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.