Microsoft

PRODUTO MICROSOFT LEARNING OFICIAL

24742B

Identidade com o Windows Server 2016

Conteúdo complementar

Número do produto: 24742B

Lançamento: 08/2017

TERMOS DE LICENÇA DA MICROSOFT PARA UM AMBIENTE VIRTUAL QUE INCLUI OS SEGUINTES SOFTWARES DA MICROSOFT:

SOFTWARE DEVELOPMENT KIT (SDK) DO MICROSOFT WINDOWS IDENTITY FOUNDATION

Microsoft Office 2013

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 dos títulos de softwares individuais da Microsoft identificados acima e de qualquer documentação, conteúdo, guia de configuração de sala de aula, arquivos de configuração e suporte, serviços online e aplicativos de amostra fornecidos como parte do ambiente virtual (coletivamente chamados de "**Ambiente Virtual**"), que inclui a mídia na qual você o recebeu, se houver. Os termos também se aplicam a atualizações, suplementos, serviços de Internet e de suporte para os componentes do Ambiente Virtual.

As imagens do disco rígido virtuais do software da Microsoft para o Ambiente Virtual podem ser fornecidas a você em um ou mais discos rígidos virtuais. Os títulos de software individuais listados acima geralmente são licenciados separadamente, mas são fornecidos a você sob estes termos de licença consolidados para sua conveniência.

CONFORME DESCRITO A SEGUIR, O USO DO AMBIENTE VIRTUAL TAMBÉM IMPLICARÁ A AUTORIZAÇÃO DA TRANSMISSÃO DE DETERMINADAS INFORMAÇÕES DO COMPUTADOR DURANTE A ATIVAÇÃO E A VALIDAÇÃO E PARA FINS DE SERVIÇOS DE INTERNET.

O ACESSO A QUALQUER PARTE DO AMBIENTE VIRTUAL SIGNIFICA SUA ACEITAÇÃO DOS REFERIDOS TERMOS. SE VOCÊ NÃO ACEITAR OS TERMOS, NÃO ACESSE NEM USE NENHUM COMPONENTE DO AMBIENTE VIRTUAL.

SEU DIREITO DE USO OU DE FORNECER ACESSO AO AMBIENTE VIRTUAL ESTÁ LIMITADO AO PERÍODO DE TEMPO ESPECIFICADO. CONSULTE A SEÇÃO 8 PARA OBTER DETALHES.

Ao cumprir estes termos de licença, você terá os direitos abaixo desde que você tenha uma licença válida para o Ambiente Virtual.

1. DEFINIÇÕES.

1.1. "**Centro de Treinamento Autorizado**" significa um Parceiro de Treinamento, Membro do Programa Microsoft IT Academy ou uma outra entidade que a Microsoft possa designar por escrito.

1.2. "**Sessão de Treinamento Autorizado**" significa a aula de treinamento conduzida pelo instrutor autorizado pela Microsoft que ministra um Curso da Microsoft conduzido por um MCT em um Centro de Treinamento Autorizado em suas instalações de treinamento.

1.3. "**Dispositivo em Sala de Aula**" significa um computador pessoal dedicado que pertence ou é controlado por um Centro de Treinamento Autorizado, localizado nas instalações de treinamento do Centro de Treinamento Autorizado, no qual a Sessão de Treinamento Autorizado está sendo ministrada, que atende ou excede o nível de hardware especificado para o título do Curso da Microsoft específico.

1.4. "**Usuário Final**" significa uma pessoa devidamente registrada e que está participando de uma Sessão de Treinamento Autorizado.

1.5. "**Parceiro de Treinamento**" significa um membro ativo do programa Microsoft Partner Network de boa reputação que no momento possui e mantém a Competência de Treinamento.

1.6. "**MCT**" ou "**Instrutor Certificado pela Microsoft**" significa um indivíduo que (i) é contratado para ministrar uma Sessão de Treinamento Autorizado em um Centro de Treinamento Autorizado; (ii) é atualmente certificado como um Instrutor Certificado pela Microsoft do Programa de Certificação da Microsoft com boa reputação e (iii) possui no momento uma Certificação da Microsoft na tecnologia objeto da Sessão de Treinamento Autorizado.

1.7. "**Curso da Microsoft**" significa a versão do kit do aluno do curso de treinamento conduzido pelo instrutor com a marca da Microsoft licenciado pela Microsoft para instruir indivíduos sobre as tecnologias da Microsoft. Um título de Curso da Microsoft pode ser um curso com a marca Curso Oficial da Microsoft, Microsoft Dynamics ou Microsoft Business Group.

1.8. "**Membro do Programa Microsoft IT Academy**" significa uma instituição acadêmica que é membro ativo do programa Microsoft IT Academy.

1.9. "**Você**" significa o Parceiro de Treinamento ou um MCT que exerce direitos sob esta licença.

2. DIREITOS DE INSTALAÇÃO E USO.

2.1. Substituição de outros termos de licença de software da Microsoft. Os termos do presente contrato de licença substituem os termos de qualquer contrato de licença de software Microsoft que possa ser encontrado em qualquer software de Ambiente Virtual, mesmo que a instalação ou o uso do software exija a "aceitação" de um contrato de termo de licença separado.

2.2. Direitos de uso limitado. O Ambiente Virtual é licenciado, não vendido. O Ambiente Virtual só pode ser usado junto com o título do Curso da Microsoft associado ao Ambiente Virtual, de modo que você deve comprar uma licença do título do Curso da Microsoft associado ao Ambiente Virtual para cada Usuário Final que acessa o Ambiente Virtual, e você deve fornecer a cada Usuário Final sua cópia devidamente licenciada do título do Curso da Microsoft. O presente documento traz dois conjuntos separados de direitos de uso. Somente um conjunto de direitos de uso se aplica ao seu caso.

a. **Se você for um Parceiro de Treinamento** para cada Sessão de Treinamento Autorizado que você está fornecendo, poderá:

   i. baixar e instalar apenas aqueles componentes do Ambiente Virtual listados no guia de configuração da sala de aula do título do Curso da Microsoft sujeito à Sessão de Treinamento Autorizado em 1 (um) Dispositivo de Sala de Aula host executando uma cópia devidamente licenciada do Microsoft Hyper-V para criar o Ambiente Virtual associada ao Curso da Microsoft;

   ii. além de

      1. instalar o Ambiente Virtual em 1 (um) servidor interno localizado nas instalações de treinamento no Centro de Treinamento Autorizado na qual a Sessão de Treinamento Autorizado está sendo ministrada **OU**

      2. duplicar o Ambiente Virtual e instalar 1 (uma) instância do Ambiente Virtual em 1 (um) dos seus Dispositivos de Sala de Aula que estão executando uma cópia devidamente licenciada do Microsoft Hyper-V desde que você não instale o Ambiente Virtual em mais Dispositivos de Sala de Aula do que o número de Usuários Finais registrados naquela Sessão de Treinamento Autorizado específica e

   iii. permitir acesso a e uso do Ambiente Virtual exclusivamente por meio de um Dispositivo de Sala de Aula e exclusivamente por:

      1. 1 (um) Usuário Final que comprou uma licença válida do título do Curso da Microsoft associado ao Ambiente Virtual exclusivamente para executar atividades práticas para o Curso da Microsoft e apenas ao participar da Sessão de Treinamento Autorizado e

      2. um MCT para preparar e ministrar a Sessão de Treinamento Autorizado.

b. **Se você for um MCT** para cada Sessão de Treinamento Autorizado que você está ministrando, poderá:

   i. baixar e instalar apenas aqueles componentes do Ambiente Virtual listados no guia de configuração da sala de aula do título do Curso da Microsoft sujeito à Sessão de Treinamento Autorizado em 1 (um) Dispositivo de Sala de Aula host executando uma cópia devidamente licenciada do Microsoft Hyper-V para criar o Ambiente Virtual associada ao Curso da Microsoft;

   ii. além de

      1. instalar os componentes do Ambiente Virtual em 1 (um) servidor interno localizado nas instalações de treinamento no Centro de Treinamento Autorizado na qual a Sessão de Treinamento Autorizado está sendo ministrada **OU**

      2. duplicar e instalar 1 (uma) instância dos componentes do Ambiente Virtual nos Dispositivos de Sala de Aula que estão executando uma cópia devidamente licenciada do Microsoft Hyper-V desde que você não instale o Ambiente Virtual em mais Dispositivos de Sala de Aula do que o número de Usuários Finais registrados naquela Sessão de Treinamento Autorizado específica e

   iii. duplicar e instalar 1 (uma) instância do Ambiente Virtual em 1 (um) computador pessoal que pertence a você e que esteja executando uma cópia devidamente licenciada do Microsoft Hyper-V apenas para você preparar a Sessão de Treinamento Autorizado.

2.3. Ausência de Outros Direitos. O Ambiente Virtual não pode ser acessado nem usado de forma independente. O Ambiente Virtual só pode ser acessado e usado junto com a Sessão de Treinamento Autorizado, ministrando o título do Curso da Microsoft associado ao Ambiente Virtual. O Ambiente Virtual licenciado a você sob este contrato de licença não pode ser usado em um ambiente operacional ativo nem em um ambiente de produção. Não é concedido nenhum direito de distribuir, exibir publicamente nem de executar o Ambiente Virtual nem qualquer um dos seus componentes.

2.4. Separação de Componentes. O Ambiente Virtual do título do Curso da Microsoft pode incluir vários títulos de software, conteúdo e de outros componentes que podem ser fornecidos a você em várias mídias ou em vários downloads. O Ambiente Virtual é fornecido e licenciado a você como uma única unidade a ser usada conforme permitido na Seção 2.2. Você não poderá separar os componentes do Ambiente Virtual nem instalá-los em dispositivos ou servidores diferentes.

2.5. Ausência de Acesso de Rede. Você não poderá instalar o Ambiente Virtual nos Dispositivos de Sala de Aula ou servidores que estejam acessíveis a outras redes, a menos que seja explicitamente autorizado pela Microsoft, conforme documentado e especificado no guia de configuração de sala de aula do Curso da Microsoft associado.

2.6. Reprodução/Redistribuição das Imagens do Disco Rígido Virtuais do Software da Microsoft no Ambiente. Você reconhece e concorda que:

a. o Ambiente Virtual contém imagens do disco rígido virtual do software da Microsoft;

b. o software da Microsoft fornecido a você sob este contrato são ativos valiosos para a Microsoft, e a duplicação e distribuição não autorizada de tal software desprovê a Microsoft de receitas que ela geralmente recolhe pelo licenciamento do referido software da Microsoft;

c. a Microsoft está fornecendo o software da Microsoft a você gratuitamente exclusivamente para auxiliar os Usuários Finais a ganharem proficiência no uso das tecnologias da Microsoft, conforme estabelecido neste contrato de licença;

d. você não poderá vender, alugar, arrendar, emprestar, transferir, ceder nem sublicenciar nenhuma parte do software e

e. você não poderá sublicenciar, transferir nem ceder esta licença ou o contrato de licença a um terceiro.

2.7. Software de Terceiros. O Ambiente Virtual pode incluir código de terceiros que a Microsoft, não o terceiro, licencia para você de acordo com este contrato. As notificações, se houver, relativas ao código de terceiros, serão incluídas apenas para fins informativos.

2.8. Serviços Online. Se a Microsoft disponibilizar qualquer serviço online a você como parte do Curso da Microsoft ("**Serviços Online**"), o uso que você faz dos Serviços Online será regido por esta seção, e os termos não conflitantes do contrato de serviços online separado serão apresentados a você. Ao usar os Serviços Online durante um Curso da Microsoft, você concorda (a) que os Serviços Online só poderão ser usados para executar atividades práticas do título do Curso da Microsoft associado ao Ambiente Virtual, (b) que as credenciais de autenticação que você usa (ou que seu Usuário Final usa) para acessar os Serviços Online não devem estar vinculadas a nenhuma conta "ativa", (c) que você licencia para a Microsoft, suas afiliadas e todos os sublicenciados necessários todos os direitos exigidos para usar e processar todos os arquivos de texto, som, imagens ou arquivos ("Dados") carregados, processados ou armazenados usando os Serviços Online, (d) que você não inserirá, carregará, processará nem armazenará nenhum Dado, nem permitirá que seus Usuários Finais o façam, que contenham informações de identificação pessoal nos Serviços Online, (e) que nenhum dispositivo pessoal dos Usuários Finais será usado com nem registrado nos Serviços Online, (f) que a Microsoft poderá excluir qualquer Dado a qualquer momento sem notificação e sem nenhuma responsabilidade atribuída a você e (g) que a Microsoft não prestará nenhum serviço de suporte para os Serviços Online.

3. REQUISITOS DE LICENCIAMENTO E DIREITOS DE USO ADICIONAIS.

3.1 Você só poderá usar o Ambiente Virtual se cumprir os termos e as condições deste contrato de licença e os seguintes requisitos de segurança:

a. Você poderá acessar, instalar e usar apenas os componentes listados como componentes do Ambiente Virtual listados no guia de configuração da sala de aula do título do Curso da Microsoft sujeito à Sessão de Treinamento Autorizado programada e só poderá usar o Ambiente Virtual para fornecer ou ministrar uma Sessão de Treinamento Autorizado que esteja ensinando o título do Curso da Microsoft associado ao Ambiente Virtual.

b. Você só poderá usar as imagens do disco rígido virtual do software que acompanham este contrato de licença para formar o Ambiente Virtual.

c. Você deverá formar e configurar o Ambiente Virtual de acordo com o guia de configuração da sala de aula do título do Curso da Microsoft objeto da Sessão de Treinamento Autorizado programada. Você não poderá incluir nem usar nenhum dos seus conteúdos ou softwares nem de terceiros no Ambiente Virtual, a menos que seja explicitamente autorizado pela Microsoft, conforme documentado no guia de configuração de sala de aula do título do Curso da Microsoft relevante.

d. Você não poderá instalar o Ambiente Virtual nos Dispositivos de Sala de Aula ou servidores que estejam acessíveis a outras redes, a menos que seja explicitamente autorizado pela Microsoft, conforme documentado no guia de configuração de sala de aula relevante do título do Curso da Microsoft.

e. Antes de iniciar a Sessão de Treinamento Autorizado, você deverá fornecer a todos os Usuários Finais uma cópia impressa da declaração a seguir:

"Ao acessar e usar o ambiente virtual de qualquer forma, você declara e concorda que (a) você só poderá acessar e usar o ambiente virtual a partir de seu dispositivo de sala de aula exclusivamente para executar as atividades práticas para esta sessão de treinamento, (b) você não poderá contornar nenhuma limitação técnica no ambiente virtual, (c) você não poderá baixar, reproduzir, transmitir nem encaminhar nenhum software ou componente do ambiente virtual de nenhuma forma nem por qualquer meio sem a permissão expressa por escrito da Microsoft, (d) você não poderá inserir, carregar, processar nem armazenar nenhuma informação de identificação pessoal no ambiente virtual, (e) você não permitirá que um terceiro use nem acesse este ambiente virtual e (f) estes termos substituem os termos de qualquer contrato de licença da Microsoft que você possa encontrar em qualquer componente de ambiente virtual mesmo que a instalação de ou o uso do componente exija a "aceitação" de um contrato de licença separado. **O uso do ambiente virtual representa sua aceitação em cumprir estes termos. Se você não concordar com estes termos, não use o ambiente virtual**.

Este ambiente virtual é fornecido "No Estado em que se Encontra". A Microsoft não oferece garantias expressas nem implícitas.

f. Você só poderá fornecer acesso a e o uso do Ambiente Virtual para Usuários Finais que tenham concordado em cumprir a declaração no parágrafo 3.1.e acima.

g. Antes de iniciar cada Sessão de Treinamento Autorizado, você deverá fornecer a cada Usuário Final sua própria cópia devidamente licenciada do título do Curso da Microsoft sujeito à Sessão de Treinamento Autorizado.

h. Você não poderá permitir que outros acessem, encaminhem, copiem ou baixem o Ambiente Virtual.

i. Você deverá cumprir rigorosamente todas as instruções da Microsoft relacionadas à instalação, à ativação, ao uso, à desativação e à segurança do Ambiente Virtual.

j. Você não poderá modificar o Ambiente Virtual nem qualquer componente relacionado, a menos que seja explicitamente autorizado pela Microsoft, conforme documentado no guia de configuração de sala de aula do título do Curso da Microsoft associado.

k. Se você for um Parceiro de Treinamento, deverá remover todas as cópias do Ambiente Virtual de seu servidor interno e todos os Dispositivos de Sala de Aula no final da Sessão de Treinamento Autorizado.

l. Se você for um MCT, deverá remover todas as cópias do Ambiente Virtual (1) do seu computador pessoal e (2) instaladas por você a partir do servidor interno do Parceiro de Treinamento e de todos os Dispositivos de Sala de Aula no final de cada Sessão de Treinamento Autorizado.

3.2 Se o Ambiente Virtual incluir o software do sistema operacional desativado, você precisará obter uma chave de produto da Microsoft para ativar o software antes de configurar o software do Ambiente Virtual. Instruções específicas sobre como obter e ativar o software usando a chave de produto da Microsoft são incluídas no guia de configuração da sala de aula do título do Curso da Microsoft. Você é responsável pelo uso das chaves de produto que lhe forem consignadas. Você não poderá compartilhar suas chaves de produto com terceiros e você não poderá usar as chaves do produto atribuídas a terceiros.

A ativação associa o uso do software a um dispositivo específico. Durante a ativação, o software enviará informações sobre o software e o dispositivo à Microsoft. Essas informações incluem a versão, o idioma e a chave de produto (Product Key) do software, o endereço do protocolo de Internet do dispositivo e as informações derivadas da configuração de hardware do dispositivo. **USAR O SOFTWARE SIGNIFICA QUE VOCÊ AUTORIZA A TRANSMISSÃO DESSAS INFORMAÇÕES.** Se tiver obtido a devida licença, você terá o direito de usar a versão do software instalada durante o processo de instalação pelo tempo permitido para ativação. **A MENOS QUE O SOFTWARE SEJA ATIVADO, VOCÊ NÃO TERÁ O DIREITO DE USÁ-LO DEPOIS DO TEMPO PERMITIDO PARA ATIVAÇÃO.** Isso se destina a impedir o uso não licenciado. **É VEDADO BURLAR OU CONTORNAR A ATIVAÇÃO.** Se o dispositivo estiver conectado à Internet, o software poderá conectar-se automaticamente à Microsoft para realizar a ativação. Você também pode ativar o software manualmente pela Internet ou por telefone. Se você fizer isso, as taxas aplicáveis do serviço de Internet e de telefone poderão ser cobradas. Além disso, poderá ser necessário reativar o software se os componentes do computador ou o software forem alterados. **O SOFTWARE CONTINUARÁ EXIBINDO UM LEMBRETE PARA A ATIVAÇÃO ATÉ QUE VOCÊ A EXECUTE**.

3.3 Se o Ambiente Virtual incluir software do sistema operacional que não exige uma chave de produto para uso, você precisará verificar o estado do sistema operacional depois da instalação do software no Ambiente Virtual. Se o sistema operacional estiver no modo "Notificação", você deverá executar o comando rearm no software para alterar o estado do sistema operacional antes da Sessão de Treinamento Autorizado.

4. SERVIÇOS DE INTERNET. A Microsoft poderá prestar serviços de Internet com o software no Ambiente Virtual. A Microsoft poderá alterá-los ou cancelá-los a qualquer momento. Se o Ambiente Virtual contiver versões de pré-lançamento do software, alguns dos seus serviços de Internet poderão ser ativados por padrão. A configuração padrão nessas versões do software não reflete necessariamente como os recursos serão configurados nas versões lançadas comercialmente. No entanto, serão aplicados os seguintes termos se o software for configurado para transmissão pela Internet:

a. Consentimento para Serviços de Internet. Alguns dos softwares poderão incluir recursos que se conectam a sistemas de computador da Microsoft ou do provedor de serviços pela Internet. Em alguns casos, você não receberá uma notificação separada quando ocorrer essa conexão. Em alguns casos, você poderá optar por desativar esses recursos ou não usá-los. **O USO DESTES RECURSOS SIGNIFICA QUE VOCÊ CONSENTE COM A TRANSMISSÃO DESSAS INFORMAÇÕES E É RESPONSÁVEL POR OBTER TODO O CONSENTIMENTO NECESSÁRIO DE TODOS OS USUÁRIOS FINAIS PARA TRANSMITIR ESSAS INFORMAÇÕES PARA A MICROSOFT.** A Microsoft não usa as informações para identificar nem contatar você.

b. Informações sobre o Computador. Esses recursos conhecidos como serviços de Internet usam protocolos de Internet, que enviam aos sistemas adequados informações sobre o computador, como endereço de protocolo de Internet, tipo de sistema operacional, navegador, o nome e a versão do software que está sendo usado, bem como o código de idioma do dispositivo no qual o software é executado. A Microsoft usa essas informações para disponibilizar os serviços de Internet para você.

c. Uso de Informações. A Microsoft pode usar as informações e os relatórios para aprimorar nosso software e serviços. Podemos ainda compartilhar essas informações com terceiros, como fornecedores de hardware e software. Estes poderão usá-las para aprimorar seus produtos executados com software da Microsoft.

d. Uso Indevido dos Serviços de Internet. Você não poderá usar esses serviços de maneira que possa danificá-los nem prejudicar seu uso por outros. Você não poderá usar os serviços para tentar obter acesso não autorizado a serviços, dados, contas ou redes por qualquer meio.

5. **ESCOPO DA LICENÇA.** O Ambiente Virtual é licenciado, não vendido. Este contrato simplesmente confere a você alguns direitos de uso do Ambiente Virtual. A Microsoft reserva para si todos os outros direitos. Salvo quando a lei aplicável conferir outros direitos, não obstante a presente limitação, o software e o Ambiente Virtual devem ser usados conforme expressamente permitido neste contrato de licença. Ao fazer isso, você deverá respeitar todas as limitações técnicas dos componentes do Ambiente Virtual que permitam seu uso apenas de determinadas formas. Você não poderá nem permitirá que outras pessoas:
    a. façam ou instalem mais cópias do Ambiente Virtual nos Dispositivos de Sala de Aula do que o número de Usuários Finais que estão participando da Sessão de Treinamento Autorizado;
    b. permitam que mais Dispositivos de Sala de Aula acessem o Ambiente Virtual no servidor do que o número de Usuários Finais que estão participando da Sessão de Treinamento Autorizado;
    c. permitam o acesso a ou uso do Ambiente Virtual a qualquer pessoa com exceção dos Usuários Finais que compraram uma licença válida do título do Curso da Microsoft sujeito à Sessão de Treinamento Autorizado e somente ao participar da Sessão de Treinamento Autorizado que está ensinando o título do Curso da Microsoft associado ao Ambiente Virtual;
    d. transmitam, publiquem, vinculem a, postem, exibam publicamente ou encaminhem o Ambiente Virtual ou de outra forma usem o Ambiente Virtual de uma forma não autorizada ou ilícita;
    e. reproduzam, usem, baixem, forneçam acesso ou distribuam o Ambiente Virtual, exceto conforme expressamente permitido segundo os termos deste contrato;
    f. aluguem, vendam, arrendem ou emprestem o Ambiente Virtual ou reproduzam o Ambiente Virtual em qualquer servidor ou locais para reprodução ou acesso posterior, exceto conforme expressamente permitido segundo os termos deste contrato;
    g. acessem ou usem qualquer parte do Ambiente Virtual para (i) serviços de hospedagem de software comercial, (ii) finalidades comerciais em geral ou (iii) qualquer finalidade que não tenha sido expressamente autorizada pela Microsoft sob este contrato;
    h. adicionem conteúdo ou software a, alterem, modifiquem, adaptem, editem ou de outra forma criem trabalhos derivados com base no Ambiente Virtual;
    i. usem o Ambiente Virtual em um outro sistema operacional ou aplicativo executado em outro sistema operacional;
    j. contornem quaisquer limitações técnicas do Ambiente Virtual ou
    k. façam engenharia reversa, descompilem, personalizem ou desmontem o Ambiente Virtual de alguma forma.

    O direito de acessar o Ambiente Virtual em qualquer dispositivo não concede a você o direito de implementar patentes da Microsoft ou outras propriedades intelectuais da Microsoft no Ambiente Virtual nem em dispositivos que acessam o referido Ambiente Virtual.

6. **RESERVA DE DIREITOS E PROPRIEDADE.** A Microsoft e seus fornecedores reservam para si toda a titularidade de direito, os direitos autorais e os direitos de propriedade intelectual no Ambiente Virtual e em seus componentes.

7. **SOFTWARE COM LIMITE DE TEMPO.** Depois da ativação inicial, algum software no Ambiente Virtual poderá parar de funcionar na data indicada para o software aplicável no guia de configuração da sala de aula do Curso da Microsoft. Você não receberá nenhuma outra notificação. Você poderá usar o comando rearm para redefinir o software no Ambiente Virtual para executá-lo por um período de tempo adicional. O número de dias em que o software será executado por ativação e o número de vezes que você pode executar o comando rearm variam conforme indicado no guia de configuração da sala de aula do Curso da Microsoft.

    Você deve interromper todo o acesso e uso do Ambiente Virtual se algum software no Ambiente Virtual parar de executar e você tiver esgotado todos os seus comandos rearm (se estiverem disponíveis). Você não poderá acessar, usar nem recuperar dados do Ambiente Virtual assim que o software parar de executar.

8. **VIGÊNCIA E RESCISÃO.** Este contrato terminará automática e imediatamente (a) na data do término do software conforme indicado no guia de configuração de sala de aula e assim que todos os comandos rearms forem usados (se disponível); (b) no término deste contrato por parte da Microsoft; (c) (i) mediante a expiração ou o término do seu status de Competência de Treinamento do programa Microsoft Partner Network se você for um Parceiro de Aprendizagem ou (ii) no término ou na expiração do seu status de MCT se você for um MCT ou (d) na conclusão do primeiro prazo do beta para qualquer software de pré-lançamento incluído no Ambiente Virtual (se aplicável), o que ocorrer primeiro.

A Microsoft poderá rescindir imediatamente este contrato se tiver motivos para acreditar que você não cumpriu qualquer um de seus termos e condições.

Mediante a expiração ou o término deste contrato por qualquer motivo, todos os direitos concedidos a você sob este contrato serão rescindidos imediatamente, e você deverá interromper imediatamente todo o acesso e uso do Ambiente Virtual e excluir e destruir permanentemente todas as cópias do Ambiente Virtual e de seus componentes que estão em seu poder ou sob seu controle.

9. **FEEDBACK.** O envio de feedback sobre o Ambiente Virtual à Microsoft representa a sua concessão gratuita à Microsoft do direito de usar, compartilhar e comercializar seu comentário de qualquer forma e para qualquer finalidade. Além disso, você concede gratuitamente a terceiros todos os direitos de patente de que eles necessitam em seus produtos, tecnologias e serviços para usar ou estabelecer conexão com qualquer parte específica de um software ou serviço da Microsoft que inclua o feedback. Você não deverá enviar feedback que esteja sujeito a uma licença que requeira da Microsoft o licenciamento do software, de produtos, tecnologias, serviços ou documentação a terceiros em virtude da inclusão do seu feedback nesses elementos. Estes direitos permanecerão em vigor após o término deste contrato.

10. **RESTRIÇÕES DE EXPORTAÇÃO.** O software no Ambiente Virtual está sujeito às leis e aos regulamentos de exportação dos Estados Unidos. Devem ser cumpridos todas as leis e os regulamentos de exportação nacionais e internacionais aplicáveis ao software. Essas leis incluem restrições relacionadas a destinos, usuários finais e uso final. Para obter informações adicionais, consulte a página www.microsoft.com/exporting.

11. **SERVIÇOS DE SUPORTE.** Como o Ambiente Virtual é fornecido "no estado em que se encontra", a Microsoft poderá não prestar serviços de suporte para ele.

12. **ACORDO INTEGRAL.** Este contrato e os termos dos suplementos, das atualizações, dos serviços de Internet, dos Serviços Online (se aplicáveis) e dos serviços de suporte por você usados constituem o acordo integral para o Ambiente Virtual e os serviços de suporte.

13. **LEI APLICÁVEL.**
    a. Nos Estados Unidos. Se você tiver adquirido os componentes do Ambiente Virtual nos Estados Unidos, este contrato será regido e interpretado de acordo com as leis do Estado de Washington, que serão aplicadas aos requerimentos judiciais ou extrajudiciais de violação de contrato, independentemente dos princípios de conflito de leis. As leis do estado no qual você reside regerão todos os outros requerimentos judiciais ou extrajudiciais, incluindo leis de defesa do consumidor, concorrência desleal e atos ilícitos extracontratuais.
    b. Fora dos Estados Unidos. Tendo sido os componentes do Ambiente Virtual adquiridos em qualquer outro país, aplicar-se-ão as leis do respectivo país.

14. **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. Este contrato não altera seus direitos previstos nas leis do seu país, caso essas leis não o permitam.

15. **ISENÇÃO DE GARANTIA. O AMBIENTE VIRTUAL, CADA UM DOS SEUS COMPONENTES E SERVIÇOS ONLINE SÃO LICENCIADOS "NO ESTADO EM QUE SE ENCONTRAM". VOCÊ ASSUME INTEGRALMENTE O RISCO DE USÁ-LOS. A MICROSOFT NÃO OFERECE GARANTIAS NEM CONDIÇÕES CONTRATUAIS. A LEI LOCAL PODERÁ CONFERIR A VOCÊ DIREITOS DE CONSUMIDOR ADICIONAIS, OS QUAIS NÃO SERÃO AFETADOS PELO SEU CONTRATO. ATÉ O LIMITE PERMITIDO PELAS LEIS LOCAIS, A MICROSOFT EXCLUI TODAS E QUAISQUER GARANTIAS LEGAIS DE PADRÕES DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA E NÃO VIOLAÇÃO.**

    PARA A AUSTRÁLIA - VOCÊ TEM GARANTIAS ESTATUTÁRIAS RESGUARDADAS PELA LEI DE CONSUMO AUSTRALIANA, E NADA NESTES TERMOS SE DESTINA A AFETAR ESSES DIREITOS.

16. **LIMITAÇÃO E EXCLUSÃO DE RECURSOS E DANOS. VOCÊ PODERÁ PLEITEAR DA MICROSOFT E DE SEUS FORNECEDORES APENAS DANOS DIRETOS LIMITADOS AO MAIOR VALOR PAGO PELO AMBIENTE VIRTUAL OU 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:

a. toda e qualquer questão relacionada ao Ambiente Virtual, seus componentes, Serviços Online e ao conteúdo (inclusive código) em sites ou programas de terceiros e

b. requerimentos judiciais ou extrajudiciais 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.

Módulo 1

Instalação e configuração de controladores de domínio

Sumário:

Lição 1

Visão geral do AD DS

Sumário:

Perguntas e respostas

Pergunta: Quais são as duas principais finalidades das UOs?

> **Resposta:** As duas principais finalidades das UOs são fornecer uma estrutura para a delegação de administração e oferecer uma estrutura para habilitar a implantação direcionada do GPO.

Pergunta: Por que seria necessário implantar uma árvore adicional na floresta do AD DS?

> **Resposta:** Seria necessário implantar uma árvore adicional na floresta do AD DS se você precisasse de mais de um namespace do DNS (Sistema de Nomes de Domínio).

Recursos

Componentes do AD DS

Leitura adicional: Para obter mais informações sobre domínios e florestas, consulte: "Visão geral dos Serviços de Domínio Active Directory" em: http://aka.ms/M2lr5a

O que há de novo no AD DS no Windows Server 2016?

Leitura adicional: Para obter mais informações sobre o PAM, consulte: "Privileged Access Management para Active Directory Domain Services" em: http://aka.ms/Ibsyai

Leitura adicional: Para obter mais informações sobre o Ingresso no Azure AD, consulte: "Windows 10 para a empresa: maneiras de usar dispositivos para o trabalho" em: http://aka.ms/F7dfxe

Leitura adicional: Para obter mais informações sobre como usar o Microsoft Passport com o AD DS no Windows Server 2016, consulte: "Autenticação de identidades sem senhas com o Microsoft Passport" em: http://aka.ms/Nyrund

Leitura adicional: Para obter mais informações sobre os novos recursos do AD DS no Windows Server 2016, consulte: "O que há de novo no Active Directory Domain Services para Windows Server 2016" em: http://aka.ms/Nzrl6u

Demonstração: Como usar o Centro Administrativo do Active Directory para administrar e gerenciar o AD DS

Etapas da demonstração

Navegar no Centro Administrativo do Active Directory

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Centro Administrativo do Active Directory**.
2. Clique em **Adatum (local)**, clique em **Controle de Acesso Dinâmico** e em **Pesquisa Global**.
3. No painel de navegação, clique na guia **Modo de Exibição de Árvore** e expanda o nó **Adatum (local)** para exibir os detalhes do domínio Adatum.com.

Executar uma tarefa administrativa no Centro Administrativo do Active Directory

1. No Centro Administrativo do Active Directory, clique em **Visão Geral**.
2. Na caixa **Redefinir Senha**, na caixa **Nome de usuário**, digite **Adatum\Adam**.
3. Nas caixas **Senha** e **Confirmar senha**, digite **Pa55w.rd**.

4. Desmarque a caixa de seleção **O usuário deverá alterar a senha no próximo logon** e clique em **Aplicar**.
5. Na caixa **Pesquisa Global**, na caixa **Pesquisa**, digite **lon** e pressione Enter.

Criar um objeto

1. No Centro Administrativo do Active Directory, no modo de exibição de árvore do painel de navegação, expanda **Adatum (local)** e clique no contêiner **Computadores**.
2. No painel **Tarefas**, na seção **Computadores**, clique em **Novo** e selecione **Computador**.
3. Na caixa de diálogo **Criar Computador**, insira as informações a seguir e clique em **OK**:
   - Nome do computador: **LON-CL4**
   - Nome do computador (NetBIOS): **LON-CL4**
4. Clique em **OK**.

Exibir todos os atributos de objeto

1. No Centro Administrativo do Active Directory, clique duas vezes em **Adatum (local)** e, na lista de gerenciamento, clique duas vezes em **Computadores**.
2. Selecione **LON-CL4** e, no painel **Tarefas**, na seção **LON-CL4**, clique em **Propriedades**.
3. Na janela **LON-CL4**, role para baixo até a seção **Extensões**, clique na guia **Editor de Atributos** e observe que todos os atributos do objeto de computador estão disponíveis aqui.
4. Clique em **Cancelar** para fechar a janela **LON-CL4**.

Usar o visualizador de Histórico do Windows PowerShell

1. No Centro Administrativo do Active Directory, clique na barra de ferramentas **Histórico do Windows PowerShell** na parte inferior da tela.
2. Exiba os detalhes do cmdlet **New-ADComputer** que você usou para executar a tarefa mais recente.
3. Em **LON-DC1**, feche todas as janelas abertas.

Lição 2

Visão geral de controladores de domínio do AD DS

Sumário:

Perguntas e respostas

Pergunta: Um controlador de domínio deveria ser um catálogo global?

> **Resposta:** O posicionamento do catálogo global afeta o tempo que o usuário leva para entrar. Portanto, você deve planejar cuidadosamente como posicionar os catálogos globais. Em um ambiente de domínio único, cada controlador de domínio deve hospedar o catálogo global, pois cada controlador de domínio já mantém uma cópia completa do domínio. Em um cenário de vários domínios, você precisa considerar os tempos de entrada do usuário, as dependências do programa, a necessidade de alta disponibilidade do catálogo global e o tráfego de replicação ao planejar o posicionamento do catálogo global.

Pergunta: Em uma floresta de vários domínios, é necessário armazenar uma cópia do catálogo global em todos os controladores de domínio.

( ) Verdadeiro

( ) Falso

> **Resposta:**
>
> ( ) Verdadeiro
>
> (√) Falso
>
> **Comentários:**
>
> Em um domínio único, você deve configurar todos os controladores de domínio para manter uma cópia do catálogo global. No entanto, em um ambiente de vários domínios, o mestre de infraestrutura não deve ser um servidor de catálogo global, salvo se todos os controladores de domínio do domínio também forem servidores de catálogo global.

Recursos

Transferência e execução de funções

Leitura adicional: Para obter mais informações sobre como usar o Windows PowerShell para transferir ou executar funções FSMO, consulte: "Mover (transferindo ou executando) funções FSMO com o comando AD-Powershell para outro controlador de domínio" em: http://aka.ms/Rn7kfi

Leitura adicional: Para obter mais informações sobre como usar o ntdsutil.exe para transferir ou executar funções FSMO, consulte: "Como usar o Ntdsutil.exe para transferir ou executar funções FSMO para um controlador de domínio" em: http://aka.ms/Npye86

Demonstração: Exibição dos registros SRV no DNS

Etapas da demonstração

Exibir os registros SRV usando o Gerenciador DNS

1. Em **LON-DC1**, entre com o nome de usuário **Adatum\Administrador** e a senha **Pa55w.rd**.
2. No **Gerenciador do Servidor**, clique no menu **Ferramentas**.
3. Na lista **Ferramentas**, clique em **DNS**.

4. Na janela do **Gerenciador DNS**, no menu da árvore, expanda **LON-DC1**, expanda **Zonas de Pesquisa Direta** e clique em **Adatum.com**. Mostre as quatro subzonas a seguir do DNS (Sistema de Nomes de Domínio):
   - **_msdcs**
   - **_sites**
   - **_tcp**
   - **_udp**
5. Expanda **Adatum.com**, expanda **_sites**, expanda **Default-First-Site-Name**, expanda **_tcp** e selecione o seguinte registro:
   - **_ldap Service Location (SRV) [0][100][389] lon-dc1.adatum.com**
6. Se os alunos tiverem experiência e interesse suficientes, abra **c:\windows\system32\config** e abra o arquivo **netlogon.dns** no Bloco de notas. Mostre todos os registros de serviços (registros SRV) que esse controlador de domínio registrará no DNS.

Lição 3

Implantação de um controlador de domínio

Sumário:

Perguntas e respostas

Pergunta: Qual é a maneira mais rápida de replicar controladores de domínio em um ambiente virtualizado?

Resposta: Clonando

Comentários: A clonagem é a maneira mais rápida de implantar vários computadores com configurações idênticas, especialmente quando esses computadores são executados em um ambiente virtualizado, como o Hyper-V. A clonagem copia os discos rígidos virtuais dos computadores e altera configurações secundárias, como nomes do computador e endereços IP, para que sejam exclusivos. Em seguida, os computadores entram em operação imediatamente.

Pergunta: Quais são as duas considerações principais para a implantação de controladores de domínio no Azure?

Resposta: As duas considerações principais são limitações de reversão e máquina virtual.

- Reversão. A reversão de um sistema do AD DS pode criar USNs (Números de Sequência de Atualização) duplicados. Como a replicação do controlador de domínio depende de USNs, números duplicados podem causar problemas. Para evitar isso, o Active Directory Domain Services do Windows Server 2016 tem um identificador chamado **VM-Generation ID**. O **VM-Generation ID** pode detectar uma reversão. Ele impede que o controlador de domínio virtualizado replique alterações de saída até que o AD DS virtualizado seja convergido com os outros controladores de domínio do domínio.
- Limitações de máquina virtual. As máquinas virtuais do Azure estão limitadas a 14 gigabytes (GB) de memória RAM e um adaptador de rede. Além disso, não há suporte para o recurso de ponto de verificação.

Recursos

Instalação de um controlador de domínio em uma instalação Server Core do Windows Server 2016

Leitura adicional: Para obter mais informações sobre como usar o cmdlet do Windows PowerShell **Install-ADDSDomainController**, consulte: "Instalar o Active Directory Domain Services (Nível 100)" em: http://aka.ms/A9jlvk

Leitura adicional: Para obter mais informações, consulte: "Cmdlets de implantação do AD DS no Windows PowerShell" em: http://aka.ms/Lnxifx

Instalação de um controlador de domínio usando mídia

Leitura adicional: Para obter mais informações sobre as etapas necessárias para instalar o AD DS, consulte: "Instalar o Active Directory Domain Services (Nível 100)" em: http://aka.ms/Rvcwlz

Melhores práticas para virtualização do controlador de domínio

Leitura adicional: Para obter mais informações sobre a virtualização de controladores de domínio, consulte: "Execução de controladores de domínio no Hyper-V" em: http://aka.ms/Tjjl9g

Demonstração: Clonagem de um controlador de domínio

Etapas da demonstração

Preparar um controlador de domínio de origem para clonagem

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Central Administrativa do Active Directory**.
2. No Centro Administrativo do Active Directory, clique duas vezes em **Adatum (local)** e, na lista de gerenciamento, clique duas vezes na UO de **Controladores de Domínio**.
3. Na lista de gerenciamento, selecione **LON-DC1**, se ainda não estiver selecionado, e no painel **Tarefas**, na seção **LON-DC1**, clique em **Adicionar ao grupo**.
4. Na caixa de diálogo **Selecionar Grupos**, na caixa **Digite os nomes de objeto a serem selecionados**, digite **Clonável** e, em seguida, clique em **Verificar Nomes**.
5. Certifique-se de que o nome de grupo seja expandido para **Controladores de Domínio Clonáveis** e, em seguida, clique em **OK**.
6. No menu Iniciar, clique em **Windows PowerShell**.
7. No prompt de comando do Windows PowerShell, digite o comando a seguir e pressione Enter.

```
Get-ADDCCloningExcludedApplicationList
```

8. Verifique a lista de aplicativos críticos. Na produção, é necessário verificar cada aplicativo ou usar um controlador de domínio que tenha menos aplicativos instalados por padrão. Digite o comando a seguir e pressione Enter.

```
Get-ADDCCloningExcludedApplicationList –GenerateXML
```

9. Digite o comando a seguir para criar o arquivo **DCCloneConfig.xml** e pressione Enter.

```
New-ADDCCloneConfigFile
```

10. Digite o comando a seguir para desligar o **LON-DC1** e pressione Enter.

```
Stop-Computer
```

11. Aguarde até que a máquina virtual seja desligada. Você pode ser solicitado a confirmar o desligamento.

Exportar a máquina virtual de origem

1. No computador host, no **Gerenciador do Hyper-V** da Microsoft, no painel de detalhes, selecione a máquina virtual **24742B-LON-DC1**.
2. No painel **Ações**, na seção **24742B-LON-DC1**, clique em **Exportar**.
3. Na caixa de diálogo **Exportar Máquina Virtual**, vá para o local **D:\Arquivos de Programas\Microsoft Learning\24742** e clique em **Exportar**. Aguarde até que a exportação termine.
4. No painel **Ações**, na seção **24742-LON-DC1**, clique em **Iniciar**.

Criar e iniciar o controlador de domínio clonado

1. No computador host, no **Gerenciador do Hyper-V**, no painel **Ações**, na seção nomeada para o computador host, clique em **Importar Máquina Virtual**.
2. No **Assistente para Importar Máquina Virtual**, na página **Antes de Começar**, clique em **Avançar**.
3. Na página **Localizar Pasta**, clique em **Procurar**, procure a pasta **D:\Arquivos de Programas\Microsoft Learning\24742\24742B-LON-DC1**, clique em **Selecionar Pasta** e em **Avançar**.
4. Na página **Selecionar Máquina Virtual**, selecione **24742B-LON-DC1** (se ainda não estiver selecionado) e clique em **Avançar**.
5. Na página **Escolher Tipo de Importação**, selecione **Copiar a máquina virtual (criar uma ID exclusiva nova)** e clique em **Avançar**.
6. Na página **Escolher Pastas para Arquivos de Máquinas Virtuais**, marque a caixa de seleção **Armazenar a máquina virtual em outro local**. Para cada local de pasta, especifique **D:\Arquivos de Programas\Microsoft Learning\24742** como o caminho. Clique em **Avançar**.
7. Na página **Escolher Pastas para Armazenar Discos Rígidos Virtuais**, forneça o caminho **D:\Arquivos de Programas\Microsoft Learning\24742** e clique em **Avançar**.
8. Na página **Concluindo o Assistente de Importação**, clique em **Concluir**.
9. Na lista de gerenciamento, identifique e selecione a máquina virtual recém-importada chamada **24742B-LON-DC1**, cujo **Estado** é **Desativado**. Na seção inferior do painel **Ações**, clique em **Renomear**.
10. Digite **24742B-LON-DC3** como o nome e pressione Enter.
11. No painel **Ações**, na seção **24742B-LON-DC3**, clique em **Iniciar** e clique em **Conectar** para que a máquina virtual seja iniciada.
12. Enquanto o servidor estiver iniciando, talvez você veja a mensagem **"Clonagem de Controlador de Domínio na Conclusão *x*%"**.

Revisão do módulo e informações complementares

Perguntas de revisão

Pergunta: Qual método de implantação você usaria para instalar um controlador de domínio adicional em um local remoto com uma conexão WAN limitada?

> **Resposta:** Você usaria a opção **Instalar da mídia**, pois ela elimina a necessidade de copiar todo o banco de dados do AD DS pelo link WAN.

Pergunta: Que ferramenta ou ferramentas você pode usar para promover uma instalação Server Core do Windows Server 2016 para que ele seja um controlador de domínio?

> **Resposta:** Para promover uma instalação Server Core do Windows Server 2016 para que ele seja um controlador de domínio, você pode usar as seguintes ferramentas:
>
> - Gerenciador do Servidor, que permite instalar o AD DS remotamente.
> - Windows PowerShell.
> - O comando **dcpromo /unattend**, que é executado no servidor que executa a instalação Server Core.

Pergunta: Se você quiser executar um controlador de domínio na nuvem, que serviço deverá usar: Azure AD ou máquinas virtuais do Azure de IaaS (Infraestrutura como Serviço)?

> **Resposta:** As respostas variam dependendo das necessidades dos alunos. O Azure Active Directory (Azure AD) fornece gerenciamento de acesso e identidade para aplicativos baseados na Web. Usando máquinas virtuais do Azure de IaaS (infraestrutura como serviço), você pode implantar o controlador de domínio do AD DS completo.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Erros de sintaxe	Os erros de sintaxe, em geral, ocorrem em função de erros de digitação ou quando você esquece um parâmetro ao digitar cmdlets do Windows PowerShell. Examine a saída do console para obter informações específicas sobre o motivo de falha do comando.
Problemas de pré-requisitos	Muitos erros sérios estão diretamente relacionados a erros que o verificador de pré-requisitos encontra. Examine os resultados com atenção e siga as orientações fornecidas.
Problemas de configuração de floresta e rede	Problemas de configuração de rede ou outros problemas de configuração de floresta do AD DS podem impedir a promoção de novos controladores de domínio. Use os arquivos **dcpromoui.log** e **dcpromo.log** para exibir erros específicos de promoção ou o log de eventos para erros que indicam problemas de configuração. Você também pode usar o dcdiag.exe e o repadmin.exe para verificar a integridade geral da floresta.

Módulo 2

Gerenciamento de objetos no AD DS

Sumário:

Lição 1

Gerenciamento de contas de usuário

Sumário:

Perguntas e respostas

Pergunta: Qual é a finalidade de um perfil móvel?

> **Resposta:** Ele armazena e sincroniza o perfil do usuário em um compartilhamento de rede. Isso permite que o usuário migre de um computador para outro e ainda receba o mesmo perfil quando entrar em um novo computador.

Pergunta: Qual é a diferença entre desabilitar uma conta e bloquear uma conta?

> **Resposta:** Desativar uma conta é uma ação intencional feita por um administrador para impeder o uso de uma conta. O bloqueio de conta é o resultado de muitas tentativas de logon malsucedidas (supondo-se que a política de senha aplique essa configuração).

Demonstração: Gerenciamento de contas de usuário

Etapas da demonstração

Criar uma nova conta de usuário

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Central Administrativa do Active Directory**.
2. No Centro Administrativo do Active Directory, clique em **Adatum (local)** e clique duas vezes em **Managers**.
3. No painel **Tarefas**, clique em **Novo** e, depois, em **Usuário**.
4. Na caixa de diálogo **Criar usuário**, no campo **Primeiro nome**, digite **Vendas**.
5. No campo **Sobrenome**, digite **Gerente**.
6. Na caixa de texto **Logon UPN do usuário**, digite **SalesManager**.
7. Nos campos **Senha** e **Confirmar senha**, digite **Pa55w.rd** e clique em **OK**.

Excluir uma conta de usuário

1. Clique na **conta** Art Odum.
2. No painel **Tarefas**, em **Art Odum**, clique em **Excluir**.
3. Na caixa **Excluir confirmação**, clique em **Sim**.

Mover uma conta de usuário

1. Clique na conta Burton Bartels.
2. No painel Tarefas, em Burton Bartels, clique em Mover...
3. Clique na development ou e clique em OK.
4. No painel de navegação, clique em **Adatum (local)**.
5. No painel direito, clique duas vezes na **UO Desenvolvimento** e certifique-se de que a conta **Burton Bartels** está presente.

Configurar características de usuário

1. Clique duas vezes na conta Burton Bartels.
2. No painel esquerdo, clique em Organização e altere o campo Departamento de Gerentes para Desenvolvimento.
3. No painel esquerdo, clique em Membro de.
4. Na seção Membro de, clique em Gerentes e em Remover.

5. Clique em Adicionar. Na caixa de diálogo Selecionar grupos, na janela Digite os nomes de objeto a serem selecionados (exemplos):, digite Desenvolvimento e clique em OK.
6. Clique em OK para fechar as propriedades Burton Bartels.
7. Feche o Centro Administrativo do Active Directory. Deixe o **Gerenciador de servidor** aberto para a próxima demonstração.

Demonstração: Como usar modelos para gerenciar contas

Etapas da demonstração

Criar um modelo de usuário

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Usuários e Computadores do Active Directory**.
2. Expanda **Adatum.com** e clique na **UO Vendas**.
3. Clique no ícone de novo usuário na barra de ferramentas.
4. Na caixa de diálogo **Novo objeto – usuário**, digite as informações a seguir e clique em **Avançar**:
   - Nome: **_vendas**
   - Sobrenome: **modelo**
   - Nome de logon do usuário: **modelodevendas**
5. Nos campos **Senha** e **Confirmar senha**, digite **Pa55w.rd**.
6. Desmarque a caixa de seleção **O usuário deve alterar a senha no próximo logon**, marque a caixa de seleção **A senha nunca expira**, marque a caixa de seleção **A conta está desabilitada** e clique em **Avançar**.
7. Clique em **Concluir**.

Configurar propriedades de modelos

1. Clique duas vezes na **conta** _modelo de vendas.
2. Na caixa de diálogo **propriedades do _modelo de vendas**, clique na guia **Membro de** e, depois, em **Adicionar**.
3. Na caixa de diálogo **Selecionar Grupos**, digite **Vendas** e clique em **OK**.
4. Clique na guia **Organização**. No campo **Departamento**, digite **Vendas**.
5. Na seção **Gerente**, clique em **Alterar**. Na caixa de diálogo **Selecionar usuário ou contato**, digite **Erin** e clique em **Verificar nomes**. Clique em **OK**.
6. Clique na guia **Perfil**. Na seção **Perfil do usuário**, no campo **Script de logon**, digite **\\lon-dc1\netlogon\logon.bat** e clique em **OK**.

Criação de um novo usuário copiando o modelo

1. Clique com o botão direito do mouse na conta **_modelo de vendas** e clique em **Copiar**.
2. Na caixa de diálogo **Copiar objeto - usuário**, no campo **Primeiro nome**, digite **Sales**. Digite **Usuário** no campo **Sobrenome**.
3. Digite **usuáriodevendas** no campo **Nome de logon de usuário** e clique em **Avançar**.
4. Nos campos **Senha** e **Confirmar senha**, digite **Pa55w.rd**.

5. Desmarque a caixa de seleção **A senha nunca expira**, desmarque a caixa de seleção **A conta está desabilitada**, marque a caixa de seleção **O usuário deve alterar a senha no próximo logon** e clique em **Avançar**.
6. Clique em **Concluir**.
7. Clique duas vezes na conta **Usuário de vendas** e clique na guia **Membro de**. Verifique se o usuário é um membro do grupo **Vendas**.
8. Clique na guia **Organização**. Certifique-se de que o **Departamento** está como **Vendas** e o **Gerente** está como **Erin Bull**.
9. Clique na guia **Perfil**. Certifique-se de que o Caminho do script de logon seja **\\lon-dc1\netlogon\logon.bat**. Clique em **OK** para fechar a caixa de diálogo.
10. Feche **Usuários e Computadores do Active Directory**.

Lição 2

Gerenciamento de grupos no AD DS

Sumário:

Demonstração: Gerenciamento de grupos no Windows Server

Etapas da demonstração

Criar um novo grupo e adicionar membros

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Centro Administrativo do Active Directory**.
2. Expanda **Adatum (local)** e clique duas vezes em **TI**.
3. Na lista **Tarefas**, em **TI**, aponte para **Novo** e clique em **Grupo**.
4. Na caixa de diálogo **Criar grupo**, no campo **Nome do grupo**, digite **Gerentes de TI**. Observe que o padrão é um grupo de segurança global.
5. No painel esquerdo, clique em **Membros** e em **Adicionar**.
6. Na caixa de diálogo **Selecionar usuários, contatos, computadores, contas de serviço ou grupos**, em **Digite os nomes de objeto a serem selecionados (exemplos)**, digite **Beth; Logan**, clique em **Verificar nomes** e em **OK**.
7. Clique em **OK** para fechar a caixa de diálogo **Criar grupo: Gerentes de TI**.

Adicionar um usuário ao grupo

1. Clique com o botão direito do mouse no usuário chamado **Maj Hojski** e clique em **Adicionar ao grupo**.
2. Na caixa de diálogo **Selecionar grupos**, em **Digite os nomes de objeto a serem selecionados (exemplos)**, digite **Gerentes de TI**.
3. Clique em **Verificar nomes** e em **OK**.

Alterar o tipo e o escopo do grupo

1. Clique duas vezes no **grupo** Gerentes de TI.
2. Na janela **Gerentes de TI**, em **Tipo de grupo**, clique em **Distribuição**. Leia a mensagem em destaque. Em **Escopo do grupo**, clique em **Universal** e em **OK**.

Configurar um gerente para o grupo

1. Clique duas vezes no **grupo** Gerentes de TI.
2. Na seção **Gerenciado por**, clique em **Editar**.
3. Na caixa de diálogo **Selecionar Usuário, Contato ou Grupos**, em **Digite os nomes de objeto a serem selecionados (exemplos)**, digite **Parsa**, clique em **Verificar Nomes** e, em seguida, em **OK**.
4. Marque a caixa de seleção ao lado da caixa de diálogo **O gerente pode atualizar a lista de membros**.
5. Clique em **OK** para fechar a caixa de diálogo Propriedades de Gerentes de TI.
6. Feche o **Centro Administrativo do Active Directory**.

Lição 3

Gerenciamento de objetos de computador no AD DS

Sumário:

Perguntas e respostas

Pergunta: O que faz com que um computador perca sua relação de confiança com o domínio?

Resposta: Normalmente, isso é resultado de uma incompatibilidade de senha entre o computador local e o conteúdo armazenado no AD DS.

Lição 4

Uso do Windows PowerShell para a administração do AD DS

Sumário:

Perguntas e respostas

Pergunta: O que é Ambiente de Script Integrado do Windows PowerShell?

> **Resposta:** O Ambiente de Script Integrado do Windows PowerShell fornece um ambiente para gravação, execução e teste de scripts do Windows PowerShell. Ele apresenta codificação de sintaxe com cores, preenchimento por tabulação, depuração visual e ajuda contextual que não estão disponíveis na janela padrão do Windows PowerShell.

Recursos

Consulta de objetos com o Windows PowerShell

Leitura adicional: para obter mais informações, consulte a página about_ActiveDirectory_Filter: http://aka.ms/Kv5dy3

Leitura adicional: para obter mais informações, consulte Como usar os sinalizadores UserAccountControl para manipular propriedades de conta de usuário em: http://aka.ms/Mxt8a1

Modificação de objetos com o Windows PowerShell

Leitura adicional: Para obter mais informações, consulte Set-ADUser: http://aka.ms/K34c8d

Demonstração: Uso de ferramentas gráficas para executar operações em massa

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Usuários e Computadores do Active Directory**.
2. Expanda **Adatum.com** e clique na **UO Pesquisa**.
3. No painel de detalhes, clique no topo da coluna **Tipo** para classificar o objeto por tipo.
4. Clique no primeiro objeto do usuário da lista (que deve ser **Arturs Priede**).
5. Role para a parte inferior da lista, mantenha a tecla Shift pressionada e clique no último **Objeto do usuário** da lista (que deve ser **Vera Pace**).
6. Clique com o botão direito do mouse nos objetos selecionados e, depois, em **Propriedades**.
7. Na caixa de diálogo **Propriedades de vários itens**, marque a caixa de seleção ao lado de **Escritório**, digite **Winnipeg** no campo e clique em **OK**.
8. Clique duas vezes em qualquer objeto de usuário e observe que o campo **Escritório** está definido como **Winnipeg** agora.
9. Clique em **Cancelar** e feche Usuários e Computadores do Active Directory.

Demonstração: execução de operações em massa com o Windows PowerShell

Etapas da demonstração

Criar um novo grupo global no departamento de TI

1. Em **LON-DC1**, clique com o botão direito do mouse no botão **Iniciar**, clique em **Executar**, digite **PowerShell** e pressione Enter.
2. Na janela **Administrador: Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
New-ADGroup -Name Helpdesk -Path “ou=IT,dc=Adatum,dc=com” –GroupScope Global
```

Adicionar todos os usuários do departamento de TI ao grupo Assistência Técnica

- Na janela **Administrador: Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
Get-ADUser -Filter “Department -eq 'IT'” | Foreach {Add-ADGroupMember “Helpdesk” -
members $_}
```

Definir o endereço de todos os usuários no departamento de pesquisa

- Na janela **Administrador: Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
Get-ADuser -Filter {Department -eq “Research”} | Set-ADuser -StreetAddress
“1530 Nowhere Ave.” -City “Winnipeg” -State “Manitoba” -Country “CA”
```

Observação: observe que esse comando filtra usando colchetes em vez de aspas e usa o cmdlet **Set-ADUser** em vez de um loop **foreach**.

Criar uma nova UO

- Na janela **Administrador: Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
New-ADOrganizationalUnit London -Path “dc=Adatum,dc=com”
```

Executar um script para criar novos usuários a partir de um arquivo .csv

1. Abra o Explorador de Arquivos, digite **E:\Labfiles\Mod02** na barra de endereços e pressione Enter.
2. Clique com botão direito em **DemoUsers.csv**, clique em **Abrir com**e, depois, em **Bloco de notas**. Explique a estrutura do arquivo aos alunos.
3. Feche o Bloco de notas.
4. Volte para a janela **Windows PowerShell** e digite **cd E:\Labfiles\Mod02**.
5. Para executar o script, digite **.\DemoUsers.ps1** e pressione Enter.

Verificar se as contas de usuário foram criadas e modificadas

1. No **Gerenciador do Servidor**, clique em **Ferramentas**, e em **Usuários e Computadores do Active Directory**.
2. Certifique-se de que a UO de Londres existe.
3. Clique na UO **Londres**. Veja que há três usuários, conforme definido no arquivo.csv. Observe que as contas dos usuários estão desabilitadas. Isso ocorre porque nenhuma senha foi fornecida.
4. Clique na **UO** TI. Verifique se o grupo **Assistência Técnica** existe.
5. Clique duas vezes no grupo **Assistência Técnica** e, depois, em **Propriedades de Assistência Técnica** e na guia **Membros**. Verifique se os membros estão preenchidos com os usuários do departamento de TI e clique em **Cancelar**.
6. Clique na **UO Pesquisa** e clique duas vezes em uma das contas de usuário.
7. Na página de propriedades do usuário, clique na guia **Endereço**. Certifique-se de que os campos de endereço estão preenchidos conforme esperado e clique em **Cancelar**.

Lição 5

Implementação e gerenciamento de UOs

Sumário:

Perguntas e respostas

Pergunta: Qual é a vantagem de usar o **Assistente para Delegação de Controle**?

> **Resposta:** O **Assistente para Delegação de Controle** pode simplificar a delegação de administração atribuindo permissões com base na tarefa selecionada.

Demonstração: Delegação de permissões administrativas em uma UO

Etapas da demonstração

Criar uma nova UO

1. Em **LON-DC1**, em Usuários e Computadores do Active Directory, clique em **Adatum.com**.
2. Clique no ícone **Nova** UO na barra de ferramentas.
3. Na caixa de diálogo **Novo Objeto – Unidade Organizacional**, digite **Recursos humanos** no campo **Nome** e clique em **OK**.

Usar o Assistente para delegação de controle para atribuir uma tarefa

1. Clique com o botão direito do mouse no objeto de domínio **Adatum.com** e clique em **Delegar controle**.
2. No **Assistente para Delegação de Controle**, clique em **Avançar**.
3. Na página **Usuários ou grupos**, clique em **Adicionar**.
4. Na caixa de diálogo **Selecionar usuários, computadores ou grupos**, em **Digite os nomes de objeto a serem selecionados (exemplos)**, digite **Assistência técnica**, clique em **Verificar nomes**, depois em **OK**, e em **Avançar**.
5. Na página **Tarefas para delegar**, marque as caixas de seleção ao lado de **Redefinir senhas de usuário e forçar alteração no próximo logon** e **Adicionar um computador ao domínio**, e clique em **Avançar**.
6. Clique em **Concluir**.

Atribuição do direito de modificar endereços e cargos de usuário na UO Pesquisa ao grupo Pesquisa

1. Em Usuários e Computadores do Active Directory, clique em **Exibir** e em **Recursos Avançados**.
2. Clique com o botão direito do mouse na **UO** Pesquisa e clique em **Propriedades**.
3. Clique na guia **Segurança**, depois em **Avançado** e em **Adicionar**.
4. Na janela **Entrada de permissão para pesquisa**, clique em **Selecionar uma entidade de segurança**.
5. Na caixa de diálogo **Selecionar usuários, computadores ou grupos**, em **Digite os nomes de objeto a serem selecionados (exemplos)**, digite **Research**. Clique em **Verificar Nomes** e em **OK**.
6. Na caixa de listagem suspensa **Aplicar**, selecione **Objetos de usuário descendentes**. (Dica: está localizado no final da lista.)
7. Na seção **Propriedades**, role a tela para baixo e selecione a caixa de seleção ao lado de **Escrever endereço residencial**.
8. Role a tela para baixo novamente, selecione a caixa de seleção ao lado de **Escrever cargo** e clique em **OK** duas vezes.
9. Clique em **OK** para fechar a **caixa de diálogo** Propriedades de pesquisa.

Revisão do módulo e informações complementares

Práticas recomendadas

Considere as seguintes práticas recomendadas para a administração do AD DS:

- Evite usar os grupos internos para delegar acesso administrativo, a menos que você compreenda todas as permissões que a associação do grupo concede.
- Crie grupos administrativos especializados e atribua a esses grupos apenas os direitos e as permissões necessários para concluir as tarefas atribuídas.
- Desenvolva scripts do Windows PowerShell para executar tarefas repetitivas.
- Não entre com sua conta administrativa para atividades diárias. Use-a apenas quando precisar executar uma tarefa administrativa.

Problemas e cenários reais

Muitas organizações criarão algumas contas de usuário com base na função de trabalho, em vez de no usuário que ocupa a função. Por exemplo: a organização sempre terá uma recepcionista. Para fornecer continuidade, a pessoa que ocupa a função usa uma conta genérica denominada recepção. Dessa forma, quando uma nova pessoa ocupa a posição, a única tarefa necessária é alterar a senha do usuário recepção. Aplicativos, configurações, documentos e emails permanecerão consistentes.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo.

Ferramenta	Usada para	Onde encontrar
Windows PowerShell	Linha de comando e scripts de todas as tarefas administrativas.	Nativo do sistema operacional.
Centro Administrativo do Active Directory	Execução de tarefas administrativas diárias no AD DS.	No **Gerenciador do Servidor**, no menu **Ferramentas**, ou no **Painel de Controle**, em **Ferramentas Administrativas**.
Usuários e Computadores do Active Directory	Execução de tarefas administrativas diárias no AD DS.	No **Gerenciador do Servidor**, no menu **Ferramentas**, ou no **Painel de Controle**, em **Ferramentas Administrativas**.
Assistente para Delegação de Controle	Atribuição de permissões para executar tarefas administrativas.	Clique com o botão direito do mouse em uma UO em Usuários e Computadores do Active Directory.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Os usuários não podem acessar recursos de rede.	Verifique as associações de grupo. Procure grupos aninhados que estão causando conflitos.
Você atribuiu a um usuário alguns direitos administrativos no AD DS, mas ele diz que não tem nenhuma ferramenta para executar a tarefa.	Você deve baixar e instalar Ferramentas de Administração de Servidor Remoto para Windows 10 e instalá-las na estação de trabalho do usuário para fornecer a ele as ferramentas administrativas necessárias.

Perguntas e respostas da revisão do laboratório

Laboratório A: Gerenciamento de objetos do AD DS

Perguntas e respostas

Pergunta: Quais tipos de objetos podem ser membros de grupos globais?

Resposta: Os usuários e outras funções (grupos globais) do mesmo domínio podem ser membros de grupos globais.

Pergunta: Quais são as credenciais necessárias para que um computador ingresse em um domínio?

Resposta: Você deve fornecer as credenciais de um usuário que tenha permissão para adicionar computadores ao domínio. Normalmente, essas seriam as credenciais de um administrador de domínio.

Laboratório B: Administração do AD DS

Perguntas e respostas

Pergunta: Por que os usuários que este script criou estão habilitados?

Resposta: O script atribui uma senha aos usuários ao criá-los.

Pergunta: Qual é o status das contas que o cmdlet **New-ADUser** cria?

Resposta: Por padrão, essas contas serão desabilitadas se você não atribuir senhas a elas ao criá-las.

Módulo 3

Gerenciamento avançado de infraestrutura do AD DS

Sumário:

Lição 1

Visão geral de implantações avançadas do AD DS

Sumário:

Perguntas e respostas

Pergunta: Quais dos seguintes requisitos precisam da implantação de um ambiente de várias florestas do AD DS?

( ) Requisitos de isolamento de segurança

( ) Requisitos do esquema

( ) Requisitos de namespace do DNS

( ) Fusões de negócios

( ) Requisitos de administração distribuída

Resposta:

(√) Requisitos de isolamento de segurança

(√) Requisitos do esquema

( ) Requisitos de namespace do DNS

( ) Fusões de negócios

( ) Requisitos de administração distribuída

Comentários:

Isolamento de segurança e requisitos de esquema são os únicos requisitos apresentados nas opções que requerem implementação de várias florestas. Namespace de DNS (Sistema de Nomes de Domínio) e requisitos de administração distribuída precisam de vários domínios, mas florestas separadas não são necessárias porque uma única floresta pode ter vários namespaces e não é necessária para a autonomia administrativa. Em um cenário de fusão de negócios, você pode decidir manter florestas separadas se existir uma pequena necessidade de colaboração entre organizações, mas isso não é obrigatório.

Pergunta: Antes de você implantar uma réplica do controlador de domínio do AD DS em uma máquina virtual do Azure, quais dos seguintes requisitos devem ser atendidos?

( ) Criar um site do AD DS para controle de replicação de suas redes locais para a Rede Virtual do Azure.

( ) Incluir um disco rígido adicional à máquina virtual que tenha cache de leitura e gravação desabilitado.

( ) Criar e configurar uma Rede Virtual do Azure.

( ) Criar, manualmente, SRVs (registros de recurso de serviços) requeridos em uma zona DNS do Azure para seu domínio.

( ) Configurar o endereço IP dinâmico inicial da máquina virtual como estático usando o Set-AzureStaticVNetIP cmdlet.

Resposta:

( ) Criar um site do AD DS para controle de replicação de suas redes locais para a Rede Virtual do Azure.

(√) Incluir um disco rígido adicional à máquina virtual que tenha cache de leitura e gravação desabilitado.

(√) Criar e configurar uma Rede Virtual do Azure.

( ) Criar manualmente os registros requeridos de recurso de serviço (SRV) em uma zona DNS do Azure para seu domínio.

(√) Configurar o endereço IP dinâmico inicial da máquina virtual como estático usando o cmdlet Set-AzureStaticVNetIP.

Comentários:

Embora seja recomendável que você crie um site do AD DS para um controle mais rígido de replicação, isso não é necessário. De qualquer forma, você deveria criar um disco rígido adicional na máquina virtual do Azure em que o cache esteja desabilitado. Esse disco rígido deve conter o arquivo **NTDS.DIT** e a pasta **SYSVOL**. Você também já deve ter provisionado e configurado corretamente uma Rede Virtual do Azure e conectado a máquina virtual a ela. A criação manual de SRVs (registros de recurso de serviços) em um DNS do Azure é uma resposta incorreta porque fazer isso não é possível. A máquina virtual também deve ter um IP estático configurado antes de implantar o AD DS. Isso garante que o IP nunca seja alterado se a máquina virtual for desalocada devido a desligamento ou ações de recuperação de serviço.

Lição 2

Implantação de um ambiente distribuído do AD DS

Sumário:

Perguntas e respostas

Pergunta: Qual é o nível mínimo funcional de domínio que você deve implantar em um controlador de domínio AD DS do Windows Server 2016?

( ) Windows Server 2003

( ) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

Resposta:

( ) Windows Server 2003

(√) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

Comentários:

O Windows Server 2008 é o nível mínimo funcional de domínio recomendado no qual você deve implantar um controlador de domínio do Windows Server 2016 AD DS. Não há mais suporte para o Windows Server 2003. Embora os níveis funcionais de floresta e domínio do Windows Server 2003 ainda sejam suportados, você deve estar nos níveis funcionais do Windows Server 2008 para garantir que a replicação da pasta **SYSVOL** ocorra pelo uso da Replicação DFS (Sistema de Arquivos Distribuído) e não pelo método FRS (serviço de replicação de arquivo) preterido, que o Windows Server 2003 e versões anteriores usavam. Você deve remover os controladores de domínio que ainda estão em operação no Windows Server 2003 do domínio antes de introduzir um controlador de domínio do Windows Server 2016.

Pergunta: Qual dos procedimentos a seguir você pode usar para otimizar a resolução de nomes entre namespaces DNS?

( ) Encaminhadores condicionais

( ) Sites do AD DS

( ) Ordem de pesquisa de sufixo DNS

( ) Zonas de stub do DNS

( ) Servidores de catálogo global

Resposta:

(√) Encaminhadores condicionais

( ) Sites do AD DS

(√) Ordem de pesquisa de sufixo DNS

(√) Zonas de stub do DNS

( ) Servidores de catálogo global

Comentários:

As respostas corretas são encaminhadores condicionais, zonas de stub do DNS e ordem de pesquisa de sufixo DNS. Os encaminhadores condicionais e as zonas de stub do DNS permitem que você crie atalhos para que a resolução de nomes não precise percorrer para cima e para baixo em uma árvore de domínio ou entre florestas. Ao configurarem a ordem de pesquisa de sufixo DNS, os clientes não dependem de devolução do DNS para resolver nomes de rótulo único.

As respostas incorretas são sites do AD DS e servidores de catálogo global. Embora os sites do AD DS possam ajudar você a otimizar a replicação de zonas DNS integradas ao AD DS, eles não tornam a resolução de nomes mais eficiente. Servidores de catálogo global não estão envolvidos em resolução de nomes de DNS.

Recursos

Níveis funcionais de domínio AD DS

Leitura adicional: para obter mais informações sobre os recursos do AD DS no Windows Server 2016, consulte: http://aka.ms/Bxg2z0

Leitura adicional: para mais informações sobre níveis funcionais de domínio AD DS, consulte: http://aka.ms/Ynmvma

Migração de uma versão anterior para o AD DS do Windows Server 2016

Leitura adicional: para obter mais informações sobre o uso do ADMT, consulte: http://aka.ms/Jiauyg

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

Etapas da demonstração

Instalar binários do AD DS em TOR-DC1

1. Em **TOR-DC1**, clique em **Iniciar** e em **Gerenciador do Servidores**.
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**, verifique se a **Instalação baseada em função ou recurso** está selecionada e clique em **Avançar**.
5. Na página **Selecionar servidor de destino**, verifique se **Selecionar um servidor no pool de servidor** está selecionado.
6. Na página **Pool de Servidores**, verifique se **TOR-DC1.Adatum.com** está realçado e clique em **Avançar**.
7. Na página **Selecionar funções do servidor**, marque a caixa de seleção **Active Directory Domain Services**, clique em **Adicionar Recursos** e em seguida, clique em **Avançar**.
8. Na página **Selecionar recursos**, clique em **Avançar**.
9. Na página **Active Directory Domain Services**, examine a mensagem e clique em **Avançar**.
10. Na página **Confirmar seleções de instalação**, examine a mensagem e clique em **Instalar**.
    A instalação levará vários minutos.
11. Na página **Resultados,** clique em **Promover este servidor a um controlador de domínio**.
    O assistente continua.

Configurar TOR-DC1 como um controlador de domínio do AD DS usando o Assistente de Configuração do Active Directory Domain Services

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 **Domínio Filho** está selecionado.
2. No campo **Nome do domínio pai**, verifique se **Adatum.com** está listado.
3. Na caixa **Novo nome de domínio**, digite **NA** e clique em **Avançar**.
4. Na página **Opções do Controlador de Domínio**, verifique se **Windows Server 2016** está selecionado como **Nível funcional do domínio**, se **Servidor DNS (Sistema de Nomes de Domínio)** está selecionado e se **GC (Catálogo Global)** está selecionado.
5. Nas caixas de texto **Digite a senha do DSRM (Modo de Restauração dos Serviços de Diretório)**, digite **Pa55w.rd** em ambas as caixas e clique em **Avançar**.
6. Na página **Opções de DNS**, clique em **Avançar**.
7. Na página **Opções Adicionais**, clique em **Avançar**.
8. Na página **Caminhos**, clique em **Avançar**.
9. Na página **Examinar Opções**, clique em **Avançar**.
10. Na janela **Verificação de Pré-requisitos**, clique em **Instalar**.
11. Examine as informações e permita que **TOR-DC1** seja reiniciado como um controlador de domínio do AD DS no novo domínio do AD DS que você criou na floresta do AD DS.
12. Entre no **TOR-DC1** como **NA\Administrador** com a senha **Pa55w.rd** 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

Sumário:

Perguntas e respostas

Pergunta: Qual das opções a seguir deve estar no lugar antes de você criar uma relação de confiança da floresta?

( ) Resolução de nomes entre os domínios raiz em cada floresta.

( ) Nível funcional da floresta do Windows Server 2003 ou posterior.

( ) Nível funcional da floresta do Windows Server 2008 ou posterior.

( ) Nível funcional da floresta do Windows Server 2012 ou posterior.

( ) Controladores de domínio devem estar ativados para autenticação seletiva.

Resposta:

(√) Resolução de nomes entre os domínios raiz em cada floresta.

(√) Nível funcional da floresta do Windows Server 2003 ou posterior.

( ) Nível funcional da floresta do Windows Server 2008 ou posterior.

( ) Nível funcional da floresta do Windows Server 2012 ou posterior.

( ) Controladores de domínio devem estar ativados para autenticação seletiva.

Comentários:

Para criar uma relação de confiança da floresta, você deve ter configurado a resolução de nomes entre os domínios raiz em cada floresta. Adicionalmente, o nível funcional de floresta de cada floresta deve ser o Windows Server 2003 ou posterior.

Pergunta: Qual configuração de relação de confiança do AD DS permite que você controle o escopo de autenticação de entidades de segurança confiáveis?

( ) Roteamento de sufixo de nome

( ) Delegação restrita de Kerberos

( ) Autenticação seletiva

( ) Filtragem de SID

( ) **Histórico-SID**

Resposta:

( ) Roteamento de sufixo de nome

( ) Delegação restrita de Kerberos

(√) Autenticação seletiva

( ) Filtragem de SID

( ) **Histórico-SID**

Comentários:

A autenticação seletiva permite que você gerencie o escopo de autenticação de entidades de segurança confiáveis permitindo a autenticação de serviços somente em computadores que você especificar.

Recursos

Definição das configurações de confiança avançadas do AD DS

Leitura adicional:

- Para obter mais informações sobre como configurar a colocação em quarentena do filtro de SID em relações de confiança externas, consulte: http://aka.ms/Sveqfn
- Para obter mais informações sobre como habilitar a autenticação seletiva em relação a uma confiança de floresta, consulte: http://aka.ms/Blp826
- Para obter mais informações sobre roteamento de sufixo de nome, consulte: http://aka.ms/Egc6g7

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 do DNS** é aberto.
2. Em **Gerenciador de DNS**, expanda **LON-DC1**, clique com o botão direito do mouse em **Encaminhadores Condicionais** e clique em **Novo Encaminhador Condicional**.
3. Na janela **Novo Encaminhador Condicional,** na caixa de texto **Domínio do DNS,** digite **treyresearch.net**.
4. Na caixa de texto **Endereços IP de servidores mestre,** digite **172.16.10.10**, clique no espaço aberto e em **OK**. Se um erro for exibido, ignore-o.
5. Feche o **Gerenciador DNS**.
6. Alterne para **TREY-DC1** e repita as etapas de 1 a 5. Use o nome de domínio **adatum.com** com o endereço IP **172.16.0.10**.

Configurar uma relação de confiança bidirecional de floresta seletiva

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 de floresta**, e em **Avançar**.
7. Na página **Direção da relação de confiança**, clique em **Bidirecional** e em **Avançar**.
8. Na página **Lados da relação de confiança**, clique em **Este domínio e o domínio especificado** e em **Avançar**.

9. Na caixa de texto **Nome do usuário**, digite **Administrador**.
10. Na caixa de texto **Senha,** digite **Pa55w.rd** e clique em **Avançar**.
11. Na página **Nível de Autenticação de relação de confiança de saída-floresta local**, clique em **Autenticação seletiva** e em **Avançar**.
12. Na página **Nível de Autenticação de Relação de Confiança de Saída - Floresta Especificada,** clique em **Autenticação seletiva** e em **Avançar**.
13. Na página **Seleções de relação de confiança concluídas**, clique em **Avançar**.
14. Na página **Criação de relação de confiança concluída**, clique em **Avançar**.
15. Na página **Confirmar relação de confiança de saída**, clique em **Sim, confirmar a relação de confiança de saída** e em **Avançar**.
16. Na página **Confirmar Relação de Confiança de Entrada**, clique em **Sim, confirmar a relação de confiança de entrada** e em **Avançar**.
17. Na página **Concluindo o Assistente de nova relação de confiança,** clique em **Concluir**.
18. Na caixa de diálogo **Propriedades de Adatum.com**, clique em **OK**.

Revisão do módulo e informações complementares

Pergunta de revisão

Pergunta: Você é um administrador de AD DS da A. Datum Corporation. Atualmente, seu ambiente do AD DS está configurado em um modelo de domínio único e floresta única usando o namespace Adatum.com. A. Datum anunciou recentemente que está se expandindo da Europa para novos continentes através da aquisição de uma empresa chamada Trey Research. A Trey Research opera atualmente na América do Norte e na Ásia. O ambiente de AD DS da Trey Research consiste em uma única floresta chamada Treyresearch.net com um domínio raiz de floresta e domínios filho vazios que alinham para cada continente nos quais operam (Na.treyresearch.net e Asia.treyresearch.net). O objetivo a longo prazo da A. Datum é a total integração da Trey Research nas operações diárias da A. Datum. A liderança da A. Datum também quer adotar o modelo regional de operações que a Trey Research usa. Como administrador de AD DS para a A. Datum, como você combinaria a floresta da Adatum.com com a floresta da Treyresearch.net? Discuta objetivos de curto e longo prazo para a integração de AD DS e como requisitos diferentes podem alterar sua abordagem.

Resposta:

Objetivos a curto prazo

- Criar uma relação de confiança de floresta entre as florestas de AD DS da Adatum.com e da Treyresearch.net. Isso permitirá uma autenticação e autorização entre florestas para que os funcionários, tanto da A. Datum quanto da Trey Research, possam acessar recursos em qualquer floresta.

Objetivos a longo prazo

- Criar os seguintes novos domínios filho na Adatum.com:
  - Europe.adatum.com
  - Na.adatum.com
  - Asia.adatum.com
- Você deve planejar um esforço de reestruturação de floresta para a floresta Adatum.com:
  - Migrar os objetos de domínio existentes da Adatum.com para a Europe.adatum.com. Deixar os objetos de nível de floresta necessários no domínio raiz da floresta Adatum.com.
  - Mover os objetos do domínio Na.treyresearch.net para Na.adatum.com.
  - Mover os objetos do domínio Asia.treyresearch.net para Asia.adatum.com.

Nesse cenário, o objetivo de curto prazo é a integração mais rápida possível dos ambientes do AD DS, para que funcionários de ambas as empresas possam começar uma colaboração imediata. A maneira mais fácil e rápida para você realizar isso seria a criação de uma relação de confiança de floresta entre as duas florestas. Embora essa abordagem possa funcionar para as necessidades de longo e curto prazo da A. Datum, a liderança expressou que a Trey Research faz parte de sua estratégia de longo prazo. Além disso, a liderança demonstrou um desejo de adotar um modelo regional de operações semelhante ao que a Trey Research já usa. Dadas essas duas peças chave de informações, o plano a longo prazo para o AD DS deve ser reestruturar a floresta Adatum.com e criar domínios filho para cada região de operação da A. Datum.

Se a aquisição da Trey Research foi apenas um objetivo de curto prazo e a futura redução da Trey Research é uma possibilidade, você poderá implementar somente uma relação de confiança de floresta para se separar facilmente da Trey Research no futuro.

Se um modelo regional de operações não for um requisito, você poderá manter um modelo de domínio único e floresta única e migrar todos os objetos da Treyresearch.net para o domínio raiz da floresta da Adatum.com.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Você recebe mensagens de erro como: • Falha de pesquisa de DNS • Servidor RPC não disponível • O domínio não existe • O controlador de domínio não pode ser localizado	Geralmente, uma falha de pesquisa de registro de DNS ou firewall configurado incorretamente causa esses erros. Certifique-se de que pelo menos dois servidores DNS funcionais estejam disponíveis na rede. Certifique-se de que todos os computadores tenham pelo menos dois servidores DNS configurados na rede. Verifique se os servidores DNS podem resolver com êxito, consultas em registros DNS fora de seu domínio DNS; por exemplo, em 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 **Domínios e Relações de Confiança do Active Directory**, o **Domain.msc** ou a ferramenta de linha de comandos **Netdom** para validar relacionamentos de confiança. Se necessário, redefina 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 SRVs (registros de recursos de serviço) corretos no banco de dados DNS. Você pode reiniciar o serviço Netlogon em um controlador de domínio do AD DS para forçá-lo a registrar novamente os SRVs (registros de recursos de serviços) no banco de dados DNS.

Perguntas e respostas da revisão do laboratório

Laboratório: Gerenciamento de domínios e relações de confiança no AD DS

Perguntas e respostas

Pergunta: Ao criar a relação de confiança de floresta entre a Adatum.com e a TreyResearch.net, as zonas stub de DNS foram criadas para habilitar a resolução de nomes entre as duas florestas. Qual alternativa você poderia ter usado no lugar de uma zona stub de DNS?

Resposta: Em vez de criar zonas stub de DNS em cada floresta, você também poderia usar um encaminhador condicional. Um DNS secundário também executaria a resolução de nomes necessária, mas causaria uma replicação desnecessária.

Pergunta: Ao criar uma relação de confiança de floresta, por que você criaria uma relação de confiança seletiva em vez de uma relação de confiança completa?

Resposta: Usando uma autenticação seletiva ao configurar uma relação de confiança, você tem mais controle sobre os recursos que os usuários da floresta/domínio confiável podem autenticar. Se você não usar a autenticação seletiva, os usuários da floresta de domínio poderão fazer autenticação em qualquer recurso.

Módulo 4

Implementação e administração de replicação e sites do AD DS

Sumário:

Lição 1

Visão geral da replicação do AD DS

Sumário:

Perguntas e respostas

Pergunta: Por que a replicação é importante para o catálogo global?

> **Resposta:** A partição de configuração contém informações de catálogo global que são replicadas em todos os controladores de domínio, que são designados como servidores de catálogo global.

Como a replicação do AD DS funciona em um site

Pergunta: Descreva as circunstâncias resultantes quando você cria um objeto de conexão manualmente entre os controladores de domínio em um site.

> **Resposta:** Não é recomendável criar um objeto de conexão manualmente e, em geral, isso não é necessário, pois o Knowledge Consistency Checker não verifica nem usa o objeto de conexão manual para failover. O Knowledge Consistency Checker também não remove objetos de conexão manual, o que significa que você deve se lembrar de excluir os objetos de conexão criados manualmente.

Lição 2

Configuração de sites do AD DS

Sumário:

Perguntas e respostas

Pergunta: Qual das opções a seguir não é uma consideração para implementar sites do AD DS?

( ) Reduzir o uso da largura de banda entre locais de rede

( ) Aplicar configurações da Política de Grupo a uma única localização na sua organização

( ) Controlar o controlador de domínio que computadores clientes usam para autenticação

( ) Criar um site de backup para recuperação de desastres

( ) Controlar o acesso a serviços e aplicativos para determinado segmento da sua rede

Resposta:

( ) Reduzir o uso da largura de banda entre locais de rede

( ) Aplicar configurações da Política de Grupo a uma única localização na sua organização

( ) Controlar o controlador de domínio que computadores clientes usam para autenticação

(√) Criar um site de backup para recuperação de desastres

( ) Controlar o acesso a serviços e aplicativos para determinado segmento da sua rede

Recursos

Como computadores cliente localizam controladores de domínio em sites

Leitura adicional: Para obter mais informações, consulte Localização de um controlador de domínio no site mais próximo: http://aka.ms/Cjpzdd

Demonstração: Configuração de sites do AD DS

Etapas da demonstração

1. Em **LON-DC1**, clique em **Iniciar** e em **Gerenciador do Servidores**.
2. No **Gerenciador do Servidor**, clique em **Ferramentas** e em **Serviços e Sites do Active Directory**.
3. No console **Serviços e Sites do Active Directory**, expanda **Sites** e clique em **Default-First-Site-Name**.
4. Clique com o botão direito do mouse em **Default-First-Site-Name**, clique em **Renomear**, 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 **Sub-redes** 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 em **OK**.
12. No painel de navegação, clique com o botão direito do mouse em **Sub-redes** 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 em **OK**.
15. No painel de navegação, expanda **LondonHQ** e **Servers**.
16. Clique com o botão direito 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 **Servers**.
19. Verifique se **TOR-DC1** agora está localizado no site **Toronto**.

Lição 3

Configuração e monitoramento da replicação do AD DS

Sumário:

Perguntas e respostas

Pergunta: A menor duração de replicação que você pode configurar com o agendamento de replicação de site é de 15 minutos.

( ) Verdadeiro

( ) Falso

Resposta:

(√) Verdadeiro

( ) Falso

Recursos

Ferramentas para monitorar e gerenciar a replicação

 **Leitura adicional:** Para obter mais informações, consulte Cmdlets de Administração de AD DS no Windows PowerShell: http://aka.ms/Itjgof

Demonstração: Configuração da replicação entre sites do AD DS

Etapas da demonstração

1. Em **TOR-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Serviços e Sites do Active Directory**.
2. No console **Serviços e Sites do Active Directory**, expanda **Sites** e **Transportes entre Sites**.
3. Clique em **IP**, clique com o botão direito do mouse em **DEFAULTIPSITELINK**, clique em **Renomear**, digite **LON-TOR** e pressione Enter.
4. Clique com o botão direito do mouse em **LON-TOR** e clique em **Propriedades**. Explique as opções **Custo**, **Replicar a cada** e **Alterar Agendamento**.
5. Na caixa de diálogo **Propriedades de LON-TOR**, na caixa de rotação **Replicar a cada**, configure o valor como **60** minutos.
6. Clique em **Alterar Agendamento**.
7. Realce o intervalo de **segunda-feira às 12h** até **sexta-feira às 16h**, da seguinte forma:
   - Clique no bloco **segunda-feira às 12h**, mantenha pressionado o botão do mouse e arraste o cursor para o bloco **sexta-feira às 16h**.
8. Clique em **Replicação Não Disponível** e 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**.

Revisão do módulo e informações complementares

Práticas recomendadas

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.
- Ao configurar agendas de replicação para a replicação entre sites, não configure intervalos longos sem replicação.
- Evite usar o protocolo SMTP como um a protocolo para replicação.

Perguntas de revisão

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

Resposta: Você pode tornar o processo de localizar controladores de domínio e outros serviços mais eficiente referenciando 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 pertença a um site, ele consultará todos os controladores de domínio no domínio. Essa não é uma estratégia eficiente. Na realidade, um único cliente pode executar ações em controladores de domínio em sites diferentes, o que pode gerar resultados inesperados caso essas alterações ainda não tenham sido replicadas. Portanto, é fundamental que cada cliente saiba o site em que está. Você pode obter esta identificação 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, será principalmente um problema de tempo de replicação, e não de quantidade de replicação. Entretanto, em algumas situações extremas, permitir que um número menor de alterações ocorra com mais frequência pode ser menos preferível do que permitir que um grande número de alterações seja replicado com menos frequência.

Pergunta: Qual é a finalidade de um servidor bridgehead?

Resposta: Um servidor bridgehead é responsável por toda a replicação que entra e sai de um 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. No entanto, se determinado servidor bridgehead não for especificamente necessário por motivos de desempenho ou outros fatores, uma prática recomendada é permitir que o ISTG escolha servidores bridgehead entre o pool disponível de controladores de domínio do site.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo.

Ferramenta	Uso	Local
Console de **Serviços e Sites do Active Directory**	Criar sites, sub-redes, links de site, pontes de links de site, forçar a replicação e reiniciar o Knowledge Consistency Checker.	Ferramentas do **Gerenciador do Servidor**
Repadmin.exe	Relatar o status de replicação em cada controlador de domínio, criar topologia de replicação e forçar a replicação, e exibir níveis de detalhe até os metadados de replicação.	Linha de comando
Dcdiag.exe	Executa vários testes e relata sobre a integridade geral de replicação e segurança do AD DS.	Linha de comando
Get-ADReplicationConnection	Uma conexão de replicação AD DS específica ou um conjunto de objetos de conexão de replicação do AD DS baseado em um filtro especificado.	Windows PowerShell
Get-ADReplicationFailure	Uma descrição de uma falha de replicação do AD DS.	Windows PowerShell
Get-ADReplicationPartnerMetadata	Metadados de replicação para um conjunto de um ou mais parceiros de replicação.	Windows PowerShell
Get-ADReplicationSite	Um site de replicação AD DS específico ou um conjunto de objetos de site de replicação baseado em um filtro especificado.	Windows PowerShell
Get-ADReplicationSiteLink	Um link do site específico do Active Directory ou um conjunto de links de sites baseado em um filtro especificado.	Windows PowerShell
Get-ADReplicationSiteLinkBridge	Uma ponte do link do site específico do Active Directory, ou um conjunto de objetos de ponte de link baseado em um filtro especificado.	Windows PowerShell
Get-ADReplicationSubnet	Uma sub-rede específica do Active Directory ou um conjunto de sub-redes do Active Directory baseado em um filtro especificado.	Windows PowerShell

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Um cliente não consegue localizar um controlador de domínio em seu site.	• Verifique se todos os registros 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 a configuração de tempo correta.
A replicação entre sites não funciona.	• Verifique se a configuração de links de site está correta. • Verifique a agenda de replicação. • Verifique se o firewall entre os sites permite o tráfego de replicação do AD DS. Use **repadmin /bind**.
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 configuração de hora em cada servidor é válida.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação de sites e replicação do AD DS

Perguntas e respostas

Pergunta: Você decide adicionar um novo controlador de domínio chamado **LON-DC2** ao site **LondonHQ**. Como garantir que **LON-DC2** passe todo o tráfego de replicação para o site **Toronto**?

> **Resposta:** Você precisa configurar este novo controlador de domínio como o servidor bridgehead preferencial para o site **LondonHQ**.

Pergunta: Você adicionou um novo controlador de domínio chamado **LON-DC2** ao site **LondonHQ**. Que partições de AD DS serão modificadas como resultado?

> **Resposta:** É provável que todas as partições, exceto a partição de esquema, sejam modificadas. Você adiciona o novo controlador de domínio à partição de domínio e à partição de configuração para garantir a correta configuração da replicação de AD DS. Se você estiver usando o DNS integrado pelo Active Directory, os registros do controlador de domínio também serão atualizados nas partições de aplicativo DNS.

Pergunta: No laboratório, você criou um link de site separado para os sites **Toronto** e **TestSite**. Existem outras etapas que talvez sejam necessárias para garantir que **LondonHQ>** não crie automaticamente um objeto de conexão diretamente com o site **TestSite**?

> **Resposta:** Talvez você precise desativar a ponte de link de site automática para poder desabilitar a transitividade de site entre **LondonHQ**, **Toronto** e **TestSite**.

Módulo 5

Implementação da Política de Grupo

Sumário:

Lição 1

Introdução à Política de Grupo

Sumário:

Perguntas e respostas

Categorizar atividade

Pergunta: Inclua cada item na categoria apropriada. Indique sua resposta, escrevendo o número da categoria à direita de cada item.

Itens	
1	Domínio
2	Usuário
3	Unidade organizacional
4	Computador
5	Site
6	Grupo
7	Contêiner Usuários
8	Contêiner Computadores

Categoria 1		Categoria 2
É possível vincular GPOs a		Não é possível vincular GPOs a

Resposta:

Categoria 1		Categoria 2
É possível vincular GPOs a		Não é possível vincular GPOs a
Domínio Unidade organizacional Site		Usuário Computador Grupo Contêiner Usuários Contêiner Computadores

Demonstração: Exploração das ferramentas e dos consoles da Política de Grupo

Etapas da demonstração

1. Em **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. Se necessário, alterne para a janela **Gerenciamento de Política de Grupo**.
3. No **Console de Gerenciamento de Política de Grupo**, no painel de navegação, expanda **Floresta: Adatum.com**, **Domínios**, **Adatum.com** e clique em **Objetos de Política de Grupo**.
4. Clique com o botão direito do mouse em **Objetos de Política de Grupo** e clique em **Novo**.
5. Na caixa de diálogo **Novo GPO**, digite **Desabilitar Painel de Controle** e clique em **OK**.
6. No painel de detalhes, clique com o botão direito do mouse em **Desabilitar Painel de Controle** e clique em **Editar**.
7. No Editor de Gerenciamento de Política de Grupo, no painel de navegação, em **Configuração do Usuário**, expanda **Políticas**, **Modelos Administrativos** e clique em **Painel de Controle**.
8. No painel de detalhes, clique duas vezes em **Proibir acesso ao Painel de Controle e às opções do PC**.
9. Na caixa de diálogo **Proibir acesso ao Painel de Controle e às opções do PC**, mostre os três valores possíveis para uma configuração em **Modelos Administrativos**, mostre o texto **Com suporte em** e o texto **Ajuda**.
10. Clique em **Habilitado**. Na caixa de texto **Comentário**, digite **Habilitado em** <*date*> **por** <*name*>, onde você substitui <*date*> pela data de hoje e <*name*> pelo nome, e clique em **OK**.
11. No painel de navegação, em **Configuração do Usuário**, expanda **Preferências** e mostre as categorias diferentes em **Políticas** e **Preferências**.
12. Feche a janela **Editor de Gerenciamento de Política de Grupo**.
13. Na janela **Gerenciamento de Política de Grupo**, no painel de navegação, expanda **Objetos de Política de Grupo** e clique em **Desabilitar Painel de Controle**.
14. No painel de detalhes, mostre as guias **Escopo**, **Detalhes** e **Configurações**.
15. No painel de navegação, clique e clique com o botão direito do mouse em **Adatum.com** e clique em **Vincular com GPO Existente**.
16. Na caixa de diálogo **Selecionar GPO**, clique em **Desabilitar Painel de Controle** e clique em **OK**.
17. No painel de navegação, clique em **Adatum.com**.
18. No painel de detalhes, mostre as guias **Objetos de Política de Grupo Vinculados** e **Herança de Política de Grupo**.
19. Clique em **Iniciar** e em **Windows PowerShell**.
20. Na janela **Administrador: Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
gpupdate
```

21. Verifique se o computador e as configurações de usuário foram atualizados com êxito.
22. No prompt de comando do Windows PowerShell, digite o seguinte comando e pressione Enter:

```
gpresult /r
```

23. Na saída do comando, na seção **Configurações de Usuário**, na lista **GPOs Aplicados**, verifique se o GPO **Desabilitar Painel de Controle** está listado.
24. Feche a janela do **Windows PowerShell**.

Lição 2

Implementação e administração de GPOs

Sumário:

Perguntas e respostas

Pergunta: Membros de quais grupos internos do AD DS podem criar GPOs por padrão? (Selecione três.)

( ) Admins. do domínio

( ) Opers. de contas

( ) Administradores de empresa

( ) Administradores de GPO

( ) Proprietários criadores de Política de Grupo

Resposta:

(√) Admins. do domínio

( ) Opers. de contas

(√) Administradores de empresa

( ) Administradores de GPO

(√) Proprietários criadores de Política de Grupo

Comentários:

O grupo Administradores de GPO não existe. Os grupos Admins. do domínio e Administradores de empresa podem realizar todas as tarefas administrativas no domínio, inclusive criar GPOs. Proprietários criadores de Política de Grupo é o único grupo que será possível adicionar se você quiser que eles sejam capazes de criar GPOs sem ter direitos administrativos no domínio ou na floresta. Opers. de contas não têm permissões em relação à Política de Grupo. Apenas usuários, computadores e grupos de administração no AD DS.

Demonstração: Delegação de administração da Política de Grupo

Etapas da demonstração

Tornar Beth um administrador local em LON-SVR1

1. Alterne para **LON-DC1**.
2. Na barra de tarefas, clique no ícone do **Explorador de Arquivos**.
3. Na janela **Explorador de Arquivos**, no painel de navegação, expanda **Allfiles (E:)**, **Labfiles** e clique em **Mod05**.
4. No painel de detalhes, clique com o botão direito do mouse no arquivo **Set-LocalAdmin.ps1** e clique em **Executar com o PowerShell**. Digite **S**, caso solicitado, e pressione Enter.

Verificar permissões do usuário antes da delegação

1. Alterne para **LON-SVR1**.
2. Entre como **Adatum\Beth** com a senha **Pa55w.rd**.
3. No Gerenciador do Servidor, clique em **Adicionar funções e recursos**.
4. No **Assistente de Adição de Funções e Recursos**, na página **Antes de começar**, clique em **Avançar**.
5. Na página **Selecionar tipo de instalação**, clique em **Avançar**.
6. Na página **Selecionar servidor de destino**, clique em **Avançar**.

7. Na página **Selecionar funções do servidor**, clique em **Avançar**.
8. Na página **Selecionar recursos**, marque a caixa de seleção **Gerenciamento de Política de Grupo** e clique em **Avançar**.
9. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
10. Quando a instalação for concluída, clique em **Fechar**.
11. No Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
12. Se necessário, alterne para a janela **Gerenciamento de Política de Grupo**.
13. Em **Gerenciamento de Política de Grupo**, expanda **Floresta: Adatum.com**, **Domínios**, **Adatum.com** e clique em **Objetos de Política de Grupo**.
14. Clique com o botão direito do mouse em **Objetos de Política de Grupo** e observe que o item **Novo** permanece esmaecido porque Beth não tem permissões para criar GPOs.
15. No painel de navegação, clique com o botão direito do mouse no domínio **Adatum.com** e observe que o item de menu **Vincular com GPO Existente** permanece esmaecido porque Beth não tem permissões para vincular GPOs ao domínio.
16. No painel de navegação, clique com o botão direito do mouse na UO **TI** e observe que o item de menu **Vincular com GPO Existente** permanece esmaecido porque Beth também não tem permissões para vincular GPOs à UO **TI**.
17. Clique em **Iniciar** e em **Windows PowerShell**.
18. Na janela **Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
GPResult /r
```

19. Na saída do comando, observe que apenas as configurações de **Usuário** são exibidas porque Beth não recebeu as permissões para exibir resultados da Política de Grupo do computador.

Delegar permissões

1. Em **LON-DC1**, alterne para a janela**Gerenciamento de Política de Grupo**.
2. Em **Gerenciamento de Política de Grupo**, no painel de navegação, clique no contêiner **Objetos de Política de Grupo** e, no painel de detalhes, clique na guia **Delegação**.
3. Clique em **Adicionar**. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, digite **Beth**, clique em **Verificar Nomes** e clique em **OK**.
4. No painel de navegação, clique na UO **TI** e, no painel de detalhes, clique na guia **Delegação**.
5. Na lista suspensa **Permissão**, verifique se **Vincular GPOs** está selecionado e clique em **Adicionar**.
6. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, digite **Beth**, clique em **Verificar Nomes** e clique em **OK**.
7. Na caixa de diálogo **Adicionar Grupo ou Usuário**, clique em **OK**.
8. No painel de navegação, clique no domínio **Adatum.com** e, no painel de detalhes, clique na guia **Delegação**.
9. Na lista suspensa **Permissão**, selecione **Ler dados de Resultados de Política de Grupo** e clique em **Adicionar**.
10. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, digite **Usuários Autenticados**, clique em **Verificar Nomes** e em **OK**.
11. Na caixa de diálogo **Adicionar Grupo ou Usuário**, clique em **OK**.

Verificar permissões depois da delegação

1. Alterne para **LON-SVR1**.
2. Alterne para **Gerenciamento de Política de Grupo**.
3. Na janela **Gerenciamento de Política de Grupo**, clique e clique com o botão direito do mouse no domínio **Adatum.com** e clique em **Atualizar**.
4. No painel de navegação, clique com o botão direito do mouse em **Objetos de Política de Grupo** e clique em **Novo**.
5. Na caixa de diálogo **Novo GPO**, na caixa de texto **Nome**, digite **GPO de Beth** e clique em **OK**.
6. No painel de navegação, clique com o botão direito do mouse em **Adatum.com** e observe que **Vincular com GPO Existente** continua esmaecido.
7. No painel de navegação, clique com o botão direito do mouse em **TI** e clique em **Vincular com GPO Existente**.
8. Na caixa de diálogo **Selecionar GPO**, clique em **GPO de Beth** e em **OK**.
9. Alterne para a janela **Windows PowerShell**.
10. Na janela **Windows PowerShell**, digite o seguinte comando e pressione Enter:

```
GPResult /r
```

11. Na saída do comando, observe que as configurações de **Computador** e **Usuário** são exibidas.

Lição 3

Escopo e processamento da Política de Grupo

Sumário:

Perguntas e respostas

Pergunta: É possível vincular mais de um filtro WMI a um GPO.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Embora não possa vincular mais de um filtro WMI a um GPO, você pode criar filtros WMI avançados que incluam mais de uma consulta WMI.

Pergunta: Qual das opções a seguir é possível configurar no GPMC para alterar a ordem de processamento da Política de Grupo padrão? (Selecione todas as opções que se aplicam.)

( ) Filtros WMI

( ) Filtros de segurança

( ) Bloquear Herança

( ) Impor

( ) Processamento de loopback

Resposta:

(√) Filtros WMI

(√) Filtros de segurança

(√) Bloquear Herança

(√) Impor

(√) Processamento de loopback

Comentários:

Todas as opções são viáveis para alterar a maneira como a Política de Grupo normalmente se aplica. Você deve usar bem as diferentes opções porque a solução de problemas fica cada vez mais difícil quando você usa essas opções.

Demonstração: Vinculação de GPOs

Etapas da demonstração

Criar e editar dois GPOs

1. Em **LON-DC1**, se necessário, abra Gerenciador do Servidor.
2. No Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
3. Na janela **Gerenciamento de Política de Grupo**, expanda **Floresta: Adatum.com**, **Domínios** e **Adatum.com**, clique com o botão direito do mouse no contêiner **Objetos de Política de Grupo** e clique em **Novo**.
4. Na caixa de diálogo **Novo GPO**, digite **Remover Comando Executar** na caixa de texto **Nome** e clique em **OK**.

5. Na janela **Gerenciamento de Política de Grupo**, clique com o botão direito do mouse no contêiner **Objetos de Política de Grupo** e clique em **Novo**.
6. Na caixa de diálogo **Novo GPO**, digite **Não Remover Comando Executar** na caixa de texto **Nome** e clique em **OK**.
7. Expanda **Objetos de Política de Grupo**, clique com o botão direito do mouse no GPO **Remover Comando Executar** e clique em **Editar**.
8. Na janela **Editor de Gerenciamento de Política de Grupo**, em **Configuração de Usuário**, expanda **Políticas**, **Modelos Administrativos**, clique em **Menu Iniciar e Barra de Tarefas** e clique duas vezes em **Remover o comando Executar do menu Iniciar**.
9. Na janela **Remover o comando Executar do menu Iniciar**, clique em **Habilitado** e em **OK**.
10. Feche a janela **Editor de Gerenciamento de Política de Grupo**.
11. Em **Gerenciamento de Política de Grupo**, clique com o botão direito do mouse no GPO **Não Remover Comando Executar** e clique em **Editar**.
12. Na janela **Editor de Gerenciamento de Política de Grupo**, em **Configuração de Usuário**, expanda **Políticas**, **Modelos Administrativos**, clique em **Menu Iniciar e Barra de Tarefas** e clique duas vezes em **Remover o comando Executar do menu Iniciar**.
13. Na janela **Remover o comando Executar do menu Iniciar**, clique em **Desabilitado** e em **OK**. Feche a janela **Editor de Gerenciamento de Política de Grupo**.

Vincular os GPOs a locais diferentes

1. Na janela **Gerenciamento de Política de Grupo**, clique com o botão direito do mouse no nó do domínio **Adatum.com** do painel de navegação e clique em **Vincular com GPO Existente**.
2. Na janela **Selecionar GPO**, clique em **Remover Comando Executar** e em **OK**. Agora o GPO **Remover Comando Executar** está vinculado ao domínio Adatum.com.
3. Clique e arraste o GPO **Não Remover Comando Executar** na parte superior da UO **TI**.
4. Na janela **Gerenciamento de Política de Grupo**, clique em **OK** para vincular o GPO.
5. Clique na UO **TI** no painel de navegação e na guia **Herança de Política de Grupo** no painel de detalhes. A guia **Herança de Política de Grupo** mostra a ordem de precedência dos GPOs.

Desabilitar um link de GPO

- No painel à esquerda, clique com o botão direito do mouse no link **Remover Comando Executar** listado em **Adatum.com** e clique em **Vínculo Habilitado** para limpar a marca de seleção. Atualize o painel **Herança de Política de Grupo** da UO de tecnologia da informação (**TI**) e observe os resultados no painel de detalhes. O GPO **Remover Comando Executar** não está mais listado.

Excluir um link de GPO

1. No painel esquerdo, expanda a UO **TI**, clique com o botão direito do mouse no link **Não Remover Comando Executar** e, em seguida, clique em **Excluir**. Clique em **OK** na janela pop-up.
2. Clique na UO **TI** no painel à esquerda e clique na guia **Herança de Política de Grupo** no painel de detalhes. Verifique a remoção de **Não Remover Comando Executar** e a ausência dos GPOs **Remover Comando Executar**.
3. No painel esquerdo, clique com o botão direito do mouse no GPO **Remover Comando Executar**, listado abaixo de **Adatum.com**, e clique em **Vínculo Habilitado** para reabilitar o link. Atualize o painel **Herança de Política de Grupo** da UO **TI** e observe os resultados no painel à direita.
4. Feche **Gerenciamento de Política de Grupo.**

Demonstração: Filtragem do aplicativo da Política de Grupo

Etapas da demonstração

Criar um novo GPO e vinculá-lo à UO TI

1. Em **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. Na janela **Gerenciamento de Política de Grupo**, expanda **Floresta: Adatum.com**, expanda **Domínios**, **Adatum.com** e clique na UO **TI**.
3. Clique com o botão direito do mouse em **TI** e clique em **Criar um GPO neste domínio e fornecer um link para ele aqui**.
4. Na janela **Novo GPO**, digite **Remover o menu Ajuda** na caixa de texto **Nome** e clique em **OK**.
5. Na janela **Gerenciamento de Política de Grupo**, expanda **Objetos de Política de Grupo**, clique com o botão direito do mouse no GPO **Remover o menu Ajuda** e clique em **Editar**.
6. Na janela **Editor de Gerenciamento de Política de Grupo**, em **Configuração de Usuário**, expanda **Políticas**, **Modelos Administrativos**, clique em **Menu Iniciar e Barra de Tarefas** e clique duas vezes em **Remover o menu Ajuda do Menu Iniciar**.
7. Na janela **Remover o menu Ajuda do Menu Iniciar**, clique em **Habilitado** e em **OK**.
8. Feche a janela **Editor de Gerenciamento de Política de Grupo**.

Filtrar a aplicação de Política de Grupo usando filtros de grupo de segurança

1. Expanda **TI** e clique no link de GPO **Remover o menu Ajuda**.
2. Na caixa de mensagem **GPMC**, clique em **OK**.
3. No painel de detalhes, em **Filtros de Segurança**, clique em **Usuários autenticados** e em **Remover**.
4. Na caixa de diálogo de confirmação, clique em **OK**.
5. No painel de detalhes, em **Filtro de Segurança**, clique em **Adicionar**.
6. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, na caixa de texto **Inserir Nomes de Objeto para seleção (Exemplos)**, digite **Beth Burke** e clique em **OK**.
7. No painel de detalhes, em **Filtro de Segurança**, clique em **Adicionar**.
8. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, clique em **Tipos de Objeto**.
9. Na caixa de diálogo **Tipos de Objeto**, marque a caixa de seleção **Computadores** e clique em **OK**.
10. Na caixa de diálogo **Selecionar Usuário, Computador ou Grupo**, na caixa de texto **Inserir Nomes de Objeto para seleção (Exemplos)**, digite **LON-SVR1** e clique em **OK**.

 **Observação:** LON-SVR1 é adicionado à lista de filtros de segurança porque os computadores nos quais os usuários entram também precisam da permissão de leitura no GPO.

Filtre a aplicação de Política de Grupo usando filtros WMI

1. Na janela **Gerenciamento de Política de Grupo**, clique com o botão direito do mouse em **Filtros WMI** e clique em **Novo**.
2. Na caixa de diálogo **Novo Filtro WMI**, na caixa de texto **Nome**, digite **Filtro da Versão de SO**.
3. No painel **Consultas**, clique em **Adicionar**.
4. Na caixa de diálogo **Consulta WMI**, na caixa de texto **Consulta**, digite a seguinte consulta e clique em **OK**:

```
select * from Win32_OperatingSystem where Version like "10.%"
```

5. Se uma caixa de diálogo **Aviso** for exibida, clique em **OK**.
6. Na caixa de diálogo **Novo Filtro WMI**, clique em **Salvar**.
7. Clique com o botão direito do mouse na pasta **Objetos de Política de Grupo** e clique em **Novo**.
8. Na janela **Novo GPO**, digite **Atualizações de Software** na caixa de texto **Nome** e clique em **OK**.
9. Expanda **Objetos de Política de Grupo** e clique no GPO **Atualizações de Software**.
10. No painel de detalhes, na guia **Escopo**, em **Filtros WMI**, na lista **Este GPO está vinculado ao filtro WMI a seguir**, selecione **Filtro da Versão de SO**.
11. Na caixa de diálogo de confirmação, clique em **Sim**.
12. Feche **Gerenciamento de Política de Grupo**.

Lição 4

Solução de problemas da aplicação de GPOs

Sumário:

Recursos

Exame dos logs de eventos da Política de Grupo

Leitura adicional: Para baixar a Exibição de log da Política de Grupo, vá até: http://aka.ms/E8oi7g

Demonstração: Realização de uma análise hipotética com Assistente para Modelagem de Política de Grupo

Etapas da demonstração

Usar o GPResult.exe para criar um relatório

1. Em **LON-DC1**, clique em **Iniciar**, digite **cmd** e pressione Enter.
2. Na janela **Administrador: Prompt de Comando**, digite **cd ** e pressione Enter.
3. Digite o seguinte comando e pressione Enter:

```
GPResult /r
```

4. Revise a saída na janela **Prompt de Comando**.
5. Digite o seguinte comando e pressione Enter:

```
GPResult /h results.html
```

6. Feche a janela **Prompt de Comando**.
7. Clique em **Iniciar**, em **Acessórios do Windows** e em **Internet Explorer**.
8. Na janela **Internet Explorer**, pressione a tecla Alt, clique em **Arquivo** e em **Abrir**.
9. Na caixa de diálogo **Abrir**, na caixa de texto **Abrir**, digite **C:\results.html** e clique em **OK**.
10. Na mensagem de aviso, clique em **Permitir conteúdo bloqueado**.
11. Exiba os resultados do relatório.
12. Feche o Microsoft Internet Explorer.

Usar o Assistente de Relatórios de Política de Grupo para criar um relatório

1. Abra o Gerenciador do Servidor, clique em **Ferramentas** e clique em **Gerenciamento de Política de Grupo**.
2. Na janela **Gerenciamento de Política de Grupo**, no painel de navegação, clique com o botão direito do mouse em **Resultados de Política de Grupo** e clique em **Assistente de Resultados de Política de Grupo**.
3. No **Assistente de Resultados de Política de Grupo**, clique em **Avançar**.
4. Na página **Seleção de Computador** clique em **Avançar**.
5. Na página **Seleção de Usuário**, clique em **Avançar**.
6. Na página **Resumo das Seleções**, clique em **Avançar**.
7. Na página **Concluindo o Assistente de Resultados de Política de Grupo**, clique em **Concluir**.
8. Revise os resultados de Política de Grupo.
9. Expanda **Resultados de Política de Grupo**, clique com o botão direito do mouse em **Administrador em LON-DC1** e clique em **Salvar Relatório**.
10. Na caixa de diálogo **Salvar Relatório GPO**, clique em **Desktop** e em **Salvar**.

Usar o Assistente para Modelagem de Política de Grupo para criar um relatório

1. Clique com o botão direito do mouse em **Modelagem da Política de Grupo** e clique em **Assistente para Modelagem de Política de Grupo**.
2. No **Assistente para Modelagem de Política de Grupo**, clique em **Avançar**.
3. Na página **Seleção de Controlador de Domínio**, clique em **Avançar**.
4. Na página **Seleção de Usuário e Computador**, em **Informações sobre o usuário**, clique em **Usuário** e em **Procurar**.
5. Na caixa de diálogo **Selecionar Usuário**, na caixa de texto **Digite nomes de objeto a serem selecionados (Exemplos)**, digite **Beth** e clique em **OK**.
6. Em **Informações do Computador**, verifique se a opção **Contêiner** está selecionada e clique em **Procurar**.
7. Na caixa de diálogo **Escolha o contêiner de computador**, expanda **Adatum**, clique em **TI** e em **OK**.
8. Na página **Seleção de Usuário e Computador**, clique em **Avançar**.
9. Na página **Opções de Simulação Avançadas**, clique em **Avançar**.
10. Na página **Caminhos alternativos do Active Directory**, clique em **Avançar**.
11. Na página **Grupos de Segurança de Usuário**, clique em **Avançar**.
12. Na página **Grupos de segurança do computador**, clique em **Avançar**.
13. Na página **Filtros WMI para usuários**, clique em **Avançar**.
14. Na página **Filtros WMI para Computadores**, clique em **Avançar**.
15. Na página **Resumo das Seleções**, clique em **Avançar**.
16. Na página **Concluindo o Assistente para Modelagem de Política de Grupo**, clique em **Concluir**.
17. Revise o relatório.
18. Feche todas as janelas abertas.

Revisão do módulo e informações complementares

Perguntas de revisão

Pergunta: Você atribuiu um script de logon a uma UO por meio da Política de Grupo. O script está localizado em uma pasta de rede compartilhada chamada **Scripts**. Alguns usuários na UO recebem o script e outros, não. Quais podem ser as causas possíveis?

> **Resposta:** As permissões de segurança podem ser um problema. Se não tiverem acesso de leitura à pasta **Scripts**, alguns usuários não poderão aplicar a política. Além disso, os filtros de segurança em um GPO podem ser a causa desse problema.

Pergunta: Quais configurações de GPO se aplicam entre links lentos por padrão?

> **Resposta:** Processamento da política do Registro e da política de segurança se aplica mesmo quando um link lento é detectado. Não é possível alterar essa configuração.

Pergunta: Você deve verificar se uma política no nível do domínio é aplicada, mas o grupo Gerentes deve estar isento da política. Como você conseguiria isso?

> **Resposta:** Defina o link a ser imposto no nível de domínio e use filtros do grupo de segurança para negar a permissão Aplicar Política de Grupo ao grupo Gerentes.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
As configurações da Política de Grupo não são aplicadas a todos os usuários em uma UO ou onde um GPO é aplicado.	• Verifique os filtros de segurança no GPO. • Verifique os filtros WMI no GPO.
Às vezes, as configurações da Política de Grupo precisam de duas reinicializações para serem aplicadas.	Habilite a configuração de política **Sempre Esperar pela Rede ao Iniciar o Computador e Fazer Logon**.

Perguntas e respostas da revisão do laboratório

Laboratório A: Implementação de uma infraestrutura de Política de Grupo

Perguntas e respostas

Pergunta: Muitas organizações dependem muito dos filtros do grupo de segurança para delimitar o escopo de GPOs, em vez de vincular GPOs a UOs específicas. Nessas organizações, os GPOs normalmente estão vinculados na parte superior da estrutura lógica do Active Directory – ao próprio domínio ou a uma UO de primeiro nível. Quais são as vantagens que você obtém usando filtros do grupo de segurança, em vez de links de GPO, para gerenciar o escopo de um GPO?

Resposta: O problema fundamental de depender de UOs para delimitar o escopo da aplicação de GPOs é que a UO é uma estrutura inflexível dentro do AD DS; um único usuário ou computador pode existir apenas dentro de uma UO. À medida que as organizações ficam mais maiores e mais complexas, os requisitos de configuração ficam difíceis de serem atendidos em uma relação um-para-um com qualquer estrutura de contêiner. Com os grupos de segurança, um usuário ou um computador pode existir em quantos grupos for necessário, e é possível adicionar ou removê-los facilmente sem afetar a segurança ou o gerenciamento da conta de computador ou de usuário.

Pergunta: Por que seria útil criar um grupo isento – um grupo cuja permissão Aplicar Política de Grupo é negada – para cada GPO que você criasse?

Resposta: Existem pouquíssimos cenários nos quais é possível garantir que todas as configurações em um GPO sempre precisarão ser aplicadas a todos os usuários e computadores dentro do escopo. Tendo um grupo isento, você precisará ser capaz de responder a situações nas quais você deve excluir um usuário ou um computador. Isso também pode ajudar na solução de problemas de compatibilidade e funcionalidade. Às vezes, as configurações de GPO específicas podem interferir na funcionalidade de um aplicativo. Para testar se o aplicativo funciona em uma instalação limpa do sistema operacional Windows, você talvez precise excluir o usuário ou o computador temporariamente do escopo de GPOs.

Pergunta: Você usa o processamento da política de loopback na organização? Em quais cenários e a quais configurações de política o processamento da política de loopback agrega valor?

Resposta: As respostas variam. Entre os cenários podem estar: em salas de conferência e quiosques, em computadores de Virtual Desktop Infrastructure e em outros ambientes padrão.

Laboratório B: Solução de problemas da infraestrutura da Política de Grupo

Perguntas e respostas

Pergunta: Em quais situações você usou relatórios RSoP para solucionar problemas de aplicação da Política de Grupo na organização?

Resposta: As respostas irão variar com base nas experiências e nas situações dos alunos. Entre as respostas possíveis podem estar:

- Resolveu um problema da Política de Grupo em que um GPO não foi aplicado por causa dos filtros de segurança.
- Resolveu um problema da Política de Grupo em que uma extensão do lado do cliente demorou 20 segundos para ser aplicada por causa de um problema do DNS (Sistema de Nomes de Domínio).
- Localizou uma configuração GPO que foi configurado no GPO errado.
- Localizou um problema da Política de Grupo em que as configurações de usuário incorretas foram aplicadas por causa do processamento de loopback.

Pergunta: Em quais situações você usou a modelagem da Política de Grupo? Caso você ainda não tenha feito isso, em quais situações é possível prever usar a modelagem da Política de Grupo?

Resposta: As respostas irão variar com base nas experiências e nas situações dos alunos. Entre as respostas possíveis podem estar:

- Conseguiu configurar a Política de Grupo corretamente com base em simulações de modelagem da Política de Grupo.
- Testou o resultado de adicionar um usuário a um grupo de segurança.
- Testou o resultado de mover um usuário para outra UO.
- Testou o resultado de configurar o processamento de loopback de um computador.

Módulo 6

Gerenciamento de configurações de usuários com a Política de Grupo

Sumário:

Lição 1

Implementação de modelos administrativos

Sumário:

Perguntas e respostas

Pergunta: Quais seções estão disponíveis no nó **Modelos Administrativos** no nó **Configuração do Usuário**? (Selecione todas as opções que se aplicam.)

( ) Área de Trabalho

( ) Componentes do Windows

( ) Servidor

( ) Sistema

( ) Painel de Controle

Resposta:

(√) Área de Trabalho

(√) Componentes do Windows

( ) Servidor

(√) Sistema

(√) Painel de Controle

Comentários:

Algumas seções são exibidas nos **Modelos Administrativos** nas seções de computador e usuário de um GPO. A seção Área de trabalho está somente na seção do usuário e a seção Servidor está apenas na seção do computador. Componentes do Windows, Sistema e Painel de controle estão em ambas as seções, do computador e do usuário, de um GPO, embora as configurações que você pode configurar nessas seções não sejam as mesmas.

Pergunta: É possível criar o repositório central através do GPMC.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Para criar o repositório central, é necessário criar manualmente a pasta **PolicyDefinitions** no SYSVOL e copiar os arquivos .admx e .adml para a pasta **PolicyDefinitions**.

Discussão: Utilizações práticas de modelos administrativos

Pergunta: Como você oferece segurança de área de trabalho atualmente?

Resposta: As respostas variam.

Pergunta: Quantos acessos administrativos os usuários têm para seus sistemas?

Resposta: As respostas variam.

Pergunta: Quais configurações de Política de Grupo você acha útil para sua organização?

Resposta: As respostas variam.

Recursos

Importação de modelos de segurança

Leitura adicional: Para obter mais informações, consulte SCM (Gerenciador de Compatibilidade de Segurança): http://aka.ms/Ypdcmd

Gerenciamento de modelos administrativos

Leitura adicional: Para obter mais informações, consulte ADMX Migrator: http://aka.ms/Ny5p5c

Leitura adicional: Para obter mais informações, consulte os arquivos do Modelo Administrativo do Office 2016 (ADMX/ADML) e a Ferramenta de Personalização do Office: http://aka.ms/Nknzlx

Demonstração: Definição de configuração com modelos administrativos

Etapas da demonstração

Configurar uma configuração de política de modelos administrativos

1. Alterne para **LON-DC1**.
2. No **Gerenciador do Servidor**, clique em **Ferramentas** e clique em **Gerenciamento** de **Política de Grupo**.
3. No painel de navegação, expanda **Floresta: Adatum.com**, expanda **Domínios**, expanda **Adatum.com** e clique no contêiner **Objetos de Política de Grupo**.
4. Clique com o botão direito do mouse no contêiner **Objetos de Política de Grupo** e clique em **Novo**.
5. Na caixa de diálogo **Novo GPO**, no campo **Nome**, digite **GPO1** e clique em **OK**.
6. No painel de detalhes, clique com o botão direito do mouse em **GPO1** e clique em **Editar**.
7. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, expanda **Configuração do Usuário**, expanda **Políticas**, **Modelos Administrativos** e clique em **Sistema**.
8. No painel de detalhes, clique duas vezes em **Impedir acesso ao prompt de comando**.
9. Na caixa de diálogo **Impedir Acesso ao prompt de comando**, mostre os três valores possíveis e clique em **Cancelar**.

Filtrar configurações de política de modelos administrativos

1. Clique com o botão direito do mouse em **Modelos Administrativos** e clique em **Opções de Filtragem**.
2. Marque a caixa de seleção **Habilitar Filtros de Palavra-chave**.
3. Na caixa de texto **Filtro para palavra(s)**, digite **proteção de tela**.
4. Na caixa suspensa ao lado da caixa de texto, selecione **Todos** e clique em **OK**.
5. Destaque que as configurações de política dos modelos administrativos são filtradas para mostrar apenas aquelas que contêm as palavras **proteção de tela**. Reserve alguns minutos para examinar as configurações encontradas. Explique que configurações podem aparecer sem a proteção de tela no título, já que a proteção de tela também pode ser exibida no texto de ajuda.

6. Na árvore de console, em **Configuração do Usuário**, clique com o botão direito do mouse em **Modelos Administrativos** e clique em **Opções de Filtro**.
7. Desmarque a caixa de seleção **Habilitar Filtros de Palavra-chave**.
8. Na caixa de listagem suspensa **Configurado**, selecione **Sim** e clique em **OK**. Destaque que as configurações de política dos modelos administrativos são, agora, filtradas para mostrar apenas aquelas que foram configuradas como habilitadas ou desabilitadas. Nenhuma configuração foi configurada.
9. Na árvore de console, em **Configuração do Usuário**, clique com o botão direito do mouse em **Modelos Administrativos** e desmarque a opção **Filtro Ativado**.

Adicionar comentários a uma configuração de política

1. Na árvore de console, em **Configuração do Usuário**, expanda **Políticas**, **Modelos Administrativos** e **Painel de Controle** e clique em **Personalização**.
2. No painel de detalhes, clique duas vezes na configuração de política **Habilitar Proteção de Tela**.
3. Na seção **Comentário**, digite **Política de segurança de IT corporativa implementada com essa política em combinação com Proteger com Senha a Proteção de Tela**. Clique em **Habilitado** para habilitar a política e clique em **OK**.
4. Clique duas vezes na configuração da política **Proteger com senha a proteção de tela** e clique em **Habilitado**.
5. Na seção **Comentário**, digite **Política de segurança de IT corporativa implementada em combinação com Habilitar Proteção de Tela** e clique em **OK**.

Adicionar comentários a um GPO

1. No **Editor de Gerenciamento de Política de Grupo**, na árvore do console, clique com o botão direito no nó raiz **GPO1 [LON-DC1.ADATUM.COM]** e clique em **Propriedades**.
2. Clique na guia **Comentário**.
3. Digite as **políticas padrão corporativas Adatum. As configurações são definidas para todos os usuários e computadores no domínio. Pessoa responsável por esse GPO: *seu nome*** e, em seguida, clique em **OK**.
4. Destaque que este comentário é mostrado na guia **Detalhes** do GPO no **Console de Gerenciamento de Política de Grupo**.
5. Feche a janela Editor de Gerenciamento de Política de Grupo.

Criar um novo GPO copiando um GPO já existente

1. No GPMC, no painel de navegação, clique no contêiner **Objetos de Política de Grupo**, clique com o botão direito do mouse em **GPO1** e clique em **Copiar**.
2. Clique com o botão direito do mouse no contêiner **Objetos de Política de Grupo**, clique em **Colar** e clique duas vezes em **OK** .

Criar um novo GPO importando configurações que foram exportadas de outro GPO

1. No GPMC, no painel de navegação, clique no contêiner **Objetos de Política de Grupo**, clique com o botão direito do mouse em **GPO1** e clique em **Fazer backup**.
2. Na caixa **Local**, digite **c:** e, em seguida, clique em **Fazer backup**.
3. Quando o backup terminar, clique em **OK**.
4. No GPMC, no painel de navegação, clique com o botão direito do mouse no contêiner **Objetos de Política de Grupo** e depois clique em **Novo**.
5. Na caixa **Nome**, digite **ADATUM Import** e clique em **OK**.
6. No GPMC, no painel de navegação, clique com o botão direito do mouse em **ADATUM Import** GPO e, em seguida, clique em **Importar Configurações**.
7. No **Assistente para Importar Configurações**, clique em **Avançar** três vezes.
8. Selecione **GPO1** e clique em **Avançar** duas vezes.
9. Clique em **Concluir** e em **OK**.
10. Feche o GPMC.

Lição 2

Configuração de Redirecionamento de Pasta, instalação de software e scripts

Sumário:

Perguntas e respostas

Pergunta: Qual das seguintes pastas pode ser redirecionada usando o Redirecionamento de Pasta? (Selecione todas as opções que se aplicam.)

( ) Documentos

( ) Favoritos

( ) AppData (Roaming)

( ) AppData (local)

( ) Arquivos de Programas

Resposta:

(√) Documentos

(√) Favoritos

(√) AppData (Roaming)

( ) AppData (local)

( ) Arquivos de Programas

Comentários:

Você pode redirecionar **Documentos**, **Favoritos** e **AppData (roaming)**. Existem três diretórios e um diretório AppData do usuário: **Local**, **LocalLow** e **Roaming**. Você só pode redirecionar **Roaming** usando o Redirecionamento de Pasta. Não é possível redirecionar **Arquivos de Programas**. Esta pasta precisa estar localizada no disco rígido local.

Categorizar atividade

Pergunta: Inclua cada item na categoria apropriada. Indique sua resposta, escrevendo o número da categoria à direita de cada item.

Itens	
1	Scripts de logon
2	Scripts de inicialização
3	Atribuição do software
4	Scripts de logoff
5	Scripts de desligamento
6	Redirecionamento de pastas
7	Publicação do software

Categoria 1		Categoria 2		Categoria 3
Configuração do Usuário		**Configuração do Computador**		**Configuração do Usuário e Configuração do Computador**

Categoria 1		Categoria 2		Categoria 3

Resposta:

Categoria 1		Categoria 2		Categoria 3
Configuração do Usuário		**Configuração do Computador**		**Configuração do Usuário e Configuração do Computador**
Scripts de logon **Scripts de logoff** **Redirecionamento de pastas** **Publicação do software**		**Scripts de inicialização** **Scripts de desligamento**		**Atribuição do software**

Configurações para configuração de redirecionamento de pasta

Pergunta: Usuários no mesmo departamento geralmente entram em computadores diferentes. Eles precisam de acesso às pastas **Documentos:** Eles também precisam que os dados permaneçam confidenciais. Qual configuração de Redirecionamento de Pasta você escolheria?

> **Resposta: Criar uma pasta para cada usuário no caminho raiz**. Isso cria uma pasta **Documentos**, à qual somente o usuário tem acesso.

Demonstração: Configuração do Redirecionamento de Pasta

Etapas da demonstração

Criar uma pasta compartilhada

1. Em **LON-DC1**, na barra de tarefas, clique no ícone do **Explorador de Arquivos**.
2. No painel de navegação, clique em **Este PC**.
3. No painel de detalhes, clique duas vezes em **Disco Local (C:)** e, na guia **Início**, clique em **Nova pasta**.
4. Na caixa de texto **Nome**, digite **Redirecionar** e pressione Enter.
5. Clique com o botão direito do mouse na pasta **Redirecionar**, clique em **Compartilhar com** e clique em **Pessoas específicas**.
6. Na caixa de diálogo **Compartilhamento de Arquivo**, clique na seta suspensa, selecione **Todos** e clique em **Adicionar**.
7. No grupo Todos, clique na seta suspensa **Nível de Permissão** e clique em **Leitura/gravação**.
8. Clique em **Compartilhar** e em **Pronto**.
9. Feche a janela **Disco Local (C:)**.

Criar um GPO para redirecionar a pasta Documentos

1. No Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. No painel de navegação, clique com o botão direito do mouse no domínio **Adatum.com** e, em seguida, clique em **Criar um GPO neste domínio e fornecer um link para ele aqui**.
3. Na caixa de diálogo **Novo GPO**, na caixa de texto **Nome**, digite **Redirecionamento de Pasta** e clique em **OK**.
4. No painel de navegação, clique com o botão direito do mouse em **Redirecionamento de Pasta** e, em seguida, em **Editar**.
5. Na janela **Editor de Gerenciamento de Política de Grupo**, em **Configuração do Usuário**, expanda **Políticas**, expanda **Configurações do Windows** e expanda **Redirecionamento de Pasta**.
6. Clique com o botão direito do mouse em **Documentos** e clique em **Propriedades**.
7. Na caixa de diálogo **Propriedades do Documento**, na guia **Destino**, clique na seta suspensa **Configuração** e selecione **Básico – Redirecionar a pasta de todas as pessoas para o mesmo local**.
8. Verifique se a caixa **Local da pasta de destino** está configurada para **Criar uma pasta para cada usuário no caminho raiz**.
9. Na caixa de texto **Caminho Raiz**, digite **\\LON-DC1\Redir** e clique em **OK**.
10. Na caixa de diálogo **Aviso**, clique em **Sim**.
11. Feche o Editor de Gerenciamento de Política de Grupo.

Testar o Redirecionamento de Pasta

1. Entre em **LON-CL1** como **Adatum\Administrador** com a senha **Pa55w.rd**.
2. Clique com o botão direito em **Iniciar** e clique em **Prompt de Comando**.
3. Na janela Prompt de Comando, digite o seguinte comando e pressione Enter:

```
Gpupdate /force
```

4. Na janela do prompt de comando, quando solicitado, digite o seguinte comando e pressione Enter:

```
S
```

5. Entre em **LON-CL1** como **Adatum\Administrador** com a senha **Pa55w.rd**.
6. Na barra de tarefas, clique no ícone do **Explorador de Arquivos**.
7. No painel de navegação, na seção **Acesso Rápido**, clique com o botão direito do mouse em **Documentos** e, em seguida, em **Propriedades**.
8. Verifique se, na guia **Geral**, o campo Local tem um valor **\\lon-dc1\redir\Administrator**.
9. Se o teste não tiver êxito, repita as etapas de 2 a 7 e, em seguida, verifique o redirecionamento mais uma vez.
10. Saia de **LON-CL1**.

Demonstração: Configuração de scripts com GPOs

Etapas da demonstração

Criar um script de logon para exibir a mensagem

1. Em LON-DC1, clique em **Iniciar**, digite **Bloco de notas** e, em seguida, clique em **Bloco de notas**.
2. No bloco de notas, digite o seguinte comando e pressione Enter:

```
Msgbox “This is the script”
```

3. Clique no menu **Arquivo** e em **Salvar como**.
4. Na caixa de diálogo **Salvar como** na caixa de texto **Nome do arquivo** digite **Logon.vbs**.
5. Na lista **Salvar como tipo**, selecione **Todos os Arquivos (*.*)**.
6. No painel de navegação, clique em **Área de Trabalho** e em **Salvar**.
7. Feche o **Bloco de notas**.
8. Na área de trabalho, clique com o botão direito do mouse no arquivo **Logon.vbs** e clique em **Copiar**.

Criar e vincular um GPO para usar o script

1. Abra o **Gerenciador do Servidor**, clique em **Ferramentas** e clique em **Gerenciamento de Política de Grupo**.
2. Expanda a **Floresta: Adatum.com** e expanda **Domínios**.
3. Clique com o botão direito do mouse em **Adatum.com** e clique em **Criar um GPO neste domínio e forneça um link para ele aqui**.
4. Na caixa de diálogo **Novo GPO**, na caixa de texto **Nome**, digite **Script de Logon de Usuário** e clique em **OK**.
5. Expanda **Adatum.com**, clique com o botão direito do mouse no GPO **Script de Logon de Usuário** e, em seguida, clique em **Editar**.
6. Na janela **Editor de Gerenciamento de Política de Grupo**, em **Configuração do Usuário**, expanda **Políticas**, expanda **Configurações do Windows** e clique em **Scripts (Logon/Logoff)**.
7. No painel de detalhes, clique duas vezes em **Logon**.
8. Na caixa de diálogo **Propriedades de Logon**, clique em **Mostrar Arquivos**.
9. No painel de detalhes, clique com o botão direito do mouse na área em branco e clique em **Colar**.
10. Feche a janela de **logon**.
11. Na caixa de diálogo **Propriedades de Logon**, clique em **Adicionar**.
12. Na caixa de diálogo **Adicionar um Script**, clique em **Procurar**.
13. Clique no script **Logon.vbs** e clique em **Abrir**.
14. Clique em **OK** duas vezes para fechar todas as caixas de diálogo.
15. Feche a janela **Editor de Gerenciamento de Política de Grupo** e o **Console de Gerenciamento de Política de Grupo**.

Entre em um computador do cliente para testar os resultados

1. Em **LON-CL1**, saia e entre como **Adatum\Administrador** com a senha **Pa$$word**.
2. Clique com o botão direito em **Iniciar** e clique em **Prompt de Comando**.
3. Na janela Prompt de Comando, digite o seguinte comando e pressione Enter:

```
Gpupdate /force
```

4. Se solicitado, na janela do prompt de comando, digite o seguinte comando e pressione Enter:

```
Y
```

5. Entre em **LON-CL1** como **Adatum\Connie** com a senha **Pa55w.rd**.
6. Verifique se o script é executado, exibindo a mensagem que você configurou anteriormente no GPO.

 **Observação:** A mensagem pode levar até dez minutos para ser exibida. Se a mensagem não for exibida, reinicie o **LON-CL1** e repita as etapas de um a cinco.

7. Saia de **LON-CL1**.

Lição 3

Configuração de preferências de Política de Grupo

Sumário:

Perguntas e respostas

Pergunta: Quais configurações de preferências da Política de Grupo você pode usar para configurar uma experiência do usuário do Internet Explorer? (Selecione todas as opções que se aplicam.)

( ) Internet Explorer

( ) Atalhos

( ) Registro

( ) Opções de Energia

( ) Opções de pasta

Resposta:

(√) Internet Explorer

(√) Atalhos

(√) Registro

( ) Opções de Energia

( ) Opções de pasta

Comentários:

É possível usar as configurações do Internet Explorer nas preferências da Política de Grupo para configurar o Microsoft Internet Explorer. Os atalhos podem criar favoritos que os usuários podem abrir no Internet Explorer. É possível usar o registro para configurar as configurações baseadas em registro do Internet Explorer. Não é possível usar Opções de Energia ou Opções de Pasta para configurar o Internet Explorer.

Pergunta: É possível usar o direcionamento no nível de item para limitar as preferências de Política de Grupo dependendo de qual floresta do AD DS o usuário pertence.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

A Política de Grupo não pode percorrer florestas. Você pode usar domínios, sites, grupos de segurança e unidades organizacionais em direcionamento em nível de item.

Pergunta: Em quais cenários você usou as preferências de Política de Grupo e direcionamento em nível de item?

Resposta: As respostas variam. Além de obter respostas dos alunos, compartilhe suas próprias experiências com o resto da classe.

Demonstração: Configuração de preferências de Política de Grupo

Etapas da demonstração

Criar uma impressora com as preferências de Política de Grupo

1. Em LON-DC1, clique com o botão direito do mouse em **Iniciar**, e clique em **Painel de Controle**.
2. No Painel de Controle, clique em **Exibir impressoras e dispositivos**.
3. Clique em **Adicionar uma impressora**.
4. Na caixa de diálogo **Adicionar um dispositivo**, clique em **A impressora que desejo não está na lista**.
5. Na caixa de diálogo **Adicionar Impressora**, selecione **Adicionar uma impressora local ou de rede usando configurações manuais** e, em seguida, clique em **Avançar**.
6. Na página **Escolher uma porta de impressora**, clique em **Avançar**.
7. Na página **Instalar o driver de impressora**, clique em **Avançar**.
8. Na página **Digitar o nome de uma impressora**, na caixa de texto **Nome da impressora**, digite **Brother** e clique em **Avançar**.
9. Na página **Compartilhamento de impressora**, clique em **Avançar**.
10. Na página **Você adicionou Brother com êxito**, clique em **Concluir**.
11. Feche o Painel de controle.
12. Se necessário, alterne para o **Gerenciador do Servidor**.
13. No **Gerenciador do Servidor**, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
14. No painel de navegação, expanda **Floresta: Adatum.com**, expanda **Domínios**, expanda **Adatum.com** e clique no domínio **Adatum.com**.
15. Clique com o botão direito do mouse no domínio **Adatum.com** e clique em **Criar um GPO neste domínio e fornecer um link para ele aqui**.
16. Na caixa de diálogo **Novo GPO**, digite **GP Prefs** e clique em **OK**.
17. No painel de navegação, clique com o botão direito do mouse em **GP Prefs** e, em seguida, em **Editar**.
18. Em **Editor de Gerenciamento de Política de Grupo**, expanda **Configuração do Usuário**, expanda **Preferências**, expanda **Configurações do Painel de Controle**, clique com o botão direito do mouse em **Impressoras**, passe o mouse sobre **Novo** e clique em **Impressora Compartilhada**.
19. Na caixa de diálogo **Propriedades da Nova Impressora Compartilhada**, na caixa de texto **Caminho do Compartilhamento**, digite **\\LON-DC1\Brother**.
20. Marque a caixa de seleção **Definir esta impressora como padrão**.

Indicar a preferência

1. Na guia **Comum**, marque a caixa de seleção **Direcionamento de nível de item** e clique em **Direcionamento**.
2. Na caixa de diálogo **Editor de Destino**, clique em **Novo Item** e clique em **Intervalo de Endereços IP**.
3. Na caixa de texto **entre**, digite **172.16.0.50**, na caixa de texto **e**, digite **172.16.0.99** e clique duas vezes em **OK**.

Configure um plano de energia com preferências de Política de Grupo

1. No Editor de Gerenciamento de Política de Grupo, expanda **Configuração do Computador**, expanda **Preferências**, expanda **Configurações do Painel de Controle** e clique em **Opções de Energia**.
2. Clique com o botão direito do mouse em **Opções de Energia**, passe o mouse sobre **Novo** e clique em **Plano de Energia (Windows 7 ou posterior)**.
3. Na caixa de diálogo **Propriedades do Novo Plano de Energia (Windows 7 ou posterior)** clique na lista suspensa **Equilibrado** e, em seguida, digite **Plano de Energia Adatum**.
4. Marque a caixa de seleção **Definir como um plano de energia ativo**.

Indicar a preferência

1. Na guia **Comum**, marque a caixa de seleção **Direcionamento de nível de item** e clique em **Direcionamento**.
2. Na caixa de diálogo **Editor de Destino**, clique em **Novo Item** e clique em **Sistema Operacional**.
3. Na lista **Produto**, selecione **Windows 10** e clique em **OK** duas vezes.
4. Feche a janela **Editor de Gerenciamento de Política de Grupo**.

Testar as preferências

1. Entre em **LON-CL1** como **Adatum\Administrador** com a senha **Pa55w.rd**.
2. Na janela que é aberta, clique em **OK**.
3. Clique com o botão direito em **Iniciar** e clique em **Prompt de Comando**.
4. Na janela **Prompt de Comando**, digite o seguinte comando e pressione Enter:

```
gpupdate /force
```

5. Na janela do prompt de comando, quando solicitado, digite o seguinte comando e pressione Enter:

```
Y
```

6. Entre em LON-CL1 como **Adatum\Administrador** com a senha **Pa55w.rd**.
7. Na janela que é aberta, clique em **OK**.
8. Clique com o botão direito do mouse em **Iniciar** e clique em **Painel de Controle**.
9. Clique em **Hardware e Sons** e em **Dispositivos e Impressoras**.
10. Verifique a presença da impressora **Brother no LON-DC1**.
11. Clique na seta para trás e, em seguida, em **Opções de Energia**.
12. Verifique se o **Plano de Energia Adatum** está presente e é o plano de energia ativo.

Revisão do módulo e informações complementares

Práticas recomendadas

Práticas recomendadas relacionadas ao gerenciamento da Política de Grupo

- Ao definir as configurações nos GPOs, inclua os comentários nas configurações do GPO.
- Use um repositório central para Modelos administrativos.
- Use preferências de Política de Grupo para definir configurações que não estão disponíveis nas configurações de Política de Grupo.

Perguntas de Revisão

Pergunta: Por que algumas configurações de Política de Grupo precisam de dois logons para entrarem em vigor?

> **Resposta:** Os usuários entram normalmente com credenciais armazenadas em cache o que pode prevenir a Política de Grupo de ser aplicada a sessão atual. As configurações entrarão em vigor no próximo logon.

Pergunta: Qual é a vantagem de ter um repositório central?

> **Resposta:** Um repositório central é uma única pasta em SYSVOL que armazena todos os arquivos .admx e .adml que são requeridos. Depois que você configurar o repositório central, o Editor de Gerenciamento de Política de Grupo irá reconhecê-lo e carregará todos os Modelos administrativos a partir do repositório central em vez da máquina local.

Pergunta: Qual é a principal diferença entre as configurações de Política de Grupo e as preferências de Política de Grupo?

> **Resposta:** As configurações da Política de Grupo impõem algumas configurações no lado do cliente e desabilitam interfaces de cliente para modificação. No entanto, as preferências de Política de Grupo fornecem configurações e permitem que o cliente as modifiquem.

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Você configurou o Redirecionamento de Pasta para uma UO, mas nenhuma das pastas de usuários está sendo redirecionada para o local de rede. Na pasta raiz, você observa que um subdiretório nomeado para cada usuário foi criado, mas eles estão vazios.	O problema provavelmente está relacionado a permissões. A Política de Grupo cria os subdiretórios nomeados do usuário, mas os usuários não possuem permissões suficientes para suas pastas redirecionadas neles.
Você tem uma mistura de computadores Windows 7 e Windows 10. Depois de definer várias configurações nos Modelos administrativos de um GPO, os usuários com o sistemas operacionais Windows 7 relatam que alguns configurações são aplicadas, mas outras não.	Nem todas as novas configurações se aplicam a sistemas operacionais mais antigos como o Windows 7. Verifique a própria configuração para ver para quais sistemas operacionais a configuração se aplica.
As preferências de Política de Grupo não são aplicadas.	Verifique as configurações de preferência para redirecionamento de nível de item ou se há configuração incorreta.

Perguntas e respostas da revisão do laboratório

Laboratório: Gerenciamento de configurações de usuários com a Política de Grupo

Perguntas e respostas

Pergunta: Quais opções você pode usar para separar as pastas redirecionadas dos usuários para servidores diferentes?

> **Resposta:** É possível usar a configuração **Avançado** no Redirecionamento de Pasta para escolher diferentes pastas compartilhadas em diferentes servidores para grupos de segurança diferentes.

Pergunta: É possível nomear dois métodos que você pode usar para atribuir um GPO a objetos selecionados dentro de uma UO?

> **Resposta:** É possível usar os filtros de WMI (Instrumentação de Gerenciamento do Windows) para definir um critério para aplicação da Política de Grupo, por exemplo, se o computador é um notebook ou qual versão do sistema operacional está instalada. Também é possível usar permissões no próprio GPO para permitir ou negar configurações do GPO para usuários ou computadores.

Pergunta: Você criou as preferências de Política de Grupo para configurar novas opções de energia. Como você pode certificar-se de que as preferências se aplicam somente a computadores laptop?

> **Resposta:** É possível usar o direcionamento de nível de item para aplicar as preferências aos computadores portáteis. Em seguida, as preferências serão aplicadas se o perfil de hardware do computador identificá-lo como um computador portátil.

Módulo 7

Proteção do Active Directory Domain Services

Sumário:

Lição 1

Proteção dos controladores de domínio

Sumário:

Perguntas e respostas

Pergunta: Como fornecer maior segurança para unidades de disco rígido nos controladores de domínio?

> **Resposta:** Para fornecer um nível a mais de segurança, use a criptografia de unidade de disco BitLocker para criptografar discos rígidos do controlador de domínio.

Demonstração: Configuração de uma política de replicação de senha

Etapas da demonstração

Preparar uma instalação delegada de um RODC

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Serviços e Sites do Active Directory**.
2. Em **Serviços e Sites do Active Directory**, no painel de navegação, clique em **Sites**. No menu **Ação**, clique em **Novo Site**.
3. Na caixa de diálogo **Novo Objeto – Site**, no campo **Nome**, digite **Munique**, selecione o objeto de link de site **DEFAULTIPSITELINK** e clique em **OK**.
4. Na caixa de mensagem **Active Directory Domain Services**, clique em **OK**.
5. Alterne para **Gerenciador do Servidor**, clique em **Ferramentas** e em **Central Administrativa do Active Directory**.
6. Em **Central Administrativa do Active Directory**, no painel de navegação, clique em **Adatum (local)** e, no painel de detalhes, clique duas vezes na unidade organizacional (UO) **Domain Controllers**.
7. No painel **Tarefas**, na seção **Domain Controllers**, clique em **Pré-criar uma conta do controlador de domínio Somente leitura**.
8. No **Assistente para Instalação do Active Directory Domain Services**, na página **Assistente de Instalação dos Serviços de Domínio Active Directory**, clique em **Avançar**.
9. Na página **Credenciais de Rede**, clique em **Avançar**.
10. Na página **Especifique o Nome do Computador**, digite o nome do computador como **MUC-RODC1** e clique em **Avançar**.
11. Na página **Selecione um Site**, clique em **Munique** e em **Avançar**.
12. Na página **Opções Adicionais de Controlador de Domínio**, aceite a configuração padrão, marque as caixas de seleção **Servidor DNS** e **Catálogo global** e clique em **Avançar**.
13. Na página **Instalação e Administração de Delegação de RODC,** clique em **Definir**.
14. Na caixa de diálogo **Selecionar Usuário ou Grupo**, no campo **Digite o nome do objeto a ser selecionado**, digite **Bill**, e clique em **Verificar Nomes**.
15. Verifique se Bill Norman está resolvido e clique em **OK**.
16. Na página **Instalação e Administração de Delegação de RODC**, clique em **Avançar**.
17. Na página **Resumo**, revise sua seleção e clique em **Avançar**.
18. Na página **Concluindo o Assistente para Instalação do Active Directory Domain Services**, clique em **Concluir**.

Exibir uma política de replicação de senha de RODC

1. No **Central Administrativa do Active Directory**, na UO **Controladores de Domínio**, selecione **MUC-RODC1**.
2. No painel **Tarefas**, na seção **MUC-RODC1**, clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades** do **MUC-RODC1 (Desabilitado)**, role para baixo até **Extensões**, e clique na guia **Política de Replicação de Senha**.
4. Examine os grupos, usuários e computadores padrão na Política de Replicação de Senha.
5. Deixe a caixa de diálogo aberta.

Configurar uma política de replicação de senha específica de RODC

1. Alterne para **Gerenciador do Servidor**, clique em **Ferramentas** e em **Usuários e Computadores do Active Directory**.
2. No painel de navegação, expanda **Adatum.com** e clique em **Usuários**.
3. No menu **Ação**, clique em **Novo** e em Grupo.
4. Na caixa de diálogo **Novo Objeto – Grupo**, digite o nome do grupo como **Grupo de Replicação de Senha RODC Permitido de Munique** e clique em **OK**.
5. Clique duas vezes em **Grupo de Replicação de Senha RODC Permitido de Munique**, clique na guia **Membros** e clique em **Adicionar**.
6. Na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Ana** e clique em **Verificar Nomes**.
7. Na caixa de diálogo **Diversos Nomes Encontrados**, selecione **Ana Cantrell** e clique em **OK**.
8. Na caixa de diálogo **Selecionar Usuários, Contatos, Computadores, Contas de Serviço ou Grupos**, clique em **OK** e, na caixa de diálogo **Propriedades de Grupo de Replicação de Senha RODC Permitido de Munique**, clique em **OK**.
9. Feche **Usuários e Computadores do Active Directory**.
10. Alterne para **Centro Administrativo do Active Directory** e abra as propriedades de **MUC-RODC1**. Na seção **Extensões**, na guia **Política de Replicação de Senha**, clique em **Adicionar**.
11. Na caixa de diálogo **Adicionar Grupos, Usuários e Computadores**, selecione a opção **Permitir a replicação de senhas da conta para este RODC** e clique em **OK**.
12. Na caixa de diálogo **Selecionar Usuários, Computadores, Contas de Serviço ou Grupos**, na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Munique**, clique em **Verificar Nomes** e em **OK**.
13. Na caixa de diálogo **MUC-RODC1 (Desabilitado)**, clique em **OK**.

Verificar a política de senha resultante

1. No **Centro Administrativo do Active Directory**, no painel **Tarefas,** na seção **MUC-RODC1**, clique em **Propriedades**.
2. Na caixa de diálogo **Propriedades de MUC-RODC1 (Desabilitado)**, na seção **Extensões** da guia **Política de Replicação de Senha**, clique em **Avançado**.

 **Observação:** a caixa de diálogo **Política de Replicação de Senha Avançada para MUC-RODC1** exibe todas as contas com senhas armazenadas neste RODC.

3. Na lista suspensa **Exibir usuários e computadores que atendam aos seguintes critérios**, clique em **Contas que foram autenticadas para este Controlador de Domínio Somente Leitura** e informe aos alunos que esta página mostrará apenas as contas que têm as permissões solicitadas e autenticadas pelo RODC.
4. Na guia **Política Resultante**, clique em **Adicionar** e, na caixa de diálogo **Selecionar Usuários ou Computadores**, no campo **Digite o nome do objeto a ser selecionado**, digite **Ana**, clique em **Verificar Nomes** e em **OK** duas vezes.
5. Observe que Ana tem uma **Configuração Resultante Permitir**.
6. Feche ou cancele todas as caixas de diálogo.

Lição 2

Implementação de segurança da conta

Sumário:

Perguntas e respostas

Pergunta: Qual tecnologia permite usar a funcionalidade biométrica para entrar nos dispositivos Windows?

> **Resposta:** Windows Hello é uma nova tecnologia no Windows 10 e Windows 10 Mobile que permite autenticação usando impressões digitais, varredura de íris ou outros dados biométricos.

Recursos

Opções de segurança da conta no Windows Server 2016

 **Leitura adicional:** Para obter mais informações sobre a proteção de credenciais e gerenciamento, consulte: http://aka.ms/R5bfid

Demonstração: Configuração de políticas de conta de domínio

Etapas da demonstração

Configurar uma política de senha baseada em domínio

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. No console de **Gerenciamento de Política de Grupo,** expanda **Floresta: Adatum.com\Domains\Adatum.com\Objetos de Política de Grupo**, clique com o botão direito do mouse em **Política de Domínio Padrão** e clique em **Editar**.
3. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, em **Configuração do Computador**, expanda **Políticas\Configurações do Windows\Configurações de Segurança\Políticas de Conta**, clique duas vezes em **Política de Senha** e duas vezes em **Aplicar histórico de senhas**.
4. Na caixa de diálogo de propriedades de **Aplicar histórico de senhas**, no campo **Manter histórico da senha por** , digite **20**, clique em **OK** e clique duas vezes em **Tempo de vida máximo da senha**.
5. Na caixa de diálogo de propriedades de **Tempo de vida máximo da senha**, no campo **A senha expirará em**, digite **45**, clique em **OK** e clique duas vezes em **Tempo de vida mínimo da senha**.
6. Na caixa de diálogo de propriedades de **Tempo de vida mínimo da senha**, verifique se o campo **A senha pode ser alterada após** está definido como **1**, clique em **OK** e clique duas vezes em **Comprimento mínimo da senha**.
7. Na caixa de diálogo de propriedades de **Comprimento mínimo da senha**, no campo **A senha deve ter pelo menos**, digite **10**, clique em **OK** e clique duas vezes em **A senha deve atender aos requisitos de complexidade**.
8. Na caixa de diálogo de propriedades de **A senha deve atender aos requisitos de complexidade**, clique em **Habilitado** e em **OK**.
9. Não feche a janela **Editor de Gerenciamento de Política de Grupo**.

Configurar uma política de bloqueio de conta

1. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, clique em **Política de Bloqueio de Conta** e clique duas vezes em **Duração do bloqueio de conta**.
2. Na caixa de diálogo **Propriedades de Duração do bloqueio de conta**, clique em **Definir esta configuração de política** e, no campo **Minutos**, digite **30** e clique em **OK**.
3. Na caixa de diálogo **Alterações de valor sugeridas**, observe os valores sugeridos, inclusive a configuração automática de **Limite de bloqueio de conta**, clique em **OK** e clique duas vezes em **Zerar contador de bloqueios de conta após**.
4. Na caixa de diálogo de propriedades de **Zerar contador de bloqueios de conta após**, no campo **Zerar contador de bloqueios de conta após**, digite **15** e clique em **OK**.
5. Feche a janela **Editor de Gerenciamento de Política de Grupo** e o console de **Gerenciamento de Política de Grupo**.

Demonstração: Configuração de uma política de senha refinada

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Centro Administrativo do Active Directory**.
2. No **Centro Administrativo do Active Directory**, no painel de navegação, clique em **Adatum (local)**.
3. No painel de detalhes, clique duas vezes na UO **Gerentes**.
4. No painel de detalhes, clique com o botão direito do mouse no grupo **Gerentes** e clique em **Propriedades**.

 **Observação:** verifique se você abriu a caixa de diálogo **Propriedades** do grupo Gerentes, não da UO Gerentes.

5. Na caixa de diálogo **Managers**, em **Escopo do grupo**, clique em **Global** e em **OK**.
6. No Central Administrativa do Active Directory, no painel de navegação, clique em **Adatum (local)**.
7. No painel de detalhes, clique duas vezes no contêiner **System**.
8. No painel de detalhes, clique com o botão direito do mouse em **Passowrd settings container**, clique em **Novo** e em **Password Settings**.
9. Na janela **Criar Configurações de Senha**, conclua as seguintes etapas:
   a. No campo **Nome**, digite **ManagersPSO**.
   b. No campo **Precedência**, digite **10**.
   c. Marque a caixa de seleção **Impor comprimento mínimo da senha** e, no campo **Comprimento mínimo da senha (caracteres)**, digite **15**.
   d. Marque a caixa de seleção **Impor histórico de senhas** e, no campo **Número de senhas lembradas**, digite **20**.

e. Marque a caixa de seleção **A senha deve atender aos requisitos de complexidade**, caso ainda não esteja marcada.

f. Marque a caixa de seleção **Impor duração mínima da senha**, caso ainda não esteja marcada e, no campo **O usuário não pode alterar a senha dentro de (dias)**, digite **1**.

g. Marque a caixa de seleção **Impor duração máxima da senha** caso ainda não esteja marcada e, no campo **O usuário deve alterar a senha após (dias)**, digite **30**.

h. Marque a caixa de seleção **Impor política de desbloqueio de conta**.

i. No campo **Número de tentativas de logon com falha permitido**, digite **3**.

j. No campo **Redefinir contagem de tentativas de logon com falha após (min)**, digite **30** e clique em **Até que um administrador desbloqueie manualmente a conta**.

10. Na seção **Aplica-se Diretamente a**, clique em **Adicionar**.
11. Na caixa de texto **Digite os nomes de objeto a serem selecionados**, digite **Adatum\Managers**, clique em **Verificar Nomes** e em **OK**.
12. Na janela **Criar Configurações de Senha: ManagersPSO**, clique em **OK**.
13. Feche o **Central Administrativa do Active Directory**.

Lição 3

Implementação da autenticação de auditoria

Sumário:

Perguntas e respostas

Pergunta: Quando um usuário entra em um controlador de domínio, é gerado um evento de logon.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Quando um usuário entra em um controlador de domínio, é gerado um evento de logon de conta, não um evento de logon.

Demonstração: Configuração de políticas de auditoria relacionadas à autenticação

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique no menu **Ferramentas** e em **Gerenciamento de Política de Grupo**.
2. No console de **Gerenciamento de Política de Grupo**, no painel de navegação, expanda **Floresta: Adatum.com\Domains\Adatum.com\Objetos de Política de Grupo** e selecione a **Política de Controladores de Domínio Padrão**.
3. Clique com o botão direito do mouse em **Política de Controladores de Domínio Padrão** e clique em **Editar**.
4. Na janela **Editor de Gerenciamento de Políticas de Grupo**, no painel de navegação, expanda **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais** e clique em **Política de Auditoria**.
5. No painel de detalhes, clique duas vezes em **Auditoria de eventos de logon de conta** e explique as seguintes opções de configuração:
   - Se você marcar a caixa de seleção **Definir estas configurações de políticas**, a política será aplicada.
   - Se você selecionar **Êxito**, somente as auditorias com êxito serão registradas.
   - Se você selecionar **Falha**, somente as auditorias com falha serão registradas.

   Se várias políticas contiverem a configuração e ela estiver definida de forma diferente, as opções de êxito e falha serão aplicadas com base na última política aplicada que definiu essas configurações. Se uma política definir auditorias com êxito e a outra definir auditorias com falha, elas não serão mescladas. Clique em **Definir estas configurações de políticas**, marque as caixas de seleção **Êxito** e **Falha** e clique em **OK**.
6. No painel de detalhes, clique duas vezes em **Auditoria de eventos de logon de conta**. Clique na guia **Explicar** e mostre e discuta a explicação. Clique em **Cancelar** para fechar a caixa de diálogo de propriedades de **Auditoria de eventos de logon de conta**.
7. Repita as etapas 5 e 6 com a política de **Auditoria de eventos de logon**.
8. Na janela **Editor de Gerenciamento de Política de Grupo**, no painel de navegação, vá para **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Configuração Avançada de Política de Auditoria\Políticas de Auditoria** e clique em **Políticas de Auditoria**.

9. Na política **Políticas de Auditoria**, mostre as 10 principais categorias e clique duas vezes em **Logon de Conta**.
10. Mostre as quatro subcategorias e clique duas vezes em **Auditoria de Serviço de Autenticação Kerberos**.
11. Mostre que a subcategoria tem as mesmas configurações que **Logon de Conta de Auditoria da Política de Auditoria** e explique que agora elas estão em nível mais detalhado, permitindo uma auditoria mais seletiva.
12. Selecione **Configurar estes eventos de auditoria**, selecione **Êxito** e **Falha** e clique em **Aplicar**.
13. Na guia **Explicar**, mostre e discuta a explicação, as configurações padrão e o volume de auditoria previsto.
14. Para fechar a caixa de diálogo de propriedades de **Auditoria de Serviço de Autenticação Kerberos**, clique em **OK**.

Demonstração: Exibição de eventos de logon

Etapas da demonstração

1. Em **LON-DC1**, na tela inicial, digite **cmd** e clique em **Prompt de Comando**.
2. Digite **gpupdate /force** e pressione Enter.
3. Espere até a política ser atualizada.
4. Alterne para a tela Iniciar. Clique no ícone **Administrador** e em **Sair**.
5. Em **LON-DC1**, tente entrar como **Adatum\Aidan** com a senha **123456**.

   Você receberá uma mensagem informando que o nome de usuário ou a senha está incorreta. Clique em **OK**.
6. Entre como **Adatum\Administrador** com a senha **Pa55w.rd**.
7. Aguarde até o logon ser finalizado e o **Gerenciador do Servidor** ser iniciado.
8. No **Gerenciador do Servidor**, clique em **Ferramentas** e em **Visualizador de Eventos**.
9. No Visualizador de Eventos, no painel de navegação, expanda **Logs do Windows** e clique em **Segurança**.
10. No painel de detalhes, localize o **ID do Evento 4771** e mostre que esse evento é de Falha de Auditoria. Clique duas vezes no evento **Falha de Auditoria**. Mostre que esse evento foi registrado quando Adatum\Aidan tentou entrar com a senha incorreta. Clique em **Fechar**.
11. Localize o evento com o **ID do Evento 4768**. Mostre que se trata de um evento de Êxito de Auditoria. Clique duas vezes no evento **Êxito de Auditoria**. Mostre que esse evento foi registrado quando Adatum\Administrador entrou com êxito. Clique em **Fechar**.
12. Feche o Visualizador de Eventos.

Lição 4

Configuração de contas de serviço gerenciado

Sumário:

Perguntas e respostas

Pergunta: Qual é a diferença entre MSAs de grupo e MSAs padrão?

> **Resposta:** As MSAs de grupo permitem estender os recursos das MSAs padrão para mais de um servidor no domínio.

Demonstração: Configuração de MSAs de grupo

Etapas da demonstração

Criar a chave raiz KDS para o domínio

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e abra o console do **Módulo Active Directory do Windows PowerShell**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
```

Criar e associar uma MSA

1. No prompt de comando, digite o seguinte comando e pressione Enter:

```
New-ADServiceAccount –Name SampleApp_SVR1 –DNSHostname LON-DC1.Adatum.com -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
```

2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Add-ADComputerServiceAccount –identity LON-SVR1 –ServiceAccount SampleApp_SVR1
```

3. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Get-ADServiceAccount -Filter *
```

4. Verifique se a conta de serviço **SampleApp_SVR1** está listada.

Instalar uma MSA

1. Em **LON-SVR1**, clique em **Iniciar** e em **Gerenciador do Servidor**, em seguida, no menu **Ferramentas**, abra o console do **Módulo Active Directory do Windows PowerShell**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

3. Em **Gerenciador do Servidor**, na barra de ferramentas **Menu**, clique em **Ferramentas** e em **Serviços**.
4. No console de **Serviços**, clique com o botão direito do mouse em **Serviço de Compartilhamento de Dados** e clique em **Propriedades**.

 **Observação:** nesta demonstração, o Serviço de Compartilhamento de Dados é usado como exemplo. Em um ambiente de produção, você usaria o serviço real atribuído à MSA.

5. Na caixa de diálogo de propriedades de **Serviço de Compartilhamento de Dados (Computador Local)**, clique na guia **Logon**.
6. Na guia **Logon**, clique em **Esta conta** e digite **Adatum\SampleApp_SVR1$**.
7. Limpe a senha nas caixas **Senha** e **Confirmar senha** e clique em **OK**.
8. Clique em **OK** em todos os avisos.

Revisão do módulo e informações complementares

Perguntas de revisão

Pergunta: Por que a segurança física é tão importante, principalmente nos controladores de domínio do AD DS?

> **Resposta:** Os controladores de domínio do AD DS armazenam todas as informações sobre todos os usuários, computadores, grupos e quaisquer outros objetos do domínio. Se uma pessoa obtiver acesso físico ao servidor ou à sua unidade de disco rígido, ela poderá desviar da proteção de segurança com facilidade e recuperar todas essas informações. Essa pessoa poderá usar as informações para atacar a rede ou modificar o controlador de domínio e colocá-lo de volta na rede com más intenções.

Pergunta: Você precisa implementar políticas de auditoria para autenticação de domínio e alterações nos serviços de diretório. Qual é a melhor maneira de implementar essas configurações de auditoria?

> **Resposta:** Se você deseja habilitar a auditoria, é muito importante definir as mesmas configurações de auditoria para todos os servidores pertinentes nos quais o evento possa ocorrer. Se você deseja configurar a auditoria para autenticação de domínio ou alterações no AD DS, defina essas configurações na Política de Controladores de Domínio Padrão ou um GPO que esteja vinculado à UO de Controladores de Domínio.

Pergunta: Sua organização exige que seja mantida uma infraestrutura AD DS altamente confiável e segura. E também que os usuários tenham acesso ao email corporativo pela Internet, usando o Outlook Web Access. Você está pensando em implementar configurações de bloqueio de conta. O que deve ser considerado?

> **Resposta:** As configurações de bloqueio de conta não são apenas um recurso de segurança. Elas também fornecem aos invasores uma interface DoS de fácil acesso. Se o Outlook Web Access for acessado pela Internet, configure protocolos ou serviços adicionais para garantir que somente os usuários do seu domínio poderão inserir credenciais de logon. Outros usuários não devem ser autorizados a usar o site da Web para inserir senhas falsas e bloquear contas de usuário válidas.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo.

Ferramenta	Use para	Onde encontrar
Usuários e Computadores do Active Directory	Gerenciar objetos dentro do AD DS, por exemplo, usuários, grupos e computadores.	**Gerenciador do Servidor**
Central Administrativa do Active Directory	Gerenciar objetos dentro do AD DS, por exemplo, usuários, grupos e computadores.	**Gerenciador do Servidor**
Gerenciamento de Política de Grupo	Gerenciar, emitir relatório, fazer backup e restaurar GPOs.	**Gerenciador do Servidor**
Gpupdate.exe	Atualizar manualmente os GPOs de máquinas locais.	Linha de comando

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
Você definiu configurações de política de auditoria avançada, mas elas não se aplicam.	Verifique se você definiu **Auditoria: forçar configurações de subcategorias de políticas de auditoria (Windows Vista ou superior) para substituir configurações de categorias de políticas de auditoria** em **Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais\Opções de Segurança**.
Você configurou a auditoria de alterações em logon de conta ou serviços de diretório. Agora, você está testando-os, mas não consegue localizar os eventos no log de eventos do servidor.	Se você tiver vários controladores de domínio, verifique o log de segurança de cada controlador de domínio. Além disso, certifique-se de que você tenha a política de auditoria configurada para cada controlador de domínio.

Perguntas e respostas da revisão do laboratório

Laboratório: Segurança do AD DS

Perguntas e respostas

Pergunta: No laboratório, você definiu as configurações de senha para todos os usuários dentro da Política de Domínio Padrão e também para os administradores dentro de um PSO. Que outras opções estavam disponíveis para ajudá-lo na solução?

Resposta: Você poderia ter criado um PSO com configurações específicas para todos os usuários, configurado com precedência bastante elevada e vinculado ao grupo de segurança Usuários do Domínio. O benefício é haver somente uma interface de gerenciamento de políticas de senha de domínio, e as configurações padrão para contas locais nos membros do domínio podem ser definidas de modo diferente em todo o domínio.

Pergunta: No laboratório, você estava usando precedência para o PSO administrativo com valor 10. Por quê?

Resposta: O PSO administrativo é muito restritivo, portanto, a precedência precisa ser baixa. No entanto, futuramente, poderá haver grupos de administradores com configurações mais restritivas, por exemplo, um subconjunto de administradores para acessar dados de recursos humanos, ou contas de serviço às quais você pode impor senhas mais longas com direitos administrativos que mudem com menos frequência. Por esses motivos, usando o valor 10, haverá espaço para implementar PSOs que sejam mais precisos.

Módulo 8

Implantação e gerenciamento do AD CS

Sumário:

Lição 1

Implantação de ACs

Sumário:

Perguntas e respostas

Pergunta: Quais das opções a seguir descrevem as vantagens de implantar uma AC corporativa em vez de uma AC autônoma?

( ) Fornece várias maneiras pelas quais usuários e dispositivos podem receber certificados.

( ) Não exige o AD DS.

( ) As solicitações de certificado podem ser emitidas ou negadas automaticamente com base na política.

( ) Pode ficar offline para evitar comprometimento.

( ) Pode usar modelos para emitir certificados com base em dados no AD DS.

Resposta:

(√) Fornece várias maneiras pelas quais usuários e dispositivos podem receber certificados.

( ) Não exige o AD DS.

(√) As solicitações de certificado podem ser emitidas ou negadas automaticamente com base na política.

( ) Pode ficar offline para evitar comprometimento.

(√) Pode usar modelos para emitir certificados com base em dados no AD DS.

Comentários:

As vantagens de uma AC corporativa incluem as várias maneiras para se registrar para certificados, incluindo o registro automático usando modelos de certificado. As ACs corporativas também permitem a aprovação ou negação automática de solicitações com base nas políticas de emissão. As ACs corporativas, no entanto, exigem o AD DS (Active Directory Domain Services) e devem ficar online para facilitar o registro de certificado.

Pergunta: Quais das opções a seguir são motivos pelos quais convém implantar várias ACs subordinadas?

( ) Você deseja segmentar a emissão de certificados com base em políticas de uso exclusivas.

( ) Você tem vários domínios no ambiente do AD DS, e cada domínio exige sua própria AC subordinada.

( ) Você deseja segmentar a emissão de certificados com base na divisão organizacional ou na região geográfica.

( ) Você deseja várias ACs subordinadas para alta disponibilidade e balanceamento de carga de solicitações.

( ) Você precisa publicar vários modelos de certificado, e cada modelo exige sua própria AC subordinada.

Resposta:

(√) Você deseja segmentar a emissão de certificados com base em políticas de uso exclusivas.

( ) Você tem vários domínios no ambiente do AD DS, e cada domínio exige sua própria AC subordinada.

(√) Você deseja segmentar a emissão de certificados com base na divisão de organizacional ou na região geográfica.

(√) Você deseja várias ACs subordinadas para alta disponibilidade e balanceamento de carga de solicitações.

( ) Você precisa publicar vários modelos de certificado, e cada modelo exige sua própria AC subordinada.

Comentários:

Você pode implantar várias ACs para políticas de uso exclusivas, divisões organizacionais ou regiões geográficas. Além disso, você pode implantar várias ACs para garantir a alta disponibilidade de balanceamento de carga de solicitações.

Não são necessárias várias ACs subordinadas em um ambiente AD DS de vários domínios, embora você possa usar essa abordagem se seus domínios AD DS já se alinham às regiões geográficas ou divisões organizacionais. Não são necessárias várias ACs subordinadas se você precisar publicar modelos de certificado diferentes porque uma AC pode ser configurada para emitir certificados de mais de um modelo.

Demonstração: Implantação de uma AC raiz corporativa

Etapas da demonstração

1. Em **LON-SVR1**, clique em **Iniciar** e em **Gerenciador de Servidores**.
2. No **Gerenciador do Servidor**, clique em **Adicionar funções e recursos**.
3. 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**, clique em **Próximo**.
6. Na página **Selecionar funções de servidor**, selecione **Serviços de Certificados do Active Directory**.
7. No **Assistente de Adição de Funções e Recursos**, clique em **Adicionar Recursos** e, depois, em **Próximo**.
8. Na página **Selecionar recursos**, clique em **Próximo**.
9. Na página **Serviços de Certificados do Active Directory**, clique em **Próximo**.
10. Na página **Selecionar serviços de função**, verifique se a **Autoridade de Certificação** está selecionada e clique em **Próximo**.
11. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
12. Na página **Progresso da instalação**, após a instalação ser concluída, clique no texto **Configurar Serviços de Certificados do Active Directory** no servidor de destino.
13. No **Assistente de** configuração do AD CS, na **página** Credenciais, clique em **Próximo**.
14. Na página **Serviços de função**, selecione **Autoridade de certificação** e clique em **Próximo**.
15. Na página **Tipo de instalação**, selecione **AC corporativa** e clique em **Próximo**.
16. Na **página** Tipo de Autoridade de Certificação, clique na opção **AC raiz** e clique em **Próximo**.
17. Na página **Chave Privada**, verifique se a opção **Criar uma nova chave privada** está selecionada e clique em **Avançar**.

18. Na página **Criptografia para AC**, mantenha as seleções padrão para **Selecione um provedor criptográfico** e **Selecione o algoritmo de hash para certificados de autenticação emitidos por esta autoridade de certificação**, mas configure o **Comprimento da chave** para **4096** e clique em **Próximo**.
19. Na página **Nome da Autoridade de Certificação**, na caixa de texto **Nome comum da autoridade de certificação**, digite **AdatumRootCA** e clique em **Próximo**.
20. Na página **Período de validade**, clique em **Próximo**.
21. Na página **Banco de dados de AC**, clique em **Próximo**.
22. Na página **Confirmação**, clique em **Configurar**.
23. Na página **Resultados**, clique em **Fechar**.
24. Na página **Progresso da instalação**, clique em **Fechar**.

Lição 2

Administração de ACs

Sumário:

Perguntas e respostas

Pergunta: Qual das opções a seguir é verdadeira sobre a administração baseada em funções da implantação do AD CS?

( ) O AD CS cria automaticamente três funções e grupos internos para Administrador de AC, Gerenciador de certificados e Usuário registrado.

( ) Você pode conceder aos grupos de função do AD CS uma ou mais das seguintes permissões de AC: Gerenciar AC, Emitir e Gerenciar certificados, Ler e Solicitar certificados.

( ) Você pode limitar a permissão de AC para Emitir e gerenciar certificados a um determinado modelo ou conjunto de modelos.

( ) Você pode criar grupos de função do AD CS personalizados com base em necessidades específicas de sua organização.

( ) A Entidade de segurança de usuários autenticados pode se registrar para qualquer certificado que seja publicado em uma AC.

Resposta:

( ) O AD CS cria automaticamente três funções e grupos internos para Administrador de AC, Gerenciador de certificados e Usuário registrado.

(√) Você pode conceder aos grupos de função do AD CS uma ou mais das seguintes permissões de AC: Gerenciar a AC. Emitir e Gerenciar certificados, Ler e Solicitar certificados.

(√) Você pode limitar a permissão de AC Emitir e gerenciar certificados a um determinado modelo ou conjunto de modelos.

(√) Você pode criar grupos de função do AD CS personalizados com base em necessidades específicas de sua organização.

( ) A entidade de segurança Usuários autenticados pode se registrar para qualquer certificado que seja publicado em uma AC.

Comentários:

A Administração baseada em funções no AD CS é um conceito, não um recurso instalado automaticamente. Portanto, você deve criar qualquer função de grupos manualmente. Após criar um grupo de função, você pode atribuir a ele uma ou mais das seguintes permissões de AC: Gerenciar AC, Emitir e gerenciar certificados, Ler e Solicitar certificados. Você pode personalizar as funções de acordo com as necessidades da sua organização, incluindo a restrição da permissão para Emitir e gerenciar certificados para determinado modelo ou conjunto de modelos.
A **Entidade de segurança** de usuários autenticados pode solicitar qualquer certificado, mas o modelo de certificado controla a capacidade de registrar, não a AC.

Pergunta: Qual das opções a seguir é verdadeira sobre as extensões de AIA e CPD de uma AC?

( ) Cada extensão exige, no mínimo, duas URLs válidas e acessíveis para que a validação do certificado funcione corretamente.

( ) Você pode publicar certificados de AC offline e autônoma e CRLs em um ambiente do AD DS manualmente.

( ) A ordem na qual você especifica URLs de AIA e CPD não é tão importante quanto o mecanismo de encadeamento de certificados que ordena automaticamente os locais com base na conexão mais rápida.

( ) Para facilitar a validação de certificados para clientes externos, você deve publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016.

( ) Se você estiver usando uma AC corporativa, a validação de certificados internos funcionará sem nenhuma configuração adicional.

Resposta:

( ) Cada extensão exige, no mínimo, duas URLs válidas e acessíveis para que a validação do certificado funcione corretamente.

(√) Você pode publicar manualmente certificados de AC offline e autônoma e CRLs em um ambiente do AD DS.

( ) A ordem na qual você especifica URLs de CPD e AIA não é tão importante quanto o mecanismode encadeamento de certificados que classifica automaticamente locais com base na conexão mais rápida.

(√) Para facilitar a validação de certificado para clientes externo, você deve publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016.

(√) Se você estiver usando uma AC corporativa, a validação de certificados internos funcionará sem nenhuma configuração adicional.

Comentários:

Para que o certificado de validação funcione, as extensões de CPD e AIA devem conter um mínimo de uma URL válida e acessível. Para ACs offline e autônomas, você pode publicar o certificado e a CRL da AC no AD DS manualmente. A ordem das URLs de AIA e CPD é importante, pois o mecanismo de encadeamento de certificado mecanismo os procura sequencialmente. Você deve colocar as URLs com maior probabilidade de estarem disponíveis na parte superior da ordem de URL. Para facilitar a validação de certificados para clientes externos, você pode publicar URLs de AIA e CPD externas usando HTTP por meio de um Proxy de Aplicativo Web do Windows Server 2016 ou outra solução de proxy reverso de terceiros. Se você estiver usando uma AC corporativa, a validação do certificado trabalhará automaticamente para os clientes internos, mas pode exigir configuração adicional em outros cenários.

Recursos

Gerenciamento de ACs

 **Leitura adicional:** Para obter mais informações, consulte:

- Cmdlets de implantação do AD CS no Windows PowerShell http://aka.ms/Giih2g
- Cmdlets de implantação do AD CS no Windows PowerShell http://aka.ms/Dekm5i

Demonstração: configuração de propriedades de AC

Etapas da demonstração

1. Em **LON-SVR1**, abra o **Gerenciador do Servidor**, clique em **Ferramentas** e depois em **certification authority**.
2. No Console de **autoridade de certificação**, clique com o botão direito do mouse em **AdatumRootCA** e selecione **Propriedades**.
3. Na guia **Geral**, clique em **Exibir certificado**. Quando a janela do certificado abrir, revise os dados nas guias **Detalhes**, **gerais** e **Caminho de certificação** e clique em **OK**.
4. Na guia **Módulo de política**, clique em **Propriedades**. Analise as configurações disponíveis para o **Módulo de** política padrão e clique em **OK**.

5. Na guia **Módulo de saída**, clique em **Propriedades**. Mostre as **Configurações de publicação** disponíveis no Módulo de saída padrão e clique em **OK**.
6. Na guia **Extensões**, analise as opções disponíveis para a extensão de CPD e AIA **na lista suspensa** Selecionar extensão.
7. Na guia **Segurança**, analise as opções disponíveis na lista de controle de acesso (ACL) e as permissões padrão.
8. Na guia **Gerenciadores de certificado**, analise as opções e explique como restringir entidades de segurança para modelos de certificado específicos e clique em **Cancelar**.
9. Feche o console Certsrv.

Lição 3

Solução de problemas e manutenção de ACs

Sumário:

Perguntas e respostas

Pergunta: Qual dos seguintes problemas pode impedir que o registro automático funcione corretamente no AD CS?

( ) O computador que você pretende registrar automaticamente para um certificado está em uma unidade organizacional (UO) do AD DS, onde a herança de políticas está bloqueada.

( ) O usuário que você pretende registrar automaticamente para um certificado está em uma UO do AD DS, onde a configuração de Política de Grupo necessária não está vinculada ou não é herdada.

( ) A AC é autônoma.

( ) O modelo de certificado não é publicado em uma AC.

( ) A URL de AIA está configurada incorretamente na guia de extensões da AC.

Resposta:

(√) O computador que você pretende registrar automaticamente para um certificado está em uma unidade organizacional (UO) do AD DS, onde a herança de políticas está bloqueada.

(√) O usuário que você pretende registrar automaticamente para um certificado está em uma OU do AD DS, onde a configuração de Política de Grupo necessária não está vinculada ou não é herdada.

(√) A AC é autônoma.

(√) O modelo de certificado não é publicado em uma AC.

( ) A URL de AIA está configurada incorretamente na guia de extensões da AC.

Comentários:

A herança do Objeto de Política de Grupo (GPO) é um problema comum que pode impedir o registro automático. Usuários e computadores devem estar em uma organização de AD DS onde você vinculou as configurações de GPO necessárias e a herança de política não bloqueada. Além disso, as ACs devem ser corporativas para funcionarem corretamente, pois os clientes usam o AD DS para determinar ACs e modelos disponíveis. Você deve publicar modelos em uma AC corporativa e o usuário ou computador deve ter as permissões de registro automático configuradas no modelo. Uma URL de AIA ou CPD inválida na AC não impedirá o registro automático, mas pode impedir que o certificado seja validado corretamente ao ser usado por um aplicativo cliente ou serviço.

Pergunta: Qual das opções a seguir é verdadeira sobre a ferramenta PKIVIew?

( ) O PKIView mostra todas as suas ACs corporativas e a integridade atual delas.

( ) Você pode usar o PKIView para adicionar ACs autônomas manualmente.

( ) Você pode usar o PKIView para configurar o registro automático para usuários e computadores.

( ) O PKIView avalia o estado de CPD ou AIA para cada local definido em cada AC.

( ) O PKIView pode avaliar o status do serviço da função Respondente Online do AD CS.

Resposta:

(√) O PKIView mostra todas as suas ACs corporativas e a integridade atual delas.

( ) Você pode usar o PKIView para adicionar ACs autônomas manualmente.

( ) Você pode usar o PKIView para configurar o registro automático para usuários e computadores.

(√) O PKIView avalia o estado de CPD ou AIA para cada local definido em cada AC.

(√) O PKIView pode avaliar o status do serviço da função Respondente Online do AD CS.

Comentários:

Você pode usar o PKIView para ver todas as suas ACs corporativas e a integridade atual delas, mas ele não mostra o status de uma AC autônoma. Você configura o registro automático para usuários e computadores por meio da Política de Grupo, não com a ferramenta PKIView.
O PKIVIew permite avaliar o estado de CPD e AIA para cada local definido em cada AC, além do status do serviço da função Respondente Online do AD CS, caso o tenha implantado.

Revisão do módulo e informações complementares

Práticas recomendadas

- Ao implantar uma infraestrutura de AC, implante uma AC raiz autônoma (não adicionada 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.
- Analise o tempo de validação das listas de certificados revogados (CRLs) da AC raiz.
- Forneça mais de um local para AIA e CRL.

Perguntas de revisão

Pergunta: Por quais motivos uma organização utilizaria uma PKI?

> **Resposta:** Alguns dos motivos para usar uma PKI incluem melhorar a segurança, aumentar o controle de identidade e fazer assinatura digital de código.

Pergunta: Por que você deve implantar módulos personalizados de política e saída?

> **Resposta:** Se você tiver um aplicativo adicional para o gerenciamento de certificado, como o Gerenciamento de certificado MIM, você terá que instalar módulos de política e de saída personalizados para integrar seu aplicativo com a AC.

Ferramentas

- **Console de** autoridade de certificação
- Ferramenta de linha de comando CertUtil
- Windows PowerShell
- PKIView.msc
- Gerenciador do Servidor

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
O local do certificado de AC especificado na extensão de AIA não está 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.	Use o Console de **autoridade de certificação** para configurar a extensão do AIA e incluir o sufixo do nome do certificado em cada local.
AC não está configurada para incluir os locais de CPD 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.	Use o Console da **autoridade de certificação** para configurar a extensão do CPD e para especificar o local de rede da CRL.

Perguntas e respostas da revisão do laboratório

Laboratório: Implantação e configuração de uma hierarquia de AC de duas camadas

Perguntas e respostas

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

Resposta: Por motivos de segurança, AC raiz deve ficar offline e não deve ter qualquer acesso à rede. Como a AC raiz corporativa não pode estar offline, você não pode fornecer máxima proteção para a chave e a identidade dela.

Pergunta: Por quais motivos uma organização usaria uma AC raiz corporativa?

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

Módulo 9

Implantação e gerenciamento de certificados

Sumário:

Lição 1

Implantação e gerenciamento de modelos de certificado

Sumário:

Perguntas e respostas

Pergunta: Quais afirmações a seguir são verdadeiras em relação à versão 2 dos modelos de certificado no AD CS? (Escolha todas as opções aplicáveis.)

( ) Os modelos versão 2 dão suporte ao registro automático.

( ) Você só pode modificar a guia Segurança no modelo versão 2.

( ) Você pode atualizar para o modelo versão 2 duplicando um modelo versão 1.

( ) Apenas o Windows Server 2008, o Windows Vista e sistemas operacionais posteriores dão suporte aos modelos versão 2.

( ) Apenas o Windows Server 2012, o Windows 8 e sistemas operacionais posteriores dão suporte aos modelos versão 2.

Resposta:

(√) Os modelos versão 2 dão suporte ao registro automático.

( ) Você só pode modificar a guia Segurança no modelo versão 2.

(√) Você pode atualizar para o modelo versão 2 duplicando um modelo versão 1.

( ) Apenas Windows Server 2008, Windows Vista e sistemas operacionais superiores oferecem suporte a modelos versão 2.

( ) Apenas Windows Server 2012, Windows 8 e sistemas operacionais superiores oferecem suporte a modelos versão 2.

Comentários:

Um importante aspecto dos modelos versão 2 é que eles dão suporte ao registro automático pelos computadores e usuários do Active Directory Domain Services (AD DS). Ao contrário dos modelos versão 1, você pode modificar todos os aspectos do modelo versão 2. Para atualizar para o modelo versão 2, é possível duplicar um modelo versão 1. Os modelos versão 2 têm suporte no Windows Server 2003 Enterprise Edition, no Windows Server 2008 Enterprise e no Windows Server 2008 R2 e posterior.

Pergunta: Você é o administrador do AD CS na A. Datum Corporation. Vários usuários no seu ambiente do AD DS registraram automaticamente um certificado de usuário. Você deseja diminuir o prazo de validade do certificado de usuário e precisa garantir que os usuários consigam um novo certificado imediatamente sem que haja quebra de validade do certificado existente. Quais das ações a seguir devem ser executadas? (Escolha todas as opções aplicáveis.)

( ) Duplicar o modelo existente e fornecer um novo nome de modelo. Modificar o prazo de validade do novo modelo.

( ) Modificar o prazo de validade do modelo existente.

( ) Modificar as configurações do registro automático do modelo existente.

( ) Revogar todos os certificados de usuário emitidos a partir do modelo existente.

( ) Modificar o novo modelo para que ele substitua o modelo existente. Publicar o novo modelo.

Resposta:

(√) Duplicar o modelo existente e fornecer um novo nome de modelo. Modificar o período de validade do novo modelo.

( ) Modificar o prazo de validade do modelo existente.

( ) Modificar as configurações do registro automático do modelo existente.

(√) Revogar todos os certificados de usuário emitidos a partir do modelo existente.

(√) Modificar o novo modelo para que ele substitua o modelo existente. Publicar o novo modelo.

Comentários:

Nessa situação, você deve duplicar o modelo existente, fornecendo um novo nome do modelo e prazo de validade. Além disso, você deve atualizar o novo modelo para que ele substitua o anterior. Depois de publicar o novo modelo em uma AC corporativa, os usuários que tinham se registrado automaticamente em relação ao modelo anterior vão se registrar automaticamente novamente para o novo modelo. Assim que os novos certificados com prazo de validade correto tiverem substituído os certificados emitidos anteriormente, revogue todos os certificados de usuário do modelo existente para que os usuários não possam utilizá-los.

Se você modificar o prazo de validade do modelo existente, novas inscrições no modelo terão as configurações corretas, mas certificados emitidos anteriormente ainda terão o prazo de validade indesejado. Não é necessário modificar as configurações de registro automático no modelo existente, e isso não alcançaria o efeito desejado.

Demonstração: Modificação e habilitação de um modelo de certificado

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **certification authority**.
2. No console **Autoridade de Certificação**, expanda **AdatumCA**, clique com o botão direito do mouse em **Modelos de Certificado** e clique em **Gerenciar**.
3. Examine a lista de modelos padrão. Examine os modelos e suas propriedades.
4. No painel de detalhes, clique duas vezes em **IPsec**.
5. Na caixa de diálogo **Propriedades IPsec** clique nas guias e observe o que você pode modificar em cada uma. Observe que, na guia **Segurança**, é possível definir as permissões para registro. Clique em **Cancelar** para fechar o modelo.
6. No console **Modelos de Certificado**, no painel de detalhes, clique com o botão direito do mouse no modelo de certificado **Usuário do Exchange** e clique em **Modelo Duplicado**.
7. Na caixa de diálogo **Propriedades do Novo Modelo**, examine as opções na guia **Compatibilidade**.
8. Clique na guia **Geral** e, na caixa de texto **Nome para exibição do modelo** digite **Usuário do Exchange Teste 1**.
9. Clique na guia **Modelos Obsoletos** e clique em **Adicionar**.
10. Clique no modelo **Usuário do Exchange** e clique em **OK**.
11. Clique na guia **Segurança** e em **Usuários Autenticados**.
12. No nó **Permissões para Usuários Autenticados**, marque as caixas de seleção **Permitir** para **Registrar** e **Registrar automaticamente** e clique em **OK**.
13. Feche o **Console de Modelos de Certificado**.
14. No console **Autoridade de Certificação**, clique com o botão direito em **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
15. Na caixa de diálogo **Ativar Modelos de Certificado**, selecione o certificado **Usuário do Exchange Teste 1** e clique em **OK**.

Lição 2

Gerenciamento de implantação, revogação e recuperação de certificados

Sumário:

Perguntas e respostas

Pergunta: Ao revogar um certificado, onde está a impressão digital do certificado publicado?

( ) CPD (ponto de distribuição de CRL)

( ) AIA (acesso às informações da autoridade)

( ) CRL (lista de certificados revogados)

( ) AD DS

( ) O serviço Respondente Online

Resposta:

( ) CPD (ponto de distribuição de CRL)

( ) AIA (acesso às informações da autoridade)

(√) CRL (lista de certificados revogados)

( ) AD DS

( ) O serviço Respondente Online

Comentários:

Quando você revoga um certificado, a impressão digital do certificado é publicada na CRL (lista de certificados revogados). Um CPD (Ponto de distribuição de CRL) é o local da URL onde a CRL está armazenada. O AIA (acesso às informações de autoridade) é a URL onde está localizado o certificado de AC. O AD DS é um local válido para um CPD, mas certificados revogados não publicam diretamente no AD DS. Um serviço Respondente Online valida o status de um certificado específico usando a cópia local da CRL, mas os certificados revogados não publicam diretamente em um serviço Respondente Online.

Pergunta: Quais das ações a seguir você deve realizar para configurar o arquivamento de chave em uma AC do AD CS? (Escolha todas as opções aplicáveis.)

( ) Configurar o modelo de certificado KRA.

( ) Registrar um usuário designado para um certificado KRA.

( ) Publicar a chave pública KRA usando a Política de Grupo.

( ) Configurar um agente de recuperação na AC.

( ) Configurar os modelos de certificado desejados para arquivamento de chave.

Resposta:

(√) Configurar o modelo de certificado KRA.

(√) Registrar um usuário designado para um certificado KRA.

( ) Publicar a chave pública KRA usando a Política de Grupo.

(√) Configurar um agente de recuperação na AC.

(√) Configurar os modelos de certificado desejados para arquivamento de chave.

Comentários:

Para configurar o arquivamento de chave, é necessário:

1. Configurar o certificado KRA para que somente os usuários confiáveis possam se registrar para um certificado.
2. Registrar um usuário confiável para o certificado KRA.
3. Configurar um agente de recuperação na AC usando o certificado KRA.
4. Configurar os modelos de certificado desejados para arquivamento de chave.

Não é necessário publicar a chave pública KRA usando a Política de Grupo.

Demonstração: Configuração da AC para arquivamento de chave

Etapas da demonstração

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Autoridade de Certificação**. No console **Autoridade de Certificação**, expanda o nó **AdatumCA**, clique com o botão direito na pasta **Modelos de Certificado** e clique em **Gerenciar**.
2. No painel de detalhes, clique com o botão direito do mouse no certificado **Agente de Recuperação de Chave** e clique em **Propriedades**.
3. Na caixa de diálogo **Propriedades do Agente de Recuperação de Chave** clique na guia **Requisitos de Emissão** desmarque a caixa de seleção **Aprovação do gerenciador de certificados de autoridade de certificação** e clique na guia **Segurança**. Observe que os grupos **Admins. do Domínio** e **Administradores de Empresa** são os únicos que têm a permissão Registrar. Em seguida, clique em **OK**.
4. Feche o **Console de Modelos de Certificado**.
5. No console **Autoridade de Certificação**, clique com o botão direito em **Modelos de Certificado**, aponte para **Novo** e clique em **Modelo de Certificado a Ser Emitido**.
6. Na caixa de diálogo **Ativar Modelos de Certificado** clique no modelo **Agente de Recuperação de Chave** e clique em **OK**.
7. Clique em **Iniciar** e no ícone **Windows PowerShell**.
8. No prompt de comando do Windows PowerShell, digite **mmc.exe** e pressione Enter.
9. No console **Console1-[Raiz do Console]** clique em **Arquivo** e clique em **Adicionar/Remover Snap-in**.
10. Na caixa de diálogo **Adicionar ou Remover Snap-ins** clique em **Certificados** e em **Adicionar**.
11. Na caixa de diálogo **Snap-in de certificados** selecione **Minha conta de usuário**, clique em **Concluir** e em **OK**.
12. Expanda o nó **Certificados – Usuário Atual**, clique com o botão direito do mouse em **Pessoal**, aponte para **Todas as Tarefas** e clique em **Solicitar Novo Certificado**.
13. No **Assistente de Registro de Certificado**, na página **Antes de Começar**, clique em **Avançar**.
14. Na página **Selecionar política de registro de certificado**, clique em **Avançar**.
15. Na página **Solicitar Certificados**, marque a caixa de seleção **Agente de Recuperação de Chave**, clique em **Registrar** e em **Concluir**.
16. Atualize o console e, em seguida, exiba o KRA no repositório pessoal; isto é, percorra as propriedades de certificado e verifique se o modelo de certificado com a finalidade específica **Agente de Recuperação de Chave** está presente.
17. Feche o **Console1** sem salvar as alterações.
18. Retorne ao console **Autoridade de Certificação** clique com o botão direito do mouse em **AdatumCA** e clique em **Propriedades**.
19. Na caixa de diálogo **Propriedades de AdatumCA** clique na guia **Agentes de Recuperação** e selecione **Arquivar a chave**.
20. Em Certificados do agente de recuperação de chave, clique em **Adicionar**.
21. Na caixa de diálogo **Seleção de Agente de Recuperação de Chave** clique em **Mais Opções** e clique no certificado com a finalidade KRA (provavelmente é o último na lista emitido para o **Administrador**) e clique duas vezes em **OK**.
22. Quando for solicitado a reiniciar a AC, clique em **Sim**.

Lição 3

Uso de certificados em um ambiente de negócios

Sumário:

Perguntas e respostas

Pergunta: Quais destas opções são afirmações verdadeiras sobre o uso de certificados em um ambiente empresarial? (Escolha todas as opções aplicáveis.)

( ) Os certificados podem ser usados para criptografar o tráfego HTTP entre um servidor Web e o navegador.

( ) Os usuários podem usar certificados para assinar digitalmente documentos.

( ) Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo.

( ) Para enviar email criptografado para um destinatário externo que não faz parte da sua PKI interna, você deve usar um certificado de criptografia emitido por uma AC pública.

( ) Arquivos criptografados com EFS só podem ser lidos pela pessoa que os criptografou primeiro.

Resposta:

(√) Os certificados podem ser usados para criptografar o tráfego HTTP entre um servidor Web e o navegador.

(√) Os usuários podem usar certificados para assinar digitalmente documentos.

(√) Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo.

( ) Para enviar email criptografado para um destinatário externo que não faz parte da sua PKI interna, você deve usar um certificado de criptografia que um público da autoridade de certificação emitiu.

( ) Arquivos criptografados com EFS só podem ser lidos pela pessoa que os criptografou primeiro.

Comentários:

Os certificados podem ser usados para criptografar o tráfego HTTP, assinar digitalmente e criptografar documentos e emails, e para autenticação de cliente/servidor. Os documentos assinados digitalmente são inválidos se alguém modifica o conteúdo. Para enviar email criptografado para um destinatário externo, você pode usar um certificado interno ou emitido publicamente, caso tenha acesso à chave pública do destinatário. Os arquivos criptografados usando o EFS podem ser lidos pela pessoa que os criptografou e por usuários explicitamente designados para o compartilhamento do EFS. Se a chave privada de criptografia individual for perdida ou excluída, um agente de recuperação de dados pode acessar o arquivo ou um agente de recuperação de chave pode recuperar a chave privada, se você tiver configurado o arquivamento de chave no modelo de certificado EFS e na AC emissora.

Pergunta: Você é o administrador de AD CS da A. Datum. Você deseja habilitar os usuários do AD DS para realizar assinatura digital e criptografia usando certificados da sua PKI interna. Quais das etapas a seguir são necessárias?

( ) Habilitar um agente de recuperação de chave.

( ) Habilitar um agente de recuperação de dados.

( ) Publicar o modelo de certificado do Usuário e configurar os grupos de usuários desejados para registro automático.

( ) Habilitar EFS nos computadores do domínio AD DS usando a Política de Grupo.

( ) Atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Resposta:

( ) Habilitar um agente de recuperação de chave.

( ) Habilitar um agente de recuperação de dados.

(√) Publicar o modelo de certificado do Usuário e configurar os grupos de usuários desejados para registro automático.

( ) Habilitar EFS nos computadores do domínio AD DS usando a Política de Grupo.

( ) Atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Comentários:

Para habilitar a assinatura digital e a criptografia, só será necessário publicar o modelo de certificado do usuário e configurá-lo para registro automático. Embora o uso de um agente de recuperação de chave e um agente de recuperação de dados sejam práticas recomendadas, elas não são necessárias para habilitar assinaturas digitais e criptografia. Você não precisa habilitar o EFS em computadores de domínio AD DS, nem precisa atualizar todos os computadores do domínio AD DS para o Windows Server 2016 ou Windows 10.

Demonstração: Como assinar digitalmente um documento

Etapas da demonstração

1. Em **LON-CL1**, abra a interface de linha de comando do Windows PowerShell.
2. No prompt de comando do **Windows PowerShell** digite **mmc.exe** e pressione Enter.
3. Na janela **Console1 – [Raiz do Console]**, clique no menu **Arquivo** e selecione **Adicionar/Remover Snap-in**.
4. Selecione **Certificados**, clique em **Adicionar**, selecione **Minha conta de usuário**, clique em **Concluir** e clique em **OK**.
5. Expanda **Certificados - Usuário Atual**, clique com o botão direito do mouse em **Pessoal**, selecione **Todas as Tarefas** e clique em **Solicitar Novo Certificado**.
6. No **Assistente de Registro de Certificado**, clique duas vezes em **Avançar**.
7. Na página **Registro de Certificado** na lista de modelos disponíveis, selecione **Usuário**, clique em **Registrar** e clique em **Concluir**.
8. Feche a janela **Console1 – [Raiz do Console]** sem salvar as alterações.
9. Abra o Word 2016.

 **Observação:** Se o **Assistente para Ativação do Microsoft Office** aparecer, clique em **Fechar**. Clique em **Pergunte–me mais tarde** e clique em **Aceitar**.

10. Em um documento em branco, digite algum texto e, em seguida, salve o arquivo na área de trabalho.
11. Na barra de ferramentas, clique em **Inserir** e, no painel **Texto**, na lista suspensa **Linha de Assinatura**, clique em **Linha de Assinatura do Microsoft Office**.
12. Na janela **Configuração de Assinatura**, digite seu nome na caixa de texto **Signatário sugerido**, digite **Administrador** na caixa de texto **Cargo do signatário sugerido**, digite **Administrator@adatum.com** na caixa de texto **Endereço de email do signatário sugerido** e clique em **OK**.

13. Clique com o botão direito do mouse na linha de assinatura no documento e, em seguida, clique em **Assinar**.
14. Na janela **Assinar**, clique em **Alterar**.
15. Na janela **Segurança do Windows** em **Selecione um certificado**, selecione o certificado de **Administrador** com a data de hoje e clique em **OK**.
16. Na caixa de texto à direita do X, digite seu nome e clique em **Assinar** e em **OK**.

 **Observação:** explique aos alunos que é possível selecionar uma imagem em vez de digitar seu nome. Essa imagem pode ser sua assinatura manual digitalizada.

17. Certifique-se de que você não pode editar mais o documento.
18. Feche o Word 2016 e salve as alterações quando solicitado.
19. Continue conectado para a próxima demonstração.

Demonstração: Criptografia de um arquivo com EFS

Etapas da demonstração

1. Em **LON-CL1**, clique com o botão direito do mouse no documento do Microsoft Word que você salvou na área de trabalho na demonstração anterior e, em seguida, clique em **Propriedades**.
2. Na guia **Geral** da caixa de diálogo **Propriedades**, clique em **Avançado**, clique em **Criptografar o conteúdo para proteger os dados** e clique duas vezes em **OK**.
3. Na janela de prompt, selecione **Criptografar somente o arquivo** e clique em **OK**.
4. Mova o documento que você criptografou para a pasta **C:\Users\Public\Public Documents**.
5. Saia de **LON-CL1**.
6. Entre com o **Adatum\Aidan** com a senha **Pa55w.rd**.
7. Abra o Explorador de Arquivos e acesse **C:\Users\Public\Public Documents**.
8. Tente abrir o documento criptografado.
9. Verifique se não é possível abrir o documento.
10. Saia de **LON-CL1**.

Lição 4

Implementação e gerenciamento de cartões inteligentes

Sumário:

Perguntas e respostas

Pergunta: Qual destas afirmações é verdadeira sobre cartões inteligentes?

( ) Os cartões inteligentes são uma opção para a autenticação multifator.

( ) Você não pode usar cartões inteligentes para fazer logon interativo.

( ) Os cartões inteligentes contêm um certificado e uma chave privada que você pode acessar apenas usando um PIN.

( ) Os cartões inteligentes fornecem segurança aprimorada, além de uma senha.

( ) É possível usar os cartões inteligentes somente para assinatura digital e criptografia.

Resposta:

(√) Os cartões inteligentes são uma opção para a autenticação multifator.

( ) Você não pode usar cartões inteligentes para fazer logon interativo.

(√) Os cartões inteligentes contêm um certificado e uma chave privada que você pode acessar apenas usando um PIN.

(√) Os cartões inteligentes fornecem segurança aprimorada, além de uma senha.

( ) É possível usar os cartões inteligentes somente para assinatura digital e criptografia.

Comentários:

Os cartões inteligentes são uma opção para a autenticação multifator: os usuários devem ter a posse física do cartão inteligente e também devem saber seu PIN. Inserindo o PIN, os certificados e as chaves privadas armazenadas no cartão inteligente se tornam disponíveis para autenticação, assinatura digital e criptografia. O uso de cartões inteligentes para fazer logon interativo fornece segurança aprimorada, além da senha.

Pergunta: Ao implementar uma infraestrutura de cartão inteligente, qual dos seguintes processos deve fazer parte da sua estrutura de gerenciamento de certificados?

( ) Emissão

( ) Revogação

( ) Renovação

( ) Bloqueio e desbloqueio

( ) Suspensão

Resposta:

(√) Emissão

(√) Revogação

(√) Renovação

(√) Bloqueio e desbloqueio

(√) Suspensão

Comentários:

Todas as opções acima são processos corretos que você deve incluir no seu plan o de gerenciamento de certificados. É possível executar alguns dos processos com ferramentas internas. No entanto, devido à complexidade envolvida, é recomendável que você implemente uma solução dedicada para o gerenciamento de certificados e cartões inteligentes, com o a MIM.

Revisão do módulo e informações complementares

Práticas recomendadas

- Ao substituir os modelos de certificado antigos, use os modelos substitutos.
- Sempre arquive certificados que servem para criptografia.
- Use o registro automático para implantação em mass a de certificados.
- Se você estiver usando cartões inteligentes, certifique-se de que os usuários alterem seus PINs regularmente.
- Se você estiver usando cartões inteligentes, implemente uma solução de gerenciamento de cartão inteligente.

Perguntas de revisão

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 deve configurar as opções da Política de Grupo. Além disso, você deve habilitar o registro automático nos modelos de certificado desejados e deve configurar os Objetos de Política de Grupo.

Pergunta: Como os cartões virtuais funcionam?

> **Resposta:** Os Cartões inteligentes virtuais emulam a funcionalidade dos cartões inteligentes tradicionais, mas em vez de exigirem a compra de hardware adicional, eles utilizam uma tecnologia que os usuários já possuem.

Problemas e cenários reais

A Contoso, Ltd. deseja implantar uma PKI para dar suporte e proteger vários serviços. Foi decidido usar o AD CS do Windows Server 2016 como uma plataforma para PKI. A Contoso usará certificados principalmente para EFS, assinatura digital e servidores Web. Como os documentos 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. Considere as seguintes perguntas:

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

Ferramentas

- O console **Autoridade de Certificação**
- O Console de **Modelos de Certificado**
- O console **Certificados**
- **Certutil.exe**

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
O modelo de certificado não é visível durante o registro.	Verifique se você configurou corretamente as permissões Leitura e Registro no modelo.
O registro automático não funciona.	Verifique se você configurou as opções de registro automático na Política de Grupo e se atribuiu as permissões de Ler, Registar e Registrar automaticamente ao grupo apropriado de computadores ou de usuários.
O usuário que criptografou um arquivo não pode descriptografá-lo.	Verifique se o usuário possui a chave privada do par de chaves. Além disso, verifique se o certificado não expirou. Se a chave privada foi perdida ou o certificado expirou, use KRA ou DRA.

Perguntas e respostas da revisão do laboratório

Laboratório: Implantação e uso de certificados

Perguntas e respostas

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

Resposta: Para recuperar chaves privadas, você deve configurar a AC para arquivar chaves privadas de modelos específicos e emitir o certificado KRA.

Pergunta: Qual é o benefício de usar um Agente de registro restrito?

Resposta: O agente de registro permite que você limite as permissões de usuários designados com o agentes de registro para que se registrem em certificados de cartão inteligente em nome de outros usuários.

Módulo 10

Implementação e administração do AD FS

Sumário:

Lição 1

Visão geral do AD FS

Sumário:

Perguntas e respostas

Pergunta: Uma relação de confiança federada é igual a uma relação de confiança da floresta que as organizações podem configurar entre florestas do AD DS.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

Uma relação de confiança federada não é igual a uma relação de confiança da floresta que as organizações podem configurar entre florestas do AD DS. Em uma relação de confiança federada, os servidores AD FS em duas organizações nunca precisam se comunicar diretamente um com o outro. Além disso, toda a comunicação em uma implantação de federação ocorre por HTTPS, de modo que você não precisa abrir várias portas em algum firewall para permitir a federação.

Lição 2

Requisitos e planejamento do AD FS

Sumário:

Perguntas e respostas

Pergunta: No Windows Server 2016, a funcionalidade do proxy do servidor de federação faz parte da função Proxy de Aplicativo Web.

( ) Verdadeiro

( ) Falso

Resposta:

(√) Verdadeiro

( ) Falso

Comentários:

O proxy do servidor de federação é um componente opcional que você normalmente implanta em uma rede de perímetro. Ele não adiciona funcionalidade à implantação do AD FS, mas fornece uma camada de aprimoramento de segurança para conexões da Internet com o servidor de federação. No Windows Server 2016, a funcionalidade do proxy do servidor de federação faz parte do Proxy de Aplicativo Web.

Demonstração: Instalação da função de servidor AD FS

Etapas da demonstração

Instalar o AD FS

1. Em **LON-DC1**, clique em Iniciar, clique com o botão direito do mouse em **Windows PowerShell** e, depois, clique em **Executar como Administrador**.
2. No prompt de comando, digite o seguinte comando e pressione Enter:

   ```
   Add-KdsRootKey –EffectiveTime ((Get-Date).AddHours (-10))
   ```

   Esse comando cria a chave raiz do Serviço de Distribuição de Chave de Grupo da Microsoft para gerar as senhas gMSA (Conta de Serviço Gerenciado do grupo) para a conta que será usada posteriormente neste laboratório. Você deve receber um GUID (identificador global exclusivo) como uma resposta a esse comando.
3. Na **LON-DC1**, no Gerenciador do Servidor, clique em **Gerenciar** e em **Adicionar Funções e Recursos**.
4. No **Assistente de Adição de Funções e Recursos**, na página **Antes de começar,** clique em **Próximo**.
5. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e em **Próximo**.
6. Na página **Selecionar servidor de destino**, clique em **LON-DC1.Adatum.com** e em **Próximo**.
7. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Serviços de Federação do Active Directory (AD FS)** e clique em **Próximo**.
8. Na página **Selecionar recursos**, clique em **Próximo**.
9. Na página **Serviços de Federação do Active Directory (AD FS)**, clique em **Próximo**.
10. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
11. Aguarde a instalação ser concluída e clique em **Fechar**.

Adicionar um registro DNS para o AD FS

1. Em **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **DNS**.
2. No Gerenciador DNS, expanda **LON-DC1**, expanda **Zonas de Pesquisa Direta** e clique em **Adatum.com**.
3. Clique com o botão direito do mouse em **Adatum.com** e clique em **Novo Host (A ou AAAA)**.
4. Na janela **Novo Host**, na caixa **Nome**, digite **adfs**.
5. Na caixa **Endereço IP**, digite **172.16.0.10** e clique em **Adicionar Host**.
6. Na janela **DNS**, clique em **OK** e em **Concluído**.
7. Feche o Gerenciador DNS.

Configurar o AD FS

1. Na **LON-DC1**, no Gerenciador do Servidor, clique no ícone **Notificações** e clique em **Configure o serviço de federação neste servidor**.
2. No **Assistente de Configuração dos Serviços de Federação do Active Directory**, na página **Bem-vindo**, clique em **Criar o primeiro servidor de federação em um farm de servidores de federação** e em **Próximo**.
3. Na página **Conectar ao Active Directory Domain Services**, clique em **Próximo** para usar **Adatum\Administrador** para realizar a configuração.
4. Na página **Especificar Propriedades do Serviço**, na caixa de diálogo **Certificado SSL**, selecione **adfs.adatum.com**.
5. Na caixa **Nome para Exibição do Serviço de Federação**, digite **A. Datum Corporation** e clique em **Próximo**.
6. Na página **Especificar Conta de Serviço**, clique em **Criar uma Conta de Serviço Gerenciado de Grupo**.
7. Na caixa **Nome da Conta**, digite **ADFSService** e clique em **Próximo**.
8. Na página **Especificar Banco de Dados de Configuração**, clique em **Crie um banco de dados neste servidor que utiliza o Banco de Dados Interno do Windows** e em **Próximo**.
9. Na página **Examinar Opções**, clique em **Próximo**.
10. Na página **Verificações de Pré-requisitos**, clique em **Configurar**.
11. Na página **Resultados**, clique em **Fechar**.

Lição 3

Implantação e configuração do AD FS

Sumário:

Perguntas e respostas

Pergunta: O que são regras de declaração? Qual é a finalidade das regras de declaração?

Resposta: As regras de declaração definem como os servidores AD FS enviam e consomem declarações. As regras de declaração definem a lógica de negócios aplicada às declarações fornecidas pelos provedores de declarações e aceitas pelas terceiras partes confiáveis. Você pode usar as regras de declaração para:

- Definir quais declarações de entrada são aceitas de um ou mais provedores de declarações.
- Definir quais declarações de saída são fornecidas a uma ou mais terceiras partes confiáveis.
- Aplicar regras de autorização a fim de permitir o acesso a uma terceira parte confiável específica de um ou mais usuários ou grupos de usuários.

Recursos

Como funciona a descoberta de realm inicial

 **Leitura adicional:** Para saber mais sobre *RelayState*, consulte "Como oferecer suporte a RelayState iniciado pelo provedor de identidade" em: http://aka.ms/Df8hqs

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

Etapas da demonstração

Configurar uma relação de confiança do provedor de declarações

1. Na **LON-DC1**, no Gerenciador do Servidor, clique em **Ferramentas** e em **Gerenciamento do AD FS**.
2. No console de gerenciamento do **AD FS**, clique em **Confiança do Provedor de Declarações**.
3. Clique com o botão direito do mouse em **Active Directory** e clique em **Editar Regras de Declaração**.
4. Na janela **Editar Regras de Declaração para Active Directory**, na guia **Regras de Transformação de Aceitação**, clique em **Adicionar Regra**.
5. No **Assistente para Adicionar Regra de Declaração de Transformação**, na página **Selecionar Modelo de Regra**, na lista **Modelo de regra de declaração**, clique em **Enviar Atributos LDAP como Declarações** e em **Avançar**.
6. Na página **Configurar Regra**, na caixa **Nome da regra de declaração**, digite **Regra de Atributos LDAP de Saída**.
7. Na lista **Repositório de atributos**, clique em **Active Directory**.
8. 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**:
   - Endereços de Email: **Endereço de Email**
   - Nome Principal do Usuário: **UPN**
9. Clique em **Concluir** e em **OK**.

Configurar um aplicativo WIF (Windows Identity Foundation) para AD FS

1. Na **LON-SVR1**, abra o Gerenciador do Servidor, clique em **Ferramentas** e em **Windows Identity Foundation federation utility**.
2. Na página **Bem-vindo ao Assistente do Utilitário de Federação**, na caixa **Local de configuração do aplicativo**, digite **C:\inetpub\wwwroot\AdatumTestApp\web.config** para o local do arquivo **Web.config** de exemplo.
3. Na caixa **URI do Aplicativo**, digite **https://lon-svr1.adatum.com/AdatumTestApp/** de modo a indicar o caminho para o aplicativo de exemplo que confiará nas declarações de entrada do servidor de federação e clique em **Avançar**.
4. Na página **Serviço de Token de Segurança**, clique em **Usar um STS existente** e, na caixa **Local do documento de metadados da Web Services Federation do STS**, digite **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**. Clique em **Avançar**.
5. Na página **STS signing certificate chain validation error**, clique em **Disable certificate chain validation** e clique em **Avançar**.
6. Na página **Security token encryption**, clique em **No encryption** e em **Avançar**.
7. Na página **Offered claims**, 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 do Utilitário de Federação**, percorra os itens para entender a função de cada um e clique em **Concluir**.
9. Na janela **Êxito**, clique em **OK**.

Configurar um objeto de confiança de terceira parte confiável

1. Na **LON-DC1**, no prompt de comando do **Windows PowerShell**, digite o seguinte comando para adicionar um objeto de confiança de terceira parte confiável e pressione Enter:

```
Add-ADFSRelyingPartyTrust –Name ‘A. Datum Corporation Test App’ –MetadataURL ‘https:
//lon-svr1.adatum.com/AdatumTestApp/federationmetadata/2007-06/federationmetadata.xml’
```

2. No console de gerenciamento do **AD FS**, na lista de **Confianças da Terceira Parte Confiável**, clique em **Aplicativo de Teste da A. Datum Corporation** e selecione **Editar Política de Emissão de Declaração**.
3. Na janela **Editar Política de Emissão de Declaração para Aplicativo de Teste da A. Datum Corporation**, na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
4. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
5. Na caixa **Nome da regra de declaração**, digite **Passar nome da conta do Windows**.
6. Na lista **Tipo de declaração de entrada**, clique em **Nome de conta do Windows** e em **Concluir**.
7. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
8. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
9. Na caixa **Nome da regra de declaração**, digite **Passar Endereço de Email**.
10. Na lista **Tipo de declaração de entrada**, clique em **Endereço de Email** e em **Concluir**.
11. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.

12. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
13. Na caixa **Nome da regra de declaração**, digite **Passar UPN**.
14. Na lista **Tipo de declaração de entrada**, clique em **UPN** e em **Concluir**.
15. Na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
16. Na caixa de diálogo **Modelo de regra de declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
17. Na caixa **Nome da regra de declaração**, digite **Passar Nome**.
18. Na lista **Tipo de declaração de entrada**, clique em **Nome** e em **Concluir**.
19. Na guia **Regras de Transformação de Emissão**, clique em **OK**.

Demonstração: Configuração das regras de declarações

Etapas da demonstração

1. Na **LON-DC1**, no Gerenciador do AD FS, selecione **Confianças da Terceira Parte Confiável**, clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Emissão de Declaração**.
2. Na janela **Editar Política de Emissão de Declaração para Aplicativo A. Datum Corporation Test App**, na guia **Regras de Transformação de Emissão**, clique em **Adicionar Regra**.
3. Na caixa de diálogo **Modelo de Regra de Declaração**, selecione **Passar ou Filtrar uma Declaração de Entrada** e clique em **Avançar**.
4. Na caixa **Nome da regra de declaração**, digite **Regra de Envio de Nome de Grupo**.
5. Na lista **Tipo de declaração de entrada**, clique em **Grupo** e em **Concluir**.
6. Clique em **OK**.
7. Clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Controle de Acesso**
8. Na janela **Editar Política de Controle de Acesso para Aplicativo de Teste da A. Datum Corporation**, na guia **Política de controle de acesso**, clique na regra **Permitir um grupo específico**.
9. Em **Política**, clique no link **<parâmetro>**.
10. Clique em **Adicionar** e, na caixa **Selecionar Grupos**, digite **Pesquisa** e clique em **OK**. Clique em **OK** novamente para fechar a caixa **Selecionar Grupos**.
11. Clique em **OK** para fechar a caixa de diálogo **Política de Controle de Acesso**.
12. Clique com o botão direito do mouse em **Aplicativo de Teste da A. Datum Corporation** e clique em **Editar Política de Emissão de Declaração**.
13. Na guia **Regras de Transformação de Emissão**, clique em **Passar UPN** e em **Editar Regra**.
14. Na lista **Tipo de declaração de entrada**, verifique se **UPN** está selecionado.
15. Selecione **Passar apenas um valor de declaração específico**.
16. Na caixa **Valor da declaração de entrada**, digite **@adatum.com**.
17. Clique em **Exibir Idioma da Regra**.
18. Clique em **OK** e em **OK** novamente.
19. Na janela **Editar Política de Emissão de Declaração para Aplicativo de Teste da A. Datum Corporation**, clique em **OK**.

Lição 4

Visão geral do Proxy de Aplicativo Web

Sumário:

Perguntas e respostas

Pergunta: Qual das seguintes afirmações sobre a configuração do Proxy de Aplicativo Web é verdadeira? (Escolha todas as opções aplicáveis.)

( ) Para instalar o Proxy de Aplicativo Web, primeiramente, você deve implementar o AD FS na sua organização.

( ) Para instalar o Proxy de Aplicativo Web, você não precisa implementar o AD FS na sua organização.

( ) Para cada aplicativo que você publica, é preciso configurar uma URL externa e uma URL de servidor interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL externa.

Resposta:

(√) Para instalar o Proxy de Aplicativo Web, primeiramente, você deve implementar o AD FS na sua organização.

( ) Para instalar o Proxy de Aplicativo Web, você não precisa implementar o AD FS na sua organização.

(√) Para cada aplicativo que você publica, é preciso configurar uma URL externa e uma URL de servidor interna.

( ) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL interna.

(√) Ao definir a URL externa, você também deve selecionar um certificado que contenha o nome do host na URL externa.

Comentários:

A Opção 4 está incorreta. O certificado deve conter o nome do host da URL externa.

A Opção 2 está incorreta. Para instalar o Proxy de Aplicativo Web, você já deve ter o AD FS instalado.

Recursos

Cenários de uso do Proxy de Aplicativo Web

Leitura adicional: para obter mais informações sobre como configurar um site para usar IWA e delegação restrita de Kerberos, consulte "Configurar um site para usar a autenticação integrada do Windows" em: http://aka.ms/Nbsbll

Leitura adicional: para obter mais informações sobre como configurar a autenticação Kerberos para servidores Exchange com carga balanceada, consulte "Configurando a autenticação Kerberos para servidores de Acesso para Cliente com carga balanceada" em: http://aka.ms/Nd2avi

Leitura adicional: para obter mais informações sobre como publicar o Gateway de Área de Trabalho Remota por meio do Proxy de Aplicativo Web, consulte Publicando aplicativos com SharePoint, Exchange e RDG: http://aka.ms/C7f0wn

Demonstração: Instalação e configuração do Proxy de Aplicativo Web

Etapas da demonstração

Instalar o Proxy de Aplicativo Web

1. Na **LON-SVR2**, abra o Gerenciador do Servidor, clique em **Gerenciar** e 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 **Instalação baseada em função ou recurso** e em **Próximo**.
4. Na página **Selecionar servidor de destino**, clique em **LON-SVR2.Adatum.com** e em **Próximo**.
5. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Acesso Remoto** e clique em **Próximo**.
6. Na página **Selecionar recursos**, clique em **Próximo**.
7. Na página **Acesso Remoto**, clique em **Próximo**.
8. Na página **Selecionar serviços de função**, selecione **Proxy de Aplicativo Web**.
9. No **Assistente de Adição de Funções e Recursos**, clique em **Adicionar Recursos**.
10. Na página **Selecionar serviços de função**, clique em **Próximo**.
11. Na página **Confirmar seleções de instalação**, clique em **Instalar**.
12. Na página **Progresso da instalação**, clique em **Fechar**.

Exportar o certificado adfs.adatum.com da LON-DC1

1. Na Tela inicial da **LON-DC1**, digite **mmc** e pressione Enter.
2. No **Console1 – [Raiz do Console]**, clique em **Arquivo** e em **Adicionar/Remover Snap-in**.
3. Na janela **Adicionar ou Remover Snap-ins**, na coluna **Snap-ins disponíveis**, clique duas vezes em **Certificados**.
4. Na janela **Snap-in de certificados**, clique em **Conta de computador** e em **Próximo**.
5. Na janela **Selecionar Computador**, clique em **Computador Local (o computador em que este console está em execução)** e em **Concluir**.
6. Na janela **Adicionar ou Remover Snap-ins**, clique em **OK**.
7. No **Console1 – [Raiz do Console]**, expanda **Certificados (Computador Local)**, expanda **Pessoal** e clique em **Certificados**.
8. Clique com o botão direito do mouse em **adfs.adatum.com**, aponte para **Todas as Tarefas** e clique em **Exportar**.
9. No **Assistente para Exportação de Certificados**, clique em **Próximo**.
10. Na página **Exportar Chave Privada**, clique em **Sim, exportar a chave privada** e clique em **Próximo**.
11. Na página **Formato do Arquivo de Exportação**, clique em **Próximo**.
12. Na página **Segurança**, marque a caixa de seleção **Senha**.
13. Nas caixas **Senha** e **Confirmar senha**, digite **Pa55w.rd** e clique em **Próximo**.
14. Na página **Arquivo a Ser Exportado**, na caixa **Nome do arquivo**, digite **C:\adfs.pfx** e clique em **Próximo**.

15. Na página **Concluindo o Assistente para Exportação de Certificados**, clique em **Concluir** e em **OK** para fechar a mensagem de êxito.
16. Feche o **Console1 – [Raiz do Console]** e não salve as alterações.

Importar o certificado adfs.adatum.com na LON-SVR2

1. Na Tela inicial da **LON-SVR2**, digite **mmc** e pressione Enter.
2. No **Console1 – [Raiz do Console]**, clique em **Arquivo** e em **Adicionar/Remover Snap-in**.
3. Na janela **Adicionar ou Remover Snap-ins**, na coluna **Snap-ins disponíveis**, clique duas vezes em **Certificados**.
4. Na janela **Snap-in de certificados**, clique em **Conta de computador** e em **Avançar**.
5. Na janela **Selecionar Computador**, clique em **Computador Local (o computador em que este console está em execução)** e em **Concluir**.
6. Na janela **Adicionar ou Remover Snap-ins**, clique em **OK**.
7. No **Console1 – [Raiz do Console]**, expanda **Certificados (Computador Local)** e clique em **Pessoal**.
8. Clique com o botão direito do mouse em **Pessoal**, aponte para **Todas as Tarefas** e clique em **Importar**.
9. No **Assistente para Importação de Certificados**, clique em **Próximo**.
10. Na página **Arquivo a Ser Importado**, na caixa **Nome do arquivo**, digite **\\LON-DC1\c$\adfs.pfx** e clique em **Próximo**.
11. Na página **Proteção de chave privada**, na caixa **Senha**, digite **Pa55w.rd**.
12. Marque a caixa de seleção **Marcar esta chave como exportável. Isso possibilitará o backup ou o transporte das chaves posteriormente** e clique em **Próximo**.
13. Na página **Repositório de Certificados**, clique em **Colocar todos os certificados no repositório a seguir**.
14. Na caixa **Repositório de certificados**, selecione **Pessoal** e clique em **Próximo**.
15. Na página **Concluindo o Assistente para Importação de Certificados**, clique em **Concluir**.
16. Clique em **OK** para limpar a mensagem de êxito.
17. Feche o **Console1 – [Raiz do Console]** e não salve as alterações.

Configurar o Proxy de Aplicativo Web

1. Na **LON-SVR2**, no Gerenciador do Servidor, clique no ícone **Notificações** e em **Abrir o Assistente de Proxy do Aplicativo Web**.
2. No **Assistente de Configuração do Proxy de Aplicativo Web**, na página **Bem-vindo**, clique em **Próximo**.
3. Na página **Servidor de Federação**, digite as seguintes informações e clique em **Próximo**:
   - Nome do serviço de federação: **adfs.adatum.com**
   - Nome de usuário: **Adatum\Administrador**
   - Senha: **Pa55w.rd**
4. Na página **Certificado de Proxy do AD FS**, na caixa de diálogo **Selecione um certificado a ser usado pelo proxy do AD FS**, selecione **adfs.adatum.com** e clique em **Próximo**.
5. Na página **Confirmação**, clique em **Configurar**.
6. Na página **Resultados**, clique em **Fechar**.

Revisão do módulo e informações complementares

Prática recomendada

Nas versões anteriores do AD FS, era comum usar o SCW (Assistente de Configuração de Segurança) para aplicar práticas recomendadas de segurança específicas do AD FS aos servidores de federação e aos computadores do proxy do servidor de federação. No Windows Server 2016, o SCW foi removido porque os recursos tiveram a segurança aprimorada por padrão. Consequentemente, se precisar controlar as configurações de segurança específicas, você poderá usar a Política de Grupo ou o Gerenciador de Conformidade de Segurança da Microsoft (acesse http://aka.ms/Ncq8jm).

Perguntas de revisão

Pergunta: Sua organização está planejando implementar o AD FS. No curto prazo, somente clientes internos usarão o AD FS para acessar os aplicativos internos. No entanto, posteriormente, você deverá fornecer aos usuários domésticos acesso aos aplicativos baseados na Web que tiveram a segurança aprimorada pelo AD FS. Quantos certificados você deve obter de uma autoridade de certificação de terceiros?

> **Resposta:** Você precisa apenas de um certificado de uma autoridade de certificação de terceiros, pois o único certificado do AD FS que precisa ser confiável é o certificado de comunicação de serviço. Você pode deixar os certificados de autenticação de tokens e de descriptografia do token como autoassinados.

Pergunta: Sua organização implementou com êxito um único servidor AD FS e um único Proxy de Aplicativo Web. Inicialmente, o AD FS era usado apenas para um único aplicativo, mas agora ele é usado para vários aplicativos essenciais aos negócios. O AD FS deve ser configurado para ser altamente disponível.

Durante a instalação do AD FS, você escolheu usar o WID. Você pode usar esse banco de dados em uma configuração altamente disponível?

> **Resposta:** Sim, é possível usar o WID (Banco de Dados Interno do Windows) para dar suporte a até cinco servidores AD FS. O primeiro servidor AD FS é o servidor principal, onde todas as alterações da configuração ocorrem. As alterações no servidor principal são replicadas nos outros servidores AD FS.

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação do AD FS

Perguntas e respostas

Pergunta: Por que configurar adfs.adatum.com para uso como um nome de host é importante para o serviço AD FS?

Resposta: Se você usar o nome do host de um servidor existente para o servidor AD FS, não será possível adicionar mais servidores ao seu farm de servidores. Todos os servidores no farm de servidores devem compartilhar o mesmo nome de host ao fornecer serviços AD FS. Os servidores proxy do AD FS também usam o nome do host para AD FS.

Pergunta: Como você pode verificar se o AD FS está funcionando corretamente?

Resposta: Se você puder acessar **https://hostname/federationmetadata/2007-06/federationmetadata.xml** com êxito no servidor AD FS, isso significa que o AD FS está funcionando corretamente.

Módulo 11

Implementação e administração do AD RMS

Sumário:

Lição 1

Visão geral do AD RMS

Sumário:

Perguntas e respostas

Pergunta: Quando um usuário recebe um RAC?

Resposta: Um RAC é emitido na primeira vez que o usuário tenta acessar o conteúdo protegido pelo AD RMS ou executar uma tarefa do AD RMS, como criar um documento protegido.

Pergunta: O Azure RMS é implantado localmente em um servidor.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

O Azure RMS é um serviço baseado na nuvem; você não precisa implantá-lo localmente.

Recursos

O que é o Azure RMS?

Links de referência: para baixar o aplicativo RMS sharing gratuito da Microsoft, acesse: http://aka.ms/v1s1xd

Comparação do AD RMS, do Azure RMS e do Azure RMS para Office 365

Leitura adicional: para obter mais informações, consulte Comparando o Azure Rights Management e o AD RMS: http://aka.ms/sndlw0

Lição 2

Implantação e gerenciamento de uma infraestrutura do AD RMS

Sumário:

Perguntas e respostas

Pergunta: Para implementar um cluster do AD RMS, quais componentes são necessários?

( ) Office

( ) Uma conta de serviço

( ) Um banco de dados

( ) AD FS

( ) Um certificado SSL

Resposta:

( ) Office

(√) Uma conta de serviço

(√) Um banco de dados

( ) AD FS

( ) Um certificado SSL

Comentários:

É necessário ter uma conta de serviço criada para implementar o AD RMS; você precisa também ter um banco de dados disponível, como WID ou banco de dados do SQL Server.

Pergunta: Quando você decidir remover o cluster do AD RMS do AD DS, o que deverá fazer primeiro?

Resposta: Antes de remover um servidor AD RMS, você deve desativá-lo.

Recursos

Monitoramento do AD RMS

Leitura adicional: para obter mais informações sobre como monitorar cenários: http://aka.ms/Pyumg7

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

Etapas da demonstração

Configurar uma conta de serviço

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e 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**, na caixa **Nome**, digite **Contas de Serviço**, clique em **OK**, clique com o botão direito do mouse na UO (unidade organizacional) **Contas de serviço**, aponte para **Novo** e clique em **Usuário**.

4. Na caixa de diálogo **Criar Usuário**, forneça os detalhes a seguir e clique em **OK**:
   - Nome: **ADRMSSVC**
   - Logon UPN do usuário: **ADRMSSVC**
   - **Logon SamAccountName do usuário**: **Adatum\ADRMSSVC**
   - Senha: **Pa55w.rd**
   - Confirmar Senha: **Pa55w.rd**
   - A senha nunca expira: **Habilitado** (você deve clicar em **Outras opções de senha** para selecionar isso)
   - O usuário não pode alterar a senha: **Habilitado**

Preparar o DNS (Sistema de Nomes de Domínio)

1. No **Gerenciador do Servidor**, clique em **Ferramentas** e clique em **DNS**.
2. No console do **Gerenciador DNS**, expanda **LON-DC1** e expanda **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**:
   - Nome: **adrms**
   - Endereço IP: **172.16.0.21**

   Clique em **OK** e em **Concluído**.
5. Feche o console do **Gerenciador DNS**.

Instalar a função AD RMS

1. Entre em **LON-SVR1** como **Adatum\Administrador** usando a senha **Pa55w.rd**.
2. Clique em Iniciar e em **Gerenciador do Servidor**.
3. No **Gerenciador do Servidor**, clique em **Gerenciar** e em **Adicionar Funções e Recursos**.
4. No **Assistente de Adição de Funções e Recursos**, clique em **Avançar** três vezes.
5. Na página **Selecionar Funções do Servidor**, clique em **Active Directory Rights Management Services**.
6. Na caixa de diálogo **Assistente de Adição de Funções e Recursos**, clique em **Adicionar Recursos**, clique em **Avançar** quatro vezes, clique em **Instalar** e, por fim, clique em **Fechar**.

Configurar o AD RMS

1. Em **LON-SVR1**, 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 Detalhes e Notificações da Tarefa do Servidor**, clique em **Executar configuração adicional**.
4. Na página **AD RMS**, na caixa de diálogo **Configuração do AD RMS: LON-SVR1.adatum.com**, clique em **Próximo**.
5. Na página **Cluster do AD RMS**, clique em **Criar um novo cluster raiz do AD RMS** 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**, digite os detalhes a seguir, clique em **OK** e clique em **Próximo**:
   - Nome de usuário: **ADRMSSVC**
   - Senha: **Pa55w.rd**
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 **Pa55w.rd** duas vezes e clique em **Próximo**.
12. Na página **Site do Cluster**, verifique se **Site Padrão** está selecionado e clique em **Próximo**.
13. Na página **Endereço do Cluster**, forneça as informações a seguir e clique em **Próximo**:
    - Tipo de Conexão: **Usar uma conexão descriptografada (http://)**
    - Nome de Domínio Totalmente Qualificado: **adrms.adatum.com**
    - Porta: **80**
14. Na página **Certificado de Licenciante**, digite **AdatumADRMS** e clique em **Próximo**.
15. Na página **Registro de SCP**, clique em **Registrar o SCP agora** e clique em **Próximo**.
16. Na página **Confirmação**, clique em **Instalar** e, depois que a instalação for concluída, clique em **Fechar**.
17. No menu Iniciar, clique em **Administrador** e clique em **Sair**.

Observação: você deve sair para que possa gerenciar o AD RMS.

Lição 3

Configuração da proteção de conteúdo do AD RMS

Sumário:

Perguntas e respostas

Pergunta: Que tipos de permissões um grupo Superusuários possui?

> **Resposta:** Os membros do grupo Superusuários recebem plenos direitos de proprietário em todas as licenças de uso emitidas pelo cluster do AD RMS no qual o grupo Superusuários está configurado.

Recursos

O que são políticas de exclusão?

 **Leitura adicional:** para obter mais informações sobre como habilitar políticas de exclusão: http://aka.ms/Lnwbcr

Demonstração: Criação de um modelo de política de direitos

Etapas da demonstração

1. Em **LON-SVR1**, abra o **Gerenciador do Servidor**, clique em **Ferramentas** e clique em **Active Directory Rights Management Services**.
2. No console do **AD RMS**, 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**, forneça as informações a seguir, clique em **Adicionar** e, em seguida, clique em **Avançar**:
   - Idioma: **English (United States)**
   - Nome: **ReadOnly**
   - 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 **executives@adatum.com** e clique em **OK**.
8. Quando **executives@adatum.com** estiver selecionado, em **Direitos de executives@adatum.com**, clique em **Exibir**. Verifique se a opção **Conceder ao proprietário (autor) o direito ininterrupto de controle total** está selecionada e clique em **Avançar**.
9. Na página **Especificar Política de Expiração**, escolha as configurações a seguir e clique em **Avançar**:
   - Expiração do Conteúdo: **Expira após a seguinte duração (em dias): 7**
   - 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 um aplicativo

Etapas da demonstração

1. Em **LON-SVR1**, no console do **AD RMS**, clique no nó **Políticas de Exclusão** e clique em **Gerenciar lista de exclusões de aplicativos**.
2. No painel **Ações**, clique em **Habilitar a Exclusão de Aplicativo**.
3. No painel **Ações**, clique em **Excluir Aplicativo**.
4. Na caixa de diálogo **Excluir Aplicativo**, digite as informações a seguir e clique em **Concluir**:
   - Nome de Arquivo do Aplicativo: **Powerpnt.exe**
   - Versão mínima: **14.0.0.0**
   - Versão máxima: **16.0.0.0**

Revisão do módulo e informações complementares

Práticas recomendadas

- 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 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 têm acesso completo 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 executa uma configuração do AD RMS?

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

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

Resposta: Use uma conta da Microsoft para fornecer RACs aos prestadores de serviços não afiliados.

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

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

Perguntas e respostas da revisão do laboratório

Laboratório: Implementação de uma infraestrutura do AD RMS

Perguntas e respostas

Pergunta: Quais etapas você pode executar para garantir que poderá usar serviços de IRM com a função AD RMS?

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

Módulo 12

Implementação da sincronização do AD DS com o Microsoft Azure AD

Sumário:

Lição 1

Planejamento e preparação para a sincronização de diretório

Sumário:

Perguntas e respostas

Pergunta: Quando você implementa a sincronização de diretório, as contas de usuário e os grupos são movidas do seu AD DS local para o Azure AD.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

A sincronização de diretório não move objetos. Ela copia objetos do AD DS local com um subconjunto de seus atributos e cria novos objetos no Azure AD.

Recursos

Planejamento da sincronização de diretório

 **Leitura adicional:** para obter mais informações, consulte o Azure Hybrid Identity Design Considerations Guide em: http://aka.ms/ibuqek

Pré-requisitos e preparação para a sincronização de diretório

 **Leitura adicional:** para obter mais informações, consulte: "Você recebe o erro "Esta empresa excedeu o número de objetos que podem ser sincronizados" em um relatório de sincronização de diretório" em: http://aka.ms/r4x1q4

Lição 2

Implementação da sincronização de diretório usando o Azure AD Connect

Sumário:

Perguntas e respostas

Pergunta: Ao implementar a sincronização entre o AD DS e o Azure AD, onde você controla os objetos do AD DS?

> **Resposta:** Se tiver implantado o Azure AD Connect para a sincronização do Active Directory, você estará controlando os objetos de dentro do seu AD DS local usando ferramentas, como Usuários e Computadores do Active Directory ou o Windows PowerShell — a origem da autoridade é o AD DS local.

Recursos

Sincronização personalizada do Azure AD Connect

Leitura adicional: para obter mais informações, consulte: "Configurando o ID de logon alternativo" em: http://aka.ms/nqh5gc

Recursos de monitoramento do Azure AD Connect

Leitura adicional: para obter mais informações, consulte: "Monitorar infraestrutura de identidade local e serviços de sincronização na nuvem" em: http://aka.ms/dqaaps

Demonstração: Instalação e configuração do Azure AD Connect

Etapas da demonstração

1. Em **LON-SVR1**, entre como **Adatum\Administrador** com a senha **Pa55w.rd**.
2. Abra o Internet Explorer e acesse **http://www.microsoft.com/en-us/download/details.aspx?id=47594**.
3. Na página **Microsoft Azure Active Directory Connect**, clique em **Baixar**.
4. Clique em **Executar**. Aguarde alguns minutos até que o download seja concluído.

Observação: se tiver qualquer problema para iniciar o download, adicione o site https://download.microsoft.com aos seus sites confiáveis.

5. No **Assistente do Microsoft Azure Active Directory Connect**, na página **Bem-vindo ao Azure AD Connect**, selecione **Concordo com os termos de licença e o aviso de privacidade** e clique em **Continuar**.
6. Na página **Configurações Expressas**, clique em **Personalizar**.
7. Na página **Instalar componentes necessários**, examine as opções disponíveis, mas não faça alterações e, em seguida, clique em **Instalar**.
8. Na página **Entrada do usuário**, selecione **Sincronização de Senha** e clique em **Avançar**.
9. Na página **Conectar ao Azure AD**, nas caixas de texto **NOME DE USUÁRIO** e **SENHA**, digite **SYNC@seudomínio.onmicrosoft.com** para o nome de usuário da conta, digite **Pa55w.rd1** como a senha e clique em **Avançar**. Pode demorar alguns minutos para que a conexão seja estabelecida.

10. Na página **Conecte seus diretórios**, na caixa de texto **NOME DE USUÁRIO**, digite **Adatum\administrador** e, na caixa de texto **SENHA**, digite **Pa55w.rd**. Clique em **Adicionar Diretório** e, em seguida, clique em **Avançar**.
11. Na página **Configuração de entrada do Azure AD**, selecione **Continuar sem nenhum domínio verificado**, e clique em **Avançar**.
12. Na página **Filtragem de domínio e UO**, clique em **Avançar**.
13. Na página **Identificar com exclusividade seus usuários**, examine e explique as opções disponíveis, mas não faça alterações.
14. Clique em **Avançar**.
15. Na página **Filtrar usuários e dispositivos**, clique em **Sincronização selecionada**. Na caixa de texto **GRUPO**, digite **Pesquisa** e clique em **Resolver**. Verifique se uma marca de seleção verde é exibida depois que você clica em **Resolver**.
16. Clique em **Avançar**.
17. Na página **Recursos opcionais**, selecione **Write-back de senha**, explique as outras opções aos alunos e clique em **Avançar**.
18. Na página **Pronto para configurar**, clique em **Instalar** e, quando a instalação for concluída, clique em **Sair**.

A sincronização de objetos a partir do seu AD DS local e do Azure AD deve começar. Espere aproximadamente cinco minutos para que esse processo seja concluído.

19. Abra o Internet Explorer no seu computador host e, em seguida, abra o portal do Azure acessando **https://portal.azure.com**.
20. Entre com a sua conta criada durante o provisionamento da avaliação do Office 365.
21. No painel esquerdo, clique em **Azure Active Directory**.
22. Clique em **Usuários e grupos** na lista de opções **GERENCIAR**.
23. Clique em **Todos os usuários**.
24. Verifique se você pode ver as contas de usuário do seu AD DS local. Você deve ser capaz de ver todos os usuários do seu domínio adatum.com local.
25. Em **LON-SVR1**, clique em **Iniciar** e, em seguida, clique em **Azure AD Connect**. Expanda **Azure AD Connect** e clique em **Serviço de Sincronização**.
26. Na janela **Synchronization Service Manager em LON-SVR1**, clique na guia **Operações**.
27. Certifique-se de que você veja as tarefas **Exportação**, **Sincronização Completa** e **Importação Completa**.
28. Verifique se todas as tarefas têm a hora e a data atuais nas colunas **Hora de Início** e **Hora de Término**. Além disso, certifique-se de que todas as tarefas exibam **êxito** na coluna **Status**.

Lição 3

Gerenciamento de identidades com a sincronização de diretório

Sumário:

Perguntas e respostas

Pergunta: Se quiser ter SSO para o serviço baseado em nuvem e o serviço local, o que você precisa implantar? Escolha todas as opções aplicáveis.

( ) Azure AD Connect Health

( ) AD FS

( ) Azure AD Connect

( ) Office 365

( ) Azure AD

Resposta:

( ) Azure AD Connect Health

(√) AD FS

(√) Azure AD Connect

( ) Office 365

( ) Azure AD

Pergunta: Se implementar o AD FS e a federação entre o AD DS implantado localmente e o Azure AD, você não precisará usar o Azure AD Connect.

( ) Verdadeiro

( ) Falso

Resposta:

( ) Verdadeiro

(√) Falso

Comentários:

O AD DS local executa a autenticação e, em seguida, passa essas informações para o Azure AD. A senha do Azure AD não é usada. No entanto, as contas nos dois serviços de diretório devem coincidir. Portanto, é necessário que você use tanto o Azure AD Connect quanto o AD FS.

Recursos

Modificação da sincronização de diretório

Leitura adicional: para obter mais informações, consulte: "Sincronização do Azure AD Connect: configurar a filtragem" em: http://aka.ms/au8smo

Monitoramento da sincronização de diretório

Leitura adicional: para obter mais informações, consulte: "Azure Active Directory PowerShell Module" em: http://aka.ms/pfsm1x

Solução de problemas da sincronização de diretório

Leitura adicional: para obter mais informações, consulte: "Integração das suas identidades locais com o Azure Active Directory" em: http://aka.ms/cdm2kk

Leitura adicional: para obter mais informações, consulte: "How to troubleshoot Azure Active Directory Sync tool installation and Configuration Wizard errors" em: http://aka.ms/bz5cjw

Revisão do módulo e informações complementares

Práticas recomendadas

- Para ambientes simples, use as configurações expressas do Azure AD Connect.
- Habilite os usuários para usarem a funcionalidade de autoatendimento de redefinição de senha com pelo menos dois métodos de autenticação.
- Considere o uso de funcionalidades de write-back.
- Implemente o Azure AD Connect Health se tiver uma assinatura Premium do Azure AD.

Problemas e cenários reais

Como a sincronização de diretório é o vínculo entre seus objetos do AD DS local e os serviços no Azure AD, tenha cuidado ao fazer alterações no Azure AD Connect ou no Synchronization Service Manager após a implantação de produção. Por exemplo, um pequeno erro na filtragem pode excluir acidentalmente todas as caixas de correio de usuário no Office 365.

Em alguns ambientes, por exemplo, em um ambiente de teste, você pode testar todas as alterações em um outro servidor de sincronização de diretório que esteja conectado a um locatário separado do Azure AD (avaliação). Além disso, você deve iniciar manualmente os perfis de execução para cada agente de gerenciamento no Synchronization Service Manager e observar as ações pendentes antes de exportar para o Azure AD. Em alguns casos, convém criar um novo perfil de execução para a exportação para o Azure AD que inclui um limite máximo ao número de exclusões permitidas.

Pergunta de revisão

Pergunta: Qual recurso você precisa configurar para que os objetos sejam sincronizados do Azure AD com seu AD DS local?

> **Resposta:** Você precisa implantar funcionalidades de write-back. No momento, você pode usar o write-back de senha, o write-back de grupo e o write-back de dispositivos.

Ferramentas

A tabela a seguir lista as ferramentas mencionadas neste módulo:

Ferramenta	Use para	Onde encontrar
Azure AD Connect	Estabelecer a sincronização entre o AD DS e o Azure AD	Centro de Download da Microsoft
Azure AD Connect Health	Monitorar a integridade da sincronização do AD DS com o Azure AD	O portal clássico do Azure
O portal clássico do Azure	Gerenciamento do Azure AD	http://aka.ms/n2l3cb

Problemas comuns e dicas de solução de problemas

Problema comum	Dica de solução do problema
A filtragem de sincronização de diretório não está mais funcionando.	É importante ter a última versão da ferramenta de sincronização de diretório. No entanto, ao atualizar para uma nova versão da ferramenta, todos os filtros e outras personalizações do agente de gerenciamento não serão importados automaticamente para a nova instalação. Se você estiver atualizando para uma versão mais recente da sincronização de diretório, sempre reaplique manualmente as configurações de filtragem após a atualização, mas antes de executar o primeiro ciclo de sincronização.
Após a instalação do Azure AD Connect, um prompt poderá ser exibido com a seguinte mensagem de erro quando você abrir o Synchronization Service Manager: "Unable to connect to the Synchronization Service."	Adicione a conta de usuário apropriada do domínio do Azure AD Connect ao grupo ADSyncAdmins, saia e entre novamente. A conta de usuário do domínio que você usa para entrar durante a instalação do Azure AD Connect será adicionada automaticamente ao grupo, mas você ainda precisará sair e depois entrar novamente antes de conseguir abrir o Synchronization Service Manager com êxito.

Perguntas e respostas da revisão do laboratório

Laboratório: Configuração da sincronização de diretório

Perguntas e respostas

Pergunta: O que você precisa fazer antes de começar a configurar o Azure AD Connect?

Resposta: Você deve criar uma conta de sincronização no Azure AD e, em seguida, adicionar seu domínio ao locatário do Azure AD.

Pergunta: Qual cmdlet devo usar para alterar a agenda de sincronização do Azure AD Connect?

Resposta: Você deve usar o cmdlet **Set-ADSyncScheduler** no computador de instalação do Azure AD Connect.

Módulo 13

Monitoramento, gerenciamento e recuperação do AD DS

Sumário:

Lição 1

Monitoramento do AD DS

Sumário:

Recursos

Visão geral das ferramentas de monitoramento

 **Leitura adicional:** Para obter mais informações, consulte: "Uso do PowerShell para coletar dados de desempenho" no: http://aka.ms/F8mxnr

Demonstração: Monitoramento do AD DS

Etapas da demonstração

Configurar o Monitor de Desempenho para monitorar o AD DS

1. Alterne para **LON-DC1**.
2. No Gerenciador do Servidor, clique em **Ferramentas** e, depois, clique em **Monitor de Desempenho**.
3. No nó Ferramentas de Monitoramento, clique em Monitor de Desempenho.
4. Clique no botão **Adicionar** — o **Sinal de Mais** verde (**+**) na barra de ferramentas — para adicionar objetos e contadores.
5. Na caixa de diálogo **Adicionar Contadores**, na lista **Contadores Disponíveis**, expanda o objeto **DirectoryServices**.
6. Clique no contador **Total de bytes de entrada DRA/s** e, depois, clique em **Adicionar**.
7. Repita a etapa anterior (etapa 6) para adicionar os seguintes contadores:
   - **Total de bytes de saída DirectoryServices\DRA/s**
   - **Threads DirectoryServices\DS em uso**
   - **Leituras DirectoryServices\DS Directory/s**
   - **Gravações DirectoryServices\DS Directory/s**
   - **Pesquisas DirectoryServices\DS Directory/s**
   - **Objetos de entrada NTDS\DRA/s**
   - **Sincronizações NTDS\DRA com replicação pendente**
   - **Estatísticas Vastas do Sistema de Segurança\Autenticações NTLM**
   - **Estatísticas Vastas do Sistema de Segurança\Autenticações Kerberos**
8. Clique em **OK** e espere alguns momentos.
9. Na lista de contadores abaixo do gráfico, selecione **Pesquisas de pastas DS/s**.
10. Na barra de ferramentas, clique em **Realcar**. O contador selecionado é realçado, facilitando a visualização do desempenho desse contador.
11. Na barra de ferramentas, clique em **Realcar** para desligar o realce.

Criar um conjunto de coletores de dados

1. Na árvore de console, expanda **Desempenho**, expanda **Ferramentas de Monitoramento** e, em seguida, clique em **Monitor de Desempenho**. Clique com o botão direito do mouse em **Monitor de Desempenho**, aponte para **Novo** e clique em **Conjunto de Coletores de Dados**.
2. Na caixa de diálogo **Criar Novo Conjunto de Coletores de Dados**, na caixa de texto **Nome** digite **Contadores de Desempenho AD DS Personalizados** e, depois, clique em **Avançar**.
3. Anote o diretório raiz padrão em que o conjunto de coletores de dados será salvo, clique em **Avançar** e, em seguida, clique em **Concluir**.

Iniciar o conjunto de coletores de dados

1. Na árvore de console, expanda **Conjuntos de Coletores de Dados**, expanda **Definido pelo usuário** e clique em **Definido pelo usuário**.
2. Clique com o botão direito do mouse em **Contadores de Desempenho AD DS Personalizados** e, depois, clique em **Iniciar**. Enfatize que o nó **Contadores de Desempenho AD DS Personalizados** é selecionado automaticamente.

 **Observação:** Você pode identificar os coletores de dados individuais no conjunto de coletores de dados. Nesse caso, o conjunto de coletores de dados contém somente um coletor de dados — o contador de desempenho do Log do Monitor do Sistema. Você também pode identificar onde a saída de um coletor de dados está sendo salva.

3. Na árvore de console, clique com o botão direito do mouse no conjunto de coletores de dados **Contadores de Desempenho AD DS Personalizados** e, depois, clique em **Parar**.

Analisar os dados resultantes em um relatório

1. Na árvore de console, expanda **Relatórios**, expanda **Definido pelo usuário**, expanda **Contadores de Desempenho AD DS Personalizados** e, depois, clique em **Log do Monitor do Sistema.blg**.
2. Verifique o gráfico das exibições dos contadores de desempenho do log.

Lição 2

Gerenciamento do banco de dados do Active Directory

Sumário:

Demonstração: Execução do gerenciamento de banco de dados

Etapas da demonstração

Parar o AD DS

1. Se necessário, em **LON-DC1**, na barra de tarefas, clique no ícone **Gerenciador do Servidor**.
2. No **Gerenciador do Servidor**, clique em **Ferramentas** e, depois, clique em **Serviços**.
3. No console de **Serviços** clique com o botão direito do mouse em **Active Directory Domain Services** e, depois, clique em **Parar**.
4. Na caixa de diálogo **Interromper Outros Serviços**, clique em **Sim**.

Execução de uma desfragmentação offline do banco de dados do Active Directory

1. No **LON-DC1**, clique em **Iniciar** e em **Windows PowerShell**.
2. No prompt de comando do Windows PowerShell, digite o seguinte comando e pressione Enter:

```
NtdsUtil.exe
```

3. No prompt **NtdsUtil.exe:**, digite o seguinte comando e pressione Enter:

```
activate instance NTDS
```

4. No prompt **NtdsUtil.exe:**, digite o seguinte comando e pressione Enter:

```
files
```

5. No prompt **file maintenance:**, digite o seguinte comando e pressione Enter:

```
compact to C:\
```

Verificação da integridade do banco de dados do Active Directory offline

1. No prompt **file maintenance:**, digite o seguinte comando e pressione Enter:

```
Integrity
```

2. No prompt **file maintenance:**, digite o seguinte comando e pressione Enter:

```
quit
```

3. No prompt **NtdsUtil.exe:**, digite o seguinte comando e pressione Enter:

```
Quit
```

4. Feche a janela do **Windows PowerShell**.

Iniciar o AD DS

1. Na barra de tarefas, clique no ícone **Gerenciador do Servidor**.
2. No **Gerenciador do Servidor**, clique em **Ferramentas** e, depois, clique em **Serviços**.
3. No console de **Serviços** clique com o botão direito do mouse em **Active Directory Domain Services** e, depois, clique em **Iniciar**.
4. Confirme se a coluna **Status** do Active Directory Domain Services lista um status **Executando**.

Lição 3

Opções de backup e recuperação do Active Directory para o AD DS e outras soluções de identidade e acesso

Sumário:

Demonstração: Implementação da Lixeira do Active Directory

Etapas da demonstração

Habilitar a Lixeira do Active Directory

1. Em **LON-DC1**, no **Gerenciador do Servidor**, clique em **Ferramentas** e em **Centro Administrativo do Active Directory**.
2. Clique em **Adatum (local)**.
3. No painel **Tarefas**, clique em **Habilitar Lixeira**. Na caixa de mensagem de aviso, clique em **OK** e, depois, clique em **OK** novamente na janela **Atualizar Centro Administrativo do Active Directory**.
4. Pressione a tecla F5 para atualizar o Centro Administrativo do Active Directory.

Criar e depois excluir contas de teste

1. No Centro Administrativo do Active Directory, clique duas vezes em **Pesquisar** unidade organizacional (UO).
2. No painel **Tarefas**, clique em **Novo** e, depois, clique em **Usuário**.
3. Em **Conta**, digite as informações a seguir e clique em **OK**:
   - Nome completo: **Teste1**
   - Logon UPN do usuário: **Teste1**
   - Senha: **Pa55w.rd**
   - Confirmar senha: **Pa55w.rd**
4. Repita as etapas anteriores para criar um segundo usuário, **Teste2**.
5. Na caixa **Contas**, selecione **Teste1** e **Teste2**, clique com o botão direito do mouse na seleção e, depois, clique em **Excluir**.
6. No prompt de confirmação, clique em **Sim**.

Restaurar contas excluídas

1. No Centro Administrativo do Active Directory, clique em **Adatum (Local)** e, depois, clique duas vezes em **Objetos Excluídos**.
2. Clique com o botão direito do mouse em **Teste1** e clique em **Restaurar**.
3. Clique com o botão direito do mouse em **Teste2** e clique em **Restaurar em**.
4. Na janela **Restaurar em**, clique na UO **TI** e clique em **OK**.
5. Confirme se **Teste1** agora está localizado na UO Pesquisa e se **Teste2** está na UO TI.

Revisão do módulo e informações complementares

Práticas recomendadas

- Faça backup regularmente dos seus controladores de domínio.
- Considere a recuperação de banco de dados do AD DS como um cenário de restauração para controladores de domínio.
- Habilite a **Lixeira do Active Directory** para permitir recuperação simplificada de objetos excluídos.
- Use o AD DS reinicializável para realizar tarefas de manutenção de banco de dados.

Pergunta de revisão

Pergunta: Que tipo de restauração você pode executar com o AD DS?

Resposta: Você pode realizar restauração autoritativa, restauração não autoritativa e restauração de objetos únicos com a **Lixeira do Active Directory**.

Perguntas e respostas da revisão do laboratório

Laboratório: Recuperação de objetos no AD DS

Perguntas e respostas

Pergunta: Quando você restaurar um usuário excluído ou uma UO com objetos de usuário usando a restauração autoritativa, os objetos serão exatamente os mesmos de antes? Quais atributos podem não ser os mesmos?

Resposta: As respostas podem variar, mas a pergunta deve levar a uma discussão sobre associação a um grupo. A associação do usuário a um grupo não é um atributo do objeto do usuário, mas do objeto do grupo. Quando você restaura um usuário de modo autoritativo, você não está restaurando a associação do usuário a grupos. O usuário foi removido do atributo do membro de grupos quando foi excluído. Portanto, o usuário restaurado não será membro de nenhum grupo além do grupo primário do usuário. Para restaurar as associações a grupos, considere a possibilidade de restauração autoritativa de grupos. Isso nem sempre é desejável — quando restaura grupos de modo autoritativo, você retorna a associação para a data do backup.

Pergunta: No laboratório, seria possível restaurar os objetos excluídos se eles tivessem sido excluídos antes de você habilitar a **Lixeira do Active Directory**?

Resposta: Sim, mas somente como objetos marcados para exclusão sem a maioria dos atributos, ou usando restauração autoritativa do AD DS.