

Instalação e configuração do Active Directory Domain Services

O Active Directory Domain Services (AD DS, Serviços de Domínio do Active Directory) fornece a base para soluções de identidade e acesso no Windows Server 2016. Portanto, é importante saber como implementar uma infraestrutura de AD DS para suportar as necessidades de identidade de sua organização.

Neste capítulo, abordamos a instalação e a configuração de controladores de domínio, e como criar e configurar usuários, grupos, computadores e unidades organizacionais (OUs, Organizational Units). Essas habilidades são fundamentais para implementar AD DS.

Objetivos deste capítulo:

- Instalar e configurar controladores de domínio
- Criar e gerenciar usuários e computadores do Active Directory
- Criar e gerenciar grupos e OUs do Active Directory

IMPORTANTE

Você leu a página 3?

Ela contém informações valiosas a respeito das habilidades necessárias para sua aprovação no exame.

Objetivo 1.1: Instalar e configurar controladores de domínio

Os controladores de domínio hospedam a função de servidor AD DS do Windows Server 2016 e fornecem autenticação e serviços relacionados para os computadores e outros dispositivos de rede de sua organização. Antes de entender os cenários de implantação de controladores de domínio do AD DS, é preciso primeiro saber os fundamentos do AD DS, incluindo florestas, árvores, domínios e OUs.

Esta seção introduz o AD DS e aborda como:

- Instalar uma nova floresta
- Adicionar ou remover um controlador de domínio
- Instalar AD DS em uma instalação Server Core
- Instalar um controlador de domínio usando Install from Media
- Instalar e configurar um controlador de domínio somente leitura
- Configurar um servidor de catálogo global
- Configurar a clonagem de controlador de domínio
- Migrar controladores de domínio
- Transferir e executar seize de funções de mestre de operações
- Solucionar problemas de gravação de registros SRV no DNS

Fundamentos do AD DS

O AD DS é composto de componentes lógicos e físicos. Um componente físico é algo tangível, como um controlador de domínio, enquanto uma floresta de AD DS é um componente lógico, intangível. O AD DS consiste nos seguintes componentes lógicos:

- **Floresta** É um conjunto de domínios do AD DS que compartilham um mesmo esquema e são ligados por relações de confiança recíprocas criadas automaticamente. A maioria das organizações implementa o AD DS com apenas uma floresta. Motivos para usar várias florestas incluem a necessidade de:
 - Fornecer total separação administrativa entre partes diferentes de sua organização.
 - Suportar diferentes tipos de objetos e atributos no esquema do AD DS, em diferentes partes de sua organização.
- **Domínio** É uma unidade administrativa lógica que contém usuários, grupos, computadores e outros objetos. Vários domínios podem fazer parte de uma ou de várias florestas, dependendo das necessidades organizacionais. Relações pai-filho e de confiança definem a estrutura do domínio.



DICA DE EXAME

Um domínio não oferece separação administrativa, pois todos os domínios de uma floresta têm o mesmo administrador de floresta – o grupo universal de segurança Enterprise Admins. Para ter separação administrativa completa, você deve implementar várias florestas do AD DS.

- **Árvore** É um conjunto de domínios do AD DS que compartilham um domínio raiz comum e têm namespace contíguo. Por exemplo, sales.adatum.com e marketing.adatum.com compartilham uma raiz comum adatum.com, e também um namespace contíguo, adatum.com. É possível construir sua floresta do AD DS usando uma ou várias árvores. Razões para usar várias árvores incluem o requisito de suportar

vários namespaces lógicos dentro de sua organização, talvez por causa de fusões ou aquisições.

- **Esquema** O esquema do AD DS é o conjunto de tipos de objetos e suas propriedades, também conhecidas como atributos, que definem os tipos de objetos que podem ser criados, armazenados e gerenciados dentro da floresta do AD DS. Por exemplo, um usuário é um tipo de objeto lógico, tendo várias propriedades, incluindo um nome completo, um departamento e uma senha. A relação entre objetos e seus atributos é mantida no esquema, sendo que todos os controladores de domínio de uma floresta contêm uma cópia do esquema.
- **OU** É um contêiner dentro de um domínio que contém usuários, grupos, computadores e outras OUs. Elas são usadas para oferecer simplificação administrativa. Com OUs, você pode facilmente delegar direitos administrativos para uma coleção de objetos, agrupando-os em uma OU e atribuindo o direito nessa OU. Também é possível usar Group Policy Objects (GPOs, Objetos de Política de Grupo) para definir configurações de usuário e computador e vincular essas configurações da GPO a uma OU, otimizando o processo de configuração. Uma OU é criada por padrão quando você instala o AD DS e cria um domínio: Domain Controllers.
- **Contêiner** Além das OUs, também é possível usar contêineres para agrupar coleções de objetos. Estão disponíveis vários contêineres internos, incluindo: Computers, Builtin e Managed Service Accounts. Não é possível vincular GPOs aos contêineres.
- **Site** É a representação lógica de uma localização física dentro de sua organização. Ele pode representar uma área física grande, como uma cidade, ou uma área física menor, como um conjunto de sub-redes definido pelos limites de seu datacenter. Os sites do AD DS ajudam a permitir que dispositivos de rede determinem onde estão em relação aos serviços que querem conectar. Por exemplo, quando um computador com Windows 10 inicializa, ele usa sua informação de site para tentar encontrar um controlador de domínio próximo para autenticar a conexão do usuário. Os sites também permitem controlar a replicação do AD DS, através da configuração de uma agenda e um intervalo para a replicação entre sites.



DICA DE EXAME

Um site padrão, Default-First-Site-Name, é criado quando você instala o AD DS e cria sua floresta. Todos os controladores de domínio pertencem a esse site, até que você crie mais sites e atribua controladores de domínio a eles. Se você pretende criar mais objetos de site, deve renomear o site padrão.

- **Sub-rede** É a representação lógica de uma sub-rede física em sua rede. Com a definição de sub-redes, um computador em sua floresta do AD DS pode determinar sua localização física em relação aos serviços oferecidos na floresta. Não existem sub-redes por padrão. Depois de criar sub-redes, você as associa a sites. Um site pode conter mais de uma sub-rede.
- **Partição** Seu AD DS é fisicamente armazenado em um banco de dados em todos os controladores de domínio. Como algumas partes do AD DS raramente mudam, enquanto outras mudam frequentemente, algumas partições separadas estão armazenadas no banco de dados AD DS.

NOTA REPLICAÇÃO DO AD DS

Quando são feitas alterações no AD DS, outras instâncias da partição alterada devem ser atualizadas. Esse processo é referido como replicação do AD DS. Dividindo-se o banco de dados em vários elementos, a carga do processo de replicação é reduzida.

As partições separadas são:

- **Esquema** Partição em nível de floresta, a qual raramente muda. Contém o esquema da floresta do AD DS.
- **Configuração** Partição em nível de floresta que raramente muda, contendo dados de configuração da floresta.
- **Domínio** Partição em nível de domínio. Esta partição muda frequentemente, sendo que uma cópia gravável dela é armazenada em todos os controladores de domínio. Ela contém os objetos reais existentes em sua floresta, como usuários e computadores.

NOTA CONTROLADORES DE DOMÍNIO SOMENTE LEITURA

Controladores de domínio somente leitura (RODCs, Read Only Domain Controllers) contêm uma cópia somente leitura da partição de domínio.

NOTA PARTIÇÕES DE DIRETÓRIO DE APLICATIVO

Também podem ser criadas partições específicas para suportar aplicativos implantados em sua floresta. Por exemplo, você pode configurar o DNS para usar uma partição de aplicativo específica, para propósitos de replicação de zona integrada ao AD.

- **Relações de confiança** Às vezes também referida só como confiança, é um acordo de segurança entre dois domínios em uma floresta do AD DS, entre duas florestas ou entre uma floresta e um território (realm) externo de segurança. Esse acordo de segurança permite a um usuário em um lado da confiança acessar recursos no outro lado da confiança. Em uma relação de confiança, diz-se que uma parte é confiante e a outra é confiável. O lado que contém o recurso é confiante, enquanto o que contém o usuário é confiável. Para ajudar a entender isso, considere quem é confiável e quem é confiante quando você empresta a chave de seu carro a alguém.

Instale uma nova floresta

Para instalar uma nova floresta do AD DS, implante nela o primeiro controlador de domínio. Isso significa implantar a função de servidor AD DS em um computador servidor com Windows Server 2016 e, então, promover o servidor a controlador de domínio e escolher a opção Add A New Forest.

Para criar uma floresta, comece instalando a função AD DS com o procedimento a seguir:

1. No computador Windows Server 2016, efetue login como administrador local.
2. Inicie o Server Manager e, então, no Dashboard, clique em Add Roles And Features.
3. Clique no Add Roles And Features Wizard e, então, como mostrado na Figura 1-1, na página Server Roles, marque a caixa de seleção Active Directory Domain Services, clique em Add Features e depois em Next.

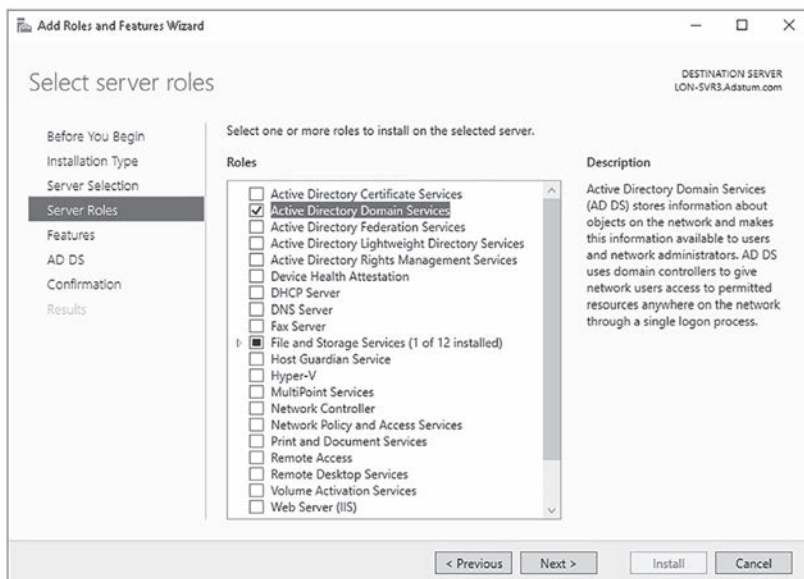


FIGURA 1-1 Instalando a função de servidor Active Directory Domain Services.

4. Clique no restante do assistente e, quando solicitado, clique em Install.
5. Quando a instalação terminar, clique em Close.



DICA DE EXAME

Você também pode usar o Windows PowerShell para instalar os arquivos necessários. Execute o comando a seguir em um prompt de comando elevado do Windows PowerShell: `Install-WindowsFeature ADDomain-Services`.

Depois de instalar os binários do AD DS é preciso criar uma floresta, promovendo o primeiro controlador de domínio nela. Para isso, use o seguinte procedimento:

1. No Server Manager, clique no triângulo de aviso amarelo em Notifications e clique em Promote This Server To A Domain Controller.

**DICA DE EXAME**

Também é possível usar o Windows PowerShell para fazer a promoção. Execute o cmdlet `InstallADDSDomainController`. Por exemplo, execute o comando `InstallADDSDomainController InstallDns -DomainName adatum.com` para adicionar o servidor local como mais um controlador de domínio no domínio Adatum.com e instalar a função de servidor DNS.

2. Na página Deployment Configuration do Active Directory Domain Services Configuration Wizard, sob Select The Deployment Operation, clique em Add A New Forest e digite o nome do domínio raiz da floresta, como mostrado na Figura 1-2. Clique em Next.

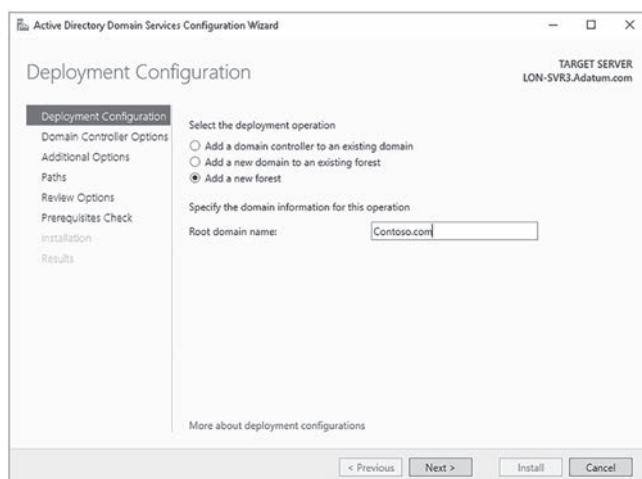


FIGURA 1-2 Adicionando uma nova floresta.

3. Na página Domain Controller Options, mostrada na Figura 1-3, configure as opções a seguir e, então, clique em Next:
 - **Forest Functional Level** O nível funcional da floresta determina os recursos disponíveis nela. O nível funcional da floresta também define o nível funcional mínimo para domínios em sua floresta. Assim, escolher Windows Server 2012 nesse nível significa que o nível funcional mínimo para domínios também é o Windows Server 2012. Escolha entre:
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

- **Domain Functional Level** Determina os recursos em nível de domínio disponíveis nesse domínio. Escolha entre:
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

PRECISA DE MAIS INFORMAÇÕES? NÍVEIS FUNCIONAIS DO WINDOWS SERVER 2016

Para ver mais detalhes sobre os níveis funcionais de domínio e floresta no Windows Server 2016, consulte o site Microsoft TechNet no endereço <https://technet.microsoft.com/windows-server-docs/identity/ad-ds/windows-server-2016-functional-levels>.

- **Domain Name System (DNS) Server** DNS fornece resolução de nomes e é um serviço importante para o AD DS. Esta opção é selecionada por padrão e, a não ser que você já tenha uma infraestrutura de DNS configurada, não a desmarque.
- **Global Catalog (GC)** Servidores de catálogo global fornecem serviços para toda a floresta. Essa opção está selecionada por padrão e não pode ser desmarcada. O primeiro (e único) controlador de domínio deve ser um servidor de catálogo global. Quando tiver adicionado outros controladores de domínio, você poderá rever esta configuração.
- **Read Only Domain Controller (RODC)** Determina se esse controlador de domínio é somente leitura. Esta opção não é selecionada por padrão e fica indisponível para o primeiro (e atualmente o único) controlador de domínio de sua floresta.
- **Directory Services Restore Mode (DSRM) Password** Usada ao se iniciar o controlador de domínio em um modo de recuperação.

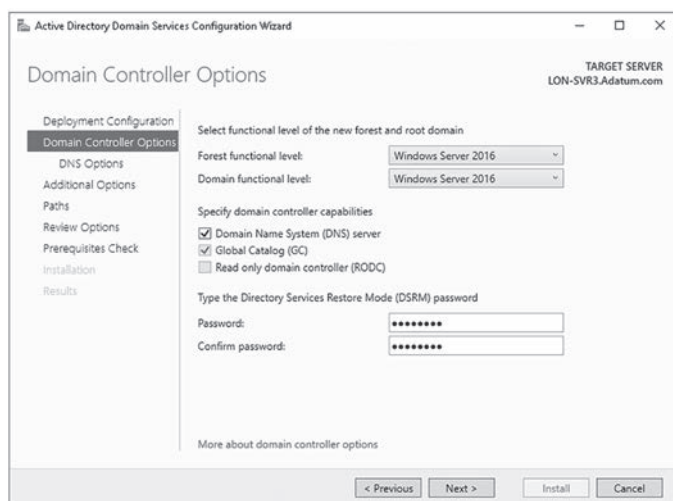


FIGURA 1-3 Configurando opções de controlador de domínio.

4. Na página Additional Options, defina o nome de domínio NetBIOS. O protocolo NetBIOS é pouco usado atualmente, e é baseado em uma estrutura de atribuição de nomes não hierárquica. O nome NetBIOS padrão é a primeira parte do nome da floresta do AD DS. Por exemplo, se sua floresta se chama Contoso.com, o nome NetBIOS padrão é CONTOSO. Geralmente, não é necessário mudar isso. Clique em Next.
5. Como mostrado na Figura 1-4, defina o local para armazenar o banco de dados do AD DS, arquivos de log e o conteúdo de SYSVOL, e clique em Next. Os padrões são:
 - Pasta do banco de dados: C:\Windows\NTDS
 - Pasta dos arquivos de log: C:\Windows\NTDS
 - Pasta SYSVOL: C:\Windows\SYSVOL

**DICA DE EXAME**

Normalmente, não há necessidade de usar caminhos diferentes. Contudo, é possível obter um pequeno aumento no desempenho separando SYSVOL, o banco de dados e os arquivos de log, caso seu servidor seja instalado com vários discos rígidos físicos, distribuindo a carga.

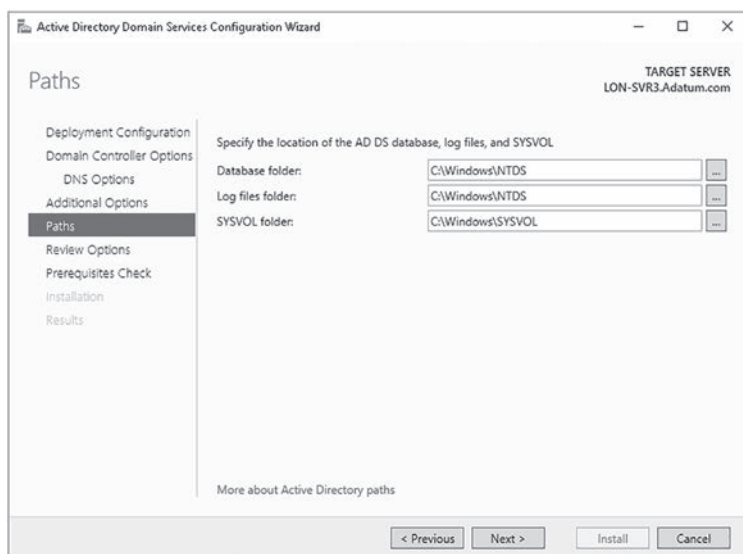


FIGURA 1-4 Configurando caminhos AD DS.

6. Examine as opções de configuração e depois clique em Next para realizar verificações de pré-requisito.
7. Quando solicitado, clique em Install. Seu computador servidor reinicia durante o processo de instalação.
8. Efetue logon em seu computador servidor usando a conta de administrador do domínio.

PRECISA DE MAIS INFORMAÇÕES? INSTALAÇÃO DE ACTIVE DIRECTORY DOMAIN SERVICES

Para ver mais detalhes sobre a implantação de AD DS, consulte o site do Microsoft TechNet, no endereço <https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/install-active-directory-domain-services--level-100->.

Adicione ou remova um controlador de domínio

Depois de implantar o primeiro controlador de domínio em sua floresta do AD DS, você pode adicionar outros controladores de domínio para fornecer resiliência e aumentar o desempenho. O processo de implantação de mais controladores de domínio é praticamente o mesmo do primeiro: instalar a função de servidor AD DS (usando Server Manager ou Windows PowerShell) e promover o controlador de domínio (novamente, usando Server Manager ou Windows PowerShell).

Contudo, as opções específicas selecionadas durante o processo de promoção variam de acordo com os detalhes da implantação. Por exemplo, adicionar um novo controlador de domínio em um domínio já existente é um pouco diferente de adicionar um novo controlador de domínio em um novo domínio.

Existem dois cenários básicos para a adição de um novo controlador de domínio:

- **Adicionar um novo controlador de domínio em um domínio já existente** Para completar esse processo, você precisa efetuar logon como membro do grupo global de segurança Domain Admins do domínio de destino.
- **Adicionar um novo controlador de domínio em um novo domínio** Para completar esse processo, você precisa efetuar logon como membro do grupo universal de segurança Enterprise Admins, contido no domínio raiz da floresta. Isso fornece a você privilégio suficiente para modificar a partição de configuração do AD DS e criar o novo domínio, ou como parte da árvore de domínios existente ou como parte de uma nova árvore de domínios.

Um motivo comum para adicionar um novo domínio é a criação de um limite de replicação. Como a maioria das alterações feitas no banco de dados do AD DS ocorre na partição de domínio, é essa partição que gera a maior parte do tráfego de replicação do AD DS. Dividindo sua floresta do AD DS em vários domínios, você pode dividir o volume de alterações e, assim, reduzir a replicação entre sites. Por exemplo, se A. Datum tivesse uma grande implantação de computadores na Europa e no Canadá, dois domínios separados poderiam ser criados a partir do domínio raiz da floresta Adatum.com: Europe.Adatum.com e Canada.Adatum.com. As alterações feitas no domínio Europe.Adatum.com não são replicadas nos controladores de domínio de Canada.Adatum.com e vice-versa.

Adicione um novo controlador de domínio em um domínio já existente

Para adicionar um novo controlador de domínio em um domínio já existente, efetue logon como administrador do domínio e complete o procedimento a seguir.

**DICA DE EXAME**

Efetuar logon como membro do grupo global de segurança Domain Admins pressupõe que o computador servidor que você pretende promover é membro do domínio de destino. Se não for, será mais fácil adicionar primeiro o computador servidor ao domínio de destino e, então, completar o procedimento. Se você optar por não adicionar o computador ao domínio de destino, deverá efetuar logon como administrador local e fornecer as credenciais de um administrador do domínio durante o processo de promoção. Também é necessário que o computador servidor que está sendo promovido possa resolver nomes usando o serviço DNS da floresta do AD DS.

1. Adicione a função de servidor Active Directory Domain Services.
2. No Server Manager, clique em Notifications e em Promote This Server To A Domain Controller.
3. Na página Deployment Configuration do Active Directory Domain Services Configuration Wizard, mostrada na Figura 1-5, clique em Add A Domain Controller To An Existing Domain.

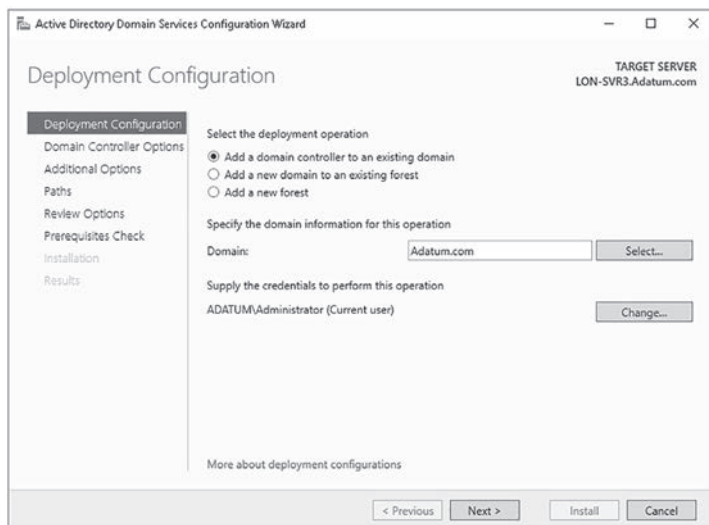


FIGURA 1-5 Implantando mais um controlador de domínio em um domínio existente

4. Especifique o nome do domínio. O nome padrão é o mesmo do domínio ao qual o computador servidor pertence. Contudo, é possível escolher outro domínio disponível na floresta.
5. Especifique as credenciais de uma conta de usuário com privilégio apropriado para executar o processo de promoção. O padrão é a conta de usuário atual. Clique em Next.

6. Na página Domain Controller Options, configure as opções Domain Name System (DNS) server (habilitada por padrão), Global Catalog (GC) (habilitada por padrão) e Read Only Domain Controller (RODC) (não habilitada por padrão). Diferente da promoção do primeiro controlador de domínio de uma floresta, é possível habilitar Read Only Domain Controller (RODC) para tornar esse um controlador de domínio somente leitura.
7. Na lista suspensa Site name, mostrada na Figura 1-6, selecione o site em que esse controlador de domínio está fisicamente posicionado. O padrão é Default-First-Site-Name. Até a criação de mais sites do AD DS, esse é o único disponível. Após a implantação, o controlador de domínio pode ser movido.

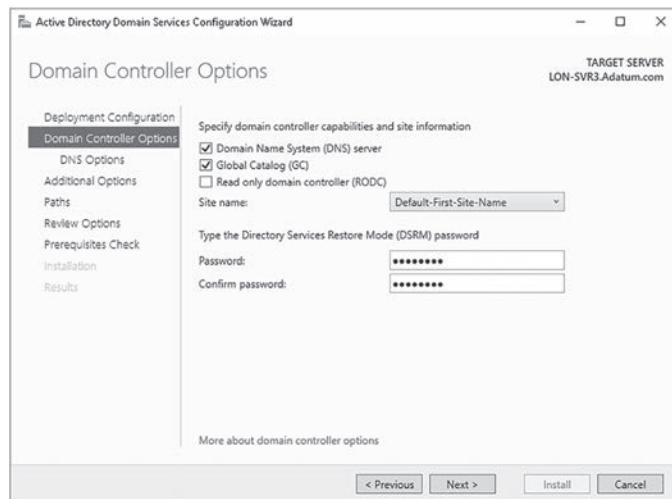


FIGURA 1-6 Configurando opções para um controlador de domínio adicional.

8. Digite a senha para Directory Services Restore Mode (DSRM) e clique em Next.
9. Na página Additional Options, configure como esse controlador de domínio irá receber o banco de dados do AD DS. É possível configurar a replicação inicial a partir de um controlador de domínio online, selecionando Any Domain Controller, como mostrado na Figura 1-7, ou especificar um controlador de domínio em particular. Como alternativa, você pode usar a opção Install from Media (IFM). Clique em Next.

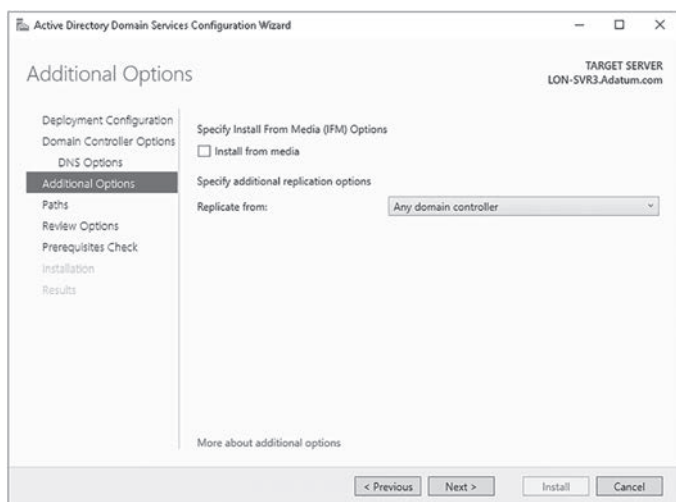


FIGURA 1-7 Configurando opções adicionais de controlador de domínio.

10. Configure os caminhos (Paths), como antes, e siga clicando para continuar o assistente de configuração.
11. Quando solicitado, clique em Install. Seu computador servidor reinicia durante o processo de promoção.

Depois de concluir o processo de promoção, efetue login usando uma conta de administrador do domínio.

Adicione um novo controlador de domínio em um novo domínio

Para adicionar um novo controlador de domínio a um novo domínio em uma floresta existente, efetue login com uma conta que seja membro do grupo universal de segurança Enterprise Admins da floresta e complete o procedimento a seguir.



DICA DE EXAME

Para efetuar login como membro do grupo universal de segurança Enterprise Admins pressupõe-se que o computador servidor que você pretende promover é membro de um dos domínios da floresta do AD DS. Se não for, será mais fácil adicionar primeiro o computador servidor ao domínio raiz da floresta e, então, completar o procedimento. Se você optar por não adicionar o computador ao domínio raiz da floresta, deverá efetuar login como administrador local e fornecer credenciais de um Enterprise Admin durante o processo de promoção. Também é necessário que o computador servidor que está sendo promovido possa resolver nomes usando o serviço DNS da floresta do AD DS.

1. Adicione a função de servidor Active Directory Domain Services.
2. No Server Manager, clique em Notifications e em Promote This Server To A Domain Controller.

3. Na página Deployment Configuration do Active Directory Domain Services Configuration Wizard, mostrada na Figura 1-8, clique em Add A New Domain To An Existing Forest.

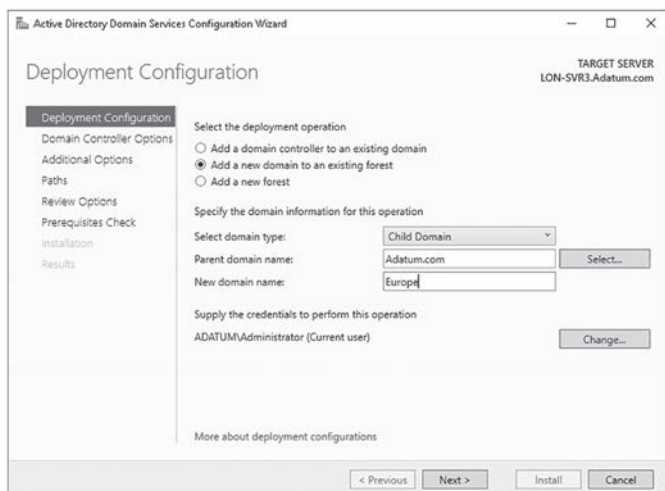


FIGURA 1-8 Adicionando um novo domínio filho a uma floresta já existente.

4. Então, você pode escolher como o novo domínio será adicionado. É possível selecionar:
 - **Child Domain** Esta opção cria um subdomínio do domínio pai especificado. Em outras palavras, o novo domínio é criado na árvore de domínios existente.
 - **Tree Domain** Selecione esta opção se quiser criar uma nova árvore na mesma floresta. A nova árvore compartilha o mesmo esquema da floresta e tem o mesmo domínio raiz, mas é possível definir um namespace não contíguo. Isso é útil quando se quer criar vários nomes de domínio DNS na infraestrutura de floresta do AD DS para suportar as necessidades organizacionais, mas não precisa ou não quer separar funções administrativas, como é possível em uma floresta separada. Se escolher Tree Domain, você deverá definir o nome da floresta em que a árvore será adicionada. O padrão é a floresta em que você está logado.
5. Digite o nome do novo domínio. No caso de um domínio filho, o nome inclui o domínio pai como sufixo. Por exemplo, adicionar o domínio Europe como filho do domínio Adatum.com cria o domínio Europe.Adatum.com. Se você criar uma nova árvore, poderá digitar qualquer nome de domínio DNS válido e ele não conterá o domínio raiz da floresta. Clique em Next.
6. Na página Domain Controller Options, selecione o nível funcional do domínio e configure os ajustes DNS, GC e RODC. Selecione o nome de site apropriado e, por fim, digite a senha DSRM e clique em Next.
7. Na página DNS Options, mostrada na Figura 1-9, marque a caixa de seleção Create DNS Delegation. Isso cria uma delegação de DNS para o subdomínio em seu namespace do DNS. Clique em Next.

PRECISA DE MAIS INFORMAÇÕES? ENTENDA A DELEGAÇÃO DE ZONAS

Para ver mais detalhes sobre delegação do DNS no Windows Server, consulte o site do Microsoft TechNet, no endereço [https://technet.microsoft.com/library/cc771640\(v=ws.11\).aspx](https://technet.microsoft.com/library/cc771640(v=ws.11).aspx).

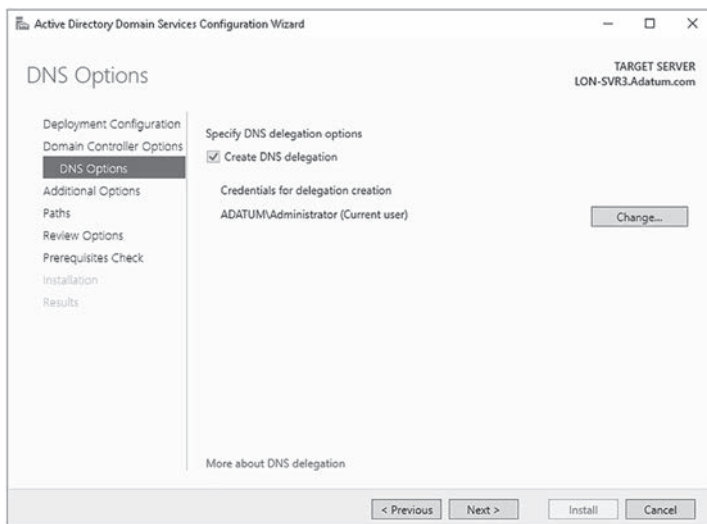


FIGURA 1-9 Adicionando um novo domínio filho a uma floresta já existente.

8. Especifique o nome de domínio NetBIOS e clique para continuar o assistente. Quando solicitado, clique em Install.
9. Seu controlador de domínio reinicia durante o processo de promoção. Após a conclusão do processo, efetue login como administrador do domínio.

Removendo controladores de domínio

De tempos em tempos pode ser necessário desativar e remover um controlador de domínio. Esse é um processo muito simples, e o Server Manager pode ser usado para cumprir a tarefa.

1. Efetue login usando uma conta que tenha privilégio suficiente. Para remover um controlador de domínio de um domínio, efetue login como administrador do domínio. Para remover um domínio inteiro, efetue login com um membro do grupo universal de segurança Enterprise Admins.
2. Abra o Server Manager e, no menu Manage, clique em Remove Roles And Features.
3. Na página Before You Begin do Remove Roles And Features Wizard, clique em Next.
4. Selecione o servidor apropriado na página Select Destination Server e clique em Next.
5. Na página Remove Server Roles, desmarque a caixa de seleção Active Directory Domain Services, clique em Remove Features e em Next.

6. Na caixa de diálogo pop-up Validation Results, mostrada na Figura 1-10, clique em Demote This Domain Controller.

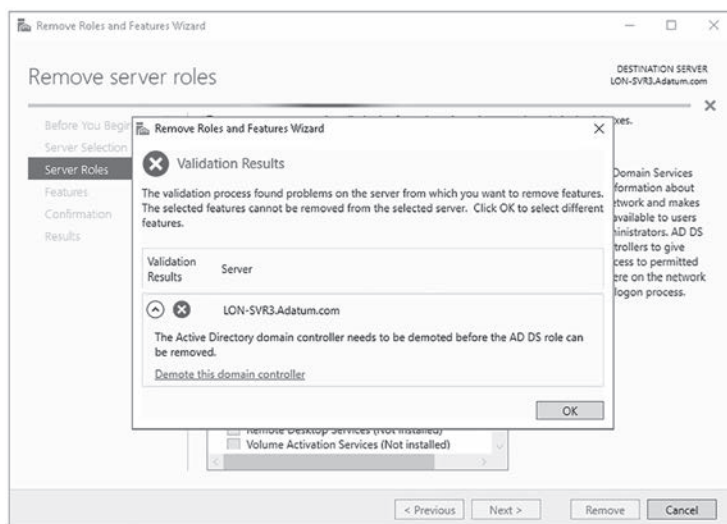


FIGURA 1-10 Removendo o AD DS.

7. O Active Directory Domain Services Configuration Wizard é carregado, como mostrado na Figura 1-11. Na página Credentials, se necessário, especifique credenciais de usuário com privilégio suficiente para fazer a remoção. Não marque a caixa de seleção Force The Removal Of This Domain Controller, a não ser que o controlador de domínio tenha falhado e não puder fazer contato. Clique em Next.

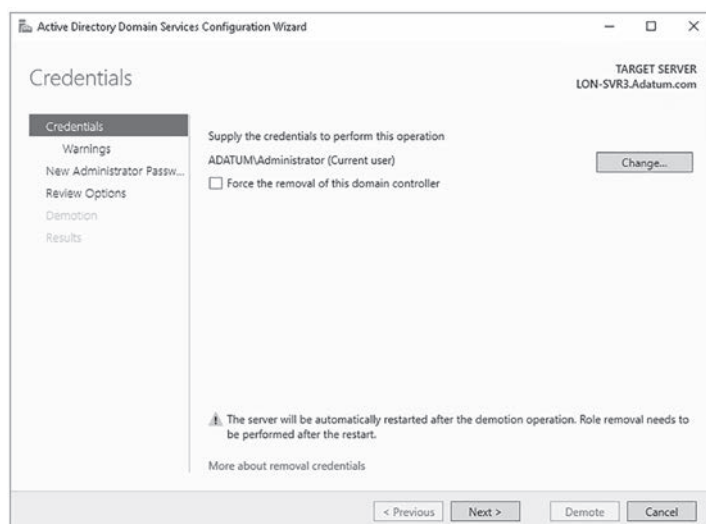


FIGURA 1-11 Rebaixando um controlador de domínio.

8. A página Warnings, mostrada na Figura 1-12, solicita confirmação da remoção das funções DNS e GC. Marque a caixa de seleção Proceed With Removal e clique em Next.

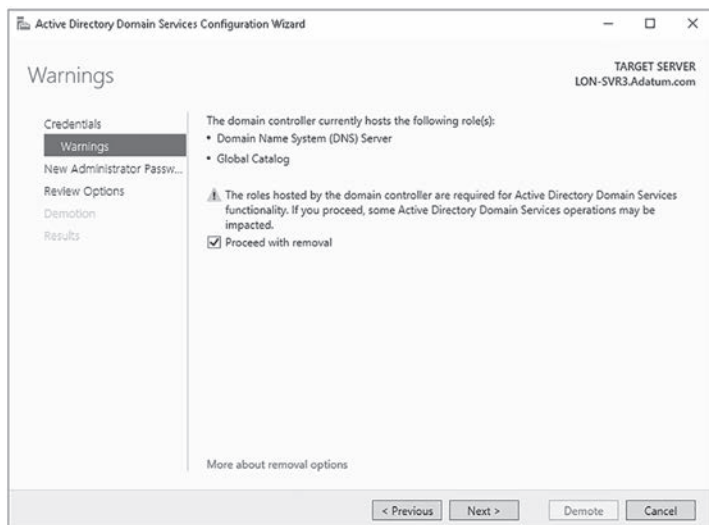


FIGURA 1-12 Removendo componentes opcionais.

9. Em New Administrator Password, digite e confirme a senha do administrador local e clique em Next.
10. Revise suas escolhas e, então, clique em Demote.
11. Seu servidor é rebaixado e, então, reiniciado. Efetue login usando a conta do administrador local.

Agora é possível verificar o rebaixamento e a remoção de função. Em um controlador de domínio:

1. Em um controlador de domínio, abra Active Directory Users And Computers. Verifique se o controlador de domínio rebaixado não está mais listado na OU Domain Controllers.
2. Clique no contêiner Computers. Você deverá ver o computador servidor rebaixado.
3. Abra Active Directory Sites And Services. Expanda Sites, expanda o site Default-First-Site-Name e, em Servers, exclua o objeto que representa o servidor rebaixado.



DICA DE EXAME

Se o servidor a ser desativado é o último controlador de domínio de um domínio, você deve primeiro remover todos os outros computadores do domínio, talvez os movendo para outros domínios dentro de sua floresta. Então, o procedimento é igual ao descrito anteriormente.

Também é possível completar o processo de rebaixamento usando o Windows PowerShell. Use os dois cmdlets a seguir para completar o processo a partir do prompt de comando do Windows PowerShell:

```
Uninstall-addsdomaincontroller
```

```
Uninstall-windowsfeature AD-Domain_Services
```

PRECISA DE MAIS INFORMAÇÕES? REBAIXANDO DOMÍNIOS E CONTROLADORES DE DOMÍNIO

Para ver mais detalhes sobre o rebaixamento de controladores de domínio, consulte o site do Microsoft TechNet, no endereço <https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/demoting-domain-controllers-and-domains--level-200->.

Instale AD DS em uma instalação Server Core

A função de servidor AD DS pode ser implantada em uma instalação Server Core. O Server Manager pode ser usado para instalar a função remotamente ou use o cmdlet `Install-WindowsFeature AD-Domain-Services` do Windows PowerShell.

Depois de instalar os arquivos exigidos, você pode ativar o Active Directory Domain Services Configuration Wizard a partir do Server Manager, para configurar a instalação Server Core remotamente, ou usar o cmdlet `InstallADDSDomainController` do Windows PowerShell para concluir o processo de promoção. Em outras palavras, o processo para instalar AD DS em uma instalação Server Core do Windows Server 2016 é o mesmo usado para um servidor com Desktop Experience.



DICA DE EXAME

A função de servidor AD DS não pode ser implantada no Nano Server. Consequentemente, não é possível usar um Nano Server como controlador de domínio.

Instale um controlador de domínio usando Install from Media

Durante o processo de implantação de um controlador de domínio, o conteúdo do banco de dados AD DS é replicado para o novo controlador. Essa replicação inclui as partições do esquema e de configuração em nível de floresta e a partição de domínio apropriada. Após esse sincronismo inicial, a replicação ocorre normalmente entre os controladores de domínio.

Em algumas circunstâncias, o sincronismo inicial pode apresentar um desafio. Por exemplo, isso pode ser desafiador quando se está implantando um controlador de domínio em um local que está conectado à infraestrutura de rede de sua organização por meio de uma conexão de baixa largura de banda. Nessa situação, o sincronismo inicial pode demorar um longo tempo ou usar uma proporção excessiva da largura de banda disponível.

Para minimizar isso, implante um controlador de domínio e faça o sincronismo do AD DS inicial usando uma cópia local, ou snapshot, do banco de dados do AD DS. Isso é conhecido como fazer uma implantação usando Install from Media (IFM). Há muitos passos envolvidos nesse processo.

1. Em um controlador de domínio já existente, usando o Explorador de Arquivos, crie uma pasta, por exemplo C:\IFM, para armazenar o snapshot do AD DS.
2. Abra um prompt de comando elevado e execute o comando `ntdsutil.exe`.
3. No prompt `ntdsutil`;, digite **Activate instance ntds** e pressione Enter.
4. No prompt `ntdsutil`;, digite **ifm** e pressione Enter.
5. No prompt `ifm`;, como mostrado na Figura 1-13, digite **create SYSVOL full C:\IFM** e pressione Enter.

```

Administrator: C:\Windows\system32\cmd.exe - ntdsutil

C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create SYSVOL full C:\IFM
Creating snapshot...
Snapshot set {dd502b28-932b-46b4-b15e-f474b7d6e308} generated successfully.
Snapshot {de415184-2c1b-4b3e-a21e-4dfb0b4d61fb} mounted as C:\$SNAP_201611280300_VOLUMEC$\
Snapshot {de415184-2c1b-4b3e-a21e-4dfb0b4d61fb} is already mounted.
Snapshot {de415184-2c1b-4b3e-a21e-4dfb0b4d61fb} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_201611280300_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: C:\IFM\Active Directory\ntds.dit

Defragmentation Status (% complete)

0 10 20 30 40 50 60 70 80 90 100
|----|----|----|----|----|----|----|----|----|
.....

Copying registry files...
Copying C:\IFM\registry\SYSTEM
Copying C:\IFM\registry\SECURITY
Copying SYSVOL...
Copying C:\IFM\SYSVOL
Copying C:\IFM\SYSVOL\Adatum.com
Copying C:\IFM\SYSVOL\Adatum.com\Policies
Copying C:\IFM\SYSVOL\Adatum.com\Policies\{31B2F340-0160-1102-945F-00C04FB984F9}
  
```

FIGURA 1-13 Criando um snapshot do NTDS para IFM

6. No prompt `ifm`;, digite **quit** e pressione Enter.
7. No prompt `ntdsutil`;, digite **quit** e pressione Enter.
8. Feche o prompt de comando.
9. Usando o Explorador de Arquivos, copie o conteúdo da pasta C:\IFM, como mostrado na Figura 1-14, para um armazenamento removível, como um cartão de memória USB.

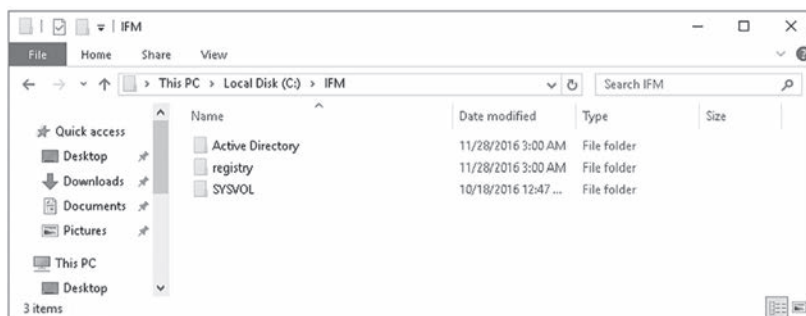


FIGURA 1-14 As pastas criadas para armazenar um snapshot do AD DS.

10. No computador servidor a ser promovido a controlador de domínio, instale a função de servidor Active Directory Domain Services normalmente, usando o Server Manager ou o Windows PowerShell.
11. Insira o cartão de memória que contém o snapshot do AD DS ou copie os arquivos de snapshot para que fiquem acessíveis no computador servidor de destino. Em seguida, ative o Active Directory Domain Services Configuration Wizard a partir do Server Manager e clique para dar continuidade no assistente.
12. Na página Additional Options, mostrada na Figura 1-15, marque a caixa de seleção Install from Media. Na caixa Path, digite o caminho para a cópia local do snapshot do AD DS, clique em Verify e em Next.

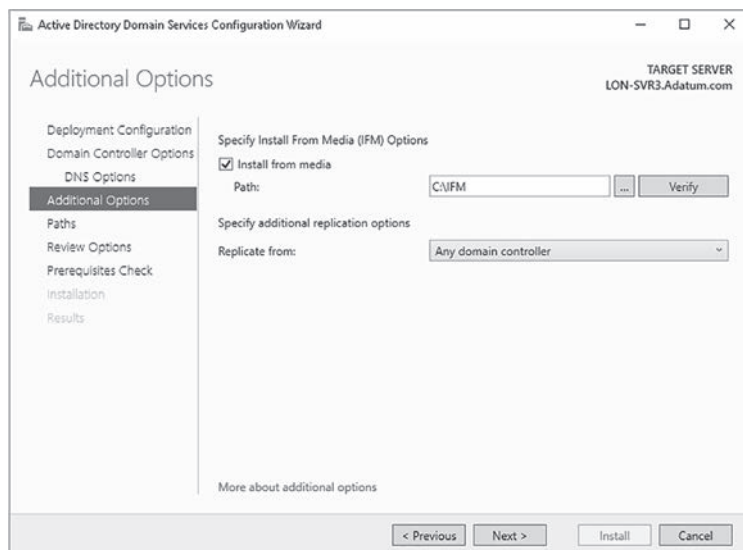


FIGURA 1-15 Escolhendo a opção Install from Media.

13. Clique para dar continuidade no assistente, revise suas seleções e, quando solicitado, clique em Install. Seu servidor reinicia durante o processo de promoção.
14. Efetue login como administrador do domínio.

Agora o controlador de domínio replica normalmente com outros controladores de domínio da floresta. Talvez você queira definir o site do AD DS ao qual o controlador de domínio pertence e, então, configurar uma agenda de replicação para esse site. Esses procedimentos são discutidos no Capítulo 2: Gerenciamento e manutenção de AD DS, Objetivo 2.3: Configurar o Active Directory em um ambiente corporativo complexo.



DICA DE EXAME

Também é possível completar a implantação usando o comando `InstallADDSDomaincontroller InstallationMediaPath x:\ifm` do Windows PowerShell, para promover o computador servidor.

Instale e configure um controlador de domínio somente leitura

RODC é um controlador de domínio que contém uma cópia somente leitura do AD DS. RODCs podem ser usados para a implantação de controladores de domínio em escritórios onde a segurança física não pode ser garantida. Por exemplo, em uma filial pode ser necessário um controlador de domínio local, mas não haver uma sala de computadores fisicamente segura para instalá-lo.

Embora RODCs ofereçam diversas vantagens administrativas, antes de implantá-los, os seguintes fatores devem ser considerados:

- Apenas um RODC deve ser implantado por site e por domínio. Se vários RODCs forem implantados por site, o uso do cache será inconsistente, resultando em possíveis problemas de logon de usuário e computador.
- A função de servidor DNS pode ser instalada junto com a função RODC. Clientes locais podem usar a função DNS instalada, assim como qualquer outra instância de DNS dentro de sua organização, com uma exceção: atualizações dinâmicas. Como as informações da zona do DNS são somente leitura, os clientes não podem fazer atualizações dinâmicas na instância de uma zona do DNS em um RODC. Nessa situação, o RODC fornece aos clientes o nome de um controlador de domínio gravável que eles podem usar para atualizar seus registros.
- RODCs não podem executar as seguintes funções do AD DS:
 - **Funções de mestre de operações** As funções de mestre de operações precisam gravar no banco de dados do AD DS. Consequentemente, RODCs não podem conter nenhuma das cinco funções de mestre de operações. As funções de mestre de operações são discutidas mais adiante neste objetivo.
 - **Bridgeheads de replicação do AD DS** Como os bridgeheads são responsáveis pela replicação do AD DS, devem suportar replicação do AD DS de entrada e saída. RODCs suportam apenas replicação de entrada e, portanto, não podem funcionar como bridgeheads de replicação do AD DS.
- RODCs não podem:
 - **Autenticar através de relação de confiança quando uma conexão de rede remota está indisponível** Se uma filial contém usuários de vários domínios da floresta do AD DS, usuários e computadores do domínio do qual o RODC não

é membro não podem ser autenticados quando um link está indisponível. Isso porque o RODC coloca em cache somente as credenciais das contas do domínio do qual é membro.

- **Suportar aplicativos que exigem interação constante com o AD DS** Alguns aplicativos, como o Microsoft Exchange Server, exigem interação com o AD DS. RODC não suporta a interatividade exigida e, portanto, deve-se implantar controladores de domínio graváveis nos sites que também contêm Exchange Servers.

Implantando um RODC

Antes de implantar um RODC é preciso garantir que haja pelo menos um controlador de domínio gravável em sua organização. Os RODCs são implantados da mesma forma que todos os outros controladores de domínio:

1. Instale a função de servidor Active Directory Domain Services no computador a ser implantado como RODC.
2. Ative o Active Directory Domain Services Configuration Wizard e clique para dar continuidade no assistente.
3. Na página Domain Controller Options, mostrada na Figura 1-16, marque a caixa de seleção Read Only Domain Controller (RODC) e quaisquer outras opções exigidas. Então, clique em Next.

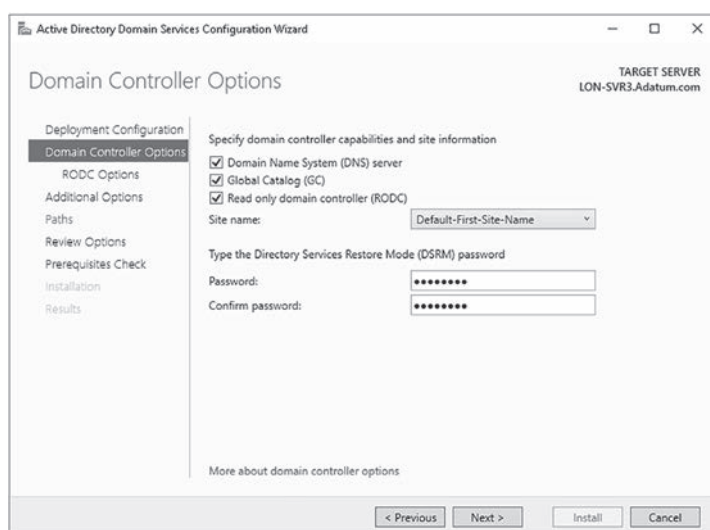


FIGURA 1-16 Instalando um RODC.

4. Na página RODC Options, mostrada na Figura 1-17, configure as opções a seguir e depois clique em Next.

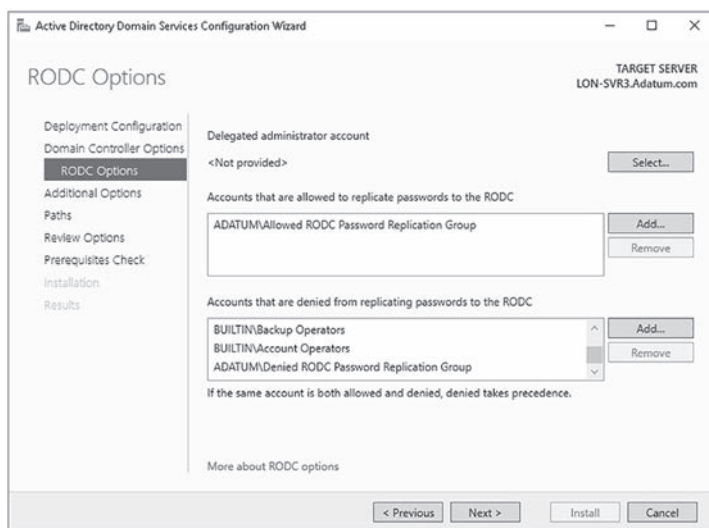


FIGURA 1-17 Configurando opções de RODC.

- **Delegated administrator account** O administrador (ou administradores) delegado pode fazer a administração local do RODC sem ter direitos e privilégios de administrador de domínio equivalentes. Normalmente, um administrador de RODC delegado pode executar as seguintes tarefas:
 - Instalar e gerenciar dispositivos e drivers, discos rígidos e atualizações
 - Gerenciar o serviço AD DS
 - Gerenciar funções e recursos de servidor
 - Ver logs de evento
 - Gerenciar pastas compartilhadas, aplicativos e serviços
- **Accounts that are allowed to replicate passwords to the RODC** Por padrão, os RODCs não armazenam informações sigilosas relacionadas a senhas. Quando um usuário efetua login, o RODC encaminha o pedido de login para um controlador de domínio gravável em outro lugar na organização.

Contudo, para melhorar a utilização, é possível definir que certas contas de usuário e computador podem ser colocadas em cache no RODC, permitindo autenticação local. Isso é feito pela definição de uma política de replicação de senha para RODC. Geralmente, você só adicionaria na política de replicação usuários e computadores que estivessem no mesmo local do RODC.



DICA DE EXAME

RODCs só armazenam um subconjunto das credenciais de usuário e computador. Consequentemente, se um RODC é roubado, a exposição da segurança fica limitada apenas às contas que estão em cache. Isso reduz a exposição global e ajuda a reduzir a carga administrativa, pois somente as senhas das contas que estão em cache precisam ser redefinidas.

Como mostrado na Figura 1-17, Allowed RODC Password Replication Group é habilitado por padrão. Depois de implantar o RODC, você pode adicionar usuários e computadores a esse grupo.

**DICA DE EXAME**

Além disso, há um grupo Denied RODC Password Replication Group. Os membros desse grupo nunca podem ter suas credenciais colocadas em cache no RODC. Por padrão, esse grupo contém Domain Admins, Enterprise Admins e Group Policy Creator Owners.

- **Accounts that are denied from replicating passwords to the RODC** O grupo Denied RODC Password Replication Group é selecionado por padrão. Depois de implantar o RODC, você pode adicionar usuários e computadores a esse grupo. Além disso, os seguintes grupos locais também não podem replicar senhas: Administrators, Server Operators, Backup Operators e Account Operators.

**DICA DE EXAME**

Os grupos Allowed RODC Password Replication Group e Denied RODC Password Replication Group permitem configurar a política de replicação de senha para todos os RODCs. Contudo, se houver várias filiais – e, portanto, vários RODCs – é mais seguro configurar um grupo separado de replicação de senha permitida para cada RODC. Nesse caso, remova o grupo Allowed RODC Password Replication Group, adicione um grupo criado manualmente e, então, adicione os membros necessários para essa filial.

5. Clique para dar continuidade no assistente, examine suas seleções e, quando solicitado, clique em Install. Seu servidor reinicia durante o processo de promoção.

**DICA DE EXAME**

Você pode usar o comando `InstallADDSDomainController ReadOnlyReplica` do Windows PowerShell para instalar um RODC.

Depois de implantar o RODC, configure os membros de Allowed RODC Password Replication Group e Denied RODC Password Replication Group para gerenciar a política de replicação de senhas para o RODC.

Configure um servidor de catálogo global

Em uma floresta do AD DS de apenas um domínio, qualquer controlador de domínio contém uma cópia de todos os objetos da floresta. Contudo, em florestas com vários domínios, isso não acontece. Embora todos os controladores de domínio contenham uma cópia das partições do esquema e de configuração, eles só armazenam a partição de domínio local. Assim, se um aplicativo consulta um controlador de domínio em seu domínio local a respeito dos atributos de um objeto em outro domínio, não há como o controlador de domínio local satisfazer essa consulta.

É aí que entra o catálogo global. O catálogo global é uma cópia parcial, somente leitura, de todos os objetos da floresta e contém um subconjunto dos atributos destas contas do AD DS. Todos os controladores de domínio configurados como servidores de catálogo global armazenam uma cópia dessas informações localmente. Isso permite que satisfaçam consultas por atributos de objetos que residem em outros domínios da floresta – sem a necessidade de solicitar a um controlador de domínio nesse outro domínio.



DICA DE EXAME

Em uma floresta de apenas um domínio, configure todos os controladores de domínio como servidores de catálogo global. Em uma floresta com vários domínios, a não ser que todos os controladores de domínio sejam servidores de catálogo global, o mestre de infraestrutura não deve ser configurado como servidor de catálogo global.

Um controlador de domínio pode ser configurado como servidor de catálogo global durante a implantação. Ao executar o Active Directory Domain Services Configuration Wizard, marque a caixa de seleção Global Catalog (GC) na página Domain Controller Options, como mostrado na Figura 1-16.

Como alternativa, após a instalação, use a ferramenta Active Directory Sites And Services:

1. Em um controlador de domínio, abra o Server Manager, clique em Tools e depois em Active Directory Sites And Services.
2. Expanda o nó Sites, expanda o site desejado, expanda a pasta Server e, então, expanda o nó do controlador de domínio a ser modificado.
3. Clique no objeto NTDS Settings, como mostrado na Figura 1-18.

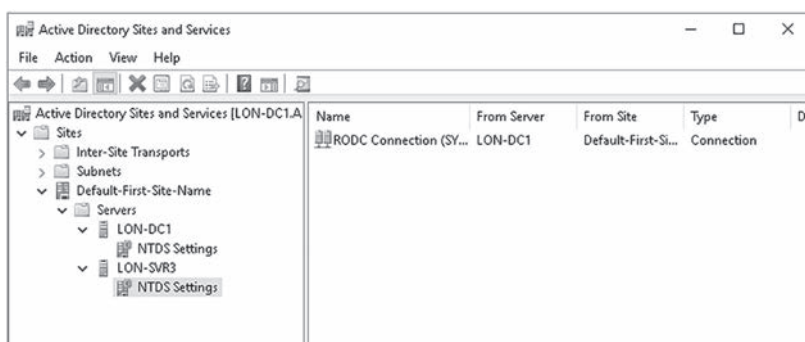


FIGURA 1-18 Configurando um servidor de catálogo global.

4. Clique com o botão direito do mouse no nó NTDS Settings e, na guia General, marque a caixa de seleção Global Catalog, como mostrado na Figura 1-19, e clique em OK.



FIGURA 1-19 Habilitando a propriedade Servidor de catálogo global.

Também é possível usar o Windows PowerShell para transformar um controlador de domínio em servidor de catálogo global.

1. Abra o Windows PowerShell (Admin).
2. Execute o comando `getADDomainController | select-object property Name,IsGlobalCatalog` para consultar uma lista de controladores de domínio e verificar seus status de catálogo global atual, como mostrado na Figura 1-20.



FIGURA 1-20 Obtendo uma lista de controladores de domínio.

3. Para o controlador de domínio apropriado, execute o comando a seguir, substituindo LONSVR3 pelo nome de seu controlador de domínio:

```
Set-ADObject -Identity (Get-ADDomainController -Identity LON-SVR3).  
NTDSSettingsObjectDN -Replace @{options='1'}
```

4. Execute o comando `getADDomainController | selectobject property Name,IsGlobalCatalog` novamente, para verificar a alteração, como mostrado na Figura 1-21.



FIGURA 1-21 Configurando um controlador de domínio como servidor de catálogo global, usando o Windows PowerShell



DICA DE EXAME

Muitas organizações agora optam por transformar todos os controladores de domínio em servidores de catálogo global.

Adicionando atributos ao catálogo global

É importante observar que o catálogo global não contém todos os atributos de todos os objetos. Em vez disso, contém um subconjunto dos atributos mais úteis, conhecidos no Windows Server 2016 como Partial Attribute Set (conjunto parcial de atributos). Contudo, é possível modificar quais atributos de objeto são armazenados no catálogo global. Às vezes isso é referido como extensão do conjunto parcial de atributos. Isso pode ser feito com o seguinte procedimento:

NOTA CUIDADO AO EDITAR O ESQUEMA DO AD DS

Tenha muito cuidado ao editar o esquema do AD DS diretamente, dessa maneira.

1. No controlador de domínio que tem acesso online à função de mestre de operações de esquema, execute o comando `regsvr32 schmmgmt.dll` em um prompt de comando elevado. Esse comando permite que o Active Directory Schema possa ser acessado por meio do console de gerenciamento.
2. Abra o console de gerenciamento executando `mmc.exe` em um prompt de comando elevado.
3. Na janela Console1 – [Console Root], clique em File e depois em Add/Remove Snap-in.
4. Na caixa de diálogo Add Or Remove Snap-ins, na lista Snap-ins, clique em Active Directory Schema, em Add e em OK.
5. Sob Console Root no painel de navegação, expanda Active Directory Schema e clique em Attributes. Aparece uma longa lista de atributos.
6. É preciso conhecer o nome do atributo específico para poder modificar suas propriedades. Localize o atributo, clique nele com o botão direito do mouse e, então, clique em Properties.

7. Na caixa de diálogo Properties do atributo (como a caixa de diálogo Properties de accountExpires mostrada na Figura 1-22), marque a caixa de seleção Replicate This Attribute To The Global Catalog e clique em OK.

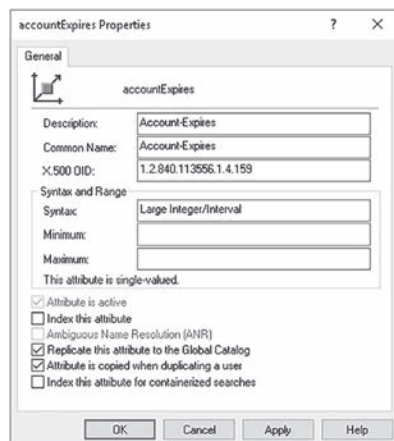


FIGURA 1-22 Adicionando um atributo ao catálogo global.

8. Feche o console de gerenciamento.

Configure a clonagem de controlador de domínio

É relativamente rápido e simples implantar controladores de domínio com os procedimentos descritos anteriormente neste capítulo. Mas se você tem muitos servidores basicamente idênticos que deseja configurar como controladores de domínio, uma estratégia mais rápida é clonar esses controladores. Isso é especialmente relevante quando os controladores de domínio são virtualizados.

Nas versões do Windows Server anteriores ao Windows Server 2012 era proibido clonar controladores de domínio virtuais. Contudo, o Windows Server 2012 e o Windows Server 2016 suportam clonagem de controlador de domínio virtual. Se você decidir implantar controladores de domínio usando clonagem, há as seguintes vantagens em potencial:

- **Implantação rápida de controladores de domínio** Isso não apenas torna a implantação inicial menos demorada, como também oferece a oportunidade de responder rapidamente a interrupções de controlador de domínio, implantando um novo clone.
- **Responder à maior demanda** Seja um aumento na demanda em uma filial ou em outro lugar, é possível implantar clones rapidamente, de acordo com a necessidade.

Criando um clone

Antes de clonar um controlador de domínio virtual é preciso garantir que a infraestrutura satisfaça os seguintes requisitos:

- **Windows Server 2012 ou posterior** As máquinas virtuais convidadas do controlador de domínio devem executar Windows Server 2012 ou posterior.

- **Mestre de operações de emulador PDC** O mestre de operações de emulador PDC (Primary Domain Controller, controlador de domínio primário) deve estar executando em um controlador de domínio instalado com Windows Server 2012 ou posterior. Além disso, a função de emulador PDC deve estar online na primeira vez que os controladores de domínio clonados forem iniciados.
- **Identificadores de geração de máquina virtual** Deve-se usar um hipervisor, como o Hyper-V no Windows Server 2012 ou posterior, que suporte identificadores de geração da máquina virtual (generation_id).

Depois de ter verificado esses pré-requisitos, use o procedimento a seguir para clonar um controlador de domínio virtual. São dois estágios: preparar o controlador de domínio de origem e preparar um ou mais clones do controlador de domínio de destino.

PREPARE O COMPUTADOR DE ORIGEM

1. Efetue login no controlador de domínio com um membro do grupo global de segurança Domain Admins.
2. Abra o console Active Directory Users And Computers, vá até a pasta Users e adicione o computador de origem ao grupo global de segurança Cloneable Domain Controllers, como mostrado na Figura 1-23.

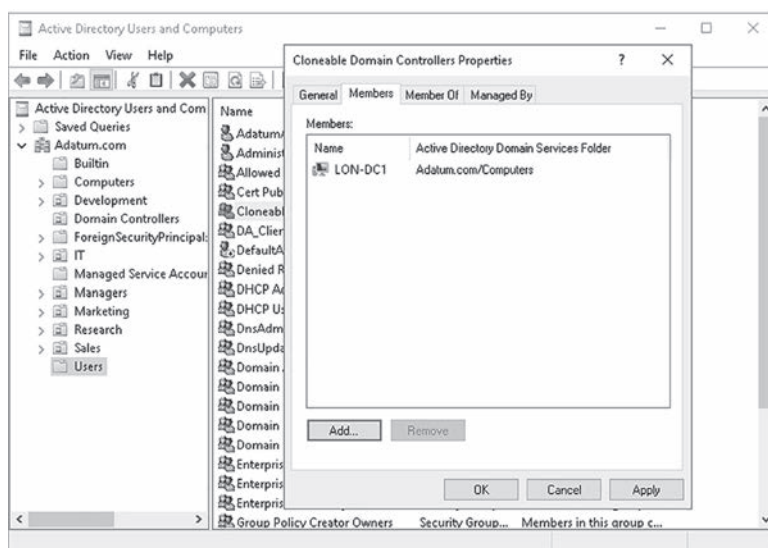


FIGURA 1-23 Adicionando um servidor ao grupo de segurança Cloneable Domain Controllers

3. Execute o cmdlet `Get-ADDCCloneingExcludedApplicationList` do Windows PowerShell para verificar se todos os aplicativos e serviços do controlador de domínio de origem suportam clonagem. Remova quaisquer aplicativos não suportados.

**DICA DE EXAME**

Se depois de clonar um controlador de domínio, você descobrir que os aplicativos funcionam, podem adicioná-los ao arquivo CustomDCCloneAllowList.xml.

4. Execute o cmdlet `Get-ADDCCloneingExcludedApplicationList -GenerateXML` do Windows PowerShell.
5. Execute o cmdlet `New-ADDCCloneConfigFile` do Windows PowerShell, como mostrado na Figura 1-24, para gerar um arquivo `DCCloneConfig.xml`. Esse arquivo é usado para configurar os clones. Especifique um nome de computador, a configuração de IP e um nome de site para o clone. Essas informações são gravadas no arquivo `DCCloneConfig.xml`. Se você pretende criar vários clones, normalmente cada um deve ter um arquivo `DCCloneConfig.xml` diferente.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDCCloneingExcludedApplicationList -GenerateXML
The inclusion list was written to 'C:\Windows\WinSxS\CustomDCCloneAllowList.xml'.
PS C:\Users\Administrator> New-ADDCCloneConfigFile -ComputerName ADatum.com -SiteName Local
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or later.
Pass: The domain controller hosting the PDC FSMO role (LON-DC1.Adatum.com) was located and running Windows Server 2012 or later.
Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (LON-DC1.Adatum.com).
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.
Starting test: Validating the cloning allow list.
NOTE: C:\Windows\WinSxS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.
No valid clone configuration files were found at any of the supported locations.
All preliminary validation checks passed.
Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\WinSxS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.
PS C:\Users\Administrator>
```

FIGURA 1-24 Criando o arquivo `DCCloneConfig.xml` com o Windows PowerShell.

6. Encerre o controlador de domínio virtual de origem.
7. Exporte o controlador de domínio virtual de origem:
 - Clique com o botão direito do mouse na máquina virtual controladora de domínio de origem no painel de navegação e clique em Export.
 - Na caixa de diálogo Export Virtual Machine, na caixa de texto Location, especifique a pasta onde deseja armazenar a máquina virtual exportada e clique em Export.

**DICA DE EXAME**

Antes de exportar, certifique-se de que não haja nenhum ponto de verificação (checkpoint) da sua máquina virtual controlador de domínio.

8. Se estiver implantando vários clones, você deve agora modificar o arquivo DCCloneConfig.xml de cada um. Faça isso montando o VHD do clone controlador de domínio de destino e executando o cmdlet New-ADDCCloneConfigFile, definindo as informações exclusivas exigidas para o clone. Se estiver implantando apenas um clone, pule este passo.

CRIE CLONE(S)

1. Certifique-se de que o emulador de PDC e um servidor de catálogo global estejam online e visíveis para seus clones de destino.
2. No Hyper-V Manager, importe a máquina virtual:
 - A. No painel Actions, clique em Import Virtual Machine.
 - B. Na página Locate Folder do Import Virtual Machine Wizard, na caixa de texto Folder, digite o caminho para os arquivos exportados de sua máquina virtual e clique em Next.
 - C. Na página Select Virtual Machine, mostrada na Figura 1-25, se necessário, selecione a máquina virtual na lista e clique em Next.

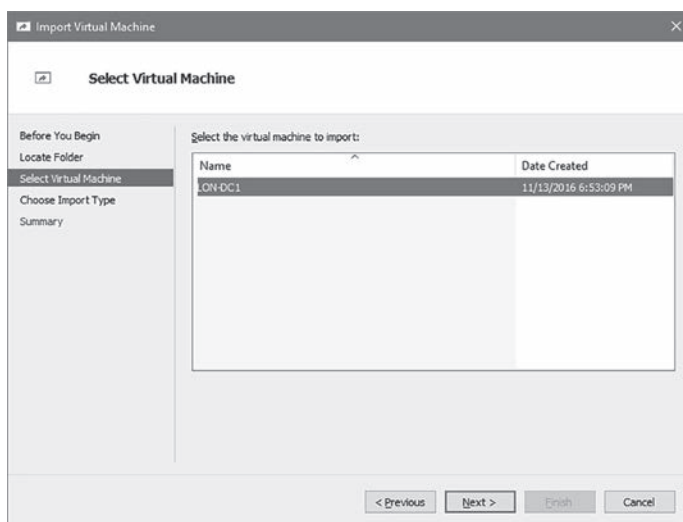


FIGURA 1-25 Importando uma máquina virtual.

3. Na página Choose Import Type, mostrada na Figura 1-26, clique em Copy The Virtual Machine (Create A New Unique ID) e depois em Next.

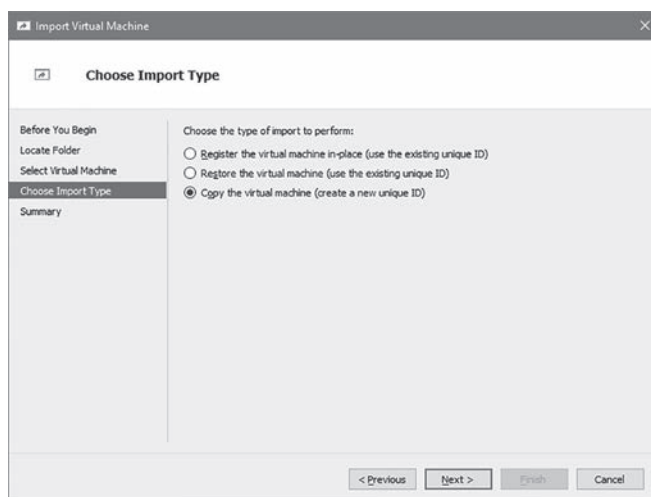


FIGURA 1-26 Especificando um tipo de importação.

4. Na página Choose Folders For Virtual Machine Files, mostrada na Figura 1-27, marque a caixa de seleção Store The Virtual Machine In A Different Location e, para cada local de pasta, especifique um caminho de pasta conveniente e clique em Next.

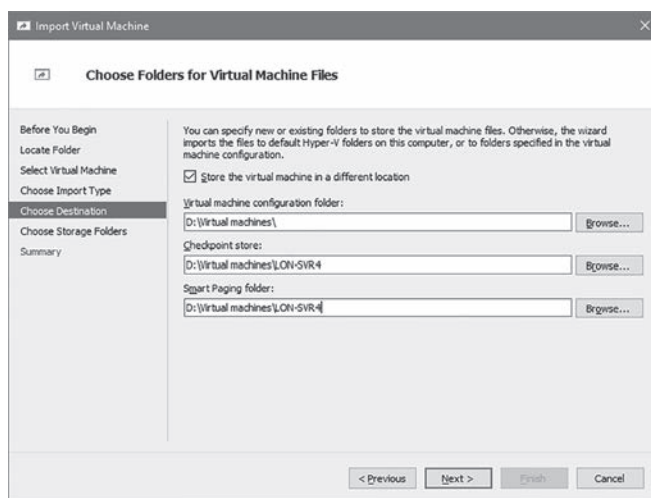


FIGURA 1-27 Especificando o local para os arquivos de máquina virtual importados.

5. Na página Choose Folders To Store Virtual Hard Disks, mostrada na Figura 1-28, especifique um caminho de pasta conveniente e clique em Next.

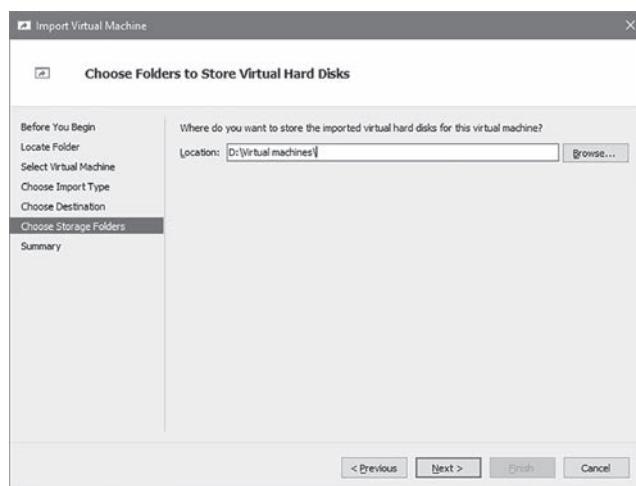


FIGURA 1-28 Especificando o local para os arquivos de máquina virtual importados.

6. Na página Completing Import Wizard, clique em Finish. A máquina virtual é importada, o que pode demorar uns 20 minutos.
7. Após a importação, no Hyper-V Manager, no painel de navegação, renomeie a máquina virtual importada.
8. No Hyper-V Manager, no painel Actions, clique na máquina virtual recentemente importada, clique em Start e depois em Connect para ver a máquina virtual inicializar. A mensagem "Domain Controller cloning is at x% completion" aparece durante a conclusão do processo de clonagem.

NOTA LEMBRETE

Certifique-se de que o emulador de PDC e um servidor de catálogo global estejam online e acessíveis para seu clone.

Quando o controlador de domínio clonado inicia, o seguinte processo ocorre:

1. O clone verifica a presença de um identificador de geração de máquina virtual. Isso é obrigatório e, se não existir, o computador iniciará normalmente, como se não existisse nenhum arquivo DCCloneConfig.xml, ou renomeará DCCloneConfig.xml e reiniciará no DSRM. Então, o administrador deve tentar saber por que não existe nenhum identificador de geração de máquina virtual.
2. Supondo a presença do identificador de geração de máquina virtual, o clone determina se esse identificador mudou:
 - Se não mudou, esse é o controlador de domínio de origem original. Qualquer arquivo DCCloneConfig.xml é renomeado e ocorre uma inicialização normal.
 - Se mudou, o processo de clonagem continua. Se o arquivo DCCloneConfig.xml existe, o computador recebe as novas configurações de nome e endereço IP do arquivo e a inicialização continua, criando um controlador de domínio.

Migre controladores de domínio

Se você está usando uma versão anterior do Windows Server e quer migrar seus controladores de domínio para o Windows Server 2016, pode fazer uma migração local (in-place). Contudo, esse processo apresenta alguns riscos. Geralmente é mais seguro adicionar um (ou mais) novo(s) controlador(es) de domínio Windows Server 2016 na infraestrutura existente e, então, migrar funções para o(s) controlador(es) de domínio recentemente implantado(s).

NOTA MIGRAÇÕES LOCAIS

Uma migração local é aquela em que o Windows Server 2016 é instalado no mesmo computador servidor que está executando uma versão anterior, por exemplo, Windows Server 2008 R2.

Antes de implantar o primeiro controlador de domínio Windows Server 2016 na infraestrutura existente, é preciso determinar se os níveis funcionais de floresta e domínio atuais são pelo menos Windows Server 2008. Isso pode ser feito com o seguinte procedimento:

1. No console Active Directory Domains And Trusts, no painel de navegação, clique com o botão direito do mouse no nó Active Directory Domains And Trusts e, então, clique em Raise Forest Functional Level.
2. O nível funcional de floresta atual aparece na caixa de diálogo Raise Forest Functional Level, como mostrado na Figura 1-29.
3. Se necessário, na lista Select An Available Forest Functional Level, clique em um nível maior que Windows Server 2008 e, então, clique em Raise.

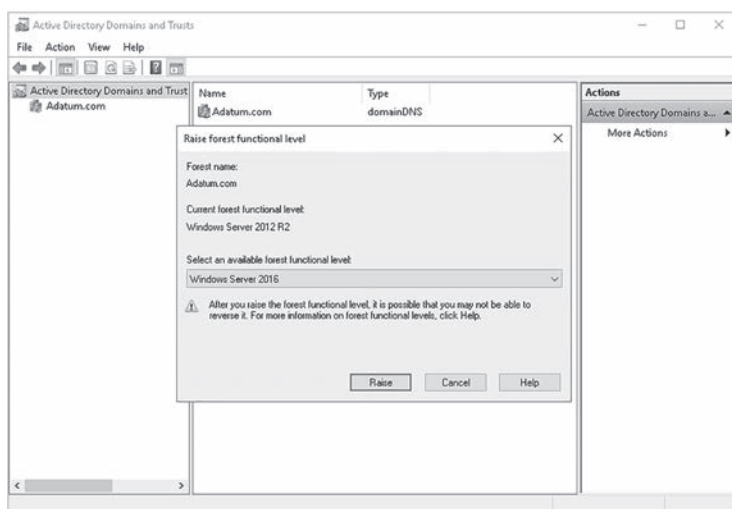


FIGURA 1-29 Verificando o nível funcional de floresta.

4. No painel de navegação, localize e clique com o botão direito do mouse no domínio do AD DS apropriado e, então, clique em Raise Domain Functional Level.
5. O nível funcional de domínio atual aparece na caixa de diálogo Raise Domain Functional Level, como mostrado na Figura 1-30.
6. Se necessário, na lista de Select An Available Domain Functional Level, clique em um nível maior que Windows Server 2008 e, então, clique em Raise.

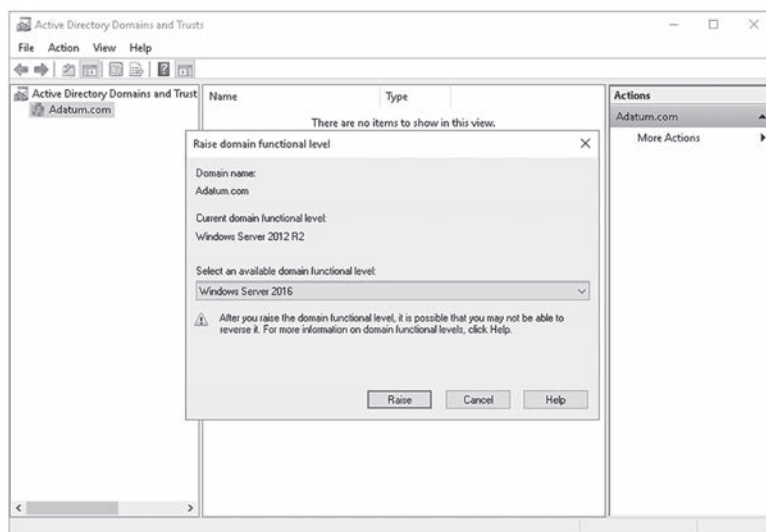


FIGURA 1-30 Verificando o nível funcional de domínio.

Depois de verificar e (se necessário) elevar os níveis funcionais de floresta e domínio, e se a infraestrutura existente é baseada no Windows Server 2008 ou no Windows Server 2008 R2, execute as seguintes tarefas:

- **Prepare sua floresta do AD DS** Em um controlador de domínio de sua floresta existente, execute `adprep /forestprep`.
- **Prepare seu domínio do AD DS** Em um controlador de domínio de sua floresta existente, execute `adprep /domainprep`.

Se sua infraestrutura atual é baseada em Windows Server 2012 ou posterior, o Active Directory Domain Services Configuration Wizard executa esses passos automaticamente. Contudo, ainda é possível optar por executá-los como etapas independentes.



DICA DE EXAME

Adprep.exe está na pasta `\Support\Adprep` do DVD do Windows Server 2016.

Depois de elevar os níveis funcionais de floresta e domínio, se necessário, e preparar a floresta e o domínio do AD DS, você pode implantar o primeiro controlador de domínio Windows Server 2016. Para executar essa tarefa, use os procedimentos discutidos anteriormente neste capítulo. Então, pode transferir as funções de mestre de operações para

o(s) novo(s) controlador(es) de domínio Windows Server 2016, como descrito na próxima seção. Por fim, rebaixe e remova os controladores de domínio antigos.

Transfira e execute seize de funções de mestre de operações

O banco de dados do AD DS suporta atualizações de múltiplos mestres. Em linhas gerais, isso significa que uma alteração pode ser feita em qualquer instância, ou réplica, do banco de dados. Então, essa alteração é replicada em todas as outras instâncias do banco de dados, em todos os controladores de domínio por toda a floresta.

Contudo, existem certas operações que não são convenientes para uma estratégia de múltiplos mestres. Por exemplo, a manipulação de alterações de senha de usuário é mais segura quando feitas por apenas um controlador de domínio e, então, replicadas em todos os outros controladores de domínio.

Quais são as funções de mestre de operações?

Para manipular os tipos de operações convenientes para atualizações por apenas um mestre, o Windows Server AD DS suporta a ideia de mestres de operações. Especificamente, existem cinco proprietários de função de mestre de operações, às vezes também chamadas de funções FSMO (flexible single master operations). Dois deles são mestres de operações em nível de floresta:

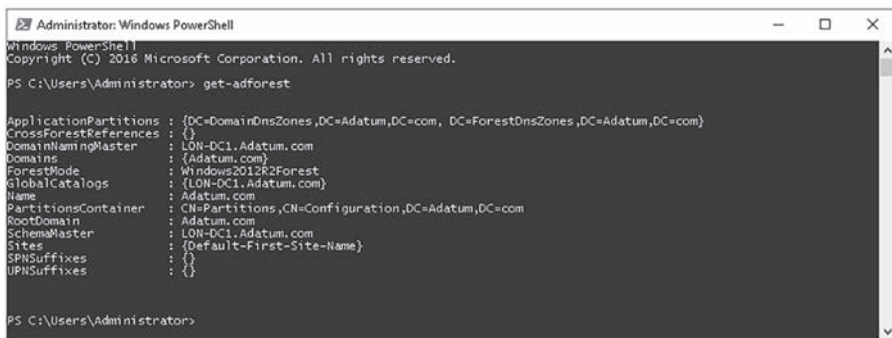
- **Mestre de esquema** O mestre de esquema mantém o esquema e é responsável por propagar quaisquer alterações feitas nele para as outras cópias dessa partição do AD DS em todos os outros controladores de domínio da floresta. Como o esquema raramente muda, a ausência temporária desse mestre de operações pode passar despercebida facilmente. Contudo, ele deve estar online quando você fizer mudanças no esquema, por exemplo, quando instalar um aplicativo, como o Exchange Server, que exige tipos de objeto e atributos adicionais em relação aos tipos de objeto existentes.
- **Mestre de nomeação de domínio** O mestre de nomeação de domínio manipula a adição ou a remoção de domínios na floresta do AD DS. Como esses tipos de alterações não são frequentes, se o mestre de nomeação de domínio ficar indisponível temporariamente, você pode não perceber isso imediatamente.



DICA DE EXAME

Por padrão, essas duas funções são atribuídas ao primeiro controlador de domínio da floresta do AD DS.

Para recuperar informações sobre os proprietários atuais da função de mestre de esquema e de nomeação de domínio, use o cmdlet `get-ADForest` do Windows PowerShell, como mostrado na Figura 1-31.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> get-adforest

ApplicationPartitions : {DC=DomainDnsZones,DC=Adatum,DC=com, DC=ForestDnsZones,DC=Adatum,DC=com}
CrossForestReferences : {}
DomainNamingMaster    : LON-DC1.Adatum.com
Domains               : {Adatum.com}
ForestMode             : Windows2012R2Forest
GlobalCatalogs        : {LON-DC1.Adatum.com}
Name                  : Adatum.com
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=Adatum,DC=com
RootDomain             : Adatum.com
SchemaMaster           : LON-DC1.Adatum.com
Sites                 : {Default-First-Site-Name}
SPNSuffixes            : {}
UPNSuffixes            : {}

PS C:\Users\Administrator>

```

FIGURA 1-31 Determinando as funções de mestre de operações da floresta atual.

Os mestres de operações restantes são em nível de domínio. Isso significa que cada domínio contém essas três funções de mestre de operações e que elas são específicas do domínio. São eles:

- **Emulador PDC** Executa várias operações importantes em nível de domínio:
 - Atua como fonte de sincronização de hora para o domínio
 - Propaga alterações de senha
 - Fornece uma fonte primária para GPOs para propósitos de edição
- **Mestre de infraestrutura** Mantém referências entre domínios e, consequentemente, essa função só é relevante em florestas com vários domínios. Por exemplo, o mestre de infraestrutura mantém a integridade da lista de controle de acesso de segurança de um objeto, quando essa lista contém entidades de segurança (security principals) de outro domínio.



DICA DE EXAME

Você não deve atribuir a função de mestre de infraestrutura a um servidor de catálogo global, a não ser que sua floresta consista de apenas um domínio. A única exceção a isso é se todos os controladores de domínio também são servidores de catálogo global, neste caso a função mestre de infraestrutura é redundante.

- **Mestre RID** Fornece blocos de identificações para cada um dos controladores de domínio em seu domínio. Cada objeto em um domínio exige um identificador única.



DICA DE EXAME

Por padrão, todas essas funções são atribuídas ao primeiro controlador de domínio promovido em determinado domínio.

Para recuperar informações sobre os proprietários atuais da função de mestre de infraestrutura, RID e emulador PDC, use o cmdlet `Get-AdDomain` do Windows PowerShell, como mostrado na Figura 1-32.