançar**.
16. Na página **Concluindo o Assistente de Nova Relação de Confiança**, clique em **Concluir**.
17. Na caixa de diálogo **Propriedades de Adatum.com**, clique em **OK**.

Revisão e informações complementares do módulo

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
Você recebe mensagens de erro como: falha de pesquisa de DNS, servidor RPC não disponível, o domínio não existe, não foi possível encontrar o controlador de domínio.	Em geral, esses erros são causados por uma falha de pesquisa do registro DNS. Verifique se há pelo menos dois servidores DNS funcionais disponíveis na rede. Verifique se todos os computadores têm pelo menos dois servidores DNS configurados na rede. Verifique se os servidores DNS podem resolver consultas para registros DNS fora de seu domínio DNS (por exemplo, endereços da Internet). Use várias ferramentas de solução de problemas como nslookup, dnslint, DCdiag, netdiag, repadmin, replmon e Visualizador de Eventos.
O usuário não pode ser autenticado para acessar recursos em outro domínio do AD DS ou realm Kerberos.	Use o console de Domínios e Relações de Confiança do Active Directory, (Domain.msc), ou netdom para validar relações de confiança. Se necessário, reinicie a senha de confiança. Verifique se as relações de confiança estão configuradas para a direção certa. Verifique se todos os controladores de domínio do AD DS registraram todos os registros SRV corretos no banco de dados DNS. (Você pode reiniciar o serviço netlogon em um controlador de domínio AD DS para forçá-lo a registrar novamente os registros SRV no banco de dados DNS).

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação de implantações do AD DS distribuídas

Pergunta: Por que você configurou um registro de subdomínio delegado no DNS em LON-DC1 antes de adicionar o domínio filho na.adatum.com?

Resposta: Você fez isso para que o Sistema de Nomes de Domínio executado em LON-DC1 possa localizar um servidor DNS para o domínio DNS na.adatum.com.

Pergunta: Quais são as alternativas à criação de um registro de subdomínio delegado na pergunta anterior?

Resposta: Em LON-DC1, você poderia criar uma zona de stub para na.adatum.com para fornecer uma lista atualizada dos servidores DNS para o domínio DNS na.adatum.com. Você também poderia configurar em LON-DC1 um arquivo de zona DNS secundário para na.adatum.com, mas isso exigiria mais tráfego de replicação DNS.

Pergunta: Quando você está criando uma relação de confiança de floresta, por que você criaria uma relação de confiança seletiva, em vez de uma relação de confiança completa?

Resposta: Você criaria uma relação de confiança seletiva, em vez de uma relação de confiança completa se não precisasse de um link completo entre duas florestas, mas quisesse uma quantidade rigorosamente controlada de interatividade.

Módulo 5

Implementação de sites e da replicação dos Serviços de Domínio do Active Directory

Conteúdo:

Lição 2: Configuração de sites do AD DS	57
Lição 3: Configuração e monitoramento da replicação do AD DS	59
Lição 4: Revisão e informações complementares do módulo	62
Lição 5: Perguntas e respostas da revisão do laboratório	64

Lição 2

Configuração de sites do AD DS

Conteúdo:

Leitura adicional	58
Demonstração	58

Leitura adicional

Como computadores cliente localizam controladores de domínio dentro de sites



Leitura adicional: Para obter mais informações sobre como a cobertura do site é avaliada, consulte <http://go.microsoft.com/fwlink/?LinkId=168550>.

Demonstração

Demonstração: Configuração de sites do AD DS

Etapas da demonstração

1. Em LON-DC1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Serviços e Sites do Active Directory**.
2. Em Serviços e Sites do Active Directory, expanda **Sites** e clique em **Default-First-Site-Name**.
3. Clique com o botão direito do mouse do mouse em **Default-First-Site-Name** e clique em **Renomear**.
4. Digite **LondonHQ** e pressione Enter.
5. No painel de navegação, clique com o botão direito do mouse em **Sites** e clique em **Novo Site**.
6. Na caixa de diálogo **Novo Objeto – Site**, na caixa de texto **Nome**, digite **Toronto**.
7. Selecione **DEFAULTIPSITELINK** e clique em **OK**.
8. Na caixa de diálogo **Serviços de Domínio Active Directory**, clique em **OK**.
9. No painel de navegação, clique com o botão direito do mouse em **Subnets** e clique em **Nova Sub-rede**.
10. Na caixa de diálogo **Novo Objeto – Sub-rede**, na caixa de texto **Prefixo**, digite **172.16.0.0/24**.
11. Em **Selecione um objeto de site para este prefixo**, clique em **LondonHQ** e clique em **OK**.
12. No painel de navegação, clique com o botão direito do mouse em **Subnets** e clique em **Nova Sub-rede**.
13. Na caixa de diálogo **Novo Objeto – Sub-rede**, na caixa de texto **Prefixo**, digite **172.16.1.0/24**.
14. Em **Selecione um objeto de site para este prefixo**, clique em **Toronto** e clique em **OK**.
15. No painel de navegação, expanda **LondonHQ** e, em seguida, **Servers**.
16. Clique com o botão direito do mouse do mouse em **TOR-DC1** e clique em **Mover**.
17. Na caixa de diálogo **Mover Servidor**, selecione **Toronto** e clique em **OK**.
18. No painel de navegação, expanda **Toronto** e, em seguida, **Servers**.
19. Verifique se TOR-DC1 agora está localizado no site Toronto.

Lição 3

Configuração e monitoramento da replicação do AD DS

Conteúdo:

Demonstração

60

Demonstração

Demonstração: Configuração da replicação entre sites do AD DS

Etapas da demonstração

1. Em TOR-DC1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Serviços e Sites do Active Directory**.
2. Em Serviços e Sites do Active Directory, expanda **Sites** e **Inter-Site Transports**.
3. Clique em **IP**, clique com o botão direito do mouse em **DEFAULTIPSITELINK** e clique em **Renomear**.
4. Digite **LON-TOR** e pressione Enter.
5. Clique com o botão direito do mouse em **LON-TOR** e clique em **Propriedades**. Descreva as opções **Custo**, **Replicar a cada** e **Alterar agendamento**.
6. Na caixa de diálogo **Propriedades de LON-TOR**, ao lado de **Replicar a cada**, configure o valor para ser **60** minutos.
7. Clique em **Alterar agendamento**.
8. Realce o intervalo de **segunda-feira a sexta-feira de 12:00 a 16:00**, clique em **Replicação não disponível** e clique em **OK**.
9. Clique em **OK** para fechar a caixa de diálogo **Propriedades de LON-TOR**.
10. No painel de navegação, clique com o botão direito do mouse em **IP** e clique em **Propriedades**.
11. Na caixa de diálogo **Propriedades de IP**, mostre e explique a opção **Ponte entre links de sites**.
12. Clique em **OK** para fechar a caixa de diálogo **Propriedades de IP**.

Demonstração: Configuração de políticas de replicação de senha

Etapas da demonstração

1. Em LON-DC1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Usuários e Computadores do Active Directory**.
2. Na árvore de console, expanda o domínio **Adatum.com** e clique na UO (unidade organizacional) **Domain Controllers**.
3. Clique com o botão direito do mouse em **Domain Controllers** e clique em **Pré-criar Conta do Controlador de Domínio Somente Leitura**.
4. Na página **Bem-vindo** do Assistente de Instalação de Serviços de Domínio Active Directory, clique em **Avançar**.
5. Na página **Credenciais de rede**, clique em **Avançar**.
6. Na página **Especifique o Nome do computador**, digite **LON-RODC1** e clique em **Avançar**.

7. Na página **Selecione um Site**, clique em **Toronto** e clique em **Avançar**.
8. Na página **Opções Adicionais de Controlador de Domínio**, clique em **Avançar**.



Observação: Observe que a opção **Controlador de domínio somente leitura** é selecionada e não pode ser desmarcada. Isso acontece porque você iniciou o assistente escolhendo pré-criar uma conta de RODC.

9. Na página **Instalação e Administração de Delegação de RODC**, clique em **Avançar**.
10. Revise suas seleções na página **Resumo** e clique em **Avançar**.
11. Na página **Concluindo o Assistente de Instalação dos Serviços de Domínio Active Directory**, clique em **Concluir**.
12. No console, clique na UO **Domain Controllers**.
13. Clique com o botão direito do mouse do mouse em **LON-RODC1** e clique em **Propriedades**.
14. Clique na guia **Diretiva de Replicação de Senha** e exiba a política padrão.
15. Clique em **Cancelar** para fechar a janela **Propriedades de LON-RODC1**.
16. No console **Usuários e Computadores do Active Directory**, clique no contêiner **Users**.
17. Clique duas vezes em **Grupo de Replicação de Senha RODC Permitido** e clique na guia **Membros**.
18. Examine a associação padrão do Grupo de Replicação de Senha RODC Permitido e clique em **OK**. Por padrão, não deve haver nenhum membro.
19. Clique duas vezes em **Grupo de Replicação de Senha RODC Negado**.
20. Clique na guia **Membros**.
21. Clique em **Cancelar** para fechar a caixa de diálogo de propriedades de **Grupo de Replicação de Senha RODC Negado**.

Revisão e informações complementares do módulo

Prática recomendada

Implemente as seguintes práticas recomendadas ao gerenciar sites do Active Directory e a replicação em seu ambiente:

- Sempre forneça pelo menos um ou mais servidores de catálogo global por site.
- Verifique se todos os sites têm sub-redes apropriadas associadas.
- Não configure intervalos longos sem replicação ao configurar agendas de replicação para a replicação entre sites.
- Evite usar o SMTP como um protocolo de replicação.

Perguntas de revisão

Pergunta: Por que é importante que todas as sub-redes sejam identificadas e associadas a um site em uma empresa multissite?

Resposta: O processo de localizar controladores de domínio e outros serviços pode se tornar mais eficiente com a indicação de clientes ao site correto com base no endereço IP do cliente e na definição de sub-redes. Se um cliente tiver um endereço IP que não pertence a um site, ele consultará todos os controladores de domínio no domínio. Essa não é uma estratégia eficiente. Na realidade, um único cliente pode estar executando ações em controladores de domínio em sites diferentes, o que poderá gerar resultados estranhos se essas alterações ainda não tiverem sido replicadas. Portanto, é fundamental que cada cliente saiba o site em que ele está, o que você poderá obter assegurando que os controladores de domínio possam identificar o local do site de um cliente.

Pergunta: Quais são as vantagens e desvantagens de reduzir o intervalo de replicação entre sites?

Resposta: A redução do intervalo de replicação entre sites melhora a convergência. As alterações feitas em um site são replicadas mais rapidamente em outros sites. Há realmente poucas desvantagens, se houver alguma. Se você considerar que as mesmas alterações devem ser replicadas quer elas aguardem 15 minutos ou três horas pela replicação, realmente será um problema de tempo de replicação e não de quantidade de replicação. Entretanto, em algumas situações extremas, talvez seja menos preferível permitir que um número menor de alterações ocorra com mais frequência do que permitir que um grande número de alterações seja replicado com menos frequência.

Pergunta: Qual é a finalidade de um servidor bridgehead?

Resposta: O servidor bridgehead é responsável por toda a replicação que entra e sai do site. Em vez de replicar todos os controladores de domínio de um site com todos os controladores de domínio em outro site, você pode usar servidores bridgehead para gerenciar a replicação entre sites.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
O cliente não consegue localizar o controlador de domínio em seu site.	Verifique se todos os registros de recursos de serviços (SRV) do controlador de domínio estão presentes no DNS. Verifique se o controlador de domínio tem um endereço IP da sub-rede que está associada a esse site. Verifique se o cliente é um membro do domínio e tem o horário correto.
A replicação entre sites não funciona.	Verifique se os links de sites estão configurados corretamente. Verifique a agenda de replicação. Verifique se o firewall entre os sites permite o tráfego de replicação do Active Directory.
A replicação entre dois controladores de domínio no mesmo site não funciona.	Verifique se ambos os controladores de domínio aparecem no mesmo site. Verifique se o AD DS está funcionando corretamente nos controladores de domínio. Verifique a comunicação de rede, e se a hora em cada servidor é válida.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação de sites e replicação do AD DS

Pergunta: Você decide adicionar um novo controlador de domínio ao site LondonHQ denominado LON-DC2. Como você pode garantir que LON-DC2 seja usado para passar todo o tráfego de replicação para o site Toronto?

Resposta: Você precisaria configurar esse novo controlador de domínio como o servidor bridgehead preferencial para o site LondonHQ.

Pergunta: Você adicionou o novo controlador de domínio denominado LON-DC2 ao site LondonHQ. Como resultado, que partições do AD DS serão modificadas?

Resposta: É provável que todas as partições, exceto a partição de esquema, serão modificadas. Você adiciona o novo controlador de domínio à partição de domínio e à partição de configuração para assegurar que a replicação do AD DS seja configurada corretamente. Se você estiver usando DNS integrado ao AD DS, os registros do controlador de domínio também serão atualizados nas partições de aplicativos DNS.

Pergunta: No laboratório, você criou um link de site separado para os sites Toronto e TestSite. O que você também pode fazer para assegurar que LondonHQ não crie de forma automática um objeto de conexão diretamente com o site TestSite?

Resposta: Também pode ser necessário desativar a ponte de link de site automática, assim você desabilita a transitividade de site entre LondonHQ, Toronto e TestSite.

Módulo 6

Implementação dos Serviços de Certificados do Active Directory

Conteúdo:

Lição 1: Visão geral do PKI	66
Lição 2: Implantação de autoridades de certificação	68
Lição 3: Implantação e gerenciamento de modelos de certificados	70
Lição 4: Implementação da distribuição e revogação de certificados	72
Lição 5: Gerenciamento da recuperação de certificados	76
Revisão e informações complementares do módulo	80
Perguntas e respostas da revisão do laboratório	82

Lição 1

Visão geral do PKI

Conteúdo:

Perguntas e respostas

67

Perguntas e respostas

O que é hierarquia de certificação cruzada?

Pergunta: Sua empresa está adquirindo outra empresa. As duas empresas executam PKIs próprias. O que você poderia fazer para minimizar a interrupção e continuar fornecendo serviços de PKI de modo integrado?

Resposta: Você pode implementar uma hierarquia de certificação cruzada.

Lição 2

Implantação de autoridades de certificação

Conteúdo:

Demonstração

69

Demonstração

Demonstração: Implantação de uma AC raiz

Etapas da demonstração

Implantar uma AC raiz

1. Em LON-SVR1, no Gerenciador do Servidor, clique em **Adicionar funções e recursos**.
2. Na página **Antes de começar**, clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
4. Na página **Selecionar servidor de destino**, clique em **Próximo**.
5. Na página **Selecionar funções de servidor**, escolha **Serviços de Certificados do Active Directory**. No Assistente de Adição de Funções e Recursos, clique em **Adicionar Recursos** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Serviços de Certificados do Active Directory**, clique em **Próximo**.
8. Na página **Selecionar serviços de função**, verifique se **Autoridade de Certificação** está selecionado e clique em **Próximo**.
9. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
10. Na página **Progresso da instalação**, depois que a instalação for concluída com êxito, clique no texto **Configurar os Serviços de Certificados do Active Directory no servidor de destino**.
11. No Assistente de Configuração do AD CS, na página **Credenciais**, clique em **Próximo**.
12. Na página **Serviços de Função**, selecione **Autoridade de Certificação** e clique em **Próximo**.
13. Na página **Tipo de Instalação**, selecione **AC Corporativa** e clique em **Próximo**.
14. Na página **Tipo de Autoridade de Certificação** clique na opção **AC Raiz** e clique em **Próximo**.
15. Na página **Chave Privada**, verifique se **Criar uma nova chave privada** está selecionado e clique em **Próximo**.
16. Na página **Criptografia para AC** mantenha as seleções padrão do CSP (Provedor de Serviços de Criptografia) e Algoritmo de Hash, mas defina o **Comprimento da chave** como **4096** e clique em **Próximo**.
17. Na página **Nome de Autoridade de Certificação**, na caixa **Nome comum da autoridade de certificação**, digite **AdatumRootCA** e clique em **Próximo**.
18. Na página **Período de Validade**, clique em **Próximo**.
19. Na página **Banco de Dados de AC**, clique em **Próximo**.
20. Na página **Confirmação**, clique em **Configurar**.
21. Na página **Resultados**, clique em **Fechar**.
22. Na página **Progresso da instalação**, clique em **Fechar**.

Lição 3

Implantação e gerenciamento de modelos de certificados

Conteúdo:

Demonstração

71

Demonstração

Demonstração: Modificação e habilitação de um modelo de certificado

Etapas da demonstração

Modificar e habilitar um modelo de certificado

1. Em LON-SVR1, na barra de tarefas, clique no ícone Gerenciador do Servidor.
2. No Gerenciador do Servidor, clique em **Ferramentas** e em **certification authority**.
3. No console **Autoridade de certificação (Local)**, expanda **AdatumRootCA**, clique com o botão direito do mouse em **Modelos de Certificado** e clique em **Gerenciar**.
4. Examine a lista de modelos padrão. Examine os modelos e as suas propriedades.
5. No painel **Detalhes**, clique duas vezes em **IPSec**.
6. Na caixa de diálogo **Propriedades de IPSec**, percorra as guias e observe o que você pode modificar em cada guia. Observe que na guia **Segurança**, é possível definir as permissões para registro. Clique em **Cancelar** para fechar o modelo.
7. No console **Modelos de Certificados**, no painel Detalhes, clique com o botão direito do mouse no modelo de certificado **Trocar Usuário** e clique em **Modelo Duplicado**.
8. Na caixa de diálogo **Propriedades do novo modelo**, examine as opções na guia **Compatibilidade**.
9. Clique na guia **Geral** e no nome para exibição da caixa de texto **Nome de exibição do modelo**; digite **Trocar Usuário Teste 1**.
10. Clique na guia **Modelos Obsoletos** e clique em **Adicionar**.
11. Clique no modelo **Trocar usuário** e clique em **OK**.
12. Clique na guia **Segurança** e clique em **Usuários autenticados**.
13. No nó **Permissões para Usuários autenticados**, marque as caixas de seleção **Permitir de Ler**, **Registrar**, **Registrar automaticamente** e clique em **OK**.
14. Feche o console **Modelos de Certificados**.
15. No console **Autoridade de certificação (Local)**, clique com o botão direito em **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
16. Na caixa de diálogo **Ativar Modelos de Certificado**, selecione o certificado **Trocar Usuário Teste 1** e clique em **OK**.

Lição 4

Implementação da distribuição e revogação de certificados

Conteúdo:

Demonstração

73

Demonstração

Demonstração: Configuração de um agente de registro restrito

Etapas da demonstração

Configurar o Agente de Registro Restrito

1. Em LON-SVR1, na barra de tarefas, clique no ícone Gerenciador do Servidor.
2. No console do Gerenciador do Servidor, clique em **Ferramentas** e abra a **certification authority**.
3. No console certsrv, expanda **AdatumRootCA**, clique com o botão direito do mouse em **Modelos de Certificado** e clique em **Gerenciar**.
4. No console Modelos de Certificados, clique duas vezes em **Agente de Registro**, clique na guia **Segurança** e clique em **Adicionar**.
5. Na janela Selecionar Usuários, Computadores, Contas de Serviços ou Grupos, digite **Allie**, clique em **Verificar nomes** e clique em **OK**.
6. Na guia **Segurança**, clique em **Allie Bellew**, selecione as permissões **Permitir a Ler** e **Registrar** e clique em **OK**.
7. Feche o console Modelos de Certificados.
8. No console certsrv clique com o botão direito do mouse em **Modelos de Certificado**, aponte para **Novo**, clique em **Modelo de Certificado a Ser Emitido**.
9. Na lista de modelos, clique em **Agente de Registro** e clique em **OK**.
10. Alterne para LON-CL1 e faça logon como **Adatum\Allie** com a senha **Pa\$\$w0rd**.
11. Na tela inicial, digite **mmc.exe** e pressione Enter.
12. No **Console1**, abra o menu **Arquivo** e clique em **Adicionar/remover snap-in**.
13. Clique em **Certificados**, em **Adicionar** e clique em **OK**.
14. Expanda **Certificados – Usuário Atual** e clique em **Pessoal**.
15. Clique com o botão direito do mouse do mouse em **Pessoal**, aponte para **Todas as tarefas** e clique em **Solicitar novo certificado**.
16. No Assistente de Registro de Certificado, na página **Antes de Começar**, clique em **Avançar**.
17. Na página **Selecionar Política de Registro de Certificado**, clique em **Avançar**.
18. Na página **Solicitar Certificados**, selecione **Agente de Registro**, clique em **Registrar** e clique em **Concluir**.
19. Alterne para **LON-SVR1**.
20. No console Autoridade de Certificação, clique com o botão direito do mouse em **AdatumRootCA** e clique em **Propriedades**.
21. Na caixa de diálogo **Propriedades de AdatumRootCA**, clique na guia **Agentes de Inscrição**.
22. Na guia **Agentes de Inscrição**, clique em **Restringir agentes de inscrição**.

23. Na janela pop-up, clique em **OK**.
24. Na guia **Agentes de Inscrição**, em **Agentes de registro**, clique em **Adicionar**.
25. Na janela Selecionar Usuário, Computador ou Grupo, digite **Allie**, clique em **Verificar nomes** e clique em **OK**.
26. Clique em **Todos** e clique em **Remover**.
27. Na seção **Modelos de Certificado**: clique em **Adicionar**.
28. Na lista de modelos, selecione **Usuário** e clique em **OK**.
29. Na seção **Modelos de Certificado**:, clique em **<Todas>** e clique em **Remover**.
30. Na seção Permissão, clique em **Adicionar**.
31. Na janela Selecionar Usuário, Computador ou Grupo, digite **Marketing**, clique em **Verificar nomes** e clique em **OK**.
32. Na seção Permissão, clique em **Todos** e clique em **Remover** e clique em **OK**.

Demonstração: Configuração de um respondente online

Etapas da demonstração

Configurar um respondente online

1. Em LON-SVR1, na barra de tarefas, clique no ícone Gerenciador do Servidor.
2. No **Gerenciador do Servidor**, clique em **Adicionar funções e recursos**.
3. Clique três vezes em **Próximo**
4. Na página **Selecionar funções de servidor**, expanda **Serviços de Certificados do Active Directory (Instalado)** e selecione **Respondente Online**.
5. Clique em **Adicionar Recursos**.
6. Clique duas vezes em **Próximo** e clique em **Instalar**.
7. Quando a instalação for concluída com sucesso, clique em **Configurar os Serviços de Certificados do Active Directory no servidor de destino**.
8. No Assistente de Configuração AD CS, clique em **Próximo**.
9. Selecione **Respondente Online** e clique em **Próximo**.
10. Clique em **Configurar** e clique duas vezes em **Fechar**.
11. No console **Gerenciador do Servidor**, clique em **Ferramentas** e no console certification authority em **LON-SVR1**.
12. No console Autoridade de Certificação, clique com o botão direito do mouse em **AdatumRootCA** e clique em **Propriedades**.
13. Na caixa de diálogo **Propriedades de AdatumRootCA**, na guia **Extensões**, na lista **Selecione a extensão**, clique em **Acesso a Informações da Autoridade (AIA)** e clique em **Adicionar**.

14. Na caixa de diálogo **Adicionar Local**, digite **http://LON-SVR1/ocsp** e clique em **OK**.
15. Marque a caixa de seleção **Incluir na extensão AIA de certificados emitidos**.
16. Marque a caixa de seleção **Incluir na extensão do protocolo de status de certificados online (OCSP)** e clique em **OK**.
17. Na caixa **certification authority**, reinicie os Serviços de Certificados do Active Directory clicando em **Sim**.
18. No console certsrv console, expanda **AdatumRootCA**, clique com o botão direito do mouse na pasta **Modelos de Certificado** e clique em **Gerenciar**.
19. No console Modelos de Certificados, clique duas vezes no modelo **Assinatura de Resposta OCSP**.
20. Na caixa de diálogo **Propriedades de Assinatura de Resposta OCSP**, clique na guia **Segurança**. Em **Permissões para Usuários autenticados**, marque a caixa de seleção **Permitir** o **Registrar** e clique em **OK**.
21. Feche o console Modelos de Certificados.
22. No console Autoridade de Certificação, clique com o botão direito do mouse na pasta **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
23. Na caixa de diálogo **Ativar Modelos de Certificado**, selecione o modelo **Assinatura de Resposta OCSP** e clique em **OK**.
24. Em LON-SVR1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Gerenciamento de Respondentes Online**.
25. No console Gerenciamento do Respondente Online, clique com o botão direito do mouse em **Configuração de Revogação** e clique em **Adicionar Configuração de Revogação**.
26. No assistente Adicionar Configuração de Revogação, clique em **Avançar**.
27. Na página **Nomear a Configuração de Revogação**, na caixa de texto **Nome**, digite **Respondente Online de AdatumCA** e clique em **Avançar**.
28. Na página **Selecionar a Localização do Certificado CA**, clique em **Avançar**.
29. Na página **Escolher o Certificado CA**, clique em **Procurar**, no certificado **AdatumRootCA**, em **OK** e clique em **Avançar**.
30. Na página **Selecione um certificado de autenticação**, verifique se **Selecionar automaticamente um certificado de autenticação** e **Fazer Inscrição Automática para um certificado de autenticação OCSP** estão selecionados e clique em **Avançar**.
31. Na página **Provedor de Revogação**, clique em **Concluir**. O status da configuração de revogação aparecerá como **Processando**.
32. Feche o console do respondente online.

Lição 5

Gerenciamento da recuperação de certificados

Conteúdo:

Demonstração

77

Demonstração

Demonstração: Configuração da AC do arquivamento de chave

Etapas da demonstração

Configurar o arquivamento de chave automático

1. Em LON-SVR1, abra o console certification authority.
2. No console certification authority, expanda o nó **AdatumRootCA**, clique com o botão direito do mouse na pasta **Modelos de Certificado** e clique em **Gerenciar**.
3. No painel detalhes, clique com o botão direito do mouse no certificado **Agente de recuperação de chave** e clique em **Propriedades**.
4. Na caixa de diálogo **Propriedades de agente de recuperação de chave**, na guia **Requisitos de Emissão** limpe a caixa de seleção **Aprovação do gerenciador de certificados de autoridade de certificação**.



Observação: Isso é somente para fins de teste. Em um ambiente de produção, você não deve mudar esse valor.

5. Na guia **Segurança**, observe que os Administradores de domínio e de empresa são os únicos grupos que tem a permissão **Registrar**, e clique em **OK**. Não faça nenhuma alteração aqui.
6. Feche o console de Modelos de Certificados.
7. No console de Modelos de Certificados, clique com o botão direito do mouse em **Modelos de Certificado**, clique em **Novo**, clique em **Modelo de Certificado a ser emitido**, clique em **Agente de recuperação de chave** e clique em **OK**. Esse processo configura uma AC para emitir certificados baseados no modelo do agente de recuperação de chave.
8. Clique na tela inicial, digite **mmc.exe** e pressione Enter.
9. Na janela Console 1, clique em **Arquivo** e clique em **Adicionar/remover snap-in**.
10. Na página **Adicionar ou Remover Snap-ins**, selecione **Certificados** e clique em **Adicionar**.
11. Selecione **Minha conta de usuário**, clique em **Concluir** e clique em **OK**.
12. Expanda **Certificados - Usuário Atual** e clique em **Pessoal**. Clique com o botão direito do mouse do mouse em **Pessoal**, selecione **Todas as tarefas** e clique em **Solicitar novo certificado**.
13. No Assistente de registro de certificado, clique duas vezes em **Avançar**.
14. Na página **Solicitar certificados**, selecione **Agente de recuperação de chave** e clique em **Registrar**.
15. Clique em **Concluir**.
16. Verifique se o novo certificado aparece no repositório de certificados. Se sim, você registrou o Administrador como o KRA. Minimize o console de certificados.

17. Abra as propriedades de AdatumRootCA.
18. Na guia **Agentes de recuperação** clique em **Arquivar a chave**, clique em **Adicionar** e escolha o certificado do administrador. Clique em **OK**.
19. Clique em **OK** e clique em Sim para reiniciar o AD CS.
20. Clique com o botão direito do mouse do mouse em **Modelos de Certificados** e clique em **Gerenciar**.
21. Clique duas vezes no certificado **Trocar usuário Teste1** para abrir a caixa de diálogo **Propriedades**. Na guia **Tratamento de Solicitação**, clique em **Arquivar chave privada de criptografia de requerente** e clique em **Incluir algoritmos simétricos permitidos pelo requerente**. Se a janela pop-up aparecer, clique em **OK**.
22. Clique em **OK** para fechar o modelo.

Demonstração: Recuperação de uma chave privada perdida (opcional)

Etapas da demonstração

Recuperar uma chave privada perdida

1. Em LON-SVR1, clique na tela inicial, digite **mmc.exe** e pressione Enter.
2. Clique em **Arquivo** e clique em **Adicionar/remover snap-in**.
3. Selecione **Certificados** e clique em **Adicionar**.
4. Clique em **Minha conta de usuário**, clique em **Concluir** e clique em **OK**.
5. Expanda **Certificados - Usuário Atual**, expanda **Pessoal**, clique com o botão direito do mouse em **Certificados**, selecione **Todas as tarefas** clique em **Solicitar novo certificado**.
6. Registre-se no certificado Trocar usuário Teste1 usando o assistente. Quando você seleciona o modelo **Trocar usuário Teste1** no assistente, clique para abrir as configurações em uma observação para inserir o nome da entidade. Na lista **Tipo**, clique em **Email**, no campo valor, digite **administrator@adatum.com**, clique em **Adicionar**, clique em **OK** e clique em **Registrar**.
7. Verifique se o novo certificado aparece em Pessoal->Repositório de certificados.
8. Simule uma chave privada perdida excluindo o certificado **administrator@adatum.com** do repositório de certificados pessoal. Faça isso clicando com o botão direito do mouse em **administrator@adatum.com**, clique em **Excluir** e clique em **Sim**. Minimize o console de certificados (Console1).
9. No console Autoridade de Certificação na pasta Certificados Emitidos, clique duas vezes no certificado com o nome de modelo **Trocar usuário Teste1**. Esse é o certificado que você emitiu em uma etapa anterior. Na guia **Detalhes**, registre o número de série. (Você pode copiar e colar isso no Bloco de Notas e remover os espaços entre os números).
10. Abra uma janela do prompt de comando com privilégios elevados. (No menu **Iniciar**, digite **cmd**, clique com o botão direito em **Prompt de Comando** e clique em **Executar como administrador**).

11. Na janela do prompt de comando, alterne para a raiz da Unidade C digitando **cd..** e pressionando Enter. (Você pode ter que fazer isso duas vezes).
12. Selecione o número de série do certificado do Bloco de Notas, clique com o botão direito do mouse e selecione **Cópia**.
13. Retorne para a janela do prompt de comando e digite o comando a seguir:

```
Certutil -getkey <númerodesérie> outputblob
```

em que <número de série> é um número que você cola do Bloco de Notas. Pressione Enter.



Observação: Se um ponto de interrogação aparecer no começo do número depois de colá-lo, exclua-o. Certifique-se também de remover todos os espaços do número de série, ou coloque o número de série entre aspas.

14. Depois que o comando for concluído com êxito, abra a unidade C e verifique se o arquivo **BlobdeSaída** é exibido.
15. Retorne para a janela do prompt de comando. No prompt de comando, digite o seguinte e pressione Enter:

```
Certutil -recoverkey outputblob recover.pfx
```

16. Quando for solicitado, digite **Pa\$\$w0rd** como a nova senha e confirme-a.
17. Navegue até a unidade C e verifique se o arquivo o Recuperar.pfx (a chave recuperada) foi criado.
18. Clique duas vezes em **recuperar.pfx**.
19. Clique duas vezes em **Avançar**.
20. Insira a senha **Pa\$\$w0rd**, clique duas vezes em **Avançar**, clique em **Concluir** e clique em **OK**.
21. Restaurar o console de certificados (Console 1). Atualize o repositório de certificados.
22. Verifique se o certificado administrator@adatum.com aparece agora.

Revisão e informações complementares do módulo

Prática recomendada

- Ao implantar a infraestrutura de AC, implante uma AC raiz autônoma (servidor associado que não pertence ao domínio) e uma AC corporativa subordinada (AC emissora). Depois que a AC corporativa subordinada receber um certificado da AC raiz, coloque a AC raiz offline.
- Emita um certificado para a AC raiz por um longo período de tempo, como 15 ou 20 anos.
- Use o registro automático para certificados que são amplamente usados.
- Use um agente de registro restrito sempre que possível.
- Use os cartões inteligentes virtuais para melhorar a segurança de logon.

Perguntas de revisão

Pergunta: Por que razões uma organização utilizaria a PKI?

Resposta: Algumas razões são a melhora da segurança, o controle de identidade e a assinatura digital de código.

Pergunta: Por que razões uma organização usaria uma AC raiz corporativa?

Resposta: Se uma organização desejar usar só uma AC, e desejar usar modelos de certificado e registro automático, então uma AC raiz corporativa será a única escolha.

Pergunta: Liste os requisitos para usar o registro automático em certificados.

Resposta: Para usar o registro automático em certificados, você deve ter uma AC corporativa e você deve configurar as opções da Política de Grupo. Além disso, você deve habilitar o registro automático nos certificados desejados e você deve configurar os GPOs (Objetos de Política de Grupo).

Pergunta: Quais são as etapas para configurar um respondente online?

Resposta: Para configurar um respondente online você deve criar a configuração de respondente e você deve se registrar em um certificado de autenticação de OCSP. Você também deve acrescentar uma URL de respondente a AIA.

Problemas e cenários reais

Contoso, Ltd. deseja implantar a PKI para dar suporte e proteger vários serviços. Eles decidiram usar os Serviços de Certificados do Windows Server 2012 como uma plataforma para a PKI. Os certificados serão usados principalmente para EFS, assinatura digital, e para servidores Web. Como os documentos que serão criptografados são importantes, é essencial ter uma estratégia de recuperação de desastres no caso de perda da chave. Além disso, os clientes que terão acesso às partes seguras do site da empresa não devem receber nenhum aviso nos seus navegadores.

1. Que tipo de implantação a Contoso deve escolher ?
2. Que tipo de certificados a Contoso deve usar para EFS e assinatura digital?
3. Que tipo de certificados a Contoso deve usar para um site?
4. Como a Contoso assegurará que dados com criptografia EFS não serão perdidos se um usuário perder um certificado?

Ferramentas

- Console da Autoridade de Certificado
- Console de modelos de certificado
- Console de certificados
- Certutil.exe

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
<p>O local do certificado de Autoridade de Certificação que é especificado na extensão de acesso a informações da autoridade não é configurado para incluir o sufixo do nome de certificado. Os clientes podem não conseguir localizar a versão correta do certificado da AC emissora para compilar uma cadeia de certificados e a validação do certificado pode falhar.</p>	<p>Use o snap-in Autoridade de Certificação para configurar a extensão do acesso a informações da autoridade para incluir o sufixo do nome do certificado em cada local.</p>
<p>A AC não é configurada para incluir os locais de ponto de distribuição de CRL nas extensões de certificados emitidos. Os clientes podem não conseguir localizar uma CRL para verificar o status de revogação de um certificado, e a validação de certificado pode falhar.</p>	<p>Use o snap-in Autoridade de Certificação para configurar a extensão de ponto de distribuição de CRL e para especificar o local de rede da CRL. Os locais padrão da CRL são adicionados às configurações de extensão de ponto de distribuição de CRL durante a instalação da AC e a AC é configurada para incluir os locais padrão nas extensões de todos os certificados emitidos.</p>
<p>A AC foi instalada como uma AC corporativa, mas as configurações da Política de Grupo de registro automático de usuário não foram habilitadas. Uma AC corporativa pode usar o registro automático para simplificar a emissão e a renovação de certificado. Se o registro automático não for habilitado, a emissão e a renovação de certificado pode não ocorrer como esperado.</p>	<p>Use o GPMC para definir as configurações da política de registro automático de usuário e use o snap-in dos modelos de certificados para definir as configurações de registro automático no modelo de certificado.</p>

Perguntas e respostas da revisão do laboratório

Laboratório A: Implantação e configuração da hierarquia de autoridades de certificação

Pergunta: Por que não é recomendado instalar apenas uma AC raiz corporativa?

Resposta: Por motivo de segurança, as ACs raiz devem estar offline, sem qualquer acesso à rede. As ACs raiz corporativas não podem estar offline, por isso, não há proteção máxima para a chave correspondente.

Laboratório B: Implantação e gerenciamento de certificados

Pergunta: Quais são os principais benefícios do OCSP sobre a CRL?

Resposta: O OCSP fornece o status de um único certificado solicitado pelos clientes, em vez de baixar a CRL inteira e as CRLs delta. Além disso, as respostas são muito mais rápidas e mais confiáveis porque os clientes não as armazenam em cache.

Pergunta: O que você deve fazer para recuperar as chaves privadas?

Resposta: Para recuperar as chaves privadas, você deve configurar a AC para arquivar as chaves privadas de modelos específicos e você deve emitir um certificado de agente de recuperação de chave.

Módulo 7

Implementação do Active Directory Rights Management Services

Conteúdo:

Lição 2: Implantação e gerenciamento de uma infraestrutura do AD RMS	84
Lição 3: Configuração da proteção de conteúdo do AD RMS	87
Lição 4: Configuração do acesso externo ao AD RMS	90
Revisão e informações complementares do módulo	92
Perguntas e respostas da revisão do laboratório	93

Lição 2

Implantação e gerenciamento de uma infraestrutura do AD RMS

Conteúdo:

Demonstração

85

Demonstração

Demonstração: Instalação do primeiro servidor de um cluster do AD RMS

Etapas da demonstração

Configurar conta de serviço

1. No Gerenciador do Servidor, clique em **Ferramentas** e clique em **Central Administrativa do Active Directory**.
2. Selecione e clique com o botão direito do mouse em **Adatum (local)**, clique em **Novo** e clique em **Unidade Organizacional**.
3. Na caixa de diálogo **Criar Unidade Organizacional**, no campo **Nome**, digite **Contas de Serviço** e clique em **OK**.
4. Clique com o botão direito do mouse na unidade organizacional **Contas de Serviço**, clique em **Novo** e clique em **Usuário**.
5. Na caixa de diálogo **Criar Usuário**, digite os seguintes detalhes e clique em **OK**:
 - o Primeiro nome: **ADRMSSVC**
 - o Logon UPN do usuário: **ADRMSSVC**
 - o Senha: **Pa\$\$w0rd**
 - o Confirmar senha: **Pa\$\$w0rd**
 - o A senha nunca expira: **Habilitado**
 - o O usuário não pode alterar a senha: **Habilitado**

Preparar o DNS

1. No Gerenciador do Servidor, clique em **Ferramentas** e clique em **DNS**.
2. No console do Gerenciador DNS, expanda **LON-DC1** e **Zonas de pesquisa direta**.
3. Selecione e clique com o botão direito do mouse em **Adatum.com** e clique em **Novo Host (A ou AAAA)**.
4. Na caixa de diálogo **Novo Host**, digite as informações a seguir e clique em **Adicionar Host**:
 - o Nome: **adrms**
 - o Endereço IP: **172.16.0.21**
5. Clique em **OK** e clique em **Concluído**, e depois feche o console do Gerenciador DNS.

Instalar a função AD RMS

1. Entre em LON-SVR1 com a conta **Adatum\Administrador** e a senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, clique em **Gerenciar** e clique em **Adicionar Funções e Recursos**.
3. No Assistente de Adição de Funções e Recursos, clique em **Próximo** três vezes.

4. Na página **Funções do Servidor**, clique em **Active Directory Rights Management Services**.
5. Na caixa de diálogo **Adicionar Funções e Recursos**, clique em **Adicionar Recursos** e clique em **Próximo** quatro vezes.
6. Clique em **Instalar** e clique em **Fechar**.

Configurar o AD RMS

1. No Gerenciador do Servidor, clique no nó **AD RMS**.
2. Ao lado de Configuração necessária para o Active Directory Rights Management Services em LON-SVR1, clique em **Mais**.
3. Na página **Todos os Servidores Detalhes da Tarefa**, clique em **Realize configuração adicional**.
4. Na caixa de diálogo **Configuração do AD RMS: LON-SVR1.adatum.com**, clique em **Próximo**.
5. Na página **Cluster AD RMS**, clique em **Criar novo cluster AD RMS raiz** e clique em **Próximo**.
6. Na página **Banco de Dados de Configuração**, clique em **Usar o Banco de Dados Interno do Windows neste servidor** e clique em **Próximo**.
7. Na página **Conta de Serviço**, clique em **Especificar**.
8. Na caixa de diálogo **Segurança do Windows**, insira os detalhes a seguir, clique em **OK** e clique em **Próximo**:
 - o Nome de Usuário: **ADRMSSVC**
 - o Senha: **Pa\$\$w0rd**
9. Na página **Modo Criptográfico**, clique em **Modo Criptográfico 2** e clique em **Próximo**.
10. Na página **Armazenamento de Chave do Cluster**, clique em **Usar armazenamento de chave centralmente gerenciada no AD RMS** e clique em **Próximo**.
11. Na página **Senha da Chave de Cluster**, digite a senha **Pa\$\$w0rd** duas vezes e clique em **Próximo**.
12. Na página **Site do Cluster**, verifique se **Default Web Site** está selecionado e clique em **Próximo**.
13. Na página **Endereço do Cluster**, forneça as seguintes informações e clique em **Próximo**:
 - o Tipo de Conexão: **Usar uma conexão descriptografada (http://)**
 - o Nome de Domínio Totalmente Qualificado: **adrms.adatum.com**
 - o Porta: **80**
14. Na página **Certificado de Licenciante**, digite **Adatum AD RMS** e clique em **Próximo**.
15. Na página **Registro de SCP**, clique em **Registrar o SCP agora** e clique em **Próximo**.
16. Clique em **Instalar** e clique em **Fechar**.
17. Clique na tela Iniciar, em **Administrador** e clique em **Sair**.



Observação: Você deve sair antes de poder gerenciar o AD RMS.

Lição 3

Configuração da proteção de conteúdo do AD RMS

Conteúdo:

Leitura adicional	88
Demonstração	88

Leitura adicional

O que são políticas de exclusão?



Leitura adicional: Para saber mais sobre como habilitar políticas de exclusão, consulte *Habilitando políticas de exclusão* em <http://go.microsoft.com/fwlink/?LinkId=270031>.

Demonstração

Demonstração: Criação de um modelo de política de direitos

Etapas da demonstração

1. No Gerenciador do Servidor, clique em **Ferramentas** e clique em **Active Directory Rights Management Services**.
2. No console do Active Directory Rights Management Services, clique no nó **LON-SVR1\Modelos de Política de Direitos**.
3. No painel Ações, clique em **Criar Modelo de Política de Direitos Distribuídos**.
4. No Assistente para Criar Modelo de Política de Direitos Distribuídos, na página **Adicionar Informações de Identificação de Modelo**, clique em **Adicionar**.
5. Na página **Adicionar Novas Informações de Identificação de Modelo**, digite as informações a seguir e clique em **Adicionar** e clique em **Avançar**:
 - o Idioma: **Português (Brasil)**
 - o Nome: **ReadOnly**
 - o Descrição: **Acesso somente leitura. Sem cópia ou impressão.**
6. Na página **Adicionar Direitos de Usuário**, clique em **Adicionar**.
7. Na página **Adicionar Usuário ou Grupo**, digite **executivos@adatum.com** e clique em **OK**.
8. Quando **executivos@adatum.com** estiver selecionado, em Direitos, clique em **Exibir**. Verifique se **Conceder ao proprietário (autor) o direito ininterrupto de controle total** está selecionado e clique em **Avançar**.
9. Na página **Especificar Política de Expiração**, escolha as configurações a seguir e clique em **Avançar**:
 - o Expiração do Conteúdo: Expira após a seguinte duração (em dias): **7**
 - o Expiração da licença de uso: Expira após a seguinte duração (em dias): **7**
10. Na página **Especificar Política Estendida**, clique em **Solicitar uma nova licença de uso sempre que o conteúdo for consumido (desabilitar cache no lado do cliente)**, clique em **Avançar** e clique em **Concluir**.

Demonstração: Criação de uma política de exclusão para excluir um aplicativo

Etapas da demonstração

1. Em LON-SVR1, alterne para o console do Active Directory Rights Management Services.
2. Clique no nó **Políticas de Exclusão** e clique em **Gerenciar lista de exclusões de aplicativos**.
3. No painel Ações, clique em **Habilitar a Exclusão de Aplicativo**.
4. No painel Ações, clique em **Excluir Aplicativo**.
5. Na caixa de diálogo **Excluir Aplicativo**, digite as informações a seguir e clique em **Concluir**:
 - o Nome de arquivo do aplicativo: **Powerpnt.exe**
 - o Versão mínima: **14.0.0.0**
 - o Versão máxima: **16.0.0.0**

Lição 4

Configuração do acesso externo ao AD RMS

Conteúdo:

Leitura adicional

91

Leitura adicional

Opções para habilitar o acesso ao AD RMS para usuários externos

 **Leitura adicional:** Para saber mais sobre as políticas de confiança do AD RMS, consulte <http://go.microsoft.com/fwlink/?LinkId=270032>.

Implementação de TPD

 **Leitura adicional:** Para saber mais sobre como importar TPDs, consulte Adicionar um domínio de publicação confiável em <http://go.microsoft.com/fwlink/?LinkId=270033>.

Compartilhamento de documentos protegidos pelo AD RMS usando o Windows Live ID

 **Leitura adicional:** Para saber mais sobre como usar o Windows Live ID para estabelecer RACs para usuários, consulte <http://go.microsoft.com/fwlink/?LinkId=270034>.

Revisão e informações complementares do módulo

Prática recomendada

- Antes de implantar o AD RMS, você deve analisar os requisitos comerciais de sua organização e criar os modelos necessários. Você deve se reunir com os usuários para informá-los da funcionalidade do AD RMS e também solicitar comentários sobre os tipos de modelos que eles gostariam de ter à disposição.
- Controle estritamente a associação do grupo Superusuários. Os usuários desse grupo podem acessar todo o conteúdo protegido. Conceder a associação desse grupo ao usuário dá a ele completo acesso a todo o conteúdo protegido pelo AD RMS.

Perguntas de revisão

Pergunta: Quais são os benefícios de ter um certificado SSL instalado no servidor AD RMS quando você está executando a configuração do AD RMS?

Resposta: Você pode proteger a conexão entre clientes e o servidor AD RMS com SSL.

Pergunta: Você precisa fornecer acesso ao conteúdo protegido pelo AD RMS a cinco usuários que são prestadores de serviços não afiliados e não são membros de sua organização. Qual método você deve usar para fornecer esse acesso?

Resposta: Usar o Windows Live ID para fornecer RAC aos prestadores de serviços não afiliados.

Pergunta: Você deseja impedir que os usuários protejam o conteúdo do Office PowerPoint usando modelos do AD RMS. Que etapas você deve executar para alcançar esse objetivo?

Resposta: Você deve configurar uma exclusão de aplicativo para o aplicativo Office PowerPoint.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do AD RMS

Pergunta: Que etapas você pode executar para garantir que você possa usar o Gerenciamento de Direitos de Informação com a função AD RMS?

Resposta: Você precisa configurar um certificado do servidor para o servidor AD RMS antes de implantar o AD RMS.

Módulo 8

Implementação dos Serviços de Federação do Active Directory

Conteúdo:

Lição 1: Visão geral do AD FS	95
Lição 2: Implantação do AD FS	97
Lição 3: Implementação do AD FS para uma única organização	100
Lição 4: Implantação do AD FS em um cenário de federação B2B	103
Revisão e informações complementares do módulo	106
Perguntas e respostas da revisão do laboratório	108

Lição 1

Visão geral do AD FS

Conteúdo:

Leitura adicional

96

Leitura adicional

O que é o AD FS?



Leitura adicional: Para obter informações sobre os produtos de federação de identidade diferentes que podem interoperar com o AD FS e guias passo a passo sobre como configurar os produtos consulte os Guias Passo a Passo e de Instruções do AD FS 2.0, localizados em <http://go.microsoft.com/fwlink/?LinkId=270035>.

Lição 2

Implantação do AD FS

Conteúdo:

Demonstração

98

Demonstração

Demonstração: Instalação da função de servidor do AD FS

Etapas da demonstração

Instalar a função de servidor do AD FS

1. Em LON-DC1, no Gerenciador do Servidor, clique em **Gerenciar** e clique em **Adicionar Funções e Recursos**.
2. Na página **Antes de começar**, clique em **Próximo**.
3. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
4. Na página **Selecionar servidor de destino**, clique em **Próximo**.
5. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Serviços de Federação do Active Directory**, clique em **Adicionar Recursos** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Serviços de Federação do Active Directory (AD FS)**, clique em **Próximo**.
8. Na página **Selecionar serviços de função**, clique em **Próximo**.
9. Na página **Confirmar seleções de instalação**, clique em **Instalar** e aguarde a conclusão da instalação. Não feche a janela.

Configurar a função de servidor do AD FS

1. Na página **Progresso da Instalação**, clique em **Executar o snap-in Gerenciamento do AD FS**.
2. No painel Visão Geral, clique no link **Assistente de Configuração do Servidor de Federação do AD FS**.
3. Na página **Bem-vindo**, verifique se a opção **Criar um novo Serviço de Federação** está selecionada e clique em **Avançar**.
4. Na página **Selecionar Implantação Autônoma ou de Farm**, clique em **Servidor de federação autônomo** e clique em **Avançar**.
5. Na página **Especifique o Nome do Serviço de Federação**, verifique as seguintes configurações e clique em **Avançar**:
 - o Certificado SSL: **LON-DC1.Adatum.com**
 - o Porta: **443**
 - o Nome do Serviço de Federação: **LON-DC1.Adatum.com**

6. Na página **Pronto para Aplicar as Configurações**, verifique se as configurações corretas estão listadas e clique em **Avançar**.
7. Aguarde o término da instalação e clique em **Fechar**.
8. Abra o Windows® Internet Explorer® e conecte-se a **<https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml>**.
9. Descreva as informações de metadados aos alunos.
10. Feche o Internet Explorer.

Lição 3

Implementação do AD FS para uma única organização

Conteúdo:

Demonstração

101

Demonstração

Demonstração: Configuração de relações de confiança do provedor de declarações e de terceira parte confiável

Etapas da demonstração

Configurar uma relação de confiança de provedor de declarações

1. Em LON-DC1, no console do AD FS, expanda **Relações de Confiança** e clique em **Confianças do Provedor de Declarações**.
2. No painel intermediário, clique com o botão direito do mouse em **Active Directory** e clique em **Editar Regras de Declaração**.
3. Na caixa de diálogo **Editar Regras de Declaração para Active Directory**, na guia **Regras de Transformação de Aceitação**, clique em **Adicionar Regra**. O Assistente para Adicionar Regra de Declaração de Transformação é aberto.
4. Na página Seleccionar Modelo de Regra, em **Modelo de regra de declaração**, clique em **Enviar Atributos LDAP como Declarações** e clique em **Avançar**.
5. Na página **Configurar Regra**, na caixa **Nome da regra de declaração**, digite **Regra de Atributos LDAP de Saída**.
6. Na lista suspensa **Repositório de atributos**, clique em **Active Directory**.
7. Na seção **Mapeamento de atributos LDAP para tipos de declaração de saída**, selecione os seguintes valores para o Atributo LDAP e o Tipo de Declaração de Saída:
 - o E-Mail-Addresses = **Endereço de Email**
 - o User-Principal-Name = **UPN**
8. Clique em **Concluir** e clique em **OK**.

Configure um aplicativo do Windows Identity Foundation para AD FS

1. Em LON-SVR1, alterne para a tela inicial e clique em **Windows Identity Foundation Federation Utility**.
2. Na página **Welcome to the Federation Utility wizard**, em **Application configuration location**, digite **C:\inetpub\wwwroot\AdatumTestApp\web.config** para o local do arquivo web.config de exemplo.
3. Em **Application URI**, para indicar o caminho para o aplicativo de exemplo que confiará nas declarações de entrada do servidor de federação, digite **https://lon-svr1.adatum.com/AdatumTestApp/** e clique em **Avançar**.
4. Na página **Security Token Service**, selecione a opção **Use an existing STS**, para o local de documento de metadados de WS-Federation STS, digite **https://lon-dc1.adatum.com/federationmetadata/2007-06/federationmetadata.xml** e clique em **Next**.

5. Na página **Erro de validação da cadeia de certificados de assinatura STS**, selecione a opção **Desabilitar validação da cadeia de certificados** e clique em **Next**.
6. Na página **Security token encryption**, selecione a opção **No encryption** e clique em **Next**.
7. Na página **Declarações oferecidas**, examine as declarações que serão oferecidas pelo servidor de federação e clique em **Next**.
8. Na página **Resumo**, examine as alterações que serão feitas no aplicativo de exemplo pelo Assistente de Utilitário de Federação, percorra os itens para entender o que cada item está fazendo, clique em **Concluir**, e clique em **OK**.

Configure uma relação de confiança de terceira parte confiável

1. Em LON-DC1, no console do AD FS, clique em **AD FS**.
2. No painel intermediário, clique em **Necessário: Adicionar uma terceira parte confiável**.
3. No Assistente para Adicionar Terceira Parte Confiável, na página **Bem-vindo**, clique em **Iniciar**.
4. Na página **Selecionar Fonte de Dados**, selecione a opção **Importar dados sobre a terceira parte confiável publicados online ou em uma rede local** e digite **https://lon-svr1.adatum.com/adatumtestapp**.
5. Para continuar, clique em **Avançar**. Esta ação solicita que o assistente procure Metadados do aplicativo que a função de servidor Web hospeda.
6. Na página **Especificar Nome para Exibição**, na caixa **Nome para exibição**, digite **ADatum Test App** e clique em **Avançar**.
7. Na página **Escolher Regras de Autorização de Emissão**, verifique se a opção **Permitir que todos os usuários acessem esta terceira parte confiável** está selecionada e clique em **Avançar**.
8. Na página **Pronto para Adicionar Confiança**, examine as configurações da relação de confiança da terceira parte confiável e clique em **Avançar**.
9. Na página **Concluir**, clique em **Fechar**. A caixa de diálogo **Editar Regras de Declaração para Adatum Test App** é aberta.

Lição 4

Implantação do AD FS em um cenário de federação B2B

Conteúdo:

Leitura adicional	104
Demonstração	104

Leitura adicional

Como a descoberta de realm inicial funciona



Leitura adicional: Para obter mais informações sobre RelayState, consulte o site de suporte ao RelayState iniciado pelo provedor de identidade localizado em <http://go.microsoft.com/fwlink/?LinkId=270036>.

Demonstração

Demonstração: Configuração de regras de declarações

Etapas da demonstração

Configurar regras de declarações

1. Em LON-DC1, se necessário, abra o console do AD FS.
2. Em **Relações de Confiança**, clique em **Confianças da Terceira Parte Confiável**.
3. Selecione **Adatum Test App** e, no painel **Ações**, clique em **Editar Regras de Declaração**.
4. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
5. Em **Modelo de regra de declaração**, clique em **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
6. Em **Nome da regra de declaração**, digite **Regra de Envio de Nome de Grupo**.
7. Na lista suspensa **Tipo de declaração de entrada**, clique em **Group** e clique em **Concluir**.
8. Na caixa de diálogo **Editar Regras de Declaração para Adatum Test App**, na guia **Regras de Autorização de Emissão**, selecione a regra chamada **Permitir Acesso a Todos os Usuários** e clique em **Remover Regra**. Clique em **Sim** para confirmar. Sem regras, os usuários não têm permissão de acesso.
9. Na guia **Regras de Autorização de Emissão**, clique em **Adicionar Regra**.
10. Na página **Selecionar Modelo de Regra**, em **Modelo de regra de declaração**, selecione **Permitir ou Negar Usuários com Base em uma Declaração de Entrada** e clique em **Avançar**.
11. Na página **Configurar Regra**, na caixa **Nome da regra de declaração**, digite **Regra de Permissão de Grupo de Produção** e, na lista suspensa **Tipo de declaração de entrada**, selecione **Grupo**. No campo **Valor de declaração de entrada**, digite **Production**, selecione a opção para **Permitir acesso a usuários com esta declaração de entrada** e clique em **Concluir**.
12. Na guia **Regras de Autorização de Emissão**, clique em **Adicionar Regra**.
13. Na página **Selecionar Modelo de Regra**, em **Modelo de regra de declaração**, selecione **Permitir ou Negar Usuários com Base em uma Declaração de Entrada** e clique em **Avançar**.

14. Na página **Configurar Regra**, na caixa **Nome da regra de declaração**, digite **Permitir Usuários da A Datum** e, na lista suspensa **Tipo de declaração de entrada**, selecione **UPN**. No campo **Valor de declaração de entrada**, digite **@adatum.com**, selecione a opção para **Permitir acesso a usuários com esta declaração de entrada** e clique em **Concluir**.
15. Clique na regra **Permitir Usuários da A Datum** e clique em **Editar Regra**.
16. Na caixa de diálogo **Editar Regra .- Permitir Usuários da Adatum**, clique em **Exibir Idioma da Regra**. Observe que os alunos editarão o idioma da regra no laboratório.
17. Clique em **OK** e clique em **Cancelar**.

Revisão e informações complementares do módulo

Pergunta: Quais são as vantagens de implantar o AD FS com um aplicativo ou serviço baseado na nuvem?

Resposta: As principais vantagens são que as organizações precisam apenas gerenciar contas de usuário no domínio do AD DS local e os usuários só precisam se lembrar de um único conjunto de credenciais. Além disso, a organização no local tem que gerenciar apenas contas de usuário, enquanto a empresa de hospedagem de aplicativo na nuvem tem que gerenciar apenas seus aplicativos.

Pergunta: Em quais circunstâncias você optaria por implantar um servidor proxy de federação? Em quais circunstâncias você não precisa implantar um servidor proxy de federação?

Resposta: Você deve implantar um servidor proxy de federação sempre que os usuários que estiverem fora da rede precisarem acessar a implantação do AD FS. Se os únicos usuários que acessarem a implantação do AD FS forem internos à rede, um servidor proxy de federação não será necessário.

Problemas e cenários reais

Pergunta: A Tailspin Toys está implantando um novo aplicativo Web baseado em declarações, que precisa estar acessível aos usuários da Tailspin Toys e aos usuários da Trey Research. Quais componentes do AD FS você precisará implantar na Tailspin Toys para permitir esse nível de acesso?

Resposta: Você deve implantar um proxy de servidor de federação. Além disso, no servidor de federação Tailspin Toys, será necessário configurar a relação de confiança de provedor de declarações do Active Directory e criar uma relação de confiança de provedor de declarações para a Trey Research. Também será necessário configurar uma relação de confiança de terceira parte confiável no servidor de federação da Tailspin Toys para o aplicativo Web.

Pergunta: A Fabrikam, Inc. está examinando os requisitos de AD FS. A empresa deseja usar um servidor proxy de federação para obter segurança máxima. Atualmente, a Fabrikam tem uma rede interna com servidores DNS internos e seu DNS voltado para Internet é hospedado por uma empresa de hospedagem. A rede de perímetro usa os servidores DNS da empresa de hospedagem para resolução de DNS. O que a empresa deve fazer para se preparar para a implantação?

Resposta: O servidor proxy de federação deve ser capaz de resolver os endereços IP para o servidor AD FS interno. Portanto, você precisaria adicionar os servidores AD FS internos a um arquivo Hosts no servidor proxy de federação ou alterar a maneira como os servidores de rede de perímetro resolvem nomes.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
Erros de certificado no servidor de federação	<ul style="list-style-type: none">• Verificar se o certificado está no repositório de certificados.• Verifique se o certificado expirou ou foi revogado.• Verifique se o certificado tem uma chave privada associada.• Verifique se há permissões válidas no certificado.• Verifique se o certificado é confiável.
Erros de certificado no cliente	Verifique se todos os certificados necessários para interação de cliente são confiáveis.
Falha do aplicativo cliente na autenticação do AD FS	<ul style="list-style-type: none">• Valide a configuração das declarações e das regras de declaração.• Peça ao usuário para tentar entrar em outros aplicativos.• Verifique se a conta não expirou ou foi bloqueada.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação dos Serviços de Federação do Active Directory

Pergunta: Neste laboratório, você implementou o acesso a um aplicativo com reconhecimento de declarações para usuários internos e externos. Que etapas adicionais você teve que executar na terceira parte confiável para permitir o acesso para usuários externos?

Resposta: Você precisou configurar uma relação de confiança de provedor de declarações na terceira parte confiável. Quando o servidor de federação de terceira parte confiável confiou nas credenciais do provedor de declarações, os usuários tiveram acesso ao aplicativo. Observe que você também teve que configurar uma relação de confiança de terceira parte confiável no provedor de declarações. Em uma situação real, você provavelmente também configuraria regras de confiança adicionais para limitar quais usuários podem acessar o aplicativo.

Pergunta: Como você pode identificar quais declarações foram usadas para fornecer acesso de usuário ao aplicativo de exemplo do Windows Identity Foundation usado no laboratório?

Resposta: O site exibido quando o usuário acessa o site que exibe informações sobre quais declarações o usuário apresentou para obter acesso ao site.

Módulo 9

Implementação do Balanceamento de Carga de Rede

Conteúdo:

Lição 2: Configuração de um cluster NLB	110
Lição 3: Planejamento de uma implementação do NLB	114
Revisão e informações complementares do módulo	116
Perguntas e respostas da revisão do laboratório	117

Lição 2

Configuração de um cluster NLB

Conteúdo:

Demonstração

111

Demonstração

Demonstração: Implantação do NLB

Etapas da demonstração

Criação de um cluster NLB do Windows Server 2012

1. Em LON-SVR1, na barra de tarefas, clique no ícone Gerenciador do Servidor.
2. No console do Gerenciador do Servidor, clique no menu **Ferramentas** e clique em **Windows PowerShell ISE**.
3. Na janela do ISE do Windows PowerShell, digite o comando a seguir e pressione Enter:

```
Invoke-Command -ComputersName LON-SVR1,LON-SVR2 -command {Install-WindowsFeature NLB,RSAT-NLB}
```

4. Digite o seguinte comando e pressione Enter:

```
New-NlbCluster -InterfaceName "Conexão Local" -OperationMode Multicast - ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
```

5. Digite o seguinte comando e pressione Enter:

```
Add-NlbClusterNode -InterfaceName "Conexão Local" -NewNodeName "LON-SVR2" - NewNodeInterface "Conexão Local"
```

6. No console do Gerenciador do Servidor, clique no menu **Ferramentas** e clique em **Gerenciador de Balanceamento de Carga de Rede**.
7. Verifique que os nós LON-SVR1 e LON-SVR2 são exibidos com o status **Convergiado** para o cluster LON-NLB.
8. Clique com o botão direito do mouse do mouse no cluster **LON-NLB** e clique em **Propriedades do cluster**.
9. Regras de portde **LON-NLB (172.16.0.42)**, na guia **Parâmetros do Cluster**, verifique se o cluster está definido para usar o modo de operação Multicast.
10. Na guia **Regras de porta**, verifique se há uma única regra de porta chamada **Tudo** que inicia na porta **0** e termina na porta **65535** para os protocolos TCP e UDP, e usa a afinidade Única.
11. Clique em **OK** para fechar a caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**.

Demonstração: Configuração das regras de porta e da afinidade do NLB

Etapas da demonstração

Configurar a afinidade dos nós de cluster NLB

1. Em LON-SVR2, na barra de tarefas, clique no ícone do Windows PowerShell.
2. No prompt do Windows PowerShell, digite os seguintes comandos, pressionando Enter depois de cada um deles:

```
Cmd.exe
Mkdir c:\porttest
Xcopy /s c:\inetpub\wwwroot c:\porttest
Exit
New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678
New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678
```

Configurar as regras de porta do NLB

1. Em LON-SVR1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Gerenciador de Balanceamento de Carga de Rede**.
2. No Gerenciador de Balanceamento de Carga de Rede, clique com o botão direito do mouse em **LON-NLB** e clique em **Propriedades do cluster**.
3. Na caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**, na guia **Regras de porta**, selecione a regra **Tudo** e clique em **Remover**.
4. Clique em **OK** para fechar a caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**.
5. No Gerenciador de Balanceamento de Carga de Rede, clique com o botão direito do mouse em **LON-NLB**, e clique em **Propriedades do cluster**.
6. Na caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**, na guia **Regras de porta**, clique em **Adicionar**.
7. Na caixa de diálogo **Adicionar/editar regra de porta**, digite as informações a seguir e clique em **OK**:
 - o Intervalo de portas: **80 A 80**
 - o Protocolos: **Ambos**
 - o Modo de filtragem: **Vários hosts**
 - o Afinidade: **Nenhuma**
8. Clique em **OK** para fechar a caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**.
9. No Gerenciador de Balanceamento de Carga de Rede, clique com o botão direito do mouse em **LON-NLB** e clique em **Propriedades do cluster**.
10. Na guia **Regras de porta**, clique em **Adicionar**.

11. Na caixa de diálogo **Adicionar/editar regra de porta**, digite as informações a seguir e clique em **OK**:
 - Intervalo de portas: **5678 A 5678**
 - Protocolos: **Ambos**
 - Modo de filtragem: **Host único**
12. Clique em **OK** para fechar a caixa de diálogo **Propriedades de LON-NLB (172.16.0.42)**.
13. No Gerenciador de Balanceamento de Carga de Rede, clique com o botão direito do mouse em **LON-SVR1** e clique em **Propriedades do host**.
14. Na guia **Regras de porta**, clique na regra de porta que tem **5678** como valor de Início e Fim, e clique em **Editar**.
15. Clique no valor **Prioridade de tratamento** e altere-o para **10**.
16. Clique em **OK** duas vezes para fechar as caixas de diálogo **Adicionar/editar regra de porta** e **Propriedades de LON-SVR1 (Conexão Local)**.

Lição 3

Planejamento de uma implementação do NLB

Conteúdo:

Leitura adicional

115

Leitura adicional

Considerações sobre a atualização dos clusters NLB



Links de referência: Obtenha mais informações sobre como atualizar clusters NLB em <http://go.microsoft.com/fwlink/?LinkId=270037>.

Revisão e informações complementares do módulo

Perguntas de revisão

Pergunta: Você criou um cluster NLB do Windows Server 2012 de quatro nós. O cluster hospeda um site que é hospedado no IIS. O que acontecerá com o cluster se você desligar o serviço de publicação na World Wide Web em um dos nós?

Resposta: Nada acontecerá, porque o NLB só detecta falha de servidor, e não a falha de um aplicativo específico.

Pergunta: Você deseja hospedar os sites `www.contoso.com`, `www.adatum.com` e `www.fabrikam.com` em um cluster NLB de quatro nós. O endereço IP do cluster será um endereço IP público, e cada nome de domínio totalmente qualificado (FQDN) é mapeado no DNS para o endereço IP público do cluster. Quais etapas você deve executar em cada nó para assegurar que tráfego será direcionado para o site apropriado?

Resposta: Você precisará configurar cabeçalhos de host para cada site em cada nó. Além disso, você deve assegurar que a configuração de cabeçalho de host é idêntica.

Pergunta: Você tem um cluster NLB do Windows de oito nós que hospeda um aplicativo Web. Você deseja assegurar que o tráfego de um cliente que usa o cluster permanece com o mesmo nó ao longo de toda a sessão, mas esse tráfego de clientes separados é distribuído equitativamente por todos os nós. Qual opção você configurará para atingir essa meta?

Resposta: Você deve definir as configurações de afinidade para obter o resultado desejado.

Problemas e cenários reais

Para se tornar uma verdadeira solução de alta disponibilidade, use uma solução de monitoramento com NLB que detectará falha de aplicativo. Isso acontece porque os clusters NLB continuarão direcionando tráfego para nós que têm aplicativos com falha, contanto que o NLB, que é independente do aplicativo, continue enviando tráfego de pulsação.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do balanceamento de carga de rede

Pergunta: Quantos nós adicionais você pode adicionar ao cluster LON-NLB?

Resposta: O cluster LON-NLB pode crescer até 32 nós.

Pergunta: Quais etapas você executaria para assegurar que LON-SVR1 sempre gerenciara as solicitações de tráfego da Web na porta 5678, considerando as regras de porta existentes no final deste exercício?

Resposta: Você configura a prioridade de host. Você também define a regra para usar um único modo de filtragem de host.

Pergunta: Qual é a diferença entre a ação Parada e Interrupção de descarga?

Resposta: A Parada encerra todas as conexões ativas imediatamente. A Interrupção de descarga bloqueia novas conexões, mas permite que as conexões existentes sejam concluídas normalmente.

Módulo 10

Implementação do cluster de failover

Conteúdo:

Lição 2: Implementação de um cluster de failover	119
Lição 3: Configuração de aplicativos e serviços altamente disponíveis em um cluster de failover	121
Lição 4: Manutenção de um cluster de failover	123
Revisão e informações complementares do módulo	126
Perguntas e respostas da revisão do laboratório	128

Lição 2

Implementação de um cluster de failover

Conteúdo:

Demonstração

120

Demonstração

Demonstração: Validação e configuração de um cluster de failover

Etapas da demonstração

Validar e configurar um cluster

1. Em LON-SVR3, na barra de tarefas, clique no ícone Gerenciador do Servidor.
2. No Gerenciador do Servidor, clique em **Ferramentas** e clique em **Gerenciador de Cluster de Failover**.
3. No snap-in Gerenciador de Cluster de Failover, na árvore do console, verifique se **Gerenciador de Cluster de Failover** está selecionado, em **Gerenciamento**, clique em **Validar Configuração** e clique em **Próximo**.
4. No campo **Digitar nome**, digite **LON-SVR3** e clique em **Adicionar**.
5. No campo **Digitar nome**, digite **LON-SVR4**.
6. Clique em **Adicionar** e clique em **Próximo**.
7. Verifique se **Executar todos os testes (recomendado)** está selecionado e clique em **Próximo**.
8. Na janela Confirmação, clique em **Próximo**.
9. Aguarde a conclusão dos testes de validação e, na janela Resumo, clique em **Exibir Relatório**.
10. Revise as informações e feche o relatório.
11. No Assistente para Validar uma Configuração, desmarque a caixa de seleção ao lado de **Criar o cluster agora usando os nós validados** e clique em **Concluir**.
12. Em LON-SVR3, no console do Gerenciador de Cluster de Failover, na seção **Gerenciamento** do painel central, clique em **Criar Cluster**.
13. Revise a página **Antes de começar**.
14. Clique em **Avançar**, digite **LON-SVR3** e clique em **Adicionar**. Digite **LON-SVR4** e clique em **Adicionar**.
15. Verifique as entradas e clique em **Próximo**.
16. Na página **Ponto de Acesso para Administrar o Cluster**, digite **Cluster1** como nome do cluster. Em **Endereço**, no campo **Endereço IP**, digite **172.16.0.125** e clique em **Próximo**.
17. Na caixa de diálogo **Confirmação**, verifique as informações, desmarque a caixa de seleção ao lado de **Adicione todo o armazenamento qualificado ao cluster** e clique em **Próximo**.
18. Na página **Resumo**, clique em **Concluir** para retornar ao Gerenciador de Cluster de Failover.

Lição 3

Configuração de aplicativos e serviços altamente disponíveis em um cluster de failover

Conteúdo:

Demonstração

122

Demonstração

Demonstração: Clustering de uma função de servidor de arquivos

Etapas da demonstração

Clusterizar uma função de servidor de arquivos

1. Em LON-SVR3, abra o **Gerenciamento de Cluster de Failover**.
2. Expanda **Cluster1.Adatum.com**, expanda **Armazenamento** e clique em **Discos**.
3. No painel Ações, clique em **Adicionar Disco**.
4. Desmarque as três caixas de seleção.
5. Marque a caixa de seleção ao lado de **Disco de Cluster 2** e clique em **OK**.
6. Clique com o botão direito do mouse em **Funções** e clique em **Configurar Função**.
7. Na página **Antes de começar**, clique em **Próximo**.
8. Na página **Selecionar Função**, clique em **Servidor de Arquivos** e clique em **Próximo**.
9. Na página **Tipo de Servidor de Arquivos**, clique em **Servidor de Arquivos para uso geral** e clique em **Próximo**.
10. Na página **Ponto de Acesso do Cliente**, na caixa **Nome**, digite **Adatum-FS**. Na caixa **Endereço**, digite **172.16.0.55** e clique em **Próximo**.
11. Na página **Selecionar Armazenamento**, clique na caixa de seleção anterior a **Disco de Cluster 2** e clique em **Próximo**.
12. Na página **Confirmação**, clique em **Próximo**.
13. Na página **Resumo**, clique em **Concluir**.

Lição 4

Manutenção de um cluster de failover

Conteúdo:

Demonstração

124

Demonstração

Demonstração: Configuração da CAU

Etapas da demonstração

Configurar a CAU

1. Entre em LON-DC1 com o nome de usuário **Adatum\Administrador** e a senha **Pa\$\$w0rd**.
2. No Gerenciador do Servidor, clique em **Adicionar funções e recursos**.
3. No Assistente de Adição de Funções e Recursos, na página **Antes de começar**, clique em **Próximo**.
4. Na página **Selecionar tipo de instalação**, clique em **Próximo**.
5. Na página **Selecionar servidor de destino**, verifique se **Selecionar servidor no pool de servidor** está selecionado e clique em **Próximo**.
6. Na página **Selecionar funções de servidor**, clique em **Próximo**.
7. Na página **Selecionar recursos**, na lista de recursos, clique em **Clustering de Failover**.
8. Na caixa de diálogo **Adicionar recursos que são necessários para Clustering de Failover?**, clique em **Adicionar Recursos** e clique em **Próximo**.
9. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
10. Quando a instalação for concluída, clique em **Fechar**.
11. Em LON-DC1, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Atualização com Suporte a Cluster**.
12. Na janela Atualização com Suporte a Cluster, na lista suspensa **Conectar ao cluster de failover**, clique em **CLUSTER1** e clique em **Conectar**.
13. No painel Ações de Cluster, clique em **Visualizar atualizações para este cluster**.
14. Na janela Visualizar Atualizações de Cluster1, clique em **Gerar Lista de Visualização da Atualização**.



Observação: Você precisa ter uma conexão com Internet para executar esta etapa.

15. Após vários minutos, as atualizações serão exibidas na lista. Revise as atualizações e clique em **Fechar**.
16. No painel Ações de Cluster, clique em **Criar ou modificar Perfil de Execução da Atualização**.
17. Revise e explique as opções disponíveis. Não faça nenhuma alteração e, quando você terminar, clique em **Fechar**.
18. Clique em **Aplicar atualizações a este cluster**.
19. Na página **Guia de Introdução**, clique em **Próximo**.
20. Na página **Opções avançadas**, revise as opções de atualização e clique em **Próximo**.

21. Na página **Opções Adicionais de Atualização**, clique em **Próximo**.
22. Na página **Confirmação**, clique em **Atualizar** e clique em **Fechar**.
23. No painel Nós de cluster, revise o andamento das atualizações.



Observação: Você deve enfatizar que um nó do cluster está no estado Aguardando, enquanto o outro nó está reiniciando depois de ser atualizado.

24. Aguarde a conclusão do processo. (Observação: isso pode exigir a reinicialização de ambos os nós).
25. Entre em LON-SVR3 com o nome de usuário **Adatum\Administrador** e a senha **Pa\$\$w0rd**.
26. Em LON-SVR3, no Gerenciador do Servidor, clique em **Ferramentas** e clique em **Atualização com Suporte a Cluster**.
27. Na janela Atualização com Suporte a Cluster, na lista suspensa **Conectar ao cluster de failover**, selecione **CLUSTER1** e clique em **Conectar**.
28. Clique em **Configurar opções de autoatualização de cluster**.
29. Na página **Guia de Introdução**, clique em **Próximo**.
30. Na página **Adicionar Função Clusterizada CAU com Autoatualização Habilitada**, clique em **Adicionar a função clusterizada CAU, com o modo de autoatualização habilitado, a este cluster** e clique em **Próximo**.
31. Na área **Especificar agenda de autoatualização**, clique em **Semanalmente**, selecione **4:00AM** para Hora do dia, selecione **Domingo** para Dia da semana e clique em **Próximo**.
32. Na página **Opções Avançadas**, clique em **Próximo**.
33. Na página **Opções Adicionais de Atualização**, clique em **Próximo**.
34. Na página **Confirmação**, clique em **Aplicar**.
35. Na página Conclusão, clique em **Fechar**.

Revisão e informações complementares do módulo

Perguntas de revisão

Pergunta: Por que usar uma configuração de quorum Sem Maioria: Somente Disco geralmente não é uma boa ideia?

Resposta: Quando você usa uma configuração de quorum Sem Maioria: Somente Disco, o cluster de failover para de funcionar quando o LUN que é usado como disco de quorum falha. Mesmo se todos os outros recursos – incluindo discos para os aplicativos – estiverem disponíveis, nenhum dos nós fornecerá serviço quando o disco de quorum não estiver disponível.

Pergunta: Qual é a finalidade da CAU?

Resposta: A CAU é um recurso que permite que os administradores atualizem nós de cluster automaticamente, com pouca ou nenhuma perda de disponibilidade durante o processo de atualização, o que garante que cada nó do cluster seja atualizado.

Pergunta: Qual é a principal diferença entre replicação síncrona e assíncrona em um cenário de cluster multissite?

Resposta: Quando você usa a replicação síncrona, o host recebe uma resposta de gravação concluída do armazenamento primário depois que os dados são gravados com êxito em ambos os sistemas de armazenamento. Se os dados não forem gravados com êxito em ambos os sistemas de armazenamento, o aplicativo deverá tentar gravar novamente em disco. Com a replicação síncrona, ambos os sistemas de armazenamento são idênticos.

Quando você usa a replicação assíncrona, o nó recebe uma resposta de gravação concluída do armazenamento depois que os dados são gravados com êxito no armazenamento primário. Os dados são gravados no armazenamento secundário em uma programação diferente, dependendo da implementação do fornecedor de hardware ou software.

Pergunta: O que é o recurso aprimorado de cluster multissite no Windows Server 2012?

Resposta: No Windows Server 2012, você pode ajustar as configurações de quorum do cluster de forma que, quando o cluster determinar se tem quorum, alguns nós tenham um voto e outros não.

Problemas e cenários reais

Pergunta: Sua organização está considerando o uso de um cluster geograficamente disperso que inclua um datacenter alternativo. Sua organização tem apenas um local físico aliado a um datacenter alternativo. Você pode fornecer um failover automático nessa configuração?

Resposta: Não. Você não pode fornecer um failover automático nessa configuração. Para fornecer um failover automático, você deve ter pelo menos três locais.

Ferramentas

As ferramentas para implementação do cluster de failover incluem:

- Console do Gerenciador de Cluster de Failover
- Console Atualização com Suporte a Cluster
- Windows PowerShell
- Gerenciador do Servidor
- Iniciador iSCSI
- Gerenciamento de Disco

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do cluster de failover

Pergunta: Que informações você terá de coletar enquanto planeja uma implementação de cluster de failover e escolhe um modo de quorum?

Resposta: Você tem de coletar informações como:

- O número de aplicativos ou serviços que você implantará no cluster.
- Os requisitos de desempenho e características de cada aplicativo ou serviço.
- O número de servidores que devem estar disponíveis para atender aos requisitos de desempenho.
- O local dos usuários que usarão o cluster de failover.
- O tipo de armazenamento do cluster compartilhado.

Pergunta: Depois de executar o Assistente para Validar uma Configuração, como você pode resolver o único ponto de falha de comunicação de rede?

Resposta: Você pode resolver o único ponto de falha de comunicação de rede adicionando adaptadores de rede em uma rede separada. Isso fornecerá redundância de comunicação entre os nós do cluster.

Pergunta: Em quais situações poderia ser importante habilitar o failback de um aplicativo clusterizado apenas durante um período específico?

Resposta: Definir o failback como um nó preferido em um período específico é importante quando você tem de garantir que o failback não interfira com as conexões de cliente, janelas de backup ou outra manutenção que um failback interromperia.

Módulo 11

Implementação do cluster de failover com o Hyper-V

Conteúdo:

Lição 2: Implementação de máquinas virtuais do Hyper-V em clusters de failover	130
Lição 3: Implementação da movimentação de máquinas virtuais do Hyper-V	132
Revisão e informações complementares do módulo	135
Perguntas e respostas da revisão do laboratório	136

Lição 2

Implementação de máquinas virtuais do Hyper-V em clusters de failover

Conteúdo:

Demonstração

131

Demonstração

Demonstração: Implementação de máquinas virtuais em clusters (opcional)

Etapas da demonstração

Movimentação do armazenamento da máquina virtual para o destino iSCSI

1. Na LON-HOST1, abra uma janela do Explorador de Arquivos. No Explorador de Arquivos, expanda a unidade **E**, expanda **Arquivos de Programas, Microsoft Learning, 24412, 24412B-LON-CORE** e **Discos Rígidos Virtuais**.
2. Na pasta Discos Rígidos Virtuais, mova o arquivo de disco rígido virtual **24412B-LON-CORE.vhd** para **C:\ClusterStorage\Volume1**.

Configure a máquina como altamente disponível.

1. No console do Gerenciador de Cluster de Failover, clique em **Funções** e, no painel Ações, clique em **Máquinas Virtuais**.
2. Clique em **Nova Máquina Virtual**.
3. Clique em **LON-HOST2** e clique em **OK**.
4. No Assistente de Nova Máquina Virtual, clique em **Avançar**.
5. Na página **Especificar Nome e Local**, na caixa de texto **Nome**, digite **TestClusterVM**, clique em **Armazenar a máquina virtual em outro local** e clique em **Procurar**.
6. Navegue até **C:\ClusterStorage\Volume1** e selecione-o, clique em **Selecionar Pasta** e clique em **Avançar**.
7. Na página **Atribuir Memória**, digite **1536** e clique em **Avançar**.
8. Na página **Configurar Rede**, clique em **Rede Externa**, e clique em **Avançar**.
9. Na página **Conectar Disco Rígido Virtual**, clique em **Usar um disco rígido virtual existente** e clique em **Procurar**.
10. Navegue até **C:\ClusterStorage\Volume1**, selecione **24412B-LON-CORE.vhd** e clique em **Abrir**.
11. Clique em **Avançar** e clique em **Concluir**.
12. No Assistente para Alta Disponibilidade, na página **Resumo**, clique em **Concluir**.
13. Clique com o botão direito do mouse do mouse em **TestClusterVM**, e clique em **Iniciar**.
14. Verifique se a máquina é iniciada com êxito.

Lição 3

Implementação da movimentação de máquinas virtuais do Hyper-V

Conteúdo:

Demonstração

133

Demonstração

Demonstração: Implementação da Réplica do Hyper-V (opcional)

Etapas da demonstração

Configuração de uma réplica

1. Em LON-HOST2, abra o Gerenciador Hyper-V.
2. No Gerenciador Hyper-V, clique com o botão direito do mouse em **LON-HOST2** e clique em **Configurações do Hyper-V**.
3. Em **Configurações do Hyper-V para LON-HOST2**, clique em **Configuração de Replicação**.
4. No painel Configuração de Replicação, clique em **Habilitar este computador como um Servidor de réplica**.
5. Na seção Autenticação e portas, clique em **Usar Kerberos (HTTP)**.
6. Na seção Autorização e armazenamento, clique em **Permitir replicação em qualquer servidor autenticado** e clique em **Procurar**.
7. Clique em **Computador**, clique duas vezes em **Disco Local (E)**, clique em **Nova pasta**, na caixa de texto **Nome**, digite **VMReplica** e pressione Enter.
8. Clique na pasta **E:\VMReplica** e clique em **Selecionar Pasta**.
9. Em **Configurações do Hyper-V para LON-HOST2**, clique em **OK**.
10. Na janela Configurações, leia o aviso e clique em **OK**.
11. Clique em **Iniciar**, em **Painel de Controle**, em **Sistema e Segurança** e clique em **Firewall do Windows**.
12. Clique em **Configurações avançadas** e clique em **Regras de Entrada**.
13. No painel direito, na lista de regras, localize a regra **Ouvinte de HTTP da Réplica do Hyper-V (TCP-In)**. Clique com o botão direito do mouse na regra e clique em **Habilitar Regra**.
14. Feche o console do Firewall do Windows com Segurança Avançada e feche o Firewall do Windows.
15. Repita as etapas de 1 a 14 em LON-HOST1.

Configuração da replicação

1. Em LON-HOST1, abra o Gerenciador Hyper-V, clique em **LON-HOST1**, clique com o botão direito em **24412B-LON-CORE** e clique em **Habilitar Replicação**.
2. Na página **Antes de Começar**, clique em **Avançar**.
3. Na página **Especificar Servidor de Réplica**, clique em **Procurar**.
4. Na janela Selecionar Computador, digite **LON-HOST2**, clique em **Verificar Nomes**, clique em **OK** e clique em **Avançar**.
5. Na página **Especificar Parâmetros de Conexão**, revise as configurações, assegure que a opção **Usar autenticação Kerberos (HTTP)** está selecionada e clique em **Avançar**.

6. Na página **Escolher VHDs de Replicação**, assegure que **24412B-LON-CORE.vhd** esteja selecionado e clique em **Avançar**.
7. Na página **Configurar Histórico de Recuperação**, clique em **Somente o ponto de recuperação mais recente** e clique em **Avançar**.
8. Na página **Escolher Método de Replicação Inicial**, clique em **Enviar cópia inicial pela rede**, clique em **Iniciar replicação imediatamente** e clique em **Avançar**.
9. Na página **Concluindo o assistente Habilitar Replicação**, clique em **Concluir**.
10. Aguarde de 10 a 15 minutos. No Gerenciador Hyper-V, na coluna **Status**, você pode monitorar o progresso da replicação inicial. Quando a replicação for concluída, assegure que 24412B-LON-CORE aparece em LON-HOST2 no Gerenciador Hyper-V.

Revisão e informações complementares do módulo

Prática recomendada

- Desenvolva as configurações padrão antes de implementar máquinas virtuais altamente disponíveis. Os computadores host devem ser configurados da forma mais idêntica possível. Para garantir que você tenha uma plataforma Hyper-V consistente, configure nomes de rede padrão e use padrões de nomenclatura consistentes para volumes CSV.
- Implemente o VMM. O VMM fornece uma camada de gerenciamento sobre o Hyper-V e o Gerenciamento de Cluster de Failover que pode impedi-lo de cometer erros ao gerenciar máquinas virtuais altamente disponíveis. Por exemplo, ele impedirá você de criar máquinas virtuais em um armazenamento que não possa ser acessado em todos os nós do cluster.

Perguntas de revisão

Pergunta: No Windows Server 2008 R2, você precisa implementar o CSV para fornecer alta disponibilidade para máquinas virtuais no VMM?

Resposta: Não, você não precisa implementar o CSV para oferecer alta disponibilidade. Entretanto, o CSV facilita a implementação e o gerenciamento de um ambiente no qual haja vários hosts do Hyper-V acessando vários LUNs no armazenamento compartilhado.

Ferramentas

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
O failover de máquina virtual apresenta falha após a implementação do CSV e a migração do armazenamento compartilhado para o CSV	A pasta base do CSV está localizada na unidade do sistema do servidor host. Você não pode movê-la. Se os computadores host usarem unidades de sistema diferentes, os failovers falharão porque os hosts não podem acessar o mesmo local de armazenamento. Todos os nós de cluster de failover devem usar a mesma configuração de disco rígido.
Uma máquina virtual faz failover para outro nó no cluster de host, mas perde toda a conectividade de rede.	Todos os nós em um cluster de host devem ter as mesmas redes configuradas. Caso contrário, as máquinas virtuais não poderão se conectar a uma rede quando fizerem failover para outro nó.
Quatro horas após reiniciar um host do Hyper-V que é membro de um cluster de host, ainda não há máquinas virtuais em execução no host.	Por padrão, as máquinas virtuais não fazem failback para um computador host após migrarem para outro host. Você pode habilitar o failback nas propriedades de máquina virtual do Gerenciador de Cluster de Failover ou implementar o PRO no VMM.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do cluster de Failover com o Hyper-V

Pergunta: O que é a principal finalidade da Réplica do Hyper-V?

Resposta: A Réplica do Hyper-V fornece basicamente uma cópia auxiliar de uma máquina virtual em execução em outro host que você pode ativar sob demanda. Você pode usar essa máquina virtual em cenários de recuperação de desastre.

Pergunta: Qual é a diferença entre migração ao vivo e migração de armazenamento?

Resposta: A migração ao vivo requer que o cluster de Failover seja implementado com o Hyper-V. Com a migração ao vivo, os nós de cluster devem ter o armazenamento compartilhado onde os arquivos de máquina virtual estão armazenados. A migração de armazenamento pode migrar os arquivos de máquina virtual em um servidor ou entre dois servidores, sem armazenamento compartilhado e clustering.

Módulo 12

Implementação da recuperação de desastres

Conteúdo:

Lição 2: Implementação do backup do Windows Server	138
Lição 3: Implementação da recuperação de dados e de servidor	141
Revisão e informações complementares do módulo	143
Perguntas e respostas da revisão do laboratório	145

Lição 2

Implementação do backup do Windows Server

Conteúdo:

Leitura adicional	139
Demonstração	139

Leitura adicional

O que é o Windows Azure Online Backup?



Links de referência: Obtenha mais informações sobre o Windows Azure em <http://go.microsoft.com/fwlink/?LinkId=270041>.



Observação: Neste momento, o Windows Azure Backup Online não está disponível em todos os países. Para obter informações atualizadas, visite <http://go.microsoft.com/fwlink/?LinkId=270042>.

Demonstração

Demonstração: Configuração de um backup agendado

Etapas da demonstração

1. Alterne para LON-SVR1.
2. Em LON-SVR1, no Gerenciador do Servidor, clique em **Ferramentas**, e clique em **Backup do Windows Server**.
3. Clique em **Backup Local**, e, no painel Ações, clique em **Agendamento de Backup**.
4. No Assistente de Agendamento de Backup, na página **Ponto de Partida**, clique em **Avançar**.
5. Na página **Selecionar Configuração de Backup**, clique em **Personalizar**, e clique em **Avançar**.
6. Na página **Selecionar Itens para Backup**, clique em **Adicionar Itens**.
7. Expanda **Disco Local (C:)**, marque a caixa de seleção **HR Data** e clique em **OK**.
8. Clique em **Configurações Avançadas**.
9. Clique em **Adicionar Exclusão**, em **C:\HR Data\Old HR file.txt** e clique em **OK**.
10. Clique em **OK** para fechar a caixa de diálogo **Configurações Avançadas**.
11. Clique em **Avançar**.
12. Na página **Especificar horário do backup**, ao lado de **Selecione a hora do dia**, selecione **1:00** e clique em **Avançar**.
13. Na página **Especificar Tipo de Destino**, clique em **Fazer Fazer backup em uma pasta de rede compartilhada**, e clique em **Avançar**. Examine o aviso e clique em **OK**.
14. Na página **Especificar Pasta Compartilhada Remota**, na caixa de texto **Local**, digite **\\LON-DC1\Backup** e clique em **Avançar**.
15. Na caixa de diálogo **Registrar Agendamento de Backup**, na caixa de texto **Nome do usuário**, digite **Administrador**, na caixa de texto **Senha**, digite **Pa\$\$w0rd** e clique em **OK**.

16. Clique em **Concluir** e clique em **Fechar**.
17. No painel Ações, clique em **Backup Único**.
18. No Assistente de Backup Único, selecione **Opções de backup agendado** e clique em **Avançar**.
19. Na página **Confirmação**, clique em **Backup**.
20. Na página **Progresso do backup**, clique em **Fechar**.
21. Feche o Backup do Windows Server.

Lição 3

Implementação da recuperação de dados e de servidor

Conteúdo:

Demonstração

142

Demonstração

Demonstração: Uso do Backup do Windows Server para restaurar uma pasta

Etapas da demonstração

1. Em LON-SVR1, abra o Explorador de Arquivos, vá para a unidade C e exclua a pasta **HR Data**.
2. No Gerenciador do Servidor, inicie o **Backup do Windows Server**, e clique em **Recuperar**.
3. No Assistente de Recuperação, na página **Ponto de Partida**, clique em **Um backup armazenado em Outro local** e clique em **Avançar**.
4. Na página **Especificar Tipo de Local**, clique em **Pasta compartilhada remota** e clique em **Avançar**.
5. Na página **Especificar Pasta Remota**, digite `\\LON-DC1\Backup`, e clique em **Avançar**.
6. Na página **Selecionar a data do backup**, clique em **Avançar**.
7. Na página **Selecionar tipo de recuperação**, clique em **Avançar**.
8. Na página **Selecionar itens que serão recuperados**, expanda **LON-SVR1**, clique na unidade **Disco Local (C:)** e, no painel direito, clique em **HR Data**, e clique em **Avançar**.
9. Na página **Especificar opções de recuperação**, em **Outro local**, digite `C:\` e clique em **Avançar**.
10. Na página **Confirmação**, clique em **Recuperar**.
11. Na página **Andamento da recuperação**, clique em **Fechar**.
12. No Explorador de Arquivos, vá para a unidade C e assegure que a pasta **HR Data** foi restaurada.

Revisão e informações complementares do módulo

Prática recomendada

- Analise seus recursos de infraestrutura importantes e dados de missão crítica e essenciais para os negócios. Com base nessa análise, crie uma estratégia de backup que protegerá os recursos de infraestrutura críticos da empresa e os dados comerciais.
- Trabalhe com os gerentes comerciais da organização para identificar o tempo de recuperação mínimo para obter dados essenciais para os negócios. Com base nessas informações, crie uma estratégia de restauração ideal.
- Sempre teste os procedimentos de backup e de restauração regularmente. Execute testes em um ambiente isolado e não de produção.

Perguntas de revisão

Pergunta: Você deseja criar uma estratégia que inclua como fazer backup de tecnologias diferentes usadas na organização, como DHCP, DNS, AD DS e SQL Server. O que fazer?

Resposta: Leia a documentação sobre a estratégia de backup ideal para cada tecnologia, pois cada uma delas tem práticas recomendadas específicas referentes ao backup e à restauração. Com base nessas informações, crie a documentação e uma lista de verificação para procedimentos de backup e restauração.

Pergunta: Com que frequência você deve executar backups em dados críticos?

Resposta: A frequência com que você executa que um backup de dados críticos depende dos requisitos de sua organização e da frequência de alteração dos dados. Você sempre deve planejar estratégias de backup de acordo com avaliações de risco. Se seus dados críticos forem alterados significativamente durante o dia, você deverá executar o backup pelo menos uma vez por dia e considerar a execução de vários instantâneos de VSS durante o dia.

Problemas e cenários reais

Sua organização precisa de informações sobre quais dados incluir no backup, com que frequência fazer backup de tipos diferentes de dados e tecnologias, onde armazenar seus dados de backup (no local ou na nuvem) e com que rapidez pode restaurar os dados de backup. Como você melhoraria a capacidade da sua organização para restaurar dados com eficiência quando necessário?

Resposta: Sua empresa deve desenvolver estratégias de backup e restauração com base em vários parâmetros, como necessidades de continuidade comercial, procedimentos de avaliação de risco e identificação de recursos e dados críticos. Você deve desenvolver estratégias que devem ser avaliadas e testadas. Essas estratégias devem levar em conta as alterações dinâmicas que ocorrem com novas tecnologias e as alterações que ocorrem com o crescimento da organização.

Ferramentas

Ferramenta	Uso	Onde encontrar
Backup do Windows Server	Execute o backup e a restauração sob demanda ou agendados de dados e servidores.	Gerenciador do Servidor - Ferramentas
Windows Azure Online Backup	Execute o backup sob demanda ou agendado para a nuvem e restaure os dados do backup localizado na nuvem.	Gerenciador do Servidor - Ferramentas

Problemas comuns e dicas de solução de problemas

Problema comum	Dica para a solução de problemas
O servidor sofreu uma falha principal em seus componentes.	Execute uma restauração bare-metal em um novo sistema usando o conjunto de backup que você criou. Use a documentação e a lista de verificação que você criou como parte da estratégia de backup e restauração da sua empresa e procedimentos.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do backup e restauração do Windows Server

Pergunta: Você está preocupado com dados empresariais críticos localizados nos servidores da sua empresa. Você deseja executar backups diariamente, mas não durante o horário comercial. O que você deve fazer?

Resposta: Você deve executar um backup agendado que ocorre diariamente após o horário comercial, por exemplo, 1:00.

Pergunta: Os usuários relatam que não podem mais acessar dados localizados no servidor. Você se conecta ao servidor e percebe que a pasta compartilhada onde os usuários estavam acessando dados está faltando. O que você deve fazer?

Resposta: Você deve restaurar a pasta usando o Backup do Windows Server.

Pergunta: Os servidores que armazenam dados financeiros para a organização são incluídos no backup usando o Windows Azure Online Backup. Um dos servidores falhou e teve que ser substituído, o que poderia demorar um dia útil. Os usuários têm que acessar dados financeiros assim que possível. O que você deve fazer?

Resposta: Você deve usar o Windows Azure Online Backup para restaurar dados financeiros em outro servidor que está executando sistema operacional Windows Server 2012.

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 support@microsoft.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.