INSTITUTO DE ENSINO SUPERIOR - FACULDADE LABORO
TECNÓLOGO EM REDES DE COMPUTADORES

CALEBE ABRAÃO REIS DA SILVA
APOLO DE CARVALHO LIMA

WINDOWS SERVER 2016: ACTIVE DIRECTORY

TRABALHO DE CONCLUSÃO DE CURSO

SÃO LUÍS - MA
2019

CALEBE ABRAÃO REIS DA SILVA
APOLO DE CARVALHO LIMA

WINDOWS SERVER 2016: ACTIVE DIRECTORY

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Esp. Carlos Rayllan Lima Sousa

SÃO LUÍS - MA
2019

CALEBE ABRAÃO REIS DA SILVA
APOLO DE CARVALHO LIMA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Redes de Computadores da Faculdade Laboro, para obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em: / /

BANCA EXAMINADORA

_____

Prof. Esp. Carlos Rayllan Lima Sousa (Orientador)

_____

Prof. Ms. Milson Louseiro Lima

_____

Prof. Ms. Yanna Leidy Ketley Fernandes Cruz

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, pela força e coragem durante toda esta longa caminhada e a minha família por acreditar em mim.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Carlos Rayllan Lima Sousa, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala.

A Secretaria do Curso, pela cooperação.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

EPÍGRAFE

“Há pessoas que não gostam do capitalismo, e pessoas que não
gostam de PCs. Mas não existe ninguém que goste de PCs e não goste da Microsoft.”

William Henry (Bill Gates)

RESUMO

ABRAÃO - LIMA, Calebe e Apolo. **Windows Server 2012:** Active Directory. 2019. 20 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

Este trabalho descreve a instalação de um serviço de diretório ou mais conhecido como active directoty (serve a uma rede como um deposito central para armazenamento de informações, todas as informações são chamadas de objetos), utilizando-se do sistema operacional Windows Server e seu serviço de diretório no protocolo LDAP (Lightweight Directory Access Protocol), que em português significa protocolo leve de acesso a diretórios, utilizado em uma rede Windows, visando a resolução das dificuldades práticas e a criação de um tutorial. Dessa forma, os resultados funcionais obtidos farão parte de uma comparação de desempenho onde os administradores de rede que usam o active directory para organizar elementos de uma rede em uma estrutura corporativa hierárquica convivem no dia a dia.

Palavras-chave: AD DS, Permissões, AD, Diretório.

ABSTRACT

ABRAÃO - LIMA, Calebe e Apolo. **Windows Server:** Active Directory. 2019. 20 f. Trabalho de Conclusão de Curso (Graduação) – Tecnólogo em Redes de Computadores. Instituto de Ensino Superior – Faculdade Laboro. São Luís - MA, 2019.

This work describes the installation of a directory service or better known as active directoty (serving a network as a central storage location for information, all information is called objects), using the Windows Server operating system and its service directory in the Lightweight Directory Access Protocol (LDAP), which means a lightweight directory access protocol, used in a Windows network, to solve practical difficulties and create a tutorial. In this way, the obtained functional results will be part of a comparison of performance where the network administrators who use the active directory to organize elements of a network in a hierarchical corporate structure coexist in the day to day.

Keywords: AD DS, Permissions, AD, Directory.

LISTA DE FIGURAS

Figure 1. Instalando a função do Active Directory Domain Services 22
Figure 2. Adicionando uma nova floresta. 23
Figure 3. Adicionando uma nova floresta. 25
Figure 4. Configurando caminhos do AD DS. 26
Figure 5. Implantando controlador de domínio adicional em domínio existente. 28
Figure 6. Configurando opções controlador de domínio para controlador adicional. .30
Figure 7. Configurando opções adicionais do controlador de domínio. 30
Figure 8. Adicionando um novo domínio filho a uma floresta existente. 32
Figure 9. Adicionando um novo domínio filho a uma floresta existente. 34
Figure 10. Removendo o AD DS. 35
Figure 11. Rebaixando um controlador de domínio. 36
Figure 12. Removendo componentes opcionais. 36
Figure 13. Criando um snapshot NTDS para IFM. 39
Figure 14. As pastas criadas para um snapshot do AD DS. 40
Figure 15. Escolhendo a opção Instalar da Mídia. 40
Figure 16. Configurando opções do RODC. 43
Figure 17. Instalando um RODC. 44
Figure 18. Configurar um servidor de catálogo global. 47
Figure 19. Ativando a propriedade do Servidor de Catálogo Global. 47
Figure 20. Obtendo uma lista de controladores de domínio. 48
Figure 21. Configurando um DC como um servidor de catálogo global. 48
Figure 22. Adicionando atributos ao catálogo global. 50
Figure 23. Adicionando um servidor ao grupo de segurança. 51
Figure 24. Criando o DCCloneConfig.xml usando o Windows. 52
Figure 25. Importando uma máquina virtual. 53
Figure 26. Especificando um tipo de importação. 54
Figure 27. Especificando o local para os arquivos importados. 54
Figure 28. Especificando o local para os arquivos importados da máquina virtual. ..55
Figure 29. Verificando o nível funcional da floresta. 56
Figure 30. Verificando o nível funcional da floresta. 57
Figure 31. Centro administrativo do Active Directory. 59
Figure 32.Usuários e computadores do Active Directory. 59
Figure 33. Adicionando conta de usuário. 60
Figure 34. Configurando opções de senha e conta. 61
Figure 35. Modificando propriedades da conta do usuário. 62
Figure 36. Modificando propriedades do perfil do usuário. 63
Figure 37. Aplicando opções de perfil de usuário. 63
Figure 38. Modificando participações em grupos. 64
Figure 39. Renomeando conta de usuário. 66
Figure 40. Adicionando um computador ao domínio. 69
Figure 41. Concluindo o processo de adição ao domínio. 69

Figure 42. Movendo a conta do computador. 70
Figure 43. Adicionando grupo. 73
Figure 44. Configurando o grupo. 73
Figure 45. Atribuindo um gerente de grupo. 74
Figure 46. Adicionando uma OU. 76
Figure 47. Configurando uma conta de serviço. 79
Figure 48. Configurando uma conta virtual para um serviço. 82
Figure 49. Exibindo objetos de diretiva de grupo padrão 83
Figure 50. Editando diretivas de conta na diretiva de 83
Figure 51. Delegando o gerenciamento de configurações 85
Figure 52. Criando e aplicando um PSO com o Windows PowerShell. 87
Figure 53. Incluindo um Nó de Navegação. 88
Figure 54. Selecionando o contêiner de configurações de senha. 88
Figure 55. Criando um novo PSO. 89
Figure 56. Selecionando o grupo ao qual o PSO está vinculado. 89
Figure 57. Parando o serviço dos Serviços de Domínio Active 90
Figure 58. Remoção forçada de um controlador de domínio. 92
Figure 59. Excluindo o objeto de configurações NTDS. 93
Figure 60. Habilitando a Lixeira do Active Directory. 94
Figure 61. Exibindo objetos excluídos na lixeira do Active Directory. 95
Figure 62. Instalando o Backup do Windows Server. 98
Figure 63. Selecionando os itens para backup. 99
Figure 64. Selecionando o estado do sistema para backup, ... 100
Figure 65. Especificando o Destino de Backup. 100
Figure 66. Configurando uma política de replicação de senha do RODC. 104
Figure 67. Especificando a política de permissão. 104
Figure 68. Visualizando um Objeto de Conexão. 108
Figure 69. Executando Repadmin. 109

LISTA DE TABELAS

Tabela 1. Cmdlets do Windows PowerShell para gerenciamento de usuários. 67
Tabela 2. Os cmdlets de gerenciamento de computador do Windows PowerShell...70
Tabela 3. Cmdlets do Windows PowerShell para gerenciamento de grupos. 74
Tabela 4. Cmdlets do Windows PowerShell para gerenciamento de OU.....75

LISTA DE ABREVIATURA E SIGLAS

IP – Internet Protocol

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

LAN – Local Area Network

QoS – Quality of Service

TCP – Transmission Control Protocol

SLA – Service Level Agreement

AD DS – Active directory domain service

AD – Active Directory (Diretório Ativo)

VPN – Virtual Private Network

LDAP – Lightweight Directory Access Protocol (Protocolo leve de acesso a Diretórios)

SUMÁRIO

1. INTRODUÇÃO 14
2. Justificativa 15
3. Objetivos 16
   3.1. Geral 16
   3.2. Específicos 16
4. Fundamentação teórica 16
5. Metodologia 18
6. INSTALAÇÃO E CONFIGURAÇÃO DO AD DS 19
   6.1. Instalação e configuração do controlador de domínio. 19
      6.1.1. Fundamentos do AD DS 19
      6.1.2. Instale uma nova floresta 22
      6.1.3. Adicionar ou remover um controlador de domínio 27
      6.1.4. Instale o AD DS em uma instalação Server Core 37
      6.1.5. Instale e configure um controlador de domínio somente leitura 41
      6.1.6. Configurar um servidor de catálogo global 46
      6.1.7. Criando um clone 50
      6.1.8. Atualizar controladores de domínio 55
   6.2. Criar e gerenciar usuários e computadores do Active Directory 57
      6.2.1. Criar, copiar, configurar e excluir usuários e computadores 58
   6.3. Criar e gerenciar grupos do Active Directory e unidades organizacionais ... 71
      6.3.1. Criar, configurar e excluir grupos 72
      6.3.2. Criar e gerenciar OUs 75
7. Gerenciar e manter o AD DS 76
   7.1. Configure a autenticação de serviço e políticas de conta 76
      7.1.1. Criar e configurar MSAs e gMSAs 77
      7.1.2. Gerenciar SPNs 79
      7.1.3. Configurar delegação restrita de Kerberos 80
      7.1.4. Configurar contas virtuais 81
      7.1.5. Configurar diretivas de conta 82
      7.1.6. Delegar gerenciamento de configurações de senha 85
      7.1.7. Configurar e aplicar objetos de configurações de senha 86
   7.2. Manter o Active Directory 90
      7.2.1. Gerenciar o Active Directory off-line 90

7.2.2. Backup e recuperação do Active Directory 94
7.2.3. Gerenciar controladores de domínio somente leitura 103
7.2.4. Gerenciando a replicação do AD DS 106
8. Conclusão 113
Referência 115

1. INTRODUÇÃO

Nos dias de hoje no campo da TI (Tecnologia da Informação), o AD (Active Directory) exerce uma grande função para os profissionais de tecnologia. O AD fornece acesso a equipamentos encontrados na rede chamados de objetos como: impressoras e arquivos que guardados em seus diretórios com seus respectivos atributos. Além de que, é visto como um local de armazenamento centralizado para contas de usuários, adesões, acesso e configurações de softwares.

Um serviço de diretório é um software que armazena e organiza informações sobre os recursos e os usuários de uma rede de computadores, e que permite aos administradores de rede gerenciar o acesso de usuários e sistemas a esses recursos. Além disso, os serviços de diretório atuam como uma camada de abstração entre os usuários e esses recursos.

O serviço do AD DS é um software que mesmo sendo pago permite as companhias baixar, significativamente, os custos com gerenciamento, gerando um único espaço para os usuários, grupos e recursos de rede. O Active Directory foi criado pela Microsoft. Está em uso desde a versão Windows Server 2000. O principal protocolo utilizado é o LDAP, responsável pelo acesso rápido as informações de diretórios. A relação entre AD e LDAP é muito parecida com a relação entre o Apache e HTTP. LDAP é um protocolo de serviços de diretório. Active Directory é um servidor de diretório que usa o protocolo LDAP. Active Directory é apenas um exemplo de um serviço de diretório que suporta LDAP.

Este trabalho irá explorar as questões correlacionadas a esta tecnologia em um ambiente simples, com a utilização de um cliente Windows 10, que trabalhará com um servidor Windows.

2. JUSTIFICATIVA

Este trabalho foi motivado pela curiosidade de testar e avaliar funcionalidades típicas do Active Directory e verificar seus desempenhos. A compreensão da tecnologia do AD DS é importante devido à popularidade do sistema operacional Windows.

O Active Directory permite o uso de um único diretório para controle de acesso a todos sistemas e serviços dentro de uma rede corporativa. Isso significa que o colaborador de uma empresa não precisa criar um usuário e senha para cada sistema que tiver acesso, e sim utilizar seu usuário e senhas únicos(as).

- Autenticação centralizada
- Nível de segurança controlado
- Facilita a Delegação de tarefas administrativas
- Torna eficiente o gerenciamento de acesso
- Proporciona um índice dos recursos na rede
- Subdivisão de domínios em unidades lógicas
- Fornece recursos de replicação de dados
- Facilita a atribuição e manutenção de múltiplos domínios
- Unificação do sistema de nomes baseado em DNS
- Facilita a implementação de políticas de utilização (Políticas de Grupos).

A partir do domínio da tecnologia AD sobre o servidor Windows, é possível usufruir de todas as vantagens das ferramentas que o active directory disponibiliza.

Seria importante a elaboração de uma apostila didática sobre o tema active directory, que poderia está disponível aos alunos do curso de Redes de Computadores da Faculdade Laboro, tornando-se um material de estudo

complementar do aluno, uma vez que possuiria alguns descritivos das operações, fazendo o aprendizado mais direto e simples.

3. OBJETIVOS

3.1. Geral

Propor um serviço de diretório (Active Directory) atraves do serviço do Windows Server, elaborando um tutorial de implementação simples.

3.2. Específicos

Integralizar o Active Directory com serviço de rede local.

Apresentar as ferramentas em um cenário virtual

Validar a implementação do ambiente proposto

Efetivar o referencial teórico sobre o AD DS (Active Directory Domain Controller)

Implementar Active Directory em um laboratório com sistemas Windows.

4. FUNDAMENTAÇÃO TEÓRICA

Nosso roteiro para o referencial teórico é a base para alcançar o conhecimento sugerido, abordando o tema de acordo com Histórico do conceito/conceitos centrais; Apresentação de abordagens de diferentes autores; Análise comparativa dos autores.

O Microsoft Active Directory foi lançado em 1999 com o Windows 2000 Server Edition. Segundo a Microsoft (WINDOWS SERVER, 2014), historicamente, os seus principais recursos eram:

- Grupos universais: Tanto para grupos de segurança e distribuição.
- Aninhamento de grupos+
- Conversão de grupos: Permite a conversão entre grupos de segurança.
- distribuição
- Identificadores de segurança (SID)

O Active Directory foi lançado oficialmente em 1999 com o Windows 2000 Server. Já são 20 anos de vida.

O objetivo principal de uma rede de dados é compartilhar informações. Mas esse compartilhamento requer medidas de segurança a fim de evitar que pessoas não autorizadas tenham acesso a determinadas informações. Essa medida de segurança chama-se “Identidade e Acesso” (Identity and Access ou simplesmente, IDA).

Tendo o conceito em mente, o próximo passo era criar um repositório para armazenar as informações de IDA. Este repositório foi chamado de “Serviço de Diretório de Rede” (Network Directory Services ou mais comumente, Directory Services).

O objetivo do Serviço de Diretório é armazenar, organizar, gerenciar e compartilhar informações e recursos comuns de rede, como: usuários, grupos, computadores, impressoras, pastas compartilhadas, entre outros. Cada um desses recursos citados é considerado como um objeto dentro do diretório. Informações sobre um recurso em particular são armazenadas como atributos daquele objeto.

Com o Active Directory (AD), a Microsoft deu um salto gigantesco e trouxe novos conceitos, novas funcionalidades e novas tecnologias ao seu Serviço de Diretório. Dentre eles:

- A promoção ou demoção de um Controlador de Domínio passou a ser realizada sem a necessidade de reinstalação do sistema operacional;
- O acesso às informações do Diretório foi facilitado através de métodos mais simplificados de segurança e interfaces de acesso, o que permitiu maior integração com aplicações baseadas em servidor e a utilização de login único (Single Sign-On – SSO) para acesso a vários serviços de rede.

Segundo o docs.microsoft.com (página inicial da documentação da Microsoft para usuários finais, desenvolvedores e profissionais de TI.), o Active Directory armazena informações sobre objetos na rede e facilita para os administradores e usuários a localizar e usar essas informações. Active Directory usa um armazenamento de dados estruturados como base para uma organização lógica e hierárquica de informações de diretório.

Foram utilizados conceitos para implementação da segurança em um ambiente com uma versão recente do sistema operacional e com base nas estações de trabalhos utilizando o sistema operacional Windows Server.

5. METODOLOGIA

Este trabalho foi elaborado no intuito da construção do conhecimento e na sua posterior difusão, sob o formato de um tutorial. A pesquisa descritiva realiza um estudo detalhado, com levantamento de informações através de livros (Identity with Windows server 2016 Exam Ref 70-742) e fontes na internet com por exemplo o docs.microsoft encontrado no site da Microsoft.

A liderança do Windows no mercado continua indisputável. São 86,20% dos desktops com o sistema operacional em dezembro. MacOS conta com 10,65% de presença e o Linux apenas 2,78%.

Segundo resultados de pesquisa da Net Applications, o Windows 10 enfim ultrapassou o Windows 7 em fatia de mercado, o que significa que ele se tornou o sistema operacional mais usado em computadores desktop no mundo, três anos após o seu lançamento oficial.

A adoção do Windows 10 começou bem rápida, ainda mais com a Microsoft promovendo agressivamente o update do sistema, através da atualização gratuita e muita propaganda. O update gratuito parou de ser oferecido em julho de 2016, o que fez com que o crescimento da adoção diminuísse muito de ritmo. Ainda assim, a presença do Windows 10 em computadores desktop continuou crescendo até atingir 39,22% da fatia de mercado mundial em dezembro passado, segundo a Net Applications.

A importância do Active Directory nasce principalmente no uso majoritário do sistema operacional Windows a nível mundial, conhecer a tecnologia do AD é essencial para os profissionais e estudantes do ramo de tecnologia da informação. Buscou -se sempre informações e avaliações idôneas.

A todo momento e em todas as etapas serão observadas e respeitadas todas as diretrizes legais incluídas, o material não implica em qualquer tipo de ilícito.

6. INSTALAÇÃO E CONFIGURAÇÃO DO AD DS

6.1. Instalação e configuração do controlador de domínio.

6.1.1. Fundamentos do AD DS

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

O AD DS consiste nos seguintes componentes lógicos:

- **Floresta** Uma floresta é uma coleção de domínios do AD DS que compartilham um esquema comum e são vinculados por relações de confiança bidirecionais criadas automaticamente. A maioria das organizações escolhe implementar o AD DS com uma única floresta. Os motivos para usar várias florestas incluem o requerimento para:
  - Proporcione uma separação administrativa completa entre partes díspares da sua organização.
  - Ofereça suporte a diferentes tipos de objetos e atributos no esquema do AD DS em diferentes partes da sua organização.
- **Domínio** Um domínio é uma unidade administrativa lógica que contém usuários, grupos, computadores e outros objetos. Vários domínios podem fazer parte de uma ou várias florestas, dependendo de suas necessidades organizacionais. Relações pai-filho e confiança definem sua estrutura de domínio.
- **Árvore** Uma árvore é uma coleção de domínios do AD DS que compartilham um domínio raiz comum e têm um espaço para nome contíguo. Por exemplo, sales.adatum.com e marketing.adatum.com compartilham a raiz comum adatum.com; eles também compartilham um namespace contíguo, adatum.com. Você pode criar sua floresta do AD DS usando uma única árvore ou pode usar várias árvores. Os motivos para o uso de várias árvores incluem o requisito de

suporte a vários namespaces lógicos em sua organização, talvez devido a fusões ou aquisições.

- **Esquema** O esquema do AD DS é a coleção de tipos de objetos e suas propriedades, também conhecidas como atributos, que definem os tipos de objetos que você pode criar, armazenar e gerenciar na floresta do AD DS. Por exemplo, um usuário é um tipo de objeto lógico e possui várias propriedades, incluindo um nome completo, um departamento e uma senha. O relacionamento entre objetos e seus atributos é mantido no esquema, e todos os controladores de domínio em uma floresta mantêm uma cópia do esquema.
- **OU** Uma OU é um contêiner dentro de um domínio que contém usuários, grupos, computadores e outras unidades organizacionais. Eles são usados para fornecer simplificação administrativa. Com UOs, você pode delegar facilmente direitos administrativos a uma coleção de objetos, agrupando-os em uma UO e atribuindo o direito a essa UO. Você também pode usar objetos de diretiva de grupo (GPOs) para definir configurações de usuário e computador e vincular essas configurações de GPO a uma UO, simplificando o processo de configuração. Uma OU é criada por padrão quando você instala o AD DS e cria um domínio: Controladores de Domínio
- **Container** Além das OUs, você também pode usar contêineres para agrupar coleções de objetos. Há vários contêineres internos, incluindo: Computadores, Construídos e Contas de Serviço Gerenciado. Você não pode vincular GPOs a contêineres.
- **Site** Um site é uma representação lógica de um local físico dentro da sua organização. Pode representar uma grande área física, como uma cidade, ou pode representar uma área física menor, como uma coleção de sub-redes definidas pelos limites do seu datacenter. Os sites do AD DS ajudam a permitir que os dispositivos em rede determinem onde eles estão em relação aos serviços com os quais desejam se conectar. Por exemplo, um computador com Windows 10 é inicializado, ele usa o local determinado do site para tentar encontrar um controlador de domínio adjacente para dar suporte à entrada do usuário. Os sites também permitem controlar a replicação do AD DS, configurando um agendamento e intervalo de replicação entre sites.

- **Sub-rede** Uma sub-rede é uma representação lógica de uma sub-rede física em sua rede. Ao definir sub-redes, você possibilita que um computador na floresta do AD DS determine sua localização física em relação aos serviços oferecidos na floresta. Nenhuma sub-rede existe 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 seus controladores de domínio. Como algumas partes do seu AD DS são alteradas com pouca frequência, enquanto outras são alteradas com frequência, várias partições separadas são armazenadas no banco de dados do AD DS.

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

Essas partições separadas são:

- **Esquema** Uma partição no nível da floresta, que muda raramente. Contém o esquema da floresta do AD DS.
- **Configuração** Uma partição no nível da floresta que muda raramente, esta partição contém os dados de configuração para a floresta.
- **Domínio** Partição no nível do domínio. Essa partição muda com freqüência e uma cópia gravável da partição é armazenada em todos os controladores de domínio. Ele contém os objetos reais, como usuários e computadores, existentes na sua floresta.
- **Relacionamentos de confiança** Um relacionamento de confiança, também às vezes chamado de confiança, é um contrato de segurança entre dois domínios em uma floresta do AD DS, entre duas florestas ou entre uma floresta e uma região de segurança externa. Este contrato de segurança permite que um usuário em um lado da confiança tenha acesso aos recursos do outro lado da confiança. Em uma relação de confiança, uma parte é considerada confiante, enquanto a outra é considerada confiável. A entidade de retenção de recursos é confiável, enquanto a entidade de retenção de usuário é confiável. Para ajudar a

entender isso, considere quem é confiável e confiante quando você empresta a alguém as chaves do seu carro.

6.1.2. Instale uma nova floresta

Para instalar uma nova floresta do AD DS, você deve implantar o primeiro controlador de domínio nessa floresta. Isso significa implantar a função de servidor AD DS em um computador servidor com Windows Server 2016 e, em seguida, promover o servidor em um controlador de domínio e escolher a opção Adicionar uma nova floresta.

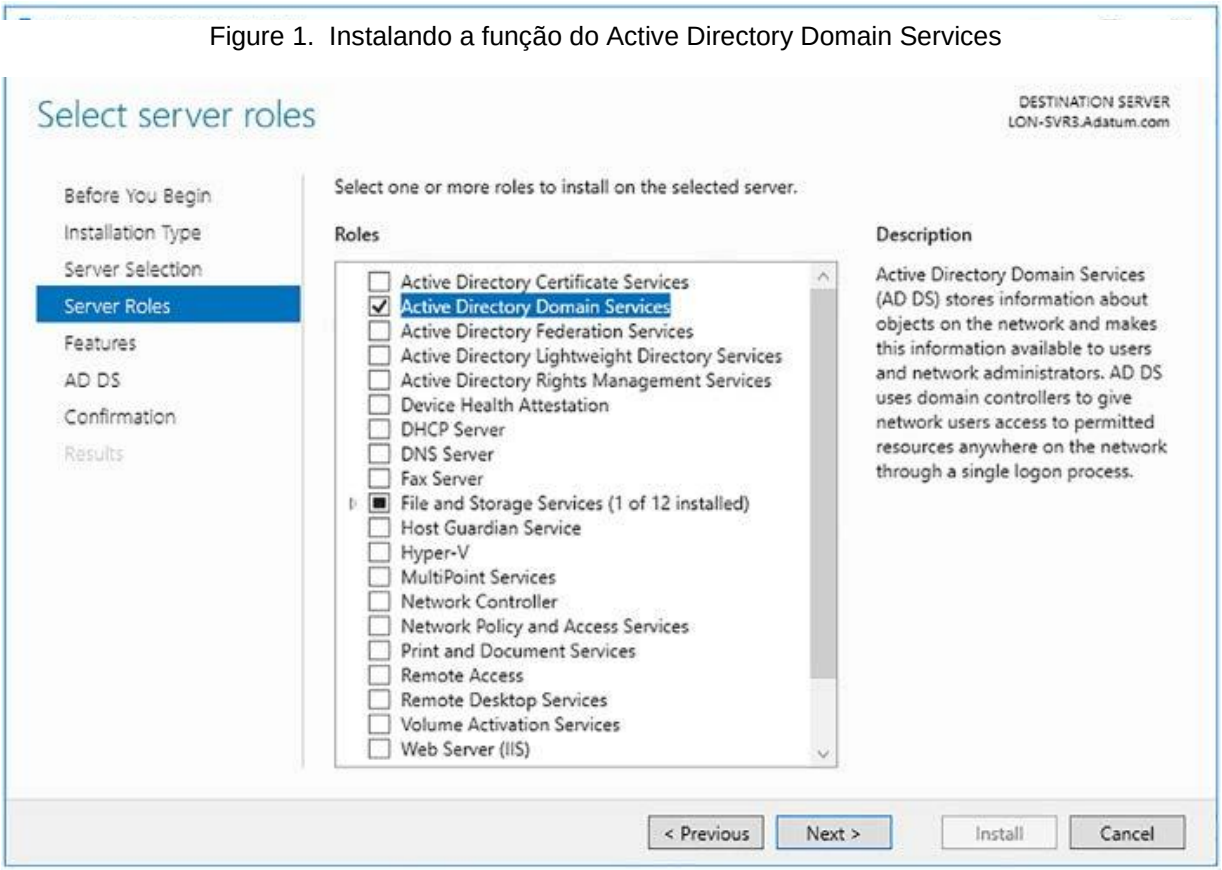
Para criar uma nova floresta, comece instalando a função do AD DS usando o seguinte procedimento:

1. Entre no computador com Windows Server 2016 como administrador local.

2. Inicie o Gerenciador do Servidor e, no Painel, clique em Adicionar Funções e Recursos.

3. Clique no Assistente para Adicionar Funções e Recursos e, como mostra a Figura 1, na página Funções do Servidor, marque a caixa de seleção Serviços de Domínio Active Directory, clique em Clique em Adicionar recursos, e

Figure 1. Instalando a função do Active Directory Domain Services



depois clique avançar.

Fonte: (Warren, 2017, p. 5)

4. Clique no restante do assistente e, quando solicitado, clique em Instalar.

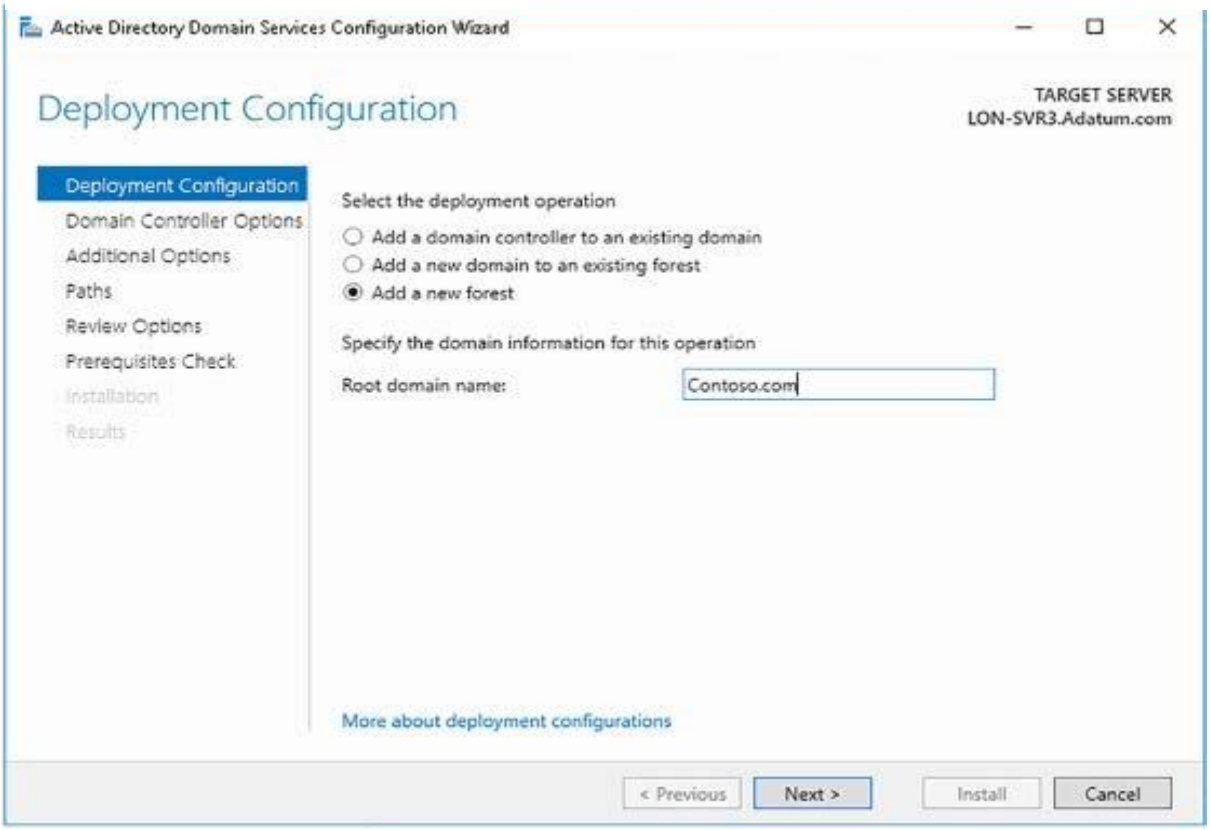
5. Quando a instalação estiver concluída, clique em Fechar.

Depois de instalar os binários do AD DS, você deve criar uma nova floresta promovendo o primeiro controlador de domínio na floresta. Para fazer isso, use o seguinte procedimento:

1. No Gerenciador do Servidor, clique no triângulo de aviso amarelo em Notificações e clique em Promover este servidor em um controlador de domínio.

2. No Assistente de Configuração dos Serviços de Domínio Active Directory, na página Configuração de Implantação, em Selecione A Operação de Implantação, clique em Adicionar Uma Nova Floresta e digite o nome do domínio

Figure 2. Adicionando uma nova floresta.



raiz da floresta, como mostra a Figura 2.

Fonte: (Warren, 2017, p. 6)

3. Clique em Avançar. Na página Opções do Controlador de Domínio, como mostra a Figura 3, configure as seguintes opções e clique em Avançar:

Nível funcional da floresta: O nível funcional da floresta determina quais recursos no nível da floresta estão disponíveis em sua floresta. O nível funcional da floresta também define o nível funcional mínimo do domínio para domínios na sua floresta. Portanto, escolher o Windows Server 2012 nesse nível significa que o nível funcional mínimo do domínio 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.

Nível funcional do domínio: Determina os recursos em nível de domínio disponíveis neste domínio. Escolher entre:

Windows Server 2008.

Windows Server 2008 R2.

Windows Server 2012.

Windows Server 2012 R2.

Windows Server 2016.

Servidor DNS: (sistema de nomes de domínio) O DNS fornece resolução de nomes e é um serviço crítico para o AD DS. Esta opção está selecionada por padrão e, a menos que você já tenha uma infraestrutura DNS configurada, não desmarque essa opção.

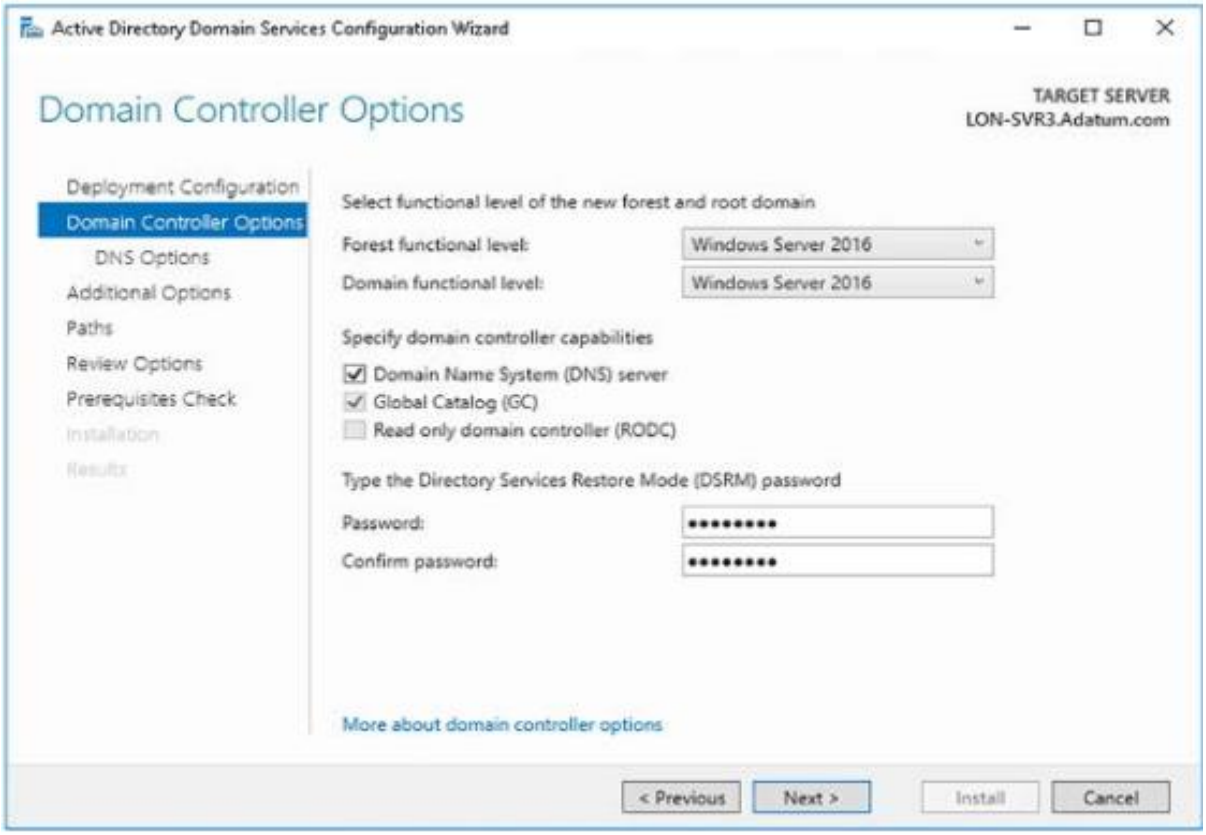
Catálogo Global (GC): Os servidores de catálogo global fornecem serviços em toda a floresta. Eles são selecionados por padrão e não podem ser desmarcados. O primeiro (e único) controlador de domínio deve ser um servidor de

catálogo global. Quando você adicionar controladores de domínio adicionais, poderá revisar essa configuração.

Controlador de domínio somente leitura (RODC): Determina se esse controlador de domínio é um controlador de domínio somente leitura. Essa opção não está selecionada por padrão e não está disponível para o primeiro (e atualmente somente) controlador de domínio em sua floresta.

Senha do modo de restauração dos serviços de diretório (DSRM):

Figure 3. Adicionando uma nova floresta.



Usado quando você inicia o controlador de domínio em um modo de recuperação.

Fonte: (Warren, 2017, p. 7)

4. Na página Opções Adicionais, defina o nome do domínio NetBIOS. O protocolo NetBIOS não é mais amplamente usado e é baseado em uma estrutura de nomeação 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 é padronizado como CONTOSO; geralmente, você não precisa alterar isso. Clique em Next.

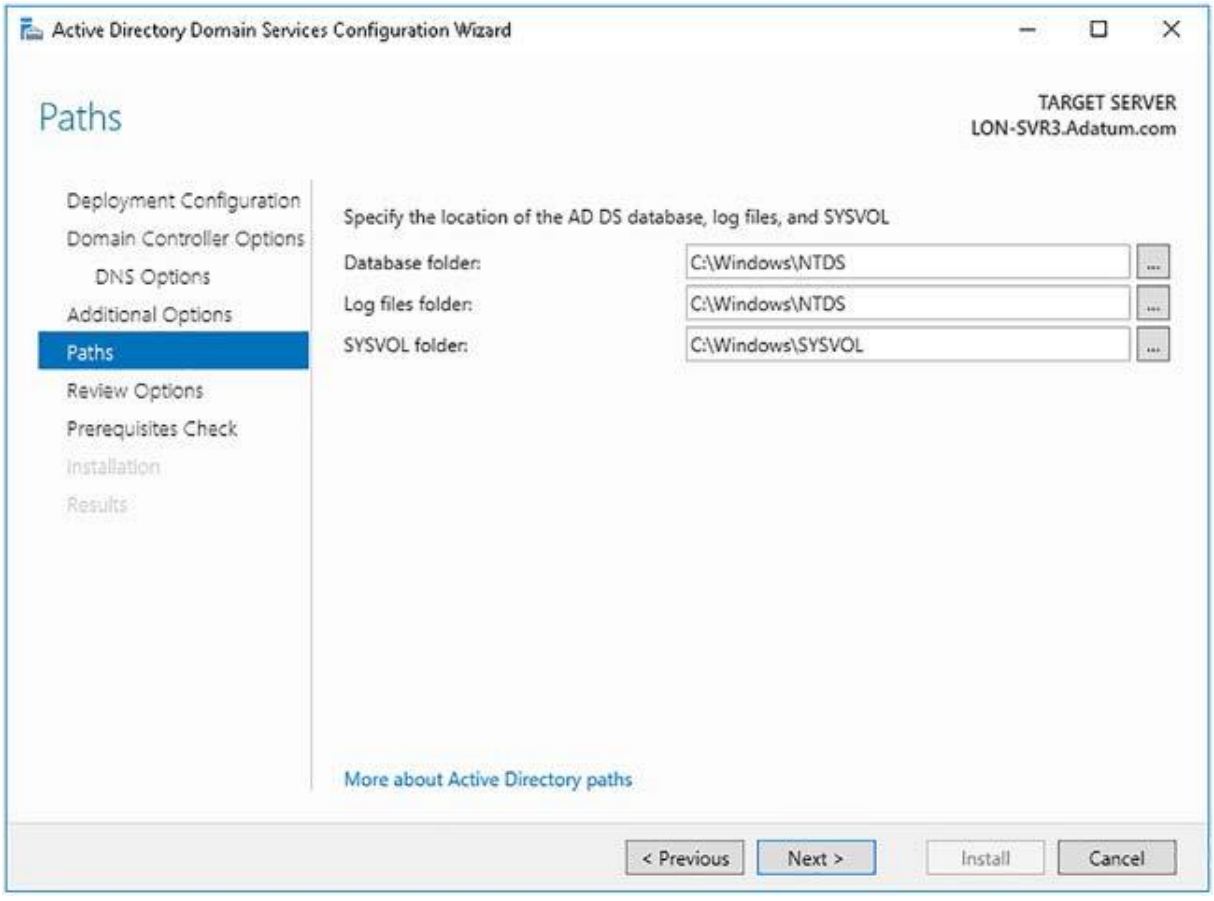
5. Como mostra a Figura 4, defina o local para armazenar o banco de dados do AD DS, os arquivos de log e conteúdo do SYSVOL e clique em Avançar. Os padrões são:

Pasta do banco de dados: C: \ Windows \ NTDS.

Pasta de arquivos de log: C: \ Windows \ NTDS.

Pasta SYSVOL: C: \ Windows \ SYSVOL.

Figure 4. Configurando caminhos do AD DS.



Fonte: (Warren, 2017, p. 8)

6. Revise as opções de configuração e clique em Avançar para executar verificações de pré-requisito.

7. Quando solicitado, clique em Instalar. O computador servidor reinicia durante o processo de instalação.

8. Entre no computador servidor usando a conta de administrador do domínio.

6.1.3. Adicionar ou remover um controlador de domínio

Depois de implantar o primeiro controlador de domínio em sua floresta do AD DS, você pode adicionar controladores de domínio adicionais para fornecer resiliência e desempenho aprimorado. O processo para implantar controladores de domínio adicionais é basicamente o mesmo do primeiro controlador de domínio: instale a função de servidor AD DS (usando o Gerenciador do Servidor ou o Windows PowerShell) e promova o controlador de domínio (novamente, usando o Gerenciador do Servidor ou o Windows PowerShell).

No entanto, as opções específicas que você seleciona durante o processo de promoção variam dependendo dos detalhes da implantação. Por exemplo, adicionar um novo controlador de domínio a um domínio existente é um pouco diferente de adicionar um novo controlador de domínio a um novo domínio.

Existem dois cenários básicos para adicionar um novo controlador de domínio:

Adicionar um novo controlador de domínio em um domínio existente:

Para concluir esse processo, você deve fazer login como membro do grupo de segurança global Admins. Do domínio do domínio de destino.

Adicionar um novo controlador de domínio em um novo domínio:

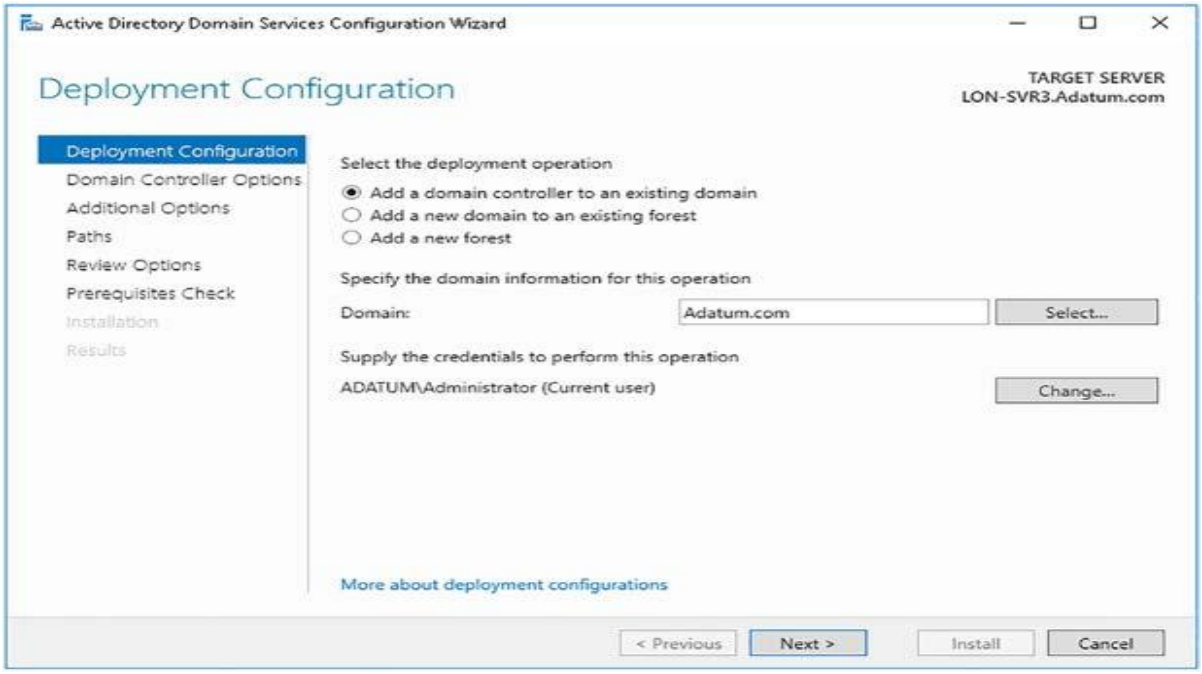
Para concluir esse processo, você deve entrar como membro do grupo de segurança universal Enterprise Admins raiz da floresta. Isso fornece privilégios suficientes para modificar a partição de configuração do AD DS e criar o novo domínio, como parte da árvore de domínio existente ou como parte de uma nova árvore de domínio.

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

Adicionar um novo controlador de domínio em um domínio existente

Para adicionar um novo controlador de domínio em um domínio existente, entre como administrador de domínio e execute o procedimento a seguir.

Figure 5. Implantando controlador de domínio adicional em domínio existente.



Fonte: (Warren, 2017, p. 10)

A entrada como membro do grupo de segurança global Admins. Do Domínio pressupõe que o computador servidor que você pretende promover seja um membro do domínio de destino. Caso contrário, é mais fácil adicionar o computador servidor ao domínio de destino primeiro e depois concluir o procedimento. Se você

decidir não adicionar o computador ao domínio de destino, deverá entrar como administrador local e fornecer credenciais de Administrador do Domínio durante o processo de promoção. Também é um requisito que o computador servidor que você está promovendo possa resolver nomes usando o serviço DNS na floresta do AD DS.

1. Adicione a função de servidor dos Serviços de Domínio Active Directory.

2. No Gerenciador do Servidor, clique em Notificações e clique em Promover este servidor para um controlador de domínio.

3. No Assistente de Configuração dos Serviços de Domínio Active Directory, na página Configuração de Implantação, como mostra a Figura 5, clique em Adicionar um controlador de domínio a um domínio existente.

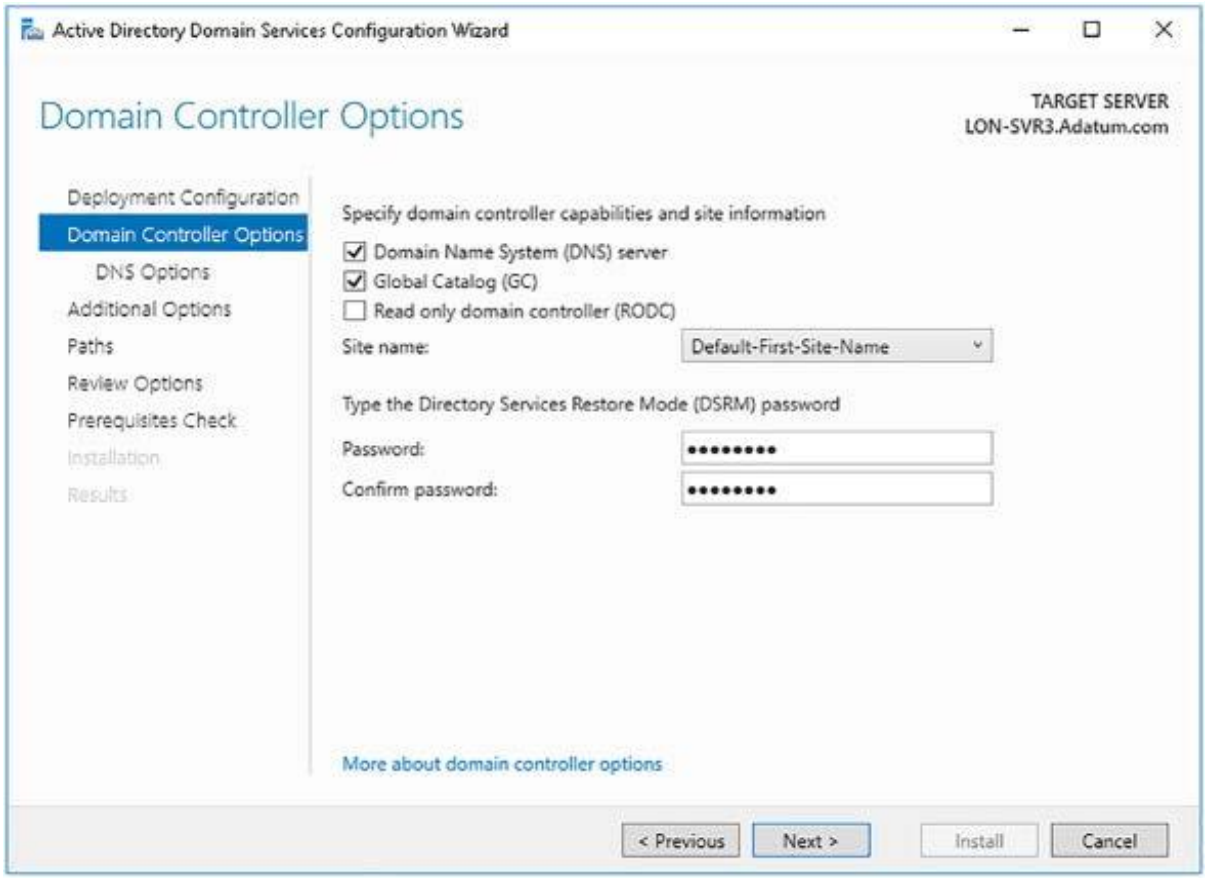
4. Especifique o nome do domínio. O nome padrão é o mesmo que o domínio ao qual o computador servidor pertence. No entanto, você pode selecionar outros domínios disponíveis na floresta.

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 Avançar.

6. Na página Opções do Controlador de Domínio, configure as opções de servidor DNS (Sistema de Nome de Domínio) (ativado por padrão), Catálogo Global (GC) (ativado por padrão) e Controlador de Domínio Somente Leitura (RODC) (não ativado por padrão). Diferente da promoção do primeiro controlador de domínio em uma floresta, você pode habilitar o controlador de domínio somente leitura (RODC) para tornar esse controlador de domínio um controlador de domínio somente leitura.

7. Na lista suspensa Nome do site, mostrada na Figura 6, selecione o site no qual esse controlador de domínio está fisicamente colocado. O padrão é Nome do Primeiro Site Padrão. Até você criar sites adicionais do AD DS, este é o único site

Figure 6. Configurando opções controlador de domínio para controlador adicional.



disponível. Você pode mover o controlador de domínio após a implantação.

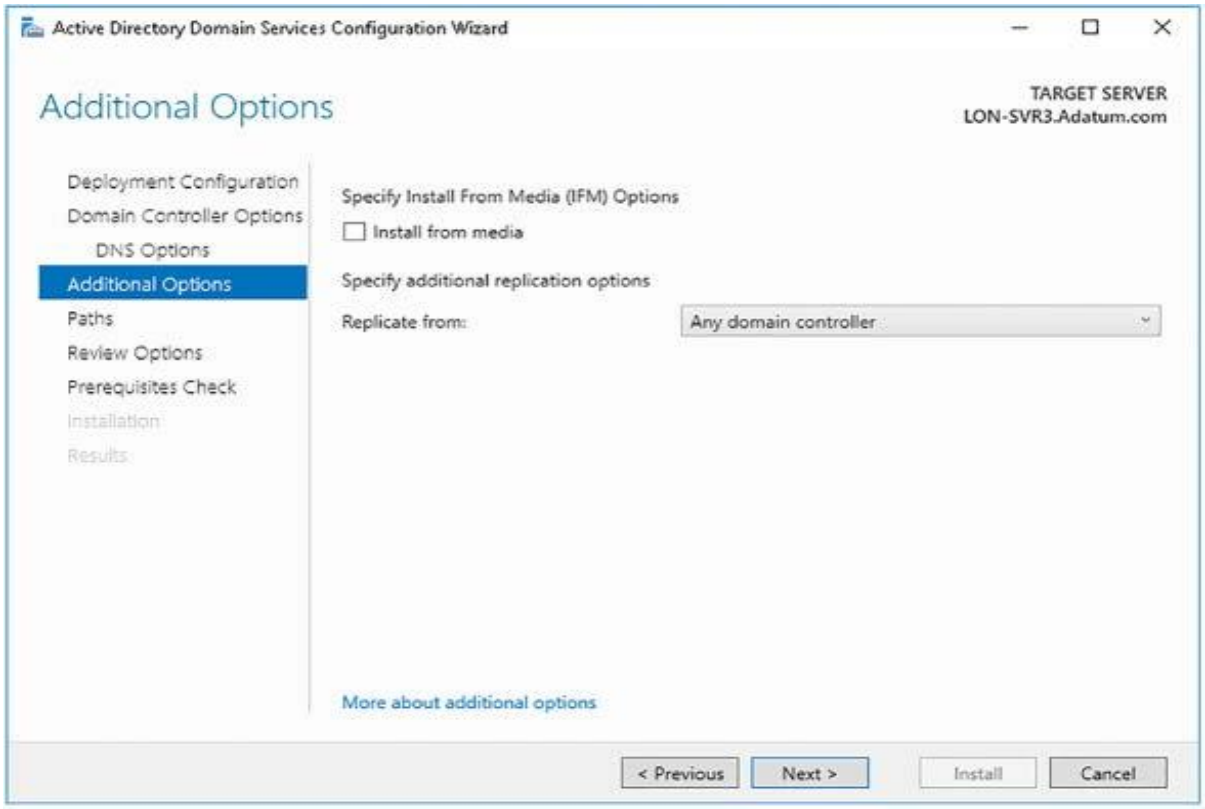
Fonte: (Warren, 2017, p. 11)

8. Digite a senha do modo de restauração dos serviços de diretório (DSRM) e clique em Avançar.

9. Na página Opções Adicionais, você deve configurar como esse controlador de domínio preenche o banco de dados do AD DS. Você pode configurar a população inicial de um controlador de domínio online, selecionando qualquer um dos Controladores de Domínio, como mostra a Figura 7, ou especificando um controlador de domínio específico. Como alternativa, você pode usar a opção

Figure 7. Configurando opções adicionais do controlador de domínio.

Instalar da Mídia (IFM). Clique em Avançar.



Fonte: (Warren, 2017, p. 12)

10. Configure os Caminhos, como antes, e clique no assistente de configuração.

11. Clique em Instalar quando solicitado. O computador servidor reinicia durante o processo de promoção.

Depois de concluir o processo de promoção, entre usando uma conta de administrador de domínio.

Adicionar um novo controlador de domínio em um novo domínio

Para adicionar um novo controlador de domínio a um novo domínio em uma floresta existente, entre como membro do grupo de segurança universal Administradores da Empresa da floresta e, em seguida, execute o procedimento a seguir.

Para entrar como membro do grupo de segurança universal de Administradores da Empresa, pressupõe que o computador servidor que você pretende promover seja membro de um dos domínios da floresta do AD DS. Caso

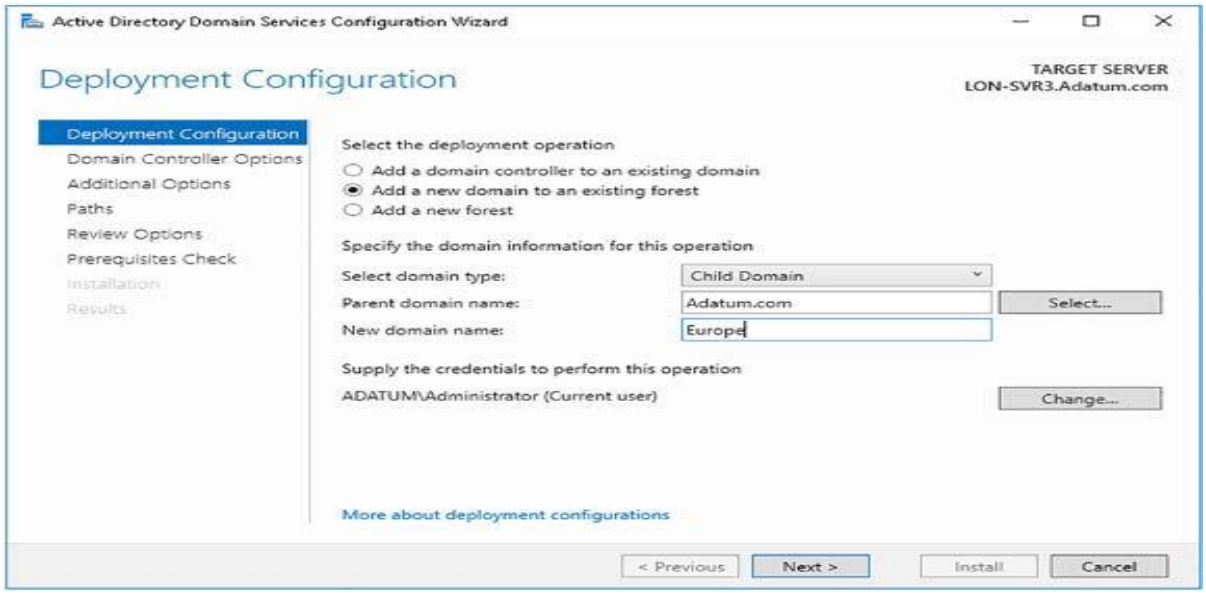
contrário, é mais fácil adicionar o computador servidor ao domínio raiz da floresta primeiro e concluir o procedimento. Se você decidir não adicionar o computador ao domínio raiz da floresta, deverá entrar como administrador local e fornecer credenciais de Administrador Corporativo durante o processo de promoção. Também é um requisito que o computador servidor que você está promovendo possa resolver nomes usando o serviço DNS na floresta do AD DS.

1. Adicione a função de servidor dos Serviços de Domínio Active Directory.

2. No Gerenciador do Servidor, clique em Notificações e clique em Promover este servidor para um controlador de domínio.

3. No Assistente de Configuração dos Serviços de Domínio Active Directory, na página Configuração de Implantação, como mostra a Figura 8, clique

Figure 8. Adicionando um novo domínio filho a uma floresta existente.



em Adicionar um novo domínio a uma floresta existente.

Fonte: (Warren, 2017, p. 13)

4. Você pode escolher como o novo domínio é adicionado. Você pode selecionar:

Domínio filho: A seleção dessa opção cria um subdomínio do domínio pai especificado. Em outras palavras, o novo domínio é criado na árvore de domínio existente.

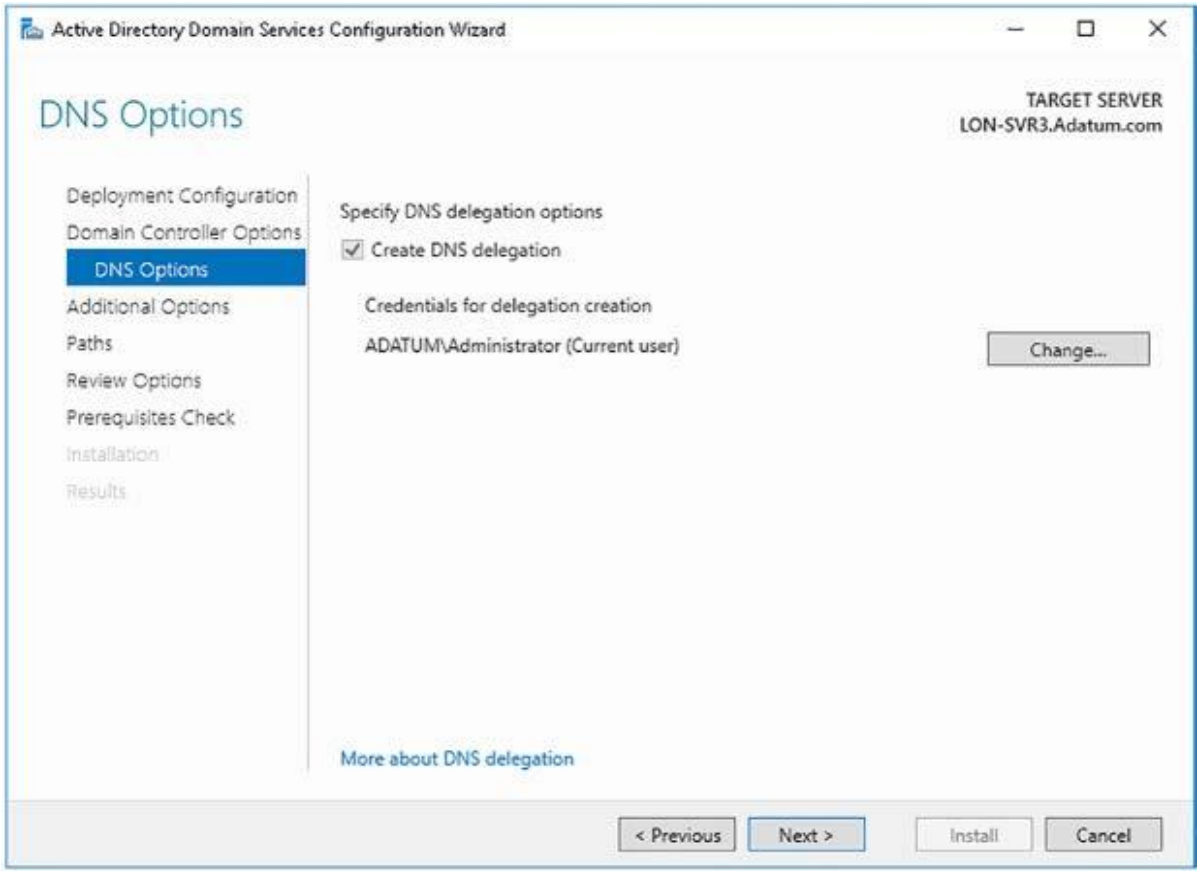
Domínio de árvore: Selecione esta opção se desejar criar uma nova árvore na mesma floresta. A nova árvore compartilha o mesmo esquema de floresta e tem o mesmo domínio raiz da floresta, mas você pode definir um espaço para nome não contíguo. Isso é útil quando você deseja criar vários nomes de domínio DNS na infraestrutura de floresta do AD DS para dar suporte às suas necessidades organizacionais, mas não precisa, ou deseja, separar a função administrativa possível com uma floresta separada. Se você escolher o Domínio da Árvore, deverá definir o domínio da floresta ao qual a árvore é adicionada. O padrão é a floresta na qual você está conectado.

5. Digite o novo nome de domínio. No caso de um domínio filho, o nome inclui o domínio pai como sufixo. Por exemplo, adicionar o domínio da Europa como filho do domínio Adatum.com cria o domínio Europa.Adatum.com. Se você criar uma nova árvore, poderá inserir qualquer nome de domínio DNS válido e ele não contém o domínio raiz da floresta. Clique em Avançar.

6. Na página Opções do Controlador de Domínio, selecione o nível funcional do domínio e defina as configurações de DNS, GC e RODC. Selecione o nome do site apropriado e, finalmente, digite a senha do DSRM e clique em Avançar.

7. Na página Opções de DNS, como mostrado na Figura 9, marque a caixa de seleção criar delegação de DNS. Isso cria uma delegação DNS para o subdomínio no seu espaço para nome DNS. Clique em Avançar.

Figure 9. Adicionando um novo domínio filho a uma floresta existente.



Fonte: (Warren, 2017, p. 14)

8. Especifique o nome de domínio NetBIOS e clique no assistente. Quando solicitado, clique em Instalar.

9. Seu controlador de domínio é reiniciado durante o processo de promoção. Entre como administrador de domínio após a conclusão do processo.

Removendo controladores de domínio

De tempos em tempos, pode ser necessário encerrar e remover um controlador de domínio. Este é um processo bastante simples e você pode usar o Gerenciador do Servidor para concluir a tarefa.

1. Entre usando uma conta com privilégios suficientes. Para remover um controlador de domínio de um domínio, entre como administrador de domínio. Para remover um domínio inteiro, entre como um membro do grupo de segurança universal de Administradores da Empresa.

2. Abra o Gerenciador do Servidor e, no menu Gerenciar, clique em Remover Funções e Recursos.

3. No Assistente para Remover Funções e Recursos, na página Antes de Começar, clique em Avançar.

4. Selecione o servidor apropriado na página Selecionar servidor de destino e clique em Avançar.

5. Na página Remover Funções do Servidor, desmarque a caixa de seleção Serviços de Domínio Active Directory, clique em Remover Recursos e, em seguida, clique em Avançar.

6. Na caixa de diálogo pop-up Resultados da validação, mostrada na

Figure 10. Removendo o AD DS.

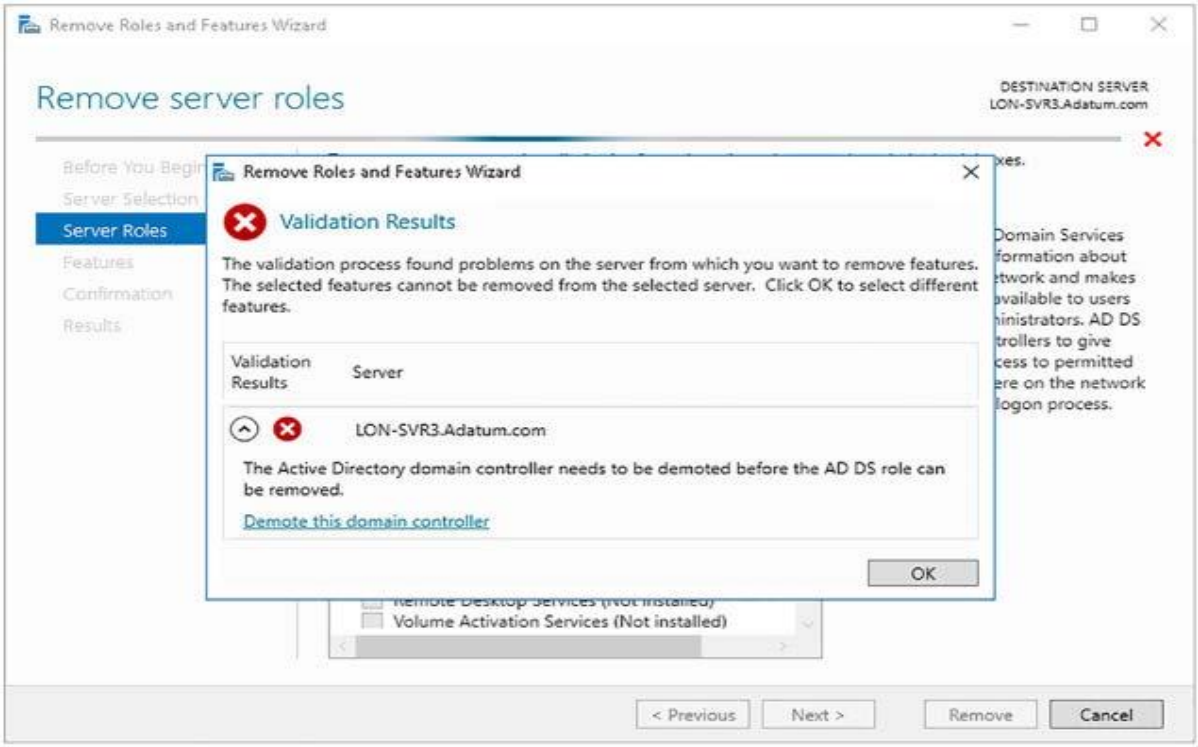
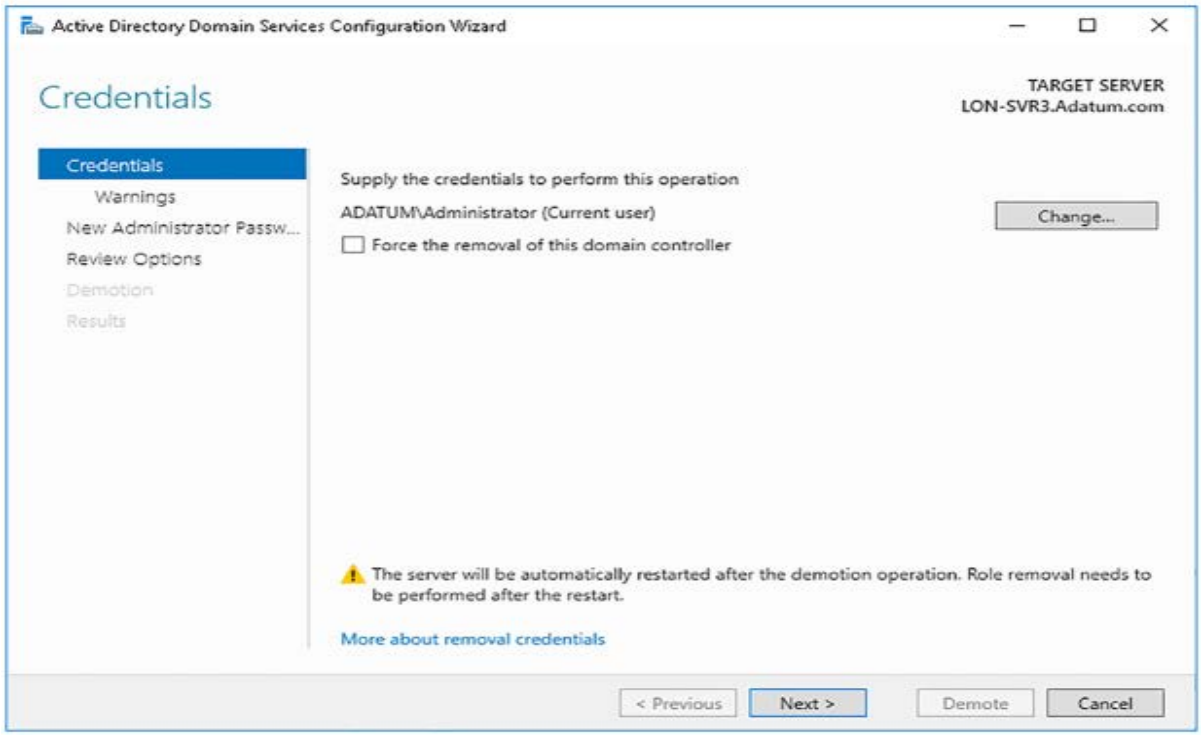


Figura 10, clique em Rebaixar este controlador de domínio.

Fonte: (Warren, 2017, p. 15)

7. O Assistente de Configuração dos Serviços de Domínio Active Directory é carregado, como mostra a Figura 11. Na página Credenciais, se necessário, especifique credenciais do usuário que tenham privilégios suficientes para executar a remoção. Não marque a caixa de seleção Forçar a remoção deste controlador de domínio, a menos que o controlador de domínio falhe e não possa ser contatado. Clique em Avançar.

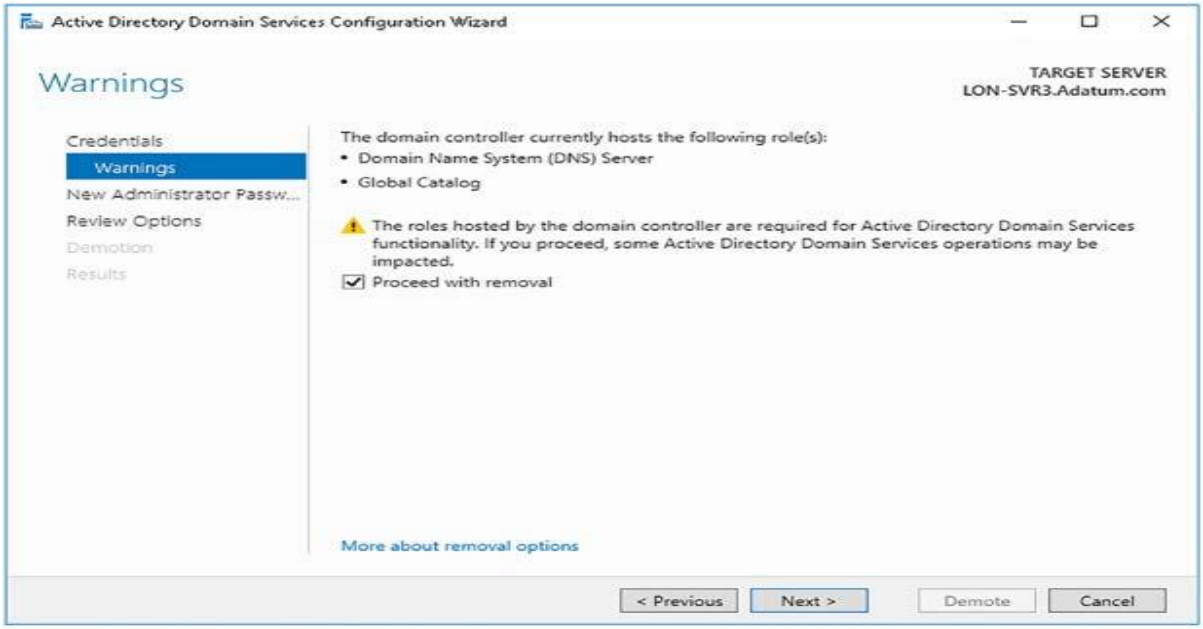
Figure 11. Rebaixando um controlador de domínio.



fonte: (Warren, 2017, p. 16)

8. Na página Avisos, mostrada na Figura 12, você é solicitado a confirmar a remoção das funções DNS e GC. Marque a caixa de seleção Continuar com

Figure 12. Removendo componentes opcionais.



remoção e clique em Avançar.

Fonte: (Warren, 2017, p. 16)

9. Na nova senha de administrador, digite e confirme a senha definida como a senha de administrador local e clique em Avançar.

10. Revise suas opções e clique em Rebaixar.

11. Seu servidor é rebaixado e reinicia. Faça login usando a conta de administrador local. Agora você pode verificar o rebaixamento adequado e a remoção da função. Em um controlador de domínio:

1.Em um controlador de domínio, abra Usuários e Computadores do Active Directory. Verifique se o controlador de domínio rebaixado não está mais listado na UO Controladores de Domínio.

2.Clique no recipiente Computadores. Você deve ver seu computador servidor rebaixado.

3. Abra sites e serviços do Active Directory. Expanda Sites, expanda o site Nome do Primeiro Site Padrão e, em Servidores, exclua o objeto que representa o servidor que você rebaixou.

Você também pode concluir o processo de rebaixamento usando o Windows PowerShell. Use os dois cmdlets a seguir para concluir o processo no prompt de comando do Windows PowerShell:

Uninstall-addsdomaincontroller.

Uninstall-windowsfeature AD-Domain_Services.

6.1.4. Instale o AD DS em uma instalação Server Core

Você pode implantar a função de servidor AD DS em uma instalação Server Core. Você pode usar o Gerenciador de servidores para instalar remotamente a função ou o cmdlet Windows PowerShell Install-Windows Feature AD-Domain-Services.

Depois de instalar os arquivos necessários, você pode iniciar o Assistente de Configuração dos Serviços de Domínio Active Directory no Server Manager para configurar remotamente a instalação Server Core ou usar o cmdlet Windows

PowerShell Install-ADDSDomainController para concluir o processo de promoção. Em outras palavras, o processo de instalação do AD DS em uma instalação Server Core do Windows Server 2016 é o mesmo de um servidor com o Desktop Experience.

Você não pode implantar a função de servidor AD DS no Nano Server. Consequentemente, você não pode usar um Nano Server como um controlador de domínio.

Instale um controlador de domínio usando Implantação de instalação da Mídia.

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

Essa sincronização inicial pode apresentar um desafio em algumas circunstâncias. Por exemplo, isso pode ser desafiador quando você está implantando um controlador de domínio em um local conectado à infraestrutura de rede da sua organização usando uma conexão de baixa largura de banda. Nessa situação, a sincronização inicial pode levar muito tempo ou usar uma proporção excessiva da largura de banda disponível.

Para atenuar isso, você pode optar por implantar um controlador de domínio e executar a sincronização inicial do AD DS usando uma cópia local ou instantâneo do banco de dados do AD DS; isso é conhecido como executar uma implantação de instalação da mídia (IFM). Há muitas etapas envolvidas nesse processo.

1. Em um controlador de domínio existente, usando o File Explorer, crie uma pasta, por exemplo C: \ IFM, para armazenar o instantâneo do AD DS.

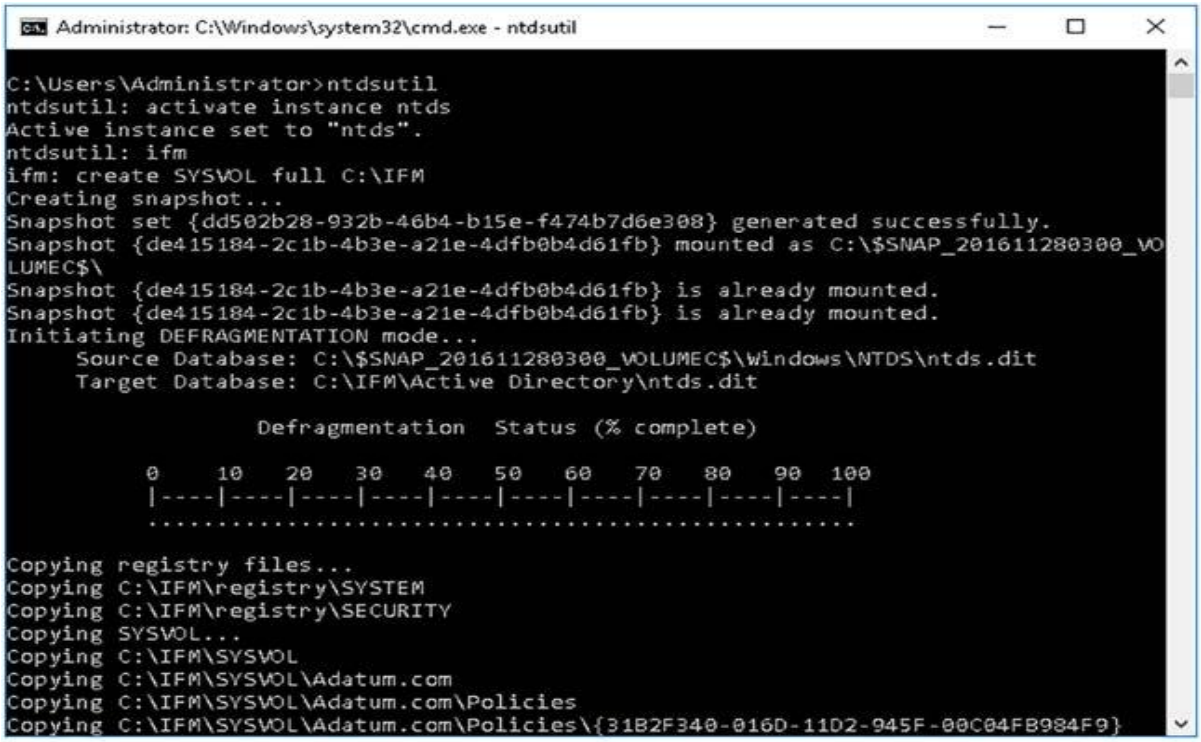
2. Abra um prompt de comando elevado e execute o comando ntdsutil.exe.

3. No prompt ntdsutil:, digite Ativar instância ntds e pressione Enter.

4. No prompt ntdsutil:, digite ifm e pressione Enter.

5. No prompt ifm:, como mostrado na Figura 13, digite create SYSVOL full

Figure 13. Criando um snapshot NTDS para IFM.



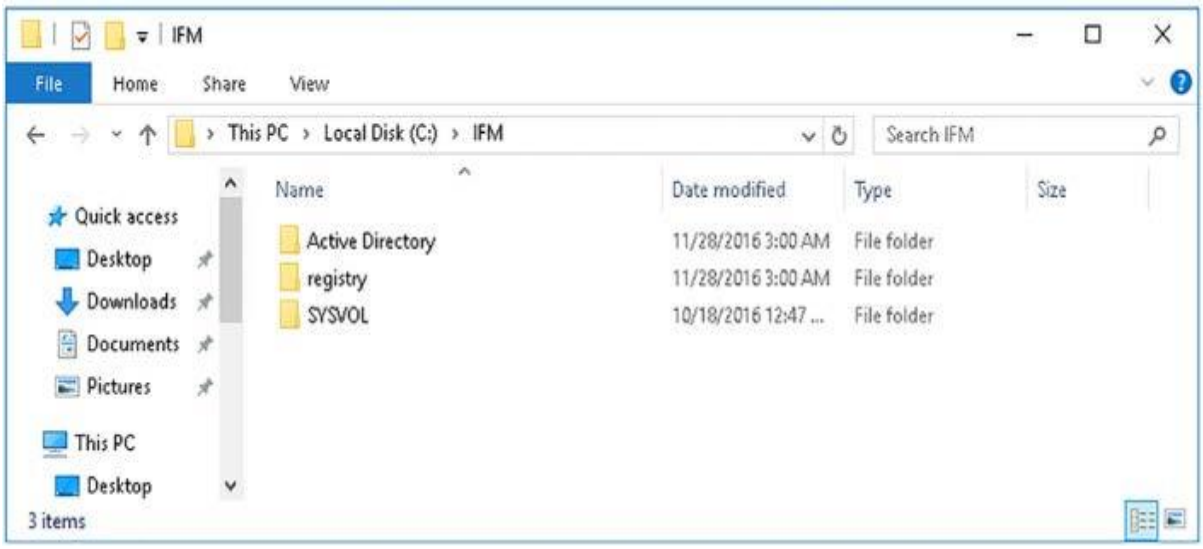
C: \ IFM e pressione Enter.

Fonte: (Warren, 2017, p. 18)

6. No prompt ifm:, digite quit e pressione Enter.

7. No prompt ntdsutil:, digite quit e pressione Enter.

Figure 14. As pastas criadas para um snapshot do AD DS.



8. Feche o prompt de comando.

Fonte: (Warren, 2017, p. 19)

9. Usando o File Explorer, copie o conteúdo da pasta C: \ IFM, mostrada na Figura 14, para armazenamento removível, como um cartão de memória USB.

10. No computador servidor que você deseja promover em um controlador de domínio, instale a função de servidor dos Serviços de Domínio Active Directory da maneira usual, usando o Gerenciador do Servidor 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 e inicie o Assistente de Configuração dos Serviços de Domínio Active Directory no Gerenciador de Servidores, e clique no assistente.

12. Na página Opções Adicionais, mostrada na Figura 15, marque a caixa

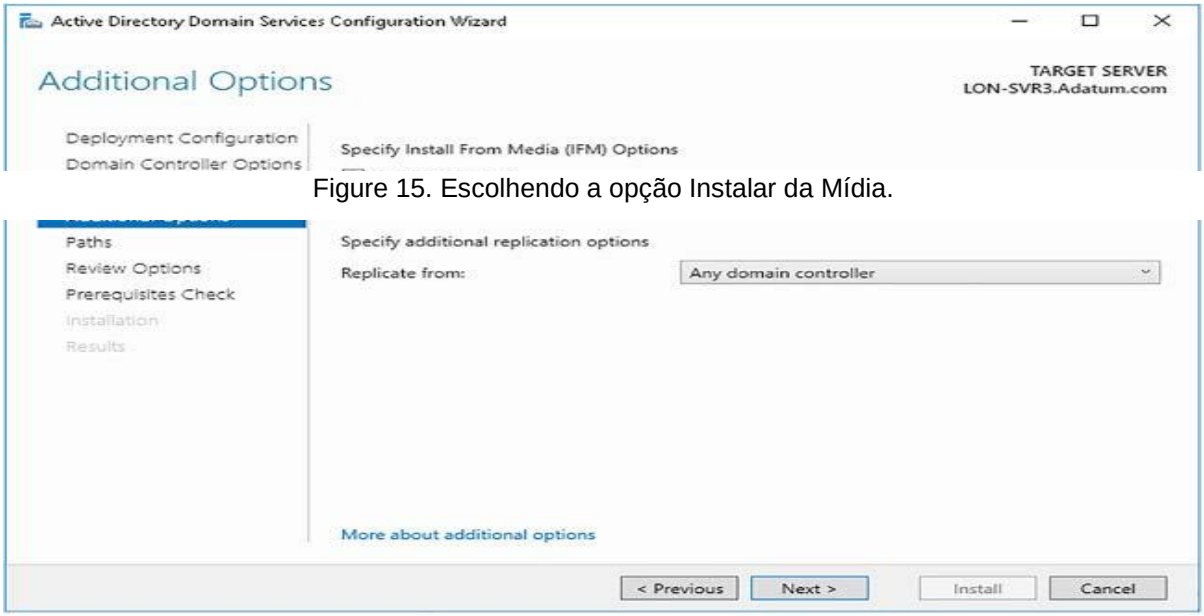


Figure 15. Escolhendo a opção Instalar da Mídia.

de seleção Instalar da Mídia. Na caixa Caminho, digite o caminho para a cópia local da captura instantânea do AD DS, clique em Verificar e, em seguida, clique em Avançar.

Fonte: (Warren, 2017, p. 20)

13. Clique no assistente, revise suas seleções e, quando solicitado, clique em Instalar. Seu servidor é reiniciado durante o processo de promoção.

14. Entre como um administrador de domínio.

O controlador de domínio agora se replica da maneira normal com outros controladores de domínio na floresta. Você pode definir o site do AD DS ao qual o controlador de domínio pertence e, em seguida, configurar um agendamento de replicação para esse site. Estes procedimentos são discutidos no Capítulo 2: Gerenciar e manter o AD DS, Habilidade 2.3: Configurar o Active Directory em um ambiente corporativo complexo.

Você também pode concluir a implantação usando o comando Windows PowerShell Install-ADDSDo-maincontroller -InstallationMediaPath x: \ ifm para promover o computador servidor.

6.1.5. Instale e configure um controlador de domínio somente leitura

Um RODC é um controlador de domínio que contém uma cópia somente leitura do AD DS. Você pode usar RODCs para permitir implantar controladores de domínio em escritórios onde a segurança física não pode ser garantida. Por exemplo, em uma filial, você pode precisar de um controlador de domínio local, mas não possui uma sala de computadores fisicamente segura para instalá-lo.

Embora os RODCs ofereçam vários benefícios administrativos, antes de implantá-los, você deve considerar os seguintes fatores:

Você deve implantar apenas um RODC por site, por domínio. Se você implantar vários RODCs por site, o armazenamento em cache é inconsistente, resultando em possíveis problemas de entrada do usuário e do computador.

Você pode instalar a função de servidor DNS junto com a função RODC.

Os clientes locais podem usar a função DNS instalada como em qualquer outra instância do DNS na sua organização, com uma exceção: atualizações

dinâmicas. Como as informações da zona DNS são somente leitura, os clientes não podem executar atualizações dinâmicas na instância RODC de uma zona DNS. Nessa situação, o RODC fornece aos clientes o nome de um controlador de domínio gravável que o cliente pode usar para atualizar seus registros.

Os RODCs não podem executar as seguintes funções do AD DS:

Funções de mestre de operações: As funções de mestre de operações precisam poder gravar no banco de dados do AD DS. Consequentemente, os RODCs não podem conter nenhuma das cinco funções de mestre de operações. As funções de mestre de operações são discutidas posteriormente nesta habilidade.

Bridgeheads de replicação do AD DS: Como os bridgeheads são responsáveis pela replicação do AD DS, eles devem oferecer suporte à replicação de entrada e saída do AD DS. Os RODCs oferecem suporte apenas à replicação de entrada e, portanto, não podem funcionar como pontes de replicação do AD DS.

Os RODCs não podem:

Autenticar entre relações de confiança quando uma conexão WAN estiver indisponível. Se uma filial hospedar usuários de vários domínios na floresta do AD DS, usuários e computadores do domínio do qual o RODC não é membro não poderão se autenticar quando um link WAN estiver indisponível. Isso ocorre porque o RODC armazena em cache credenciais apenas para as contas de domínio das quais é membro.

Suporte a aplicativos que exigem interação constante do AD DS Alguns aplicativos, como o Microsoft Exchange Server, exigem interação do AD DS. O RODC não suporta a interatividade necessária e, portanto, você deve implantar controladores de domínio graváveis nos locais que também hospedam Servidores Exchange.

Implantando um RODC

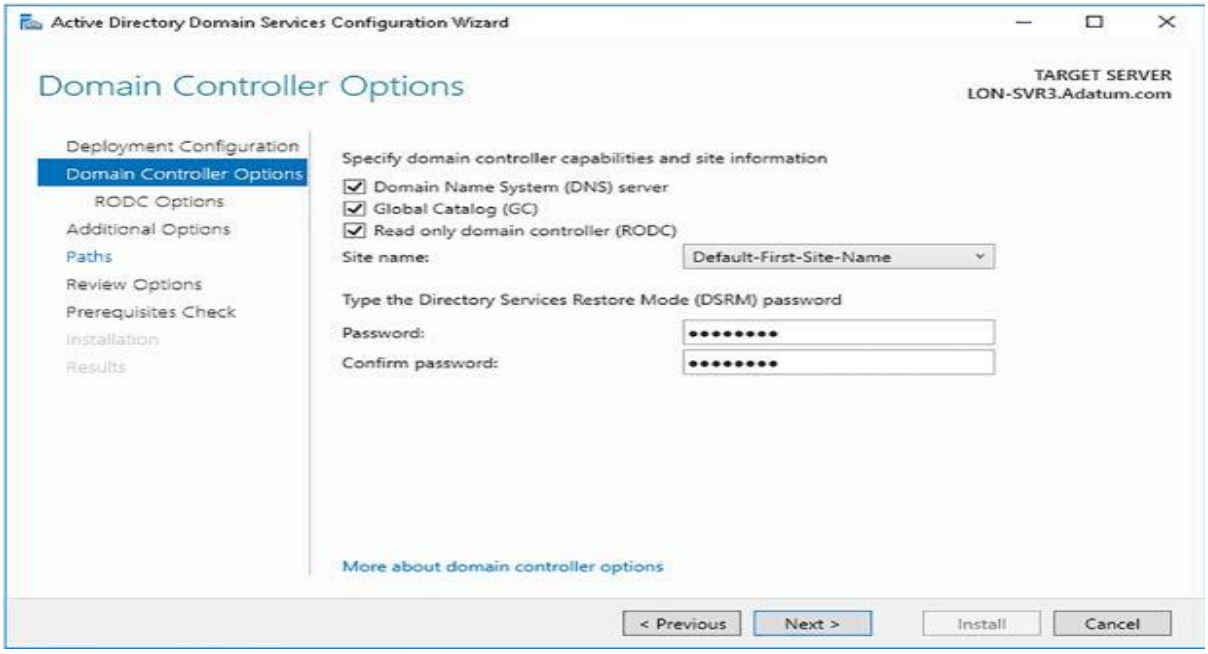
Antes de implantar um RODC, você deve garantir que haja pelo menos um controlador de domínio gravável em sua organização. Você implanta RODCs da mesma maneira que em todos os outros controladores de domínio:

1. Instale a função de servidor dos Serviços de Domínio Active Directory no computador servidor que você deseja implantar como um RODC.

2. Inicie o Assistente de Configuração dos Serviços de Domínio Active Directory e clique em o bruxo.

3. Na página Opções do controlador de domínio, mostrada na Figura 16, marque a caixa de seleção Read Only Domain Controller (RODC) e quaisquer outras opções necessárias e clique em Next.

Figure 16. Configurando opções do RODC.

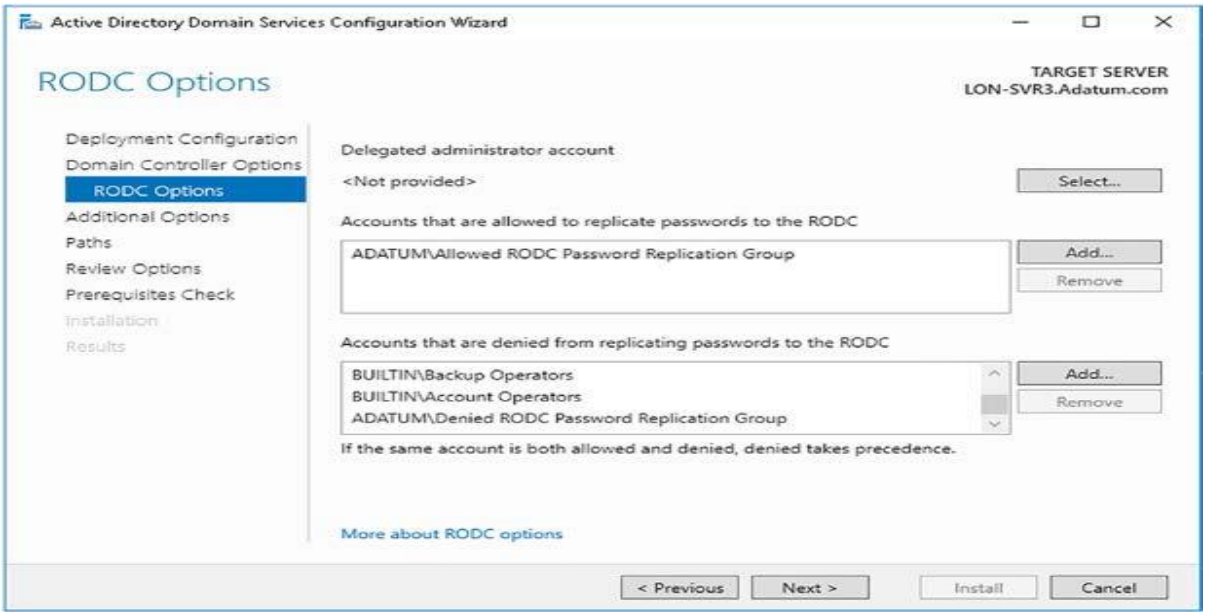


Fonte: (Warren, 2017, p. 22)

Na página Opções do RODC, mostrada na Figura 17, configure as seguintes opções e clique em Avançar.

Conta de administrador delegado: Os administradores delegados podem executar a administração local do RODC sem ter direitos e privilégios de administrador de domínio equivalentes. Normalmente, um administrador delegado do RODC pode executar as seguintes tarefas:

Figure 17. Instalando um RODC.



Fonte: (Warren, 2017, p. 22)

Instale e gerencie dispositivos e drivers, discos rígidos e atualizações.

Gerenciar o serviço AD DS.

Gerenciar funções e recursos do servidor.

Exibir os logs de eventos.

Gerenciar pastas, aplicativos e serviços compartilhados.

Contas autorizadas a replicar senhas no RODC: Por padrão, os RODCs não armazenam informações confidenciais relacionadas à senha. Quando um usuário entra, o RODC encaminha a solicitação de entrada para um controlador de domínio gravável online em outro local da organização.

No entanto, para melhorar a usabilidade, você pode definir que determinadas contas de usuário e computador possam ser armazenadas em cache no RODC, permitindo a autenticação local. Você faz isso definindo uma política de replicação de senha do RODC. Geralmente, você adicionaria apenas os usuários e computadores que estão no mesmo site local que o RODC à política de replicação.

Os RODCs armazenam apenas um subconjunto de credenciais de usuário e computador. Consequentemente, se um RODC for roubado, a exposição de segurança será limitada apenas às contas em cache. Isso reduz a exposição geral e ajuda a reduzir a carga administrativa porque apenas as contas em cache as senhas devem ser redefinidas.

Por padrão, conforme mostrado na Figura 17, o Grupo de replicação de senha permitida do RODC está ativado. Depois de implantar o RODC, você pode adicionar usuários e computadores a este grupo.

Além disso, há um grupo de replicação de senha negada do RODC. Os membros deste grupo nunca podem ter suas credenciais armazenadas em cache no RODC. Por padrão, esse grupo contém Administradores de Domínio, Administradores Corporativos e Proprietários Criadores de Diretiva de Grupo.

Contas negadas pela replicação de senhas no RODC: Por padrão, o Grupo de replicação de senha negada do RODC está selecionado. Depois de implantar o RODC, você pode adicionar usuários e computadores a este grupo. Além disso, os seguintes grupos locais também são impedidos de replicar senhas: Administradores, Operadores de servidor, Operadores de backup e Operadores de contas.

Os grupos Grupo de replicação de senha permitida do RODC e Grupo de replicação de senha negada do RODC permitem configurar a política de replicação de senha em todos os RODCs. No entanto, se você tiver várias filiais - e, portanto, vários RODCs -, é mais seguro configurar um grupo separado para cada RODC para a replicação de senha permitida. Nesta instância, remova o Grupo de replicação de senha permitida do RODC e adicione um grupo que você criou manualmente e adicione os membros necessários para essa ramificação.

Você pode usar o comando Install-ADDSDomainController –ReadOnlyReplica do Windows PowerShell para instalar um RODC.

Depois de implantar o RODC, você pode configurar as associações de grupo de replicação de senha permitida e de grupo de replicação de senha negada do RODC para gerenciar sua política de replicação de senha do RODC.

6.1.6. Configurar um servidor de catálogo global

Em uma floresta do AD DS de domínio único, qualquer controlador de domínio mantém uma cópia de todos os objetos dentro da floresta. No entanto, em várias florestas de domínio, isso não é mais verdade. Embora todos os controladores de domínio tenham uma cópia das partições de esquema e configuração, eles armazenam apenas a partição de domínio local. Portanto, se um aplicativo consulta um controlador de domínio em seu domínio local sobre os atributos de um objeto em outro domínio, não há como o controlador de domínio local atender a essa consulta.

É aqui que o catálogo global é útil. O catálogo global é uma cópia parcial, somente leitura, de todos os objetos na floresta e hospeda um subconjunto de todos os atributos do esquema da conta do AD DS. Todos os controladores de domínio habilitados como servidores de catálogo global armazenam uma cópia dessas informações localmente. Isso permite que eles atendam a consultas sobre os atributos de objetos que residem em outros domínios da floresta - sem a necessidade de solicitar um controlador de domínio nesse outro domínio.

Em uma floresta de domínio único, configure todos os controladores de domínio como servidores de catálogo global. Em uma floresta de vários domínios, a menos que todos os controladores de domínio sejam servidores de catálogo global, você não deve configurar o mestre de infraestrutura como um servidor de catálogo global.

Você pode configurar um controlador de domínio como um servidor de catálogo global durante a implantação do controlador de domínio. Você seleciona a caixa de seleção Catálogo Global (GC) na página Opções do Controlador de Domínio, mostrada na Figura 16, quando você executa o Assistente de Configuração dos Serviços de Domínio Active Directory.

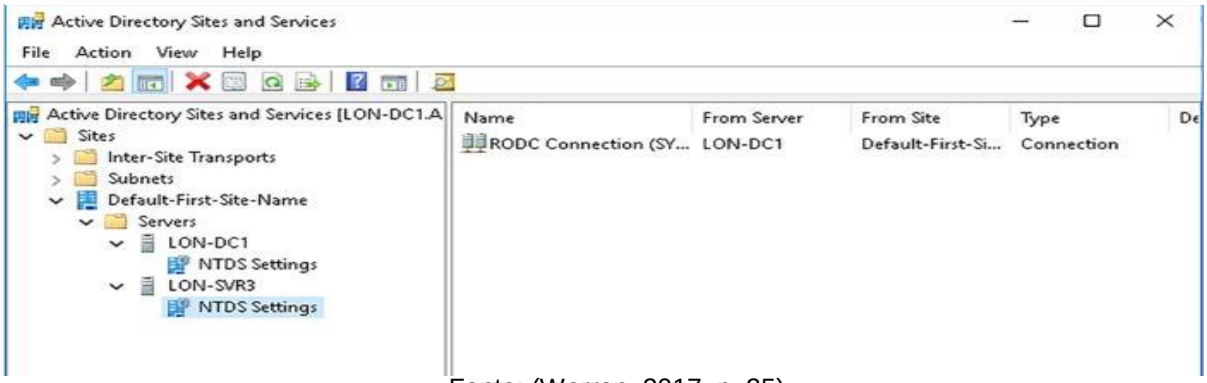
Como alternativa, após a instalação, você pode usar a ferramenta Serviços e Sites do Active Directory:

1. Em um controlador de domínio, abra o Gerenciador do Servidor, clique em Ferramentas e clique em Sites e Serviços do Active Directory.

2. Expanda o nó Sites, expanda o site relevante, expanda a pasta Servidor e expanda o nó do controlador de domínio que você deseja modificar.

3. Clique no objeto de configurações NTDS, como mostra a Figura 18.

Figure 18. Configurar um servidor de catálogo global.

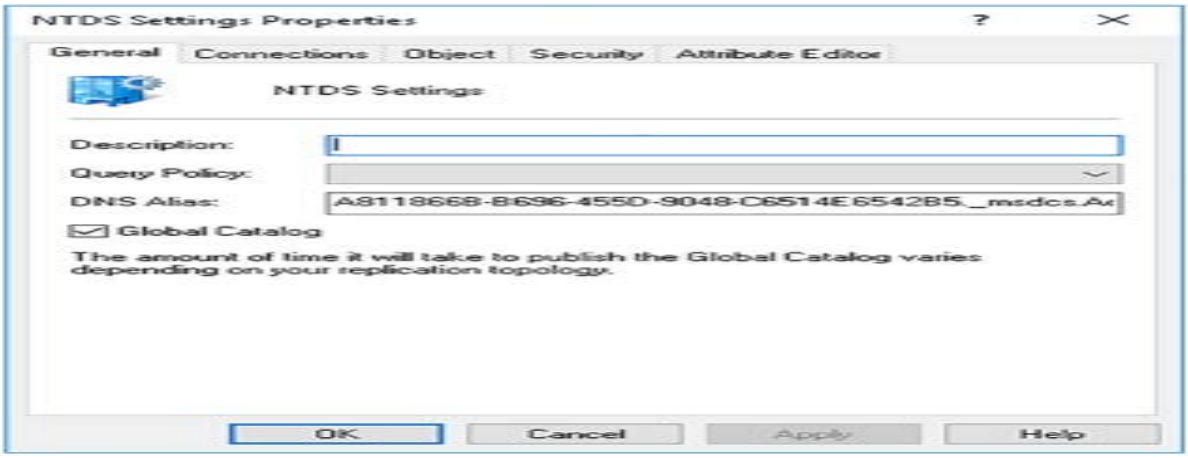


Fonte: (Warren, 2017, p. 25)

4. Clique com o botão direito do mouse no nó Configurações NTDS e, na guia Geral, marque a caixa de seleção Catálogo global, como mostra a Figura 19, e clique em OK.

Você também pode usar o Windows PowerShell para transformar um controlador de domínio de catálogo global.

Figure 19. Ativando a propriedade do Servidor de Catálogo Global.

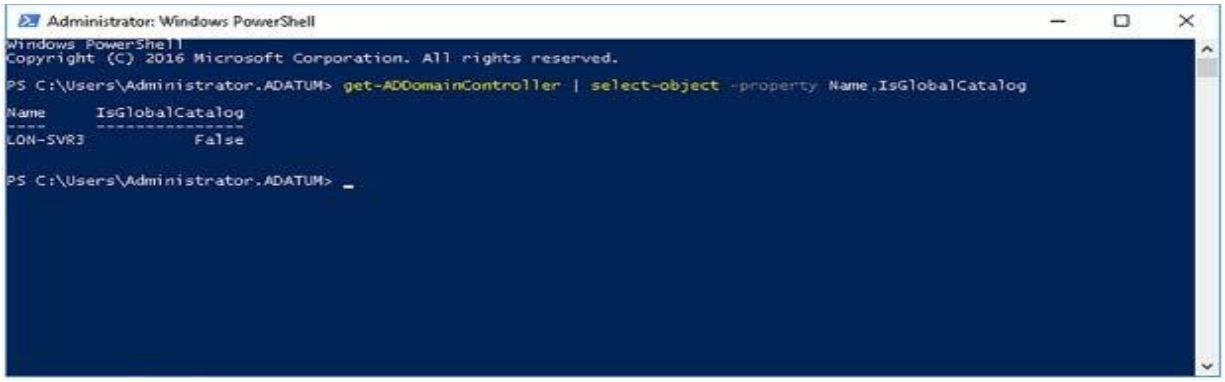


Fonte: (Warren, 2017, p. 25)

1. Abra o Windows PowerShell (Admin).

2. Execute o get-ADDomainC ontroller | select-object -property Name, comando IsGlobalCatalog para consultar uma lista de controladores de domínio e

Figure 20. Obtendo uma lista de controladores de domínio.



verificar seu status atual do catálogo global, como mostra a Figura 20.

Fonte: (Warren, 2017, p. 26)

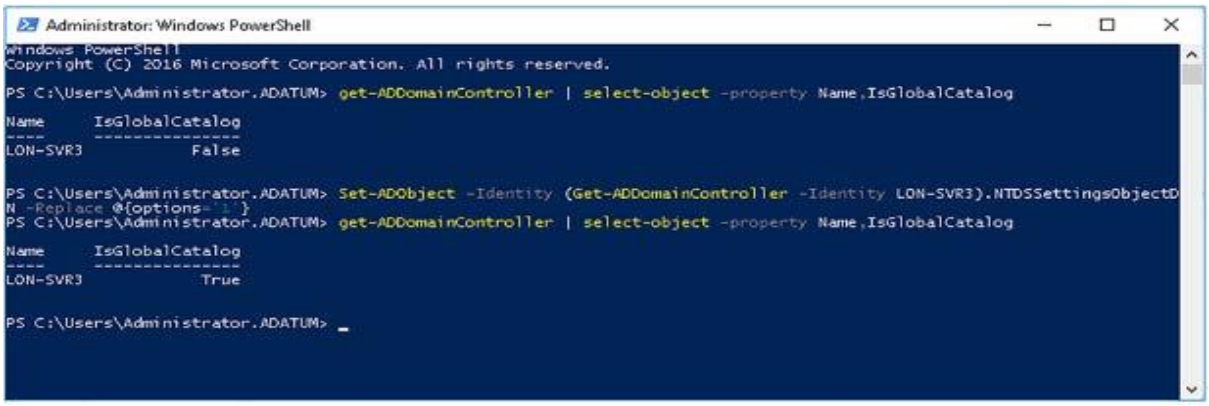
3. Para o controlador de domínio apropriado, execute o seguinte comando, substituindo LON-SVR3 pelo nome do seu controlador de domínio:

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

4. Execute o get-ADDomainController | nome do objeto -property, IsGlobalCatalog comando novamente para verificar a alteração, como mostra a Figura 21.

Muitas organizações agora optam por tornar todos os controladores de domínio servidores de catálogo globais.

Figure 21. Configurando um DC como um servidor de catálogo global.



fonte: (Warren, 2017, p. 26)

Incluindo atributos no catálogo global

É importante observar que o catálogo global não contém todos os atributos para todos os objetos; em vez disso, contém um subconjunto dos atributos mais úteis, conhecidos no Windows Server 2016 como o Conjunto de Atributos Parciais. No entanto, é possível modificar quais atributos do objeto são armazenados no catálogo global; isso às vezes é chamado de extensão do conjunto de atributos parciais. Você pode fazer isso usando o seguinte procedimento:

1. No controlador de domínio que possui acesso online ao mestre de operações do esquema função, execute o comando regsvr32 schmmgmt.dll em um prompt de comando elevado. Este comando permite que o esquema do Active Directory seja acessível 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 - [Raiz do console], clique em Arquivo e, em seguida, clique em Adicionar / remover snap-in.

4. Na caixa de diálogo Adicionar ou remover snap-ins, na lista Snap-in, clique em Active Directory.

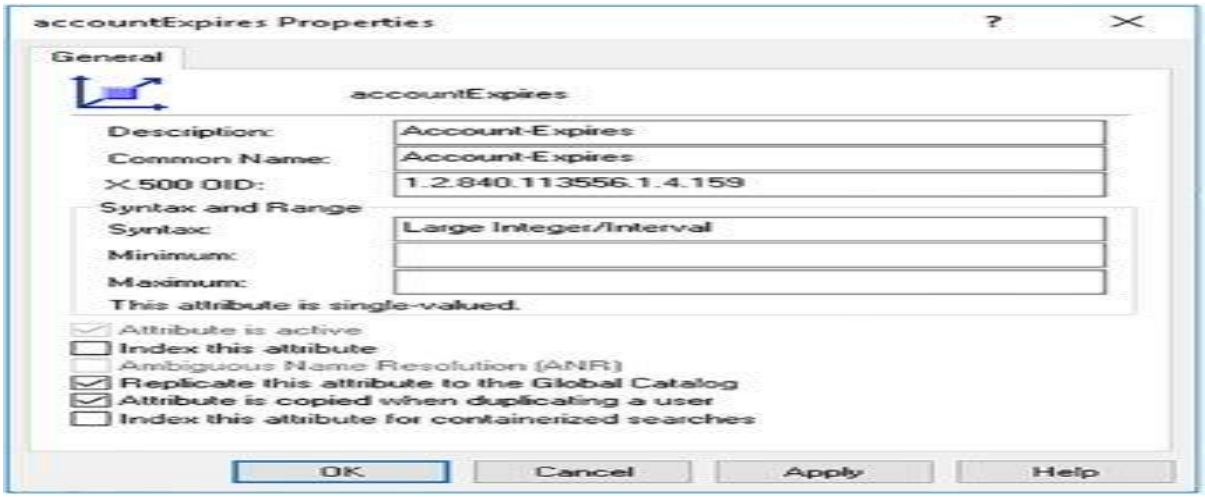
Esquema, clique em Adicionar e, em seguida, clique em OK.

5. Em Raiz do console no painel de navegação, expanda Esquema do Active Directory e clique em Atributos. Uma longa lista de atributos é exibida.

6. Você deve saber o nome do atributo específico para poder modificar suas propriedades. Localizar o atributo, clique com o botão direito do mouse e clique em Propriedades.

7. Na caixa de diálogo Propriedades do atributo, a caixa de diálogo Propriedades accountExpires é mostrada na Figura 22, marque a caixa de seleção

Figure 22. Adicionando atributos ao catálogo global.



Replicar Este Atributo para o Catálogo Global e clique em OK.

Fonte: (Warren, 2017, p. 27)

8. Feche o console de gerenciamento.

6.1.7. Criando um clone

Antes de poder clonar um controlador de domínio virtual, você deve garantir que sua infraestrutura atenda aos seguintes requisitos:

Windows Server 2012 ou posterior: Suas máquinas virtuais convidadas do controlador de domínio devem executar o Windows Server 2012 ou posterior.

Mestre de operações do emulador PDC O mestre de operações do emulador do controlador de domínio primário (PDC) deve estar em execução em um controlador de domínio instalado com o Windows Server 2012 ou posterior. Além disso, a função de emulador PDC deve estar online quando você inicia os controladores de domínio clonados pela primeira vez.

Identificadores de geração de máquina virtual: Você deve usar um hipervisor, como o Hyper-V no Windows Server 2012 ou posterior, que suporte identificadores de geração de máquina virtual.

Depois de verificar esses pré-requisitos, você pode usar o procedimento a seguir para clonar um controlador de domínio virtual. Isso consiste em dois estágios:

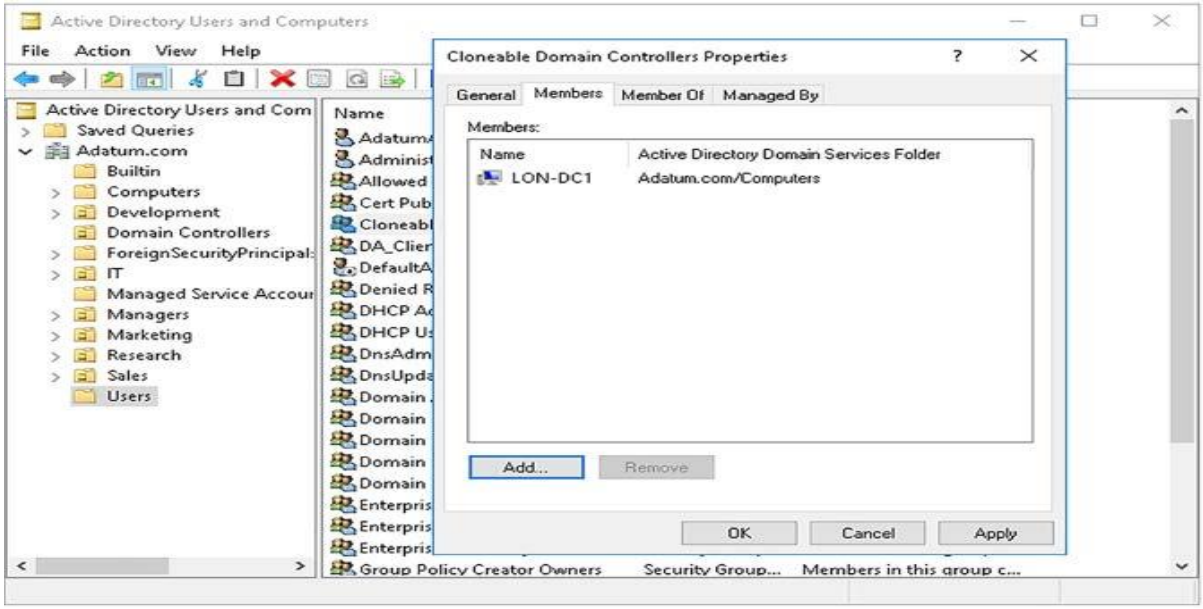
preparar o controlador de domínio de origem e preparar um ou mais clones de controlador de domínio de destino.

PREPARAR O COMPUTADOR DE FONTE

1. Entre no seu controlador de domínio como um membro do grupo de segurança global Admins. Do Domínio.

2. Abra o console Usuários e Computadores do Active Directory, navegue até a pasta Usuários e adicione o computador de origem ao grupo de segurança

Figure 23. Adicionando um servidor ao grupo de segurança.



global Cloneable Domain Controllers, como mostra a Figura 23.

Fonte: (Warren, 2017, p. 29)

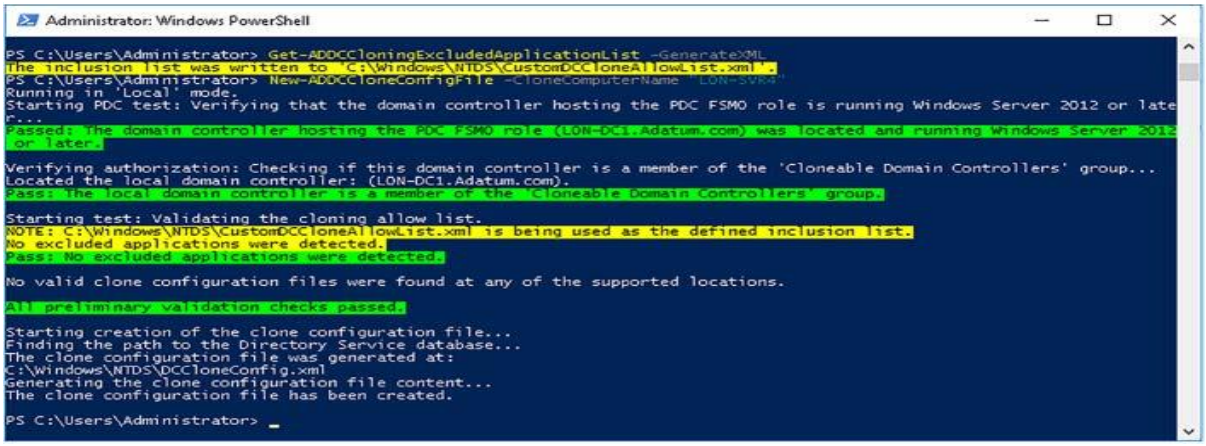
3.Execute o cmdlet Windows PowerShell Get-ADDCCloneingExcludedApplicationList para verificar se todos os aplicativos e serviços no seu controlador de domínio de origem suportam clonagem. Remova todos os aplicativos não suportados.

4.Execute o Windows PowerShell Get-ADDCCloneingExcludedApplicationList –GenerateXML cmdlet.

5. Execute o cmdlet Windows-PowerShell New-ADDCCloneConfigFile, conforme mostrado na Figura 24, para gerar um arquivo DCCloneConfig.xml. Este arquivo é usado para configurar os clones.

Você especifica um nome de computador, configuração de IP e nome do site para o clone pretendido. Esta informação é gravada em DCCloneConfig.xml. Se você pretende criar vários clones, normalmente, cada um deve ter um arquivo

Figure 24. Criando o DCCloneConfig.xml usando o Windows.



DCCloneConfig.xml diferente.

Fonte: (Warren, 2017, p. 30)

6. Desligue 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 do controlador de domínio de origem no painel de navegação e clique em Exportar.

Na caixa de diálogo Exportar máquina virtual, na caixa de texto Localização, especifique a pasta em que deseja armazenar a exportação da máquina virtual e clique em Exportar.

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

CRIAR O CLONE

1. Verifique se o emulador PDC e um servidor de catálogo global estão online e visíveis para seus clones de destino.

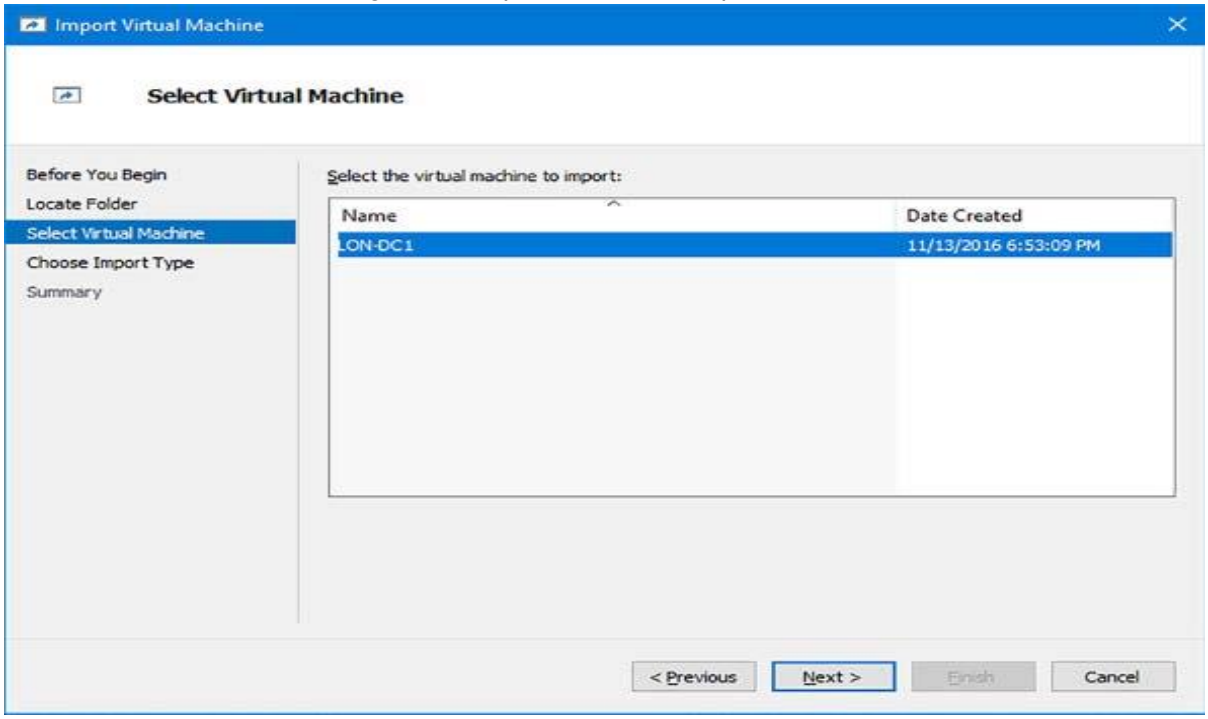
2. No Gerenciador Hyper-V, importe a máquina virtual:

A. No painel Ações, clique em Importar Máquina Virtual.

B. No Assistente para Importação de Máquina Virtual, na página Localizar Pasta, na caixa de texto Pasta, digite o caminho para os arquivos exportados para sua máquina virtual e clique em Avançar.

C. Na página Selecionar Máquina Virtual, conforme mostrado na Figura

Figure 25. Importando uma máquina virtual.



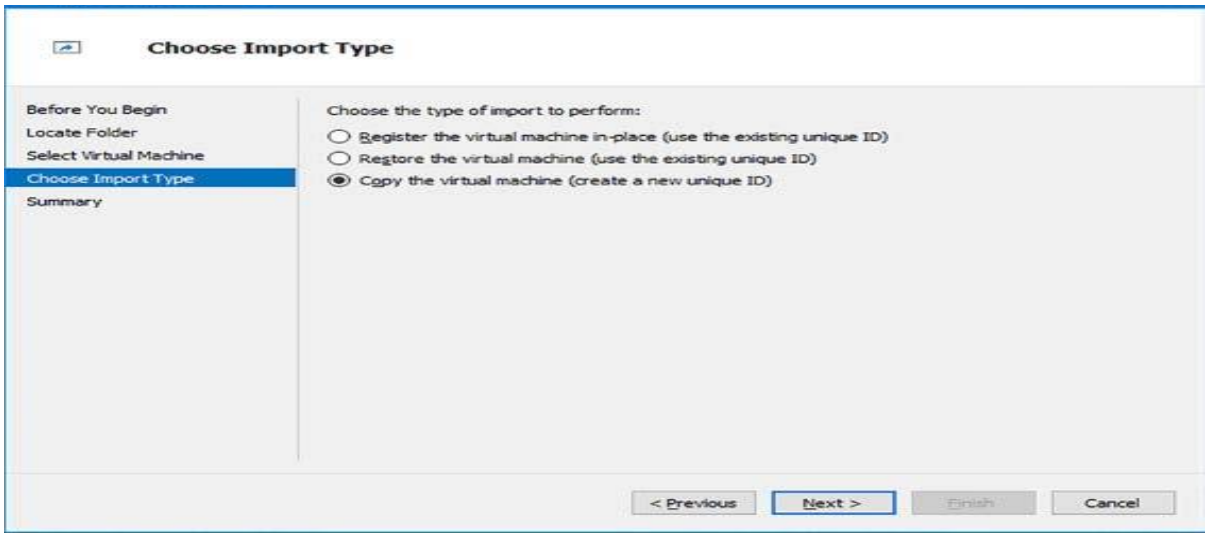
25, se necessário, selecione a máquina virtual na lista e clique em Avançar.

Fonte: (Warren, 2017, p. 31)

3. Na página Escolha o tipo de importação, mostrada na Figura 26, clique em Copiar a máquina virtual (criar um novo ID exclusivo) e clique em Avançar.

.

Figure 26. Especificando um tipo de importação.

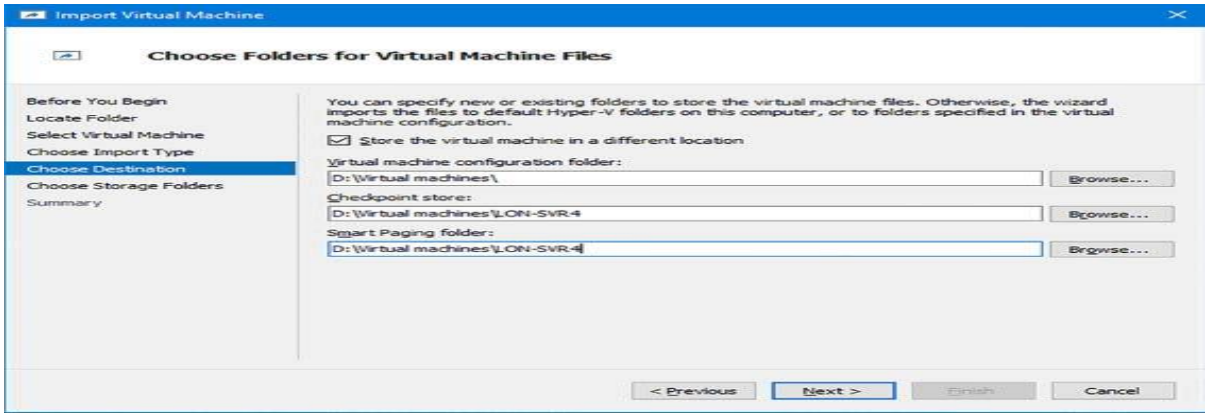


Fonte: (Warren, 2017, p. 31)

4. Na página Escolher pastas para arquivos da máquina virtual, mostrada na Figura 27, marque a caixa de seleção Armazenar a máquina virtual em um local diferente e, para cada local da pasta, especifique um caminho de pasta adequado e clique em Avançar.

5. Na página Escolha pastas para armazenar discos rígidos virtuais, mostrada na Figura 28, especifique um caminho de pasta adequado e clique em

Figure 27. Especificando o local para os arquivos importados.



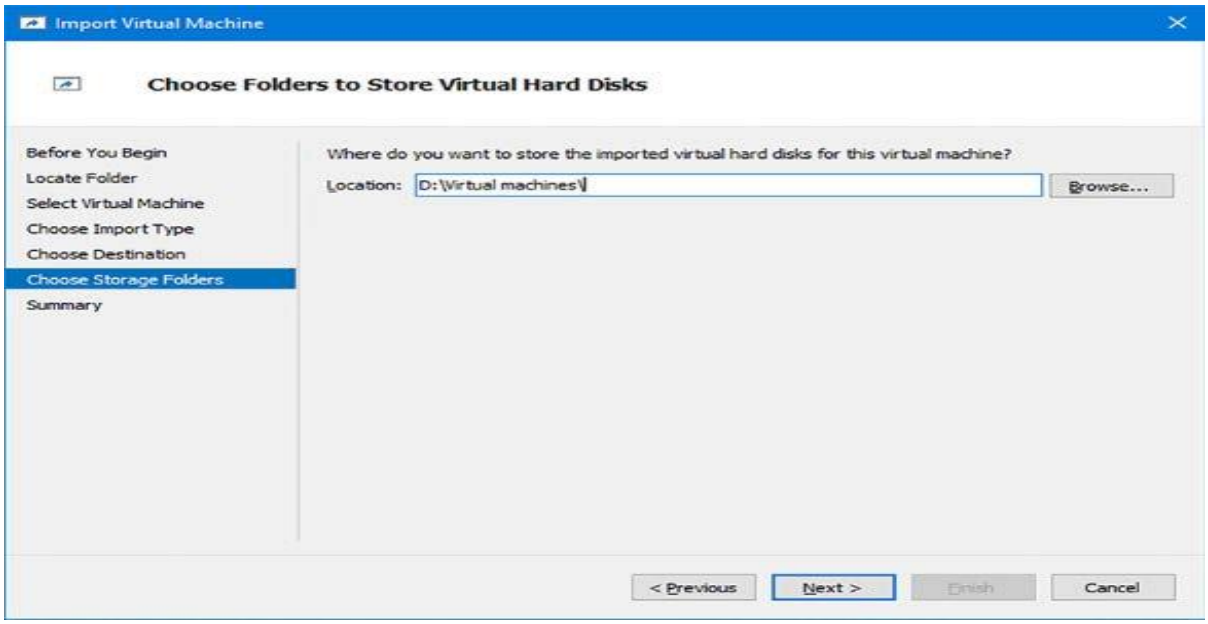
Avançar.

Fonte: (Warren, 2017, p. 32)

6. Na página Concluindo Assistente de Importação, clique em Concluir. A máquina virtual é importada, o que pode levar até 20 minutos ou mais.

7. Após a importação, no Gerenciador Hyper-V, no painel de navegação, renomeie a máquina virtual importada.

Figure 28. Especificando o local para os arquivos importados da máquina virtual.



fonte: (Warren, 2017, p. 32)

8. No Gerenciador Hyper-V, no painel Ações, clique na máquina virtual importada recentemente, clique em Iniciar e, em seguida, clique em Conectar para ver a máquina virtual iniciando. Uma mensagem “A clonagem do controlador de domínio está com x% de conclusão” é exibida durante a conclusão do processo de clonagem.

6.1.8. Atualizar controladores de domínio

Se você estiver usando uma versão anterior do Windows Server e quiser atualizar seus controladores de domínio para o Windows Server 2016, poderá executar uma atualização no local. No entanto, esse processo apresenta alguns riscos. Geralmente, é mais seguro adicionar um novo controlador de domínio do Windows Server 2016 à sua infraestrutura existente e migrar funções para os controladores de domínio recém-implantado.

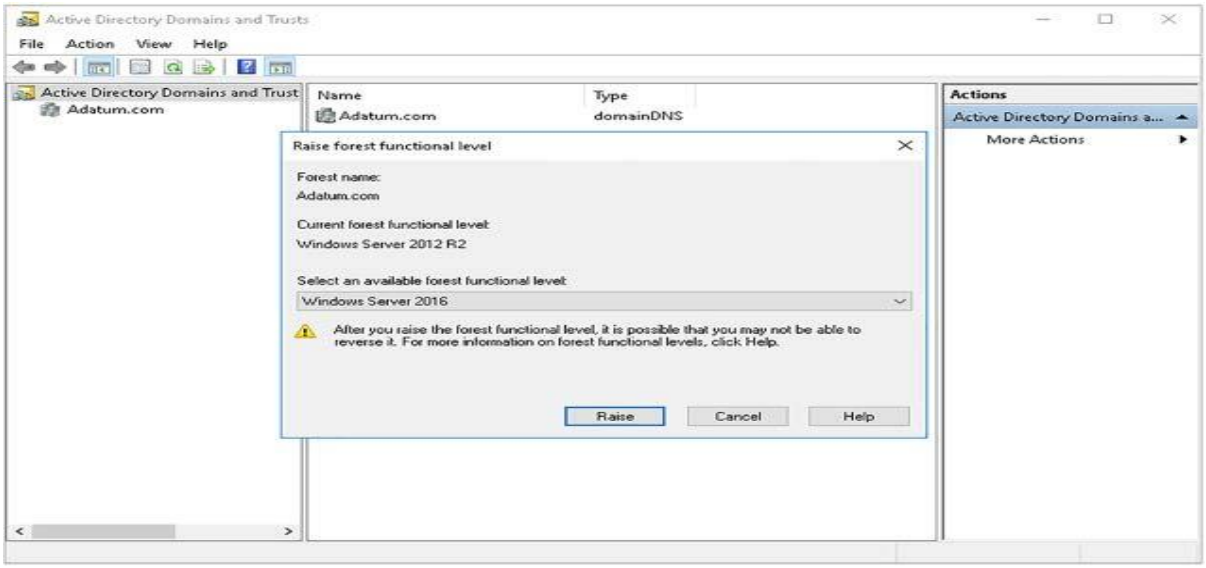
Antes de implantar o primeiro controlador de domínio do Windows Server 2016 em sua infraestrutura existente, você deve determinar se o nível funcional da floresta e o nível funcional do domínio atuais são pelo menos o Windows Server 2008. Você pode fazer isso usando o seguinte procedimento:

1. No console Domínios e Relações de Confiança do Active Directory, no painel de navegação, clique com o botão direito do mouse no nó Domínios e Relações de Confiança do Active Directory e clique em Aumentar Nível Funcional da Floresta.

2. Na caixa de diálogo Elevar nível funcional da floresta, o nível funcional atual da floresta é exibido, conforme mostrado na Figura 29.

3. Se necessário, na lista Selecionar um nível funcional de floresta disponível, clique em um nível maior que o Windows Server 2008 e, em seguida,

Figure 29. Verificando o nível funcional da floresta.



clique em Aumentar.

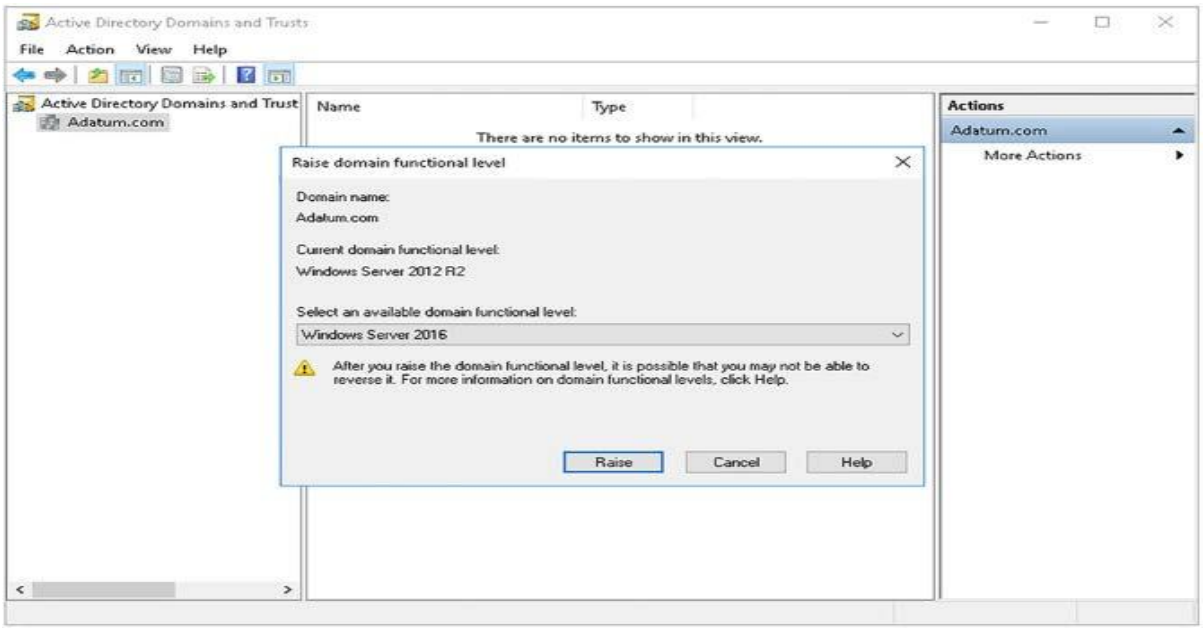
Fonte: (Warren, 2017, p. 34)

4. No painel de navegação, localize e clique com o botão direito do mouse no domínio AD DS apropriado e clique em Aumentar Nível Funcional do Domínio.

5. Na caixa de diálogo Elevar nível funcional do domínio, o Nível funcional do domínio atual é exibido, conforme mostrado na Figura 30.

6. Se necessário, na lista Selecionar um nível funcional de domínio disponível, clique em um nível maior que o Windows Server 2008 e clique em Aumentar.

Figure 30. Verificando o nível funcional da floresta.



Fonte: (Warren, 2017, p. 34)

Depois de verificar e, se necessário, elevar os níveis funcionais da floresta e do domínio, se sua infraestrutura existente for baseada no Windows Server 2008 ou no Windows Server 2008 R2, você deverá executar as seguintes tarefas:

Prepare sua floresta do AD DS Em um controlador de domínio em sua floresta existente, execute adprep / forestprep.

Prepare seu domínio do AD DS Em um controlador de domínio na floresta existente, execute adprep / domainprep.

Se sua infraestrutura atual é baseada no Windows Server 2012 ou posterior, o Assistente de Configuração dos Serviços de Domínio de Diretório Ativo executa essas etapas automaticamente. No entanto, você ainda pode optar por executá-las como etapas independentes.

6.2. Criar e gerenciar usuários e computadores do Active Directory

Depois de instalar e implantar seus controladores de domínio, você pode começar a preencher o AD DS com objetos, incluindo usuários e computadores. Você pode usar várias ferramentas gráficas acessíveis no Gerenciador do Servidor para executar essas tarefas administrativas ou usar o Windows PowerShell para ajudar a automatizar essas tarefas.

6.2.1. Criar, copiar, configurar e excluir usuários e computadores

Para cada usuário em sua organização, você deve criar uma conta de usuário no AD DS. Isso os identifica como indivíduos quando tentam executar tarefas (direitos) ou acessar recursos (permissões).

Você pode preencher esta conta de usuário com propriedades (atributos) que descrevem o usuário. Isso pode incluir nome completo, detalhes de contato, função na organização, departamento e muitas configurações que definem o escopo de suas habilidades na rede.

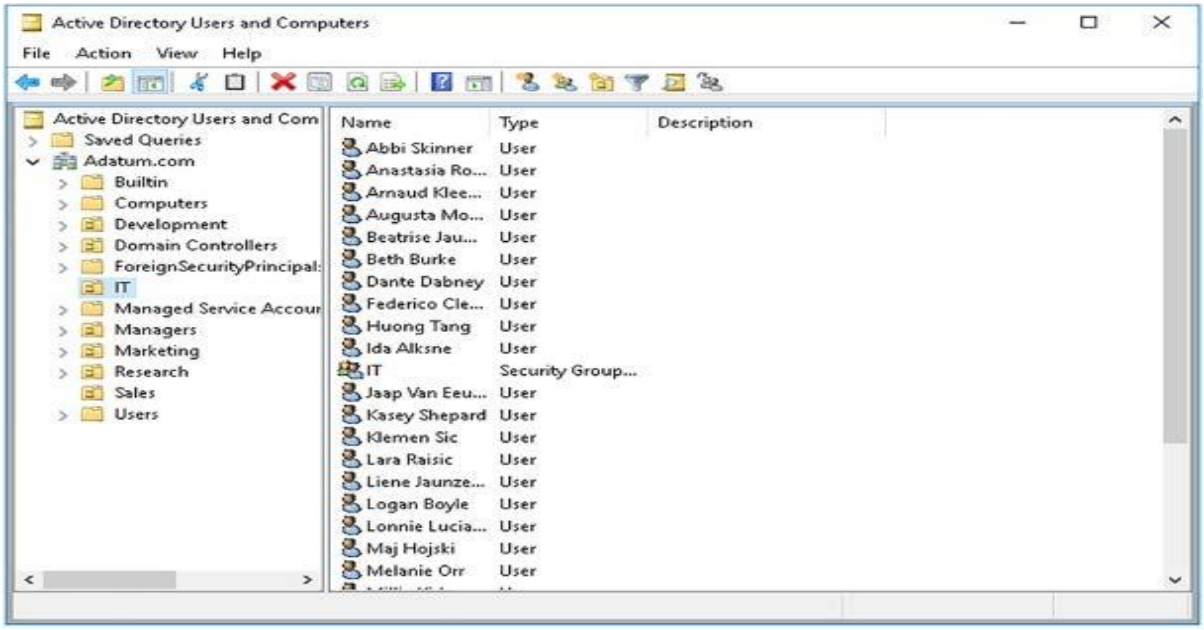
É importante que, antes de iniciar esse processo, dedique um pouco de tempo a pensar em um padrão de nomeação para suas contas de usuário. O nome da conta do usuário deve identificá-lo claramente e deve ser exclusivo dentro da sua organização. Normalmente, as organizações usam uma combinação do sobrenome e das iniciais de um usuário para gerar um nome exclusivo. Se sua organização for grande, isso poderá exigir uma consideração cuidadosa, pois muitos usuários podem compartilhar um sobrenome e alguns podem compartilhar tanto o nome quanto o sobrenome.

No AD DS, não são apenas os usuários que devem ter uma conta. Os computadores que se conectam aos recursos de rede da sua organização também devem ser identificados. Em alguns aspectos, isso é mais simples, porque você toma a decisão sobre o nome da conta do computador ao implantar o computador e o nomeia durante o processo de instalação. Portanto, é essencial que, ao implantar os computadores de seus usuários, considere o nome do dispositivo com cuidado.

Adicionando contas de usuário

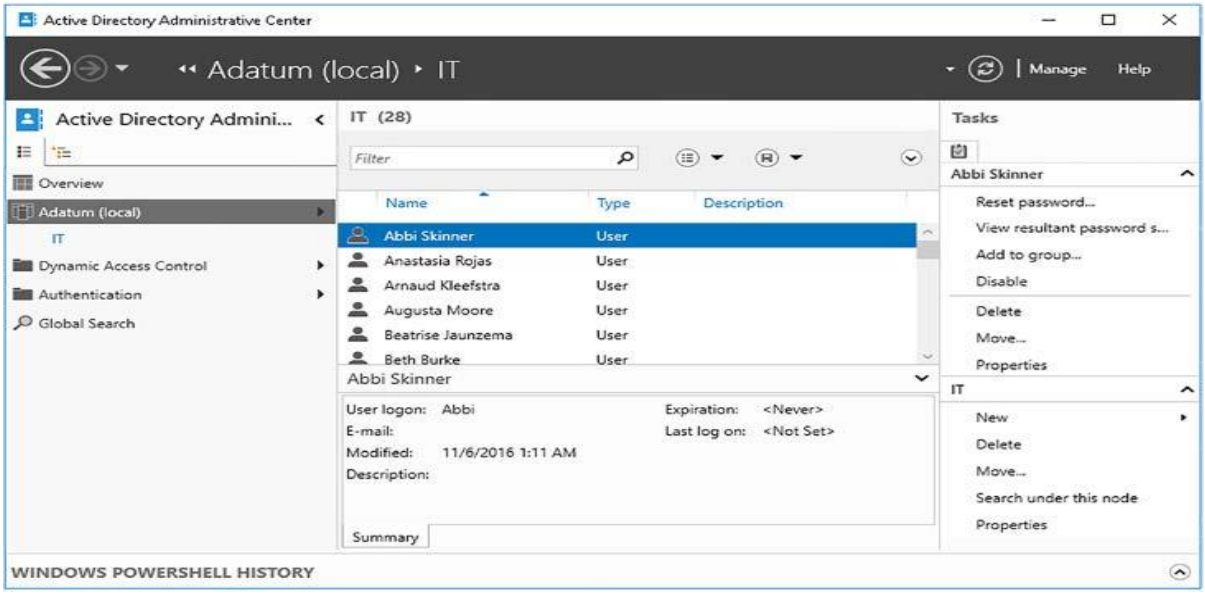
Existem várias ferramentas que você pode usar para criar e gerenciar contas de usuário, incluindo Windows PowerShell, a ferramenta de linha de comando dsadd.exe, Usuários e Computadores do Active Directory, mostrados na Figura 31, e o Centro Administrativo do Active Directory, mostrado em Figura 32. Para os fins dos procedimentos deste capítulo, usaremos Usuários e Computadores do Active Directory e o Windows PowerShell.

Figure 32.Usuários e computadores do Active Directory.



Fonte: (Warren, 2017, p. 45)

Figure 31. Centro administrativo do Active Directory.



Fonte: (Warren, 2017, p. 45)

Centro administrativo do Active Directory.

Após definir o padrão de nomenclatura da conta de usuário, use o procedimento a seguir para adicionar uma conta de usuário:

1. Entre como um membro do grupo de segurança global Admins. Do Domínio.

2. Abra o console Usuários e computadores do Active Directory e selecione a UO na qual deseja criar sua conta de usuário.

3. Clique com o botão direito do mouse na UO, aponte para Novo e clique em Usuário.

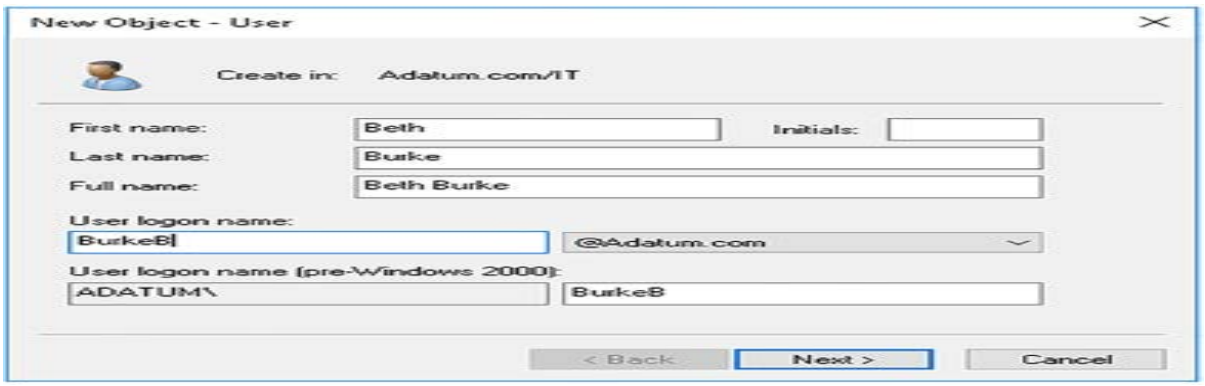
4. Na caixa de diálogo Novo objeto - usuário, mostrada na Figura 33, digite as seguintes informações e clique em Avançar:

Nome, iniciais e sobrenome Estes devem identificar exclusivamente o usuário. Esses elementos foram combinados para criar o nome completo do usuário, que deve ser exclusivo no contêiner do AD DS em que você o criou. No entanto, é aconselhável tentar garantir que o nome seja exclusivo dentro da floresta.

Nome de logon do usuário Esse nome é combinado com o sufixo exibido ao lado (@ Adatum.com na Figura 33) para criar um nome principal de usuário (UPN); por exemplo, BurkeB@Adatum.com. Esse UPN deve ser exclusivo na floresta do AD DS. O sufixo UPN geralmente é o nome de domínio em que você está adicionando a conta. No entanto, você pode definir sufixos UPN adicionais usando o console de Domínios e Relações de Confiança do Active Directory.

Nome de logon do usuário (anterior ao Windows 2000) esse nome também é chamado de nome da conta SAM. Ele deve ser exclusivo no domínio

Figure 33. Adicionando conta de usuário.



atual.

Fonte: (Warren, 2017, p. 46)

5. Em seguida, digite uma senha e confirme a senha, conforme mostrado na Figura 34. Tudo o que você digitar deve atender às regras atuais de complexidade de senha em seu domínio. Defina as configurações restantes e clique

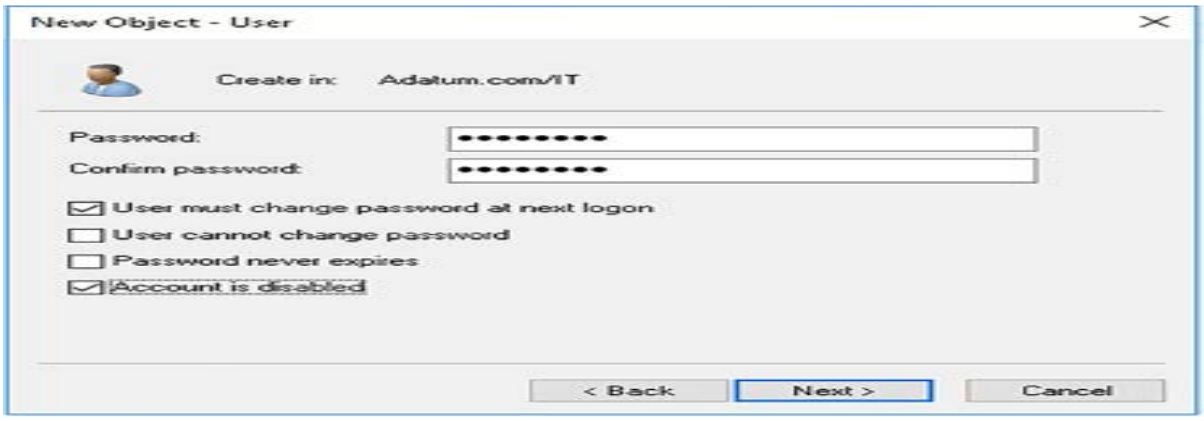
em Avançar: O usuário deve alterar a senha no próximo logon É uma boa prática forçar um usuário a escolher uma nova senha quando entrar pela primeira vez.

O usuário não pode alterar a senha Selecione: esta opção se a conta do usuário for uma conta especializada, como a usada por um aplicativo ou serviço e não por uma pessoa. Esta opção é mutuamente exclusiva com O usuário deve alterar a senha no próximo logon.

A senha nunca expira Da mesma forma, escolha essa opção se a conta do usuário for uma conta especializada, como a usada por um aplicativo ou serviço. Essa opção também é mutuamente exclusiva com o usuário deve alterar a senha no próximo logon.

A conta está desativada: É uma boa prática desativar todas as contas de usuário até que o usuário esteja pronto para entrar pela primeira vez. Muitas organizações adicionam contas de usuário e criam contas de email para novos funcionários iniciantes antes do primeiro dia do novo funcionário. No entanto, deixar uma conta de usuário ativada e não utilizada, com sua senha inicial, não é segura.

Figure 34. Configurando opções de senha e conta.



6. Quando solicitado, clique em Concluir.

Fonte: (Warren, 2017, p. 47)

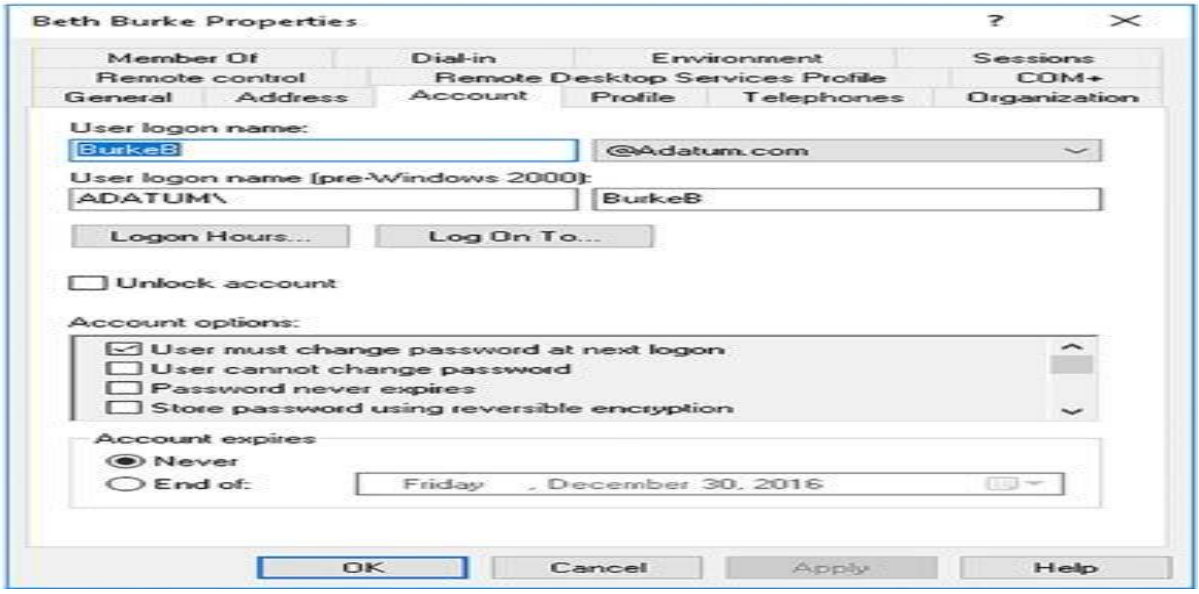
Depois de criar a conta, você deve modificar suas propriedades para poder configurar associações a grupos, detalhes organizacionais e propriedades mais avançadas da conta. Para fazer isso, use o seguinte procedimento:

1. Em Usuários e computadores do Active Directory, localize a UO que contém sua nova conta de usuário.

2. Clique com o botão direito do mouse na conta e clique em Propriedades. Há um grande número de propriedades configuráveis da conta do usuário, mas as seguintes são as mais críticas.

3. Na caixa de diálogo Propriedades do usuário, clique na guia Conta, mostrada na Figura 35 e, em seguida,

Figure 35. Modificando propriedades da conta do usuário.



Defina as seguintes configurações:

Fonte: (Warren, 2017, p. 48)

Horário de logon: especifique os dias e horários da semana em que a conta pode ser usada. O padrão é sempre.

Fazer logon em: defina em quais computadores a conta de usuário pode ser conectada. O padrão é Todos os computadores.

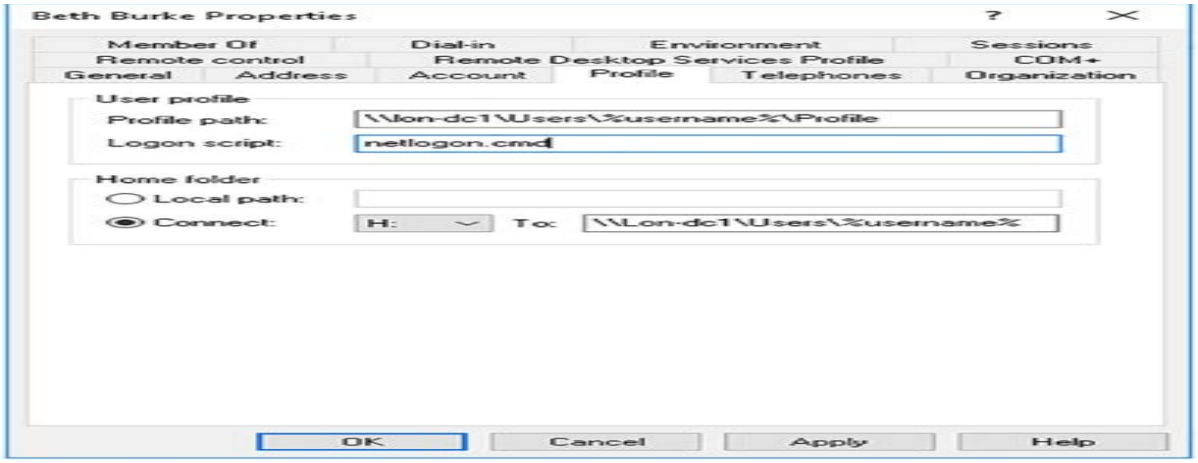
Desbloquear conta: esta opção só pode ser selecionada quando a conta estiver bloqueada. Isso ocorre quando um usuário tenta entrar usando uma senha incorreta e excede o limite de senhas incorretas.

Opções da conta: além das opções definidas quando você criou a conta (o usuário deve alterar a senha no próximo logon e assim por diante), é possível ativar algumas opções mais avançadas para contas usadas em situações sensíveis que exigem mais segurança. As configurações incluem: O cartão inteligente é

necessário para logon interativo, a conta é sensível e não pode ser delegada e esta conta oferece suporte à criptografia Kerberos AES 256 bits.

A conta expira: você pode configurar uma data de validade para uma conta. Isso geralmente é útil para contas usadas por estagiários ou funcionários temporários. Depois que a conta expirar, você poderá reatribuir a conta ao próximo estagiário e reconfigurar a configuração de expiração.

Figure 36. Modificando propriedades do perfil do usuário.

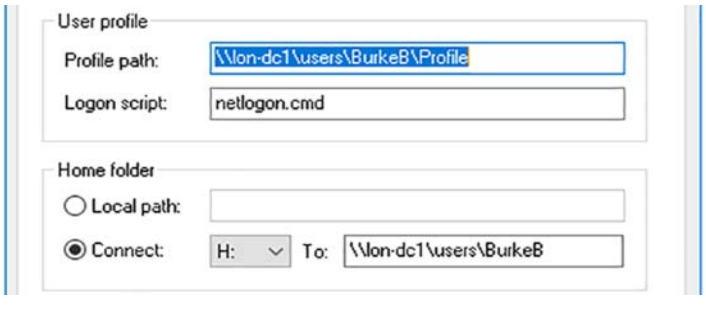


4. Na guia Perfil, mostrada na Figura 36, as seguintes configurações.

fonte: (Warren, 2017, p. 49)

Caminho do perfil: se você definir um caminho de perfil em uma pasta compartilhada, as configurações da área de trabalho e do aplicativo do usuário vagam com a conta do usuário. Quando um usuário sai, as configurações da área de trabalho e do aplicativo são salvas neste local. Defina um nome UNC e use a variável% username% para definir uma subpasta da pasta compartilhada. Por exemplo, conforme mostrado na Figura 36, o nome UNC aponta para a pasta compartilhada Users no servidor LON-DC1. Uma subpasta para esse usuário, nomeada após a conta do usuário, será criada automaticamente quando você clicar em Aplicar, como mostra a Figura 37. Abaixo disso, uma subpasta para o perfil do

Figure 37. Aplicando opções de perfil de usuário.



usuário é criada automaticamente.

Fonte: (Warren, 2017, p. 50)

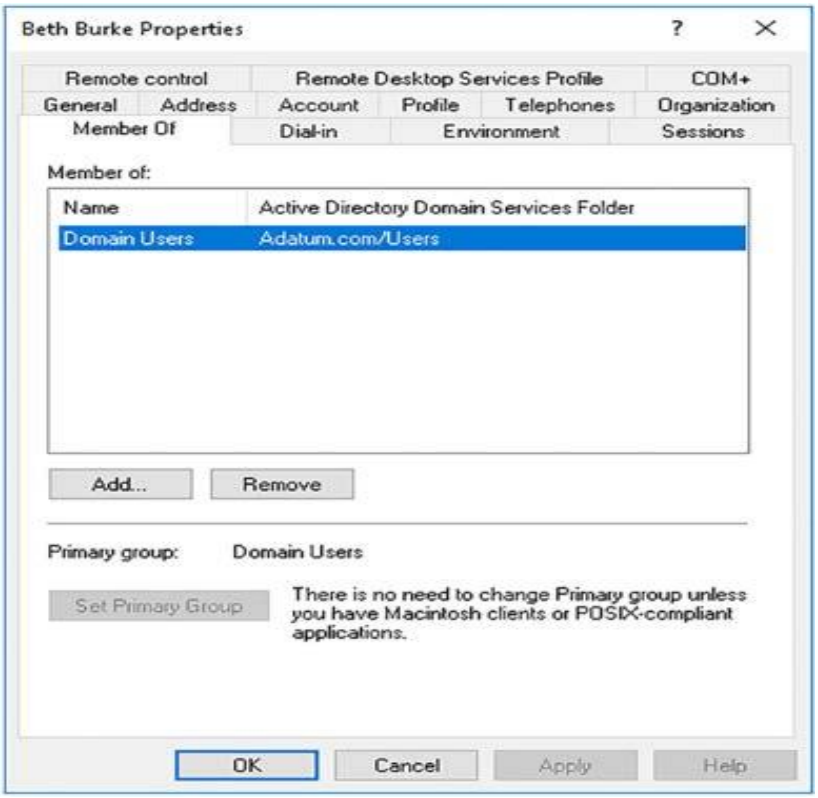
Script de logon: especifique o nome de um arquivo em lotes a ser usado como script de logon para este usuário. Você não deve especificar o caminho para este arquivo; todos os scripts devem ser armazenados na pasta compartilhada NET-LOGON (parte do SYSVOL) para que possam ser replicados para todos os controladores de domínio. Geralmente, esse campo raramente é usado. A maioria dos administradores prefere aplicar scripts de logon usando GPOs.

Pasta pessoal: é uma boa prática criar uma área de armazenamento pessoal na sua rede para cada usuário. Isso é chamado de pasta pessoal. Se você usar a variável% username% para definir uma subpasta de uma pasta compartilhada válida, o nome de usuário será aplicado quando a pasta inicial do usuário for criada automaticamente. Especifique uma letra de unidade a ser usada para mapear para a pasta inicial do usuário.

5. Na guia Membro, mostrada na Figura 38, adicione o usuário aos grupos

Figure 38. Modificando participações em grupos.

necessários e clique em OK. Os grupos são discutidos na próxima habilidade.



Fonte: (Warren, 2017, p. 50)

Configurar modelos

Se você tiver muitas contas de usuário amplamente semelhantes para adicionar, considere usar modelos para ajudar a acelerar o processo. Uma conta de usuário modelo é uma conta de usuário comum preenchida com propriedades e configurações comuns. Você copia a conta em Usuários e Computadores do Active Directory e define apenas as configurações individuais exclusivas:

Nome e Sobrenome.

Nome completo.

Nome de logon do usuário.

Senha.

As seguintes propriedades da conta do usuário são copiadas quando você cria e copia uma conta de modelo:

Associações de grupo.

Diretórios Domésticos.

Configurações de perfil.

Scripts de logon.

Horário de início de sessão.

Configurações de senha.

Nome do departamento.

Gerente.

Gerenciando contas de usuário

Quando suas contas de usuário foram criadas, você deve estar preparado para gerenciar essas contas. Você pode usar Usuários e Computadores do Active Directory ou o Windows PowerShell para executar as seguintes tarefas típicas de gerenciamento:

Redefinindo senhas Clique com o botão direito do mouse na conta de usuário relevante e clique em Redefinir Senha. No Windows PowerShell, use o cmdlet Set-ADAccountPassword. Por exemplo, para redefinir a senha de Beth Burke, use o seguinte comando:

Desbloquear contas: clique com o botão direito do mouse na conta de usuário relevante e clique em Desbloquear. No Windows PowerShell, use o cmdlet Unlock-ADAccount.

Renomeando contas: clique com o botão direito do mouse na conta de usuário relevante e clique em Renomear. Digite o novo nome completo e pressione Enter. Na caixa de diálogo Renomear usuário, mostrada na Figura 39, digite as

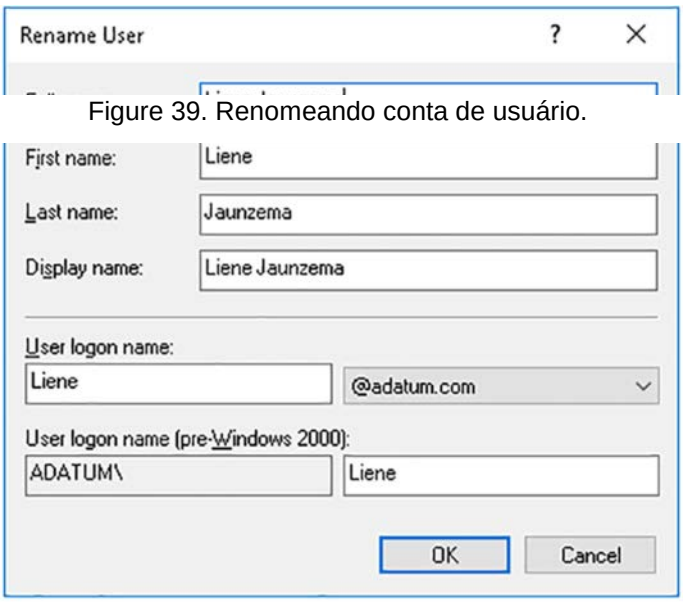


Figure 39. Renomeando conta de usuário.

informações relevantes e clique em OK. No Windows PowerShell, use o cmdlet Rename-ADObject.

Fonte: (Warren, 2017, p. 52)

Movendo usuários: Clique com o botão direito do mouse na conta de usuário relevante e clique em Mover. Na caixa de diálogo Mover, clique no novo local e, em seguida, clique em OK. No Windows PowerShell, use o cmdlet Move-ADObject. Por exemplo, para mover Beth Burke de TI para Marketing no domínio Adatum.com, use o seguinte comando:

Move-ADObject -Identity 'CN = Beth Burke, OU = IT, DC = Adatum, DC = com' -TargetPath 'OU = Marketing, DC = Adatum, DC = com'

Você pode usar os cmdlets do Windows PowerShell para executar todas as tarefas comuns de gerenciamento de usuários. A Tabela 1 lista os cmdlets importantes e explica seu uso.

Tabela 1. Cmdlets do Windows PowerShell para gerenciamento de usuários.

Cmdlet	Descrição
New-ADUser	Cria contas de usuário.
Set-ADUser	Modifica as propriedades das contas de usuário.
Remove-ADUser	Exclui contas de usuário.
Set-ADAccountPassword	Redefine a senha de uma conta de usuário.
Set-ADAccountExpiration	Modifica a data de validade de um usuário
Unlock-ADAccount	Desbloqueia uma conta de usuário.
Enable-ADAccount	Habilita uma conta de usuário.
Disable-ADAccount	Desativa uma conta de usuário.

Fonte: (Warren, 2017, p. 53)

Adicionar e gerenciar contas de computador

Para dispositivos de computador de sua organização, você deve criar uma conta do AD DS para o computador. Isso ajuda a proteger a infraestrutura de

rede da sua organização, porque o computador pode se identificar no domínio do AD DS do qual é membro.

Por padrão, as contas de computador são criadas e armazenadas no contêiner Computadores padrão. Esta não é uma UO e, portanto, você não pode delegar administração nela nem aplicar GPOs a ela. Em organizações maiores, considere colocar seus computadores nas UOs em vez do contêiner Computadores.

Para adicionar um computador ao domínio, você deve entrar com uma conta que tenha privilégios suficientes. De fato, você precisa de permissões para adicionar um objeto de computador ao domínio. Além disso, você precisa de privilégios de administrador local no próprio computador. Por padrão, os seguintes grupos têm permissões para criar objetos de computador em qualquer UO:

Administradores da empresa.

Administradores de domínio.

Administradores.

Operadores de conta.

Usuários padrão podem adicionar no máximo 10 computadores a um domínio. Use o console do Editor de Interfaces de Serviços do Active Directory (ADSI Edit) para aumentar a cota de conta da máquina se 10 for insuficiente.

Para adicionar um computador com Windows 10 a um domínio em uma única etapa, use o seguinte procedimento:

1. Entre no computador com Windows 10 como administrador local.

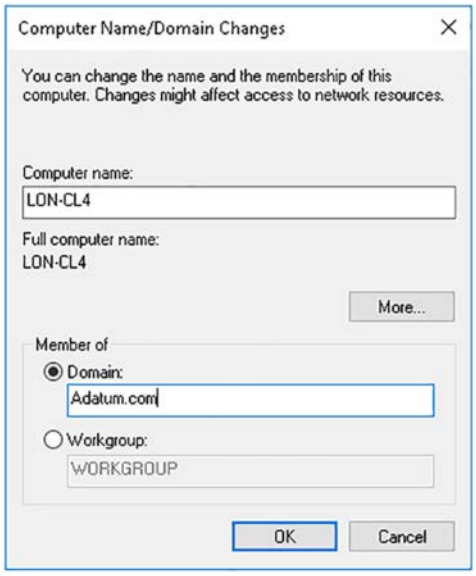
2. Clique com o botão direito do mouse em Iniciar e, em seguida, clique em Sistema.

3. No sistema, clique em Configurações avançadas do sistema.

4. Na caixa de diálogo Propriedades do sistema, na guia Nome do computador, clique em Alterar.

5. Na caixa de diálogo Alterações no nome do computador / domínio,

Figure 40. Adicionando um computador ao domínio.



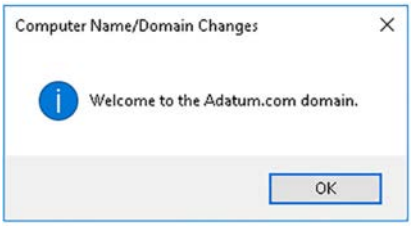
mostrada na Figura 40, selecione Domínio e digite o nome do domínio.

Fonte: (Warren, 2017, p. 54)

6. Clique em OK e, na caixa de diálogo Segurança do Windows, insira o Nome de usuário e a Senha de uma conta de usuário no domínio que tenha privilégios suficientes para adicionar uma conta de computador, então clique ESTÁ BEM.

7. Na caixa de diálogo pop-up Alterações de nome / domínio do

Figure 41. Concluindo o processo de adição ao domínio.



computador, mostrada na Figura 41, Clique OK.

Fonte: (Warren, 2017, p. 55)

8. Clique em OK no aviso de que você deve reiniciar o computador.

9. Na caixa de diálogo Propriedades do sistema, clique em Fechar e, quando solicitado, clique em Reinicie agora.

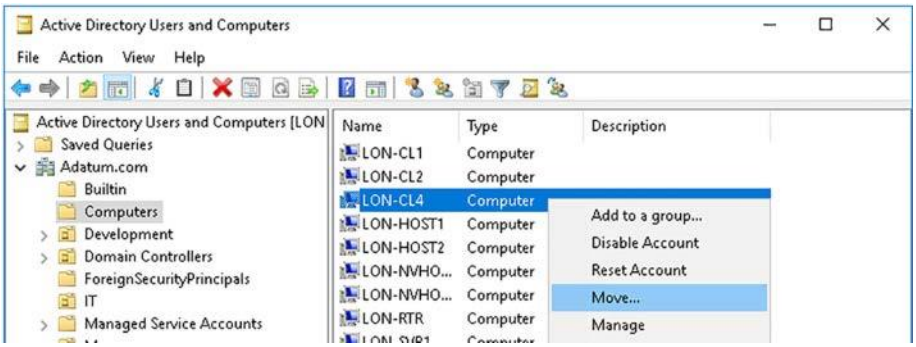
10. Entre usando uma conta de domínio no seu computador.

11. No seu controlador de domínio, abra Usuários e computadores do Active Directory.

12. Navegue até o contêiner Computadores e localize a nova conta de computador.

13. Se necessário, clique com o botão direito do mouse na nova conta e clique em Mover, conforme mostrado na Figura 42.

Figure 42. Movendo a conta do computador.



Fonte: (Warren, 2017, p. 55)

14. Selecione o novo local da UO para o computador e clique em OK.

Você também pode usar o Windows PowerShell. A Tabela 2 lista os cmdlets comuns de gerenciamento de computador do Windows PowerShell.

Tabela 2. Os cmdlets de gerenciamento de computador do Windows PowerShell.

Cmdlet	Descrição
New-ADComputer	Cria uma nova conta de computador.
Get-ADComputer	Exibe as propriedades de uma conta de computador.
Set-ADComputer	Modifica as propriedades de uma conta de computador.
Remove-ADComputer	Exclui uma conta de computador.
Test-ComputerSecureChannel	Verifica ou repara a relação de confiança

	entre um computador e o domínio.
Reset-ComputerMachinePassword	Redefine a senha para uma conta de computador.

Fonte: (Warren, 2017, p. 56)

6.3. Criar e gerenciar grupos do Active Directory e unidades organizacionais

Além de usuários e computadores, todas as florestas do AD DS contêm grupos e OUs. Você pode usar ferramentas gráficas para criar e gerenciar grupos e OUs ou, alternativamente, usar os cmdlets do Windows PowerShell.

Em alguns sentidos, grupos e OUs são semelhantes; ambos contêm objetos, como usuários, computadores ou mesmo outros grupos ou UOs. Estritamente falando, no entanto, os grupos têm membros e as OUs contêm objetos.

UOs e grupos também são usados de maneiras diferentes. Normalmente, você implementa grupos no AD DS para atribuir direitos ou permissões, enquanto usa OUs para otimizar o gerenciamento por meio do aplicativo de GPOs ou por delegação de gerenciamento.

Configurar aninhamento de grupo

No Windows Server 2016, é possível configurar o aninhamento de grupos. Este é o processo de adicionar um grupo como membro de outro grupo. O objetivo por trás do agrupamento de grupos é o dimensionamento. Se às vezes é lógico agrupar usuários e atribuir permissões (ou direitos) ao grupo, em vez de indivíduos que compõem o grupo, ocasionalmente, é lógico agrupar grupos. Isso é particularmente relevante em grandes florestas do AD DS com vários domínios.

Para facilitar o aninhamento de grupos, o AD DS no Windows Server 2016 oferece suporte a três escopos e dois tipos de grupos. Esses são:

Escopos define o escopo (ou alcance) das habilidades:

Local do domínio: só podem ser concedidos direitos e permissões na autoridade de segurança local. Ou seja, uma conta local do domínio pode receber

apenas direitos e permissões sobre recursos no domínio local. Um grupo local do domínio pode conter:

Usuários de qualquer domínio na floresta.

Grupos globais de qualquer domínio na floresta.

Grupos universais de qualquer domínio na floresta.

Global: podem ser concedidos direitos e permissões para qualquer recurso em qualquer domínio da floresta. Um grupo global pode conter:

Usuários de qualquer lugar da floresta.

Grupos globais do mesmo domínio.

Universal: Usado para operações em toda a floresta e permite a atribuição de permissões e direitos em qualquer domínio da floresta. Grupos universais podem conter:

Contas de usuário, grupos globais e outros grupos universais de qualquer domínio em toda a floresta.

Tipos: Defina a finalidade do grupo:

Segurança: Usado para atribuir permissões ou direitos. Também pode ser usado para fins de listas de distribuição de email.

Distribuição: usado apenas para fins de listas de distribuição de email.

6.3.1. Criar, configurar e excluir grupos

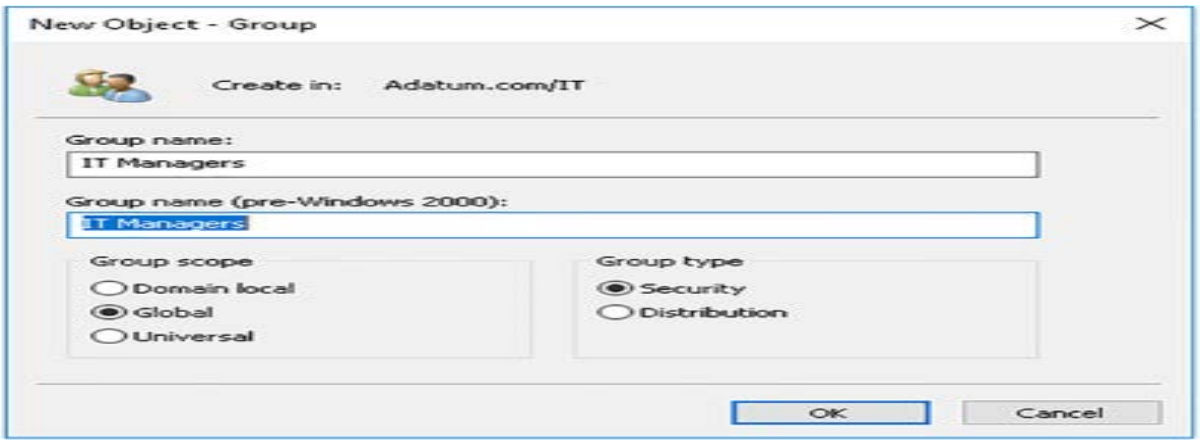
O processo de criação e gerenciamento de grupos é direto. Assim como os usuários e computadores, você pode usar Usuários e Computadores do Active Directory, o Centro Administrativo do Active Directory ou o Windows PowerShell para executar todas as tarefas de gerenciamento de grupo.

Para criar um grupo em Usuários e Computadores do Active Directory, use o seguinte procedimento:

1. Localize a UO apropriada. Clique com o botão direito do mouse na UO, aponte para Novo e clique em Grupo.

2. Na caixa de diálogo New Object - Group, mostrada na Figura 43, digite

Figure 43. Adicionando grupo.



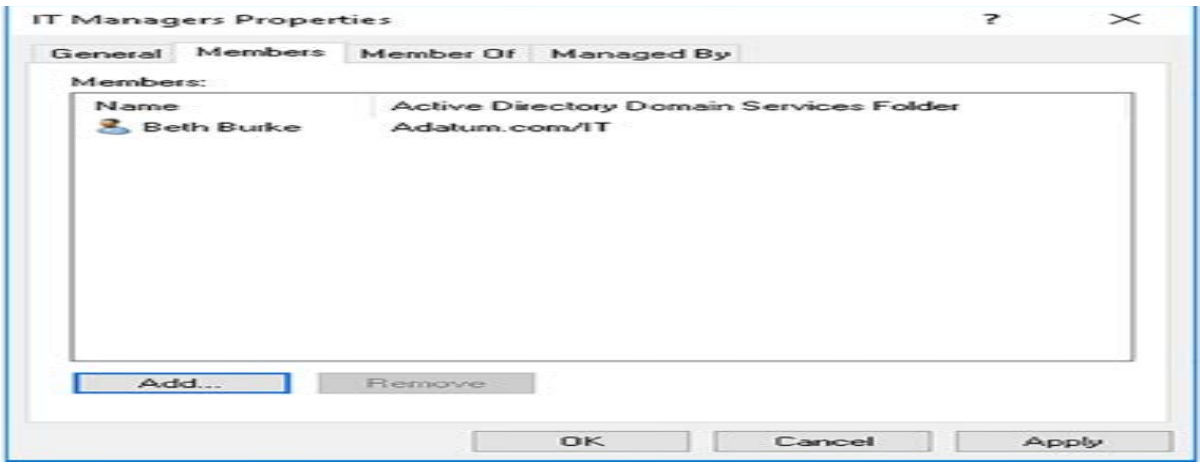
o nome do grupo.

Fonte: (Warren, 2017, p. 66)

3. Especifique o escopo e o tipo do grupo. O padrão é segurança global. Clique OK.

Depois de adicionar o grupo, no painel de detalhes em Usuários e Computadores do Active Directory, clique duas vezes no grupo para configurar suas propriedades, incluindo membros. Para adicionar um membro, clique na guia Membros, como mostra a Figura 44, clique em Adicionar, procure e selecione seu usuário ou grupo e, em seguida, clique em OK.

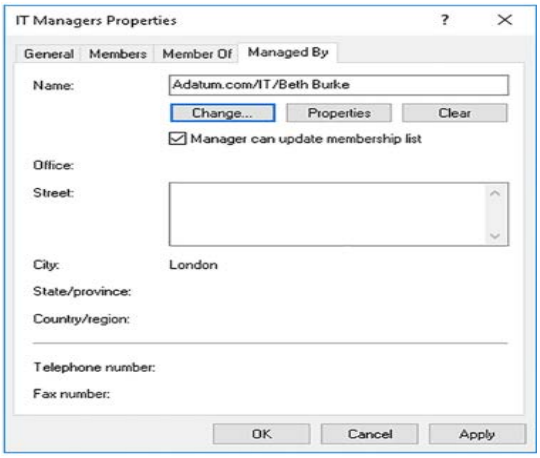
Figure 44. Configurando o grupo.



fonte: (Warren, 2017, p. 66)

Você pode configurar gerenciadores de grupos. Isso permite delegar

Figure 45. Atribuindo um gerente de grupo.



responsabilidade pelo gerenciamento do grupo, como mostra a Figura 45.

Fonte: (Warren, 2017, p. 67)

Você pode executar todas as tarefas de gerenciamento de grupo usando o Windows PowerShell. A Tabela 3 mostra os cmdlets de gerenciamento de grupo.

Tabela 3. Cmdlets do Windows PowerShell para gerenciamento de grupos.

Cmdlet	Descrição
New-ADGroup	Cria novos grupos
Set-ADGroup	Modifica propriedades de grupos
Get-ADGroup	Exibe propriedades de grupos
Remove-ADGroup	Exclui grupos
Add-ADGroupMember	Adiciona membros a grupos
Get-ADGroupMember	Exibe membros de grupos
Remove-ADGroupMember	Remove membros de um grupo
Add-ADPrincipalGroupMembership	Adiciona associação de grupo a objetos
Get-ADPrincipalGroupMembership	Exibe a associação ao grupo de objetos

Remove-ADPrincipalGroupMembership	Remove a associação ao grupo de um objeto

Fonte: (Warren, 2017, p. 67)

6.3.2. Criar e gerenciar OUs

As UOs permitem gerenciar seu domínio do AD DS mais facilmente, agrupando usuários, grupos e computadores em um contêiner e, em seguida, aplique as definições de configuração a esse contêiner usando GPOs. Além disso, você pode definir configurações de segurança em suas UOs para que um subconjunto de permissões de gerenciamento seja atribuído a um usuário ou grupo nessa UO e, portanto, objetos nessa UO; isso é conhecido como delegação.

Você pode usar o Windows PowerShell. A Tabela 4 lista os cmdlets comuns de gerenciamento da OU do Windows PowerShell.

Tabela 4. Cmdlets do Windows PowerShell para gerenciamento de OU.

Cmdlet	Descrição
New-ADOrganizationalUnit	Cria OUs
Set-ADOrganizationalUnit	Modifica propriedades de UOs
Get-ADOrganizationalUnit	Exibe propriedades de UOs
Remove-ADOrganizationalUnit	Exclui UOs.

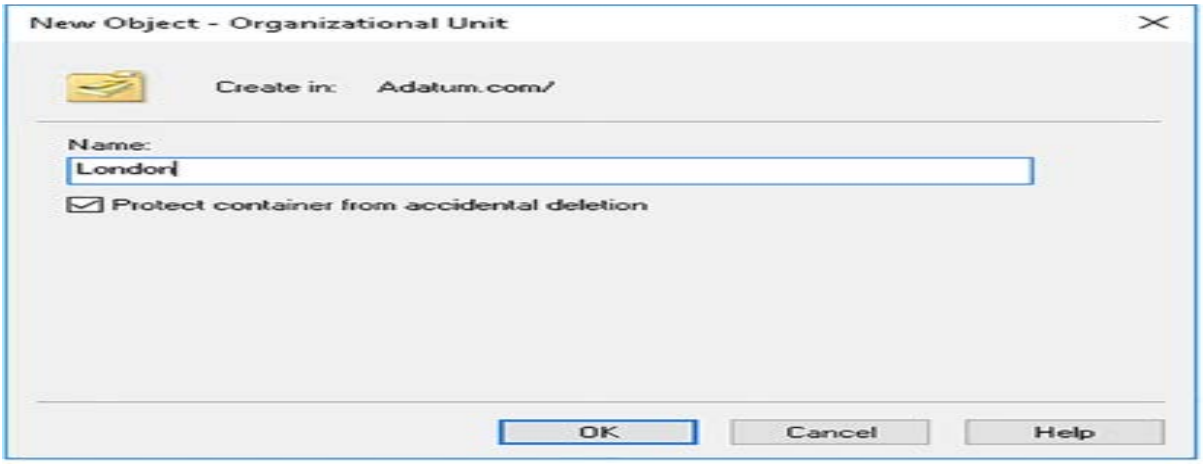
Fonte: (Warren, 2017, p. 70)

Para criar uma UO no AD DS, abra o console Usuários e Computadores do Active Directory. Navegue para o objeto de domínio e use o seguinte procedimento:

1. Clique com o botão direito do mouse no domínio (ou OU, se estiver criando OUs aninhadas), aponte para Novo e clique em Unidade Organizacional.

2. Na caixa de diálogo Novo objeto - unidade organizacional, mostrada na Figura 46, na caixa Nome, digite o nome da sua UO e clique em OK.

Figure 46. Adicionando uma OU.



Fonte: (Warren, 2017, p. 70)

Depois de criar sua UO, você pode começar a criar ou mover objetos para a UO. Depois que essa tarefa é concluída, você pode criar e vincular GPOs às UOs para definir as configurações de usuário e computador para objetos na UO.

7. GERENCIAR E MANTER O AD DS

Depois de implantar e configurar seus controladores de domínio, você deve definir contas de serviço, políticas de conta e outras configurações de segurança. Você também deve estar preparado para manter a função de servidor dos Serviços de Domínio Active Directory (AD DS) para garantir a disponibilidade desse serviço de identidade crítico. Essa manutenção pode envolver a execução de procedimentos de backup e recuperação e a manutenção do banco de dados do AD DS. Para organizações com vários locais, você também precisa saber como criar subredes e sites, além de configurar e gerenciar a replicação entre sites e AD DS dentro do site.

7.1. Configure a autenticação de serviço e políticas de conta

Muitos aplicativos e serviços que você instala no Windows Server são executados no contexto de segurança de uma conta de usuário, conhecida como conta de serviço. Como todas as contas de usuário, é importante que essas contas de serviço não são comprometidas. Windows Server 2016 fornece serviço

gerenciado Contas (MSAs) e Contas de serviço gerenciado por grupo (gMSAs) para ajudá-lo mais facilmente gerenciar contas de serviço.

As políticas de conta permitem controlar recursos fundamentais de segurança, como senha complexidade, duração, expiração e bloqueio. Você pode usar esses recursos para ajudar a proteger seu rede e os aplicativos e serviços executados nela.

7.1.1. Criar e configurar MSAs e gMSAs

Nas versões anteriores do Windows Server, era comum criar contas de usuário padrão para os fins de execução de aplicativos ou serviços. Por exemplo, você pode criar uma conta de usuário chamada Envie e-mail e configure o programa de e-mail que você instalou para executar no contexto do usuário de E-mail da conta. Gerenciamento de senha da conta A senha para essas contas de usuário padrão deve ser alterado periodicamente para ajudar a manter a segurança de seus aplicativos e serviços. Falha para mudança a conta senha resultados em falha do seu apps ou serviço.

Nomes principais de serviço os nomes principais de serviço (SPNs) são identificadores exclusivos para uma instância de serviço específica e são usadas para associar uma instância de serviço a um serviço conta.

Se você usar uma conta de usuário padrão com SPNs, isso poderá resultar em esforço administrativo e causar possíveis problemas de autenticação que podem resultar em aplicativa falha.

Uma solução possível é usar o sistema local (NT AUTHORITY \ SYSTEM), o sistema local serviço (NT AUTHORITY \ LOCAL SERVICE) ou o serviço de rede (NT AUTHORITY \ NETWORK SERVICE) para configurar seu aplicativo. No entanto, essas três contas podem não fornecer segurança suficiente, nem privilégios suficientes para muitas situações.

O Windows Server 2016 fornece MSAs e gMSAs para ajudá-lo a atenuar esses problemas: O que outras pessoas estão dizendo MSAs Ao contrário das contas de usuário padrão, os MSAs herdam parte de sua estrutura de objetos de computador, incluindo a maneira como as alterações de senha são tratadas. Isso fornece os seguintes benefícios: O que outras pessoas estão dizendo

Gerenciamento automático de senhas que outras pessoas estão dizendo Gerenciamento simplificado de SPN.

gMSAs: Permite estender a função de MSAs para vários servidores no seu domínio do AD DS. Isso é útil onde você está usando o balanceamento de carga. Para usar gMSAs, seu ambiente do AD DS deve atender aos seguintes requisitos:Os computadores clientes devem executar pelo menos o Windows Você deve criar uma chave raiz dos serviços de distribuição de chaves (KDS) para seu domínio pelo menos um controlador de domínio deve estar executando o Windows Server 2012 ou posterior.

Ao criar um gMSA, você deve definir a coleção de computadores que podem recuperar informações de senha do AD DS. Pode ser uma lista de objetos de computador ou um grupo do AD DS que contém os objetos de computador desejados.

No Windows Server 2016, você usa os mesmos cmdlets do Windows PowerShell para criar e gerenciar gMSAs e MSAs. Isso significa que no Windows Server 2016, todos os MSAs são gerenciados como gMSAs. Para criar gMSAs, comece criando a chave raiz do KDS. Em um controlador de domínio, use o seguinte cmdlet do Windows PowerShell para concluir esta tarefa Após criar a chave raiz do KDS, use o Módulo do Active Directory para Windows PowerShell cmdlet new-ADServiceAccount de qualquer controlador de domínio para criar seus gMSAs. Por exemplo:

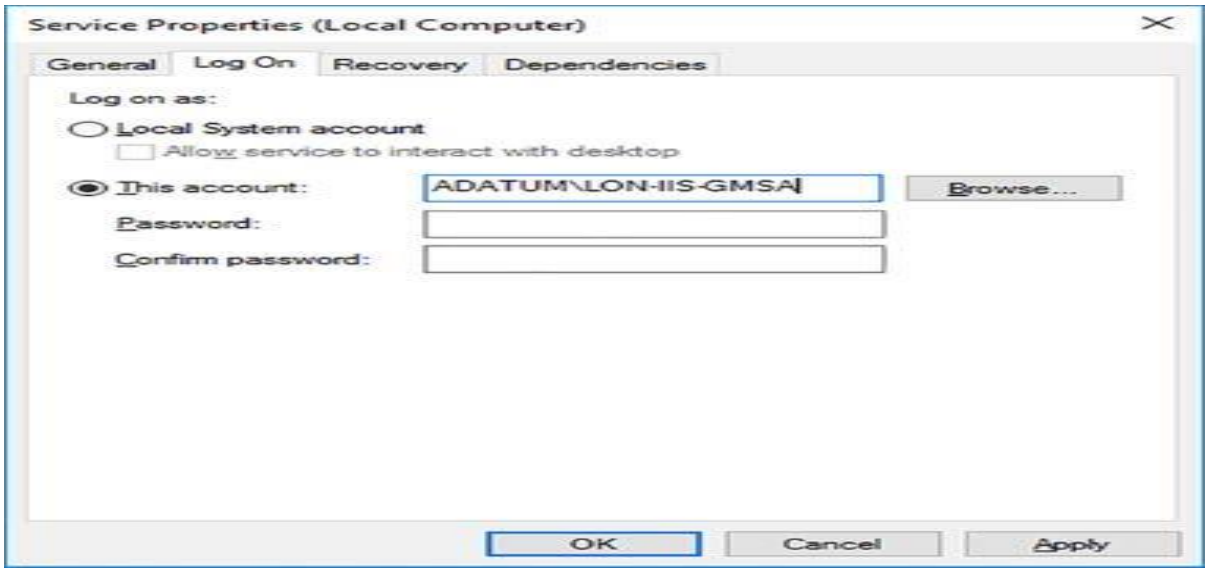
New-ADServiceAccount –Name LON-IIS-GMSA –DNSHostname LON-DC1.Adatum.com - PrincipalsAllowedToRetrieveManagedPassword LON-DC1$, LON-DC2$, LON-IIS$.

Por fim, configure o serviço ou aplicativo necessário para usar o gMSA configurado. Use o procedimento a seguir para concluir a tarefa:

1. Nos servidores de destino, no Gerenciador do Servidor, clique em Ferramentas e, em seguida, clique em Serviços.

2. Localize o serviço apropriado, clique duas vezes nele e, na guia Logon, mostrado na Figura 47, clique em Esta conta e digite o nome da sua conta. Por

Figure 47. Configurando uma conta de serviço.



exemplo, digite ADATUM \ LON-IIS-GMSA.

Fonte: (Warren, 2017, p. 80)

3. Desmarque as caixas de seleção Senha e Confirmar senha e clique em OK.

7.1.2. Gerenciar SPNs

Os SPNs são similares em conceito aos registros de alias do DNS (Sistema de Nomes de Domínio) (CNAMEs), mas, em vez de apontar para um registro de computador em uma zona DNS, os SPNs apontam para contas de domínio. Os SPNs são usados pelo Kerberos, o protocolo de autenticação nos controladores de domínio do Windows Server 2016 AD DS. Eles associam um serviço a uma conta de logon de serviço, permitindo que um aplicativo de computador cliente solicite que o serviço autentique uma conta, mesmo se o aplicativo cliente não souber o nome da conta. Antes que o Kerberos possa usar SPNs, os serviços devem registrar seus SPNs no AD DS.

Os SPNs consistem em vários elementos e devem ser exclusivos na sua floresta do AD DS. Esses elementos são:

Classe de serviço: Identifica a classe de um serviço. Por exemplo, www para um servidor da web. Existem várias classes de serviço conhecidas.

Host: O nome do computador no qual o serviço é executado. Normalmente, este é um serviço totalmente qualificado. Nome de domínio (FQDN), como LON-SVR2.Adatum.com.

Porta: Opcionalmente usada para identificar o número da porta usada por um serviço. Permite diferenciar entre várias instâncias dos mesmos serviços instalados em um computador específico. Por exemplo, um site seguro usa a porta TCP 443.

Nome do serviço: Um elemento opcional baseado no nome DNS do domínio ou em um registro do localizador de serviço (SRV) ou do Mail Exchanger (MX) no domínio. Esse elemento identifica serviços que abrangem todo o domínio.

Isso cria um SPN que compreende estes elementos:

<classe de serviço> / <host>: <port> / <nome do serviço>.

Por exemplo:

WebService / LON-SVR2.Adatum.com: 443.

Geralmente, há pouco gerenciamento de SPNs necessários. Mas, ocasionalmente, pode ser necessário forçar o registro. Você pode usar a ferramenta de linha de comando Setspn.exe para registrar SPNs.

7.1.3. Configurar delegação restrita de Kerberos

Em algumas situações, aplicativos ou serviços podem fazer conexões com aplicativos ou serviços remotos instalados em outros computadores servidores. Em essência, essas conexões estão sendo feitas em nome dos computadores clientes conectados ao aplicativo ou serviço de origem.

Normalmente, esse cenário ocorre quando um serviço front-end se comunica com um serviço de back-end em nome de usuários em computadores clientes usando o aplicativo de back-end. Para suportar esse cenário,

É necessário usar a delegação de autenticação; é o processo em que a autoridade de autenticação (no Windows Server 2016, este é um controlador de domínio) permite que um serviço atue em nome de outro serviço. O problema é que, nas versões anteriores do Windows Server, não há como impedir que a delegação

se estenda para um terceiro ou mesmo quarto serviço. A delegação restrita de Kerberos no Windows Server 2016 evita isso.

Para configurar a delegação restrita para permitir que um aplicativo front-end acesse um serviço de back-end em nome dos usuários, você deve usar um dos seguintes cmdlets para o principal de segurança que executa seu serviço front-end:

Get-ADUser.

Get-ADComputer.

Get-ADServiceAccount.

Em seguida, passe esse objeto principal de segurança como argumento usando o PrincipalsAllowed-Parâmetro ToDelegateToAccount com um dos seguintes cmdlets do Windows PowerShell:

Set-ADUser.

Set-ADComputer.

Set-ADServiceAccount.

Por exemplo:

$ computer = Get-ADComputer -Identity WEBSVR1.

Set-ADComputer LON-SVR2 -PrincipalsAllowedToDelegateToAccount $ computer.

7.1.4. Configurar contas virtuais

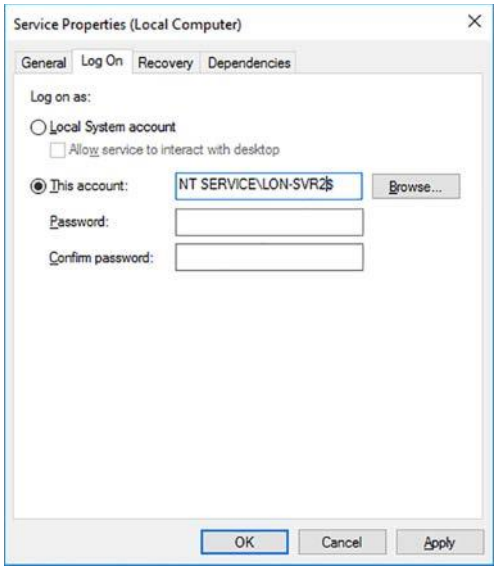
Você não pode criar, excluir ou gerenciar as senhas para contas virtuais. Eles existem automaticamente e são uma representação da conta do computador local quando usados para acessar aplicativos ou recursos.

Para configurar um serviço para usar uma conta virtual, use o seguinte procedimento:

1. No Gerenciador do Servidor, clique em Ferramentas e, em seguida, clique em Serviços.

2. Localize o serviço apropriado, clique duas vezes nele e, em seguida, na guia Logon, mostrada em Figura 48, clique em Esta conta e digite o nome

Figure 48. Configurando uma conta virtual para um serviço.



da sua conta. Por exemplo, digite NT SERVICE \ LON-SVR2 $.

Fonte: (Warren, 2017, p. 83)

3. Desmarque as caixas de seleção Senha e Confirmar senha e clique em OK.

7.1.5. Configurar diretivas de conta

As políticas de conta permitem definir configurações relacionadas à senha, incluindo a política de senha, as configurações de bloqueio de conta e as configurações de política Kerberos. Essas configurações são acessíveis através da Diretiva de Domínio Padrão no Editor de Gerenciamento de Diretiva de Grupo.

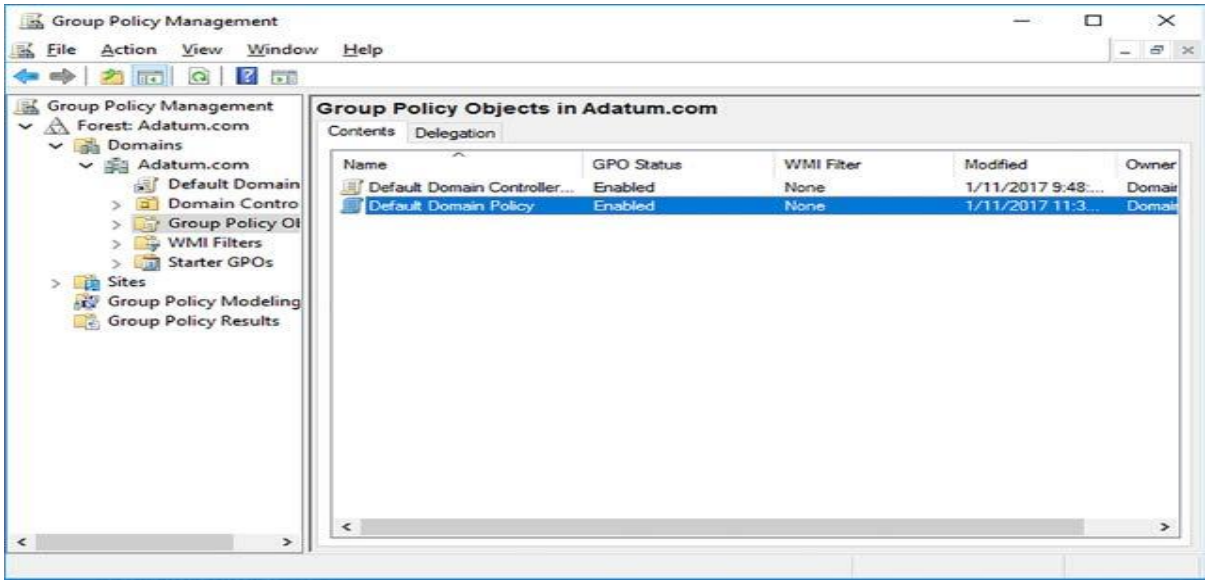
Para visualizar e definir essas configurações, use o seguinte procedimento:

1. No Gerenciador do Servidor, clique em Ferramentas e, em seguida, clique em Gerenciamento de Diretiva de Grupo.

2. Em Gerenciamento de Diretiva de Grupo, expanda sua floresta, expanda a pasta Domínios e expanda o domínio que deseja configurar.

3. Clique na pasta Objetos de Diretiva de Grupo e, no painel Detalhes, como mostra a Figura 49, clique com o botão direito do mouse na Diretiva de Domínio Padrão e clique em Editar.

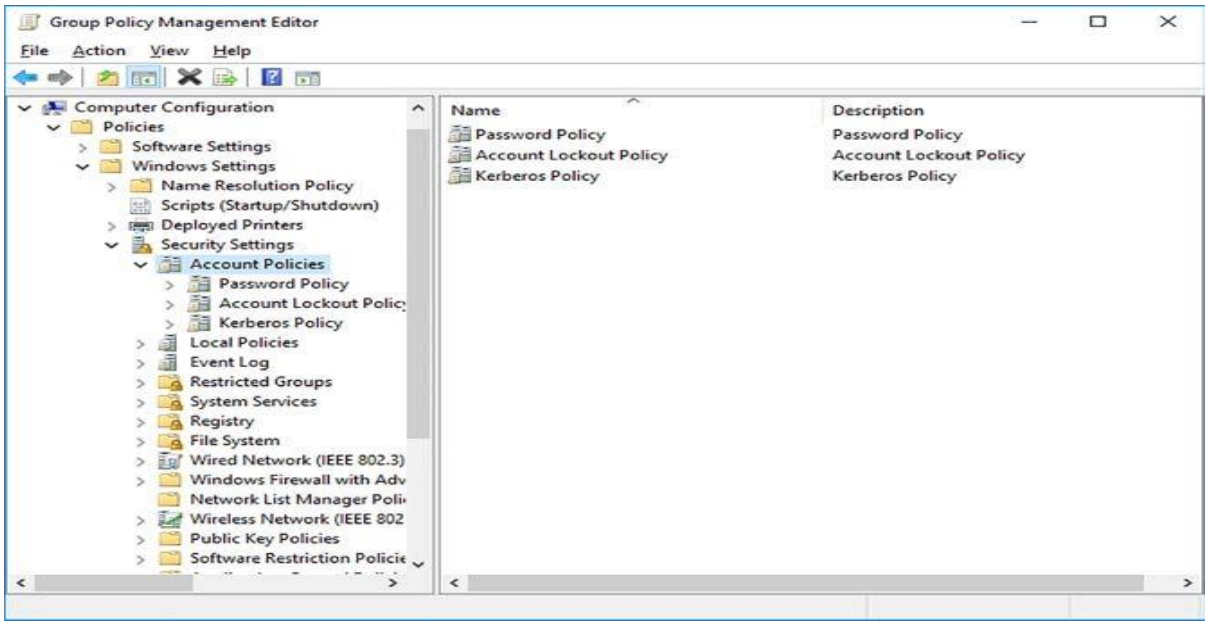
Figure 49. Exibindo objetos de diretiva de grupo padrão



fonte: (Warren, 2017, p. 84)

4. No Editor de Gerenciamento de Diretiva de Grupo, no nó Diretiva de Domínio Padrão, expanda Configuração do Computador, expanda Diretivas, expanda Configurações do Windows, expanda Configurações de segurança e clique

Figure 50. Editando diretivas de conta na diretiva de



em Diretivas de conta, como mostra a Figura 50.

Fonte: (Warren, 2017, p. 84)

Definir configurações de diretiva de domínio e senha de usuário local

As políticas de senha permitem definir configurações que controlam como as senhas dos usuários do domínio são gerenciadas. Para definir configurações de diretiva de senha de domínio, no Editor de Gerenciamento de Diretiva de Grupo, na pasta Diretivas de Conta, na pasta Diretiva de Senha, você pode definir as seguintes configurações de senha:

Aplicar histórico de senhas: Impede que os usuários reutilizem senhas. O valor padrão é 24.

Idade máxima da senha: Garante que os usuários alterem suas senhas dentro do período definido. O padrão é 42 dias.

Idade mínima da senha: Impede que os usuários alterem suas senhas até esse período expirar. Ajuda a impedir que os usuários passem por uma série de senhas de volta à sua senha favorita, alterando sua senha 24 vezes muito rapidamente. O padrão é um dia.

Comprimento mínimo da senha: Garante que as senhas não sejam muito curtas. Senhas mais longas são mais difíceis de adivinhar, especialmente se senhas complexas também forem aplicadas. Padrão tem sete caracteres.

A senha deve atender aos requisitos de complexidade: Ajuda a garantir que as senhas sejam mais difíceis de adivinhar. Ativado por padrão. Quando ativada, as senhas devem atender a vários requisitos de complexidade:

- Não é possível conter o nome do usuário ou o nome de usuário da conta.
- Deve conter pelo menos seis caracteres.
- Deve conter caracteres de pelo menos três dos quatro grupos a seguir:
- Letras maiúsculas [A – Z].
- Letras minúsculas [a – z].
- Numerais [0–9].
- Caracteres não alfanuméricos especiais, como! @ #) (* & ^%.

Armazenar senhas usando criptografia reversível: Fornece suporte para aplicativos mais antigos que exigem conhecimento da senha de um usuário. Em muitos casos, armazenar senhas usando criptografia reversível é o mesmo que armazenar senhas em texto não criptografado e deve ser evitado, a menos que seja absolutamente necessário. Isso está desativado por padrão.

7.1.6. Delegar gerenciamento de configurações de senha

Para delegar o gerenciamento das configurações de senha, você pode usar o seguinte Assistente para Delegação de Controle nos Usuários e Computadores do Active Directory, conforme descrito no procedimento a seguir:

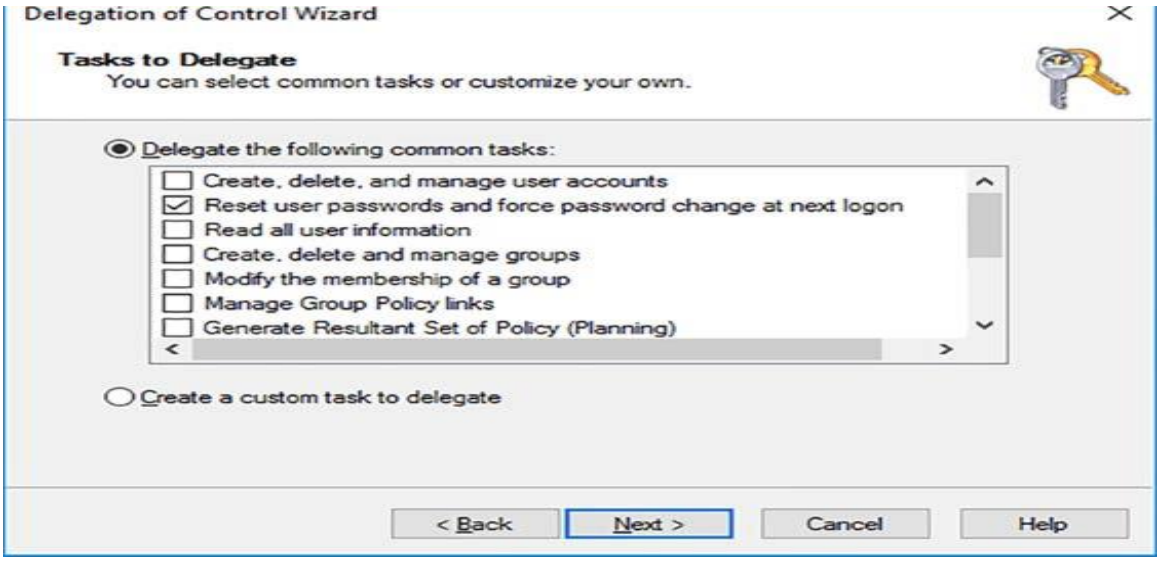
1. Em Usuários e Computadores do Active Directory, localize e clique com o botão direito do mouse na UO apropriada e clique em Delegar Controle.

2. No Assistente para Delegação de Controle, na página Bem-vindo, clique em Avançar.

3. Na página Usuários ou Grupos, clique em Adicionar e localize o usuário ou grupo ao qual você deseja delegar o gerenciamento de configurações de senha. Clique em OK e, em seguida, clique em Avançar.

4. Na página Tarefas a delegar, mostrada na Figura 51, na lista Delegar as tarefas comuns a seguir, marque a caixa de seleção Redefinir senhas de usuário e forçar alteração de senha no próximo logon e clique em Avançar. Clique em

Figure 51. Delegando o gerenciamento de configurações



Concluir quando solicitado.

Fonte: (Warren, 2017, p. 95)

7.1.7. Configurar e aplicar objetos de configurações de senha

Você só pode configurar políticas de conta para seu domínio; você não pode configurar uma política separada para unidades organizacionais (OUs) dentro do seu domínio. Nas versões anteriores do Windows Server, a necessidade de configurar uma política de conta diferente para grupos de negócios ou localizações geográficas geralmente significava a necessidade de configurar vários domínios na floresta do AD DS.

No entanto, no Windows Server 2016, você pode implementar várias diretivas de conta usando PSOs (Password Settings Objects). Usando PSOs, você pode implementar e configurar políticas de conta que afetam usuários e grupos, em vez de apenas contêineres, o que significa que você tem um controle administrativo mais direcionado.

Para implementar PSOs, você deve criar o PSO e vinculá-lo ao objeto de usuário ou grupo apropriado. Por exemplo, para configurar uma política de senha mais rigorosa para contas de administrador, use o seguinte procedimento de alto nível:

1. Crie um grupo de segurança global Secure Admins.

2. Adicione as contas de usuário necessárias ao grupo.

3. Crie um PSO e vincule-o ao grupo Secure Admins.

Se você vincular vários PSOs a um único objeto, as seguintes regras de precedência serão aplicadas:

Se não houver PSOs vinculados a um usuário, o Windows Server AD DS aplicará as configurações de Política de Conta de Domínio Padrão.

Se você vincular um PSO diretamente a um objeto de usuário, esse PSO terá precedência sobre qualquer PSO vinculado a grupos dos quais o usuário é membro.

Se você vincular PSOs a grupos, o AD DS comparará os PSOs a todos os grupos de segurança global de qual o objeto de usuário é um membro.

Criando PSOs com o Windows PowerShell

Para criar e aplicar PSOs usando o Windows PowerShell, use os dois cmdlets a seguir:

New-ADFineGrainedPasswordPolicy: Cria o PSO e atribui as propriedades que você define usando os parâmetros do cmdlet.

Add-FineGrainedPasswordPolicySubject: Vincula o PSO ao usuário ou grupo que você define usando os parâmetros do cmdlet.

Por exemplo, conforme mostrado na Figura 52, os seguintes comandos criam e vinculam um novo PSO nomeados Admins para o grupo de segurança global Secure Admins:

New-ADFineGrainedPasswordPolicy Admins -ComplexityEnabled: $ true

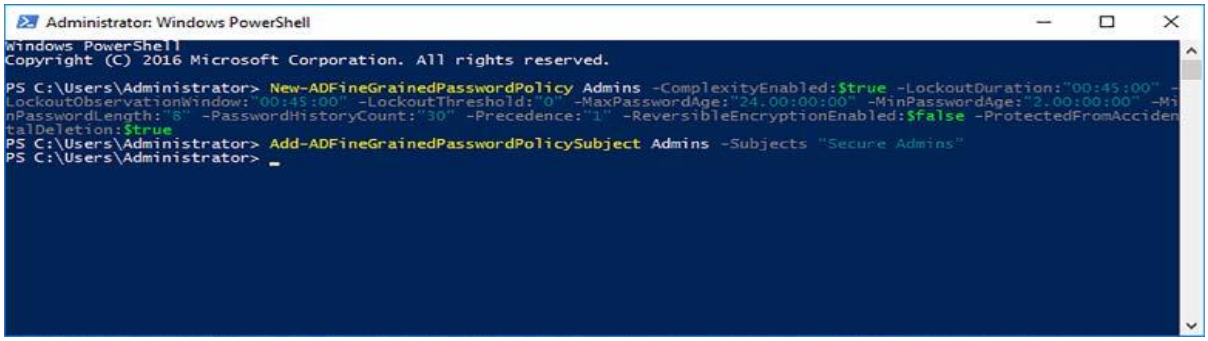
-LockoutDuration: ”00:45:00” -LockoutObservationWindow: ”00:45:00” -LockoutThreshold: ”0”

-MaxPasswordAge: ”24.00: 00: 00” -MinPasswordAge: ”2.00: 00: 00” -MinPasswordLength: ”8”

-PasswordHistoryCount: ”30” -Precedência: ”1” -ReversibleEncryptionEnabled: $ false -Protecte dFromAccidentalDeletion: $ true

Administradores Add-ADFineGrainedPasswordPolicySubject -Subject

Figure 52. Criando e aplicando um PSO com o Windows PowerShell.



“Secure Admins”

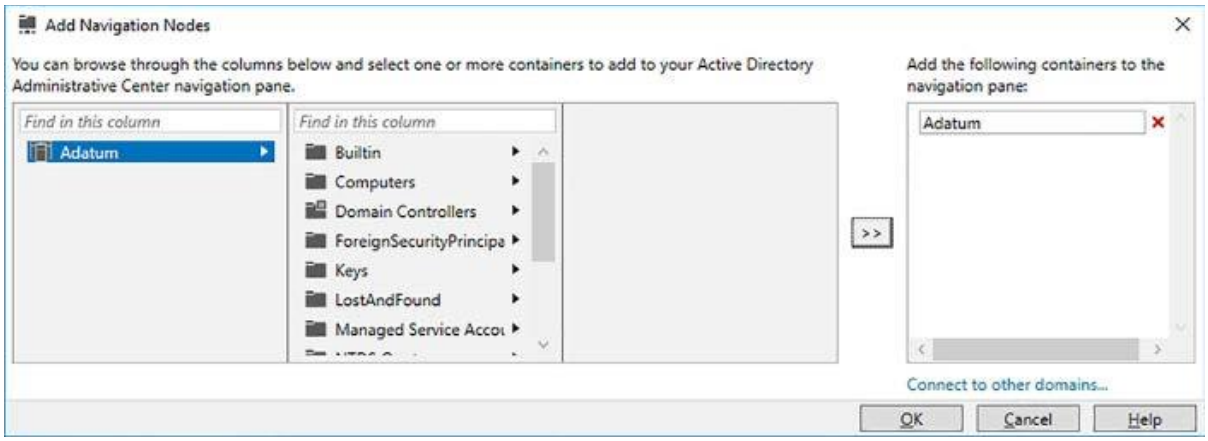
Fonte: (Warren, 2017, p. 91)

Criando PSOs com o Centro Administrativo do Active Directory

Para criar e vincular PSOs usando o console do Centro Administrativo do Active Directory, use o seguinte procedimento:

1. No Centro Administrativo do Active Directory, clique em Gerenciar, clique em Adicionar Nós de Navegação, na caixa de diálogo Adicionar nó de navegação, selecione o domínio de destino apropriado, clique no >> e clique em OK, como mostra a Figura 53.

Figure 53. Incluindo um Nó de Navegação.



Fonte: (Warren, 2017, p. 93)

2. No painel de navegação, expanda seu domínio, clique no contêiner Sistema e clique em Contêiner de configurações de senha, como mostrado na

Figure 54. Selecionando o contêiner de configurações de senha.

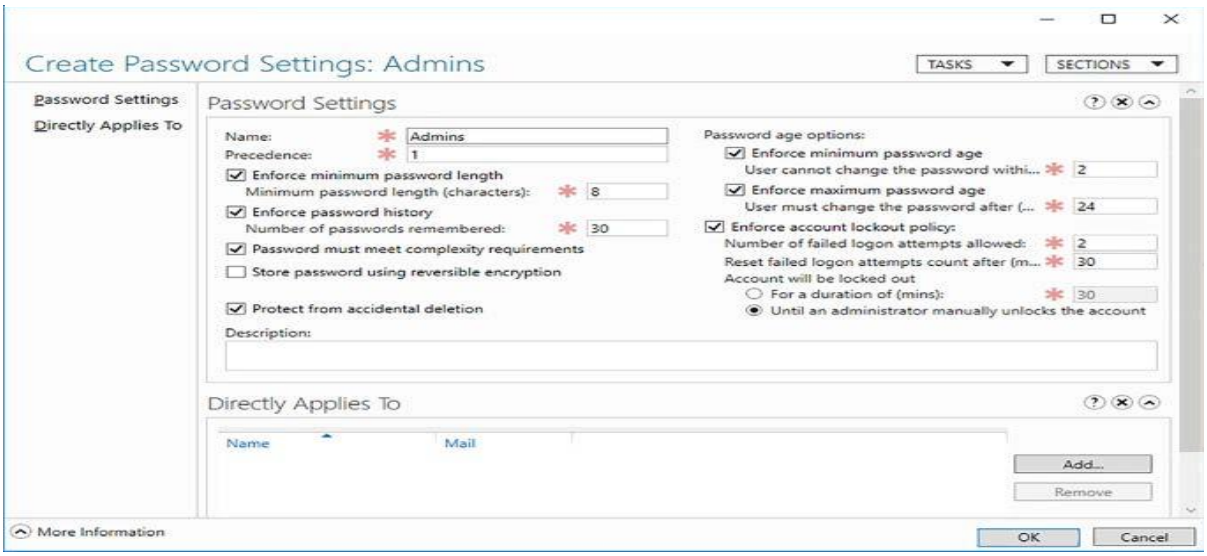
Figura 54. Pressione Enter.

Fonte: (Warren, 2017, p. 93)

3. No painel Tarefas, clique em Novo e, em seguida, clique em Configurações de senha.

4. Na caixa de diálogo Criar configurações de senha:, defina as configurações necessárias para o novo PSO, como mostra a Figura 55.

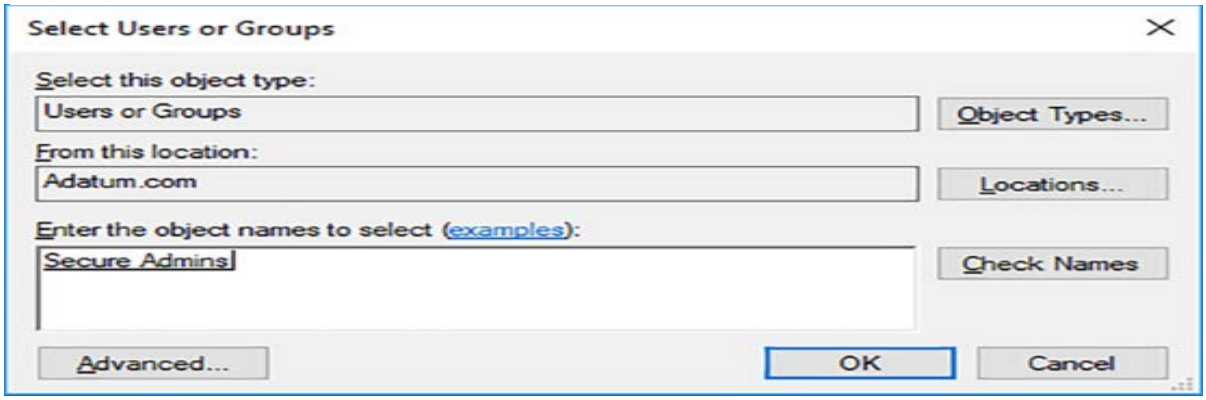
Figure 55. Criando um novo PSO.



Fonte: (Warren, 2017, p. 94)

5. Sob o título Aplica-se diretamente a, clique em Adicionar e, na caixa de diálogo Selecionar usuários ou grupos, digite o nome do usuário ou grupo

Figure 56. Selecionando o grupo ao qual o PSO está vinculado.



apropriado, conforme mostrado na Figura 56, e clique em OK

Fonte: (Warren, 2017, p. 94)

6. Clique em OK.

7.2. Manter o Active Directory

7.2.1. Gerenciar o Active Directory off-line

A maioria das operações do banco de dados do AD DS é realizada online; isto é, o serviço AD DS está em execução e está acessível na rede. No entanto, algumas operações, como a manutenção do banco de dados, devem ser executadas offline. Geralmente, isso significa que você deve reiniciar o controlador de domínio no modo de restauração de serviços de diretório (DSRM). Enquanto o servidor estiver no DSRM, ele não poderá atender a solicitações de entrada do cliente nem executar outras tarefas do AD DS. Para permitir que sua rede continue funcionando corretamente, você deve ter controladores de domínio adicionais que possam continuar a fornecer serviços relacionados ao diretório.

No Windows Server 2016, para algumas tarefas relacionadas ao banco de dados, você também pode parar o AD DSserviço em vez de reiniciar o controlador de domínio no DSRM.

Executar desfragmentação offline de um banco de dados do AD DS

Ao executar a desfragmentação offline do banco de dados do AD DS, você permite que o espaço não utilizado no banco de dados seja disponibilizado ao sistema de arquivos. Na conclusão da desfragmentação, você possui um banco de dados compactado do AD DS. Você usa a ferramenta de linha de comando NtdsUtil.exe para executar a manutenção offline do banco de dados do AD DS.

Para compactar seu AD DS, use o seguinte procedimento:

1. No seu controlador de domínio, no Gerenciador do Servidor, clique em Ferramentas e clique em Serviços para abrir o console de Serviços.

2. Pare o serviço dos Serviços de Domínio Active Directory, como mostra a

Figure 57. Parando o serviço dos Serviços de Domínio Active

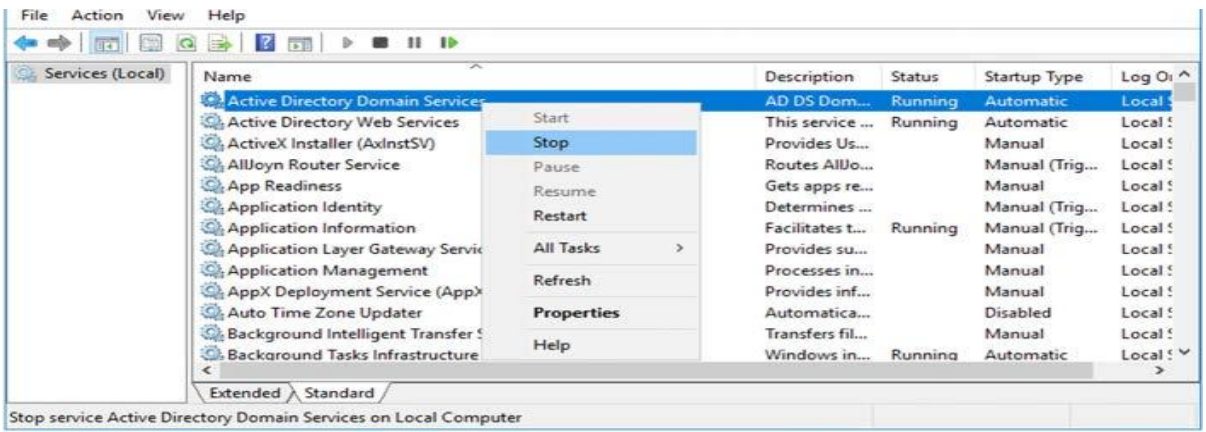


Figura 57.

Fonte: (Warren, 2017, p. 97)

3. Você é solicitado a interromper serviços relacionados, como Servidor DNS, Centro de distribuição de chaves Kerberos, Sistema de mensagens entre sites e Replicação DFS. Clique em Sim para interromper esses serviços.

4. Abra um prompt de comando elevado.

5. Execute o comando NtdsUtil.exe.

6. Execute os seguintes comandos.

Ativar instância NTDS.

Arquivos.

Compactar para C: \.

Integridade.

7. Conclua a manutenção do banco de dados executando os seguintes comandos no prompt de comando avançado:

Sair.

Sair.

Copie C: \ ntds.dit C: \ Windows \ NTDS \ ntds.dit.

Del C: \ Windows \ NTDS \ *. Log.

Saída.

8. No console de Serviços, inicie os Serviços de Domínio Active Directory. Serviços relacionados também são iniciados.

Executar limpeza de metadados

A limpeza de metadados é uma tarefa que você deve executar após remover à força um controlador de domínio da floresta do AD DS, talvez após a falha do servidor. Os metadados identificam o controlador de domínio no AD DS. Se isso não for limpo, poderá afetar a replicação do AD DS, bem como a replicação do Sistema de Arquivos Distribuídos (DFS).

Você pode executar a limpeza de metadados usando Usuários e Computadores do Active Directory e Sites e serviços do Active Directory. Você também pode usar a ferramenta de linha de comando NtdsUtil.exe.

UTILIZANDO FERRAMENTAS GRÁFICAS

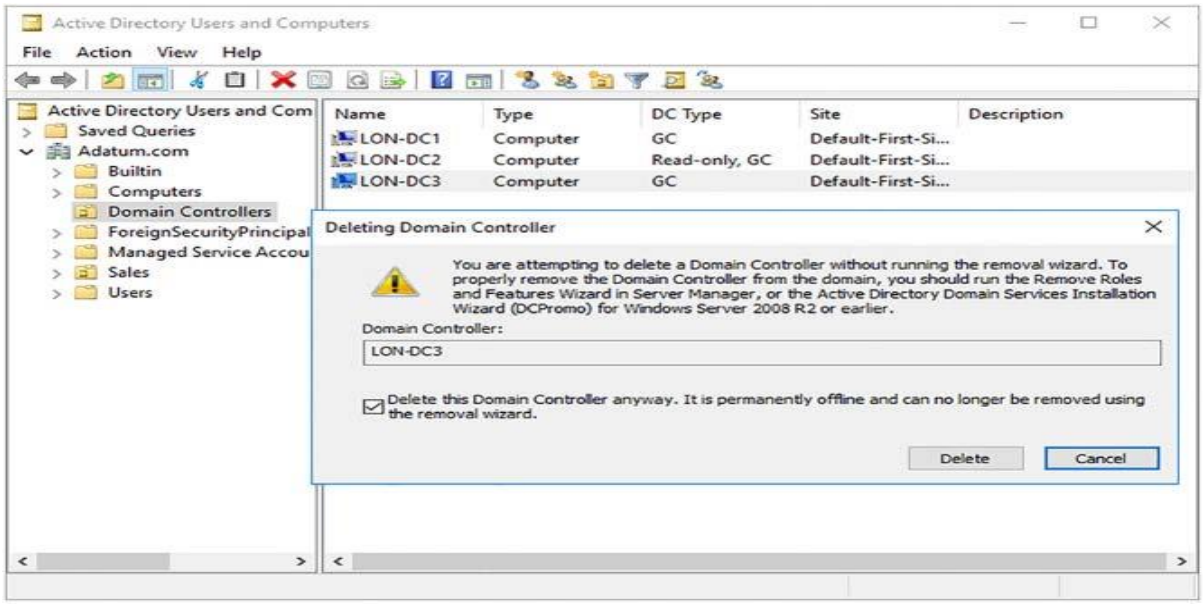
Use o procedimento a seguir para executar a limpeza de metadados do AD DS usando ferramentas gráficas:

1. Em um controlador de domínio, no Gerenciador do Servidor, clique em Ferramentas e, em seguida, clique em Active Directory Usuários E Computadores.

2. Navegue até a pasta Controladores de domínio, clique com o botão direito do mouse no controlador de domínio que você removeu anteriormente do domínio e clique em Excluir. Clique em Sim para confirmar a operação.

3. Na caixa de diálogo Excluindo controlador de domínio, mostrada na Figura 2-19, selecione a opção Excluir Na caixa de seleção Este controlador de domínio,

Figure 58. Remoção forçada de um controlador de domínio.



clique em Excluir.

Fonte: (Warren, 2017, p. 99)

4. Se o controlador de domínio for um servidor de catálogo global, clique em Sim para confirmar a exclusão.

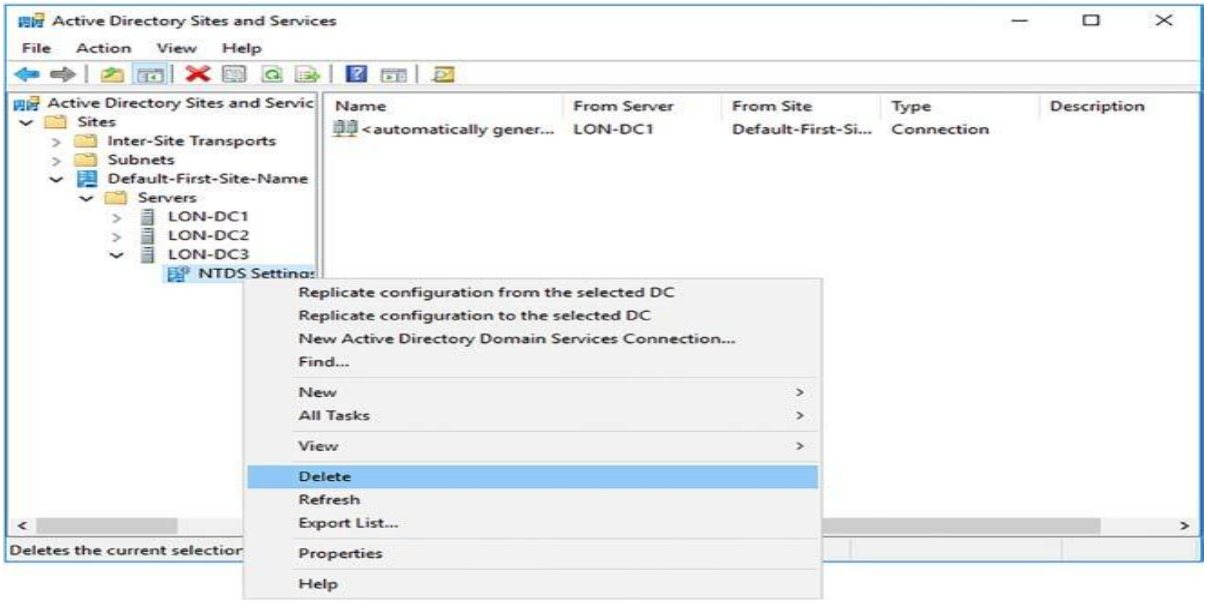
5. Se o controlador de domínio que você removeu possui uma ou mais funções de mestre de operações, mova-as para um controlador de domínio online. Clique em OK para mover as funções ao controlador de domínio sugerido. Você não pode usar um controlador de domínio diferente daquele sugerido pelo processo de exclusão. Se você deseja usar um controlador de domínio diferente para hospedar as funções de mestre de operações, mova-as após concluir o processo de limpeza de metadados. Você pode ler mais sobre a transferência de funções de mestre de operações no Skill Instalar e configurar controladores de domínio, na seção Funções de transferência e apreender operações de mestre.

6. No Gerenciador do Servidor, clique em Ferramentas e, em seguida, clique em Sites e Serviços do Active Directory.

7. Navegue até o objeto do site que contém o controlador de domínio removido. Expandir o Pasta Servers e localize o servidor que você removeu.

8. Selecione as configurações de NTDS. Clique com o botão direito do mouse no nó Configurações NTDS e clique em Excluir, como mostra a Figura 59.

Figure 59. Excluindo o objeto de configurações NTDS.



Fonte: (Warren, 2017, p. 100)

9. Na caixa de diálogo Serviços de Domínio Active Directory, clique em Sim para confirmar a exclusão.

10. Na caixa de diálogo Excluindo controlador de domínio, selecione a opção Excluir este controlador de domínio de qualquer forma, clique na caixa de seleção e clique em Excluir.

11. Se o controlador de domínio for um servidor de catálogo global, na caixa de diálogo Excluir Controlador de Domínio, clique em Sim.

12. Se o controlador de domínio que você removeu possui uma ou mais funções de mestre de operações, mova-as para um controlador de domínio online. Clique em OK para mover as funções para o controlador de domínio sugerido. Você não pode usar um controlador de domínio diferente daquele sugerido pelo processo de exclusão. Se você deseja usar um controlador de domínio diferente para hospedar as funções de mestre de operações, mova-as após concluir o processo de limpeza de metadados.

13. Por fim, no console de navegação, clique com o botão direito do mouse no controlador de domínio forçado removido e, em seguida, clique em Excluir. Clique em Sim para confirmar a operação.

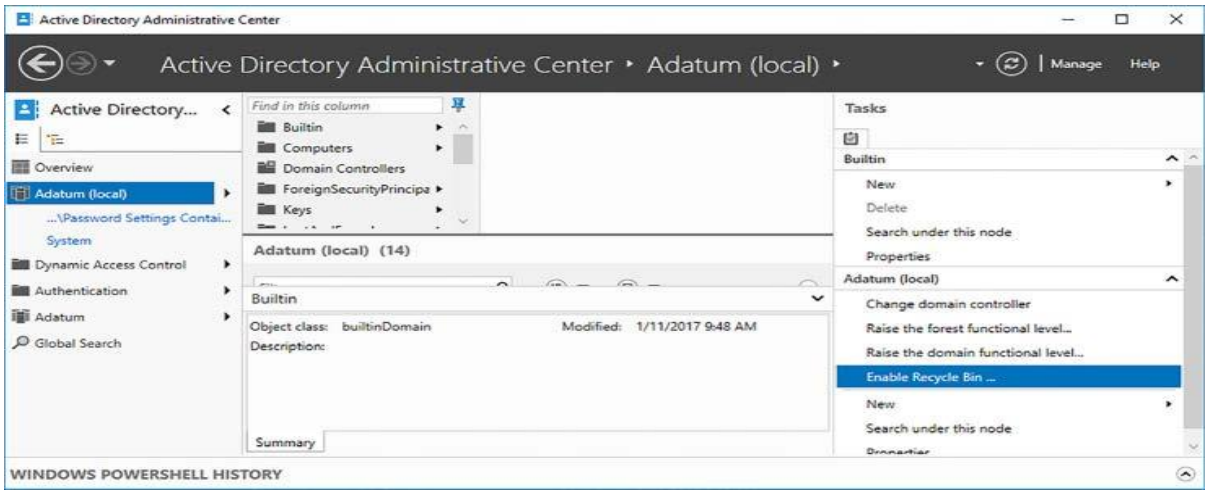
7.2.2. Backup e recuperação do Active Directory

O AD DS é um serviço crítico e, como tal, é importante que você saiba como protegê-lo contra perda e corrupção de dados. Você pode ajudar a proteger o AD DS implementando a lixeira do Active Directory e implementando um procedimento adequado de backup e recuperação.

Configurar e restaurar objetos usando a Lixeira do Active Directory

A primeira linha de proteção contra perda de dados no AD DS é a Lixeira do Active Directory. Para habilitar a Lixeira do Active Directory, no Centro Administrativo do Active Directory, mostrado na Figura 60, na lista Tarefas, clique em Habilitar Lixeira. Você também pode usar o cmdlet Windows PowerShell Enable-

Figure 60. Habilitando a Lixeira do Active Directory.

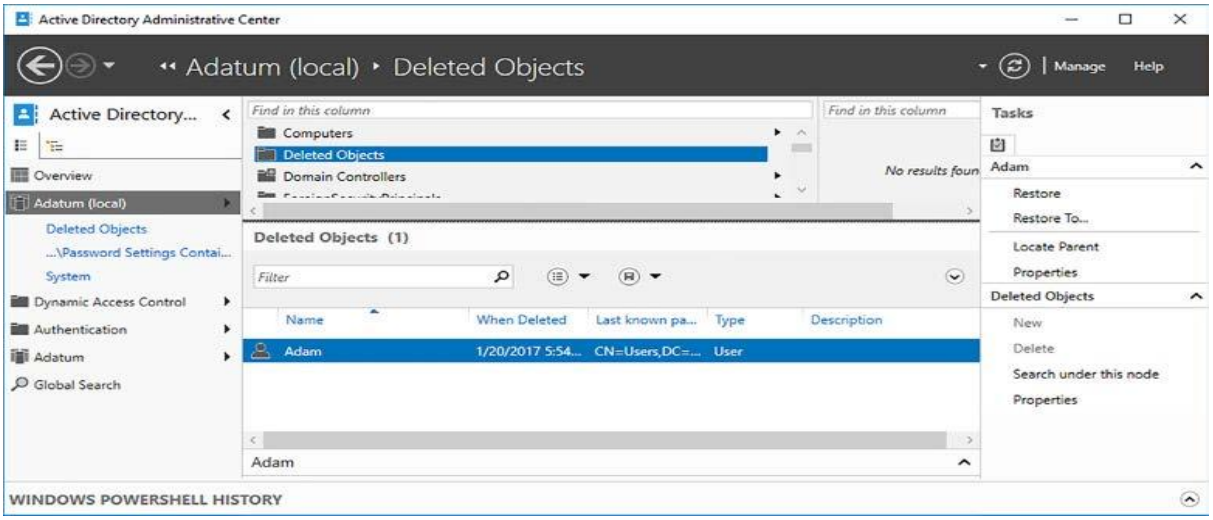


ADOptionalFeature.

Fonte: (Warren, 2017, p. 103)

Depois de habilitar a Lixeira do Active Directory, você um contêiner de Objetos Excluídos no Centro Administrativo do Active Directory. Você exclui objetos

Figure 61. Exibindo objetos excluídos na lixeira do Active Directory.



do AD, eles são armazenados na pasta Objetos Excluídos, mostrada na Figura 61.

Fonte: (Warren, 2017, p. 103)

REALIZAR RECUPERAÇÃO DE OBJETOS E RECIPIENTES

Para recuperar um objeto excluído, na pasta Objetos Excluídos, clique com o botão direito do mouse em um objeto excluído e clique em Restaurar ou Restaurar em. Escolher Restaurar permite recuperar o objeto no local original no AD DS. O uso da opção Restaurar para permite especificar um local alternativo para o objeto. Quando você recupera um objeto excluído da Lixeira do Active Directory, todos os atributos do objeto são restaurados, incluindo associações a grupos e direitos de acesso.

Por padrão, os objetos excluídos são recuperáveis por 180 dias após sua exclusão. No entanto, você pode reconfigurar esse valor alterando os valores tombstoneLifetime e msDS-DeletedObjectLifetime usando o Windows PowerShell. Por exemplo, para alterar o período recuperável para 30 dias no domínio Adatum.com, execute os dois comandos a seguir:

Set-ADObject -Identity “CN = Serviço de Diretório, CN = Windows NT, CN = Serviços, CN = Configuração, DC = Adatum, DC = com” –Partição “CN = Configuração, DC = Adatum, DC = com” –Substitua : @ {"TombstoneLifetime" = 30}.

Set-ADObject -Identity “CN = Serviço de Diretório, CN = Windows NT, CN = Serviços, CN = Configuração, DC = Adatum, DC = com” –Partição “CN = Configuração, DC = Adatum, DC = com” –Substitua : @ {"MsDS-DeletedObjectLifetime" = 30}.

Configurar snapshots do Active Directory

Um instantâneo do Active Directory é uma cópia do estado do AD DS em um determinado ponto. Você pode criar instantâneos usando a ferramenta de linha de comando NtdsUtil.exe usando o seguinte procedimento:

1. Abra um prompt de comando elevado em um controlador de domínio.

2. Execute o NtdsUtil.exe e execute os seguintes comandos, nesta ordem, para concluir o processo:

- Ativar instância NTDS.
- Instantâneo.
- Criou.
- Listar tudo.
- Sair.

Depois de criar um snapshot, você pode examiná-lo usando NtdsUtil.exe para montar o instantâneo. Depois de montá-lo, você pode usar Usuários e Computadores do Active Directory para visualizar o instantâneo. Para montar um instantâneo, use o seguinte procedimento:

1. Abra um prompt de comando elevado em um controlador de domínio.

2. Execute o NtdsUtil.exe e execute os seguintes comandos, nesta ordem, para concluir o processo:

- Ativar instância NTDS.
- Snapshots.
- Listar tudo.
- Montagem <GUID>(onde <GUID> é a identidade exclusiva da captura instantânea que você deseja montar).
- Sair.

- Sair.

3. No prompt de comando elevado, execute o seguinte comando:

dsamain -dbpath c: \ $ snap_datetime_volumec $ \ windows \ ntds \ ntds.dit -ldapport 50000.

Deixe o comando dsamain.exe em execução e conclua o próximo procedimento para visualizar um instantâneo:

1. No Gerenciador do Servidor, abra Usuários e Computadores do Active Directory.

2. Clique com o botão direito do mouse no nó raiz e clique em Alterar controlador de domínio.

3. Na caixa de diálogo Alterar servidor de diretórios, clique em <Nome do servidor de diretórios tipo A [: porta] aqui>.

4. Digite o nome do controlador de domínio seguido pelo número da porta que você especificou mais cedo. Por exemplo, digite LON-DC1: 50000 e pressione Enter e clique em OK.

Agora você pode visualizar o instantâneo montado. Quando você terminar de examinar o instantâneo,use o comando NtdsUtil.exe para desmontar o instantâneo:

1. No NtdsUtil.exe, execute os seguintes comandos:

- Ativar instância NTDS.
- Instantâneo.
- Desmontar <GUID>.
- Sair.
- Sair.

Fazer backup do Active Directory e SYSVOL

Embora útil, você não pode contar com os instantâneos da Lixeira do Active Directory ou do AD DS como forma de fornecer a recuperação do AD DS.

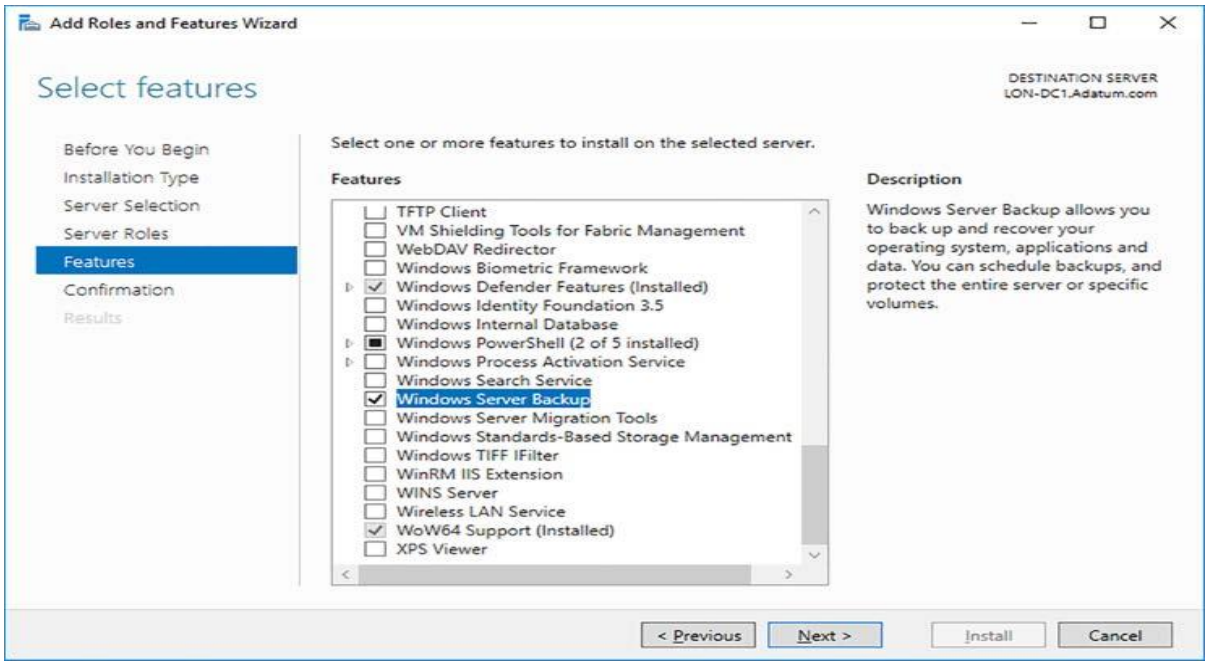
Além disso, nenhum desses métodos pode ajudar a proteger os dados armazenados no SYSVOL.

Para fornecer proteção contra perda de dados ou corrupção do AD DS, considere implementar uma solução de backup e recuperação. Você pode usar o recurso Backup do Windows Server para fornecer esta solução.

O Backup do Windows Server consiste em uma ferramenta de linha de comando, Wbadmin.exe, e um console gráfico, que você pode usar para fazer backup e, se necessário, restaurar o AD DS.

Para instalar o recurso Backup do Windows Server, você pode usar o Gerenciador do Servidor, conforme mostrado em Figura 62.

Figure 62. Instalando o Backup do Windows Server.



Fonte: (Warren, 2017, p. 106)

O Backup do Windows Server permite executar os seguintes tipos de backup:

Recuperação bare metal: no caso de falha total do servidor, talvez após a perda de um disco rígido físico, você pode usar um backup de recuperação bare metal para recuperar completamente um servidor até o ponto em que o backup foi executado.

Estado do sistema: o estado do sistema consiste na configuração do servidor, incluindo as funções e os recursos instalados. Isso inclui o banco de dados do AD DS e o conteúdo do SYSVOL.

Volumes selecionados: permite executar um backup de pastas ou arquivos específicos.

Depois de instalar o recurso Backup do Windows Server, você pode usar o Backup do Windows Server para fazer backup do AD DS usando o procedimento a seguir.

1. No seu controlador de domínio, clique em Iniciar, aponte para Acessórios do Windows e clique em Backup do Windows Server.

2. No Backup do Windows Server, no painel de navegação, clique com o botão direito do mouse em Backup Local e clique em Backup Uma vez.

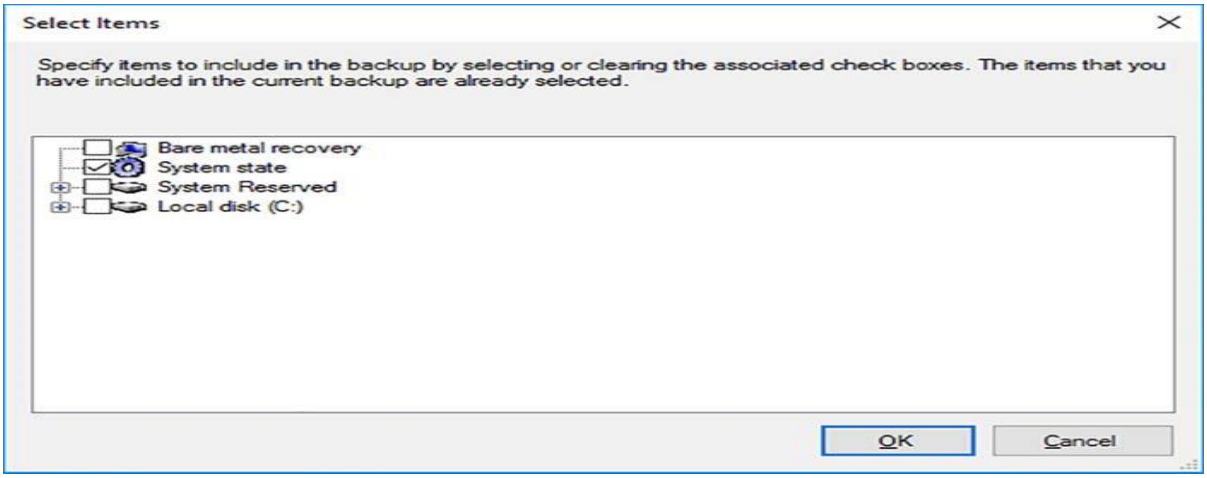
3. No Assistente de backup uma vez, na página Opções de backup, clique em Opções diferentes e clique em Avançar.

4. Selecionar Configuração, clique em Personalizado, clique em Avançar.

5. Selecionar itens para backup, clique em Adicionar itens.

6. Na caixa de diálogo Selecionar itens, marque a caixa de seleção

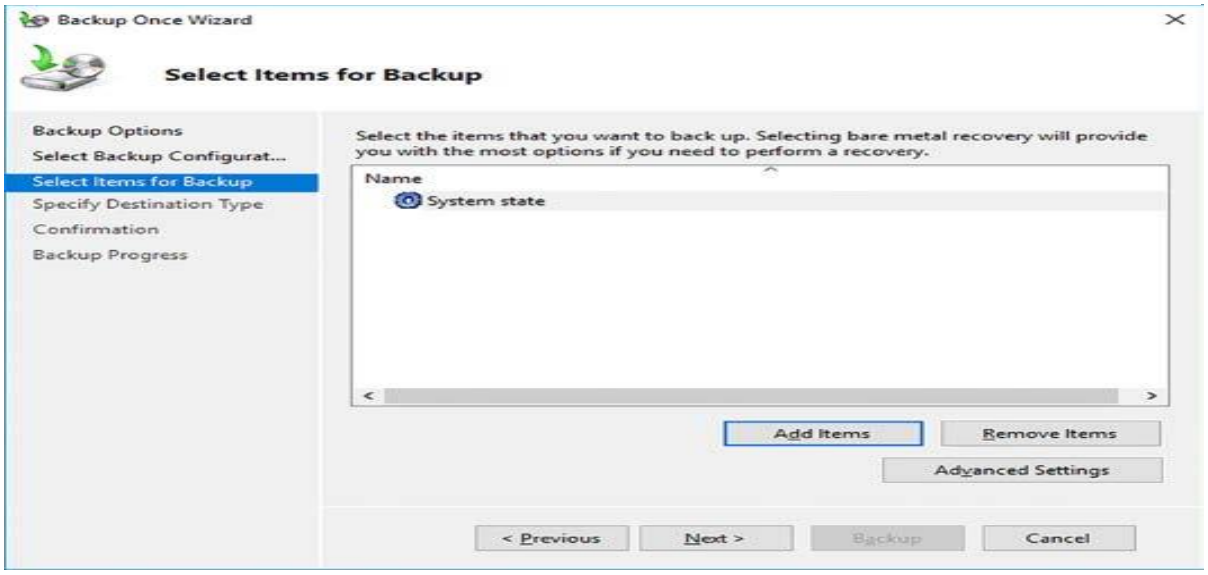
Figure 63. Selecionando os itens para backup.



Estado do sistema, conforme mostrado na Figura 63 e, em seguida, clique em OK.

Fonte: (Warren, 2017, p. 107)

Figure 64. Selecionando o estado do sistema para backup,



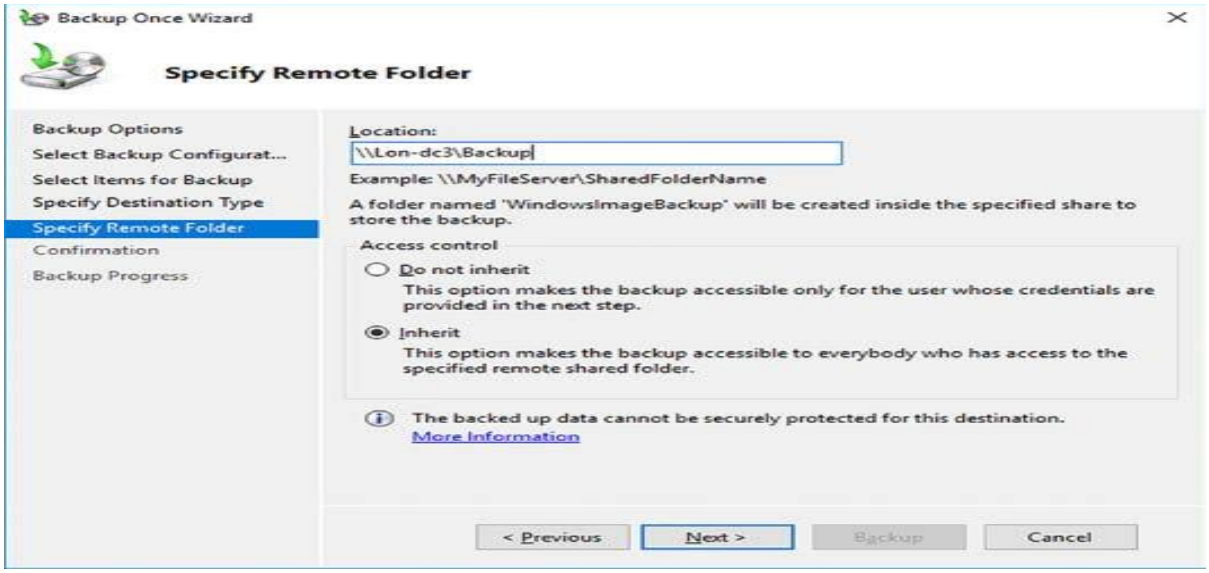
7.Selecionar itens para backup, mostrada na Figura 63, clique em Avançar.

Fonte: (Warren, 2017, p. 108)

8. Na página Especificar tipo de destino, selecione o destino. Escolha entre unidades locais e a pasta compartilhada remota. Clique em Avançar.

9. Se você selecionou uma pasta remota, na página Especificar Pasta Remota, na caixa Localização, digite o nome UNC na pasta compartilhada que

Figure 65. Especificando o Destino de Backup.



deseja usar como destino de backup, conforme mostrado na Figura 65.

Fonte: (Warren, 2017, p. 108)

10. Na seção Controle de Acesso, clique em Não Herdar ou Herdar. Essa configuração controla quem tem acesso aos arquivos de backup de destino. Se você deseja limitar o acesso ao usuário que executa o backup, clique em Não Herdar e, em seguida, clique em Avançar. Caso contrário, para ativar o backup seja acessível a todos com permissões na pasta remota, clique em Herdar e, em seguida, clique em Avançar.

11. Na página Confirmação, clique em Backup.

Executar restauração do Active Directory

Dependendo da situação, a maneira como você recupera o AD DS varia. Por exemplo, se um controlador de domínio ficar indisponível, mas você tiver um ou mais outros controladores de domínio para o mesmo domínio, basta remover o controlador de domínio, limpar os metadados e implantar um novo controlador de domínio para substituir o que falhou.

No entanto, você pode decidir que prefere restaurar o AD DS em um controlador de domínio em vez de substituir a unidade do servidor; talvez porque contenha outros aplicativos, serviços, ou dados que você não pode substituir facilmente. Ou talvez porque você só precise recuperar alguns objetos excluídos. Nessa situação, você pode executar uma operação de restauração do AD DS.

Quando você restaura o AD DS, é importante considerar a natureza do banco de dados; é um banco de dados multimaster, o que significa que, mesmo com um controlador de domínio offline, as alterações ainda podem ocorrer em outras instâncias do banco de dados em outros controladores de domínio. Se você simplesmente restaurar o banco de dados do AD DS para um momento em que você executou um backup pela última vez, esse momento será substituído pela replicação do AD DS de outros controladores de domínio quando a operação de restauração for concluída. Isso pode ser desejável; afinal, se houve alterações desde o último backup, normalmente, você deseja incluí-las.

No entanto, se você estiver tentando restaurar apenas uma parte do AD DS, não será necessário substituí-lo pelas alterações replicadas. Por exemplo, em vez de lidar com um controlador de domínio com falha, você tenta recuperar objetos que foram excluídos acidentalmente. Se você executou uma operação de backup e, posteriormente, excluiu inadvertidamente um objeto do AD DS, essa exclusão seria replicada após a operação de restauração.

Para ajudar a atenuar esse problema, você pode executar operações de restauração não autoritativa ou de restauração autorizada. Usar uma restauração autoritativa significa que os dados restaurados não são substituídos por alterações replicadas.

Para executar uma operação de restauração não autorizada do AD DS, inicie o controlador de domínio no DSRM. Em seguida, abra o console de backup do Windows Server e use o Assistente de restauração para restaurar os dados do estado do sistema de um backup anterior. Este é um procedimento simples. Em seguida, inicie seu controlador de domínio normalmente. As alterações feitas desde o último backup agora são replicadas para o controlador de domínio.

Para executar uma operação autorizada de restauração do AD DS, inicie o controlador de domínio no DSRM, restaure o Estado do Sistema e abra um prompt de comando elevado. No prompt de comando, execute o comando NtdsUtil.exe. Em seguida, execute os seguintes comandos:

Restauração autoritativa.

Restaurar objeto <DN do objeto>.

O DN do objeto terá a seguinte aparência: CN = Adam, OU = Sales, DC = adatum, DC = com. Reinicie seu controlador de domínio normalmente. Se você deseja marcar uma UO inteira como autoritativa, no prompt NtdsUtil.exe, execute os seguintes comandos:

Restauração autoritativa.

Restaurar subárvore <DN do objeto>.

Os objetos marcados como autoritativos não são substituídos e são replicados a partir do controlador de domínio restaurado em toda a floresta.

7.2.3. Gerenciar controladores de domínio somente leitura

Um RODC é um controlador de domínio que contém uma cópia somente leitura do AD DS. Você pode usar RODCs para permitir implantar controladores de domínio em escritórios nos quais a segurança física não pode ser garantida.

A implantação de RODCs é abordada no Capítulo 1: Instalar e configurar os Serviços de Domínio Active Directory, Habilidade 1.1: Instalar e configurar controladores de domínio, na seção Instalar e configurar um RODC.

Configurar diretiva de replicação de senha para RODC

Por padrão, os RODCs não armazenam informações confidenciais relacionadas à senha. Consequentemente, quando quando um usuário entra, o RODC encaminha a solicitação de entrada para um controlador de domínio gravável na sua organização.

No entanto, para melhorar a usabilidade, você pode definir que contas específicas de usuário e computador possam ser armazenadas em cache no RODC, permitindo a autenticação local. Você faz isso definindo uma política de replicação de senha do RODC. Geralmente, você adicionaria apenas os usuários e computadores que estão no mesmo site local que o RODC à política de replicação.

Para configurar uma política de replicação para um RODC, use dois grupos de segurança Local do Domínio:

Grupo de replicação de senha do RODC: permitido Adicione usuários ou computadores a este grupo para permitir que suas senhas sejam armazenadas em cache no RODC.

Grupo de replicação de senha do RODC: negado Adicione usuários ou computadores a este grupo para impedir que suas senhas sejam armazenadas em cache no RODC.

Esses grupos são criados automaticamente quando você implanta um RODC e permite configurar a política de replicação de senha em todos os RODCs. Porém, se você tiver vários escritórios de ramificação e, portanto, vários RODCs, é mais seguro configurar um grupo separado para cada RODC para a replicação de senha permitida. Nesta instância, remova o Grupo de replicação de senha permitida

do RODC e adicione um grupo que você criou manualmente e adicione os membros necessários para essa ramificação. Use o seguinte procedimento para concluir esta tarefa:

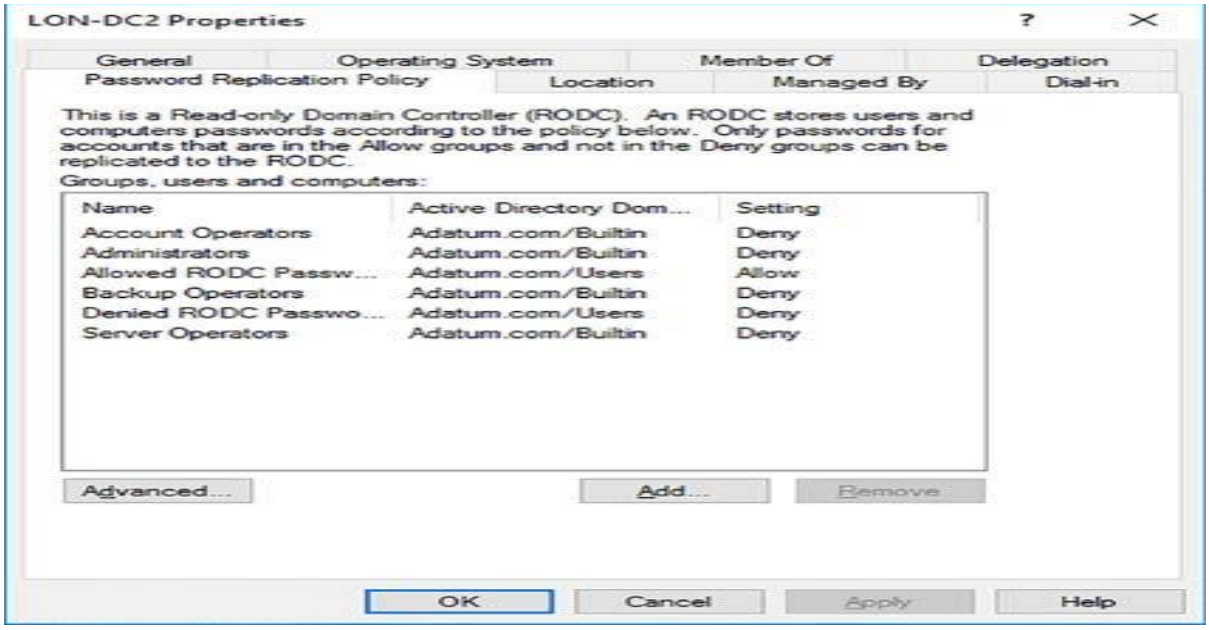
1. Em Usuários e computadores do Active Directory, crie um grupo de segurança global que contenha usuários e computadores com permissões.

2. Localize a UO dos controladores de domínio.

3. Clique com o botão direito do mouse no seu RODC e clique em Propriedades.

4. Na caixa de diálogo Propriedades, na guia Política de Replicação de Senha, mostrada na Figura 2-28, remova o Grupo de Replicação de Senha Permitida do RODC.

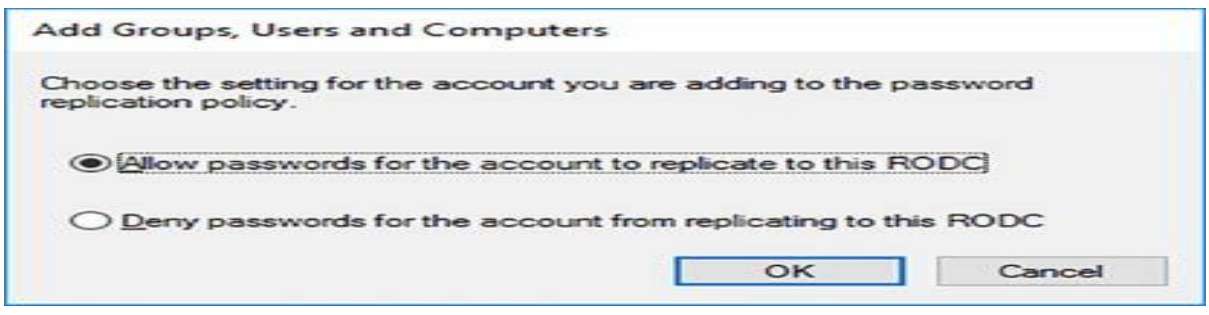
Figure 66. Configurando uma política de replicação de senha do RODC.



Fonte: (Warren, 2017, p. 111)

5. Clique em Adicionar e, como mostrado na Figura 67, clique em Permitir senhas para a conta replicar para este RODC para a conta que você está

Figure 67. Especificando a política de permissão.



adicionando à política de replicação de senha e, em seguida, clique em OK.

Fonte: (Warren, 2017, p. 112)

6. Na caixa de diálogo Selecionar usuários, computadores, contas de serviço ou grupos, digite o nome do grupo cujas senhas dos membros devem ser replicadas para este RODC e clique em OK duas vezes.

7. Adicione os usuários e computadores necessários ao grupo que você acabou de adicionar.

Você pode concluir um procedimento semelhante para modificar a política de replicação de negação específica do servidor. Remova o grupo de replicação de senha negada do RODC da política de replicação de senha e adicione seu próprio grupo aos membros cujas senhas não serão replicadas no RODC de destino.

Você pode usar a exibição Avançada na guia Diretiva de replicação de senha para exibir quais senhas de usuário ou computador são replicadas no RODC. Você também pode determinar a política efetiva para um usuário ou computador selecionado. Use o seguinte procedimento:

1. Em Usuários e computadores do Active Directory, na UO Controladores de Domínio, clique com o botão direito do mouse em seu RODC e clique em Propriedades.

2. Na guia Política de replicação de senha, clique em Avançado.

3. Na caixa de diálogo Política de replicação de senha avançada, na guia Uso da política, mostrada na Figura 2-30, na lista Exibir usuários e computadores que atendem aos seguintes critérios, clique em: Contas cujas senhas estão armazenadas neste controlador de domínio somente leitura Permite ver quais usuários e computadores tiveram suas senhas armazenadas em cache no RODC.

Contas que foram autenticadas para este controlador de domínio somente leitura Permite ver quais usuários e computadores se conectaram usando o RODC.

4. Use o botão preencher previamente senhas para recuperar senhas para usuários listados. Isso pode ajude a reduzir o tempo de entrada para usuários configurados.

5. Na guia Política resultante, adicione usuários ou computadores para determinar qual é a política de senha resultante para os objetos selecionados. Isso é útil quando você tem vários grupos de permissões ou negações configurados na guia Política de replicação de senha.

7.2.4. Gerenciando a replicação do AD DS

O AD DS é um banco de dados que reside nos controladores de domínio do Windows Server e consiste em várias partições. Esses são:

Esquema: uma partição no nível da floresta que raramente muda e mantém o esquema da floresta.

Configuração: uma partição no nível da floresta que também muda raramente e contém os dados de configuração para a floresta.

Domínio: uma partição em todo o domínio que muda frequentemente e uma cópia gravável da partição é armazenada em todos os controladores de domínio.

Alterações nas partições de esquema e configuração são raras, consequentemente, a maior parte do tráfego de replicação do AD DS são alterações na partição do domínio, como a criação de novos objetos (usuários, grupos, computadores) e a atualização de seus atributos (propriedades como senhas, participações em grupos etc.). Como administrador do AD DS, uma de suas funções é para monitorar e gerenciar a topologia e o tráfego de replicação.

A replicação do AD DS é o processo de sincronização das várias cópias do banco de dados do AD DS em toda a floresta. Essa replicação tem as seguintes características:

Multimaster Com exceção de certos elementos específicos, o AD DS é um banco de dados multimaster. Em essência, isso significa que todas as cópias são graváveis e podem ser atualizadas. Isso oferece a vantagem de remover pontos únicos de falha e também pode melhorar o desempenho.

Controladores de domínio baseados em pull extraem alterações de seus parceiros de replicação em vez de enviar por push.

Refinado Para evitar conflitos de replicação, a replicação é baseada em atributos de objetos e não em objetos inteiros. Isso reduz as chances de um conflito que poderia ocorrer se o mesmo objeto for alterado em dois controladores de domínio ao mesmo tempo.

Reconhecimento do site Como a maioria das alterações ocorre na partição de domínio, todos os controladores de domínio em um domínio solicitam essas alterações. Para ajudar a gerenciar links de rede mais lentos entre locais, você pode configurar sites do AD DS e configurar como a replicação do AD DS é tratada entre sites. Isso é conhecido como replicação entre sites.

Topologia gerada automaticamente O Windows Server gera a topologia de réplica do AD DS automaticamente, criando uma infraestrutura resiliente e eficiente. Em muitas circunstâncias, talvez você não precise reconfigurar manualmente a topologia.

Ao discutir a replicação do AD DS, é útil ter em mente que existem dois tipos de replicação:

Intrasite Isso ocorre entre controladores de domínio no mesmo site do AD DS. O Windows Server gerencia a replicação do AD DS, supondo que redes persistentes de alta velocidade conectem controladores de domínio em um site. A replicação intra-site geralmente requer pouca intervenção manual, porque o Windows Server a gerencia com eficiência automaticamente. No entanto, você deve criar e implementar uma infraestrutura de site AD DS adequada e colocar controladores de domínio no site apropriado.

Entre sites: Isso ocorre entre controladores de domínio em diferentes sites do AD DS. O Windows Server gerencia a replicação assumindo que os controladores de domínio podem não estar conectados por redes persistentes de alta velocidade. Você tem mais controle manual sobre o processo de replicação, incluindo o intervalo e a programação.

Monitorar e gerenciar a replicação

A replicação intra-site consiste em uma rede de objetos de conexão entre controladores de domínio, que são parceiros de replicação. Os objetos de conexão

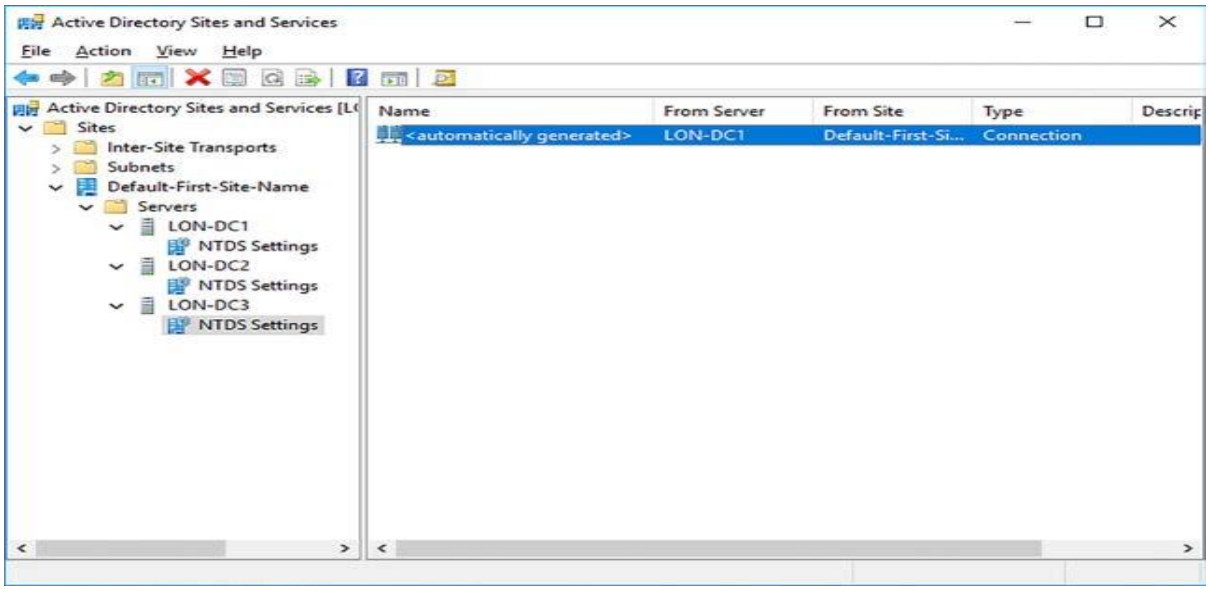
são caminhos de replicação unidirecionais e baseados em pull entre um controlador de domínio e seu parceiro de replicação.

Um componente chamado verificador de consistência do conhecimento (KCC) gera uma topologia otimizada para replicação criando esses objetos de conexão automaticamente. Essa topologia contém objetos de conexão suficientes para criar no máximo três saltos entre dois controladores de domínio, reduzindo assim os atrasos na propagação dos dados de replicação.

Se você implantar um controlador de domínio adicional em um site ou, inversamente, remover um, o verificador de consistência do conhecimento gera novamente a topologia de replicação para explicar a alteração.

A Figura 68 mostra os objetos de conexão no site Default-First-Site-Name no domínio Adat.com.

Figure 68. Visualizando um Objeto de Conexão.



Fonte: (Warren, 2017, p. 115)

Embora você possa criar manualmente objetos de conexão persistentes em um site, se desejar, isso geralmente não é necessário nem recomendado; isso ocorre porque o verificador de consistência do conhecimento não avalia objetos de conexão criados manualmente. É mais provável que você precise criar e configurar objetos de conexão para gerenciar a replicação entre sites. Isso é discutido na Habilidade 2.3: Configurar o Active Directory em um ambiente corporativo complexo, na seção Configurar sites e sub-redes do AD DS.

Você pode visualizar e gerenciar a replicação do AD DS usando a ferramenta Sites e Serviços do Active Directory, como mostra a Figura 2-31. Por exemplo, você pode forçar a replicação em um objeto de conexão entre dois controladores de domínio usando o seguinte procedimento:

1. Nos Sites e Serviços do Active Directory, navegue até o objeto de servidor que você deseja atualizar.

2. No objeto Servidor, clique no nó Configurações NTDS e, no painel de detalhes, clique com o botão direito do mouse no objeto <gerado automaticamente>.

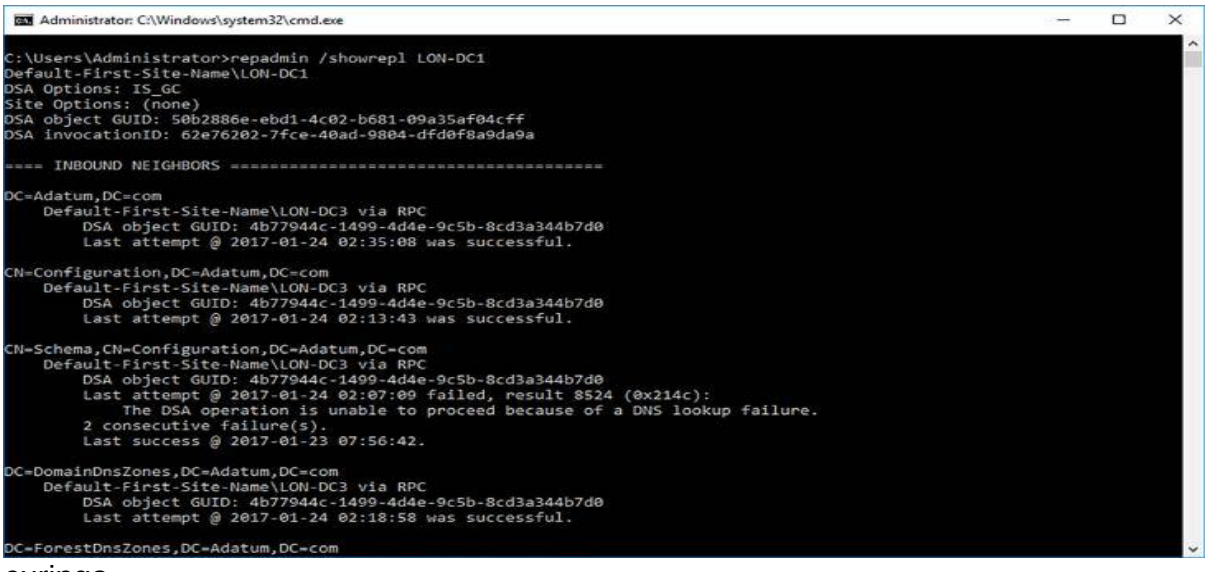
3. Clique em Replicar agora no menu de contexto. Isso puxa as alterações do parceiro de replicação designado.

Você também pode usar Repadmin.exe e as ferramentas de linha de comando DcDiag.exe:

Repadmin Use esta ferramenta para verificar o status da replicação nos controladores de domínio ou para reconfigurar a topologia de replicação:

Exibir os parceiros de replicação para um controlador de domínio usando repadmin / showrepl DC_LIST, como mostra a Figura 69. Substitua DC_LIST pelos nomes dos seus controladores de domínio. Você pode usar um asterisco como

Figure 69. Executando Repadmin.



curinga.

Fonte: (Warren, 2017, p. 117)

Exibir objetos de conexão para um controlador de domínio usando repadmin / showconn DC_LIST.

Exiba metadados sobre um objeto usando repadmin / showobjmeta DC_LIST Object. Substitua o objeto pelo nome distinto do AD DS ou pela GUID do seu objeto.

Inicie o verificador de consistência do conhecimento usando repadmin / kcc.

Forçar a replicação entre parceiros usando repadmin / replicate Destination_DC_LIST Source_DC_Name Naming_Context.

Sincronize um controlador de domínio com todos os parceiros de replicação usando repadmin /syncall DC / A / e.

DcDiag Use Dcdiag.exe para executar testes na topologia de replicação do AD DS, como mostra a Figura 2-33. Você também pode usar vários parâmetros para executar testes específicos, incluindo: FrsEvent, DFSREvent, Intersite, KccEvent, Replications, Topology e VerifyReplicas.

Configurar replicação para RODCs

Os RODCs, por sua natureza, existem em diferentes locais físicos dos controladores de domínio graváveis. Normalmente, isso significa que eles existem em um site diferente do AD DS. Portanto, qualquer configuração de replicação do RODC é entre sites e não entre sites. Isso requer que você tenha configurado corretamente os objetos de site no AD DS e movido os controladores de domínio para os sites apropriados.

O verificador de consistência do conhecimento cria automaticamente objetos de conexão para RODCs. Mas se você estiver tendo problemas, use a ferramenta de linha de comando Repadmin.exe para forçar o verificador de consistência do conhecimento a gerar novamente a topologia. Use o seguinte procedimento de alto nível:

1. Adicione o site com o RODC a um link do site e verifique se o link do site selecionado também contém um site com um controlador de domínio gravável.

2. Force a replicação da partição de configuração no RODC usando Repadmin.exe.

3. Gere novamente a topologia de replicação usando repadmin / kcc no RODC.

Atualizar a replicação SYSVOL para replicação do sistema de arquivos distribuídos.

As pastas SYSVOL residem na pasta% SystemRoot% \ SYSVOL em todos os controladores de domínio e contêm scripts de logon e Modelos de Diretiva de Grupo. Nas versões anteriores do Windows Server, o AD DS usa o Serviço de Replicação de Arquivos (FRS) para sincronizar o conteúdo da pasta SYSVOL entre os controladores de domínio.

No Windows Server 2008 e versões mais recentes, você usa a Replicação DFS (DFSR) para gerenciar a replicação SYSVOL, substituindo a infraestrutura de replicação FRS. O DFSR fornece um meio mais eficiente e confiável para replicar o SYSVOL.

Se você atualizou seus controladores de domínio do Windows Server 2003, é possível que eles ainda podem estar usando o FRS para replicar o SYSVOL. Você pode verificar isso usando a ferramenta de linha de comando Dfsrmig.exe da seguinte maneira:

1. Abra um prompt de comando elevado.

2. Execute o comando Dfsrmig.exe / GetGlobalState.

Se a mensagem retornada for Status global atual do DFSR: 'Eliminado', sua replicação do SYSVOL já está usando o DFSR. Se você receber a mensagem A migração DFSR ainda não foi inicializada, você deve migrar para o DFSR. Durante a migração, a configuração se move por quatro fases ou estados:

Estado 0 Este é o estado inicial. O FRS está sendo usado para replicar o SYSVOL.

Estado 1 O estado preparado. O FRS continua a replicar o SYSVOL, no entanto, o local O serviço DFSR cria uma cópia replicada do SYSVOL.

Estado 2 O estado redirecionado. O DFSR começa a replicar o SYSVOL e o FRS mantém apenas uma réplica local do SYSVOL.

Estado 3 O estado eliminado. O FRS não é mais usado e o DFSR fornece todo o SYSVOL replicação.

Use o procedimento a seguir para migrar a replicação SYSVOL para o DFSR:

1. No prompt de comando, execute dfsrmig / setglobalstate 1. Em seguida, execute o comando Dfsrmig.exe / GetMigrationState para verificar se todos os controladores de domínio atingiram o estado preparado.

2. No prompt de comando, execute dfsrmig / setglobalstate 2. Em seguida, execute o comando Dfsrmig.exe / GetMigrationState para verificar se todos os controladores de domínio atingiram o estado redirecionado.

3. No prompt de comando, execute dfsrmig / setglobalstate 3. Em seguida, execute o comando Dfsrmig.exe / GetMigrationState para verificar se todos os controladores de domínio atingiram o estado eliminado.

4. Em cada controlador de domínio, abra o console de Serviços e verifique se o Serviço de Réplica de Arquivos está desabilitado.

8. CONCLUSÃO

Nos dias de hoje expande a imposição de uma rede mais segura e uma melhor gestão para os usuários de uma rede. Apesar disso, com o crescimento na dimensão das redes e as insistentes mudanças pelas quais as redes passam, os usuários passaram a precisar de um serviço que aprovasse um acesso transparente aos recursos da rede. Dessa forma nasce a necessidade de se trabalhar com uma base de dados centralizados, para uma melhor gestão da rede de computadores.

Com este trabalho, apresentamos as vantagens do Serviço de Domínio do Active Directory permitindo um gerenciamento centralizado das relações entre os recursos de uma rede de computadores. Isto é importante para as organizações, oferecendo segurança, redução de custos e melhorando a funcionalidade almejada. Por isso, o serviço do active directory oferece espaço singular para o gerenciamento dos usuários, grupos e recursos de rede, bem como distribuir software e administrar configurações da área de trabalho.

O tema deste trabalho preserva a imagem do profissional formado em Redes de Computadores que atua desenvolvendo soluções baseadas em redes, planejando e definindo a topologia dos recursos de comunicação de dados, projetando, implementando, protegendo e administrando redes de computadores. Assegurando a gestão tecnológica alinhada com as necessidades de negócios, com vistas a otimização dos recursos existentes e a garantia da qualidade dos serviços

de rede. Por tanto, é de grande importância para os alunos e profissionais possuírem o conhecimento do serviço do active diretory.

Partindo do objetivo de analisar os impactos da usabilidade do active directoty dentro das corporações utilizamos o AD, passou a ser obrigatório um login e uma senha para cada usuário. O AD forneceu serviços de segurança forte e consistente que são essenciais às redes incorporadas. Como o gerenciamento de autenticação de usuário e controle. O administrador atribui as permissões ao grupo e usuário, foram definidas políticas para o grupo de usuários, de acordo com o seu perfil. Essas políticas podem ser aplicadas ou removidas para cada grupo de usuários.

A principal contribuição deste trabalho foi apresentar uma solução tecnológica advinda da Microsoft Corporation através do Windows Server, aperfeiçoando o processo de gestão de uma rede de computadores através da implementação do Active Directory influenciando o comportamento positivo dos usuários da rede.

Conforme aplicações de nosso trabalho, podemos constar que poderão ser realizadas outras tarefas, por exemplo:

- Criar e gerenciar objetos de Diretiva de Drupo.
- Definir configurações de Diretiva de Grupo.
- Configurar preferências de Diretiva de Grupo.
- Implementar o Active Directory Serviços de Certificados.
- Gerenciar modelos de certificado.
- Implementar identidade federação e acesso soluções.
- Instale e configure o AD RMS.

REFERÊNCIA

Allen, R., & Lowe-Norris, A. (2003). *Diretório Ativo.* Califórnia: O´Reilly Media.

Desmond, B. (2008). *Active Directory: Projetando e executando o Active Diretory.* Califórnia: O´Reilly Media.

Docs, M. (10 de 3 de 209). *Active Directory Domain Services*. Fonte: microsoft: https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/ad-ds-getting-started

Microsoft. (16 de 10 de 2008). *Microsoft*. Fonte: Windows Server - Active Directory: http: // www. microsoft. com / windowsserver2003 / technologies / directory / activeedirectory / default. mspx

Microsoft. (18 de 04 de 2019). *Microsoft*. Fonte: Active Directory Domain Services: https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-

Microsoft. (18 de 04 de 2019). *Microsoft*. Fonte: Microsoft: https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/deploy/upgrade-domain-controllers

Santos, A., & Camara, F. (2002). *Implantando o Active Directory.* Florianópolis: Visual Books.

Thompson, M. (2003). *Windows Server 2003: Administração de Redes.* São Paulo: Érica.

Warren, A. (2017). *Identidade com o Windows Server 2016 Ref 70-742.* Seattle: Pearson Education.